Université P. et M. Curie (Paris VI),
Deuxième semestre 2007/2008

Michel Waldschmidt
date de mise à jour: 06/04/2008

Master de sciences et technologies 1ère année -
Spécialité : Mathématiques Fondamentales

Mention : Mathématiques et applications
MO11 : Théorie des nombres (12 ECTS)

Huitième fascicule : 07/04/2008

5 Théorie analytique des nombres

Dans cette partie nous nous intéressons à la répartition des nombres premiers. On doit à Euler (1737) la démonstration du fait que la série

$$\sum_p \frac{1}{p} = \frac{1}{2} + \frac{1}{3} + \frac{1}{5} + \frac{1}{7} + \frac{1}{11} + \cdots$$

diverge.

Pour $x > 0$ on désigne par $\pi(x)$ le nombre de nombres premiers inférieurs ou égaux à x :

$$\pi(x) = \sum_{p \le x} 1. \tag{5.1}$$

Ainsi $\pi(10) = 4$, $\pi(100) = 25$, $\pi(1000) = 168$, $\pi(10\,000) = 1229$.

Le théorème des nombres premiers, conjecturé par Gauss en 1792, et par Legendre en 1798, a été démontré par Hadamard et de la Vallée Poussin en 1896. Il s'énonce :

Théorème 5.2 (Théorème des nombres premiers)**.** *Pour $x \to \infty$ on a*

$$\pi(x) \sim \frac{x}{\log x}.$$

Une approximation de $\pi(x)$ numériquement meilleure que (mais asymptotiquement équivalente à) $x/\log x$ est donnée par la fonction *logarithme intégral*

$$\mathrm{Li}(x) = \int_2^x \frac{dt}{\log t}.$$

Des estimations plus faibles étaient dues à Tchébychev (1851) :

$$0,921\cdots \frac{x}{\log x} \le \pi(x) \le 0,105\cdots \frac{x}{\log x}$$

pour $x \ge 30$. Nous établirons un tel encadrement (avec des constantes un peu moins précises) par des méthodes élémentaires. Ensuite nous introduirons la fonction zêta de Riemann pour présenter certains des arguments conduisant au théorème des nombres premiers.

Enfin nous étudierons les fonctions arithmétiques et leur produit de convolution.

On trouvera dans [T] des références aux résultats uniformes suivants

$$\prod_{p\le n} p \le 3^n \quad \text{pour tout entier } n \ge 2$$

et

$$\frac{x}{\log x}\left(1+\frac{1}{2\log x}\right) \le \pi(x) \le \frac{x}{\log x}\left(1+\frac{3}{2\log x}\right) \quad \text{pour tout } x \ge 52.$$

5.1 Méthodes élémentaires

On définit des fonctions arithmétiques $\pi(x)$, $\theta(x)$ et $\psi(x)$ (Tchébychev) et Λ (*fonction de von Mangoldt*) par

$$\pi(x) = \sum_{p\le x} 1, \qquad \theta(x) = \sum_{p\le x} \log p, \qquad \Psi(x) = \sum_{p^m \le x} \log p,$$

$$\Lambda(n) = \begin{cases} \log p & \text{si } n = p^m \text{ avec } p \text{ premier} \\ 0 & \text{si } n \text{ n'est pas une puissance d'un nombre premier.} \end{cases}$$

Ainsi

$$\psi(x) = \sum_{n\le x} \Lambda(n) = \sum_{k=1}^{\infty} \theta(x^{1/k}).$$

La somme est finie : les termes sont nuls pour k tel que $2^k > x$.

Lemme 5.3. *On a*

$$\pi(x) \sim \frac{x}{\log x} \iff p_n \sim n\log n.$$

De plus les deux conditions suivantes sont équivalentes :
(i) Il existe deux constantes c_1 et c_2 telles que, pour tout $n \ge 2$,

$$c_1 \frac{x}{\log x} \le \pi(x) \le c_2 \frac{x}{\log x}$$

(ii) Il existe deux constantes c_3 et c_4 telles que, pour tout $n \ge 2$,

$$c_3 n\log n \le p_n \le c_4 n \log n.$$

Démonstration. Les détails de la démonstration (facile) sont laissés en exercice, l'idée est d'utiliser la relation $\pi(p_n) = n$ qui résulte de la définition et permet d'établir

$$\pi(x) \sim \frac{x}{\log x} \iff n \sim \frac{p_n}{\log p_n} \iff p_n \sim n\log n.$$

□

Lemme 5.4. *On a*

$$\pi(x) \sim \frac{x}{\log x} \iff \theta(x) \sim x.$$

De plus les deux conditions suivantes sont équivalentes :
(i) Il existe deux constantes c_1 et c_2 telles que, pour tout $n \geq 2$,

$$c_1 \frac{x}{\log x} \leq \pi(x) \leq c_2 \frac{x}{\log x}$$

(ii) Il existe deux constantes c_5 et c_6 telles que, pour tout $n \geq 2$,

$$c_5 x \leq \theta(x) \leq c_6 x.$$

Démonstration. On a

$$\theta(x) = \sum_{p \leq x} \log p \leq \log x \sum_{p \leq x} 1 = \pi(x) \log x.$$

De l'autre côté pour $2 \leq y \leq x$ on a

$$\pi(x) - \pi(y) = \sum_{y < p \leq x} 1 \leq \frac{1}{\log y} \sum_{y < p \leq x} \log p = \frac{1}{\log y} \big(\theta(x) - \theta(y)\big)$$

donc

$$\pi(x) \leq \frac{\theta(x)}{\log y} + \pi(y) \leq \frac{\theta(x)}{\log y} + y.$$

On prend $y = x/(\log x)^2$:

$$\pi(x) \leq \frac{\theta(x)}{\log x - 2 \log\log x} + \frac{x}{(\log x)^2}. \tag{5.5}$$

Le lemme 5.4 en résulte.

□

Lemme 5.6. *On a l'équivalence entre les deux assertions suivantes,*

$$\psi(x) \sim x \quad \textit{pour } x \to \infty \qquad \Longleftrightarrow \quad \theta(x) \sim x \quad \textit{pour } x \to \infty \quad .$$

De plus les deux conditions suivantes sont équivalentes :
(i) Il existe deux constantes c_7 et c_8 telles que, pour tout $n \geq 2$,

$$c_7 x \leq \psi(x) \leq c_8 x$$

(ii) Il existe deux constantes c_5 et c_6 telles que, pour tout $n \geq 2$,

$$c_5 x \leq \theta(x) \leq c_6 x.$$

Démonstration. L'inégalité $\theta(x) \leq \psi(x)$ est évidente. De l'autre côté

$$\psi(x) = \theta(x) + \theta(\sqrt{x}) + \theta(\sqrt[3]{x}) + \cdots + \theta(\sqrt[N]{x})$$

où N est le plus grand entier tel que $X \geq 2^N$. Comme $\theta(\sqrt[m]{x}) \leq \theta(x)$ pour $m \geq 2$, on en déduit

$$\psi(x) \leq \theta(x) + \theta(\sqrt{x}) \frac{\log x}{\log 2}.$$

Le lemme 5.6 en résulte.

□

Nous allons donner une démonstration élémentaire du résultat suivant.

Proposition 5.7. *On a, pour tout $x \geq 2$,*

$$\theta(x) \leq 2x \log 4.$$

La démonstration utilise le lemme suivant.

