Partitions de n

dossier de maîtrise
sous la direction d'Olivier Benoist
ENS Ulm

Joël Gay Gabriel Lellouch

14 juillet 2011

Table des matières

0.1 Introduction

Toto a n billes, et autant d'amis, indiscernables. De combien de manières peut-il réaliser le partage ?
C'est cette question que nous allons tâcher de résoudre ici.

Plus formellement, le problème se pose ainsi : étant donné un entier $n \in \mathbb{N}$, on appelle *partition de* n tout p-uplet $(n_1, \ldots, n_p)$, avec $1 \leq n_1 \leq n_2 \leq \ldots \leq n_p$ tel que $n_1 + \ldots + n_p = n$. Combien existe-t-il de partitions de n ? Autrement dit, de combien de manières peut-on écrire n comme somme d'entiers naturels, sans tenir compte de l'ordre ?

Dans toute la suite, on notera $p(n)$ le nombre de partitions de n. Par exemple, on a $p(5) = 7$, car on a $1+1+1+1+1 = 1+1+1+2 = 1+1+3 = 1+4 = 1+2+2 = 2+3 = 5$. Par convention, on posera $p(0) = 1$.

En 1918, le célèbre duo Hardy-Ramanujan ([HR00]) donne un équivalent de $p(n)$ quand n tend vers l'infini, qui découle d'un développement asymptotique plus précis, de la forme :

$$p(n) = \sum_{k<\alpha\sqrt{n}} P_k(n) + O(n^{-1/4}).$$

La série de terme général $P_k(n)$ diverge pour tout n.

En 1937, le mathématicien Hans Rademacher modifie légèrement les travaux de Hardy et Ramanujan pour obtenir une série convergente, ce qui donne ainsi une formule exacte pour $p(n)$. Les sommes partielles de cette série ont également le bon goût de donner un développement asymptotique de $p(n)$. Ceci se révèle particulièrement important pour le calcul de $p(n)$, puisque, $p(n)$ étant entier, il suffit alors de tronquer la somme à un rang assez grand et de prendre le plus proche entier pour obtenir le nombre exact $p(n)$.

Nous allons ici nous intéresser à la preuve de la formule exacte de $p(n)$, obtenue par Rademacher (théorème 1.11). La preuve en elle-même est l'objet de la première partie. Pour cela, nous introduirons la fonction génératrice définie sur tout $B(0,1) = \{z \in \mathbb{C}, |z| < 1\}$:

$$F(z) = \sum_{n=0}^{\infty} p(n) z^n.$$

Nous obtiendrons une formule pour F sous forme de produit qui mettra en évidence des divergences en toutes les racines de l'unité.
Le calcul de $p(n)$ revient alors au calcul du résidu en 0 de la fonction $F(x)/x^{n+1}$.

L'intérêt de la preuve va être le choix du contour d'intégration pour appliquer le théorème des résidus. Intégrer sur le contour que nous définirons permettra de diviser l'intégrale en une somme, indexée par les racines de l'unité, d'intégrales décrivant le comportement de F au voisinage de la singularité correspondante. Il restera alors à utiliser une équation fonctionnelle vérifiée par F et reliant son comportement en une racine de l'unité à celui en 0 pour pouvoir estimer

chacune des intégrales de la somme. Nous admettrons dans un premier temps cette équation fonctionnelle.

Les trois parties restantes sont consacrées à la démonstration de l'équation fonctionnelle de F. Pour cela, nous allons devoir faire appel à des classes de fonctions bien particulières. Tout d'abord, la deuxième partie aura pour objet l'étude des fonctions dites elliptiques. Le but sera de définir la fonction Δ (section 2.3), que nous introduirons par le biais de la fonction elliptique $\wp$ de Weierstrass (section 2.2).

La troisième partie étudiera les fonctions dites modulaires, qui sont équivariantes pour un certain groupe de transformations du demi-plan supérieur, le groupe modulaire (section 3.1). Nous démontrerons le résultat principal qu'une fonction modulaire ne prenant pas toutes les valeurs possibles est constante (théorème 3.2).

Enfin, nous définirons dans la dernière partie la fonction η de Dedekind. Cette fonction nous permettra d'utiliser les résultats développés dans les deux parties précédentes. Son lien étroit avec Δ nous donnera une équation fonctionnelle qu'elle vérifie (section 4.2) ; et une relation simple entre η et F nous amènera alors à transformer cette équation en l'équation fonctionnelle de F (section 4.3) que nous avions admise dans la première partie.

Le lecteur se rendra sans doute compte que, pour les besoins de la preuve, nous ferons appel à des objets fondamentaux (fonctions elliptiques, modulaires,...), que nous n'utiliserons peut-être pas autant qu'ils le mériteraient. Il faut bien comprendre que ces objets ont de nombreuses autres applications. En présenter une ici permet de donner une idée des résultats qu'ils peuvent donner non seulement en analyse, mais également dans le cas présent, en théorie des nombres. Cette utilisation d'outils d'analyse complexe en théorie des nombres peut se généraliser. Le lecteur intéressé pourra se référer à [CC10]. En suivant l'exemple des partitions de n, on estimer le nombre de manières d'écrire un entier comme somme de carrés, ou de cubes, et pourquoi pas ? le nombre de manières d'écrire un nombre pair comme somme de nombres premiers...

Remerciements **:**
Nous voudrions vivement remercier Olivier Benoist pour sa disponibilité, son aide constante et pour le moins fondamentale, ses conseils avisés et son enthousiasme, et enfin, pour n'avoir pas osé effacer notre contour d'intégration de son tableau durant plusieurs mois.
Nous tenons également à ne pas remercier M. J-H.L. pour nous avoir évités au moment où nous avions besoin de lui.

Chapitre 1

Nombre de partitions

1.1 Expression sous forme de produit

Comme expliqué dans le préambule nous allons étudier la fonction définie sur $B(0,1)$:

$$F(z) = \sum_{n\geq 1} p(n) z^n.$$

La proposition suivante montre que cela a un sens et exprime cette série par une autre expression.

Proposition 1.1. *La série $\sum_{n\geq 1} p(n)z^n$ et le produit infini $\prod_{n\geq 1} \frac{1}{1-z^n}$ convergent absolument sur $B(0,1)$ vers une même fonction que l'on notera $F(z)$.*

Démonstration. Le fait que $\prod_{n\geq 1} \frac{1}{1-z^n}$ converge absolument sur $B(0,1)$ est immédiat étant donné que son inverse converge absolument car la série $\sum_{k\geq 1}^{\infty} z^k$ converge absolument. On note $F(z)$ la limite.

On veut montrer que la somme et le produit coïncident sur $B(0,1)$. Nous allons d'abord voir une preuve intuitive de ce résultat puis nous écrirons formellement ce qui se passe.

En fait, si l'on développe chaque facteur par la série entière qui lui est associé on a :

$$\prod_{n\geq 1} \frac{1}{1-x^n} = (1 + x + x^2 + x^3 + \dots)(1 + x^2 + x^4 + \dots)(1 + x^3 + x^6 + \dots)\dots$$

On développe alors le membre de gauche et on range les termes par puissance de x. On obtient alors une série de la forme :

$$1 + \sum_{k=1}^{\infty} a(k) x^k.$$

On voudrait montrer que $a(k) = p(k)$. Supposons que l'on ait pris dans le premier facteur le terme x^{k_1}, le terme x^{2k_2} dans le second... jusqu'au terme x^{mk_m} pour le m-ième, où tous les $k_i \geq 0$. Leur produit est :

$$x^{k_1} x^{2k_2} x^{3k_3} \dots x^{mk_m} = x^k$$

avec :

$$k = k_1 + 2k_2 + 3k_3 + \cdots + mk_m.$$

On a donc écrit k de la façon suivante :

$$k = (1 + 1 + 1 + \cdots + 1) + (2 + 2 + \cdots + 2) + \cdots + (m + m + \cdots + m),$$

où la première parenthèse contient k_1 termes, la seconde k_2 termes et ainsi de suite. On a donc écrit une partition de k. On voit donc que chaque partition de k produit un terme x^k et que, réciproquement, chaque terme x^k provient d'une partition de k. Ainsi $a(k)$, le coefficient de x^k, est égal à $p(k)$, le nombre de partitions de k.

Il est évident que cette preuve n'est pas rigoureuse, car nous avons ignoré toutes les questions de convergence et que nous avons traité des produits infinis comme des polynômes. Nous allons donc rendre cette preuve plus rigoureuse. Pour ce faire nous allons restreindre x à l'intervalle $[0, 1[$. On introduit également deux fonctions :

$$G_m(x) = \prod_{k=1}^{m} \frac{1}{1 - x^k}, \text{ et : } G(x) = \prod_{k\geq 1}^{\infty} \frac{1}{1 - x^k} = \lim_{m\to\infty} G_m(x).$$

Le produit $G(x)$ converge absolument pour $0 \leq x < 1$ comme vu précédemment. Remarquons également qu'à x fixé la suite $G_m(x)$ est croissante car :

$$G_{m+1}(x) = \frac{1}{1 - x^{m+1}} G_m(x) \geq G_m(x).$$

Ainsi : $\forall x \in [0, 1[, \forall m, G_m(x) \leq G(x)$.

Par ailleurs, $G_m(x)$ est le produit d'un nombre fini de séries absolument convergentes. C'est donc également une série absolument convergente que l'on peut écrire :

$$G_m(x) = 1 + \sum_{k=1}^{\infty} p_m(k)x^k.$$

Ici, $p_m(k)$ est le nombre de solutions à l'équation :

$$k = k_1 + 2k_2 + 3k_3 + \cdots + mk_m,$$

c'est-à-dire que $p_m(k)$ est le nombre de partitions de k en somme d'entiers tous inférieurs ou égaux à m. Dès lors, on a que si $m \geq k$, $p_m(k) = p(k)$. On a donc toujours :

$$p_m(k) \leq p(k)$$

avec égalité quand $m \geq k$. En d'autres termes :

$$\lim_{m\to\infty} p_m(k) = p(k).$$

On divise alors la série de G_m en deux termes :

$$\begin{aligned} G_m(x) &= \sum_{k=0}^{m} p_m(k)x^k + \sum_{k=m+1}^{\infty} p_m(k)x^k \\ &= \sum_{k=0}^{m} p(k)x^k + \sum_{k=m+1}^{\infty} p_m(k)x^k. \end{aligned}$$

Comme $x \geq 0$ on a :

$$\sum_{k=0}^{m} p(k)x^k \leq G_m(x) \leq G(x).$$

Ceci montre que la série $\sum_{k=0}^{\infty} p(k)x^k$ converge. De plus, comme $p_m(k) \leq p(k)$ on a :

$$\sum_{k=0}^{\infty} p_m(k)x^k \leq \sum_{k=0}^{\infty} p(k)x^k \leq G(x).$$

Ainsi, à x fixé, la série $\sum p_m(k)x^k$ converge uniformément en m. On fait tendre m vers l'infini et on obtient :

$$G(x) = \lim_{m\to\infty} G_m(x) = \lim_{m\to\infty} \sum_{k=0}^{\infty} p_m(k)x^k = \sum_{k=0}^{\infty} \lim_{m\to\infty} p_m(k)x^k = \sum_{k=0}^{\infty} p(k)x^k.$$

Ceci conclut la preuve si $0 \leq x < 1$. La série entière $\sum_{n\geq 1} p(n)z^n$ converge sur $[0,1]$ donc aussi sur $B(0,1)$. Alors, la fonction $\sum_{n\geq 1} p(n)z^n - \prod_{n\geq 1} \frac{1}{1-z^n}$ est analytique sur le disque et s'y annule une infinité de fois donc est identiquement nulle. □

1.2 Équation fonctionnelle de F

Le résultat suivant est admis pour le moment et fera l'objet des trois prochaines parties. Il sera finalement démontré à l'extrême fin de ce mémoire, au théorème 4.9.

Théorème 1.2. *Soit $F(t) = 1/\prod_{n=1}^{\infty}(1-t^n)$.*
Soit $k \in \mathbb{N}$, $z \in \mathbb{C}$, $h, H \in \mathbb{Z}$ tels que $Re(z) > 0$, $(h,k) = 1$ et $hH \equiv -1[k]$
Alors, pour

$$x = exp\left(\frac{2i\pi h}{k} - \frac{2\pi z}{k^2}\right), x' = exp\left(\frac{2i\pi H}{k} - \frac{2\pi}{z}\right)$$

on a

$$F(x) = e^{i\pi s(h,k)}\left(\frac{z}{k}\right)^{1/2} exp\left(\frac{\pi}{12z} - \frac{\pi z}{12k^2}\right) F(x'),$$

où $s(h,k) = \sum_{r=1}^{k-1} \frac{r}{k}\left(\frac{hr}{k} - \left[\frac{hr}{k}\right] - \frac{1}{2}\right)$ est appelée somme de Dedekind.

Remarque 1 : La force de cette équation est qu'elle relie le comportement de F en une racine de l'unité à son comportement en 0, que l'on connaît bien.

Remarque 2 : Les sommes de Dedekind seront étudiées en détail en 4.2.2.

1.3 Contour d'intégration

Nous arrivons maintenant à la partie centrale du calcul de $p(n)$. Comme nous l'avons expliqué dans l'introduction, nous allons appliquer le théorème des résidus : en effet, la fonction $F(x)/x^{n+1}$ admet en 0 un pôle dont le résidu est précisément $p(n)$. On a donc :

$$p(n) = \frac{1}{2i\pi}\int_C \frac{F(x)}{x^{n+1}}dx.$$

Tout l'intérêt de la preuve réside dans le choix du contour d'intégration C. Il nous faut ici décrire le contour particulier qui fut utilisé par Rademacher. Celui-ci est relié aux ensembles de Farey et aux cercles de Ford que l'on va définir et dont on va décrire certaines propriétés ici.

1.3.1 Ensemble de Farey

Définition 1.3.1. *L'ensemble des fractions de Farey d'ordre n, noté F_n, est l'ensemble des fractions irréductibles dans l'intervalle $[0,1]$ dont le dénominateur est $\leq n$, rangé par ordre croissant.*

Exemples :

$F_1 : \frac{0}{1}, \frac{1}{1}$

$F_2 : \frac{0}{1}, \frac{1}{2}, \frac{1}{1}$

$F_3 : \frac{0}{1}, \frac{1}{3}, \frac{1}{2}, \frac{2}{3}, \frac{1}{1}$

$F_4 : \frac{0}{1}, \frac{1}{4}, \frac{1}{3}, \frac{1}{2}, \frac{2}{3}, \frac{3}{4}, \frac{1}{1}$

$F_5 : \frac{0}{1}, \frac{1}{5}, \frac{1}{4}, \frac{1}{3}, \frac{2}{5}, \frac{1}{2}, \frac{3}{5}, \frac{2}{3}, \frac{3}{4}, \frac{4}{5}, \frac{1}{1}$

$F_5 : \frac{0}{1}, \frac{1}{6}, \frac{1}{5}, \frac{1}{4}, \frac{1}{3}, \frac{2}{5}, \frac{1}{2}, \frac{3}{5}, \frac{2}{3}, \frac{3}{4}, \frac{4}{5}, \frac{5}{6}, \frac{1}{1}$

Ces premiers exemples montrent déjà certaines propriétés générales de ces ensembles. On voit ainsi que $F_n \subset F_{n+1}$. On passe donc de F_n à F_{n+1} en ajoutant de nouvelles fractions. On voit aussi que si les deux fractions $\frac{a}{b}$ et $\frac{c}{d}$ sont consécutives dans F_n mais pas dans F_{n+1}, alors c'est leur *médiane* $\frac{a+c}{b+d}$ qui les sépare, et c'est la seule fraction insérée entre les deux fractions.

Dans toute la suite, on prendra $(a,b) = 1$ et $(c,d) = 1$ avec $b > 0$ et $d > 0$.

Lemme 1.3. *Si $\frac{a}{b} < \frac{c}{d}$, alors leur médiane $\frac{a+c}{b+d}$ se situe strictement entre les deux.*

Démonstration.

$$\frac{a+c}{b+d} - \frac{a}{b} = \frac{bc-ad}{b(b+d)} > 0 \text{ et } \frac{c}{d} - \frac{a+c}{b+d} = \frac{bc-ad}{d(b+d)} > 0.$$

□

Les exemples précédents montrent que $\frac{1}{2}$ et $\frac{1}{3}$ sont consécutifs pour $n = 3$ et 4. Ceci illustre la propriété générale suivante :

Lemme 1.4. *Soit $0 \leq \frac{a}{b} < \frac{c}{d} \leq 1$. Si $bc - ad = 1$ alors les fractions a/b et c/d sont consécutives dans F_n pour :*

$$\max(b,d) \leq n \leq b + d - 1.$$

Démonstration. La relation $bc-ad=1$ implique que a/b et c/d sont irréductibles. Si $\max(b,d) \leq n$ alors $b \leq n$ et $d \leq n$ donc a/b et c/d sont dans F_n. Prouvons alors qu'ils sont consécutifs pour $n \leq b+d-1$. Supposons qu'ils ne le soient pas : il existe une fraction h/k avec $a/b < h/k < c/d$. Il nous faut montrer que $k \geq b+d$ et alors on aura ce que l'on veut.
Mais on a l'égalité :

$$k = (bc-ad)k = b(ck-dh) + d(bh-ak). \quad (1)$$

Et les inégalités $a/b < h/k < c/d$ montrent qu'on a aussi $ck-dh \geq 1$ et $bh-ak \geq 1$. Et ainsi $k \geq b+d$.
En conclusion, toute fraction se trouvant entre a/b et c/d a un dénominateur $k \geq b+d$. Donc pour $n \leq b+d-1$, les fractions a/b et c/d sont consécutives dans F_n. Ceci conclut la preuve. □

Lemme 1.5. *Soit $0 \leq \frac{a}{b} < \frac{c}{d} \leq 1$ avec $bc-ad=1$. Notons h/k la médiane des fractions a/b et c/d. Alors $a/b < h/k < c/d$, et ces fractions vérifient les relations :*

$$bh-ak = 1, ck-dh = 1.$$

Démonstration. Comme h/k se trouve entre a/b et c/d, on a $ck-dh \geq 1$ et $bh-ak \geq 1$. Enfin l'équation (1) de la preuve précédente montre que $k = b+d$ si et seulement si $ck-dh=1$ et $bh-ak=1$. □

La prochaine proposition nous explique comment construire F_{n+1} à partir de F_n.

Proposition 1.6. *L'ensemble F_{n+1} contient F_n. Chaque fraction de F_{n+1} qui n'est pas dans F_n est la médiane de deux fractions consécutives dans F_n. De plus, si $a/b < c/d$ dans l'un quelconque des F_n, alors on a la relation dite unimodulaire : $bc-ad=1$.*

Démonstration. On procède par récurrence sur n. Pour $n=1$, les fractions $0/1$ et $1/1$ sont consécutives et vérifient la relation unimodulaire. On passe de F_1 à F_2 en insérant leur médiane $1/2$.

Supposons désormais que a/b et c/d sont consécutives dans F_n et satisfont la relation unimodulaire. Alors, d'après le lemme 1.4, elles sont consécutives dans F_m pour m satisfaisant :

$$\max(b,d) \leq m \leq b+d-1.$$

On forme leur médiane h/k où $h=a+c$, $k=b+d$. D'après le lemme 1.5, on a $bh-ak=1$ et $ck-dh=1$, donc h et k sont premiers entre eux. Les fractions a/b et c/d sont consécutives dans F_m pour $\max(b,d) \leq m \leq b+d-1$, mais ne sont pas consécutives dans F_k, vu que $k=b+d$ et que h/k se trouve dans F_k entre a/b et c/d. Mais les deux nouvelles paires $a/b < h/k$ et $h/k < c/d$ sont désormais consécutives dans F_k puisque $k = \max(b,k) = \max(d,k)$. Ces deux paires satisfont toujours la relation unimodulaire.

