CHAPITRE 2

Le Théorème des Nombres Premiers

On a vu dans l'introduction la preuve d'Euclide de l'infinitude des nombres premiers (par l'absurde). Dans cette partie on va s'intéresser à quantifier cet énoncé : pour cela on définit la fonction de *comptage*

$$\pi(x) = |\{p \in \mathscr{P},\ p \leqslant x\}|.$$

Le théorème d'Euclide dit donc que $\pi(x) \to +\infty$ quand $x \to +\infty$ et la question qui se pose est

à quelle vitesse ?

On peut faire assez facilement des expériences de comptage des nombres premiers : il faut d'abord en dresser la liste jusqu'à une certaine limite. Une méthode simple et systématique est donnée par le *crible d'Érathostène* :

(1) On fait la liste de tous les entiers jusqu'à X.

(2) On biffe 1 (qui n'est pas premier)

(3) On garde 2 et on biffe tous ses autres multiples

(4) On garde 3 et on biffe tous les multiples de 3 qui n'ont pas déjà été éliminés

(5) ...

(6) le premier nombre non biffé à l'étape précédente est automatiquement premier, on le garde et on biffe ces multiples

(7) ...

Par exemple pour $X = 30$, on obtient

2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
2	3		5		7		9		11		13		15		17		19		21		23		25		27		29	
2	**3**		5		7				11		13				17		19				23		25				29	
2	**3**		**5**		7				11		13				17		19				23						29	
															...													
2	**3**		**5**		**7**				**11**		**13**				**17**		**19**				**23**						**29**	

Remarque 2.1. Dans l'exemple précédent, on remarque qu'on obtient la liste des nombres premiers $\leqslant X$ dès la troisième étape (quand on biffe les multiples de 5). Cela s'explique simplement par le critère suivant :

Un entier $n \geqslant 2$ est composé, si et seulement si il admet un diviseur d vérifiant $1 < d \leqslant \sqrt{n}$.

Preuve. En effet si n admet un divisieur $d > 1$ et $\leqslant \sqrt{n}$ alors $n > 1$ et $\sqrt{n} < n$ donc $d \neq 1, n$ et n est composé. Réciproquement, n un nombre composé et $d \neq 1, n$ un diviseur, le nombre n/d est également un diviseur de n (le *diviseur complémentaire*, $n = d.(n/d)$) qui vérifie $1 < n/d < n$. Posant alors

$$d' := \min(d, n/d),$$

on a

$$1 < d' \leqslant \sqrt{n}.$$

□

Ainsi, on obtient la liste de tous les nombres premiers $\leqslant 30$ dès qu'on a biffé les multiples de 5 parce que $7^2 > 49$.

Observons que l'espacement entre les nombres premiers consécutifs semble s'accroître ce qui suggère que l'ensemble des premier doit être de moins en moins dense. A la suite d'expériences de comptage beaucoup plus intensives, Gauss et Legendre, indépendament, ont formulé aux alentour de l'année 1795 une conjecture donnant une formula asymptotique pour $\pi(x)$: *la conjecture des nombres premiers*. Une centaine d'années plus tard (1896) cette conjecture fût démontrée par Hadamard et de la Vallée-Poussin et devint ainsi le *Théorème des Nombres Premiers* :

THÉORÈME (Théorème des Nombres Premiers (TNP)). *Quand* $x \to +\infty$,

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

Jacques Hadamard (1865-1963)

Charles-Jean de La Vallée Poussin (1866-1962)

Remarque 2.2. Dans les années 1830, Dirichlet avait formulé la conjecture des nombres premiers sous une forme un peu différente : introduisant la fonction suivante, appelée *logarithme integral*

$$\mathrm{Li}(x) := \int_2^{\infty} \frac{dt}{t},$$

il avait conjecturé que

$$\pi(x) \simeq \mathrm{Li}(x).$$

Comme $\mathrm{Li}(x) \simeq \frac{x}{\log x}$ (faire une intégration par parties) cette formulation de la conjecture est bien équivalente à l'originale ; cependant la formulation de Dirichlet est meilleure : comme on va le voir, la preuve du TNP fournit en fait le développement asymptotique suivant

$$\pi(x) = \mathrm{Li}(x) + O(x \exp(-c\sqrt{\log x}))$$

pour $c > 0$ une constante absolue. D'autre part, par intégration par parties (voir l'exercice **??**), on voit que

$$\mathrm{Li}(x) = \frac{x}{\log x} + \frac{x}{\log^2 x} + O(\frac{x}{\log^3 x})$$

et comme la fonction $x\exp(-c\sqrt{\log x})$ est négligeable devant la fonction $\frac{x}{\log^2 x}$ on a

$$\pi(x) - \frac{x}{\log x} \geqslant \frac{x}{\log^2 x}$$

pour x assez grand, alors que

$$\pi(x) - \mathrm{Li}(x) = o(\frac{x}{\log^2 x})$$

quand $x \to +\infty$. En fait la célèbre *Hypothèse de Riemann* (voir ci-après) prédit que

$$\pi(x) = \mathrm{Li}(x) + O(x^{1/2}\log^2 x).$$

1. La méthode d'Euler

Avec un peu de soin, la preuve d'Euclide peut être modifiée pour fournir une minoration explicite de $\pi(x)$; celle-ci est très mauvaise. C'est une autre preuve de l'infinitude des nombres premiers, due à Euler qui ouvrit la voie à la preuve du TNP et d'une certaine manière constitue le point de départ de la théorie analytique des nombres. La méthode d'Euler est de nature combinatoire et analytique et est basée sur la série "zeta" introduite par lui-même : pour $s > 1$, on consière la série convergente

$$\zeta(s) = \sum_{n\geqslant 1} \frac{1}{n^s}.$$

Par comparaison série-intégrale, on a

$$\zeta(s) = \sum_{n\geqslant 1} \frac{1}{n^s} \geqslant \int_1^{+\infty} \frac{dx}{x^s} = \frac{1}{s-1} \to +\infty, \ s \to 1^+.$$

