Les coefficients de Fourier de la forme modulaire Δ: La fonction de Ramanujan $\tau(n)$

Travail de semestre
présenté au Département de Mathématiques
de l'École Polytechnique Fédérale de Lausanne
sous la direction du Prof. A. Wohlhauser
Hiver 1996-97

Daniel A. Steffen
DMA EPFL
daniel.steffen@dma.epfl.ch

21 août 1998

Résumé

Ce travail décrit le développement d'une expression permettant de calculer la fonction de Ramanujan $\tau(n)$ en l'exprimant comme le coefficient de Fourier de la forme modulaire Δ.

Le travail se base en grande partie sur un cours suivi chez le Prof. H. W. Burmann à l'université de Göttingen en hiver 1996.

En introduction sont donnés un certain nombre de résultats sans démonstration sur la théorie des fonctions et des formes modulaires. Ces derniers sont montrés dans le manuscrit de Burmann [1] ou chez Serre [2].

Le développement exposé en deuxième partie suit dans les grandes lignes le cours de Burmann, bien que les démonstrations présentées ici soient souvent différentes.

En conclusion sont démontrés quelques résultats de théorie des nombres découlant de théorèmes élaborés en deuxième partie.

Table des matières

1 Introduction

1.1 Le groupe modulaire Γ

Définition 1.1.1. Le *groupe spécial linéaire du deuxième ordre* sur les nombres entiers $SL(2,\mathbb{Z})$ ($= \Gamma_H =$ groupe modulaire homogène) a les éléments

$$\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \text{ avec } a,b,c,d \in \mathbb{Z}, ad-bc=1$$

Définition 1.1.2. Le *groupe modulaire (inhomogène)* Γ est le groupe des transformations rationnelles linéaires $LF(2,\mathbb{Z})$ de $\mathbb{C}$ dans $\mathbb{C}$:

$$\tau \mapsto \frac{a\tau+b}{c\tau+d} \text{ avec } a,b,c,d \in \mathbb{Z}, ad-bc=1$$

– Γ est isomorphe à $SL(2,\mathbb{Z})/\{I;-I\}$ où $I = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$.
– Soit $\overline{\mathbb{C}} = \mathbb{C} \cup \{i\infty\}$ la sphère riemannienne. Les éléments de Γ sont des applications bijectives de $\overline{\mathbb{C}}$ dans $\overline{\mathbb{C}}$.

Définition 1.1.3. La relation d'équivalence $\sim$ sur $\overline{\mathbb{C}}$ est définie comme suit:

$$\tau,\tau' \in \overline{\mathbb{C}} : \tau' \sim \tau \iff \exists M \in \Gamma \text{ tel que } \tau' = M\tau$$

On dira que τ,τ' sont *équivalents sous* Γ si $\tau' \sim \tau$.

Définition 1.1.4. Soit $\mathcal{H} = \{\tau \in \mathbb{C} \mid \operatorname{Im}\tau > 0\}$ et $\mathcal{H}^* = \mathcal{H} \cup \{i\infty\}$.
Un *domaine fondamental* de Γ est un sous-ensemble E de $\mathcal{H}^*$ qui contient un et un seul point de chaque classe d'équivalence de $\mathcal{H}^*/\sim$ et dont l'intérieur $\mathring{E}$ ne contient aucun point τ avec $M\tau = \tau, M \in \Gamma \setminus \{I\}$.

– L'ensemble

$$\Omega = \Omega_1 \cup \{i\infty\} \cup \Omega_2 = \{\tau \in \mathcal{H}^* \mid -\frac{1}{2} \le \operatorname{Re}\tau \le 0,\ |\tau| \ge 1\} \cup \\ \{i\infty\} \cup \{\tau \in \mathcal{H}^* \mid 0 < \operatorname{Re}\tau < \frac{1}{2},\ |\tau| > 1\} \quad (1.1.1)$$

est un domaine fondamental de Γ, il est appelé le *domaine fondamental standard* de Γ. Chaque moitié de Ω est un triangle sur la sphère riemannienne $\overline{\mathbb{C}}$ avec les coins i , $i\infty$ et ρ resp. $-\rho^2$, où $\rho = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$.

1.2 Les fonctions modulaires

Définition 1.2.1. Une fonction $f : \mathcal{H}^* \to \overline{\mathbb{C}}$ est une *fonction modulaire* si elle satisfait les conditions suivantes:

1. f est méromorphe dans $\mathcal{H}$.
2. Invariance sous transformation modulaire:

$$f(M\tau) = f(\tau) \quad \forall M \in \Gamma,\ \forall \tau \in \mathcal{H}^*$$

3. $\exists \eta > 0$ tel que $f(\tau)$ peut être représenté pour $\operatorname{Im} \tau > \eta$ sous la forme:

$$f(\tau) = \sum_{n=m}^{\infty} a_n e^{2\pi i n \tau} \qquad \text{avec } m \in \mathbb{Z},\ a_n \in \mathbb{C} \tag{1.2.1}$$

- Si la condition 3. est satisfaite, alors on dit que f est *méromorphe à l'infini*. Une fonction modulaire est donc méromorphe dans tout $\mathcal{H}^*$.
- Par 2. on a $f(\tau + 1) = f(\tau)$, i.e. f est périodique de période 1. Par conséquent, si $f(\tau)$ est holomorphe pour $\operatorname{Im} \tau > \eta$, on sait que le développement de Fourier (1.2.1) existe.
- Grâce à la périodicité, on peut poser $q = e^{2\pi i \tau}$, (1.2.1) devient alors le développement de Laurent suivant:

$$f(\tau) = \sum_{n=m}^{\infty} a_n q^n \qquad \text{avec } m \in \mathbb{Z},\ a_n \in \mathbb{C}$$

- Par $F(q) = f(\frac{1}{2\pi i} \log q)$, $\quad 0 < |q| < 1$, on définit une fonction méromorphe F. La condition 3. signifie que F a au plus un pôle en 0. Son développement de Laurent autour de 0 est $f(\tau) = \sum_{n=m}^{\infty} a_n q^n$.

1.2.1 L'ordre d'une fonction modulaire

Soit $f(\tau) \not\equiv 0$ une fonction modulaire et $\tau_0 \in \mathcal{H}$. Dans un voisinage approprié de τ_0, $f(\tau)$ peut être écrite comme

$$f(\tau) = \sum_{n=m(\tau_0)}^{\infty} a_n(\tau_0) \left(\frac{\tau - \tau_0}{\tau - \overline{\tau_0}} \right)^n \qquad \text{avec } a_{m(\tau_0)} \neq 0$$

où $m(\tau_0) \in \mathbb{Z}$ et $a_n(\tau_0) \in \mathbb{C}$ sont déterminés de façon univoque par τ_0 et f.

Si $\tau_0 \nsim i$ et $\tau_0 \nsim \rho$, alors $|m(\tau_0)|$ est l'ordre de f en τ_0 mesuré dans la variable $(\tau - \tau_0)$. (Il s'agit de l'ordre du zéro si $m(\tau_0) > 0$ et l'ordre du pôle si $m(\tau_0) < 0$).

Définition 1.2.2. L'*ordre σ_f de f en $\tau_0 \in \mathcal{H}$* est défini comme:

$$\sigma_f(\tau_0) = \begin{cases} m(\tau_0) & \text{si } \tau_0 \nsim i, \rho \\ \frac{1}{2} m(\tau_0) & \text{si } \tau_0 \sim i \\ \frac{1}{3} m(\tau_0) & \text{si } \tau_0 \sim \rho \end{cases}$$

L'*ordre du zéro* n_f resp. l'*ordre du pôle* p_f *en* $\tau_0 \in \mathcal{H}$ est:

$$n_f(\tau_0) = \begin{cases} \sigma_f(\tau_0) & \text{si } \sigma_f(\tau_0) \geq 0 \\ 0 & \text{si } \sigma_f(\tau_0) < 0 \end{cases}, \quad p_f(\tau_0) = \begin{cases} 0 & \text{si } \sigma_f(\tau_0) \geq 0 \\ -\sigma_f(\tau_0) & \text{si } \sigma_f(\tau_0) < 0 \end{cases}$$

– Pour évaluer l'ordre de $f(\tau)$ en $i\infty$, on détermine l'ordre de $F(q)$ en 0. On a ainsi défini l'ordre de f en $\tau_0 \ \ \forall \tau_0 \in \mathcal{H}^*$.

Définition 1.2.3. L'*ordre* de la fonction modulaire $f(\tau)$ est

$$N_f = \sum_{\tau_0 \in \Omega} n_f(\tau_0) = \sum_{\tau_0 \in \Omega} p_f(\tau_0) = P_f$$

Il s'agit du nombre de zéros N_f de f en Ω (en tenant compte de leur multiplicité) qui est égal au nombre de pôles P_f de f en Ω (en tenant compte de leur multiplicité).

– La somme ci-dessus a un sens, car une fonction modulaire $f(\tau)$ n'a qu'un nombre fini de zéros dans Ω. En effet, la fonction méromorphe $F(q)$ correspondante n'a pas de zéros dans un voisinage de 0 choisi suffisamment petit, donc $f(\tau) \neq 0$ pour $\operatorname{Im} \tau > \eta$ avec η suffisamment grand. De plus le nombre de zéros dans le compact $\Omega_\eta = \{\tau \in \Omega, \operatorname{Im} \tau \leq \eta\}$ est fini vu que f est méromorphe.

On pose $i\infty$ comme la valeur d'une fonction modulaire dans ses pôles.

Théorème 1.2.4. *Une fonction modulaire non constante f d'ordre N_f prend toute valeur $c \in \overline{\mathbb{C}}$ le même nombre N_f de fois en parcourant Ω.*

Conséquences:

– $N_f = 0 \iff f = \text{constante} \neq 0$, i.e. une fonction modulaire sans zéros ou sans pôles est constante
– Si deux fonctions modulaires f et g ont les mêmes zéros et pôles (y compris leurs multiplicités), alors $f = c \cdot g$ avec $c \in \mathbb{C}$.
– Pour une fonction modulaire non constante f et $M \in \Gamma$, on a $N_{Mf} = N_f$.