On a donc montré que pour passer de F_n à F_{n+1} on ajoute seulement des médianes de paires consécutives dans F_n, et que les nouvelles paires satisfont les relations unimodulaires. Ainsi F_{n+1} a toutes les propriétés demandées. □

1.3.2 Cercles de Ford

Définition 1.3.2. *Soit un nombre rationnel h/k avec $(h,k)=1$. Le cercle de Ford lié à cette fraction, noté $C(h,k)$, est le cercle dans le plan complexe de rayon $1/(2k^2)$ centré en $h/k+i/(2k^2)$ (figure ci-dessous).*

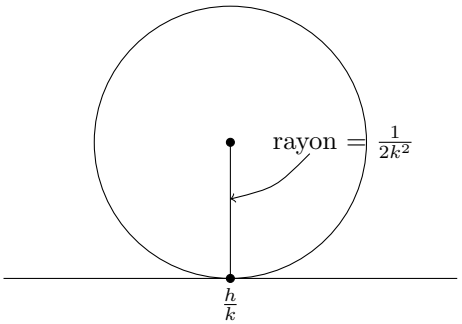


Figure 1.1

Proposition 1.7. *Deux cercles de Ford, $C(a,b)$ et $C(c,d)$ sont soit tangents l'un à l'autre, soit ne s'intersectent pas. Ils sont tangents si et seulement si $bc-ad=\pm 1$. En particulier, les cercles de Ford de deux fractions consécutives dans l'un des ensembles de Farey sont tangents l'un à l'autre.*

Démonstration.

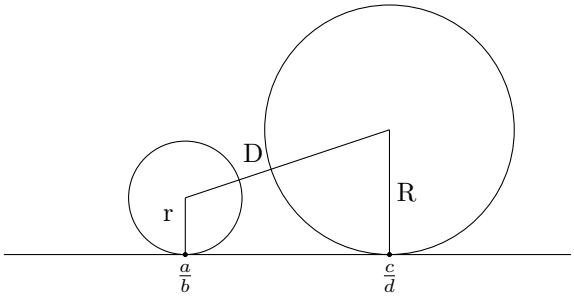


Figure 1.2

Cette figure nous montre que le carré de la distance D entre les centres est :

$$D^2=\left(\frac{a}{b}-\frac{c}{d}\right)^2+\left(\frac{1}{2b^2}-\frac{1}{2d^2}\right)^2$$

alors que le carré de la somme de leurs rayons est :

$$(r+R)^2=\left(\frac{1}{2b^2}+\frac{1}{2d^2}\right)^2.$$

Ainsi la différence $D^2-(r+R)^2$ vaut :

$$\begin{aligned}D^2-(r+R)^2&=\left(\frac{ad-bc}{bd}\right)^2+\left(\frac{1}{2b^2}-\frac{1}{2d^2}\right)^2-\left(\frac{1}{2b^2}+\frac{1}{2d^2}\right)^2\\&=\frac{(ad-bc)^2-1}{b^2d^2}\geq 0,\end{aligned}$$

avec égalité si et seulement si $(ab-cd)^2=1$. □

Proposition 1.8. *Soit $h_1/k_1 < h/k < h_2/k_2$ trois fractions de Farey consécutives (i.e. consécutives dans un des ensembles de Farey). Les points de tangence de $C(h,k)$ avec $C(h_1,k_1)$ et $C(h_2,k_2)$ sont respectivement les points :*

$$\tau_1(h,k) = \frac{h}{k} - \frac{k_1}{k(k^2+k_1^2)} + \frac{i}{k^2+k_1^2}$$

et :

$$\tau_2(h,k) = \frac{h}{k} + \frac{k_1}{k(k^2+k_2^2)} + \frac{i}{k^2+k_2^2}.$$

Démonstration.
La figure 1.3 montre que

$$\tau_1(h,k) = \left(\frac{h}{k} - a\right) + i\left(\frac{1}{2k^2} - b\right).$$

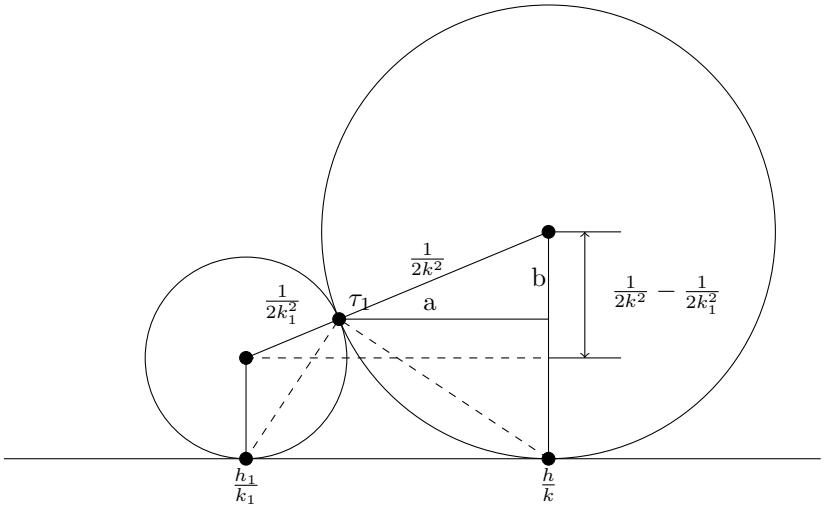


Figure 1.3

Un coup de théorème de Thalès nous permet d'obtenir que :

$$\frac{a}{\frac{h}{k}-\frac{h_1}{k_1}} = \frac{\frac{1}{2k^2}}{\frac{1}{2k^2}+\frac{1}{2k_1^2}} = \frac{k_1^2}{k^2+k_1^2} \text{ et donc } a = \frac{k_1}{k(k^2+k_1^2)}.$$

De même on trouve que :

$$\frac{b}{\frac{1}{2k^2}} = \frac{\frac{1}{2k^2}-\frac{1}{2k_1^2}}{\frac{1}{2k^2}+\frac{1}{2k_1^2}} = \frac{k_1^2-k^2}{k_1^2+k^2} \text{ et donc } b = \frac{1}{2k^2}\frac{k_1^2-k^2}{k_1^2+k^2}.$$

Et ces formules donnent celle souhaitée pour $\tau_1(h,k)$. De même, on obtient les bonnes formules pour $\tau_2(h,k)$. □

1.3.3 Retour au cercle

Pour simplifier les calculs qui suivront, nous allons ramener chacun des cercles de Ford à un même cercle. Ceci est décrit par le changement de variables suivant :

Lemme 1.9. *Le changement de variable*

$$z = -ik^2\left(\tau - \frac{h}{k}\right)$$

transforme le cercle de Ford $C(h,k)$ en un cercle K de rayon $1/2$ centré en $z = 1/2$. Les points de contact $\tau_1(h,k)$ et $\tau_2(h,k)$ du théorème 1.8 deviennent les points :

$$z_1(h,k) = \frac{k^2}{k^2+k_1^2} + i\frac{kk_1}{k^2+k_1^2}$$

et

$$z_2(h,k) = \frac{k^2}{k^2+k_2^2} - i\frac{kk_2}{k^2+k_2^2}.$$

De plus, l'arc supérieur joignant $\tau_1(h,k)$ et $\tau_2(h,k)$ devient l'arc de K reliant $z_1(h,k)$ et $z_2(h,k)$ et ne touchant pas l'axe imaginaire, comme le montre la figure 1.4.

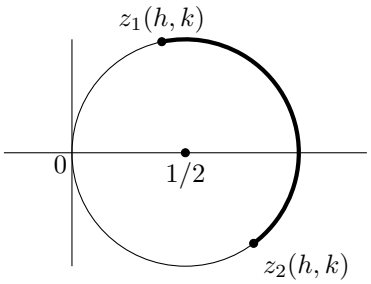


Figure 1.4

Démonstration. La translation $\tau - h/k$ déplace $C(h,k)$ vers la gauche de h/k et place donc son centre à $i/(2k^2)$. La multiplication par $-ik^2$ permet d'amener le rayon du cercle à $1/2$ et fait tourner de cercle de $-\pi/2$. Les expressions de $z_1(h,k)$ et $z_2(h,k)$ se calculent facilement. □

Enfin, on va chercher à obtenir des majorations sur ce nouveau cercle.

Lemme 1.10. *Pour les points z_1 et z_2 du lemme 1.9 on a :*

$$|z_1(h,k)| = \frac{k}{\sqrt{k^2+k_1^2}}$$

$$|z_2(h,k)| = \frac{k}{\sqrt{k^2+k_2^2}}$$

De plus, si z est sur la corde joignant z_1 à z_2 on a :

$$|z| < \frac{\sqrt{2}k}{N}$$

avec N tel que $h_1/k_1 < h/k < h_2/k_2$ sont consécutifs dans F_N. Enfin la longueur de la corde n'excède pas $2\sqrt{2}k/N$.

Démonstration. Les formules pour le calcul de $|z_1(h,k)|$ et $|z_2(h,k)|$ s'obtiennent directement. La majoration sur la corde se trouve en écrivant que, si z est sur la corde, alors $|z(h,k)| \leq \max(|z_1(h,k)|\,|z_2(h,k)|)$. Il suffit donc de prouver que :

$$|z_1| < \frac{\sqrt{2}k}{N} \text{ et } |z_2| < \frac{\sqrt{2}k}{N}.$$

On utilise pour ce faire l'inégalité arithmético-géométrique sous la forme :

$$\frac{k+k_1}{2} \leq \left(\frac{k^2+k_1^2}{2}\right)^{1/2}.$$

Ce qui nous donne :

$$(k^2+k_1^2)^{1/2} \geq \frac{k+k_1}{\sqrt{2}} \geq \frac{N+1}{2} \geq \frac{N}{2}.$$

Pour obtenir la deuxième inégalité on utilise que $k = k_1 + k_2$ et que, selon la proposition 1.6, on a $N-1 \leq k_1 + k_2$. On obtient ainsi les majorations en combinant ce résultat au calcul explicite de $|z_1(h,k)|$ et $|z_2(h,k)|$.

Enfin la longueur de la corde est $\leq |z_1| + |z_2|$. □

1.3.4 Contour $P(N)$

Comme nous allons le voir dans le vif de la preuve, intégrer directement autour de 0 n'est pas simple. Dans toute la suite, nous allons donc jongler entre le cercle unité et le demi-plan supérieur via la transformation $z \to e^{2i\pi z}$. Pour cela, au lieu d'intégrer en tournant autour de 0, nous allons choisir un chemin, dans le demi-plan supérieur, reliant les points i et $i+1$.

Pour tout entier N, nous allons considérer un contour d'intégration, noté $P(N)$, joignant les points i et $i+1$.
Pour ce faire on considère les cercles de Ford de l'ensemble de Farey F_N. Les propositions 1.7 et 1.8 montrent que l'on peut considérer le chemin constitué par les arcs supérieurs reliant deux cercles de Ford correspondant à deux fractions consécutives dans F_N. Voici par exemple le contour $P(3)$:

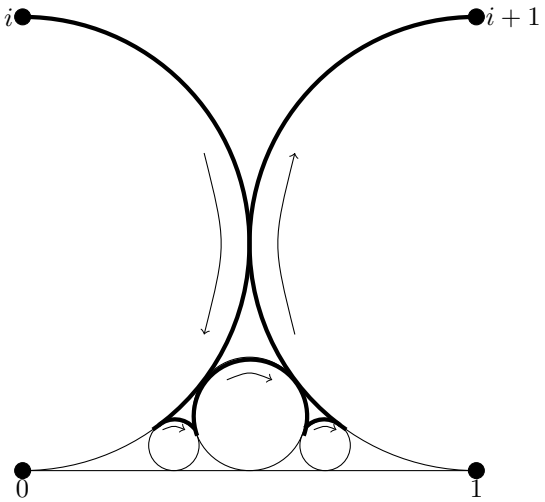


Figure 1.5 : le contour d'intégration P(3)

Une ultime remarque avant de prouver le résultat de Rademacher. On remarque que quand N augmente, on se retrouve à intégrer sur une partie de plus en plus importante du cercle de Ford et l'on se rapproche de plus en plus de l'axe des abscisses.

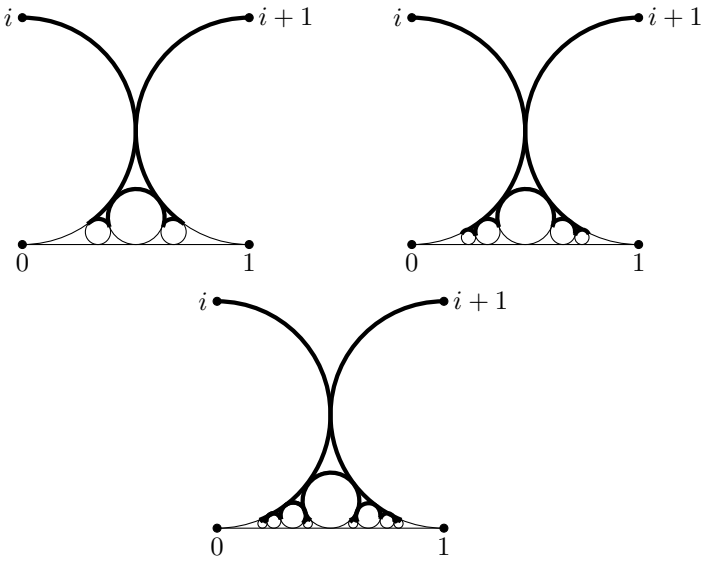


Figure 1.6 : les contours d'intégration $P(3)$, $P(4)$ et $P(5)$

Ainsi, on voit bien que ce contour permet d'intégrer dans le demi-plan supérieur au voisinage de chaque élément de $\mathbb{Q} \cap [0,1]$, ce qui correspondra à intégrer dans le disque unité près des racines de l'unité.

1.4 Nombre de partitions

1.4.1 Preuve

Théorème 1.11. *Si $n \geq 1$, le nombre de partitions $p(n)$ est égal à la série convergente :*

$$p(n) = \frac{1}{\pi\sqrt{2}} \sum_{k=1}^{\infty} A_k(n)\sqrt{k} \frac{d}{dn} \left(\frac{\sinh\left\{ \frac{\pi}{k} \sqrt{\frac{2}{3}\left(n - \frac{1}{24}\right)} \right\}}{\sqrt{n - \frac{1}{24}}} \right),$$

avec :

$$A_k(n) = \sum_{\substack{0 \leq h < k \\ (h,k)=1}} e^{\pi i s(h,k) - 2\pi i n h/k}.$$

Démonstration. On a, par le théorème des résidus que :

$$p(n) = \frac{1}{2i\pi} \int_C \frac{F(x)}{x^{n+1}} dx$$

avec $F(x) = \sum_{n\geq 1} p(n)x^n = \prod_{n\geq 1} \frac{1}{1-x^n}$,
et C est une courbe orientée dans le sens positif, entourant $x = 0$ et tracée dans le cercle unité.

Le changement de variable $x = e^{2\pi i\tau}$ transforme le cercle unité en la bande verticale semi-infinie entre 0 et 1 dans le demi-plan supérieur. Si C est un cercle de centre 0 de rayon $e^{-2\pi}$, le point τ varie de i à $i+1$ le long d'un segment horizontal. Au lieu d'intégrer selon ce segment, nous allons intégrer selon les contours $P(N)$ décrits précédemment.
On a alors :

$$p(n) = \int_i^{i+1} F(e^{2\pi i\tau})e^{2\pi in\tau}d\tau = \int_{P(N)} F(e^{2\pi i\tau})e^{2\pi in\tau}d\tau.$$

Dans toute la discussion n est fixé, et on fera tendre à la toute fin N vers l'infini.

On va découper le contour d'intégration $P(N)$ selon les différents cercles de Ford :

$$\int_{P(N)} = \sum_k \sum_{\substack{0\leq h<k \\ (h,k)=1}} \int_{\gamma(h,k)} = \sum_{h,k} \int_{\gamma(h,k)},$$

où $\gamma(h,k)$ désigne la partie du cercle de Ford $C(h,k)$ contenue dans $P(N)$, et où on a abrégé l'écriture de la double somme dans la deuxième expression.

On fait alors le changement de variable décrit plus haut :

$$z = -ik^2\left(\tau - \frac{h}{k}\right).$$

Par le lemme 1.9, on se retrouve à intégrer sur un arc de cercle du cercle K de centre 1/2 et de rayon 1/2, et joignant les points $z_1(h,k)$ et $z_2(h,k)$ définis dans ce même théorème.

On a donc désormais :

$$\begin{aligned} p(n) &= \sum_{h,k} \int_{z_1(h,k)}^{z_2(h,k)} F\left(\exp\left(\frac{2i\pi h}{k} - \frac{2\pi z}{k^2}\right)\right) \frac{i}{k^2} e^{-2\pi inh/k} e^{2n\pi z/k^2} dz \\ &= \sum_{h,k} ik^{-2} e^{-2\pi inh/k} \int_{z_1(h,k)}^{z_2(h,k)} F\left(\exp\left(\frac{2i\pi h}{k} - \frac{2\pi z}{k^2}\right)\right) e^{2n\pi z/k^2} dz. \end{aligned}$$

On utilise ici l'équation fonctionnelle du théorème 1.2 pour F qui montre que :

$$F(x) = \omega(h,k)\left(\frac{z}{k}\right)^{1/2} \exp\left(\frac{\pi}{12z} - \frac{\pi z}{12k^2}\right) F(x')$$

pour :

$$x = \exp\left(\frac{2i\pi h}{k} - \frac{2\pi z}{k^2}\right),\ x' = \exp\left(\frac{2i\pi H}{k} - \frac{2\pi}{z}\right)$$

et :

$$\omega(h,k) = e^{\pi is(h,k)}, (h,k) = 1, hH \equiv -1[k]$$

On note $\Psi_k(z) = z^{1/2}\exp(\pi/(12z) - \pi z/(12k^2))$ et on divise l'intégrale en deux parties en écrivant :

$$F(x') = 1 + [F(x') - 1].$$

Et donc on a :

$$p(n) = \sum_{h,k} ik^{-5/2}\omega(h,k)e^{-2\pi inh/k}(I_1(h,k) + I_2(h,k)),$$

où :

$$I_1(h,k) = \int_{z_1(h,k)}^{z_2(h,k)} \Psi_k(z)e^{2n\pi z/k^2}dz$$

et :

$$I_2(h,k) = \int_{z_1(h,k)}^{z_2(h,k)} \Psi_k(z)\left[F\left(\exp\left(\frac{2i\pi H}{k} - \frac{2\pi}{z}\right)\right) - 1\right]e^{2n\pi z/k^2}dz.$$

Pourquoi a-t-on scindé ainsi l'intégrale ? Dans notre problème on étudie F au voisinage des racines de l'unité et, pour ce faire, on regarde $F(x)$ pour $|z|$ petit. Mais grâce à l'équation fonctionnelle, cela nous amène à regarder $F(x')$ avec x' qui se rapproche de zéro quand $|z|$ se rapproche de zéro. Et $F(0) = 1$ donc on s'attend à avoir I_2 négligeable devant I_1 quand N augmente.