Lemme 5.8. *On a, pour $n \geq 2$,*

$$2^n \leq \binom{2n}{n} \leq 4^n.$$

Démonstration. L'inégalité de droite provient du développement de $(1+1)^{2n}$, celle de gauche de la majoration

$$\frac{n+k}{k} \geq 2 \quad \text{pour} \quad 1 \leq k \leq n.$$

□

Démonstration de la proposition 5.7. Chaque nombre premier p dans l'intervalle $n \leq p \leq 2n$ divise

$$\binom{2n}{n} = \frac{2n(2n-1)\cdots(n+1)}{n(n-1)\cdots 1}.$$

Donc

$$4^n \geq \binom{2n}{n} \geq \prod_{n \leq p \leq 2n} p.$$

Par conséquent

$$n \log 4 \geq \theta(2n) - \theta(n).$$

Ainsi

$$\theta(2^m) = \sum_{k=0}^{m-1} \big(\theta(2^{k+1}) - \theta(2^k)\big) \leq \sum_{k=0}^{m-1} 2^k \log 4 = (2^m - 1) \log 4.$$

Pour $x \geq 1$, soit m l'entier tel que $2^m \leq x < 2^{m+1}$; alors

$$\theta(x) \leq \theta(2^{m+1}) \leq 2^{m+1} \log 4 \leq 2x \log 4.$$

□

De la proposition 5.7 jointe à l'inégalité 5.5 on déduit

$$\pi(x) \leq \big(2 \log 4 + o(1)\big)x.$$

Voici maintenant une démonstration élémentaire de l'inégalité dans l'autre sens :

Proposition 5.9. *Il existe une constante $C > 0$ telle que*

$$\pi(x) \geq C \frac{x}{\log x}$$

pour tout $x \geq 2$.

On utilise le lemme bien connu suivant :

Lemme 5.10. *On a*

$$v_p(n!) = \sum_{1 \leq m \leq (\log n)/(\log p)} \left[\frac{n}{p^m} \right].$$

Démonstration. Pour chaque p et chaque $m \geq 1$ on compte le nombre d'entiers dans l'intervalle $1 \leq k \leq n$ divisibles par p^m.

□

Lemme 5.11. *On a*

$$v_p \binom{2n}{n} \leq \frac{\log(2n)}{\log p}.$$

Démonstration. On a, d'après le lemme 5.10,

$$v_p \binom{2n}{n} = v_p(2n)! - 2v_p(n!) = \sum_{m \geq 1} \left[\frac{2n}{p^m} \right] - 2 \left[\frac{n}{p^m} \right].$$

Pour $u \in \mathbf{R}$ on a

$$\begin{cases} [2u] = 2[u], & \{2u\} = 2\{u\} & \text{si } 0 \leq \{u\} < 1/2, \\ [2u] = 2[u] + 1, & \{2u\} = 2\{u\} - 1 & \text{si } 1/2 \leq \{u\} < 1. \end{cases}$$

En particulier $[2u] - 2[u] = 0$ pour $0 \leq u < 1/2$. Les m tels que $2n \leq p^m$ ne contribuent donc pas. Donc on restreint la somme à $p^m < 2n$ et pour $u = n/p^m$ on majore $[2u] - 2[u]$ par 1. Ainsi

$$v_p \binom{2n}{n} \leq \sum_{\substack{m \geq 1 \\ p^m \leq 2n}} 1 = \left[\frac{\log(2n)}{\log p} \right] \leq \frac{\log(2n)}{\log p}.$$

□

Démonstration de la proposition 5.9. Les facteurs premiers du coefficient binomial $\binom{2n}{n}$ sont majorés par $2n$:

$$\binom{2n}{n} = \prod_{p \leq 2n} p^{v_p\left(\binom{2n}{n}\right)}.$$

Du lemme 5.11 on déduit

$$\binom{2n}{n} = \prod_{p \leq 2n} p^{\log(2n)/\log p} \leq (2n)^{\sum_{p \leq 2n} 1} = (2n)^{\pi(2n)},$$

donc (lemme 5.8)

$$n \log 2 \leq \log \binom{2n}{n} \leq \pi(2n) \log(2n).$$

Soit $x \geq 2$ est soit $n \geq 1$ tel que $2n \leq x < 2(n+1)$. On obtient

$$\pi(x) \geq \pi(2n) \geq \frac{n \log 2}{\log(2n)} \geq \left(\frac{x}{2} - 1 \right) \frac{\log 2}{\log x},$$

d'où

$$\pi(x) \geq \left(\frac{1}{2}\log 2 + o(1)\right)\frac{x}{\log x}\cdot$$

□

Voici deux estimations dues à Mertens :

Proposition 5.12. *On a, pour $x \to \infty$,*

$$\sum_{p\leq x}\frac{\log p}{p} = \log x + O(1).$$

De plus il existe une constante $C > 0$ telle que pour $x \to \infty$,

$$\sum_{p\leq x}\frac{1}{p} = \log\log x + C + O(1/\log x).$$

La démonstration repose sur une comparaison entre sommes et intégrales.

Lemme 5.13. *Soit f une fonction C^1 sur un intervalle entier $[M, N]$ avec $M \geq N \geq 1$. Alors*

$$\sum_{n=M+1}^{N} f(n) = \int_M^N f(t)dt + \int_M^N (t - [t])f'(t)dt.$$

Le lemme 5.13 est un corollaire du résultat suivant :

Lemme 5.14 (Lemme d'Abel)**.** *Soit f une fonction C^1 sur un intervalle $[y, x]$ avec $x > y \geq 1$ et soit $(a_n)_{n\geq 1}$ une suite de nombres complexes. On pose*

$$A(x) = \sum_{n\leq x} a_n.$$

Alors

$$\sum_{y<n\leq x} a_n f(n) = A(x)f(x) - A(y)f(y) - \int_y^x A(t)f'(t)dt.$$

Démonstration du lemme 5.13. On utilise le lemme 5.14 avec $a_n = 1$ pour tout n, donc $A(t) = [t]$, et $y = M$, $x = N$:

$$\sum_{n=M+1}^{N} f(n) = Nf(N) - Mf(M) - \int_M^N [t]f'(t)dt.$$

On utilise ensuite l'égalité

$$Nf(N) - Mf(M) = \int_M^N f(t)dt + \int_M^N tf'(t)dt,$$

qui s'obtient en intégrant par parties.

□

Avant de démontrer ce lemme 5.14 d'Abel nous déduisons du lemme 5.13 quelques conséquences. On définit la *constante d'Euler* par l'intégrale convergente

$$\gamma = 1 - \int_1^\infty (t - [t]) \frac{dt}{t^2}.$$

Corollaire 5.15. *Pour $N \geq 2$ on a*

$$\left| \sum_{n \leq N} \frac{1}{n} - \log N - \gamma \right| \leq \frac{1}{N}.$$

Démonstration. Pour $f(t) = 1/t$ et $M = 1$, en ajoutant $n = 1$ au deuxième membre de la conclusion du lemme 5.13 on trouve

$$\sum_{n=1}^{N} \frac{1}{n} = 1 + \int_1^N \frac{dt}{t} - \int_1^N (t - [t]) \frac{dt}{t^2}.$$

Alors

$$\sum_{n=1}^{N} \frac{1}{n} = \log N + \gamma + \int_N^\infty (t - [t]) \frac{dt}{t^2},$$

et

$$0 < \int_N^\infty (t - [t]) \frac{dt}{t^2} \leq \int_N^\infty \frac{dt}{t^2} = \frac{1}{N}.$$

□

Corollaire 5.16. *Il existe une constante absolue c telle que, pour $x \to \infty$ on ait*

$$\sum_{n \leq x} \log n = x \log x - x + O(\log x) \quad \textit{quand } x \to \infty.$$

La *formule de Stirling* est un peu plus précise :

$$n! \sim n^n e^{-n} \sqrt{2\pi n}.$$

Démonstration du corollaire 5.16. On utilise le lemme 5.13 avec $f(t) = \log t$, $N = [x]$. On a

$$\sum_{2 \leq n \leq x} f(n) = \sum_{1 \leq n \leq x} \log n = \log\big([x]!\big),$$

$$\int_1^N f(t)dt = \int_1^N (\log t)dt = N \log N - N + 1$$

et

$$\int_1^N (t - [t]) f'(t)dt = \int_1^N (t - [t]) \frac{dt}{t} = O(\log N),$$

d'où

$$\log\big([x]!\big) = [x] \log x - x + 1 - \int_1^x \frac{[t] - t}{t} dt = x \log x - x + O(\log x).$$