1.2.2 L'invariante modulaire absolue J

Pour montrer l'existence des formes modulaires, on s'intéresse aux fonctions modulaires d'ordre 1; elles ont la propriété suivante:

Si on trouve une seule fonction modulaire d'ordre 1, on peut obtenir toutes les autres fonctions modulaires d'ordre 1 par le résultat suivant:

Lemme 1.2.5. *Soit f une fonction modulaire d'ordre 1. Si g est une fonction modulaire d'ordre 1, alors $\exists M \in \Gamma$ tel que $g = Mf$.*

On construit par la suite la fonction modulaire J d'ordre 1 en utilisant plusieurs résultats:

Théorème 1.2.6 (Théorème de Riemann et extension). *$\exists f$ une application bijective et holomorphe qui envoie un domaine simplement connexe $G \subsetneq \mathbb{C}$ sur le disque unité $D = \{\tau \in \mathbb{C} \mid |\tau| < 1\}$. Si G est un triangle sphérique borné $\triangle_0$, alors f peut être prolongée en un homéomorphisme $f : \overline{\triangle_0} \to \overline{D}$*

Théorème 1.2.7 (Principe de réflexion de Schwarz). *(Cas particulier) Soit G un disque ouvert centré en un point de l'axe imaginaire. Soit $f(\tau)$ holomorphe sur $G \cap \{\tau \in \mathbb{C} \mid \operatorname{Re}\tau < 0\}$, continue sur $G \cap \{\tau \in \mathbb{C} \mid \operatorname{Re}\tau \leq 0\}$ et à valeurs réelles sur $G \cap \{\tau \in \mathbb{C} \mid \operatorname{Re}\tau = 0\}$. Alors f peut être prolongée en une fonction holomorphe sur G par*

$$f(\tau) = \overline{f(-\overline{\tau})} \textit{ pour } \tau \in G \cap \{\tau \in \mathbb{C} \mid \operatorname{Re}\tau > 0\}$$

Appliquons la transformation $L_0(\tau) = \frac{1}{\tau}$ à $\triangle = \overset{\circ}{\Omega}_1$ où Ω_1 est comme dans (1.1.1). L'image $\triangle_0 = L_0\triangle$ est un triangle sphérique borné. Par le théorème 1.2.6 il existe alors une application $f : \triangle_0 \to D$ holomorphe et homéomorphe sur les bords.

Soit $L_1 \in LF(2, \mathbb{R})$ l'application holomorphe transformant D en $\mathcal{H}$ choisie de la façon que l'on ait pour la fonction $J : \overline{\triangle} \to \mathcal{H}^*$ avec $J(\tau) = L_1(f(L_0(\tau)))$ les valeurs suivantes: $J(\rho) = 0$, $J(i) = 1$, $J(i\infty) = \infty$. J envoie donc le bord de $\triangle$ sur l'axe réel de façon homéomorphe.

En utilisant le principe de réflexion de Schwarz on prolonge J à Ω et obtient ainsi une bijection $J : \Omega \to \overline{\mathbb{C}}$ holomorphe à l'intérieur de Ω.

Prolongeons J à $\mathcal{H}^*$: Soit $\tau \in \mathcal{H}^*$. On sait que $\exists M \in \Gamma$ tel que $\tau = M\tau_0$ pour un $\tau_0 \in \Omega$. Posons $J(\tau) = J(M\tau_0) := J(\tau_0)$.
De cette façon, on a construit une fonction $J : \mathcal{H}^* \to \overline{\mathbb{C}}$ holomorphe en $\mathcal{H}$.

Lemme 1.2.8. *J est une fonction modulaire d'ordre 1. J est appelée invariante modulaire absolue.*

En effet, on a par construction:
– J est méromorphe sur $\mathcal{H}$
– $J(M\tau) = J(\tau) \quad \forall M \in \Gamma,\ \forall \tau \in \mathcal{H}^*$
et le développement $J(\tau) = \sum_{n=m}^{\infty} a_n e^{2\pi i n\tau}$ converge si $\operatorname{Im}\tau > 0$ par holomorphie de J.

De plus, pour $\tau \in \mathring{\Omega}$, on a $J'(\tau) \neq 0$ par injectivité de J. Par suite la multiplicité de J en τ est 1 et la valeur $J(\tau)$ n'est pas atteinte à un autre endroit de Ω que τ. Ainsi l'ordre de J est 1.

En conclusion, on dispose maintenant de toutes les fonctions modulaires d'ordre 1 en appliquant le lemme 1.2.5 à J.

1.3 Les formes modulaires

Définition 1.3.1. Soit $k \in \mathbb{Z}$, une fonction $f : \mathcal{H}^* \to \overline{\mathbb{C}}$ est une *forme modulaire de poids* k si elle satisfait les conditions suivantes:

1. f est méromorphe dans $\mathcal{H}$.
2. Comportement sous transformation modulaire:

$$f(M\tau) = (c\tau + d)^k f(\tau) \quad \forall M = \frac{a\tau + b}{c\tau + d} \in \Gamma,\ \forall \tau \in \mathcal{H}^*$$

3. $\exists \eta > 0$ tel que $f(\tau)$ peut être représentée pour $\operatorname{Im}\tau > \eta$ sous la forme suivante (avec $q = e^{2\pi i \tau}$):

$$f(\tau) = \sum_{n=m}^{\infty} a_n q^n \qquad \text{avec } m \in \mathbb{Z},\ a_n \in \mathbb{C} \tag{1.3.1}$$

- Par 2. on a $f(\tau + 1) = f(\tau)$, i.e. f est périodique de période 1. Alors $F(q) = f(\frac{1}{2\pi i}\log q)$, $\quad 0 < |q| < 1$, est bien définie et une fonction méromorphe. La condition 2. signifie que F a au plus un pôle en 0. On dit que f est *méromorphe à l'infini*.
- Une forme modulaire de poids 0 est une fonction modulaire.
- Si k est impair, $f(\tau) \equiv 0$ est la seule fonction qui remplit la condition 2, en effet, $f(M\tau) = (c\tau + d)^k f(\tau) = (-c\tau - d)^k f(\tau) \quad \forall M \in \Gamma$, donc soit k est pair, soit $f \equiv 0$. On prendra dorénavant toujours k pair.
- Observons que

$$\frac{dM}{d\tau} = \frac{a(c\tau + d) - c(a\tau + b)}{(c\tau + d)^2} = \frac{(ac\tau - ac\tau) + (ad - bc)}{(c\tau + d)^2} = \frac{1}{(c\tau + d)^2}$$

De ce fait, la condition 2. peut être écrite comme:

$$f(M\tau) = \left(\frac{dM}{d\tau}\right)^{-\frac{k}{2}} f(\tau) \quad \forall M \in \Gamma,\ \forall \tau \in \mathcal{H}^*$$

– Les formes modulaires de poids k forment un $\mathbb{C}$-espace vectoriel.
– Soit deux formes modulaires f et g de poids k resp. l. Le poids du produit fg est $k+l$; si $g \not\equiv 0$, le poids de $\frac{f}{g}$ est $k-l$. Ainsi, le quotient de deux formes modulaires non nulles de même poids est une fonction modulaire.

1.3.1 L'ordre d'une forme modulaire

Soit $f(\tau) \not\equiv 0$ une forme modulaire de poids k et $\tau_0 \in \mathcal{H}$. Dans un voisinage approprié de τ_0, $f(\tau)$ peut être écrite comme

$$f(\tau) = \frac{(\tau_0 - \overline{\tau_0})^{\frac{k}{2}}}{(\tau - \overline{\tau_0})^k} \sum_{n=m(\tau_0)}^{\infty} a_n(\tau_0) \left(\frac{\tau - \tau_0}{\tau - \overline{\tau_0}}\right)^n \qquad \text{avec } a_{m(\tau_0)} \neq 0$$

où $m(\tau_0) \in \mathbb{Z}$ et $a_n(\tau_0) \in \mathbb{C}$ sont déterminés de façon univoque par τ_0 et f.

Définition 1.3.2. L'*ordre* σ_f *de la forme modulaire* f *de poids* k *en* $\tau_0 \in \mathcal{H}^*$ est défini comme:

$$\sigma_f(\tau_0) = \begin{cases} m(\tau_0) & \text{si } \tau_0 \nsim i, \rho \\ \frac{1}{2}m(\tau_0) & \text{si } \tau_0 \sim i \\ \frac{1}{3}m(\tau_0) & \text{si } \tau_0 \sim \rho \\ m(i\infty) & \text{si } \tau_0 = i\infty \end{cases}$$

L'*ordre du zéro* n_f resp. l'*ordre du pôle* p_f *en* $\tau_0 \in \mathcal{H}^*$ est:

$$n_f(\tau_0) = \begin{cases} \sigma_f(\tau_0) & \text{si } \sigma_f(\tau_0) \geq 0 \\ 0 & \text{si } \sigma_f(\tau_0) < 0 \end{cases}, \quad p_f(\tau_0) = \begin{cases} 0 & \text{si } \sigma_f(\tau_0) \geq 0 \\ -\sigma_f(\tau_0) & \text{si } \sigma_f(\tau_0) < 0 \end{cases}$$

Définition 1.3.3. Soit $f(\tau) \not\equiv 0$ une forme modulaire de poids k. Il n'y a qu'un nombre fini de $\tau_0 \in \Omega$ avec $\sigma_f(\tau_0) \neq 0$. On peut donc définir:

1. L'*ordre* ou *nombre de zéros en* Ω de f:

$$N_f = \sum_{\tau_0 \in \Omega} n_f(\tau_0)$$

2. Le *nombre de pôles en* Ω de f:

$$P_f = \sum_{\tau_0 \in \Omega} p_f(\tau_0)$$

Théorème 1.3.4. *Pour une forme modulaire $f(\tau) \not\equiv 0$ de poids k on a:*

$$N_f - P_f = \frac{k}{12}$$

Théorème 1.3.5. *$J'(\tau)$ est une forme modulaire de poids 2 avec*

$$\sigma_{J'}(\tau_0) = \begin{cases} 0 & si\ \tau_0 \nsim i, \rho \\ \frac{1}{2} & si\ \tau_0 \sim i \\ \frac{2}{3} & si\ \tau_0 \sim \rho \\ -1 & si\ \tau_0 = i\infty \end{cases}$$

$$N_{J'} = \frac{7}{6};\ P_{J'} = -1$$

1.4 Les formes modulaires entières

Définition 1.4.1. Une forme modulaire sans pôles dans $\mathcal{H}^*$ s'appelle *forme modulaire entière*. Il s'agit d'une fonction holomorphe partout dans $\mathcal{H}^*$.

– Pour une fonction modulaire entière f de poids k, on a $N_f = \frac{k}{12}$ car $P_f = 0$.

Théorème 1.4.2. *Les formes modulaires entières forment un $\mathbb{C}$-espace vectoriel $\mathcal{M}_k$ de dimension finie. On a $\mathcal{M}_0 = \mathbb{C}$, et pour $k < 0$ et $k = 2$, $\mathcal{M}_k = \{0\}$. En général, $\forall k \in \mathbb{Z}$ on a:*

$$\dim(\mathcal{M}_k) \leq \left[\frac{k}{12}\right] + 1 \tag{1.4.1}$$

Démonstration.