Pour évaluer $I_2(h,k)$, on modifie le contour d'intégration pour intégrer non plus selon l'arc mais selon la corde entre z_1 et z_2 comme le montre le dessin suivant :

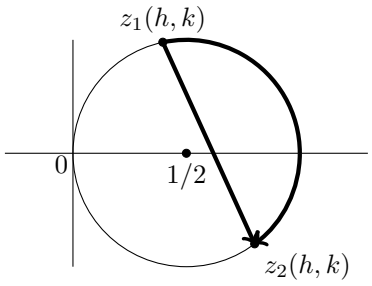


Figure 1.7

On rappelle que, par le lemme 1.10, si z est sur la corde joignant z_1 à z_2 on a $|z| < \frac{\sqrt{2}k}{N}$ et que la longueur de la corde n'excède pas $2\sqrt{2}k/N$.

De plus, on peut voir directement que la transformation $w = 1/z$ transforme le disque K en le demi-plan $Re(z) \geq 1$.

Dès lors, on a aussi les majorations : $0 < Re(z) \leq 1$ et $Re(1/z) \geq 1$. Et ce sont ces majorations qui vont permettre d'avoir un comportement intéressant en zéro.

On peut désormais estimer l'intégrande de I_2 sur la corde :

$$
\begin{aligned}
&\left|\Psi_k(z)\left[F\left(\exp\left(\frac{2i\pi h}{k}-\frac{2\pi z}{k^2}\right)\right)-1\right]e^{2n\pi z/k^2}\right| \\
&= |z|^{1/2}\exp\left\{\frac{\pi}{12}Re(\frac{1}{z})-\frac{\pi}{12k^2}Re(z)\right\}\times e^{2\pi nRe(z)/k^2}\left|\sum_{m=1}^{\infty}p(m)e^{2i\pi Hm/k}e^{-2\pi m/z}\right| \\
&\leq |z|^{1/2}\exp\left\{\frac{\pi}{12}Re(\frac{1}{z})\right\}e^{2\pi n/k^2}\sum_{m=1}^{\infty}p(m)e^{-2\pi mRe(1/z)} \\
&< |z|^{1/2}\,e^{2\pi n}\sum_{m=1}^{\infty}p(m)e^{-2\pi(m-(1/24))Re(1/z)} \\
&\leq |z|^{1/2}\,e^{2\pi n}\sum_{m=1}^{\infty}p(m)e^{-2\pi(m-(1/24))} \\
&= |z|^{1/2}\,e^{2\pi n}\sum_{m=1}^{\infty}p(m)e^{-2\pi(24m-1)/24)} \\
&< |z|^{1/2}\,e^{2\pi n}\sum_{m=1}^{\infty}p(24m-1)e^{-2\pi(24m-1)/24)} \\
&= |z|^{1/2}\,e^{2\pi n}\sum_{m=1}^{\infty}p(24m-1)y^{24m-1}\text{ où }y=e^{-2\pi/24} \\
&= c\,|z|^{1/2},
\end{aligned}
$$

où l'on a posé : $c = e^{2\pi n}\sum_{m=1}^{\infty}p(24m-1)y^{24m-1}$. La constante c ne dépend donc ni de z ni de N. Elle dépend de n, mais on l'a fixé dans cette discussion. Comme sur la corde, on a $|z| < \frac{\sqrt{2}k}{N}$, l'intégrande est borné par $c2^{1/4}(k/n)^{1/2}$. Comme la longueur de la corde est $\leq |z_1| + |z_2|$, on trouve :

$$|I_2(h,k)| < Ck^{3/2}N^{-3/2},$$

pour une certaine constante C, et donc :

$$
\begin{aligned}
\left|\sum_{h,k}ik^{-5/2}\omega(h,k)e^{-2\pi inh/k}I_2(h,k)\right| &< \sum_{k=1}^{N}\sum_{\substack{0\leq h<k\\(h,k)=1}}Ck^{-1}N^{-3/2} \\
&\leq CN^{-3/2}\sum_{k=1}^{N}1 \\
&= CN^{-1/2}
\end{aligned}
$$

On peut donc écrire :

$$p(n) = \sum_{h,k}ik^{-5/2}\omega(h,k)e^{-2\pi inh/k}I_1(h,k) + O(N^{-1/2}).$$

On s'occupe maintenant de $I_1(h,k)$. On a vu en section 1.3.4 que l'on est amené, quand N tend vers l'infini, à intégrer sur tout le cercle de Ford. Il semble

donc logique d'estimer $I_1(h,k)$, en intégrant le long du cercle K.

$$I_1(h,k) = \int_{K_-} - \int_0^{z_1(h,k)} - \int_{z_2(h,k)}^0 = \int_{K_-} -J_1 - J_2,$$

où on désigne par K_- l'intégrale le long du cercle selon le sens négatif. Pour estimer $|J_1|$, on remarque que la longueur de la corde joignant 0 à $z_1(h,k)$ est inférieure à

$$\pi \left| z_1(h,k) \right| < \pi\sqrt{2}\frac{k}{N}.$$

Comme $Re(1/z) = 1$ et $0 < Re(z) \leq 1$ sur le cercle K, on majore l'intégrande :

$$\begin{aligned} \left| \Psi_k(z) e^{2n\pi z/k^2} \right| &= e^{2n\pi Re(z)/k^2} \left| z \right|^{1/2} \exp\left\{ \frac{\pi}{12} Re(\frac{1}{z}) - \frac{\pi}{12k^2} Re(z) \right\} \\ &\leq \frac{e^{2n\pi} 2^{1/4} k^{1/2} e^{\pi/12}}{N^{1/2}} \end{aligned}$$

et ainsi :

$$|J_1| < C_1 k^{3/2} N^{-3/2},$$

où C_1 est une constante. Comme précedemment on somme sur h et k et on obtient un terme en $O(N^{-1/2})$ dans l'expression de $p(n)$.
Une estimation similaire sur J_2 nous conduit également à un terme en $O(N^{-1/2})$ dans la formule de $p(n)$. Ainsi on obtient :

$$p(n) = \sum_{k=1}^{N} \sum_{\substack{0 \leq h < k \\ (h,k)=1}} i k^{-5/2} \omega(h,k) e^{-2\pi i n h/k} \int_{K_-} \Psi_k(z) e^{2n\pi z/k^2} dz + O(N^{-1/2}).$$

On fait maintenant tendre N vers l'infini pour obtenir :

$$p(n) = i \sum_{k=1}^{\infty} A_k(n) k^{-5/2} \int_{K_-} z^{1/2} \exp\left\{ \frac{\pi}{12z} - \frac{2\pi z}{k^2} \left(n - \frac{1}{24} \right) \right\} dz,$$

où

$$A_k(n) = \sum_{\substack{0 \leq h < k \\ (h,k)=1}} e^{\pi i s(h,k) - 2\pi i n h/k}.$$

La preuve est ici terminée. Nous allons simplement l'écrire plus explicitement en terme de fonction de Bessel pour obtenir l'expression désirée.
On fait pour cela le changement de variable :

$$w = \frac{1}{z}$$

qui nous donne alors :

$$p(n) = \frac{1}{i} \sum_{k=1}^{\infty} A_k(n) k^{-5/2} \int_{1-\infty i}^{1+\infty i} w^{-5/2} \exp\left\{ \frac{\pi w}{12} - \frac{2\pi}{w k^2} \left(n - \frac{1}{24} \right) \right\} dw.$$

On pose maintenant $t = \pi w/12$ et la formule devient :

$$p(n) = 2\pi \left(\frac{\pi}{12}\right)^{3/2} \sum_{k=1}^{\infty} A_k(n) k^{-5/2} \frac{1}{2i\pi} \int_{c-\infty i}^{c+\infty i} t^{-5/2} \exp\left\{t - \frac{\pi^2}{6tk^2}\left(n - \frac{1}{24}\right)\right\} dt$$

où $c = \pi/12$. On définit la fonction de Bessel :

$$I_\nu(z) = \frac{(\frac{1}{2}z)^\nu}{2i\pi} \int_{c-\infty i}^{c+\infty i} t^{-\nu-1} e^{t+(z^2/4t)} dt \text{ où } c > 0, Re(\nu) > 0.$$

On applique cette formule à :

$$z = 2\left(\frac{\pi^2}{6k^2}(n - 1/24)\right)$$

et $\nu = 3/2$, on obtient :

$$p(n) = \frac{(2\pi)\left(n - \frac{1}{24}\right)^{-3/4}}{24^{3/4}} \sum_{k=1}^{\infty} A_k(n) k^{-1} I_{3/2}\left(\frac{\pi}{k}\sqrt{\frac{2}{3}\left(n - \frac{1}{24}\right)}\right).$$

Enfin on a l'identité, démontrée dans [Wat95] :

$$I_{3/2}(z) = \sqrt{\frac{2z}{\pi}} \frac{d}{dz}\left(\frac{\sinh z}{z}\right).$$

Ceci nous donne enfin la formule trouvée par Rademacher :

$$p(n) = \frac{1}{\pi\sqrt{2}} \sum_{k=1}^{\infty} A_k(n)\sqrt{k} \frac{d}{dn}\left(\frac{\sinh\left\{\frac{\pi}{k}\sqrt{\frac{2}{3}\left(n - \frac{1}{24}\right)}\right\}}{\sqrt{n - \frac{1}{24}}}\right).$$

□

1.4.2 Interprétation de la série

Comportement asymptotique : On va d'abord admettre que l'on a un vrai développement asymptotique c'est-à-dire que :

$$\frac{\sum_{k>k_0} A_k(n)\sqrt{k}\frac{d}{dn}\left(\frac{\sinh\left\{\frac{\pi}{k}\sqrt{\frac{2}{3}\left(n-\frac{1}{24}\right)}\right\}}{\sqrt{n-\frac{1}{24}}}\right)}{A_{k_0}(n)\sqrt{k_0}\frac{d}{dn}\left(\frac{\sinh\left\{\frac{\pi}{k_0}\sqrt{\frac{2}{3}\left(n-\frac{1}{24}\right)}\right\}}{\sqrt{n-\frac{1}{24}}}\right)} \longrightarrow_{n\to\infty} 0.$$

Dès lors le premier terme de la série nous donne l'équivalent. Ce premier terme est :

$$A_1(n)\frac{d}{dn}\left(\frac{\sinh\left\{\pi\sqrt{\frac{2}{3}\left(n - \frac{1}{24}\right)}\right\}}{\sqrt{n - \frac{1}{24}}}\right) \sim \frac{e^{\pi\sqrt{\frac{2}{3}n}}}{4n\sqrt{3}}.$$

Ceci est bien l'équivalent trouvé par Hardy et Ramanujan en 1918 dans leurs travaux.

Importance des pôles : Quand $N \to \infty$ on peut voir que l'on intègre entièrement sur les cercles de Ford et ce, en se rapprochant de plus en plus des fractions des ensembles de Farey. Cette interprétation se fait en coordonnées τ. En coordonnées x, cela correspond à des contours qui se rapprochent de plus en plus des racines de l'unité. On a donc intégré sur un contour de plus en plus proche des singularités, comme prévu.
Ceci nous permet d'interpréter la provenance de chaque terme de la série. Si l'on revient à ce qu'était k initialement, on voit que le k-ième terme correspond à la contribution des singularités de F au niveau des racines k-ièmes primitives de l'unité.
Si l'on compare ce résultat avec celui qui précède, à savoir que la formule donne un véritable développement asymptotique, on se rend compte que c'est le comportement de F en 1 qui nous donne l'équivalent de $p(n)$. Puis que le comportement en -1 donne le second terme est ainsi de suite...

Formule exacte sur des entiers : La formule précédente présente la particularité d'être exacte. De plus, $p(n)$ est entier. Ainsi cette formule permet de calculer de façon rapide le nombre de partitions de grands nombres. Le lecteur intéressé se réfèrera à [Rad73] aux pages 275 et suivantes, dans lesquelles on prouve que pour $N = [2\sqrt{n}/3]$ on peut arrondir au plus proche entier et obtenir le bon résultat.
Il existe également une technique encore plus rapide pour calculer ce nombre de partitions, en utilisant les congruences de $p(n)$. Par exemple, on connait les congruences de certains $p(n)$ modulo 11^c pour c entier, et ainsi on peut tronquer le calcul bien plus tôt et prendre le multiple de 11^c le plus proche, ce qui améliore considérablement le nombre de termes nécessaires ! On pourra par exemple se référer à [Wat95] pour une explication plus détaillée de la méthode. Des exemples de congruence du nombre de partitions sont donnés sur le site internet [MatWo].

Chapitre 2

Fonctions elliptiques

2.1 Généralités sur les fonctions périodiques

2.1.1 Fonction doublement périodique

Définition 2.1.1. *On appelle fonction périodique de période $\omega \in \mathbb{C}^*$ toute fonction complexe $f : \mathbb{C} \to \mathbb{C} \cup \{\infty\}$ telle que :*

$$\forall z \in \mathbb{C}, f(z+\omega) = f(z).$$

Cela implique en particulier :

$$\forall z \in \mathbb{C}, \forall n \in \mathbb{N}, f(z+n\omega) = f(z).$$

Définition 2.1.2. *Une fonction complexe $f : \mathbb{C} \to \mathbb{C} \cup \{\infty\}$ est dite fonction doublement périodique s'il existe deux périodes $\omega_1 \in \mathbb{C}^*$ et $\omega_2 \in \mathbb{C}^*$ de quotient non réel tels que*

$$\forall z \in \mathbb{C}, \forall n, m \in \mathbb{N}, f(z+n\omega_1+m\omega_2) = f(z).$$

Remarque : On demande au quotient $\frac{\omega_1}{\omega_2}$ de ne pas être réel afin d'éviter des cas de dégénérescence. Par exemple, si le quotient est rationnel égal à a/b avec $(a,b) = 1$, on peut voir que $\omega = \omega_1/a = \omega_2/b$ est période de la fonction. S'il est irrationnel on peut montrer qu'il possède des périodes arbitrairement petites. Dès lors, on peut voir que pour une fonction holomorphe, cela entraîne que la fonction est constante. En fait montrons plus généralement qu'une fonction f avec des périodes arbitrairement petites est constante sur chaque ouvert connexe où elle est analytique. En effet en chaque point où f est analytique on a :

$$f'(z) = \lim_{z_n \to 0} \frac{f(z+z_n) - f(z)}{z_n},$$

où les z_n sont une suite de nombres complexes non nuls tendant vers 0. Si f a des périodes arbitrairement petites alors on peut prendre pour ces z_n une suite de périodes tendant vers 0. Ceci implique que $f'(z) = 0$ et ce en tout point d'analyticité de f. Donc f doit être constante sur chaque ouvert connexe où elle est analytique.

Définition 2.1.3. *Soit f fonction doublement périodique de périodes ω_1 et ω_2 dont le quotient $\frac{\omega_1}{\omega_2}$ n'est pas réel. La paire (ω_1, ω_2) est dite paire fondamentale si toute période de f est de la forme $n\omega_1 + m\omega_2$ où m et n sont des entiers.*

Définition 2.1.4. *Si (ω_1,ω_2) est une paire fondamentale de f, on appellera parallélogramme fondamental le parallélogramme engendré par les vecteurs ω_1 et ω_2 et passant par 0 :*

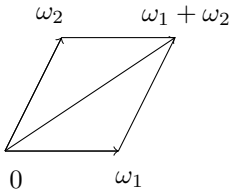


Figure 2.1

On obtient ainsi un pavage du plan en un réseau, noté $\Omega(\omega_1, \omega_2) = \omega_1\mathbb{Z} + \omega_2\mathbb{Z}$:

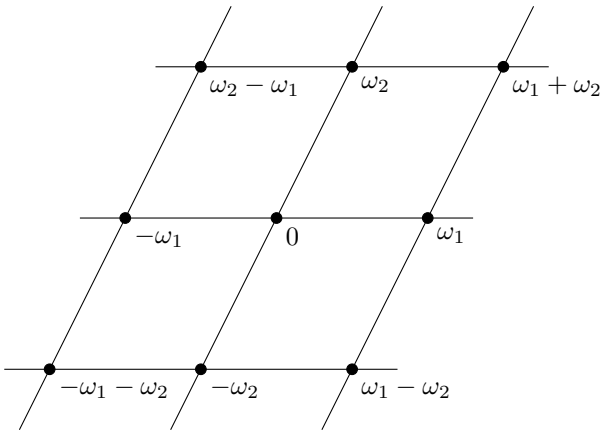


Figure 2.2

Définition 2.1.5. *Deux paires (ω_1,ω_2) et (ω'_1,ω'_2), chacune de quotient non réel, sont dites équivalentes si et seulement si elles engendrent le même réseau : $\Omega(\omega_1, \omega_2)$=$\Omega(\omega'_1, \omega'_2)$.*

Théorème 2.1. *Deux paires (ω_1,ω_2) et (ω'_1,ω'_2) sont équivalentes si et seulement s'il existe une matrice 2×2 : $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ à coefficients entiers et de déterminant $ab - cd = \pm 1$ telle que :*

$$\begin{pmatrix} \omega'_2 \\ \omega'_1 \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} \omega_2 \\ \omega_1 \end{pmatrix}$$

c'est-à-dire que

$$\omega'_2 = a\omega_2 + b\omega_1$$
$$\omega'_1 = c\omega_2 + d\omega_1.$$

Démonstration. On commence par le sens direct. La paire (ω_1, ω_2) est fondamentale pour le réseau qu'elle engendre. Donc il existe $a, b, c, d \in \mathbb{Z}$ tels que

$$\omega_2' = a\omega_2 + b\omega_1$$

$$\omega_1' = c\omega_2 + d\omega_1.$$

On inverse le système et on trouve que

$$\omega_2 = \frac{-b\omega_1 + d\omega_2}{ad - cb}$$

$$\omega_1 = \frac{a\omega_1 - c\omega_2}{ad - cb}.$$

Comme la paire (ω_1', ω_2') est équivalente à (ω_1, ω_2), elle est fondamentale sur le même réseau engendré. Les coefficients sont donc nécessairement entiers, et ainsi $ad - cb = \pm 1$

Réciproquement on suppose qu'on a la relation indiquée. Ainsi $\Omega(\omega_1', \omega_2')$ est contenu dans $\Omega(\omega_1, \omega_2)$ On inverse le système, on utilise la condition sur $ab - cd$ et on obtient l'autre inclusion, donc les deux réseaux engendrés sont les mêmes, et les deux paires sont alors équivalentes. □

Théorème 2.2. *Si (ω_1,ω_2) est une paire fondamentale de périodes, alors dans le triangle de sommets 0, ω_1, ω_2 il n'y a aucune autre période. Réciproquement, si une paire de périodes vérifie cette propriété alors elle est fondamentale.*

Démonstration. On considère le parallélogramme de vecteurs 0, ω_1, ω_2 et $\omega_1 + \omega_2$.

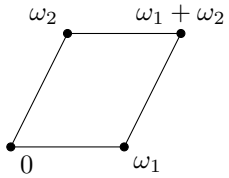


Figure 2.3

Un point à l'intérieur de ce parallélogramme a un affixe de la forme :

$$z = \alpha\omega_1 + \beta\omega_2,$$

où $0 \leq \alpha \leq 1$ et $0 \leq \beta \leq 1$. Parmi tous ces points les seules périodes sont, par définition d'une paire fondamentale, 0, ω_1, ω_2 et $\omega_1 + \omega_2$. Donc le triangle de sommets 0, ω_1, ω_2 ne contient aucune autre période.