□

Démonstration du lemme d'Abel 5.14. Pour $n \leq t < n+1$ on a

$$A(t) = A(n) = \sum_{k=0}^{n} a_k.$$

Alors

$$\int_n^{n+1} A(t)f'(t)dt = A(n)\int_n^{n+1} f'(t)dt = A(n)\big(f(n+1) - f(n)\big).$$

Supposons $x = N$ et $y = M$ entiers. On a

$$\begin{aligned}
\int_M^N A(t)f'(t)dt &= \sum_{n=M}^{N-1}\int_n^{n+1} A(t)f'(t)dt = \sum_{n=M}^{N-1} A(n)\big(f(n+1) - f(n)\big) \\
&= \sum_{n=M+1}^{N} A(n-1)f(n) - \sum_{n=M}^{N-1} A(n)f(n) \\
&= -\sum_{n=M+1}^{N} f(n)\big(A(n) - A(n-1)\big) + f(N)A(N) - f(M)A(M) \\
&= -\sum_{n=M+1}^{N} a_n f(n) + f(N)A(N) - f(M)A(M).
\end{aligned}$$

La formule est démontrée quand x et y sont entiers. Quand x n'est pas entier il suffit d'ajouter

$$\int_{[x]}^{x} A(t)f'(t)dt = A\big([x]\big)\big(f(x) - f\big([x]\big)\big)$$

avec $A\big([x]\big) = A(x)$. De même quand y n'est pas entier. □

Démonstration de la proposition 5.12. On écrit

$$\log[x]! = \sum_{p \leq x} v_p([x]!)\log p$$

et (lemme 5.10)

$$v_p[x]! = \sum_{m \geq 1}\left[\frac{x}{p^m}\right].$$

Dans le membre de droite le terme principal est obtenu pour $m = 1$, il est équivalent à x/p, ce qui va nous permettre de vérifier

$$\log[x]! \sim x\sum_{p \leq x}\frac{\log p}{p}.$$

Pour obtenir la première partie de la proposition 5.12, il suffira alors d'utiliser le corollaire 5.16.

On a

$$\log[x]! = \sum_{p\le x}\sum_{m\ge 1}\left[\frac{x}{p^m}\right]\log p,$$
$$= x\sum_{p\le x}\frac{\log p}{p} + \sum_{p\le x}\left(\left[\frac{x}{p}\right]-\frac{x}{p}\right)\log p + \sum_{p\le x}\sum_{m\ge 2}\left[\frac{x}{p^m}\right]\log p.$$

Or

$$-1 \le \left[\frac{x}{p}\right]-\frac{x}{p}\le 0$$

et (proposition 5.7)

$$\sum_{p\le x}\log p = \theta(x) = O(x).$$

Ensuite

$$\sum_{m\ge 2}\left[\frac{x}{p^m}\right] \le x\sum_{m\ge 2}\frac{1}{p^m} = x\cdot\frac{1/p^2}{1-(1/p)} = x\cdot\frac{1}{p(p-1)},$$

donc

$$\sum_{p\le x}\sum_{m\ge 2}\left[\frac{x}{p^m}\right]\log p \le x\sum_{p\le x}\frac{\log p}{p(p-1)} \le x\sum_{n\ge 2}\frac{\log n}{n^2} = O(x).$$

Finalement

$$\sum_{p\le x}\frac{\log p}{p} = \log x + O(1).$$

Pour démontrer la seconde partie de la proposition 5.12, on utilise le lemme 5.14 d'Abel avec $f(t) = 1/\log t$, $y = 2$ et

$$a_n = \begin{cases} (\log p)/p & \text{si } n = p \text{ est premier,}\\ 0 & \text{si } n \text{ est composé.}\end{cases}$$

On a

$$\sum_{1\le n<x} a_n f(n) = \sum_{p\le x}\frac{1}{p},$$

$$A(x) = \sum_{p\le x}\frac{\log p}{p} = \log x + O(1),$$

$$A(x)f(x) = \sum_{p\le x}\frac{\log p}{p}\cdot\frac{1}{\log x} = 1 + O(1/\log x),$$

$$\int_y^x A(t)f'(t)dt = -\int_2^x A(t)\frac{dt}{t(\log t)^2} = -\int_2^x\frac{dt}{t\log t} - \int_2^x\big(A(t)-\log t\big)\frac{dt}{t(\log t)^2},$$

et

$$\int_2^x\frac{dt}{t\log t} = \log\log x - \log\log 2.$$

Donc

$$\sum_{p\leq x}\frac{1}{p}=\log\log x+C+O(1/\log x).$$

□

5.2 La fonction zêta de Riemann

La démonstration par Hadamard et de la Vallée Poussin du théorème 5.2 des nombres premiers repose sur l'analyse complexe et la fonction zêta de Riemann. La série $\sum_{n\geq 1} n^{-s}$ converge normalement, donc uniformément pour s dans un compact du demi plan $\Re s > 1$. Par conséquent elle définit une fonction analytique dans ce demi-plan qui est la fonction zêta (introduite par Riemann en 1859 dans son unique article de théorie des nombres) :

$$\zeta(s)=\sum_{n\geq 1}\frac{1}{n^s}\cdot$$

Les valeurs de cette fonction pour s réel positif avaient déjà été étudiées par Euler en 1736. Il montrait notamment que pour s entier positif pair le quotient $\zeta(s)/\pi^s$ est un nombre rationnel. Par exemple $\zeta(2)=\pi^2/6$, $\zeta(4)=\pi^4/90$. Euler ne s'est pas contenté d'étudier les valeurs de cette fonction pour s positif, il a aussi considéré le cas des entiers négatifs (où la série diverge), par exemple $\zeta(0)=-1/2$, $\zeta(-1)=-1/12$. Il a établi que ζ s'annule en les entiers négatifs pairs et prend une valeur rationnelle non nulle en les entiers négatifs impairs.

5.2.1 Produit Eulérien de la fonction zêta de Riemann

Le *théorème fondamental de l'arithmétique* selon lequel l'anneau $\mathbf{Z}$ est factoriel est intégré dans l'énoncé suivant qui éclaire l'importance du rôle joué par la fonction zêta dans l'étude de la répartition des nombres premiers.

Théorème 5.17 (Produit d'Euler)**.** *Le produit infini $\prod_p(1-p^{-s})$ étendu aux nombres premiers p, est uniformément sur tout compact du demi plan $\Re s > 1$. Il définit une fonction analytique dans ce demi plan qui vérifie*

$$\zeta(s)=\prod_p\frac{1}{1-p^{-s}}\cdot$$

Le fait que la série harmonique $\sum_{n\geq 1} 1/n$ diverge permet d'en déduire que la série $\sum_p 1/p$ est aussi divergente.

Démonstration. Soit X un nombre entier suffisamment grand. En faisant le produit pour les nombres premiers $\leq X$ des séries géométriques

$$\frac{1}{1-p^{-s}}=\sum_{m\geq 0}\frac{1}{p^{ms}}$$

on trouve

$$\prod_{p\leq X}\frac{1}{1-p^{-s}}=\prod_{p\leq X}\sum_{m\geq 0}\frac{1}{p^{ms}}=\sum_{n\in\mathcal{N}(X)}\frac{1}{n^s},$$

où $\mathcal{N}(X)$ est l'ensemble des entiers positifs dont tous les facteurs premiers sont $\leq X$. Alors pour $\Re s = \sigma > 1$ on a

$$\left|\zeta(s) - \prod_{p\leq X} \frac{1}{1-p^{-s}}\right| = \left|\sum_{n\notin\mathcal{N}(X)} \frac{1}{n^s}\right| \leq \sum_{n>X} \left|\frac{1}{n^s}\right| = \sum_{n>X} \frac{1}{n^\sigma}.$$

La définition de la convergence d'un produit infini dont tous les facteurs sont différents de 0 impose que le produit ne soit pas nul. Afin de vérifier $\zeta(s) \neq 0$ pour $\Re s > 1$, on utilise le développement en série de Taylor de la détermination principale du logarithme complexe : pour $|u| < 1$,

$$\log(1-u) = -\sum_{m\geq 1} \frac{u^m}{m}.$$

On remplace u par p^{-s} :

$$\log(1-p^{-s}) = -\sum_{m\geq 1} \frac{p^{-ms}}{m}$$

et on trouve, pour $\Re s > 1$,

$$\zeta(s) = \exp\left(\sum_p \sum_{m\geq 1} \frac{1}{mp^{ms}}\right). \tag{5.18}$$

Donc $\zeta(s) \neq 0$ pour $\Re s > 1$. □

On écrit (5.18) sous la forme [5]

$$\log \zeta(s) = \sum_p \sum_{m\geq 1} \frac{1}{mp^{ms}}.$$

En dérivant, on obtient le développement en série de la dérivée logarithmique de ζ dans ce demi plan.