1. Soit $f \in \mathcal{M}_k$, pour $f \not\equiv 0$, on a $N_f \geq 0$, donc $k \geq 0$ par le fait ci-dessus. Alors $\mathcal{M}_k = \{0\}$ pour $k < 0$.
2. Une fonction modulaire sans pôles est une fonction constante, ainsi $\mathcal{M}_0 = \mathbb{C}$.
3. Supposons $f \in \mathcal{M}_0$ et $f \not\equiv 0$. On sait que $N_f = \frac{1}{6}$, donc pour certains $r, s, t \in \mathbb{N}_0$, on aurait $\frac{1}{6} = \frac{r}{3} + \frac{s}{2} + t$, i.e. $1 = 2r + 3s + 6t$. Comme cette équation n'a pas de solutions entières positives, on a $\mathcal{M}_2 = \{0\}$.
4. Soient $k \geq 4$ et $f \in \mathcal{M}_k$ avec développement de Fourier $f(\tau) = \sum_{n=m}^{\infty} a_n q^n$. Posons $h = \left[\frac{k}{12}\right] + 1$. L'application $\phi : \mathcal{M}_k \to \mathbb{C}^h$ définie par $f \mapsto (a_0, a_1, \ldots, a_{h-1})$ est un homomorphisme de $\mathbb{C}$-espaces

vectoriels de noyau nul. En effet, si $a_0 = a_1 = \cdots = a_{h-1} = 0$ et $f \not\equiv 0$, alors on aurait $n_f(i\infty) \geq h = \left[\frac{k}{12}\right] + 1$. Mais $n_f(i\infty) \leq N_f = \frac{k}{12}$. Ainsi, ϕ est injective et donc $\dim(\mathcal{M}_k) \leq h$.

□

– Vu le résultat précédent, on ne traitera par la suite plus que des $\mathcal{M}_k$ avec k pair et $k \geq 4$.

Définition 1.4.3. Une forme modulaire entière qui devient nulle en $i\infty$ s'appelle *forme cuspidale* ou *forme parabolique* (Spitzenform, cusp form).

– Une forme modulaire entière f est une forme cuspidale si et seulement si son développement de Fourier a la forme suivante:

$$f(\tau) = \sum_{n=1}^{\infty} a_n q^n \qquad \text{avec } a_n \in \mathbb{C}$$

– Les formes cuspidales forment un sous-espace vectoriel $\mathcal{S}_k$ de $\mathcal{M}_k$. On a $\dim(\mathcal{M}_k) - 1 \leq \dim(\mathcal{S}_k) \leq \dim(\mathcal{M}_k)$

1.4.1 Le discriminant Δ

Définition 1.4.4. Soient les deux formes modulaires

$$\begin{aligned} E_4 &= \frac{1}{(2\pi i)^2} \frac{J'^2}{J(J-1)} \\ E_6 &= -\frac{1}{(2\pi i)^3} \frac{J'^3}{J^2(J-1)} \end{aligned}$$

– E_4 et E_6 sont des formes modulaires entières de poids 4 resp. 6.
– $E_4(i\infty) = E_6(i\infty) = 1$.
– Les $\tau \sim \rho$ sont des zéros d'ordre $\frac{1}{3}$ de E_4.
– Les $\tau \sim i$ sont des zéros d'ordre $\frac{1}{2}$ de E_6.

Théorème 1.4.5. *Soit* $k = 4, 6, 8, \ldots$ *et* $k = 4m + 6n$ *avec* $m, n \in \mathbb{N}_0$. *Alors* $E_4^m E_6^n$ *est une forme modulaire entière de poids* k *et de valeur 1 en* $i\infty$. *Aussi* $\dim(\mathcal{M}_k) \geq 1$ *et donc* $\dim(\mathcal{S}_k) = \dim(\mathcal{M}_k) - 1$.

– Par (1.4.1), on a que $\dim(\mathcal{M}_k) = 1$ pour $k \in \{4, 6, 8, 10\}$.
– $E_4^2 E_6$ est une base de $\mathcal{M}_{14}$ et donc $\dim(\mathcal{M}_{14}) = 1$

Théorème 1.4.6. *Pour* $k \in \{4, 6, 8, 10, 14\}$, *on a* $\dim(\mathcal{M}_k) = 1$ *et les bases pour les espaces* $\mathcal{M}_k$ *sont les suivantes:*

Espace	*Base*
$\mathcal{M}_4$	E_4
$\mathcal{M}_6$	E_6
$\mathcal{M}_8$	E_4^2
$\mathcal{M}_{10}$	E_4E_6
$\mathcal{M}_{14}$	$E_4^2E_6$

Définition 1.4.7. Soit la forme modulaire

$$\Delta = \frac{(2\pi)^{12}}{12^3}\left(E_4^3 - E_6^2\right) = -\frac{(2\pi)^6}{1728}\frac{J'^6}{J^4(J-1)^3}$$

Δ est appelée *discriminant*, car à un facteur numérique prés, elle est égale au discriminant du polynôme $x^3 - \frac{\pi^4}{3}E_4x - \frac{2\pi^6}{27}E_6$ dans la théorie des courbes elliptiques.

- Δ est une forme cuspidale de poids 12. Δ ne s'annule pas sur $\mathcal{H}$ et a un zéro simple en $i\infty$.
- Ainsi $\dim(\mathcal{S}_{12}) = 1$ et donc $\dim(\mathcal{M}_{12}) = 2$. $\{\Delta, E_6^2\}$ est une base de $\mathcal{M}_{12}$.

Théorème 1.4.8. *Pour* $k = 4, 6, 8, \dots$ *on a*

$$\dim(\mathcal{M}_k) = \begin{cases} \left[\frac{k}{12}\right] + 1 & si\ k \not\equiv 2 \pmod{12} \\ \left[\frac{k}{12}\right] & si\ k \equiv 2 \pmod{12} \end{cases}$$

$$\dim(\mathcal{S}_k) = \begin{cases} \left[\frac{k}{12}\right] & si\ k \not\equiv 2 \pmod{12} \\ \left[\frac{k}{12}\right] - 1 & si\ k \equiv 2 \pmod{12} \end{cases}$$

1.5 La fonction ζ de Riemann

Définition 1.5.1. La *fonction zêta de Riemann* est définie comme suit:

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} \quad \text{avec } s \in \mathbb{C}, \mathrm{Re}(s) > 1$$

Définition 1.5.2. Les *nombres de Bernoulli* B_k sont définis par le développement en série:

$$\frac{x}{e^x - 1} = \sum_{n=0}^{\infty} \frac{B_n}{n!} x^n$$

– Les premières valeurs de B_k sont: ($B_k = 0$ pour k impair)

$$B_2 = \frac{1}{6}, B_4 = -\frac{1}{30}, B_6 = \frac{1}{42}, B_8 = -\frac{1}{30}, B_{10} = \frac{5}{66}, B_{12} = -\frac{691}{2730}, \ldots$$

Théorème 1.5.3. *Pour* $k = 2, 4, 6, \ldots$ *on a*

$$\zeta(k) = \frac{(2\pi)^k}{2(k!)} |B_k| = (-1)^{(1+\frac{k}{2})} \frac{(2\pi)^k}{2(k!)} B_k$$

– En utilisant les valeurs de B_k ci-dessus, on obtient:

$$\zeta(2) = \frac{\pi^2}{6},\ \zeta(4) = \frac{\pi^4}{90},\ \zeta(6) = \frac{\pi^6}{945},\ \zeta(8) = \frac{\pi^8}{9450},$$
$$\zeta(10) = \frac{\pi^{10}}{93555},\ \zeta(12) = \frac{691\pi^{12}}{638512875}, \ldots$$

2 Développements de Fourier des formes modulaires entières

2.1 Séries d'Eisenstein

Définition 2.1.1. Soit $k \equiv 0 \pmod 2, k \geq 4$, on définit la *série d'Eisenstein d'indice* k comme suit:

$$G_k(\tau) = \sum_{m,n=-\infty}^{\infty}{}' \frac{1}{(m\tau + n)^k} \quad \text{avec } \tau \in \mathcal{H}$$

où le symbole $\sum'$ signifie que la sommation ne porte que sur les couples (m, n) distincts de $(0, 0)$.

Définition 2.1.2. Soient $a, b \in \mathbb{Z}$. Un réseau $\mathcal{G}_\tau$ de $\mathbb{C}$ est un ensemble discret de points de $\mathbb{C}$: $\mathcal{G}_\tau = \{\omega = a\tau + b \mid a, b \in \mathbb{Z}\}$

Lemme 2.1.3. *Soit $\mathcal{G}$ un réseau de $\mathbb{C}$ et $p \in \mathbb{Z}, p > 2$. La série suivante est convergente:*

$$\sum_{\omega \in \mathcal{G}\setminus\{0\}} \frac{1}{|\omega|^p}$$

Démonstration. Choisissons $r > 0$ assez petit pour que les disques fermés $K_r(\omega) = \{\tau \in \mathbb{C} \mid |\tau - \omega| \leq r\}$ soient disjoints deux par deux $\forall \omega \in \mathcal{G}$. Observons maintenant que l'on a les inégalités suivantes pour $\omega \neq 0$:

$$\iint_{K_r(\omega)} \frac{dx\,dy}{(x^2+y^2)^{\frac{p}{2}}} \geq \iint_{K_r(\omega)} \frac{dx\,dy}{\underbrace{\max_{(x,y)\in K_r(\omega)}((x^2+y^2)^{\frac{p}{2}})}_{=(|\omega|+r)^p}} = \frac{\pi r^2}{(|\omega|+r)^p}$$

$$\geq \frac{\pi r^2}{(1 + \frac{r}{\min_{\gamma\in\mathcal{G}}|\gamma|})^p\,|\omega|^p} = \frac{c}{|\omega|^p} \quad \text{où } c \text{ est une constante.}$$

En résumé, on a donc $\forall \omega \in \mathcal{G} \setminus \{0\}$

$$\frac{1}{|\omega|^p} \leq \frac{1}{c} \iint_{K_r(\omega)} \frac{dx\,dy}{(x^2+y^2)^{\frac{p}{2}}} \quad \text{avec } c = \frac{\pi r^2}{(1 + \frac{r}{\min_{\gamma\in\mathcal{G}}|\gamma|})^p} \tag{2.1.1}$$

En utilisant l'inclusion $\bigcup_{\omega\in\mathcal{G}\setminus\{0\}} K_r(\omega) \subset \{\tau \in \mathbb{C} \mid |\tau| \geq r\}$, on tire de (2.1.1) la majoration suivante:

$$\begin{aligned}
\sum_{\omega\in\mathcal{G}\setminus\{0\}} \frac{1}{|\omega|^p} &\leq \frac{1}{c} \sum_{\omega\in\mathcal{G}\setminus\{0\}} \left(\iint_{K_r(\omega)} \frac{dxdy}{(x^2+y^2)^{\frac{p}{2}}} \right) = \frac{1}{c} \iint_{\bigcup_{\omega\in\mathcal{G}\setminus\{0\}} K_r(\omega)} \frac{dxdy}{(x^2+y^2)^{\frac{p}{2}}} \\
&\leq \frac{1}{c} \underbrace{\iint_{\{\tau\in\mathbb{C} \mid |\tau|\geq r\}} \frac{dxdy}{(x^2+y^2)^{\frac{p}{2}}}}_{(*)}
\end{aligned} \tag{2.1.2}$$