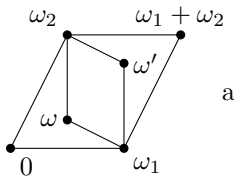
Réciproquement, supposons que le triangle de sommets 0, ω_1, ω_2 ne contient aucune autre période que les sommets et soit ω une période quelconque. Il nous faut montrer que $\omega = n\omega_1 + m\omega_2$ pour $m, n \in \mathbb{Z}$. Comme le quotient $\frac{\omega_2}{\omega_1}$ n'est pas réel les nombres ω_1 et ω_2 sont linéairement indépendants. On peut donc écrire $\omega = t_1\omega_1 + t_2\omega_2$ avec $t_1, t_2 \in \mathbb{R}$. Si on note $[t]$ la partie entière de t on écrit :

$$t_1 = [t_1] + r_1, t_2 = [t_2] + r_2, \text{ où } 0 \leq r_1 < 1 \text{ et } 0 \leq r_2 < 1.$$

Dès lors :

$$\omega - [t_1]\omega_1 - [t_2]\omega_2 = r_1\omega_1 + r_2\omega_2.$$

Si r_1 ou r_2 était non nul, alors $r_1\omega_1 + r_2\omega_2$ serait une période contenue dans le parallélogramme de sommets 0, ω_1, ω_2 et $\omega_1 + \omega_2$. Mais si une période w se trouve dans ce parallélogramme, alors l'un des deux complexes w et $\omega_1 + \omega_2 - w$ se trouve soit dans le triangle de sommets 0, ω_1, ω_2 soit sur la diagonale joignant ω_1 à ω_2 (voir figure 2.4) ce qui contredit l'hypothèse. Donc $r_1 = r_2 = 0$ et ceci complète la preuve.



avec $\omega' + \omega = \omega_1 + \omega_2$

Figure 2.4

□

2.1.2 Fonctions elliptiques

Définition 2.1.6. *Une fonction $f : \mathbb{C} \to \mathbb{C} \cup \{\infty\}$ est dite elliptique si elle vérifie les deux propriétés suivantes :*
- f est doublement périodique.
- f est méromorphe sur $\mathbb{C}$.

Proposition 2.3. *Une fonction f elliptique non constante possède une paire fondamentale de périodes.*

Démonstration. La fonction f étant elliptique elle possède au moins deux périodes de quotient non réel. Parmi toutes les périodes (non nulles), on peut en trouver au moins une dont la distance à l'origine est minimale. Dans le cas contraire, en effet, f aurait des périodes arbitrairement petites donc serait constante sur l'ensemble ouvert connexe des points où elle est analytique, donc constante sur $\mathbb{C}$. On note alors ω une de ces périodes de module minimal.

Parmi les périodes de module $|\omega|$ on prend celle de plus petit argument (qui existe pour la même raison) et on la note ω_1.

S'il y a d'autres périodes de module $|\omega|$ autre que ω_1 et $-\omega_1$, on prend de nouveau celle de plus petit argument immédiatement au dessus de ω_1 et on la note ω_2.

Dans le cas contraire, on regarde le plus petit cercle suivant contenant des périodes qui ne sont pas multiples de ω_1. Parmi les périodes ayant un tel module, on note ω_2 celle de plus petit argument.

Dans tous les cas, on a alors, par construction, qu'il n'y a pas d'autres périodes dans le triangle de sommets 0, ω_1, ω_2, exception faite de ces mêmes vecteurs. Donc d'après le théorème 2.2, la paire (ω, ω_2) est fondamentale. □

Proposition 2.4. *Si f est une fonction elliptique sans pôles dans un parallélogramme fondamental alors f est constante.*

Démonstration. Si f n'a pas de pôles alors, comme f est continue, f est bornée sur ce parallélogramme. Par périodicité, f est bornée sur $\mathbb{C}$ et donc est constante par le théorème de Liouville. □

Corollaire 2.5. *Si une fonction elliptique ne s'annule pas sur un parallélogramme fondamental, alors elle est constante.*

Démonstration. C'est le théorème précédent appliqué à $\frac{1}{f}$. □

Corollaire 2.6. *L'intégrale d'une fonction elliptique le long d'un parallélogramme fondamental vaut zéro.*

Démonstration. L'intégrale le long de deux bords parallèles s'annule par périodicité. □

Corollaire 2.7. *La somme des résidus en les pôles contenus dans un parallélogramme d'une fonction elliptique est nulle.*

Démonstration. Il suffit d'appliquer le théorème des résidus et le corollaire 2.6. □

Remarque : en particulier, ceci implique qu'une fonction elliptique qui n'est pas constante a au moins deux pôles simples ou un pôle double.

Corollaire 2.8. *Le nombre de zéros d'une fonction elliptique non nulle dans un parallélogramme fondamental est égal au nombre de pôles, chacun compté avec multiplicité.*

Démonstration. L'intégrale :

$$\frac{1}{2i\pi}\int_C \frac{f'(z)}{f(z)}\mathrm{d}z$$

prise le long du bord C d'une cellule compte la différence entre le nombre de zéros et de pôles pour la fonction dans la cellule. Mais f'/f est elliptique donc cette intégrale vaut zéro d'après le corollaire 2.6. □

Définition 2.1.7. *On appelle ordre d'une fonction elliptique non nulle son nombre de zéros dans un parallélogramme fondamental. Par le théorème précédent l'ordre donne aussi le nombre de pôles de la fonction.*

2.2 Fonction $\wp$ de Weierstrass

Le but de cette partie est d'introduire la fonction du réseau Δ, appelée discriminant, qui vérifie certaines propriétés intéressantes pour la suite de l'exposé. Nous montrons ici d'où elle provient et pourquoi il est naturel de la considérer.

2.2.1 Construction

On fixe désormais le réseau $\Omega(\omega_1, \omega_2) = \omega_1\mathbb{Z} + \omega_2\mathbb{Z}$.
Nous allons maintenant essayer de construire une fonction elliptique non constante. D'après ce qui précède, il faut que celle-ci ait au moins un pôle double ou bien deux simples. Ceci conduit vers deux possibilités de construction, la première menée par Weierstrass et la seconde par Jacobi. Dans cet exposé nous suivrons les traces de Weierstrass. Nous pouvons supposer que le pôle d'ordre 2 se trouve en zéro et donc, par périodicité, à chaque période ω. Près de chacune de ces périodes, le développement de Laurent doit avoir la forme :

$$\frac{A}{(z-\omega)^2} + \frac{B}{(z-\omega)}.$$

On peut supposer que B=0 et A=1. Nous sommes donc amenés à considérer des sommes du type :

$$\sum_{\omega} \frac{1}{(z-\omega)^2}.$$

Proposition 2.9. *Si α est réel la série :*

$$\sum_{\substack{\omega\in\Omega \\ \omega\neq 0}} \frac{1}{\omega^\alpha}$$

converge si et seulement si $\alpha > 2$.

Démonstration. On note r et R respectivement le minimum et le maximum de la distance à zéro dans le parallélogramme montré dans la figure 2.5 :

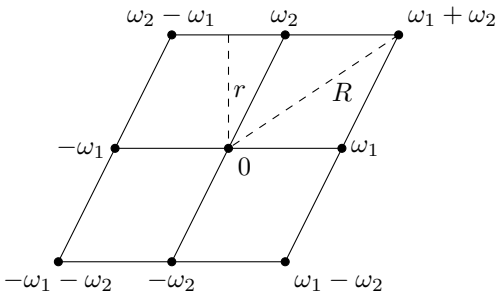


Figure 2.5

Si ω est l'une quelconque des huit périodes non nulles montrée sur ce dessin on a :

$$r \leq |\omega| \leq R \text{ pour huit périodes } \omega.$$

Dans la couche suivante de période entourant ces huit premières on a $2 \times 8 = 16$ nouvelles périodes satisfaisant les inégalités :

$$2r \leq |\omega| \leq 2R \text{ pour seize périodes } \omega.$$

Puis sur la couche suivante on a $3 \times 8 = 24$ périodes satisfaisant :

$$3r \leq |\omega| \leq 3R \text{ pour vingt-quatre périodes } \omega,$$

et ainsi de suite... Ainsi, nous avons les inégalités :

$$\frac{1}{R^\alpha} \leq \frac{1}{|\omega|^\alpha} \leq \frac{1}{r^\alpha} \text{ pour les huit premières périodes } \omega$$

$$\frac{1}{(2R)^\alpha} \leq \frac{1}{|\omega|^\alpha} \leq \frac{1}{(2r)^\alpha} \text{ pour les prochaines seize périodes } \omega$$

et ainsi de suite. Ainsi la somme $S(n) = \sum |\omega|^{-\alpha}$, prise sur les $8(1+2+\cdots+n)$ périodes non nulles les plus proches de l'origine, satisfait les inégalités :

$$\frac{8}{R^\alpha} + \frac{2\cdot 8}{(2R)^\alpha} + \cdots + \frac{n\cdot 8}{(n\cdot R)^\alpha} \leq S(n) \leq \frac{8}{r^\alpha} + \frac{2\cdot 8}{(2r)^\alpha} + \cdots + \frac{n\cdot 8}{(n\cdot r)^\alpha}$$

soit encore :

$$\frac{8}{R^\alpha}\sum_{k=1}^{n}\frac{1}{k^{\alpha-1}} \leq S(n) \leq \frac{8}{r^\alpha}\sum_{k=1}^{n}\frac{1}{k^{\alpha-1}}$$

Ceci montre que la somme partielle S(n) est majorée par $8\zeta(\alpha-1)/r^\alpha = \frac{8}{r^\alpha}\sum_{k=1}^{\infty}\frac{1}{k^{\alpha-1}} < \infty$ si $\alpha > 2$. Ceci étant vrai pour toute les sommes partielles, on a que la série est bornée et donc converge pour $\alpha > 2$. Dans le cas contraire : $\alpha \leq 2$, l'inégalité de droite nous donne que la série diverge. Ceci termine la preuve. □

Proposition 2.10. *Si $\alpha > 2$ et $R > 0$ la série*

$$\sum_{|z|>R}\frac{1}{(z-\omega)^\alpha}$$

converge absolument et uniformément sur le disque $|z| \leq R$.

Démonstration. Nous allons montrer qu'il existe une constante M (dépendant de R et de α) telle que, si $\alpha \geq 1$, on ait :

$$\frac{1}{|z-\omega|^\alpha} \leq \frac{M}{|\omega|^\alpha},$$

et ce, pour tout ω avec $|\omega| > R$ et tout $|z| \leq R$. Et alors nous utiliserons la proposition 2.9 pour prouver celle-ci.

L'inégalité précédente est équivalente à :

$$\frac{1}{M} \leq \frac{|z-\omega|^\alpha}{|\omega|^\alpha}.$$

Pour trouver un tel M on considère tout les $\omega \in \Omega$ avec $|\omega| > R$. On prend celui de module minimal, par exemple $|\omega| = R + d$ avec $d > 0$. Alors si $|z| \leq R$ et $|\omega| \geq R + d$ on a :

$$\left|\frac{z-\omega}{\omega}\right| = \left|1 - \frac{z}{\omega}\right| \geq 1 - \left|\frac{z}{\omega}\right| \geq 1 - \frac{R}{R+d}$$

et donc :

$$\left|\frac{z-\omega}{\omega}\right|^\alpha \geq \left(1 - \frac{R}{R+d}\right)^\alpha = \frac{1}{M},$$

où :

$$M = \left(1 - \frac{R}{R+d}\right)^{-\alpha}.$$

Et M ainsi choisit convient bien. Ceci conclut la preuve. □

Dès lors on ne peut plus considérer la somme initiale :

$$\sum_{\omega} \frac{1}{(z-\omega)^2}.$$

On va remplacer l'exposant 2 par 3.

Proposition 2.11. *Soit f la fonction définie par :*

$$\sum_{\omega} \frac{1}{(z-\omega)^3}.$$

Alors f est elliptique de périodes ω_1 et ω_2 avec un pôle d'ordre 3 à chaque période $\omega \in \Omega$.

Démonstration. La proposition 2.10 montre que la série obtenue en sommant les périodes de modules $\omega > R$ converge absolument sur le disque $|z| \leq R$. Ainsi f est analytique sur le disque. Les termes restants, qui sont en nombre fini, sont également analytiques sur le disque sauf pour un pôle d'ordre 3 à chaque période du disque. Ceci montre que f est bien méromorphe avec un pôle d'ordre 3 à chaque période $\omega \in \Omega$. Enfin on a bien $f(z) = f(z+\omega_1) = f(z+\omega_2)$ en remarquant que ce n'est qu'une réorganisation de la somme et en utilisant la convergence absolue pour sommer dans un ordre quelconque. □

On utilise le théorème précédent pour créer une fonction elliptique d'ordre 2. On se contente pour cela d'intégrer f terme à terme depuis l'origine (cela conserve le caractère elliptique). Ceci nous conduit, moyennant des multiplications par des constantes, à la fonction suivante.

Définition 2.2.1. *La fonction $\wp$ de Weierstrass est définie par la série :*

$$\wp(z) = \frac{1}{z^2} + \sum_{\omega \neq 0} \left\{ \frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right\}.$$

Théorème 2.12. *La fonction $\wp$ ainsi définie est elliptique et a pour périodes ω_1 et ω_2. Elle est analytique sauf pour un pôle double à chaque période. De plus c'est une fonction paire de z.*

Démonstration. Chaque terme de la série a pour module :

$$\left| \frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right| = \left| \frac{z(2\omega - z)}{\omega^2 (z-\omega)^2} \right|.$$

On considère désormais n'importe quel disque compact $|z| \leq R$. Il n'y a qu'un nombre fini de périodes dans ce disque. Si l'on exclut ces termes de la série, on obtient, d'après une étape de la preuve de la proposition 2.10,

$$\frac{1}{|z-\omega|^2} \leq \frac{M}{|\omega|^2},$$

où M est une constante ne dépendant que de R. Ceci nous donne la majoration :

$$\left|\frac{z(2\omega - z)}{\omega^2(z-\omega)^2}\right| \leq \frac{MR(2\left|\omega\right| + R)}{\left|\omega\right|^4} \leq \frac{MR(2 + R/\left|\omega\right|)}{\left|\omega\right|^3} \leq \frac{3MR}{\left|\omega\right|^3}$$

étant donné que $R < |\omega|$ pour ω extérieur au disque $|z| \leq R$. Ceci montre que la série tronquée converge uniformémement sur le disque $|z| \leq R$. Elle est donc analytique sur le disque. Les termes restants donnent chacun un pôle de second ordre pour chaque période ω dans le disque. Ainsi, $\wp$ est méromorphe avec un pôle d'ordre deux à chaque période.

On prouve maintenant que $\wp$ est une fonction paire. On remarque que :

$$(-z-\omega)^2 = (z+\omega)^2 = z - (-\omega)^2.$$

Donc $\wp(-z)$ n'est qu'un réarrangement de la somme $\wp(z)$ donc $\wp$ est paire.

Enfin on établit la périodicité de $\wp$. La dérivée de $\wp$ est donnée par

$$\wp'(z) = -2\sum_{\omega\in\Omega}\frac{1}{(z-\omega)^3},$$

et nous avons déjà prouvé que cette fonction est périodique de périodes ω_1 et ω_2. Ainsi $\wp'(z+\omega) = \wp'(z)$ pour toute période ω. La fonction $\wp(z+\omega) - \wp(z)$ est donc constante et par parité, en évaluant en $z = -\omega/2$ cette constante est nulle. D'où $\wp(z+\omega) = \wp(z)$ pour tout ω et donc $\wp$ a la périodicité demandée. □

Définition 2.2.2. *Pour $n \geq 3$ on définit la série :*

$$G_n = \sum_{\omega\neq 0}\frac{1}{\omega^n}.$$

On l'appelle terme d'ordre n de la série d'Eisenstein.

Théorème 2.13. *On note $r = min(\left|\omega\right|, \omega \neq 0)$. Alors pour $0 < |z| < r$ on a :*

$$\wp(z) = \frac{1}{z^2} + \sum_{n=1}^{\infty}(2n+1)G_{2n+2}z^{2n}.$$

Démonstration. Si $0 < |z| < r$ on a $|z/\omega| < 1$ donc on peut développer en série l'expression suivante :

$$\frac{1}{(z-\omega)^2} = \frac{1}{\omega^2(1-\frac{z}{\omega})^2} = \frac{1}{\omega^2}\left(1 + \sum_{n=1}^{\infty}(n+1)\left(\frac{z}{\omega}\right)^n\right).$$

Donc :

$$\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} = \sum_{n=1}^{\infty}\frac{n+1}{\omega^{n+2}}z^n.$$

La somme définissant $\wp$ convergeant absolument, on obtient en sommant sur tous les ω :

$$\wp(z) = \frac{1}{z^2} + \sum_{n=1}^{\infty}(n+1)\sum_{\omega\neq 0}\frac{n+1}{\omega^{n+2}}z^n = \frac{1}{z^2} + \sum_{n=1}^{\infty}(n+1)G_{n+2}z^n.$$

Comme $\wp$ est paire les coefficients G_n pour n impair sont nuls et donc on a la formule voulue pour le développement de $\wp$. □

Théorème 2.14. *La fonction $\wp$ de Weiestrass vérifie l'équation différentielle non linéaire suivante :*

$$[\wp'(z)]^2 = 4\wp^3(z) - 60G_4\wp(z) - 140G_6.$$

Démonstration. L'idée principale de cette preuve est de se ramener par combinaisons linéaires à des fonctions elliptiques sans pôle et donc constantes d'après la proposition 2.4. Plus précisement on va éliminer la singularité en zéro de $\wp$. Près de $z = 0$ on a :

$$\wp'(z) = -\frac{2}{z^3} + 6G_4 z + 20G_6 z^3 + \dots$$

Donc $\wp'$ est une fonction elliptique d'ordre 3. Son carré est d'ordre 6 comme le montre ce qui suit :

$$[\wp'(z)]^2 = \frac{4}{z^6} - \frac{24G_4}{z^2} - 80G_6 + \dots$$

Dans les deux expressions précédentes on note $+\dots$ une somme de termes en puissance de z qui s'annule quand $z = 0$.
On a par ailleurs :

$$4\wp^3(z) = \frac{4}{z^6} + \frac{36G_4}{z^2} + 60G_6 + \dots$$

Donc :

$$\wp'(z) - 4\wp^3(z) = -\frac{60G_4}{z^2} - 140G_6 + \dots$$

Soit encore, avec le développement de $\wp$:

$$\wp'(z) - 4\wp^3(z) + 60G_4\wp(z) = -140G_6 + \dots$$

Le deuxième terme est une fonction elliptique sans pôle en 0 et sans pôle dans le parallélogramme fondamental, donc il doit être constant, égal à $-140G_6$. Ceci prouve l'équation. □

2.2.2 Fonctions g_2 et g_3

Définition 2.2.3. *On appelle $g_2 = 60G_4$ et $g_3 = 140G_6$ les invariants. On a donc :*

$$[\wp'(z)]^2 = 4\wp^3(z) - g_2\wp(z) - g_3.$$

Remarque : Il peut sembler surprenant que ces deux invariants déterminent complétement la fonction de Weierstrass. Mais en fait cela provient du fait, qui ne sera pas détaillé ici, que chacun des coefficients $(2n+1)G_{2n+2}z^{2n}$ du développement de Laurent de $\wp$ peut s'exprimer en fonction de ces deux invariants. Le lecteur intéressé pourra faire lui-même la preuve en dérivant l'équation fonctionnelle de $\wp$ et en identifiant terme à terme pour obtenir une relation de récurrence.

Définition 2.2.4. *On note e_1, e_2, e_3 les valeurs de $\wp$ aux demi-périodes, c'est-à-dire :*

$$e_1 = \wp\left(\frac{\omega_1}{2}\right), e_2 = \wp\left(\frac{\omega_2}{2}\right), e_3 = \wp\left(\frac{\omega_1+\omega_2}{2}\right).$$

Le prochain théorème montre que ces nombres sont les racines du polyôme $4\wp^3 - g_2\wp - g_3$.