Corollaire 5.19. *La série*

$$\sum_p \sum_{m\geq 1} \frac{1}{mp^{ms}}$$

définit une fonction analytique dans le demi plan $\Re s > 1$ qui est une détermination analytique du logarithme de $\zeta(s)$ dans ce demi plan. De plus la dérivée logarithmique de $\zeta(s)$ vérifie pour $\Re s > 1$:

$$\frac{\zeta'(s)}{\zeta(s)} = -\sum_p \sum_{m\geq 1} \frac{\log p}{p^{ms}}.$$

Le développement en série de ζ'/ζ peut aussi s'écrire

$$\frac{\zeta'(s)}{\zeta(s)} = -\sum_{n\geq 1} \frac{\Lambda(n)}{n^s}$$

où Λ désigne la fonction de von Mangoldt (cf. § 5.1).

[5] Quand f et g sont deux fonctions complexes, on écrit $f = \log g$ pour signifier $g = e^f$.

Théorème 5.20 (Prolongement analytique de la fonction zêta de Riemann)**.** *La fonction* $\zeta(s) - 1/(s-1)$ *se prolonge en une fonction analytique dans le demi plan* $\Re s > 0$.

Démonstration. On écrit, pour $n \geq 1$,

$$\frac{1}{n^s} = s \int_n^\infty t^{-s-1} dt.$$

Alors

$$\zeta(s) = s \sum_{n \geq 1} \int_n^\infty t^{-s-1} dt = s \int_1^\infty [t] t^{-s-1} dt$$

car $\sum_{n=1}^t 1 = [t]$. Donc

$$\zeta(s) = s \int_1^\infty t^{-s} dt + s \int_1^\infty ([t] - t) t^{-s-1} dt.$$

Le premier terme vaut

$$s \int_1^\infty t^{-s} dt = \frac{1}{s-1} + 1$$

et la seconde intégrale est convergente dans $\Re s > 0$ où elle définit une fonction holomorphe. □

Exercice. Vérifier

$$\lim_{s \to 1} \left(\zeta(s) - \frac{1}{s-1} \right) = \gamma$$

où γ est la *constante d'Euler* (voir Corollaire 5.15) :

$$\gamma = \lim_{N \to \infty} \frac{1}{1} + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{N} - \log N.$$

Ainsi la fonction zêta de Riemann se prolonge en une fonction méromorphe dans le demi plan $\Re s > 0$ avec un pôle simple en $s = 1$, de résidu 1. Une des étapes essentielles dans la démonstration du théorème 5.2 des nombres premiers consiste à montrer que la fonction ζ ainsi prolongée ne s'annule pas dans un ouvert contenant le demi plan fermé $\Re s \geq 1$. Plus précisément *il existe une constante* $A > 0$ *telle que la fonction* ζ*, ainsi prolongée, ne s'annule pas dans le domaine*

$$1 - \frac{A}{\log |\Im s|} < \Re s < 1.$$

Nous utiliserons dans la section 5.2.2 l'énoncé suivant :

Théorème 5.21. *La fonction* ζ *ne s'annule pas sur la droite* $\Re s = 1$, $s \neq 1$.

Il en résulte que la fonction

$$\frac{\zeta'(s)}{\zeta(s)} + \frac{1}{s-1},$$

définie pour $\Re s > 1$, s'étend en une fonction holomorphe dans un voisinage de la droite $\Re s = 1$.

5.2.2 Démonstration du théorème des nombres premiers

Nous avons vu que le théorème 5.2 des nombres premiers était équivalent à $\theta(x) \sim x$ pour $x \to \infty$. Nous allons montrer que cette équivalence résulte de l'énoncé suivant

Proposition 5.22. *L'intégrale*

$$F(0) := \int_1^\infty \big(\theta(t) - t\big)\frac{dt}{t^2}$$

converge.

Démonstration de l'équivalence $\theta(x) \sim x$ comme conséquence de la proposition 5.22. Montrons d'abord, en utilisant la proposition 5.22, que l'on a

$$\limsup_{x\to\infty} \frac{\theta(x)}{x} \leq 1.$$

On raisonne par l'absurde : si cette limite sup est > 1, il existe $\eta > 1$ et il existe une suite x_n tendant vers l'infini tels que $\theta(x_n) > (1+2\eta)x_n$ pour tout n. Comme la fonction θ est croissante , pour $x_n \leq t \leq (1+\eta)x_n$ on a $\theta(t) \geq \theta(x_n) > (1+2\eta)x_n$ et $\theta(t) - t \geq \eta x_n$,

$$\frac{x_n}{t^2} \geq \frac{1}{x_n}\cdot\frac{1}{(1+\eta)^2}, \geq \frac{1}{x_n}\cdot\frac{1}{1+\eta},$$

donc dans cet intervalle

$$\frac{\theta(t)-t}{t^2} \geq \frac{\eta x_n}{t^2} \geq \frac{\eta}{x_n(1+\eta)}.$$

Donc

$$\int_{x_n}^{x_n(1+\eta)} \big(\theta(t)-t\big)\frac{dt}{t^2} \geq x_n \cdot \frac{\eta}{2+\eta}\cdot\frac{\eta}{x_n} = \frac{\eta^2}{2+\eta},$$

donc l'intégrale ne converge pas, contrairement à ce que donne la proposition 5.22.

Le même argument montre que

$$\liminf_{x\to\infty} \frac{\theta(x)}{x} \geq 1.$$

Par conséquent la proposition 5.22 implique $\lim_{n\to\infty} \theta(x)/x = 1$. □

Remarque. Le fait que $\theta(x)$ soit équivalent à x ne suffit pas à démontrer la proposition 5.22. Si on définit un fonction $\epsilon(t)$ par $\theta(t) = t\big(1+\epsilon(t)\big)$, l'équivalence $\theta(x) \sim x$ signifie que $\epsilon(t)$ tend vers 0 quand t tend vers l'infini, mais cela ne suffit pas à assurer que l'intégrale $\int_1^\infty \epsilon(t)dt/t$ converge. Par exemple l'intégrale $\int_1^\infty dt/t\log t$ ne converge pas.

Pour s complexe de partie réelle > 0, posons

$$F(s) = \int_1^\infty \big(\theta(t)-t\big)\frac{dt}{t^{s+1}}.$$

Le changement de variable $t = e^u$ dans l'intégrale définissant F montre que, pour $\Re s > 1$ on a

$$F(s) = \int_0^\infty \big(\theta(e^u) - e^u\big)\frac{e^u du}{e^{u(s+1)}} = \int_0^\infty h(u)e^{-us}du$$

avec $h(u) = \theta(u) - e^u$. Rappelons que $|e^{-us}| = e^{-u\Re s}$. Donc pour $\Re s > 1$ l'intégrale définissant F converge, et F est analytique dans ce demi–plan.