L'intégrale $(*)$ se calcule en passant aux coordonnées polaires, i.e. en posant $x = R\cos\phi, y = R\sin\phi$, resp. $R = (x^2+y^2)^{\frac{1}{2}}, \tan(\phi) = \frac{y}{x}$

$$\iint_{\{\tau\in\mathbb{C} \mid |\tau|\geq r\}} \frac{dx\,dy}{(x^2+y^2)^{\frac{p}{2}}} = \int_0^{2\pi} \int_r^{\infty} \frac{1}{R^p} R\,dR\,d\phi = \frac{2\pi}{(p-2)r^{(p-2)}}$$

De (2.1.2), on tire alors le résultat cherché:

$$\sum_{\omega\in\mathcal{G}\setminus\{0\}} \frac{1}{|\omega|^p} \leq \frac{2\pi}{c(p-2)r^{(p-2)}} < \infty$$

$\square$

Théorème 2.1.4. *Soient $\eta > 0, \delta > 0$ et $k \geq 4$. La série $G_k(\tau)$ converge absolument $\forall \tau \in \mathcal{H}$, de plus, elle converge uniformément $\forall \tau \in \{\upsilon \in \mathcal{H} \mid \operatorname{Im}\upsilon \geq \eta, |\operatorname{Re}\upsilon| \leq \delta\}$.*

Démonstration. On a le fait suivant: Si (m,n) parcourt $\mathbb{Z}^2 \setminus \{(0,0)\}$, alors $m\tau+n$ parcourt un réseau $\mathcal{G}_\tau \setminus \{0\}$ de $\mathbb{C}$. Si on pose en outre $\omega = m\tau+n$, on obtient alors par le lemme 2.1.3 la convergence absolue de $\sum'^{\infty}_{m,n=-\infty} \frac{1}{(m\tau+n)^k}$ en $\tau \in \mathcal{H}$.

Pour montrer la convergence uniforme, on pose:

$$B(\tau_0) = \{\tau \in \mathcal{H} \mid |\tau| \geq |\tau_0|, |\operatorname{Re}(\tau)| \leq x_0\} \text{ où } \tau_0 = x_0 + y_0 i \text{ avec } x_0 > 0$$

Pour $\tau \in B(\tau_0)$ et $m, n \in \mathbb{Z}$, on a alors

$$\begin{aligned}
|m\tau+n|^2 &= m^2|\tau|^2 + 2mn\operatorname{Re}(\tau) + n^2 \\
&\leq \begin{cases} m^2|\tau_0|^2 + 2mnx_0 + n^2 & \text{si } mn \leq 0 \\ m^2|\tau_0|^2 - 2mnx_0 + n^2 & \text{si } mn > 0 \end{cases} \\
&= \begin{cases} |m\tau_0+n|^2 & \text{si } mn \leq 0 \\ |m(-\overline{\tau_0})+n|^2 & \text{si } mn > 0 \end{cases}
\end{aligned}$$

D'où la majoration indépendante de τ suivante ($\forall\tau \in B(\tau_0)$):

$$\sum_{m,n=-\infty}^{\infty}{}' \frac{1}{|(m\tau+n)^k|} \leq \sum_{m,n=-\infty}^{\infty}{}' \left(\frac{1}{|m\tau_0+n|^k} + \frac{1}{|m(-\overline{\tau_0})+n|^k}\right)$$

On a donc convergence uniforme pour $\tau \in B(\tau_0)$. En choisissant τ_0 tel que $|\tau_0| \leq \eta$ et $\mathrm{Re}(\tau_0) \geq \delta$, on obtient finalement la convergence uniforme sous les conditions mentionnées en hypothèse. □

2.2 Formes modulaires entières et séries d'Eisenstein

Théorème 2.2.1. *Pour $k \equiv 0 \pmod 2, k \geq 4$, la série $G_k(\tau)$ est une forme modulaire entière de poids k avec $G_k(i\infty) = 2\zeta(k)$, où ζ désigne la fonction zêta de Riemann.*

Démonstration. Soit $M = \frac{a\tau+b}{c\tau+d} \in \Gamma$; pour $\tau \in \mathcal{H}; m, n \in \mathbb{Z}$, on a

$$m\frac{a\tau+b}{c\tau+d} + n = \frac{(am+cn)\tau + (bm+dn)}{c\tau+d}$$

Observons que l'application $\mathbb{Z}^2 \to \mathbb{Z}^2 : (m,n) \mapsto (am+cn, bm+dn) = (m,n)\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ est une bijection, en effet $(m,n) \mapsto (m,n)\left(\begin{smallmatrix} d & -b \\ -c & a \end{smallmatrix}\right)$ est son inverse. De là, si (m,n) parcourt $\mathbb{Z}^2$, alors $((m,n)M)$ fait de même. On peut alors réordonner la suite suivante: (en effet, elle est absolument convergente vu le théorème 2.1.4)

$$\begin{aligned} G_k(M\tau) &= \sum_{(m,n)\in\mathbb{Z}^2}{}' \frac{1}{(m(M\tau)+n)^k} \\ &= \sum_{(m,n)\in\mathbb{Z}^2}{}' \frac{1}{((c\tau+d)^{-1}((am+cn)\tau+(bm+dn)))^k} \\ &= \sum_{((m',n')M^{-1})\in\mathbb{Z}^2}{}' \frac{1}{((c\tau+d)^{-1}(m'\tau+n'))^k} \end{aligned}$$

On obtient alors:

$$\begin{aligned} &= (c\tau+d)^k \sum_{(m',n')\in\mathbb{Z}^2}{}' \frac{1}{(m'\tau+n')^k} \\ &= (c\tau+d)^k G_k(\tau) \end{aligned}$$

En conclusion, G_k soumis à une transformation modulaire a un comportement identique à celui d'une forme modulaire de poids k.

On a l'holomorphie de G_k dans $\mathcal{H}$ par la convergence de $G_k(\tau)$ $\forall \tau \in \mathcal{H}$ du théorème 2.1.4. Il reste à prouver que G_k est holomorphe dans $i\infty$, i.e. que $G_k(\tau)$ a une limite pour $\mathrm{Im}(\tau) \to \infty$. Pour calculer cette limite, on peut restreindre τ à Ω. Alors, grâce à la convergence uniforme de G_k dans Ω du théorème 2.1.4, on peut passer à la limite terme à terme dans

$$\lim_{\substack{\tau\to\infty \\ \tau\in\Omega}} G_k(\tau) = \lim_{\substack{\tau\to\infty \\ \tau\in\Omega}} \left(\sideset{}{'}\sum_{m,n=-\infty}^{\infty} \frac{1}{(m\tau+n)^k} \right) = \sideset{}{'}\sum_{m,n=-\infty}^{\infty} \underbrace{\left(\lim_{\substack{\tau\to\infty \\ \tau\in\Omega}} \frac{1}{(m\tau+n)^k} \right)}_{\substack{=0 \text{ pour } m\neq 0 \\ =\frac{1}{n^k} \text{ pour } m=0}}$$

$$= \sideset{}{'}\sum_{n=-\infty}^{\infty} \frac{1}{n^k} = \sum_{n=-\infty}^{-1} \frac{1}{n^k} + \sum_{n=1}^{\infty} \frac{1}{n^k} = 2\sum_{n=1}^{\infty} \frac{1}{n^k} = 2\zeta(k)$$

Alors G_k est holomorphe dans $\mathcal{H}^*$ et donc une forme modulaire entière. □

Théorème 2.2.2. *Pour $k = 4, 6$, on a les relations suivantes entre les séries d'Eisenstein G_k et les formes modulaires entières E_k définies dans 1.4.4:*

$$E_4 = \frac{1}{2\zeta(4)} G_4, \qquad E_6 = \frac{1}{2\zeta(6)} G_6$$

Démonstration. Par le théorème 2.2.1, on sait que $G_4 \in \mathcal{M}_4$ et $G_6 \in \mathcal{M}_6$. Soit $k \in \{4, 6\}$. On a $\dim(\mathcal{M}_k) = 1$ par le théorème 1.4.2, les G_k sont donc des multiples des bases E_k de $\mathcal{M}_k$. Le théorème 2.2.1 donne en outre la valeur $G_k(i\infty) = 2\zeta(k)$, d'où $\frac{1}{2\zeta(4)} G_4(i\infty) = \frac{1}{2\zeta(6)} G_6(i\infty) = 1$. En utilisant $E_4(i\infty) = E_6(i\infty) = 1$, on obtient alors le résultat. □

Grâce au théorème 2.2.2, on peut poser la définition suivante en accord avec ce qui précède (notamment la définition 1.4.4):

Définition 2.2.3. Soit $k \equiv 0 \pmod 2, k \geq 4$. On appelle *série d'Eisenstein normée* la série

$$E_k = \frac{1}{2\zeta(k)} G_k$$

On a $E_k(i\infty) = 1$.

Corollaire 2.2.4. *Comme conclusion directe aux théorèmes 2.2.2 et 1.4.6 on obtient les relations entre E_k suivantes:*

$$E_8 = E_4^2, \qquad E_{10} = E_4 E_6, \qquad E_{14} = E_4^2 E_6$$

2.2.1 E_k et J écrits comme série

Théorème 2.2.5. *Pour $k = 4, 6, 8, \ldots,$ on a l'expression*

$$E_k(\tau) = \frac{1}{2} \sum_{\mathrm{pgdc}(m,n)=1} \frac{1}{(m\tau + n)^k}$$

Démonstration. On peut écrire

$$\begin{aligned}
G_k(\tau) &= \sideset{}{'}\sum_{m,n=-\infty}^{\infty} \frac{1}{(m\tau+n)^k} \\
&= \sum_{t=1}^{\infty} \left(\sum_{\mathrm{pgdc}(m,n)=t} \frac{1}{(m\tau+n)^k} \right) \\
&= \sum_{t=1}^{\infty} \left(\sum_{\mathrm{pgdc}(m,n)=t} \frac{1}{(t(m'\tau+n'))^k} \right) \text{avec } m' = \frac{m}{t}, n' = \frac{n}{t} \in \mathbb{Z} \\
&= \sum_{t=1}^{\infty} \left(\frac{1}{t^k} \sum_{\mathrm{pgdc}(m',n')=1} \frac{1}{(m'\tau+n')^k} \right) \\
&= \left(\sum_{t=1}^{\infty} \frac{1}{t^k} \right) \left(\sum_{\mathrm{pgdc}(m',n')=1} \frac{1}{(m'\tau+n')^k} \right) \\
&= \zeta(k) \sum_{\mathrm{pgdc}(m,n)=1} \frac{1}{(m\tau+n)^k}
\end{aligned}$$