Théorème 2.15. *On a :*

$$4\wp^3(z) - g_2\wp(z) - g_3 = 4(\wp(z) - e_1)(\wp(z) - e_2)(\wp(z) - e_3).$$

De plus les trois racines e_1, e_2, e_3 sont distinctes deux à deux.
Par conséquent, $g_2^3 - 27g_3^2 \neq 0$.

Démonstration. Étant donné que $\wp$ est paire, sa dérivée $\wp'$ est impaire.
On va d'abord montrer un premier résultat : les valeurs aux demi-périodes d'une fonction elliptique impaire sont soit des zéros soit des pôles. En effet, par périodicitié on a $\wp'(-\frac{1}{2}\omega) = \wp'(\omega - \frac{1}{2}\omega) = \wp'(\frac{1}{2}\omega)$. Mais comme $\wp'$ est impaire on a aussi : $\wp'(-\frac{1}{2}\omega) = -\wp'(\frac{1}{2}\omega)$. Donc $\wp'(-\frac{1}{2}\omega)$ est nul si fini. Dans le cas contraire c'est un pôle.

Dans le cas qui nous intéresse ici, on sait que la fonction $\wp'$ n'a pas de pôles aux demi-périodes, ce sont donc des zéros de cette fonction. Mais $\wp'$ est d'ordre 3 (cf, par exemple, la preuve de l'équation différentielle satisfaite par $\wp$, théorème 2.14) donc, d'après le corollaire 2.8 chacun de ces zéros doit être simple. Ce même théorème montre que $\wp'$ ne peut avoir d'autres zéros dans un parallélogramme fondamental. Ainsi l'équation différentielle du théorème 2.14 montre la factorisation recherchée.

Il nous reste à montrer que e_1, e_2, e_3 sont distinctes deux à deux. La fonction elliptique $\wp(z) - e_1$ s'annule à $z = \frac{1}{2}\omega_1$. Et c'est un zéro double comme $\wp'(\frac{1}{2}\omega_1) = 0$. De même, $\wp(z) - e_1$ a un zéro double en $z = \frac{1}{2}\omega_2$. Si on avait $e_1 = e_2$ alors la fonction elliptique $\wp(z) - e_1$ aurait un zéro double en $z = \frac{1}{2}\omega_1$ et en $z = \frac{1}{2}\omega_2$. Elle serait donc d'ordre au moins 4. Or elle est d'ordre 3 ce qui est absurde. Donc $e_1 \neq e_2$ et de même on a que $e_2 \neq e_3$ et $e_1 \neq e_3$.

Enfin, on rappelle que si une équation polynômiale a des racines distinctes deux à deux, alors son discriminant ne s'annule pas. Or le discriminant de l'équation polynômiale d'ordre 3 :

$$4x^3 - g_2x - g_3$$

est précisément $g_2^3 - 27g_3^2$. Quand $x = \wp(z)$, les racines de ce polynôme sont distinctes. Ainsi $g_2^3 - 27g_3^2 \neq 0$, ce qui termine la preuve. □

2.3 Fonction Δ

2.3.1 Généralités

Le nombre $\Delta = g_2^3 - 27g_3^2$ est appelé le discriminant. Dans la suite, nous considérerons les invariants g_2 et g_3 ainsi que Δ comme des fonctions du réseau, c'est-à-dire des fonctions de ω_1 et ω_2. Nous écrirons :

$$g_2 = g_2(\omega_1, \omega_2)\ ,\ g_3 = g_3(\omega_1, \omega_2)\ ,\ \Delta = \Delta(\omega_1, \omega_2).$$

Par définition de la série d'Eisenstein, on voit que les fonctions g_2 et g_3 sont homogènes de degré respectifs -4 et -6, c'est-à-dire que nous avons :

$$g_2(\lambda\omega_1, \lambda\omega_2) = \lambda^{-4}g_2(\omega_1, \omega_2),$$

$$g_3(\lambda\omega_1, \lambda\omega_2) = \lambda^{-6} g_3(\omega_1, \omega_2),$$

et ce pour tout $\lambda \neq 0$. Dès lors, il s'ensuit que Δ est homogène de degré -12 :

$$\Delta(\lambda\omega_1, \lambda\omega_2) = \lambda^{-12}\Delta(\omega_1, \omega_2).$$

On prend $\lambda = 1/\omega_1$ et on note dans toute la suite $\tau = \frac{\omega_2}{\omega_1}$. On a :

$$g_2(1,\tau) = (\omega_1)^4 g_2(\omega_1,\omega_2)\ ,\ g_3(1,\tau) = (\omega_1)^6 g_3(\omega_1,\omega_2)\ ,\ \Delta(1,\tau) = (\omega_1)^{12}\Delta(\omega_1,\omega_2).$$

On peut donc considérer ces trois fonctions comme des fonctions de la variable complexe τ. Quitte à changer ω_1 en $-\omega_1$ on peut s'arranger pour que le quotient τ ait une partie imaginaire positive. On va donc étudier ces fonctions dans le demi-plan supérieur H, appelé demi-plan de Poincaré (cf. définition 3.1.1). Pour $\tau \in H$ on appelle $g_2(\tau)$, $g_3(\tau)$ et $\Delta(\tau)$ les fonctions $g_2(1,\tau)$, $g_3(1,\tau)$ et $\Delta(1,\tau)$. On a alors :

$$g_2(\tau) = 60 \sum_{\substack{m,n=-\infty \\ (m,n)\neq(0,0)}}^{\infty} \frac{1}{(m+n\tau)^4},$$

$$g_3(\tau) = 140 \sum_{\substack{m,n=-\infty \\ (m,n)\neq(0,0)}}^{\infty} \frac{1}{(m+n\tau)^6},$$

et :

$$\Delta(\tau) = g_2^3(\tau) - 27 g_3^2(\tau).$$

De plus, le théorème 2.15 vu dans la partie précédente montre que Δ ne s'annule pas sur tout H.

2.3.2 Développements de Fourier

Cette partie est notoirement calculatoire et d'intérêt limité en première lecture. L'objectif de cette partie est d'obtenir le développement de Fourier de Δ.

Proposition 2.16. *Si $\tau \in H$ et $n > 0$, on a les développements de Fourier :*

$$\sum_{m=-\infty}^{\infty} \frac{1}{(m+n\tau)^4} = \frac{8\pi^4}{3} \sum_{r=1}^{\infty} r^3 e^{2i\pi r n \tau}$$

et :

$$\sum_{m=-\infty}^{\infty} \frac{1}{(m+n\tau)^6} = -\frac{8\pi^6}{15} \sum_{r=1}^{\infty} r^5 e^{2i\pi r n \tau}.$$

Démonstration. On commence par rappeler la décomposition de la fonction cotangente :

$$\pi \cot \pi\tau = \frac{1}{\tau} + \sum_{\substack{m=-\infty \\ m\neq 0}}^{\infty} \left(\frac{1}{\tau+m} - \frac{1}{m} \right).$$

On pose $x = e^{2i\pi\tau}$. Si $\tau \in H$ alors $|x| < 1$, donc :

$$\pi \cot \pi\tau = \pi \frac{\cos \pi\tau}{\sin \pi\tau} = \pi i \frac{e^{2i\pi\tau} + 1}{e^{2i\pi\tau} - 1} = \pi i \frac{x+1}{x-1} = -\pi i \left(\frac{x}{1-x} + \frac{1}{1-x} \right)$$
$$= -\pi i \left(\sum_{r=1}^{\infty} x^r + \sum_{r=0}^{\infty} x^r \right) = -\pi i \left(1 + 2 \sum_{r=1}^{\infty} x^r \right).$$

On égale les deux expressions et on trouve :

$$\frac{1}{\tau} + \sum_{\substack{m=-\infty \\ m \neq 0}}^{\infty} \left(\frac{1}{\tau + m} - \frac{1}{m} \right) = -\pi i \left(1 + 2 \sum_{r=1}^{\infty} x^r \right).$$

On dérive alors terme à terme plusieurs fois et on obtient :

$$-\frac{1}{\tau^2} - \sum_{\substack{m=-\infty \\ m \neq 0}}^{\infty} \frac{1}{(\tau + m)^2} = -(2\pi i)^2 \sum_{r=1}^{\infty} r e^{2i\pi\tau r},$$

$$-3! \sum_{m=-\infty}^{\infty} \frac{1}{(\tau + m)^4} = -(2\pi i)^4 \sum_{r=1}^{\infty} r^3 e^{2i\pi\tau r},$$

et :

$$-5! \sum_{m=-\infty}^{\infty} \frac{1}{(\tau + m)^6} = -(2\pi i)^6 \sum_{r=1}^{\infty} r^5 e^{2i\pi\tau r}.$$

On remplace τ par $n\tau$ et on obtient la proposition. □

Proposition 2.17. *Si $\tau \in H$ on a les développements de Fourier :*

$$g_2(\tau) = \frac{4\pi^4}{3} \left(1 + 240 \sum_{k=1}^{\infty} \sigma_3(k) e^{2\pi i k\tau} \right),$$

et :

$$g_3(\tau) = \frac{8\pi^6}{27} \left(1 - 504 \sum_{k=1}^{\infty} \sigma_5(k) e^{2\pi i k\tau} \right),$$

avec $\sigma_\alpha(k) = \sum_{d|k} d^\alpha$.

Démonstration. On rappelle que pour $s > 1$ on définit la fonction $\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$ et que l'on a les deux valeurs suivantes : $\zeta(4) = \frac{\pi^4}{90}$ et $\zeta(3) = \frac{\pi^6}{945}$. On écrit alors :

$$
\begin{aligned}
g_2(\tau) &= 60 \sum_{\substack{m,n=-\infty \\ (m,n)\neq(0,0)}}^{\infty} \frac{1}{(m+n\tau)^4} \\
&= 60 \left\{ \sum_{\substack{m=-\infty \\ m\neq 0(n=0)}}^{\infty} \frac{1}{m^4} + \sum_{n=1}^{\infty} \sum_{m=-\infty}^{\infty} \left(\frac{1}{(m+n\tau)^4} + \frac{1}{(m-n\tau)^4} \right) \right\} \\
&= 60 \left\{ 2\zeta(4) + 2 \sum_{n=1}^{\infty} \sum_{m=-\infty}^{\infty} \frac{1}{(m+n\tau)^4} \right\} \\
&= 60 \left\{ \frac{2\pi^4}{90} + \frac{16\pi^4}{3} \sum_{n=1}^{\infty} \sum_{r=1}^{\infty} r^3 x^{nr} \right\}
\end{aligned}
$$

avec $x = e^{2i\pi\tau}$. Dans la dernière double somme on assemble les termes pour lesquels nr est constant et l'on obtient le résultat souhaité pour $g_2(\tau)$. On prouve le résultat de la même façon pour $g_3(\tau)$. □

Théorème 2.18. *Si $\tau \in H$ on a le développement de Fourier :*

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

avec les coefficients $\tau(n)$ qui sont entiers et $\tau(1) = 1$.

Démonstration. On pose :

$$x = e^{2i\pi\tau}, A = \sum_{n=1}^{\infty} \sigma_3(n) x^n, B = \sum_{n=1}^{\infty} \sigma_5(n) x^n.$$

Alors :

$$\Delta(\tau) = g_2^3(\tau) - 27 g_3^2(\tau) = \frac{64\pi^{12}}{27} [(1+240A)^3 - (1-504B)^2].$$

A et B sont à coefficients entiers, et :

$$
\begin{aligned}
(1+240A)^3 - (1-504B)^2 &= 1 + 720A + 3(240)^2 A^2 + (240)^3 A^3 - 1 \\
&\quad + 1008B - (504)^2 B^2 \\
&= 12^2(5A + 7B) + 12^3(100A - 147B^2 + 8000A^3).
\end{aligned}
$$

Mais :

$$5A + 7B = \sum_{n=1}^{\infty} (5\sigma_3(n) + 7\sigma_5(n)) x^n$$

et :

$$
\begin{aligned}
5d^3 + 7d^5 = d^3(5 + 7d^2) &\equiv d^3(d^2 - 1) \equiv 0[3] \\
&\equiv d^3(1 - d^2) \equiv 0[4]
\end{aligned}
$$

donc :

$$5d^3 + 7d^5 \equiv 0[12].$$

Ainsi 12^3 est un facteur de chaque coefficient du développement de $(1+240A)^3 - (1-504B)^2$ et on a donc :

$$\Delta(\tau) = \frac{64\pi^{12}}{27}\left(12^3 \sum_{n=1}^{\infty} \tau(n) e^{2\pi i n\tau}\right) = (2\pi)^{12} \sum_{n=1}^{\infty} \tau(n) e^{2\pi i n\tau},$$

avec les $\tau(n)$ qui sont entiers. Le coefficient de x est $12^2(5+7)$ ainsi $\tau(1) = 1$. $\square$

Chapitre 3

Fonctions modulaires

Nous allons ici nous intéresser à une classe de fonctions bien particulières : les fonctions modulaires. Il s'agit de fonctions ayant un comportement assez rigide vis-à-vis de certaines transformations du demi-plan supérieur. L'étude de ces fonctions nous permettra, dans le chapitre suivant, d'obtenir une équation fondamentale pour une fonction qui l'est non moins, la fonction η de Dedekind.

3.1 Demi-plan de Poincaré et Γ

3.1.1 Définitions

Les fonctions modulaires que nous étudierons dans la section suivante seront définies sur le demi-plan supérieur.

Définition 3.1.1. *On note H et on appelle demi-plan de Poincaré le demi-plan $\{\tau : Im(\tau) > 0\}$.*

Nous allons alors pouvoir définir le groupe modulaire, que l'on notera Γ. Pour cela, on définit plus généralement le cadre des *transformations de Möbius* :

Définition 3.1.2. *On appelle transformation de Möbius toute application $f : \mathbb{C} \cup \{\infty\} \to \mathbb{C} \cup \{\infty\}$ de la forme*

$$f(z) = \frac{az + b}{cz + d},$$

avec $ad - bc \neq 0$.

Remarque : La condition $ad - bc \neq 0$ assure que l'application n'est pas constante. En fait, dans ce cas, elle réalise même une bijection de $\mathbb{C} \cup \{\infty\}$ dans lui-même.

On peut alors définir le groupe modulaire :

Définition 3.1.3. *Le groupe modulaire Γ est le sous-groupe du groupe des transformations de Möbius défini par*

$$\Gamma = \left\{ \tau \mapsto \frac{a\tau + b}{c\tau + d} : a, b, c, d \in \mathbb{Z}, ad - bc = 1 \right\}.$$

Remarque : Si l'on représente une transformation de Möbius par la matrice de taille 2 $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ à coefficients complexes, alors le sous-groupe Γ est constitué des telles matrices, à coefficients entiers, de déterminant 1, à condition d'identifier une matrice et son opposée (car elles représentent la même transformation ; et réciproquement, deux matrices représentant la même transformation sont opposées). En d'autres termes, on a $\Gamma \simeq PSL_2(\mathbb{Z})$.

Dans la suite, pour $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, on notera l'action de l'élément de Γ représenté par A sur le point τ du plan complexe par :

$$A\tau = \frac{a\tau + b}{c\tau + d}.$$

3.1.2 Générateurs de Γ

Le résultat principal sur la structure du groupe modulaire Γ est donné par le théorème suivant :

Théorème 3.1. *Le groupe modulaire Γ est engendré par les deux éléments*

$$T : \tau \mapsto \tau + 1$$

et

$$S : \tau \mapsto \frac{-1}{\tau}.$$

Remarque : Avec l'approche matricielle, ce théorème énonce que tout $A \in \Gamma$ s'écrit

$$A = T^{n_1} S T^{n_2} S \dots S T^{n_k},$$

où $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, et $S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ (on a $S^2 = 1$). En effet, ces matrices représentent bien les applications T et S définies ci-dessus. Cette écriture n'est pas unique : en effet, $T = ST^{-1}ST^{-1}S$.

Démonstration. Soit $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$. Quitte à considérer $-A$, on peut supposer $c \geq 0$. Pour montrer le théorème, nous allons raisonner par récurrence.

Si $c = 0$, alors, comme $ad - bc = 1$, on a $a = d = \pm 1$, donc $A = T^{\pm b}$: A est une puissance de T donc la propriété est vraie.

Si $c = 1$, on a alors $b = ad - 1$, donc un simple produit matriciel montre que $A = T^a S T^d$.

Supposons la propriété vraie pour tout entier strictement inférieur à c. Effectuons la division euclidienne de d par c : on a $d = cq + r$ avec $0 < r < c$. Alors un petit calcul montre que

$$AT^{-q}S = \begin{pmatrix} -aq + b & -a \\ r & -c \end{pmatrix}.$$

Par hypothèse de récurrence, comme $r < c$, cette dernière matrice est produit de T et de S. Donc A l'est aussi, ce qui termine la preuve. □

3.1.3 Domaines fondamentaux

Nous allons ici nous intéresser à certains sous-ensembles de H, appelés *domaines fondamentaux*.

Définition 3.1.4. *Soit G un sous-groupe du groupe modulaire Γ. On dit que $\tau, \tau' \in H$ sont équivalents sous G s'il existe $A \in G$ tel que $\tau' = A\tau$.*

Remarque : C'est bien sûr une relation d'équivalence puisque G est un groupe.

Définition 3.1.5. *Soit G un sous-groupe du groupe modulaire Γ. On dit que l'ouvert R_G de H est un domaine fondamental de G si les deux propriétés suivantes sont vérifiées :*
(i) Deux points distincts de R_G ne sont jamais équivalents sous G.
(ii) Pour $\tau \in H$, il existe τ' dans l'adhérence de R_G tel que τ et τ' soient équivalents sous G.

Nous admettrons le théorème suivant, prouvé dans [Apo90] :

Théorème 3.2. *L'ensemble $R_\Gamma = \left\{\tau \in H :\mid \tau \mid > 1, \mid Re(\tau) \mid < \frac{1}{2}\right\}$ est un domaine fondamental pour Γ.*
De plus, les générateurs de Γ, S et T, agissent sur cette région fondamentale comme le montre la figure suivante.

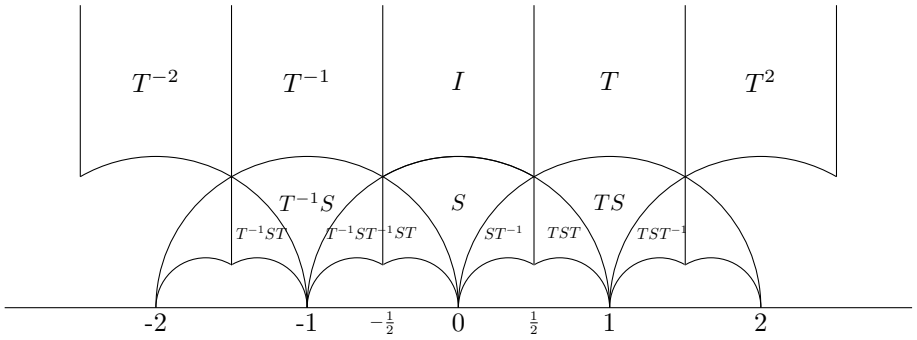


Figure 3.1

3.2 Fonctions modulaires

Définition 3.2.1. *On dit qu'une fonction $f : H \to \mathbb{C} \cup \{\infty\}$ est modulaire si elle vérifie les trois propriétés suivantes :*
(i) f est méromorphe sur H.
(ii) $f(A\tau) = f(\tau)$ pour tout $A \in \Gamma$.
(iii) Le développement en série de Fourier de f est de la forme

$$f(\tau) = \sum_{n=-m}^{\infty} a(n) e^{2i\pi n\tau}.$$

Remarque : Explicitons ces trois conditions. La condition (i) exprime simplement que f est analytique sur H en dehors de ses pôles. La condition (ii) donne l'invariance de f sous l'action de Γ. Quant à la condition (iii), elle décrit

le comportement de f en le point $i\infty$: en effet, le comportement de f en $i\infty$ est donné par sa série de Laurent en $x = e^{2i\pi\tau} = 0$. De ce fait, la condition (iii) exprime simplement qu'en $i\infty$, la fonction f a au plus un pôle (un pôle si $m \geq 0$, une singularité éliminable si $m < 0$).