Proposition 5.23. *La fonction F est analytique dans le demi plan ouvert $\Re s > 1$ et se prolonge en une fonction analytique sur un ouvert contenant le demi plan fermé $\Re s \geq 1$.*

L'énoncé suivant (que nous ne démontrerons pas) dû à Ingham (1935) permet de déduire de la proposition 5.23 que l'intégrale converge en $s = 0$, ce qui est la proposition 5.22.

Théorème 5.24 (Ingham)**.** *Soit f une fonction mesurable bornée sur $[1, \infty)$. On suppose que la fonction holomorphe*

$$F(s) = \int_1^\infty \frac{f(t)}{t^s} dt$$

définie pour $\Re s > 1$ admet un prolongement analytique au voisinage du demi–plan fermé $\Re s \geq 1$. Alors

$$\lim_{T \to \infty} \int_1^T \frac{f(t)}{t} dt = F(1).$$

La démonstration de la proposition 5.23 utilisera le lemme auxiliaire suivant.

Lemme 5.25. *La fonction définie pour $\Re s > 1$ par*

$$f(s) = \frac{\zeta'(s)}{\zeta(s)} + \sum_p \frac{\log p}{p^s},$$

se prolonge en une fonction holomorphe dans $\Re s > 1/2$.

Démonstration du lemme 5.25. Comme

$$\frac{\zeta'(s)}{\zeta(s)} = -\sum_p \sum_{m \geq 1} \frac{\log p}{p^{ms}}$$

on a

$$f(s) = -\sum_p \sum_{m \geq 2} \frac{\log p}{p^{ms}}.$$

Pour tout $\sigma_0 > 1/2$ la série à droite converge normalement dans $\Re s \geq \sigma_0$. □

Démonstration de la proposition 5.23. On écrit, pour $\Re s > 1$,

$$F(s) = \sum_{n \geq 1} \int_n^{n+1} \frac{\theta(t)}{t^{s+1}} dt - \int_1^\infty \frac{dt}{t^s}.$$

On a

$$\int_1^\infty \frac{dt}{t^s} = \frac{1}{s-1}$$

et

$$\int_n^{n+1} \frac{\theta(t)}{t^{s+1}} dt = \theta(n) \int_n^{n+1} \frac{dt}{t^{s+1}} = \frac{\theta(n)}{s} \left(\frac{1}{n^s} - \frac{1}{(n+1)^s} \right),$$

Donc

$$\begin{aligned} F(s) &= \frac{1}{s}\sum_{n\geq 1}\left(\frac{1}{n^s}-\frac{1}{(n+1)^s}\right)\theta(n)-\frac{1}{s-1} \\ &= \frac{1}{s}\sum_{n\geq 1}\frac{1}{n^s}\big(\theta(n)-\theta(n-1)\big)-\frac{1}{s-1} \\ &= \frac{1}{s}\sum_{p}\frac{\log p}{p^s}-\frac{1}{s-1} \\ &= -\frac{1}{s}\cdot\frac{\zeta'(s)}{\zeta(s)}+\frac{f(s)}{s}-\frac{1}{s-1}, \end{aligned}$$

avec la fonction f introduite au lemme 5.25.

La fonction ζ a un pôle simple en $s=1$, donc ζ'/ζ a un pôle simple de résidu -1 en $s=1$, ce qui signifie que

$$\frac{\zeta'(s)}{\zeta(s)}+\frac{1}{s-1}$$

se prolonge en une fonctions holomorphe en $s=1$. On utilise le théorème 5.21 : la fonction ζ ne s'annule pas sur la demi-droite $\Re s=1$. Donc la fonction $\frac{\zeta'(s)}{\zeta(s)}+\frac{1}{s-1}$ se prolonge en une fonction holomorphe dans un voisinage ouvert de $\Re s\geq 1$. On conclut en observant que

$$\frac{1}{s-1}\left(\frac{1}{s}-1\right)=\frac{1}{s}$$

est analytique dans $\mathbf{C}\setminus\{0\}$.

□

5.2.3 Equation fonctionnelle de la fonction zêta

Riemann a démontré en 1859 que la fonction zêta s'étendait en une fonction méromorphe dans tout le plan complexe, avec un unique pôle simple en $s=1$, et que de plus cette fonction ainsi étendue vérifiait une équation fonctionnelle. Pour l'écrire on introduit la fonction Gamma d'Euler

Proposition 5.26. *L'intégrale*

$$\Gamma(s)=\int_0^\infty e^{-t}t^{s-1}dt$$

définit une fonction holomorphe pour $\Re s>0$ qui vérifie l'équation fonctionnelle

$$\Gamma(s+1)=s\Gamma(s).$$

Elle se prolonge en une fonction méromorphe dans $\mathbf{C}$ ayant un pôle simple en tous les entiers ≤ 0.

Démonstration. Il est facile de vérifier que l'intégrale converge et définit une fonction analytique dans le demi plan $\Re s>0$. En intégrant par parties on trouve

$$\Gamma(s)=\left[\frac{1}{s}e^{-s}+t^s\right]_0^\infty-\frac{1}{s}\int_0^\infty e^{-t}t^s dt=\frac{1}{s}\Gamma(s+1).$$

Cette équation fonctionnelle permet de prolonger la fonction par la formule

$$\Gamma(s) = \frac{\Gamma(s+n+1)}{s(s+1)\cdots(s+n)}.$$

Le membre de droite est bien défini pour $\Re s > -n-1$, celui de gauche seulement pour $\Re s > 0$. Pour $\Re s > 0$, les deux membres coïncident. En prenant $s \in \mathbf{C}$ quelconque et en choisissant $n > -\Re s - 1$, on définit $\Gamma(s)$ en prenant comme définition le membre de droite : il ne dépend pas de n et on obtient ainsi une fonction analytique dans $\mathbf{C} \setminus \{0,\ -1,\ -2\ldots\}$ ayant un pôle simple en $s = -n$ pour n entier ≥ 0 ; le résidu est $(-1)^n/n!$ (avec $0! = 1$, comme il se doit). □

Remarque. Comme $\Gamma(1) = 1$ on en déduit $\Gamma(n+1) = n!$.

On définit une fonction entière dans $\mathbf{C}$ par

$$\xi(s) = s(s-1)\pi^{-s/2}\Gamma(s/2)\zeta(s).$$

Le seul pôle de ζ est $s = 1$. De plus ζ s'annule aux entiers pairs strictement négatifs et ne s'annule pas aux entiers négatifs impairs. Les pôles de $\Gamma(s/2)$ sont tous les entiers pairs ≤ 0 et Γ ne s'annule pas en $s = 1$. C'est pourquoi la fonction ξ est entière (analytique dans $\mathbf{C}$). Sa valeur en $s = 0$ et en $s = 1$ est 1, ce qui revient à dire que l'on a $\Gamma(1/2) = \sqrt{\pi}$. En effet, en effectuant le changement de variables $t = x^2$ on trouve

$$\Gamma(1/2) = \int_0^\infty e^{-t}t^{-1/2}dt = 2\int_0^\infty e^{-x^2}dx.$$

Donc

$$\frac{1}{4}\Gamma(1/2)^2 = \int_0^\infty\int_0^\infty e^{-x^2-y^2}dxdy = \int_0^\infty\int_0^{\pi/2} e^{-r^2}rdrd\theta = \left[-\frac{1}{2}e^{-r^2}\right]_0^\infty \frac{\pi}{2} = \frac{\pi}{4}.$$

B. Riemann a aussi démontré :

Théorème 5.27 (Equation fonctionnelle de la fonction zêta de Riemann)**.** *La fonction ξ vérifie*

$$\xi(s) = \xi(1-s).$$

L'axe de symétrie est $\Re s = 1/2$, l'équation fonctionnelle permet de bien connaître la fonction ζ dans le demi plan $\Re s < 0$ grâce au produit infini qui converge dans $\Re s > 1$. Par exemple les seuls zéros de ζ dans ce demi plan $\Re s < 0$ sont les entiers négatifs pairs.