En utilisant l'expression pour G_k déterminée ci-dessus dans la définition 2.2.3: $E_k = \frac{1}{2\zeta(k)} G_k$, on aboutit immédiatement au résultat cherché. □

Du théorème 2.2.5 on peut déduire une expression pour calculer J, l'invariante modulaire absolue construite de façon purement géométrique dans la partie 1.2.2:

Corollaire 2.2.6. *On a:*

$$J = \frac{\left(\sum_{\mathrm{pgdc}(m,n)=1} \frac{1}{(m\tau+n)^4} \right)^3}{\left(\sum_{\mathrm{pgdc}(m,n)=1} \frac{1}{(m\tau+n)^4} \right)^3 - 2 \left(\sum_{\mathrm{pgdc}(m,n)=1} \frac{1}{(m\tau+n)^6} \right)^2}$$

Démonstration. De la définition 1.4.4 on tire

$$E_4^3 = \frac{1}{(2\pi i)^6} \frac{J'^6}{J^3(J-1)^3} \quad \text{et} \quad E_6^2 = \frac{1}{(2\pi i)^6} \frac{J'^6}{J^4(J-1)^2}$$

On égalise les deux expression pour J'^6 ci-dessus et on déduit une expression pour J:

$$\begin{aligned} E_4^3 J^3 (J-1)^3 &= E_6^2 J^4 (J-1)^2 \qquad \Longleftrightarrow \\ E_4^3 (J-1) &= E_6^2 J \end{aligned}$$

D'où

$$J = \frac{E_4^3}{E_4^3 - E_6^2} \tag{2.2.1}$$

Si on remplace E_4 et E_6 par leur expression en série du théorème 2.2.5, on aboutit immédiatement à la conclusion. □

Corollaire 2.2.7. *On peut exprimer J en fonction de E_4 et Δ:*

$$J = \frac{(2\pi)^{12} E_4^3}{12^3 \Delta}$$

Démonstration. Conséquence immédiate de la définition 1.4.7 et de l'équation 2.2.1. □

2.3 Les coefficients de Fourier de E_k, Δ et J

2.3.1 Développement de Fourier de E_k

Définition 2.3.1. On définit la fonction suivante pour $k \in \mathbb{Z}, k \geq 4$

$$h_k(\tau) = \sum_{n=-\infty}^{\infty} \frac{1}{(\tau+n)^k}$$

Lemme 2.3.2. *Soient $\eta > 0, \delta > 0$ et $k \in \mathbb{Z}, k \geq 4$. La série $h_k(\tau)$ définie ci-dessus converge absolument $\forall \tau \in \mathcal{H}$, de plus elle converge uniformément $\forall \tau \in \{\upsilon \in \mathcal{H} \mid \operatorname{Im} \upsilon \geq \eta, |\operatorname{Re} \upsilon| \leq \delta\}$*

Démonstration. Le théorème 2.1.4 nous dit que la série d'Eisenstein, i.e. $G_k(\tau) = \sum'^{\infty}_{m,n=-\infty} \frac{1}{(m\tau+n)^k}$ converge si τ remplit les conditions énoncés en hypothèse. Comme la série $h_k(\tau)$ est une sous-suite de $G_k(\tau)$ (la sous-suite pour $m = 1$), on obtient immédiatement le résultat. □

Lemme 2.3.3. *Soit $k \in \mathbb{Z}, k \geq 4$. La fonction h_k est holomorphe dans $\mathcal{H}$ et elle est périodique: $h_k(\tau+1) = h_k(\tau)$.*
$\forall \tau \in \mathcal{H}$, le développement de Fourier de h_k est

$$h_k(\tau) = \frac{(-2\pi i)^k}{(k-1)!} \sum_{m=1}^{\infty} m^{k-1} q^m \quad \textit{avec } q = e^{2\pi i \tau}$$

Démonstration. L'holomorphie est donnée par la convergence absolue de h_k $\forall \tau \in \mathcal{H}$ du lemme 2.3.2. La périodicité suit du changement d'indice $l = n+1$ dans

$$h_k(\tau+1) = \sum_{n=-\infty}^{\infty} \frac{1}{(\tau+1+n)^k} = \sum_{l=-\infty}^{\infty} \frac{1}{(\tau+l)^k} = h_k(\tau)$$

Pour calculer la limite de h_k quand $\mathrm{Im}(\tau) \to \infty$, on peut restreindre τ à Ω. Alors, grâce à la convergence uniforme de h_k dans Ω du lemme 2.3.2, on peut passer à la limite terme à terme dans

$$\lim_{\substack{\tau\to\infty \\ \tau\in\Omega}} h_k(\tau) = \lim_{\substack{\tau\to\infty \\ \tau\in\Omega}} \left(\sum_{n=-\infty}^{\infty} \frac{1}{(\tau+n)^k} \right) = \sum_{n=-\infty}^{\infty} \underbrace{\left(\lim_{\substack{\tau\to\infty \\ \tau\in\Omega}} \frac{1}{(\tau+n)^k} \right)}_{=0} = 0$$

L'existence du développement de Fourier de h_k est une conséquence de l'holomorphie et de la périodicité de h_k dans $\mathcal{H}$; suite au calcul de limite ci-dessus, ce développement converge vers h_k partout dans $\mathcal{H}$.
Ainsi on a

$$h_k(\tau) = \sum_{m=-\infty}^{\infty} \alpha_{k,m} e^{2\pi i m\tau} = \sum_{m=-\infty}^{\infty} \alpha_{k,m} q^m \tag{2.3.1}$$

avec

$$\alpha_{k,m} = \int_{iy}^{1+iy} h_k(\tau) e^{-2\pi i m\tau}\, d\tau \quad \text{où } y \in \mathbb{R}, y > 0$$

Vu que h_k converge uniformément pour les valeurs de τ considérées (lemme 2.3.2), on peut permuter somme et intégrale dans le calcul suivant:

$$\begin{aligned} \alpha_{k,m} &= \int_{iy}^{1+iy} \left(\sum_{n=-\infty}^{\infty} \frac{1}{(\tau+n)^k} e^{-2\pi i m\tau} \right) d\tau \\ &= \sum_{n=-\infty}^{\infty} \left(\int_{iy}^{1+iy} \frac{e^{-2\pi i m\tau}}{(\tau+n)^k}\, d\tau \right) \\ &= \sum_{n=-\infty}^{\infty} \left(\int_{n+iy}^{n+1+iy} \frac{e^{-2\pi i m\tau}}{\tau^k}\, d\tau \right) \\ &= \int_{-\infty+iy}^{\infty+iy} \frac{e^{-2\pi i m\tau}}{\tau^k}\, d\tau \end{aligned} \tag{2.3.2}$$

Calculons la valeur de cette dernière intégrale $\int\limits_{-\infty+iy}^{\infty+iy} \frac{e^{i\lambda\tau}}{\tau^k}\, d\tau$, avec $\lambda = -2\pi m$ une constante réelle:

Soient $y, \eta \in \mathbb{R}$ fixés avec $\eta > y > 0$ si $\lambda \geq 0$, et $\eta < 0 < y$ si $\lambda < 0$. On calcule l'intégrale de $\frac{e^{i\lambda\tau}}{\tau^k}$ sur un chemin rectangulaire dans $\mathbb{C}$ qui parcourt les segments $[-x+iy, x+iy]$, $[x+iy, x+i\eta]$, $[x+i\eta, -x+i\eta]$ et $[-x+i\eta, -x+iy]$:

1. La fonction $\frac{e^{i\lambda\tau}}{\tau^k}$ a un unique pôle d'ordre k en 0; donc, si le rectangle ci-dessus entoure 0, on a par le théorème des résidus:

$$\int_{-x+iy}^{x+iy} \frac{e^{i\lambda\tau}}{\tau^k}\, d\tau + \int_{x+iy}^{x+i\eta} \frac{e^{i\lambda\tau}}{\tau^k}\, d\tau + \int_{x+i\eta}^{-x+i\eta} \frac{e^{i\lambda\tau}}{\tau^k}\, d\tau + \int_{-x+i\eta}^{-x+iy} \frac{e^{i\lambda\tau}}{\tau^k}\, d\tau =$$
$$= -2\pi i \operatorname*{Rés}_{\tau=0} \frac{e^{i\lambda\tau}}{\tau^k} = -2\pi i \frac{1}{(k-1)!} \frac{d^{k-1}}{d\tau^{k-1}} \left((\tau-0)^k \frac{e^{i\lambda\tau}}{\tau^k} \right) \bigg|_{\tau=0} =$$
$$= -2\pi i \frac{1}{(k-1)!} \frac{d^{k-1}}{d\tau^{k-1}} \left(e^{i\lambda\tau} \right) \Big|_{\tau=0} = -2\pi i \frac{(i\lambda)^{k-1}}{(k-1)!} \qquad (2.3.3)$$

   Si le rectangle n'entoure pas 0, la valeur de l'intégrale sur le rectangle est nulle.

2. Si $0 < y < \eta$, le rectangle n'entoure pas 0.
   Si $\eta < 0 < y$, le rectangle entoure 0.

3. La valeur de l'intégrale sur les côtés verticaux du rectangle tend vers 0 quand $|x| \to \infty$:

$$\lim_{|x|\to\infty} \left(\int_{x+iy}^{x+i\eta} \frac{e^{i\lambda\tau}}{\tau^k}\, d\tau \right) = 0$$

   En effet, si on suppose que $y < \eta$, alors pour $\tau \in [x+iy, x+i\eta]$, on a la majoration

$$\left| \frac{e^{i\lambda\tau}}{\tau^k} \right| \leq \frac{\left| e^{i\lambda(x+i\eta)} \right|}{|x+iy|^k} = \frac{e^{-\lambda\eta}}{(x^2+y^2)^{\frac{k}{2}}} \leq \frac{C}{|x|^k} \quad \text{avec } C \text{ une constante}$$

   Comme $k \geq 4$, on a $\frac{C}{|x|^k} \to 0$, quand $|x| \to \infty$; d'où la valeur limite 0 de l'intégrale ci-dessus. Pour $\eta < y$, la démonstration est analogue.