Le principal résultat sur les fonctions modulaires est donné par le théorème suivant :

Théorème 3.3. *Si f est modulaire et non identiquement nulle, alors dans l'adhérence de la région fondamentale R_Γ le nombre de zéros de f est égal au nombre de ses pôles.*

Remarque : Ce théorème nécessite pour être valable que l'on introduise des conventions adaptées (et naturelles) sur ce que l'on considère comme l'adhérence de la région fondamentale R_Γ et sur certaines singularités aux "extrémités" du domaine.

On considèrera que l'adhérence de R_Γ est l'union de quatre bords s'intersectant aux quatres points ρ, i, $\rho + 1$ et $i\infty$, où l'on note $\rho = e^{2\pi i/3}$. On a donc deux paires de bords équivalents, comme le montre la figure ci-après, à savoir ((1),(4)) et ((2),(3)).

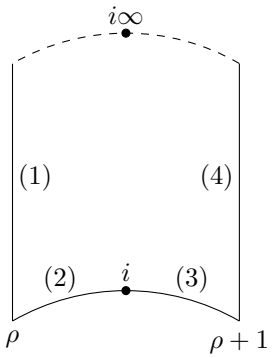


Figure 3.2

Si f a un zéro ou un pôle sur un bord, elle en a aussi un sur le bord qui lui est équivalent. On considèrera que seul le point du bord (1) ou (2) appartient à l'adhérence de R_Γ.

Enfin il nous faut détailler l'ordre du pôle aux trois points ρ, i et $i\infty$. En $i\infty$ l'ordre du pôle ou zéro sera celui obtenu en $x = 0$, où $x = e^{2i\pi\tau}$. Enfin en ρ il faudra compter un pôle ou un zéro avec multiplicité $1/3$, et avec multiplicité $1/2$ en i. En effet en comptant l'ordre en ces points, on le compte trop souvent comme le montre la figure 3.3.

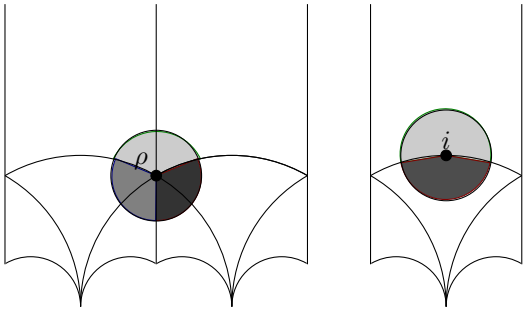


Figure 3.3

Ces dessins représentent les différentes régions fondamentales. Les parties blanches correspondent aux contributions au nombre total de pôles et zéros que l'on souhaiterait considérer dans notre théorème. Mais en fait on a aussi les parties des autres couleurs que l'on va compter. Il faut donc diviser par 3 pour ρ et par 2 pour i comme le montrent ces deux figures.

Démonstration. Supposons tout d'abord que f n'a aucun zéro ni pôle sur le bord de R_Γ. On coupe R_Γ par une droite horizontale, $Im(\tau) = M$, où $M > 0$ est pris assez grand pour que tous les pôles et zéros de f soient dans la région tronquée que nous appelerons R. (Un tel M existe bien en utilisant les propriétés des fonctions modulaires. En effet, si f avait un nombre infini de pôles dans R_Γ on aurait un point d'accumulation à $i\infty$ ce qui contredit la condition (iii) de la définition 3.2.1. Par ailleurs comme f n'est pas identiquement nulle elle n'a qu'un nombre fini de zéros.) On note ∂R le bord de cette région tronquée.

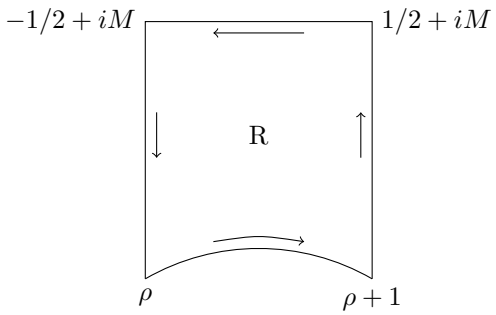


Figure 3.4

Dans toute la suite de la preuve, on notera N le nombre de zéros de f et P son nombre de pôles dans R (chacun compté avec multiplicité). Le théorème de l'argument nous donne que :

$$N - P = \frac{1}{2i\pi} \int_{\partial R} \frac{f'(\tau)}{f(\tau)} d\tau = \frac{1}{2i\pi} \left(\int_{(1)} + \int_{(2)} + \int_{(3)} + \int_{(4)} + \int_{(5)} \right),$$

où l'on a divisé l'intégrale en cinq parties indiquées sur la figure suivante :

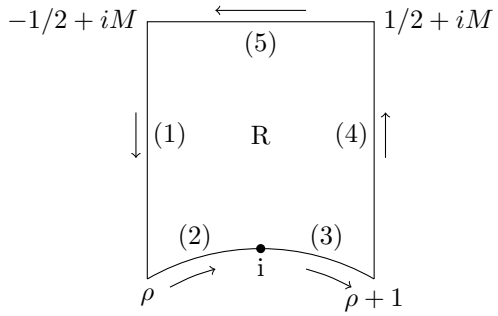


Figure 3.5

Les intégrales le long de (1) et de (4) se compensent par périodicité. Les intégrales (2) et (3) se compensent également mutuellement. En effet on passe de (2) à (3) en changeant de direction grâce à la transformation $u = S(\tau) = -1/\tau$, soit encore $\tau = S^{-1}u = S(u) = -1/u$. Et l'intégrande reste inchangé. L'invariance sous Γ donne $f[S(u)] = f(u)$ qui implique $f'[S(u)]S'(u) = f'(u)$ et ainsi :

$$\begin{aligned}\frac{f'(\tau)}{f(\tau)}d\tau &= \frac{f'[S(u)]}{f[S(u)]}S'(u)du \text{ en appliquant le changement de variable} \\ &= \frac{f'(u)}{f(u)}du \text{ par invariance sous } \Gamma.\end{aligned}$$

Ainsi il ne nous reste que :

$$N - P = \frac{1}{2i\pi}\int_{(5)}\frac{f'(\tau)}{f(\tau)}d\tau.$$

On transforme cette intégrale en posant $x = e^{2i\pi\tau}$. Comme τ varie sur le segment $u + iM$ avec $-1/2 \neq u \neq 1/2$ on a

$$x = e^{2i\pi(u+iM)} = e^{-2\pi M}e^{2i\pi u},$$

donc x varie le long d'un cercle K de rayon $e^{-2\pi M}$ tournant autour de zéro dans le sens indirect. Les points au dessus du segment sont transportés à l'intérieur de K, donc f n'a aucun zéro ou pôle dans K, sauf éventuellement en $x = 0$. Le développement de Fourier de la fonction modulaire f est :

$$f(\tau) = \frac{a_{-m}}{x^m} + \cdots = F(x).$$

Soit :

$$f'(\tau) = F'(x)\frac{dx}{d\tau} \text{ (i.e.) } \frac{f'(\tau)}{f(\tau)}d\tau = \frac{F'(x)}{F(x)}dx.$$

On en déduit, à cause du sens d'intégration, que :

$$N - P = \frac{1}{2i\pi}\int_{(5)}\frac{f'(\tau)}{f(\tau)}d\tau = -\frac{1}{2i\pi}\oint_K\frac{F'(x)}{F(x)}dx = P_F - N_F,$$

où l'on a noté P_F et N_F respectivement le nombre de pôles et de zéros de F dans K. On a déjà vu que le seul point intéressant à considérer est $z = 0$.

Si F a un pôle d'ordre m en $z = 0$, alors $P_F - N_F = -m$ donc

$$N = P + m,$$

c'est-à-dire, si l'on se souvient de nos notations, que le nombre de zéros de f dans R est égal au nombre de pôles de f dans R augmenté de l'ordre du pôle en l'infini. Ceci nous donne bien que f prend la valeur zéro aussi souvent que la valeur ∞.

Si F a un zéro d'ordre m en $z = 0$. Alors $P_F - N_F = m$ donc :

$$N + m = P.$$

Ceci nous donne encore effectivement que f prend la valeur zéro aussi souvent que la valeur ∞.

On a donc démontré le théorème dans le cas où f n'a aucun zéro ni pôle sur le bord de R_Γ.

Supposons désormais que f a un zéro ou un pôle sur le bord de R_Γ mais pas en l'un des trois points ρ, $\rho + 1$ et i. Il suffit alors de changer le contour d'intégration pour inclure le pôle ou le zéro dans l'intérieur de R_Γ afin de le compter une seule fois. On utilise le contour de la figure suivante. Les intégrales sur les bords équivalents s'annulent comme précédemment et on ne compte les nouveaux pôles et zéros qu'une seule fois par notre choix de convention. On peut donc mener la preuve comme auparavant.

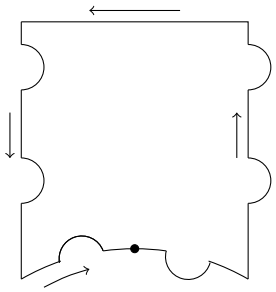


Figure 3.6

Enfin, si f a un un zéro ou un pôle sur le bord de R_Γ, en l'un des points ρ ou i, on modifie encore le contour d'intégration comme ci-dessous :

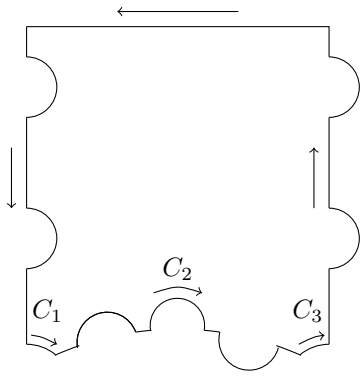


Figure 3.7

En résonnant comme précédemment on trouve :

$$\begin{aligned} N - P &= \frac{1}{2i\pi}\left\{\left(\int_{C_1} + \int_{C_3}\right) + \int_{C_2} + \int_{1/2+iM}^{-1/2+iM}\right\}\frac{f'(\tau)}{f(\tau)}d\tau \\ &= \frac{1}{2i\pi}\left\{\left(\int_{C_1} + \int_{C_3}\right) + \int_{C_2}\right\}\frac{f'(\tau)}{f(\tau)}d\tau + m, \end{aligned}$$

où m est l'ordre du pôle de F en $x = 0$, i.e. de f en $\tau = i\infty$.

Près du point ρ on écrit :

$$f(\tau) = (\tau - \rho)^k g(\tau), \text{ où } g(\rho) \neq 0.$$

L'exposant k est positif si f a un zéro en ρ et négatif s'il s'agit d'un pôle. Sur C_1 on paramètre l'arc de cercle en posant $\tau - \rho = re^{i\theta}$ où r est fixé et $\alpha \leq \theta \leq \pi/2$ avec α qui dépend du r choisi. (Voir figure précédente pour comprendre qui est où.)

On a donc :

$$\frac{f'(\tau)}{f(\tau)} = \frac{k}{\tau - \rho} + \frac{g'(\tau)}{g(\tau)}.$$

Ainsi :

$$\begin{aligned} \frac{1}{2i\pi}\int_{C_1}\frac{f'(\tau)}{f(\tau)}d\tau &= \frac{1}{2i\pi}\int_{\pi/2}^{\alpha}\left(\frac{k}{re^{i\theta}} + \frac{g'(\rho + re^{i\theta})}{g(\rho + re^{i\theta})}\right)re^{i\theta}id\theta \\ &= \frac{-k\alpha'}{2\pi} + \frac{r}{2\pi}\int_{\pi/2}^{\alpha}\frac{g'(\rho + re^{i\theta})}{g(\rho + re^{i\theta})}e^{i\theta}d\theta, \text{ où } \alpha' = \frac{\pi}{2} - \alpha. \end{aligned}$$

Quand $r \to 0$ le terme de gauche tend vers 0 car l'intégrande est borné au voisinage de zéro. Par ailleurs, quand $r \to 0$, on a $\alpha' \to \pi/3$ comme le montre le dessin suivant :

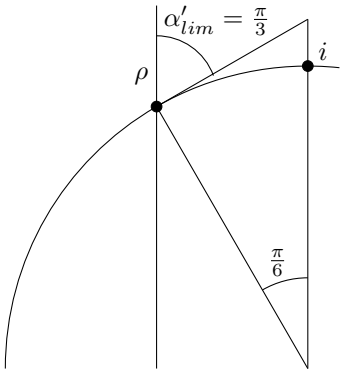


Figure 3.8

Et ainsi :

$$\lim_{r\to 0}\frac{1}{2i\pi}\int_{C_1}\frac{f'(\tau)}{f(\tau)}d\tau = -\frac{k}{6}.$$

Par un raisonnement similaire, pour ne pas dire identique, on obtient :

$$\lim_{r\to 0} \frac{1}{2i\pi} \int_{C_3} \frac{f'(\tau)}{f(\tau)} d\tau = -\frac{k}{6}.$$

On procède de même en i. On écrit :

$$f(\tau) = (\tau - i)^l h(\tau), \text{ où } h(i) \neq 0.$$

On trouve alors, par le même raisonnement :

$$\lim_{r\to 0} \frac{1}{2i\pi} \int_{C_2} \frac{f'(\tau)}{f(\tau)} d\tau = -\frac{l}{2}.$$

On obtient donc la formule suivante :

$$N - P = m - \frac{k}{3} - \frac{l}{2}.$$

On fait alors une disjonction de cas selon les natures des singularités en l'infini, i, et ρ comme menée précédemment et on voit que le résultat annoncé est le bon. On traite ici un exemple de la disjonction de cas :
Si f a un pôle en $x = 0$ et des zéros en i et ρ, alors m, k et l sont positifs et on a :

$$N + \frac{k}{3} + \frac{l}{2} = P + m.$$

Le membre de gauche compte le nombre total de zéros de f dans l'adhérence de R_Γ. On rappelle que les remarques faites avant la preuve expliquaient que l'ordre des pôles ou zéros en ρ devraient être divisés par trois et ceux en i par deux ce qui est bien en accord avec cette formule. Le membre de droite compte le nombre de pôles donc on a bien ce que l'on veut. □

On peut en déduire deux corollaires immédiats :

Corollaire 3.4. *Si f est une fonction modulaire non constante, alors dans l'adhérence de R_Γ, f prend toutes les valeurs complexes possibles, et chacune autant de fois.*

Démonstration. Pour $c \in \mathbb{C}$, le théorème précédent appliqué à $f - c$ (qui reste bien sûr modulaire) montre que f prend autant de fois la valeur c qu'elle a de pôles dans l'adhérence de R_Γ. □

Corollaire 3.5. *Si f est une fonction modulaire bornée, alors f est constante.*

Démonstration. Si f est bornée, elle ne prend pas toutes les valeurs de $\mathbb{C}$. Par le corollaire précédent, elle est donc constante. □

Chapitre 4

Fonction η de Dedekind

Il est maintenant grand temps d'appliquer les résultats sur les formes modulaires et le groupe Γ des chapitres précédents. Cette théorie va nous permettre d'obtenir l'équation fonctionnelle vérifiée par la fonction F (théorème 4.9), et que nous avions admise dans la première partie. Pour cela, nous allons utiliser la fonction η de Dedekind, et son équation fonctionnelle (théorème 4.8), qui jouent un rôle fondamental dans de nombreuses applications des fonctions elliptiques modulaires à la théorie des nombres.

4.1 Présentation

4.1.1 Définition

On définit la fonction η de Dedekind sur le demi-plan $H = \{\tau : Im(\tau) > 0\}$ par :

$$\eta(\tau) = e^{i\pi\tau/12} \prod_{n\geq 1} (1 - e^{2i\pi n\tau}).$$

Pour $\tau \in H$, on a $\left|e^{2i\pi\tau}\right| < 1$, donc le produit est bien défini, converge absolument, et ne s'annule pas sur H.

Remarquons dès maintenant le lien entre cette fonction η et la fonction F. Par la proposition 1.1, on a la relation :

$$F(e^{2i\pi\tau}) = e^{i\pi\tau/12}/\eta(\tau).$$

Dès lors, notre but sera de déterminer une équation fonctionnelle vérifiée par η pour en déduire celle vérifiée par F.

4.1.2 Action sur Γ

L'équation fonctionnelle que nous cherchons pour η va nous permettre d'exprimer, pour $A \in \Gamma$, $\eta(A\tau)$ en fonction de $\eta(\tau)$. Rappelons que le groupe Γ a deux générateurs : la translation $T : \tau \mapsto \tau + 1$, ainsi que l'inversion $S : \tau \mapsto \frac{-1}{\tau}$. Nous allons donc commencer par déterminer comment varie η sous l'action de ces deux générateurs.

Proposition 4.1. *On a :*

$$\eta(T\tau) = \eta(\tau+1) = e^{i\pi/12}\eta(\tau).$$

Démonstration. Il suffit d'écrire que :

$$\begin{aligned}\eta(\tau+1) &= e^{i\pi(\tau+1)/12}\prod_{n\geq 1}(1-e^{2i\pi n(\tau+1)}) \\ &= e^{i\pi/12}e^{i\pi\tau/12}\prod_{n\geq 1}(1-e^{2i\pi n\tau}) = e^{i\pi/12}\eta(\tau).\end{aligned}$$

□

Remarque : Cette relation montre qu'en particulier, η^{24} est périodique de période 1.

Proposition 4.2. *On a :*

$$\eta(S\tau) = \eta\left(\frac{-1}{\tau}\right) = (-i\tau)^{1/2}\eta(\tau).$$

Démonstration. Nous allons tout d'abord montrer $\eta(\frac{-1}{\tau}) = (-i\tau)^{1/2}\eta(\tau)$ pour $\tau = iy$ où $y > 0$. Comme les fonctions considérées sont holomorphes si l'on montre que leur différence est nulle sur toute une droite on pourra conclure par le principe des zéros isolés.
Si $\tau = iy$ la formule voulue devient $\eta(i/y) = y^{1/2}\eta(iy)$ qui est équivalente à :

$$\ln\eta(i/y) - \ln\eta(iy) = \frac{1}{2}\ln y.$$

Par ailleurs on a aussi :

$$\begin{aligned}\ln\eta(iy) &= -\frac{\pi y}{12} + \ln\prod_{n=1}^{\infty}(1-e^{-2\pi ny}) \\ &= -\frac{\pi y}{12} + \sum_{n=1}^{\infty}\ln(1-e^{-2\pi ny}) \\ &= -\frac{\pi y}{12} - \sum_{n=1}^{\infty}\sum_{m=1}^{\infty}\frac{e^{-2\pi mny}}{m} \\ &= -\frac{\pi y}{12} - \sum_{m=1}^{\infty}\frac{1}{m}\frac{e^{-2\pi my}}{1-e^{-2\pi my}} \text{ par Fubini car les termes sont positifs} \\ &= -\frac{\pi y}{12} + \sum_{m=1}^{\infty}\frac{1}{m}\frac{1}{1-e^{-2\pi my}}.\end{aligned}$$

Dès lors il nous faut prouver :

$$(1)\quad \sum_{m=1}^{\infty}\frac{1}{m}\frac{1}{1-e^{-2\pi my}} - \sum_{m=1}^{\infty}\frac{1}{m}\frac{1}{1-e^{-2\pi m/y}} - \frac{\pi}{12}\left(y-\frac{1}{y}\right) = -\frac{1}{2}\ln y.$$

Nous allons montrer ce résultat par un calcul de résidu. L'idée est de trouver une fonction dont la somme des résidus donne le terme de gauche de l'équation

précédente et dont l'intégrale sur un contour bien choisi donne le terme de droite. Si vous avez beaucoup de chance ou une intuition impressionnante vous trouverez peut-être ces deux éléments. Dans le cas contraire nous allons vous la donner. On fixe y et n et on pose :

$$F_n(z) = -\frac{1}{8z}\cot(\pi i N z)\cot\left(\frac{\pi N z}{y}\right),$$

où l'on note $N = n+1/2$. La suite du calcul va montrer pourquoi on peut penser à cette fonction, mais il faut être à l'aise et habitué aux calculs de résidu. Le contour C que nous choisirons sera le parallélogramme joignant les affixes y, i, $-y$, $-i$ dans cet ordre.