Le domaine $0 < \Re s < 1$ est la *bande critique* et la droite $\Re s = 1/2$ est la *droite critique*. C'est Riemann qui a montré l'importance des zéros non triviaux (c'est-à-dire dans la bande critique) de la fonction zêta pour l'étude des nombres premiers. Après Euler il a montré le lien entre la fonction zêta et la fonction π – cf. (5.1) en établissant la relation

$$\frac{1}{s}\log\zeta(s) = \int_0^s \frac{\pi(x)}{x^{s-1}}\frac{dx}{x}$$

pour $\Re s > 1$. Le *produit de Hadamard*, qui permet d'exprimer une fonction entière comme produit infini étendu à l'ensemble des zéros, s'écrit [6]

$$\zeta(s) = \frac{2^{s-1}\pi^s}{e^{((\gamma/2)+1)s}(s-1)\Gamma(1+(s/2))} \prod_{\varrho} \left(1 - \frac{s}{\varrho}\right) e^{s/\varrho}$$

où ϱ décrit les zéros de ζ dans la bande critique, et il a estimé le nombre de zéros dans un rectangle $[0,1] \times [0, iT]$ de cette bande : pour $t \to \infty$ il vaut

$$\frac{T}{2\pi} \log \frac{T}{2\pi} - \frac{T}{2\pi} + O(\log T).$$

On démontre le théorème 5.27 qui donne l'équation fonctionnelle de la fonction zêta de Riemann en utilisant la *Formule de Poisson* qui relie la série des valeurs aux entiers rationnels d'une fonction intégrable f sur $\mathbf{R}$ à la série des valeurs de sa transformée de Fourier

$$\widehat{f}(y) = \int_{-\infty}^{+\infty} f(x) e^{2i\pi xy} dx.$$

Si la fonction $x \mapsto \sum_{n\in\mathbf{Z}} f(x+n)$ est continue et à variations bornées sur $[0,1]$, alors

$$\sum_{n\in\mathbf{Z}} f(n) = \sum_{m\in\mathbf{Z}} \widehat{f}(m).$$

Cette formule de Poisson permet de montrer que la *série thêta*

$$\theta(u) = \sum_{n\in\mathbf{Z}} e^{-\pi u n^2}$$

satisfait l'équation fonctionnelle, pour $u \in \mathbf{R}_+^\times$:

$$\theta(1/u) = \sqrt{u}\theta(u).$$

On montre ensuite que la fonction ξ du théorème 5.27 satisfait, pour $\Re s > 1$,

$$\xi(s) = s(s-1) \int_0^\infty \frac{(\theta(u)-1)u^{s/2}}{2u} du.$$

Pour terminer cette section voici l'énoncé d'un des principaux problèmes ouverts en théorie des nombres.

Conjecture 5.28 (Hypothèse de Riemann)**.** *Les zéros complexes de ζ dans la bande critique sont tous sur la droite critique : si $s \in \mathbf{C}$ vérifie $0 < \Re s < 1$ et $\zeta(s) = 0$, alors $\Re s = 1/2$.*

On trouvera d'autres informations sur la fonction zêta de Riemann dans le texte de P. Cartier [Ca].

[6] Le produit infini sur ϱ est la limite, pour T tendant vers l'infini, du produit étendu à l'ensemble fini des ϱ de partie imaginaire $\leq T$.

5.3 Fonctions arithmétiques

5.3.1 Fonctions additives et multiplicatives

Une fonction arithmétique est une application de $\mathbf{N} \setminus \{0\} = \mathbf{N}_{>0}$ dans $\mathbf{C}$. Il revient au même de se donner une suite de nombres complexes $(f(n))_{n\geq 1}$: nous en avons donc déjà rencontré de nombreux exemples.

Une fonction arithmétique $f : \mathbf{N}_{>0} \to \mathbf{C}$ est dite *multiplicative* si $f(1) = 1$ et si, pour tout couple (m, n) d'entiers positifs premiers entre eux, on a

$$f(mn) = f(m)f(n).$$

Si cette relation est vraie pour tout couple (m, n) d'entiers positifs, on dit que la fonction est *complètement multiplicative.*

On dit aussi qu'une fonction arithmétique $g : \mathbf{N}_{>0} \to \mathbf{C}$ est *additive* si elle satisfait

$$g(mn) = g(m) + g(n) \quad \text{quand } \mathrm{pgcd}(m, n) = 1,$$

et qu'elle est *complètement additive* si $g(mn) = g(m) + g(n)$ pour tout couple $(m, n) \in \mathbf{N}_{>0}$.

Une fonction complètement multiplicative n'est autre que la donnée, pour chaque nombre premier p, d'un nombre complexe u_p. La valeur en un entier n de la fonction f complètement multiplicative vérifiant $f(p) = u_p$ est alors donnée par la décomposition en facteurs premiers de n :

$$f(p_1^{\alpha_1} \cdots p_s^{\alpha_s}) = u_{p_1}^{\alpha_1} \cdots u_{p_s}^{\alpha_s},$$

avec $f(1) = 1$.

De même l'unique fonction g complètement additive satisfaisant $g(p) = u_p$ pour p premier est donnée par

$$g(p_1^{\alpha_1} \cdots p_s^{\alpha_s}) = \alpha_1 u_{p_1} + \cdots + \alpha_s u_{p_s}.$$

Une fonction f multiplicative (resp. g additive) est déterminée par ses valeurs aux puissances de nombres premiers : si pour chaque entier de la forme p^m, avec p premier et m entier ≥ 1, on se donne un nombre complexe $v_{p,m}$, l'unique fonction multiplicative f (resp. additive g) prenant au point p^m la valeur $v_{p,m}$ (pour tout couple (p, m)) est définie par

$$f(p_1^{\alpha_1} \cdots p_s^{\alpha_s}) = v_{p_1,\alpha_1} \cdots v_{p_s,\alpha_s} \quad \big(\text{ resp. } \quad g(p_1^{\alpha_1} \cdots p_s^{\alpha_s}) = v_{p_1,\alpha_1} + \cdots + v_{p_s,\alpha_s} \big).$$

Le produit (resp. la somme) de fonctions multiplicatives ou complètement multiplicatives (resp. additives ou complètement additives) l'est encore.

Exemples (Fonctions complètement multiplicatives ou complètement additives)**.** Soient f et g deux fonctions arithmétiques reliées par $f = e^g$. Si g est complètement additive, alors f est complètement multiplicative. La réciproque est vraie si on suppose par exemple que g est à valeurs réelles. Noter que la fonction

$$g : n \longrightarrow v_p(n) \log 2 + 2i\pi$$

n'est pas additive alors que son exponentielle

$$f : n \longrightarrow 2^{v_p(n)}$$

est complètement multiplicative.
La fonction δ définie par

$$\delta(n) = \begin{cases} 1 & \text{si } n = 1, \\ 0 & \text{si } n \geq 2, \end{cases}$$

est complètement multiplicative.
Pour tout nombre complexe s la fonction f définie par $f(n) = n^s$ est complètement multiplicative. Pour $s = 0$ c'est la fonction arithmétique constante égale à 1, que l'on note $\mathbf{1}$, tandis que pour $s = 1$ c'est la fonction identité, que l'on note j. Pour $n \geq 1$ on a

$$\mathbf{1}(n) = 1 \quad \text{et} \quad j(n) = n.$$

Soit p un nombre premier et soit s un nombre complexe. La fonction $n \to p^{v_p(n)s}$ est complètement multiplicative et la fonction $n \to sv_p(n)$ est complètement additive.
La fonction

$$\Omega(n) = \sum_{p^m \| n} m,$$

qui compte le nombre de diviseurs de n avec multiplicités, est complètement additive ; la notation $p^m \| n$ signifie que m est la plus grande puissance de p qui divise n (ainsi $m = v_p(n)$), autrement dit p^m divise n et p^{m+1} ne divise pas n. La fonction Ω est la fonction complètement additive déterminée par

$$\Omega(p) = 1 \quad \text{pour } p \text{ premier.}$$

Si f est une fonction complètement multiplicative à valeurs > 0, pour tout $s \in \mathbf{C}$ la fonction f^s est aussi complètement multiplicative, et la fonction $\log f$ est complètement additive.
Si f est une fonction complètement additive et si s est un nombre complexe, la fonction $n \to sf(n)$ est complètement additive.