4. En passant l'équation (2.3.3) à la limite $x \to \infty$, on obtient:

$$\int_{-\infty+iy}^{\infty+iy} \frac{e^{i\lambda\tau}}{\tau^k}\, d\tau + \int_{\infty+i\eta}^{-\infty+i\eta} \frac{e^{i\lambda\tau}}{\tau^k}\, d\tau =$$
$$= \begin{cases} 0 & \text{si } 0 < y < \eta \\ -2\pi i \frac{(i\lambda)^{k-1}}{(k-1)!} & \text{si } \eta < 0 < y \end{cases} \qquad (2.3.4)$$

5. La deuxième intégrale de (2.3.4) tend vers 0 quand $|\eta| \to \infty$:
   Observons que $\lambda\eta \geq 0$ quelque soient λ, η; alors:

$$\left|\int_{-\infty+i\eta}^{\infty+i\eta} \frac{e^{i\lambda\tau}}{\tau^k}\, d\tau\right| \leq \int_{-\infty+i\eta}^{\infty+i\eta} \frac{\left|e^{i\lambda\tau}\right|}{|\tau|^k}\, d\tau = \int_{-\infty}^{\infty} \frac{\overbrace{\left|e^{i\lambda x}\right|}^{=1}\overbrace{\left|e^{-\lambda\eta}\right|}^{<1}}{(x^2+\eta^2)^{\frac{k}{2}}}\, dx \leq$$

$$\leq \int_{-\infty}^{\infty} \frac{1}{(x^2+\eta^2)^{\frac{k}{2}}}\, dx = \frac{1}{|\eta|^k} \int_{-\infty}^{\infty} \frac{1}{\left(\left(\frac{x}{\eta}\right)^2 + 1\right)^{\frac{k}{2}}}\, dx =$$

$$= \frac{1}{|\eta|^{(k-1)}} \underbrace{\int_{-\infty}^{\infty} \frac{1}{(x^2+1)^{\frac{k}{2}}}\, dx}_{<\infty} \tag{2.3.5}$$

   Si $|\eta| \to \infty$, alors $\frac{1}{|\eta|^{(k-1)}} \to 0$. De 2.3.5 suit par conséquent

$$\lim_{|\eta|\to\infty} \left(\int_{-\infty+i\eta}^{\infty+i\eta} \frac{e^{i\lambda\tau}}{\tau^k}\, d\tau\right) = 0$$

6. En passant l'équation (2.3.4) à la limite $|\eta| \to \infty$, on obtient:

$$\int_{-\infty+iy}^{\infty+iy} \frac{e^{i\lambda\tau}}{\tau^k}\, d\tau = \begin{cases} 0 & \text{si } \lambda \geq 0 \\ -2\pi i \frac{(i\lambda)^{k-1}}{(k-1)!} & \text{si } \lambda < 0 \end{cases}$$

7. Le précédent résultat donne (en remplaçant λ par $-2\pi m$) la valeur de l'expression (2.3.2):

$$\alpha_{k,m} = \begin{cases} 0 & \text{si } m \leq 0 \\ -2\pi i \frac{(-2\pi i m)^{k-1}}{(k-1)!} & \text{si } m > 0 \end{cases}$$

   Au moyen de cette expression on tire de (2.3.1) le résultat cherché:

$$h_k(\tau) = \frac{(-2\pi i)^k}{(k-1)!} \sum_{m=1}^{\infty} m^{k-1} q^m$$

□

Définition 2.3.4. Soit $n \in \mathbb{N}, k \in \mathbb{Z}$. On définit

$$\sigma_k(n) = \sum_{d|n} d^k$$

la somme des k-ièmes puissances de tout les diviseurs de n.
On pose en outre

$$\sigma_k(0) = 0$$

Théorème 2.3.5. *Soit $k \equiv 0 \pmod 2, k \geq 4$ et $\tau \in \mathcal{H}$. Le développement de Fourier de la série d'Eisenstein G_k est:*

$$G_k(\tau) = 2\zeta(k) + 2\frac{(2\pi i)^k}{(k-1)!}\sum_{n=1}^{\infty} \sigma_{k-1}(n) q^n \quad \textit{avec } q = e^{2\pi i \tau}$$

Démonstration. Décomposons la série $G_k(\tau)$ en trois parties, selon que $m < 0$, $m = 0$ ou $m > 0$:

$$\begin{aligned}
G_k(\tau) &= \sum_{m,n=-\infty}^{\infty}{}' \frac{1}{(m\tau+n)^k} \\
&= \sum_{m=-\infty}^{-1} \sum_{n=-\infty}^{\infty} \frac{1}{(m\tau+n)^k} + \sum_{n=-\infty}^{\infty}{}' \frac{1}{(0\tau+n)^k} + \sum_{m=1}^{\infty} \sum_{n=-\infty}^{\infty} \frac{1}{(m\tau+n)^k} \\
&= \sum_{m=\infty}^{1} \sum_{n=-\infty}^{\infty} \frac{1}{(-m\tau+n)^k} + \sum_{n=-\infty}^{\infty}{}' \frac{1}{n^k} + \sum_{m=1}^{\infty} \sum_{n=-\infty}^{\infty} \frac{1}{(m\tau+n)^k}
\end{aligned}$$

Par parité de k, on a $(-m\tau+n)^k = (m\tau-n)^k$ et $(-n)^k = n^k$. Du changement d'indice $n \mapsto -n$ dans les deux premières sommes, il résulte alors:

$$= \sum_{m=\infty}^{1} \sum_{n=\infty}^{-\infty} \frac{1}{(m\tau+n)^k} + \sum_{n=\infty}^{1} \frac{1}{n^k} + \sum_{n=1}^{\infty} \frac{1}{n^k} + \sum_{m=1}^{\infty} \sum_{n=-\infty}^{\infty} \frac{1}{(m\tau+n)^k}$$

Grâce à la convergence uniforme de G_k du théorème 2.1.4, on peut réordonner les deux premières sommes et regrouper:

$$\begin{aligned}
&= 2\sum_{n=1}^{\infty} \frac{1}{n^k} + 2\sum_{m=1}^{\infty} \sum_{n=-\infty}^{\infty} \frac{1}{(m\tau+n)^k} \\
&= 2\zeta(k) + 2\sum_{m=1}^{\infty} h_k(m\tau)
\end{aligned}$$

En utilisant le développement de Fourier du lemme 2.3.3, on obtient:

$$\begin{aligned}
&= 2\zeta(k) + 2\sum_{m=1}^{\infty} \left(\overbrace{\frac{(-2\pi i)^k}{(k-1)!}}^{=(2\pi i)^k} \sum_{n=1}^{\infty} n^{k-1} \left(e^{2\pi i m\tau}\right)^n \right) \\
&= 2\zeta(k) + 2\frac{(2\pi i)^k}{(k-1)!} \underbrace{\sum_{m=1}^{\infty} \sum_{n=1}^{\infty} n^{k-1} e^{2\pi i m n \tau}}_{(**)}
\end{aligned}$$

Soit $\eta > 0$. Pour $\tau = x + iy \in \mathcal{H}$ avec $y \geq \eta$, la double série $(**)$ converge absolument uniformément. En effet

$$\left|n^{k-1}e^{2\pi imn\tau}\right| \leq n^{k-1}\underbrace{\left|e^{2\pi imnx}\right|}_{=1}\left|e^{-2\pi mny}\right| = \frac{n^{k-1}}{e^{2\pi mny}} \leq \frac{n^{k-1}}{(\underbrace{e^{2\pi mn\eta}}_{>1})} \leq n^{k-1}$$

On peut donc réordonner $(**)$ de la façon suivante:

$$\sum_{m=1}^{\infty}\sum_{n=1}^{\infty} n^{k-1}e^{2\pi imn\tau} = \sum_{t=1}^{\infty}\sum_{\substack{mn=t\\ m>0,n>0}} n^{k-1}e^{2\pi it\tau} =$$

$$= \sum_{t=1}^{\infty}\left(\sum_{\substack{mn=t\\ m>0,n>0}} n^{k-1}\right)e^{2\pi it\tau} = \sum_{t=1}^{\infty}\left(\sum_{n|t} n^{k-1}\right)q^t = \sum_{t=1}^{\infty}\sigma_{k-1}(t)q^t$$

Avec cette expression pour $(**)$, on obtient immédiatement le développement de Fourier énoncé en hypothèse. □

Corollaire 2.3.6. *Soit $k \equiv 0 \pmod 2, k \geq 4$ et $\tau \in \mathcal{H}$. Le développement de Fourier de la série d'Eisenstein normée E_k est:*

$$E_k(\tau) = 1 - \frac{2k}{B_k}\sum_{n=1}^{\infty}\sigma_{k-1}(n)q^n \quad \textit{avec } q = e^{2\pi i\tau}$$

Démonstration. Par le théorème précédent, la définition 2.2.3: $E_k = \frac{1}{2\zeta(k)}G_k$ devient:

$$E_k(\tau) = 1 + \frac{(2\pi i)^k}{\zeta(k)(k-1)!}\sum_{n=1}^{\infty}\sigma_{k-1}(n)q^n$$

En appliquant le théorème 1.5.3: $\zeta(k) = (-1)^{(1+\frac{k}{2})}\frac{(2\pi)^k}{2(k!)}B_k$, on obtient:

$$\begin{aligned}
&= 1 + \frac{2(2\pi i)^k k!}{(-1)^{(1+\frac{k}{2})}(2\pi)^k(k-1)!\,B_k}\sum_{n=1}^{\infty}\sigma_{k-1}(n)q^n\\
&= 1 + \frac{2(i)^k k}{(-1)^{(1+\frac{k}{2})}B_k}\sum_{n=1}^{\infty}\sigma_{k-1}(n)q^n\\
&= 1 + \frac{(i^2)^{\frac{k}{2}}}{(-1)(-1)^{\frac{k}{2}}}\frac{2k}{B_k}\sum_{n=1}^{\infty}\sigma_{k-1}(n)q^n\\
&= 1 - \frac{2k}{B_k}\sum_{n=1}^{\infty}\sigma_{k-1}(n)q^n
\end{aligned}$$

□

2.3.2 Développement de Fourier de Δ et J

Lemme 2.3.7. *Soit $S(\tau) = \sum_{n=1}^{\infty} a(n)q^n$ une série uniformément convergente pour $\tau \in \mathcal{H}$. Alors on a pour $k \in \mathbb{C}$:*

$$\left(1 + k\sum_{n=1}^{\infty} a(n)q^n\right)^2 = 1 + 2k\sum_{n=1}^{\infty} a(n)q^n + k^2\sum_{n=2}^{\infty}\left(\sum_{r+s=n} a(r)a(s)\right)q^n$$

$$\begin{aligned}\left(1 + k\sum_{n=1}^{\infty} a(n)q^n\right)^3 = 1 + 3k\sum_{n=1}^{\infty} a(n)q^n &+ 3k^2\sum_{n=2}^{\infty}\left(\sum_{r+s=n} a(r)a(s)\right)q^n \\ &+ k^3\sum_{n=3}^{\infty}\left(\sum_{r+s+t=n} a(r)a(s)a(t)\right)q^n\end{aligned}$$

Démonstration. Trouvons des expressions directes pour S^2 et S^3:
La formule suivante explicite la multiplication de deux polynômes de terme constant nul:

$$\left(\sum_{i=1}^{n} p_i x^i\right)\left(\sum_{j=1}^{m} q_j x^j\right) = \sum_{i=2}^{n+m}\left(\sum_{r+s=i} p_r q_s\right)x^i$$