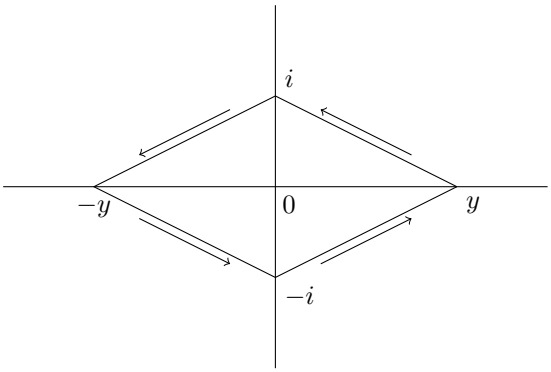


Figure 4.1

À l'intérieur de C, F_n a des pôles simples et $z = ik/N$ et $z = ky/N$ pour $k = \pm 1, \pm 2 \cdots \pm n$ avec les propriétés habituelles de la fonction cotangente. Mais aussi un pôle triple en zéro (chacun des trois facteurs du produit s'annule)

(i) **Résidu en zéro**

On le calcule simplement en faisant un développement limité en $z = 0$. On rappelle le développement de cotangente (que le lecteur avisé retrouvera aisément) : $\frac{1}{x} - x/3$. On a donc :

$$F_n(z) = \frac{1}{8z}\left(\frac{1}{\pi i N z} - \frac{\pi i N z}{3} + o(z)\right)\left(\frac{y}{\pi N z} - \frac{\pi N z}{3y} + o(z)\right).$$

En développant on obtient sans difficulté le coefficient de $1/z$, c'est-à-dire le résidu en zéro qui vaut donc : $\frac{i}{24}\left(y - \frac{1}{y}\right)$.

(ii) **Résidu en z=ik/N**

Comme on a un pôle simple on calcule le résidu en faisant :

$$\lim_{z \to ik/N} F_n(z)(z - ik/N) = \frac{-N}{8ik}\cot \pi ik/y \lim_{z \to ik/N}(z - ik/N)\cot \pi i N z.$$

On pose $h = z - ik/N$. Le développement limité précédent de cotangente nous permet de voir que quand h tend vers zéro on a :

$$\lim_{z \to ik/N}(z - ik/N)\cot \pi i N z = h \cdot \frac{1}{h\pi i N} = \frac{1}{\pi i N}.$$

Donc finalement le résidu de F_n en $z = ik/N$ est :

$$\frac{1}{8\pi k} \cot \frac{\pi i k}{y}.$$

De plus, comme c'est une fonction paire en k on a :

$$\sum_{\substack{k=-n \\ k\neq 0}}^{n} Res_{z=ky/N} F_n(z) = 2 \sum_{k=1}^{n} \frac{1}{8\pi k} \cot \frac{\pi i k}{y}.$$

Or :

$$\cot i\theta = \frac{\cos i\theta}{\sin i\theta} = i\frac{e^{-\theta} + e^{\theta}}{e^{-\theta} - e^{\theta}} = -i\frac{e^{2\theta} + 1}{e^{2\theta} - 1} = \frac{1}{i}\left(1 - \frac{2}{1 - e^{2\theta}}\right).$$

En appliquant ce résultat pour $\theta = \pi k/y$ on obtient

$$\sum_{\substack{k=-n \\ k\neq 0}}^{n} Res_{z=ik/N} F_n(z) = \frac{1}{4\pi i} \sum_{k=1}^{n} \frac{1}{k} - \frac{1}{2i\pi} \sum_{k=1}^{n} \frac{1}{k} \frac{1}{1 - e^{2\pi k/y}}.$$

(iii) **Résidu en z=ky/N**

On montre exactement de la même façon que :

$$\sum_{\substack{k=-n \\ k\neq 0}}^{n} Res_{z=ky/N} F_n(z) = \frac{i}{4\pi} \sum_{k=1}^{n} \frac{1}{k} - \frac{i}{2\pi} \sum_{k=1}^{n} \frac{1}{k} \frac{1}{1 - e^{2\pi k y}}.$$

Ainsi, la somme de tous les résidus de F_n à l'intérieur de C est :

$$\frac{1}{2i\pi}\left(-\sum_{k=1}^{n} \frac{1}{k} \frac{1}{1 - e^{2\pi k y}} - \sum_{k=1}^{n} \frac{1}{k} \frac{1}{1 - e^{2\pi k/y}} - \frac{\pi}{12}\left(y - \frac{1}{y}\right)\right),$$

expression dont la limite quand $n \longrightarrow \infty$ fait apparaître le terme de gauche de (1). Ainsi, pour finir la preuve il suffit de montrer que :

$$\lim_{n\to\infty} \int_C F_n(z) dz = -\frac{1}{2} \ln y.$$

On va maintenant montrer que zF_n tend vers une constante sur le bord du losange sauf en ses sommets. Il suffit pour cela de montrer que :

$$-\cot \pi i N z \cot \frac{\pi N z}{y} \longrightarrow 1 \text{ ou } -1.$$

On calcule pour se faire, pour $a, b \in \mathbb{R}$:

$$\begin{aligned} cot(a + ib) &= \frac{e^{2i(a+ib)} + 1}{e^{2i(a+ib)} - 1} \\ &= \frac{e^{2ia}e^{-2b} + 1}{e^{2ia}e^{-2b} - 1}. \end{aligned}$$

En écrivant encore que sur le bord entre 1 et y on a $z = ty + (1-t)i$, et en substituant dans l'équation précédente les expressions dans les cotangentes, on montre directement que $zF_n(z)$ a pour limite $1/8$ sur le bord entre 1 et y, et sur celui entre -1 et $-y$; contre $-1/8$ pour les autres bords. Enfin, on montre de la même façon que $F_n(z)$ est bornée sur C par une constante indépendante de n.

Ainsi par convergence dominée on a :

$$\begin{aligned}\lim_{n\to\infty}\int_C F_n(z)dz &= \int_C \lim_{n\to\infty} zF_n(z)\frac{dz}{z}\\ &= \frac{1}{8}\left[-\int_{-i}^{y}+\int_{y}^{i}-\int_{i}^{-y}+\int_{-y}^{-i}\right]\frac{dz}{z}\\ &= \frac{1}{4}\left[-\int_{-i}^{y}+\int_{y}^{i}\right]\frac{dz}{z}\\ &= \frac{1}{4}\left[-(\ln y+\frac{\pi i}{2}+\frac{\pi i}{2}-\ln y\right] = -\frac{1}{2}\ln y.\end{aligned}$$

La fonction posée vérifie bien tout ce que l'on voulait. Ceci prouve (1) et conclut la preuve. □

4.2 Équation fonctionnelle de η

4.2.1 Forme modulaire de poids $1/2$

Dans cette section, nous allons établir la forme de l'équation fonctionnelle de la fonction η de Dedekind. Pour cela, la stratégie est simple : nous allons nous appuyer sur une équation modulaire vérifiée par Δ (proposition 4.3), combinée à une relation simple entre Δ et η.

Proposition 4.3. *Soit* $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$. *On a, pour tout* τ,

$$\Delta\left(\frac{a\tau+b}{c\tau+d}\right) = (c\tau+d)^{12}\Delta(\tau).$$

Remarque : On dit alors que Δ est une *forme modulaire* de poids 12.

Démonstration. La démonstration est basée sur le fait que Δ est homogène de degré -12, i.e. si $\tau = \omega_2/\omega_1$, on a

$$\Delta(\omega_1,\omega_2) = \omega_1^{-12}\Delta(\tau).$$

De plus, Δ étant une fonction du réseau, si (ω_1,ω_2) et (ω_1',ω_2') sont deux paires de périodes équivalentes, alors $\Delta(\omega_1,\omega_2) = \Delta(\omega_1',\omega_2')$.
Il suffit alors de prendre $\omega_1 = 1$, $\omega_2 = \tau$, $\omega_1' = c\tau+d$ et $\omega_2' = a\tau+b$ pour avoir directement

$$\Delta(\tau) = \Delta(\omega_1,\omega_2) = \Delta(\omega_1',\omega_2') = \Delta(c\tau+d, a\tau+b) = (c\tau+d)^{-12}\Delta\left(\frac{a\tau+b}{c\tau+d}\right).$$

□

Les fonctions η et Δ sont de plus reliées par l'égalité suivante :

Théorème 4.4. *Pour $\tau \in H$, on a*

$$\Delta(\tau) = (2\pi)^{12}\eta^{24}(\tau).$$

Remarque : Ce théorème permet d'apprécier l'importance de la fonction η, reliée de manière simple à la fonction fondamentale Δ.

Démonstration. C'est à ce stade que nous allons utiliser toute la théorie des fonctions modulaires développée précédemment. L'idée de la preuve est en effet essentiellement fondée sur le fait qu'une fonction modulaire ne s'annulant pas est constante (théorème 3.2). Soit donc $f(\tau) = \Delta(\tau)/\eta^{24}(\tau)$. Rappelons que l'on a les quatre égalités suivantes :

$$\Delta(\tau+1) = \Delta(\tau),$$
$$\Delta\left(-\frac{1}{\tau}\right) = \tau^{12}\Delta(\tau),$$
$$\eta(\tau+1) = e^{i\pi/12}\eta(\tau),$$
$$\eta\left(-\frac{1}{\tau}\right) = (-i\tau)^{1/2}\,\eta(\tau).$$

Cela donne immédiatement :

$$f(\tau+1) = f(\tau)$$

et :

$$f\left(-\frac{1}{\tau}\right) = f(\tau),$$

c'est-à-dire que f est invariante sous l'action du groupe modulaire Γ. On est donc bien parti pour que f soit une fonction modulaire comme nous le souhaiterions. De plus, f est analytique et ne s'annule pas sur H : en effet, Δ et η ne s'annulent pas sur H, et Δ y est analytique. Il faut étudier son comportement à l'infini :

On a tout d'abord, pour $x = e^{2i\pi\tau}$:

$$\eta^{24}(\tau) = x\prod(1-x^n)^{24} = x(1+I_1(x)),$$

où $I_1(x)$ est une série en x s'annulant en $x = 0$. De plus, on a, par le théorème 2.18, le développement de Δ suivant :

$$\Delta(\tau) = (2\pi)^{12}x(1+I_2(x)).$$

Il reste donc finalement, en faisant le quotient :

$$f(\tau) = (2\pi)^{12}(1+I(x)),$$

c'est-à-dire que f est analytique et non nulle en $i\infty$. De plus on a $I(0) = 0$.

La fonction f est donc bien une fonction modulaire. Comme elle ne s'annule pas, il s'ensuit qu'elle est constante ; et le développement précédent montre que cette constante vaut $(2\pi)^{12}$. Cela montre l'égalité que l'on avait annoncée :

$$\Delta(\tau) = (2\pi)^{12}\eta^{24}(\tau).$$

□

Cette relation permet de déduire la forme de l'équation fonctionnelle de η. En effet, nous avions l'équation de Δ :

$$\Delta\left(\frac{a\tau+b}{c\tau+d}\right) = (c\tau+d)^{12}\Delta(\tau),$$

soit encore :

$$(2\pi)^{12}\eta^{24}\left(\frac{a\tau+b}{c\tau+d}\right) = (c\tau+d)^{12}(2\pi)^{12}\eta^{24}(\tau).$$

Prendre les racines vingt-quatrièmes permet d'obtenir la forme générale de l'équation fonctionnelle de η de Dedekind :

$$\eta\left(\frac{a\tau+b}{c\tau+d}\right) = \epsilon(a,b,c,d)(c\tau+d)^{1/2}\eta(\tau),$$

où $\epsilon(a,b,c,d)$ est une racine vingt-quatrième de l'unité, non explicite pour le moment.

4.2.2 Sommes de Dedekind

Nous avons ainsi obtenu la forme de l'équation fonctionnelle vérifiée par la fonction η. Cependant, pour qu'elle soit utilisable, il nous faut en savoir plus sur cette racine de l'unité ϵ. Pour cela, nous allons devoir introduire un nouvel outil : les sommes de Dedekind. Ce paragraphe est un intermède présentant les premières propriétés arithmétiques de ces sommes.

Définition 4.2.1. *Soit $k \in \mathbb{N}^*$, $h \in \mathbb{Z}$, premiers entre eux. On définit la somme de Dedekind $s(h,k)$ par :*

$$s(h,k) = \sum_{r=1}^{k-1} \frac{r}{k}\left(\frac{hr}{k} - \left[\frac{hr}{k}\right] - \frac{1}{2}\right).$$

Remarque : On peut exprimer cette somme grâce à la fonction $x \mapsto ((x))$ définie par

$$((x)) = \begin{cases} x - [x] - \frac{1}{2} & \text{si } x \text{ n'est pas entier.} \\ 0 & \text{si } x \text{ est entier.} \end{cases}$$

Cette fonction est clairement périodique de période 1, et impaire. De ce fait, si $(h,k) = 1$, alors hr décrit tous les restes modulo k quand r les décrit ; donc on a

$$\sum_{r \bmod k} \left(\left(\frac{hr}{k}\right)\right) = 0.$$

En particulier, en prenant les entiers de 1 à k comme représentants des classes modulo k, on a :

$$\sum_{r \bmod k} \left(\left(\frac{r}{k}\right)\right)\left(\left(\frac{hr}{r}\right)\right) = \sum_{r=1}^{k-1}\left(\frac{r}{k} - \frac{1}{2}\right)\left(\left(\frac{hr}{k}\right)\right) = \sum_{r=1}^{k-1}\left(\frac{r}{k}\right)\left(\left(\frac{hr}{k}\right)\right) = s(h,k),$$

c'est-à-dire que :

$$s(h,k) = \sum_{r \bmod k} \left(\left(\frac{r}{k}\right)\right)\left(\left(\frac{hr}{r}\right)\right).$$

Cette écriture permet une approche plus naturelle des propriétés arithmétiques des sommes de Dedekind dans la mesure où elle fait intervenir la fonction $((.))$, périodique et impaire.

Parmi les propriétés qui nous seront utiles par la suite, remarquons tout d'abord que :

$$s(-h,k) = -s(h,k),$$

qui découle directement de l'imparité de $((.))$, et pour tout entier m

$$s(km+h,k) = s(h,k),$$

qui découle directement de la périodicité.

Pour terminer ce premier contact avec les sommes de Dedekind, il nous reste à présenter la loi de réciprocité de Dedekind, qui permet d'exprimer $s(h,k)$ en fonction de $s(k,h)$. On a ainsi l'égalité suivante :

Proposition 4.5. *(Loi de réciprocité de Dedekind)*
Pour $h>0$, $k>0$, et $(h,k)=1$, on a

$$12hk(s(h,k)+s(k,h)) = h^2+k^2-3hk+1.$$

Démonstration. La démonstration est longue et calculatoire. Nous allons commencer par un petit calcul anodin. Calculons $\sum_{r=1}^{k}((hr/k))^2$ de deux manières différentes. Tout d'abord, on a :

$$\sum_{r=1}^{k}\left(\left(\frac{hr}{k}\right)\right)^2 = \sum_{r \bmod k}\left(\left(\frac{hr}{k}\right)\right)^2 = \sum_{r \bmod k}\left(\left(\frac{r}{k}\right)\right)^2 = \sum_{r=1}^{k-1}\left(\frac{r}{k}-\frac{1}{2}\right)^2.$$

(On a pris les entiers de 1 à k comme représentants des classes modulo k, et fait disparaître le h car hr décrit toutes les classes modulo k avec r).

D'autre part, on peut évaluer la même somme en développant le terme général et en rassemblant les termes se ressemblant, puis en faisant apparaître la somme de Dedekind $s(h,k)$:

$$\begin{aligned}
\sum_{r=1}^{k}\left(\left(\frac{hr}{k}\right)\right)^2 &= \sum_{r=1}^{k-1}\left(\frac{hr}{k}-\left[\frac{hr}{k}\right]-\frac{1}{2}\right)^2 \\
&= \sum_{r=1}^{k-1}\left(\frac{h^2r^2}{k^2}+\left[\frac{hr}{k}\right]^2+\frac{1}{4}+\left[\frac{hr}{k}\right]-\frac{hr}{k}-2\frac{hr}{k}\left[\frac{hr}{k}\right]\right) \\
&= 2h\sum_{r=1}^{k-1}\frac{r}{k}\left(\frac{hr}{k}-\left[\frac{hr}{k}\right]-\frac{1}{2}\right)+\sum_{r=1}^{k-1}\left[\frac{hr}{k}\right]\left(\left[\frac{hr}{k}\right]+1\right) \\
&\quad -\frac{h^2}{k^2}\sum_{r=1}^{k-1}r^2+\frac{1}{4}\sum_{r=1}^{k-1}1.
\end{aligned}$$

Égaler les deux expressions obtenues pour la même somme donne alors :

$$2hs(h,k)+\sum_{r=1}^{k-1}\left[\frac{hr}{k}\right]\left(\left[\frac{hr}{k}\right]+1\right) = \frac{h^2+1}{k^2}\sum_{r=1}^{k-1}r^2-\frac{1}{k}\sum_{r=1}^{k-1}r.$$

Ce que nous venons de faire ne semble pas faciliter les choses à première vue, mais c'est en fait une telle expression qui va nous permettre de faire apparaître le $s(k,h)$ cherché. Pour ce faire, il faudrait "renverser" les fractions, c'est-à-dire faire passer les h au dénominateur et les k au numérateur. L'avantage de l'expression que nous venons d'obtenir est que, outre dans la somme $s(h,k)$, la fraction hr/k n'est présente que sous forme de partie entière. Au lieu de sommer sur r, nous allons donc sommer sur les différentes valeurs possibles de cette partie entière. C'est ce mécanisme qui va permettre d'obtenir une somme dont le terme général sera en k/h et non en h/k.

On fait donc le changement d'indice :

$$\nu = \left[\frac{hr}{h}\right] + 1.$$

Comme $1 \leq r \leq k-1$, ν prend les valeurs de 1 jusqu'à h. Pour exprimer la somme, il reste donc à compter pour combien de valeurs de r l'indice ν prend une valeur donnée. Soit $N(\nu)$ ce nombre. On a $\nu = \left[\frac{hr}{h}\right] + 1$ si, et seulement si $\nu - 1 < \frac{hr}{k} < \nu$, c'est-à-dire $\frac{k(\nu-1)}{h} < r < \frac{k\nu}{h}$ (il n'y a pas de cas d'égalité car $r < k$ et $(h,k) = 1$).