Exemples (Fonctions multiplicatives ou additives)**.** Évidemment toute fonction complètement multiplicative (resp. complètement additive) est multiplicative (resp. additive).
Soient f et g deux fonctions arithmétiques reliées par $f = e^g$. Si g est additive, alors f est multiplicative. La réciproque est vraie si on suppose par exemple que g est à valeurs réelles.
La fonction

$$\omega(n) = \sum_{p|n} 1$$

qui compte le nombre de diviseurs de n sans multiplicités est additive. Elles est déterminée par

$$\omega(p^m) = 1 \quad (p \text{ premier}, m \geq 1).$$

Le nombre de diviseurs de n, traditionnellement noté $\tau(n)$,

$$\tau(n) = \sum_{d|n} 1,$$

est une fonction additive, déterminée par

$$\tau(p^m) = m + 1 \quad (p \text{ premier}, m \geq 1).$$

Plus généralement pour $k \in \mathbf{C}$ on définit

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

Ainsi $\tau = \sigma_0$. On écrit aussi σ au lieu de σ_1. La fonction σ_k est la fonction additive déterminée par

$$\sigma_k(p^m) = 1 + p^k + \cdots + p^{mk} = \frac{p^{k(m+1)} - 1}{p^k - 1} \quad (p \text{ premier}, m \geq 1).$$

L'indicatrice d'Euler

$$\varphi(n) = \sum_{\substack{1 \leq k \leq n \\ \text{pgcd}(k,n)=1}} 1$$

est la fonction additive déterminée par

$$\varphi(p^m) = p^{m-1}(p-1) \quad (p \text{ premier}, m \geq 1).$$

La *fonction de Möbius* μ, définie par

$$\mu(n) = \begin{cases} (-1)^{\omega(n)} & \text{si } n \text{ est sans facteur carré,} \\ 0 & \text{sinon,} \end{cases}$$

est multiplicative, déterminée par

$$\mu(p^m) = \begin{cases} -1 & \text{si } m = 1, \\ 0 & \text{si } m \geq 2, \end{cases} \quad (p \text{ premier}, m \geq 1).$$

La *fonction de von Mangoldt* Λ (cf. § 5.1) n'est ni additive ni multiplicative.

5.3.2 Séries de Dirichlet formelles

À une fonction arithmétique f on associe une série de Dirichlet formelle

$$D(f;s) = \sum_{n=1}^{\infty} f(n) n^{-s} = f(1) + \frac{f(2)}{2^s} + \frac{f(3)}{3^s} + \cdots + \frac{f(n)}{n^s} + \cdots$$

La somme et le produit de deux séries de Dirichlet est une série de Dirichlet, l'unité étant la série constante $D(\delta;s) = 1$. Par exemple la série de Dirichlet associée à la fonction $\mathbf{1}$ est la série définissant la fonction zêta de Riemann. D'après le corollaire 5.19 la série de Dirichlet associée à la fonction de von Mangoldt Λ est $D(\Lambda;s) = -\zeta'(s)/\zeta(s)$.

On définit une loi multiplicative $\star$ sur l'ensemble des fonctions arithmétiques, le *produit de convolution de Dirichlet*, par la condition

$$D(f \star g; s) = D(f;s) D(g;s).$$

Autrement dit la fonction arithmétique $f \star g$ est définie par

$$f \star g(n) = \sum_{d|n} f(d) g(n/d) = \sum_{dd'=n} f(d) g(d').$$

On obtient ainsi une structure d'anneau unitaire commutatif sur l'ensemble des fonctions arithmétiques qui en fait un anneau, noté $\mathcal{A}$, isomorphe à l'anneau des séries de Dirichlet formelles. L'élément unité est δ.

Exemples. Voici un récapitulatif de quelques relations de convolution avec les relations associées en termes de séries de Dirichlet.

$$D(\mathbf{1};s)=\zeta(s), \qquad D(\delta;s)=1, \qquad D(j^k)=\zeta(s-k) \quad (k\in\mathbf{C}),$$

$$\begin{array}{ll} \mathbf{1}\star\mathbf{1}=\tau, & D(\tau;s)=\zeta(s)^2,\\ \mathbf{1}\star j=\sigma, & D(\sigma;s)=\zeta(s)\zeta(s-1),\\ \mathbf{1}\star j^k=\sigma_k, & D(\sigma_k;s)=\zeta(s)\zeta(s-k), \quad (k\in\mathbf{C})\\ \mathbf{1}\star\mu=\delta, & D(\mu;s)=1/\zeta(s),\\ j\star\mu=\varphi, & D(\varphi;s)=\zeta(s-1)/\zeta(s). \end{array}$$

La relation $\delta=1\star\mu$, qui s'écrit aussi

$$\sum_{d|n}\mu(d)=\begin{cases}1 & \text{si } n=1,\\ 0 & \text{si } n\geq 2,\end{cases}$$

signifie que la fonction de Möbius est l'inverse de la fonction $\mathbf{1}$ pour la convolution :

$$g=f\star\mathbf{1} \iff f=g\star\mu.$$

Autrement dit :

Corollaire 5.29 (Formule d'inversion de Möbius)**.** *Soient f et g deux fonctions arithmétiques. Les deux assertions suivantes sont équivalentes.*
(i) Pour tout entier $n\geq 1$, on a

$$g(n)=\sum_{d|n}f(d).$$

(ii) Pour tout entier $n\geq 1$, on a

$$f(n)=\sum_{d|n}\mu(n/d)g(d).$$

Par exemple la relation

$$\sum_{d|n}\varphi(d)=n \quad \text{ pour tout } n\geq 1$$

s'écrit $\varphi\star\mathbf{1}=j$, elle est équivalente à $\varphi=j\star\mu$ qui s'écrit

$$\varphi(n)=\sum_{d|n}\mu(n/d)d \quad \text{ pour tout } n\geq 1$$

Voici deux variantes de la formule d'inversion de Möbius.

Proposition 5.30 (Variante 1 de la formule d'inversion de Möbius)**.** *Soient F et G deux fonctions définies sur $[1,+\infty)$ à valeurs complexes. Les deux assertions suivantes sont équivalentes.*
(i) Pour tout nombre réel $x \geq 1$ on a

$$G(x) = \sum_{n \leq x} F(x/n).$$

(ii) Pour tout nombre réel $x \geq 1$ on a

$$F(x) = \sum_{n \leq x} \mu(n) G(x/n).$$

Comme exemple, en prenant la fonction constante $F(x) = 1$ pour tout x et $G(x) = [x]$, on en déduit

$$\sum_{n \leq x} \mu(n)[x/n] = 1$$

pour tout $x \geq 1$. D'après E. Landau (1909), des formes équivalentes du théorème 5.2 des nombres premiers sont

$$\lim_{n \to \infty} \sum_{n \leq x} \mu(n)/n = 0 \Longleftrightarrow \sum_{n \leq x} \frac{\Lambda(n)}{n} = \log x - \gamma + o(1) \Longleftrightarrow M(x) = o(x),$$

où γ est la constante d'Euler et M la fonction sommatoire de la fonction de Möbius

$$M(x) = \sum_{n \leq x} \mu(n).$$

(voir par exemple [T]).