Cette formule peut être appliquée au produit de deux séries uniformément convergentes et donc à $S^2 = SS$ et $S^3 = SS^2$:

$$S^2 = \left(\sum_{n=1}^{\infty} a(n)q^n\right)^2 = \sum_{n=2}^{\infty}\left(\sum_{r+s=n} a(r)a(s)\right)q^n$$

$$\begin{aligned}S^3 &= \left(\sum_{n=1}^{\infty} a(n)q^n\right)\left(\sum_{m=1}^{\infty} a(m)q^m\right)^2 \\ &= \left(\sum_{n=1}^{\infty} a(n)q^n\right)\left(\sum_{m=2}^{\infty}\left(\sum_{r+s=m} a(r)a(s)\right)q^m\right) \\ &= \sum_{n=3}^{\infty}\left(\sum_{t+m=n} a(t)\left(\sum_{r+s=m} a(r)a(s)\right)\right)q^n \\ &= \sum_{n=3}^{\infty}\left(\sum_{t+r+s=n} a(t)a(r)a(s)\right)q^n\end{aligned}$$

En utilisant les expressions ci-dessus dans

$$(1+kS)^2 = 1 + 2kS + k^2S^2$$

$$(1+kS)^3 = 1 + 3kS + 3k^2S^2 + k^3S^3$$

on aboutit immédiatement à la conclusion. $\square$

Théorème 2.3.8. *Soit* $k \equiv 0 \pmod 2, k \geq 4$ *et* $\tau \in \mathcal{H}$. *Le développement de Fourier du discriminant* Δ *est:*

$$\Delta(\tau) = (2\pi)^{12} \sum_{n=1}^{\infty} \tau(n) q^n \quad \textit{avec } q = e^{2\pi i \tau}$$

où $\tau(n)$ *est la* fonction de Ramanujan *donnée par:*

$$\begin{aligned}\tau(n) = \frac{1}{12}(5\sigma_3(n) + 7\sigma_5(n)) + \sum_{r+s=n} &(100\sigma_3(r)\sigma_3(s) - 147\sigma_5(r)\sigma_5(s)) \\ &+ 8000 \sum_{r+s+t=n} \sigma_3(r)\sigma_3(s)\sigma_3(t)\end{aligned} \tag{2.3.6}$$

Démonstration. Le développement de Fourier de E_k du corollaire 2.3.6 utilisé dans la définition 1.4.7 mène à:

$$\begin{aligned}
\Delta(\tau) &= \frac{(2\pi)^{12}}{12^3}\Big((E_4(\tau))^3 - (E_6(\tau))^2\Big)\\
&= \frac{(2\pi)^{12}}{12^3}\left(\left(1 - \frac{8}{B_4}\sum_{n=1}^{\infty}\sigma_3(n)q^n\right)^3 - \left(1 - \frac{12}{B_6}\sum_{n=1}^{\infty}\sigma_5(n)q^n\right)^2\right)
\end{aligned}$$

Avec les valeurs pour B_k de la définition 1.5.2, on a:

$$= \frac{(2\pi)^{12}}{12^3}\left(\left(1 + 240\sum_{n=1}^{\infty}\sigma_3(n)q^n\right)^3 - \left(1 - 504\sum_{n=1}^{\infty}\sigma_5(n)q^n\right)^2\right)$$

Du lemme 2.3.7 suit alors:

$$\begin{aligned}
&= \frac{(2\pi)^{12}}{12^3}\Bigg(1 + 3\cdot 240\sum_{n=1}^{\infty}\sigma_3(n)q^n +\\
&\quad + 3\cdot 240^2\sum_{n=2}^{\infty}\left(\sum_{r+s=n}\sigma_3(r)\sigma_3(s)\right)q^n +\\
&\quad + 240^3\sum_{n=3}^{\infty}\left(\sum_{r+s+t=n}\sigma_3(r)\sigma_3(s)\sigma_3(t)\right)q^n - 1 +\\
&\quad + 2\cdot 504\sum_{n=1}^{\infty}\sigma_5(n)q^n - 504^2\sum_{n=2}^{\infty}\left(\sum_{r+s=n}\sigma_5(r)\sigma_5(s)\right)q^n\Bigg)
\end{aligned}$$

De la définition 2.3.4 suit $\sigma_5(0) = \sigma_3(0) = 0$, ainsi on peut sommer partout à partir de $n = 1$:

$$\begin{aligned}
\Delta(\tau) = \frac{(2\pi)^{12}}{12^3}\Bigg(& 3 \cdot 240 \sum_{n=1}^{\infty} \sigma_3(n) q^n + 3 \cdot 240^2 \sum_{n=1}^{\infty} \left(\sum_{r+s=n} \sigma_3(r)\sigma_3(s) \right) q^n + \\
&+ 240^3 \sum_{n=1}^{\infty} \left(\sum_{r+s+t=n} \sigma_3(r)\sigma_3(s)\sigma_3(t) \right) q^n + \\
&+ 2 \cdot 504 \sum_{n=1}^{\infty} \sigma_5(n) q^n - 504^2 \sum_{n=1}^{\infty} \left(\sum_{r+s=n} \sigma_5(r)\sigma_5(s) \right) q^n \Bigg) \\
= \frac{(2\pi)^{12}}{12^3} \sum_{n=1}^{\infty} \Bigg(& 3 \cdot 240 \sigma_3(n) + 2 \cdot 504 \sigma_5(n) + \\
&+ 3 \cdot 240^2 \left(\sum_{r+s=n} \sigma_3(r)\sigma_3(s) \right) - 504^2 \left(\sum_{r+s=n} \sigma_5(r)\sigma_5(s) \right) + \\
&+ 240^3 \left(\sum_{r+s+t=n} \sigma_3(r)\sigma_3(s)\sigma_3(t) \right) \Bigg) q^n
\end{aligned}$$

En faisant entrer $\frac{1}{12^3}$ dans la parenthèse, on parvient au résultat cherché:

$$\begin{aligned}
= (2\pi)^{12} \sum_{n=1}^{\infty} \Bigg(& \frac{5}{12}\sigma_3(n) + \frac{7}{12}\sigma_5(n) + \\
&+ \sum_{r+s=n} (100\sigma_3(r)\sigma_3(s) - 147\sigma_5(r)\sigma_5(s)) + \\
&+ 8000 \left(\sum_{r+s+t=n} \sigma_3(r)\sigma_3(s)\sigma_3(t) \right) \Bigg) q^n
\end{aligned}$$

□

Corollaire 2.3.9. *Les deux premières valeurs de la fonction de Ramanujan $\tau(n)$ sont:*

$$\tau(1) = 1, \quad \tau(2) = -24$$

Démonstration.

$$\tau(1) = \frac{5}{12}\sigma_3(1) + \frac{7}{12}\sigma_5(1) = \frac{5+7}{12} = 1$$

$$\begin{aligned}
\tau(2) &= \frac{5}{12}\sigma_3(2) + \frac{7}{12}\sigma_5(2) + 100\sigma_3(1)\sigma_3(1) - 147\sigma_5(1)\sigma_5(1) \\
&= \frac{5}{12}(1+2^3) + \frac{7}{12}(1+2^5) + 100 - 147 \\
&= \frac{45+231}{12} - 47 = -24
\end{aligned}$$

□

Théorème 2.3.10. *Soit* $k \equiv 0 \pmod 2, k \geq 4$ *et* $\tau \in \mathcal{H}$. $\exists$ *des coefficients* $c(n) \in \mathbb{C}$; $n = 0, 1, 2, \ldots$ *tels que le développement de Fourier de l'invariante absolue* J *est:*

$$J(\tau) = \frac{1}{12^3}\left(\frac{1}{q} + \sum_{n=0}^{\infty} c(n)q^n\right) \quad \textit{avec } q = e^{2\pi i\tau}$$

Démonstration. Par le corollaire 2.2.7, on a

$$\begin{aligned}
J(\tau) &= \frac{(2\pi)^{12}(E_4(\tau))^3}{12^3\Delta(\tau)} \\
&= \frac{1}{12^3}\left(\frac{\left(1+240\sum_{n=1}^{\infty}\sigma_3(n)q^n\right)^3}{\sum_{n=1}^{\infty}\tau(n)q^n}\right) \\
&= \frac{1}{12^3}\cdot\frac{1}{q}\left(\frac{\left(1+240\sum_{n=1}^{\infty}\sigma_3(n)q^n\right)^3}{\tau(1) + \underbrace{\sum_{n=2}^{\infty}\tau(n)q^{n-1}}_{=\sum_{n=1}^{\infty}\tau(n+1)q^n}}\right)
\end{aligned}$$

Grâce au corollaire 2.3.9, on sait que $\tau(1) = 1$. On peut alors développer $J(\tau)$ de la façon suivante (pour certains $c(n) \in \mathbb{C}$; $n = 0, 1, 2, \ldots$):

$$\begin{aligned}
J(\tau) &= \frac{1}{12^3}\cdot\frac{1}{q}\left(1 + \sum_{n=1}^{\infty} c(n-1)q^n\right) \\
&= \frac{1}{12^3}\left(\frac{1}{q} + \sum_{n=0}^{\infty} c(n)q^n\right)
\end{aligned}$$

□

3 Applications en théorie des nombres

3.1 La fonction de Ramanujan $\tau(n)$

Ramanujan a été le premier à étudier la fonction $\tau(n)$ de façon approfondie, il a démontré vers 1916 de nombreuses propriétés de $\tau(n)$ dans [3]. D'autres résultats ont été montrés dans les années 40 notamment par Lehmer [4].