Pour $1 \leq \nu \leq h-1$, il s'ensuit que r peut varier de $\left[\frac{k(\nu-1)}{h}\right] + 1$ à $\left[\frac{k\nu}{h}\right]$, et donc on a

$$N(\nu) = \left[\frac{k\nu}{h}\right] - \left[\frac{k(\nu-1)}{h}\right].$$

Lorsque $\nu = h$, c'est légèrement différent puisque la borne supérieure de l'inégalité est un entier (c'est k), donc égal à sa partie entière ; mais la valeur $r = k$ est exclue, donc r a une possibilité de moins que dans les autres cas :

$$N(h) = k - 1 - \left[\frac{k(h-1)}{h}\right].$$

On peut donc maintenant calculer la somme avec ce nouveau changement d'indice. On a donc :

$$\begin{aligned}
\sum_{r=1}^{k-1} \left[\frac{hr}{k}\right] \left(\left[\frac{hr}{k}\right] + 1\right) &= \sum_{\nu=1}^{h} (\nu-1)\nu N(\nu) \\
&= \sum_{\nu=1}^{h} (\nu-1)\nu \left(\left[\frac{k\nu}{h}\right] - \left[\frac{k(\nu-1)}{h}\right]\right) - h(h-1) \\
&= \sum_{\nu=1}^{h-1} \left[\frac{k\nu}{h}\right] ((\nu-1)\nu - \nu(\nu+1)) + kh(h-1) - h(h-1) \\
&= -2\sum_{\nu=1}^{h-1} \nu \left[\frac{k\nu}{h}\right] + h(h-1)(k-1).
\end{aligned}$$

Il reste à écrire que, par définition de $s(k,h)$, on a :

$$-2\sum_{\nu=1}^{h-1} \nu \left[\frac{k\nu}{h}\right] = 2hs(k,h) - 2\frac{k}{h}\sum_{\nu=1}^{h-1} \nu^2 + \sum_{\nu=1}^{h-1} \nu,$$

ce qui, injecté dans l'égalité précédente, donne :

$$\sum_{r=1}^{k-1}\left[\frac{hr}{k}\right]\left(\left[\frac{hr}{k}\right]+1\right)=2hs(k,h)-2\frac{k}{h}\sum_{\nu=1}^{h-1}\nu^2+\sum_{\nu=1}^{h-1}\nu+h(h-1)(k-1).$$

On reporte enfin ceci dans la première égalité reliant cette somme à $s(h,k)$:

$$2hs(h,k)+2hs(k,h)-2\frac{k}{h}\sum_{\nu=1}^{h-1}\nu^2+\sum_{\nu=1}^{h-1}\nu+h(h-1)(k-1)=\frac{h^2+1}{k^2}\sum_{r=1}^{k-1}r^2-\frac{1}{k}\sum_{r=1}^{k-1}r,$$

c'est-à-dire que :

$$\begin{aligned}2hs(h,k)+2hs(k,h)=2\frac{k}{h}\frac{h(h-1)(2h-1)}{6}-\frac{h(h-1)}{2}\\+\frac{h^2+1}{k^2}\frac{k(k-1)(2k-1)}{6}-\frac{1}{k}\frac{k(k-1)}{2}-h(h-1)(k-1).\end{aligned}$$

Il suffit alors de multiplier par $6k$ et d'effectuer les simplifications nécessaires pour obtenir la loi de réciprocité de Dedekind :

$$12hk(s(h,k)+s(k,h))=h^2+k^2-3hk+1.$$

□

4.2.3 Racine 24-ième de l'unité

Avec cette brève présentation des sommes de Dedekind, nous avons à présent tous les outils nécessaires pour déterminer de façon précise l'équation fonctionnelle vérifiée par η. Il nous manquait simplement la valeur de ϵ, cette racine 24-ième de l'unité intervenant dans l'équation.

Définition 4.2.2. *On définit, pour* $A=\begin{pmatrix}a & b\\ c & d\end{pmatrix}\in\Gamma$ *avec* $c>0$, *le nombre*

$$\epsilon(A)=exp\left\{i\pi\left(\frac{a+d}{12c}-s(d,c)\right)\right\},$$

où $s(d,c)$ *est la somme de Dedekind introduite au paragraphe précédent.*

Commençons par quelques propositions décrivant le comportement de ϵ sous l'action des deux générateurs du groupe modulaire Γ, $T=\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}$, et $S=\begin{pmatrix}0 & -1\\ 1 & 0\end{pmatrix}$.

Lemme 4.6. *Soit* $A=\begin{pmatrix}a & b\\ c & d\end{pmatrix}\in\Gamma$, *avec* $c>0$. *Alors, pout tout entier* m, *on a*

$$\epsilon(AT^m)=e^{im\pi/12}\epsilon(A).$$

Démonstration. On a $AT^m = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 & m \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a & am+b \\ c & cm+d \end{pmatrix}$, donc on a

$$\epsilon(AT^m) = exp\left\{ i\pi \left(\frac{a+cm+d}{12c} - s(cm+d,c) \right) \right\}.$$

Or, $s(cm+d,c) = s(d,c)$ (c'est l'une des propriétés des sommes de Dedekind vues au paragraphe précédent). Il reste alors à factoriser par $e^{im\pi/12}$ pour obtenir

$$\epsilon(AT^m) = e^{im\pi/12}\epsilon(A).$$

□

Lemme 4.7. *Soit* $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$, *avec* $c > 0$. *On a alors*

$$\epsilon(AS) = \begin{cases} e^{-i\pi/4}\epsilon(A) & si\ d > 0. \\ e^{i\pi/4}\epsilon(A) & si\ d < 0. \end{cases}$$

Démonstration. On a $AS = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} b & -a \\ d & -c \end{pmatrix}$.

Nous allons maintenant utiliser la loi de réciprocité de Dedekind pour exprimer $\epsilon(AS)$ en fonction de $\epsilon(A)$. Cependant, rappelons que cette loi impose que les deux arguments h et k de la somme de Dedekind soient positifs. De ce fait, il faut différencier les cas.

Si $d > 0$, on a donc

$$\epsilon(AS) = exp\left\{ i\pi \left(\frac{b-c}{12d} - s(-c,d) \right) \right\} = exp\left\{ i\pi \left(\frac{b-c}{12d} + s(c,d) \right) \right\}.$$

Or, $s(c,d)+s(d,c) = \frac{c}{12d} + \frac{d}{12c} - \frac{1}{4} + \frac{1}{12cd}$ (loi de réciprocité), donc, cela combiné au fait que $ad-bc = 1$ montre que

$$\frac{b-c}{12d} + s(c,d) = \frac{a+d}{12c} - s(d,c) - \frac{1}{4}.$$

Cela donne directement, lorsque $d > 0$:

$$\epsilon(AS) = exp\left\{ i\pi \left(\frac{a+d}{12c} - s(d,c) - \frac{1}{4} \right) \right\} = e^{-i\pi/4}\epsilon(A).$$

Lorsque $d < 0$, maintenant, on ne peut plus utiliser ainsi la loi de réciprocité. L'astuce consiste à représenter la matrice AS par $\begin{pmatrix} -b & a \\ -d & c \end{pmatrix}$: en effet, rappelons qu'une matrice et son opposée sont égales dans le groupe Γ ; de ce fait, les deux représentations sont équivalentes. Donc si $-d > 0$, la loi de réciprocité et la relation $ad-bc = 1$, donnent que

$$\frac{-b+c}{-12d} - s(c,-d) = \frac{a+d}{12c} - s(d,c) + \frac{1}{4}.$$

On a alors enfin, lorsque $d < 0$:

$$\epsilon(AS) = exp\left\{i\pi\left(\frac{-b+c}{-12d} - s(c,-d)\right)\right\}$$
$$= exp\left\{i\pi\left(\frac{a+d}{12c} - s(d,c) + \frac{1}{4}\right)\right\} = e^{i\pi/4}\epsilon(A).$$

□

Grâce à ces deux propositions, nous pouvons enfin en déduire l'équation fonctionnelle vérifiée par η :

Théorème 4.8. *Soit* $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$*, avec* $c > 0$*. Alors, pour tout* $\tau \in H$*, on a*

$$\eta\left(\frac{a\tau+b}{c\tau+d}\right) = \epsilon(A)\left(-i(c\tau+d)\right)^{1/2}\eta(\tau)$$

avec

$$\epsilon(A) = exp\left\{i\pi\left(\frac{a+d}{12c} - s(d,c)\right)\right\}.$$

Démonstration. Maintenant que nous savons comment se comporte ϵ sous l'action des générateurs du groupe modulaire, l'idée de la preuve de l'équation fonctionnelle va être très simple.

Tout $A \in \Gamma$ peut se décomposer $A = T^{n_1}ST^{n_2}\dots T^{n_k}$. Nous allons procéder par récurrence : on va supposer que l'équation est vraie pour $A \in \Gamma$ avec $c > 0$, et montrer qu'elle l'est alors pour AS et pour AT^m. Mais il va falloir faire un peu attention. En effet, l'équation n'a de sens que pour $c \neq 0$. Il va donc falloir s'assurer que les étapes successives de la récurrence ne font pas intervenir de matrice avec un $c = 0$, pour pouvoir appliquer l'hypothèse de récurrence sans crainte. C'est-à-dire que pour que tout se passe bien, il faut qu'aucune des matrices T^{n_1}, $T^{n_1}S$, $T^{n_1}ST^{n_2}$, …, $T^{n_1}ST^{n_2}\dots T^{n_k}$ (on prend k minimal dans la décomposition) n'ait son coefficient en bas à gauche nul. Si c'était le cas, alors une telle matrice s'écrirait comme puissance de T, et alors A pourrait se factoriser en $A = T^mB$ avec $m \neq 0$ (toujours pour une décomposition minimale, pour éviter de pouvoir écrire $A = T^mT^{-m}A$).

Commençons donc par le cas "simple", c'est-à-dire le cas où A ne peut pas s'écrire $A = T^mB$ avec $m \neq 0$. Dans ce cas, la récurrence va parfaitement fonctionner, car aucune des étapes ne fera intervenir de matrice ayant un $c = 0$ pour laquelle l'équation et donc l'hypothèse de récurrence n'auraient pas de sens. Dans ce cas, l'initialisation est assurée par la proposition 4.2, puisque toute décomposition de A commence par un S.

Pour l'hérédité, on suppose donc que l'équation est vraie pour un certain $A \in \Gamma$, avec $c > 0$: i.e. pour tout $\tau \in H$,

$$\eta\left(\frac{a\tau+b}{c\tau+d}\right) = \epsilon(A)\left(-i(c\tau+d)\right)^{1/2}\eta(\tau).$$

Appliquons cela à $T^m\tau$: on obtient

$$\eta\left(AT^m\tau\right) = \epsilon(A)\left(-i(cT^m\tau+d)\right)^{1/2}\eta(T^m\tau),$$

c'est-à-dire, avec la proposition 4.1,

$$\eta\left(AT^m\tau\right) = \epsilon(A)\left(-i(c\tau + mc + d)\right)^{1/2} e^{im\pi/12}\eta(\tau).$$

Par le lemme 4.6, on obtient

$$\eta\left(AT^m\tau\right) = \epsilon(AT^m)\left(-i(c\tau + mc + d)\right)^{1/2}\eta(\tau),$$

ce qui est exactement l'équation fonctionnelle pour $T^m\tau$.

Appliquons maintenant l'équation pour A et $S\tau$. On a

$$\eta\left(AS\tau\right) = \epsilon(A)\left(-i(cS\tau + d)\right)^{1/2}\eta(S\tau) = \epsilon(A)\left(-i(cS\tau + d)\right)^{1/2}(-i\tau)^{1/2}\eta(\tau),$$

grâce à la proposition 4.2.

Il faut à nouveau différencier les cas :
(i) Si $d > 0$, on écrit $cS\tau + d = \frac{d\tau - c}{\tau}$. Il s'ensuit que

$$\left(-i(cS\tau + d)\right)^{1/2}(-i\tau)^{1/2} = \left(-i(d\tau - c)\right)^{1/2}\frac{(-i\tau)^{1/2}}{\tau^{1/2}} = e^{-i\pi/4}\left(-i(d\tau - c)\right)^{1/2}.$$

On obtient alors :

$$\eta\left(AS\tau\right) = \epsilon(A)e^{-i\pi/4}\left(-i(d\tau - c)\right)^{1/2}\eta(\tau) = \epsilon(AS)\left(-i(d\tau - c)\right)^{1/2}\eta(\tau),$$

ce qui est l'équation fonctionnelle pour AS et $d > 0$.

(ii) Si $d < 0$, il suffit d'écrire que $cS\tau + d = \frac{-d\tau + c}{-\tau}$. Cela donne

$$\left(-i(cS\tau + d)\right)^{1/2}(-i\tau)^{1/2} = e^{i\pi/4}\left(-i(-d\tau + c)\right)^{1/2}$$

et donc, de même,

$$\eta\left(AS\tau\right) = \epsilon(A)e^{i\pi/4}\left(-i(-d\tau + c)\right)^{1/2}\eta(\tau) = \epsilon(AS)\left(-i(-d\tau + c)\right)^{1/2}\eta(\tau),$$

ce qui est l'équation fonctionnelle pour AS et $d < 0$ (rappelons que lorsque le coefficient en bas à gauche est négatif, on ne considère pas la matrice elle-même mais son opposée).

Ainsi, si l'équation fonctionnelle est vraie pour $A \in \Gamma$ avec $c > 0$, elle l'est pour AS et pour AT^m. Ceci clôt la récurrence, i.e. pour tout $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$, avec $c > 0$, et telle qu'on n'ait pas $A = T^m B$ avec $m \neq 0$, on a

$$\eta\left(\frac{a\tau + b}{c\tau + d}\right) = \epsilon(A)\left(-i(c\tau + d)\right)^{1/2}\eta(\tau).$$

Il reste le cas où A peut s'écrire $A = T^m B$ avec $m \neq 0$. On peut de plus supposer que B ne peut pas s'écrire $B = T^p C$, et donc que l'équation fonctionnelle est vraie pour B. Alors, en appliquant successivement la propriété 4.1 et l'équation fonctionnelle à B, on peut écrire que :

$$\eta(A\tau) = \eta(T^m B\tau) = e^{im\pi/12}\eta(B\tau) = e^{im\pi/12}\epsilon(B)\left(-i(c\tau + d)\right)^{1/2}\eta(\tau).$$

Il ne reste plus qu'à voir que $\epsilon(T^m B) = e^{im\pi/12}\epsilon(B)$. C'est exactement la même preuve que pour la proposition 4.6. Donc finalement, on a bien l'équation fonctionnelle pour A :

$$\eta(A\tau) = \epsilon(A)\left(-i(c\tau+d)\right)^{1/2}\eta(\tau).$$

□

4.3 Équation fonctionnelle de F

À partir de l'équation fonctionnelle de η, nous allons enfin pouvoir en déduire l'équation fonctionnelle de F que nous avions admise dans la première partie. La force de l'équation que nous allons obtenir est qu'elle relie le comportement de F en une racine de l'unité à son comportement en 0, que l'on connaît bien. Pour ce faire, nous allons appliquer l'équation fonctionnelle de η à un point τ proche de h/k (et cela correspondra au comportement de F en $e^{2i\pi h/k}$), avec un élément A de Γ bien choisi. Bien choisi dans le sens où le conjugué de τ par l'action de A sera non pas un autre nombre rationnel, qui donnerait encore le comportement de F en une autre racine de l'unité, mais un point τ' proche du point $i\infty$ qui, lui, donnera, après la transformation canonique $x = e^{2i\pi\tau}$, le comportement de F près de 0.

Théorème 4.9. *Soit $F(t) = 1/\prod_{n=1}^{\infty}(1-t^n)$.*
Soit $k \in \mathbb{N}$, $z \in \mathbb{C}$, $h, H \in \mathbb{Z}$ tels que $Re(z) > 0$, $(h,k) = 1$ et $hH \equiv -1[k]$
Alors, pour

$$x = exp\left(\frac{2i\pi h}{k} - \frac{2\pi z}{k^2}\right), x' = exp\left(\frac{2i\pi H}{k} - \frac{2\pi}{z}\right)$$

on a :

$$F(x) = e^{i\pi s(h,k)}\left(\frac{z}{k}\right)^{1/2} exp\left(\frac{\pi}{12z} - \frac{\pi z}{12k^2}\right)F(x').$$

Démonstration. On a, pour tout $\tau \in H$, la relation $F(e^{2i\pi\tau}) = e^{i\pi\tau/12}/\eta(\tau)$.

De plus, l'équation fonctionnelle de η s'écrit, lorsque $\tau' = A\tau$ pour $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$:

$$\frac{1}{\eta(\tau)} = \frac{1}{\eta(\tau')}\left(-i(c\tau+d)\right)^{1/2} exp\left\{i\pi\left(\frac{a+d}{12c} + s(-d,c)\right)\right\}.$$

En combinant ces deux relations, on obtient :

$$F(e^{2i\pi\tau}) = F(e^{2i\pi\tau'})exp\left(\frac{\pi i(\tau-\tau')}{12}\right)\left(-i(c\tau+d)\right)^{1/2} exp\left\{i\pi\left(\frac{a+d}{12c} + s(-d,c)\right)\right\}.$$

On choisit alors $a = H$, $c = k$, $d = -h$, et $b = -\frac{hH+1}{k}$ (entier car on a supposé $hH \equiv -1[k]$). On a bien $c > 0$, et $ad - bc = 1$. On prend alors $\tau = \frac{iz+h}{k}$, ce qui donne $\tau' = \frac{iz^{-1}+H}{k}$, et l'équation devient :

$$F\left(exp\left(\frac{2i\pi h}{k} - \frac{2\pi z}{k}\right)\right) = F\left(exp\left(\frac{2i\pi H}{k} - \frac{2\pi}{kz}\right)\right) z^{1/2} exp\left(\frac{\pi}{12kz} - \frac{\pi z}{12k} + \pi i s(h,k)\right).$$

Il ne vous reste plus qu'à remplacer z par z/k pour obtenir l'équation fonctionnelle de F. □

Bibliographie

[Apo76] Tom M. Apostol. *Introduction to analytic number theory.* Springer-Verlag, New York, 1976. Undergraduate Texts in Mathematics.

[Apo90] Tom M. Apostol. *Modular functions and Dirichlet series in number theory*, volume 41 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1990.

[CC10] David Chudnovsky and Gregory Chudnovsky, editors. *Additive number theory.* Springer, New York, 2010. Festschrift in honor of the sixtieth birthday of Melvyn B. Nathanson.

[Har59] G. H. Hardy. *Ramanujan : twelve lectures on subjects suggested by his life and work.* Chelsea Publishing Company, New York, 1959.

[HR00] G. H. Hardy and S. Ramanujan. Asymptotic formulæ in combinatory analysis [Proc. London Math. Soc. (2) **17** (1918), 75–115]. In *Collected papers of Srinivasa Ramanujan*, pages 276–309. AMS Chelsea Publ., Providence, RI, 2000.

[Wat95] G. N. Watson. *A treatise on the theory of Bessel functions.* Cambridge Mathematical Library. Cambridge University Press, Cambridge, 1995. Reprint of the second (1944) edition.

[Rad73] Rademacher, Hans. *Topics in analytic number theory.* Edited by E. Grosswald, J. Lehner and M. Newman, Die Grundlehren der mathematischen Wissenschaften, Band 169. Springer-Verlag, New York, second edition, 1973.

[MatWo] Weisstein, Eric W. *Partition Function P Congruences* . From MathWorld – A Wolfram Web Resource. *http ://mathworld.wolfram.com/PartitionFunctionPCongruences.html.*