Proposition 5.31 (Variante 2 de la formule d'inversion de Möbius)**.** *Soient G un groupe multiplicatif et f, g deux applications de $\mathbf{N}_{>0}$ dans G. Les deux assertions suivantes sont équivalentes.*
(i) Pour tout entier $n \geq 1$, on a

$$g(n) = \prod_{d|n} f(d).$$

(ii) Pour tout entier $n \geq 1$, on a

$$f(n) = \prod_{d|n} g(d)^{\mu(n/d)}.$$

Exemple. Prenons pour G le groupe multiplicatif $K(X)^\times$ où K est un corps. Le n-ième polynôme cyclotomique Φ_n a été défini par récurrence grâce à la formule

$$X^n - 1 = \prod_{d|n} \Phi_d(X).$$

Par conséquent

$$\Phi_n = \prod_{d|n} (X^n - 1)^{\mu(n/d)}.$$

Un élément $f \in \mathcal{A}$ est inversible si et seulement si $f(1) \neq 0$. En effet la solution g au système d'équations

$$\sum_{d|n} f(n/d)g(d) = \delta(n) \quad (n \geq 1)$$

existe si et seulement si $f(1) \neq 1$; dans ce cas elle est donnée par $g(1) = 1/f(1)$, et par récurrence (une fois qu'on connaît la valeur de g pour les entiers $< n$ qui divisent n)

$$g(n) = -f(1)^{-1} \sum_{\substack{d|n \\ d<n}} f(n/d)g(d) \quad (n > 1).$$

La démonstration du Théorème donne plus généralement (voir par exemple [T], § I.2.4, Th. 4) :

Proposition 5.32. *Un élément f de $\mathcal{A}^\times$ est une fonction multiplicative si et seulement si sa série de Dirichlet formelle $D(f, s)$ est développable en un produit Eulérien*

$$D(f; s) = \prod_p \left(1 + \sum_{m=1}^{\infty} f(p^m)p^{-ms}\right).$$

L'inverse g d'une fonction multiplicative f est déterminée par l'identité formelle

$$\left(1 + \sum_{m=1}^{\infty} g(p^m)p^{-ms}\right) \cdot \left(1 + \sum_{m=1}^{\infty} f(p^m)p^{-ms}\right) = 1.$$

On en déduit que les fonctions multiplicatives constituent un sous-groupe du groupe $\mathcal{A}^\times$ des éléments inversibles de l'anneau $\mathcal{A}$: *le produit de convolution de deux fonctions multiplicatives est une fonction multiplicative.*

Proposition 5.33. *La fonction de von Mangoldt Λ, que nous avons définie au § 5.1) est égale à $\mu \star \log$.*

Démonstration. Posons $L = \mu \star \log$. Pour $n \geq 1$ on a

$$L(n) = \sum_{d|n} \mu(d) \log(n/d) = -\sum_{d|n} \mu(d) \log d + \delta(n) \log n = -\sum_{d|n} \mu(d) \log d = -\mu \log \star \mathbf{1}.$$

Cela permet de vérifier, quand m et n sont des entiers positifs premiers entre eux,

$$L(mn) = \delta(n)L(m) + \delta(m)L(n).$$

Il reste à remarquer que la fonction Λ satisfait la même relation pour en déduire par récurrence qu'elle coïncide avec L. □

Exercice. Vérifier, pour $k \in \mathbf{C}$,

$$D(\sigma_k; s) = \sum_{n \geq 1} \frac{\sigma_k(n)}{n^s} = \zeta(s)\zeta(s-k) = \prod_p \left(1 - (p^k + 1)p^{-s} + p^{k-2s}\right)^{-1}.$$

5.3.3 Caractères de Dirichlet

Soit q un entier ≥ 2. Le groupe multiplicatif $(\mathbf{Z}/q\mathbf{Z})^\times$ des éléments inversibles de l'anneau $\mathbf{Z}/q\mathbf{Z}$ est d'ordre $\varphi(q)$. Un élément du dual de $(\mathbf{Z}/q\mathbf{Z})^\times$ définit une application de l'ensemble des entiers premiers avec q à valeurs dans $\mathbf{C}^\times$ qui vérifie

$$\chi(ab) = \chi(a)\chi(b) \quad \text{pour tout } (a,b) \in \mathbf{Z}^2 \text{ avec } (ab,q) = 1$$

et

$$\chi(a+q) = \chi(a) \quad \text{pour tout } a \in \mathbf{Z} \text{ avec } (a,q) = 1.$$

On prolonge χ en une application notée encore χ de $\mathbf{Z}$ dans $\mathbf{C}$ par $\chi(a) = 0$ si $(a,q) \neq 1$ et $\chi(0) = 0$.

On appelle *caractère de Dirichlet* (ou encore *caractère modulaire*) les applications $\mathbf{Z} \to \mathbf{C}$ ainsi obtenues. On notera D_q l'ensemble de celles qui proviennent de $(\mathbf{Z}/q\mathbf{Z})^\times$: ce sont les *caractères modulo* q. L'ensemble D_q a donc $\varphi(q)$ éléments. Pour $\chi \in D_q$ on a

$$\chi^{-1}(0) = \{a \in \mathbf{Z}\ ;\ (a,q) \neq 1\}.$$

Le *caractère principal modulo* q est l'application $\chi_1 = \mathbf{Z} \to \mathbf{C}^\times$ définie par

$$\chi_1(n) = \begin{cases} 0 & \text{si } (n,q) \neq 1, \\ 1 & \text{si } (n,q) = 1. \end{cases}$$

Pour $q = 1$ le quotient $\mathbf{Z}/1\mathbf{Z}$ n'est pas un anneau, mais on convient que $(\mathbf{Z}/1\mathbf{Z})^\times = \{1\}$. Avec cette convention $D_1 = \{\chi_1\}$ où

$$\chi_1(n) = \begin{cases} 0 & \text{si } n = 0, \\ 1 & \text{si } n \neq 0. \end{cases}$$

Exemple. Il y a deux caractères modulo 4, le caractère principal χ_1 modulo 4 et le caractère χ_2 défini par

$$\chi_2(n) = \begin{cases} 0 & \text{si } n \text{ est pair}, \\ 1 & \text{si } n \equiv 1 \pmod 4, \\ -1 & \text{si } n \equiv -1 \pmod 4. \end{cases}$$

Il y a quatre caractères modulo 8, le caractère principal χ_1, le caractère χ_2, le caractère χ_3 défini par

$$\chi_3(n) = \begin{cases} 0 & \text{si } n \text{ est pair}, \\ 1 & \text{si } n \equiv \pm 1 \pmod 8, \\ -1 & \text{si } n \equiv \pm 5 \pmod 8 \end{cases}$$

et le caractère $\chi_2\chi_3$.

Si p est un nombre premier impair le groupe $(\mathbf{Z}/p\mathbf{Z})^\times$ est cyclique d'ordre $p-1$, donc le groupe dual aussi. Soit a une racine primitive modulo p (la classe de a modulo p est un générateur de $(\mathbf{Z}/p\mathbf{Z})^\times$). Pour chacune des $p-1$ racines $p-1$-ièmes de l'unité ζ, on définit un caractère ψ_ζ modulo p par

$$\psi_\zeta(n) = \begin{cases} 0 & \text{si } p|n, \\ \zeta^u & \text{si } n \equiv a^u \pmod p. \end{cases}$$

Par exemple le choix $\zeta = -1$ (licite car p est impair) correspond à l'unique caractère de Dirichlet modulo p qui soit d'ordre 2 ; il est associé au symbole de Legendre :

$$\psi_{-1}(n) = \begin{cases} 0 & \text{si } p|n, \\ \left(\dfrac{n}{p}\right) & \text{si } (n,p) = 1. \end{cases}$$

Références

[Ca] Pierre Cartier, An introduction to Zeta functions, *From number theory to physics*, Springer-Verlag, Berlin, (1992), Chap. I p. 1–63.

[Co] Henri Cohen, A course in computatioonal algebraic number theory, Graduate Textes in Math. **138** (1993).

[T] G. Tenenbaum, *Introduction à la théorie analytique et probabiliste des nombres*, Institut Élie Cartan, **13**, Chap. I.2.