Théorème 3.1.1. *$\tau(n)$ est une fonction à valeurs entières:*

$$\tau(n) \in \mathbb{Z} \quad \forall n \in \mathbb{N}$$

Démonstration. Vu la forme générale (2.3.6) de $\tau(n)$, il suffit de démontrer que

$$\frac{1}{12}(5\sigma_3(n) + 7\sigma_5(n)) \in \mathbb{Z}$$

Clairement le reste de la somme qui compose $\tau(n)$ est entier $\forall n \in \mathbb{N}$.
Montrons donc que

$$5\sigma_3(n) + 7\sigma_5(n) \equiv 0 \pmod{12} \tag{3.1.1}$$

Les seuls diviseurs pouvant intervenir dans les σ_k sur $\mathbb{Z}/12\mathbb{Z}$ sont compris entre -6 et 6.
Or on a que

$$5d^3 + 7d^5 \equiv 0 \pmod{12} \quad \forall d \in \mathbb{Z}^* \text{ avec } |d| \leq 6 \tag{3.1.2}$$

En effet, sur $\mathbb{Z}/12\mathbb{Z}$:

$$5d^3 + 7d^5 = 5d^3 - 5d^5 = 5(d^3 - d^5)$$

Comme la seule solution à l'équation $5k = 0$ sur $\mathbb{Z}/12\mathbb{Z}$ est $k = 0$, il suffit de vérifier que l'on a sur $\mathbb{Z}/12\mathbb{Z}$:

$$d^3 = d^5 \quad \text{pour } d \in \{1, 2, 3, 4, 5, 6\} :$$

$$\begin{aligned}
1 = 1^3 &\equiv 1^5 = 1 \pmod{12} \\
8 = 2^3 &\equiv 2^5 = 32 = 8 + 2 \cdot 12 \pmod{12} \\
2 \cdot 12 + 3 = 27 = 3^3 &\equiv 3^5 = 243 = 3 + 20 \cdot 12 \pmod{12} \\
5 \cdot 12 + 4 = 64 = 4^3 &\equiv 4^5 = 1024 = 4 + 85 \cdot 12 \pmod{12} \\
10 \cdot 12 + 5 = 125 = 5^3 &\equiv 5^5 = 3125 = 5 + 260 \cdot 12 \pmod{12} \\
18 \cdot 12 + 0 = 216 = 6^3 &\equiv 6^5 = 7776 = 0 + 648 \cdot 12 \pmod{12}
\end{aligned}$$

Ainsi, la congruence (3.1.2) est vraie pour tout élément pouvant intervenir dans la somme des diviseurs de n dans (3.1.1), la même congruence est donc vérifiée pour toute cette somme et l'équation (3.1.1) est vérifiée.

□

Théorème 3.1.2 (Ramanujan). *La fonction de Ramanujan possède des propriétés arithmétiques très intéressantes:*

$$\tau(nm) = \tau(n)\tau(m) \quad \forall n, m \in \mathbb{N} \text{ avec } \operatorname{pgdc}(n, m) = 1$$
$$\tau(p^{r+1}) = \tau(p)\tau(p^r) - p^{11}\tau(p^{r-1}) \quad \forall p \text{ premier}, r \in \mathbb{N}$$

Sans démonstration. Il n'est pas possible de prouver ce théorème avec la théorie introduite ici car la démonstration utilise les opérateurs de Hecke. On trouvera la démonstration dans [1] ou [2]. □

Le problème suivant est ouvert:

Conjecture 3.1.3 (Lehmer).

$$\forall n \in \mathbb{N}, \tau(n) \neq 0$$

Vérifiée numériquement pour $n \leq 2 \cdot 10^{11}$

3.1.1 Congruence de Ramanujan

Théorème 3.1.4. $\forall n \in \mathbb{N}$, *on a la égalité suivante:*

$$756\tau(n) = 65\sigma_{11}(n) + 691\sigma_5(n) - 691 \cdot 252 \sum_{r+s=n} \sigma_5(r)\sigma_5(s)$$

Démonstration. $\{\Delta, E_6^2\}$ est une base de $\mathcal{M}_{12}$ (c.f. p. 11). On peut donc exprimer la série $E_{12} \in \mathcal{M}_{12}$ dans cette base. De plus $E_{12}(i\infty) = 1, E_6(i\infty) = 1$ et $\Delta(i\infty) = 0$. D'où $\exists \mu \in \mathbb{C}$ avec:

$$E_{12} = E_6^2 + \mu\Delta$$

Posons $\lambda = -\mu(2\pi)^{12} \in \mathbb{C}$:

$$\frac{\lambda}{(2\pi)^{12}}\Delta = E_6^2 - E_{12}$$

Passons aux développements de Fourier: $\forall \tau \in \mathcal{H}$ on a:

$$\lambda \sum_{n=1}^{\infty} \tau(n)q^n = \left(1 - \frac{12}{B_6} \sum_{n=1}^{\infty} \sigma_5(n)q^n\right)^2 - \left(1 - \frac{24}{B_{12}} \sum_{n=1}^{\infty} \sigma_{11}(n)q^n\right)$$

Appliquons le lemme 2.3.7 et utilisons les valeurs pour B_k de la définition 1.5.2:

$$\begin{aligned}\lambda \sum_{n=1}^{\infty} \tau(n) q^n &= 1 - 2\cdot 504 \sum_{n=1}^{\infty} \sigma_5(n) q^n + 504^2 \sum_{n=1}^{\infty} \left(\sum_{r+s=n} \sigma_r(n)\sigma_5(s) \right) q^n - \\ &\quad - 1 - \frac{65520}{691} \sum_{n=1}^{\infty} \sigma_{11}(n) q^n \\ &= \sum_{n=1}^{\infty} \left(-2\cdot 504\sigma_5(n) + 504^2 \sum_{r+s=n} \sigma_r(n)\sigma_5(s) - \frac{65520}{691}\sigma_{11}(n) \right) q^n\end{aligned}$$

Cette égalité conduit à la relation suivante entre les coefficients de Fourier:

$$\lambda\tau(n) = -2\cdot 504\sigma_5(n) + 504^2 \sum_{r+s=n} \sigma_r(n)\sigma_5(s) - \frac{65520}{691}\sigma_{11}(n) \tag{3.1.3}$$

Posons $n = 1$; comme $\sigma_5(1) = \sigma_{11}(1) = \tau(1) = 1$, on a alors:

$$\lambda = -2\cdot 504 - \frac{65520}{691} = -\frac{2\cdot 504\cdot 691}{691} - \frac{2\cdot 504\cdot 65}{691} = -\frac{2\cdot 504\cdot 756}{691}$$

Avec cette valeur pour λ, l'équation (3.1.3) devient:

$$756\tau(n) = 691\sigma_5(n) - \frac{504\cdot 691}{2} \sum_{r+s=n} \sigma_r(n)\sigma_5(s) + 65\sigma_{11}(n)$$

Par $\frac{504\cdot 691}{2} = 691\cdot 252$ on aboutit au résultat. □

Corollaire 3.1.5 (Ramanujan). *On a la congruence remarquable:*

$$\tau(n) \equiv \sigma_{11}(n) \pmod{691} \quad \forall n \in \mathbb{N}$$

Démonstration. Par le théorème précédent on a:

$$\begin{aligned}756\tau(n) &= 65\sigma_{11}(n) + 691\sigma_5(n) - 691\cdot 252 \sum_{r+s=n} \sigma_5(r)\sigma_5(s) \\ &= 65\sigma_{11}(n) + 691 \underbrace{\left(\sigma_5(n) - 252 \sum_{r+s=n} \sigma_5(r)\sigma_5(s) \right)}_{=k\in\mathbb{Z}} \\ &= 65\sigma_{11}(n) + 691k\end{aligned}$$

Or $756 = 65 + 691$, donc on a la congruence suivante:

$$65\tau(n) \equiv 65\sigma_{11}(n) \pmod{691}$$

Comme 691 est un nombre premier, $\mathbb{Z}/691\mathbb{Z}$ est un corps, d'où:

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

□

3.2 Congruences entre puissances de premiers

Théorème 3.2.1. *On a la relation suivante entre σ_3 et σ_7:*

$$\sigma_7(n) = \sigma_3(n) + 120 \sum_{r+s=n} \sigma_3(r)\sigma_3(s) \quad \forall n \in \mathbb{N}$$

Démonstration. Le corollaire 2.2.4 donne une relation entre E_8 et E_4:

$$E_8 = E_4^2$$

Passons aux développements de Fourier:

$$1 - \frac{16}{B_8} \sum_{n=1}^{\infty} \sigma_7(n) q^n = \left(1 - \frac{8}{B_4} \sum_{n=1}^{\infty} \sigma_3(n) q^n\right)^2$$

Appliquons le lemme 2.3.7 et utilisons les valeurs pour B_k de la définition 1.5.2:

$$1 + 480 \sum_{n=1}^{\infty} \sigma_7(n) q^n = 1 + 2 \cdot 240 \left(\sum_{n=1}^{\infty} \sigma_3(n) q^n + 120 \sum_{n=1}^{\infty} \sum_{r+s=n} \sigma_3(r)\sigma_3(s) q^n\right)$$

D'où la relation entre les coefficients de Fourier:

$$\sigma_7(n) = \sigma_3(n) + 120 \sum_{r+s=n} \sigma_3(r)\sigma_3(s)$$

□

Corollaire 3.2.2. *Soit p premier, alors*

$$p^7 \equiv p^3 \pmod{120}$$

Démonstration. Observons que pour p premier,

$$\sigma_k(p) = p^k + 1$$

Le théorème précédent devient donc

$$p^7 + 1 = p^3 + 1 + 120 \underbrace{\sum_{r+s=p} \sigma_3(r)\sigma_3(s)}_{\in \mathbb{Z}}$$

Ceci amène immédiatement au résultat. □

En tirant profit des autres relations données par le corollaire 2.2.4:

$$E_{10} = E_4 E_6, \qquad E_{14} = E_4^2 E_6$$

et des relations supplémentaires suivantes (elles se déduisent du corollaire 2.2.4):

$$E_{14} = E_6 E_8, \qquad E_{14} = E_4 E_{10}$$

on obtient de nouvelles congruences par la même technique de démonstration qui a été utilisée pour prouver le théorème et le corollaire ci-dessus:

Exemple 1: $E_{10} = E_4 E_6$

Théorème 3.2.3.

$$11\sigma_9(n) = -10\sigma_3(n) + 21\sigma_5(n) + 5040 \sum_{r+s=n} \sigma_3(r)\sigma_5(s) \quad \forall n \in \mathbb{N}$$

Corollaire 3.2.4. *Soit p premier, alors*

$$11p^9 \equiv 21p^5 - 10p^3 \pmod{5040}$$

Exemple 2: $E_{14} = E_4 E_{10}$

Théorème 3.2.5.

$$\sigma_{13}(n) = -10\sigma_3(n) + 11\sigma_9(n) + 2640 \sum_{r+s=n} \sigma_3(r)\sigma_9(s) \quad \forall n \in \mathbb{N}$$

Corollaire 3.2.6. *Soit p premier, alors*

$$p^9 \equiv 11p^5 - 10p^3 \pmod{2640}$$

Les démonstrations de ces quatre affirmations sont essentiellement les mêmes que celles du théorème 3.2.1 et du corollaire 3.2.2.

Références

[1] H.W. Burmann. Modulfunktionen und -formen. Vorlesung am Mathematischen Institut der Universität Göttingen, 1996.

[2] J.P. Serre. *Cours d'Arithmétique*. Presses universitaires de France, Paris, 1977.

[3] S. Ramanujan. On certain arithmetical functions. *Proceedings of the Cambridge Philosophical Society*, 19:117–124, 1917.

[4] D.H. Lehmer. Ramanujan's function $\tau(n)$. *Amer. J. Math.*, 64:483–492, 1942.

[5] B. Schoeneberg. *Elliptic Modular Functions*, volume 203 of *Grundlehren der mathematischen Wissenschaften*. Springer, Berlin, Heidelberg, New York, 1974.

[6] R.A. Rankin. *Modular forms and functions*. Cambridge University Press, Cambridge, 1977.