L'observation fondamentale d'Euler est le fait que le Théorème Fondamental de l'Arithmétique permet d'exprimer $\zeta(s)$ en fonction des nombres premiers : pour $s > 1$ considérons pour chaque nombre premier p la série

$$\zeta_p(s) = 1 + \frac{1}{p^s} + \frac{1}{(p^2)^s} + \cdots + \frac{1}{(p^\alpha)^s} + \ldots$$

(ie. la série ζ "restreinte" aux puissances de p) c'est une série géométrique qui vaut

$$\zeta_p(s) = (1 - \frac{1}{p^s})^{-1}.$$

Ainsi, par unicité de la factorisation dans le Théorème Fondamental de l'Arithmétique,

$$\zeta_2(s)\zeta_3(s) = \sum_{\alpha_2,\alpha_3\geqslant 0}\sum \frac{1}{(2_2^\alpha 3_3^\alpha)^s}$$

est la série ζ "restreinte" aux entiers dont la décomposition en puissance de nombre premiers ne contient que des 2 et des 3 ; de même $\zeta_2(s)\zeta_3(s)\zeta_5(s)$ est la série ζ "restreinte" aux entiers dont la décomposition en puissance de nombre premiers ne contient que des 2 des 3 et et des 5...

Supposont que

$$\mathscr{P} = \{2, 3, 5, \cdots, p_{max}\}$$

est fini, poursuivant le raisonnement précédent, on obtient l'identité :

$$\zeta(s) = \sum_{n\geqslant 1} \frac{1}{n^s} = \prod_{p\in\mathscr{P}} \zeta_p(s) = \prod_{p\in\mathscr{P}} (1 - \frac{1}{p^s})^{-1} \tag{2.1}$$

Comme le produit $\prod_{p\in\mathscr{P}}(1-\frac{1}{p^s})^{-1}$ est fini et que pour tout p premier, $\zeta_p(s)$ est bien défini en $s=1$ (et vaut $1-1/p$), on voit que $\zeta(s)$ devrait avoir une limite finie quand $s\to 1^+$: une contradiction, donc $\mathscr{P}$ est infini.

En fait on montrera bientôt que, bien que $\mathscr{P}$ soit infini, l'identié (2.1) est valide pour $s>1$ (le produit infini converge et vaut $\zeta(s)$). La méthode d'Euler permet alors d'avoir des résultats quantitatifs précis sur le comptage des nombres premier : prenons le logarithme de l'identité (2.1) : pour $s>1$, on a

$$\log(\zeta(s)) = -\sum_p \log(1-\frac{1}{p^s}) = \sum_p \big(\frac{1}{p^s}+O(\frac{1}{p^{2s}})\big) = \sum_p \frac{1}{p^s} \ + \ O(1)$$

D'autre part, on a vu que

$$\log(\zeta(s)) \geqslant \log(\frac{1}{s-1}) = -\log(s-1).$$

Ainsi pour $s>1$,

$$\sum_p \frac{1}{p^s} \geqslant -\log(s-1)+O(1).$$

Faisant tendre s vers 1, on obtient donc (par convergence dominée) que

Théorème. *La série*

$$\sum_p \frac{1}{p}$$

est divergente.

2. La méthode de Chebychef

Nous commençerons par le resultat suivant dû a Chebycheff (~ 1850), qui n'utilise que des méthodes élémentaires et qui donne le bon ordre de grandeur pour la fonction $\pi(x)$:

Théorème 2.3. *Il existe des constantes $0<c<C$ telles que pour $x\geqslant 2$ on ait*

$$c\frac{x}{\log x} \leqslant \pi(x) \leqslant C\frac{x}{\log x}.$$

Preuve. Soit $n\geqslant 1$, considérons sa factorielle

$$n! = \prod_{1\leqslant k\leqslant n} k.$$

La méthode de Chebycheff est basée sur le fait que ce nombre $n!$ est divisible (et n'est divisible que) par tous les nombres premier $\leqslant n$. Commençons par rappeler la

Définition 2.4. *Pour $n\in\mathbb{Z}-\{0\}$ et p un nombre premier la valuation p-adique de n, $v_p(n)$ est le plus grand entier $\alpha\geqslant 0$ tel que p^α divise n : ie. $p^\alpha|n$ et $p^{\alpha+1}\not| n$. En particulier on a*

$$n = \prod_{p|n} p^{v_p(n)} = \prod_{p\in\mathscr{P}} p^{v_p(n)}.$$

Si $n=0$ on pose $v_p(0)=\infty$.

On a donc

$$n! = \prod_{p\leqslant n} p^{v_p(n!)}, \quad \text{de plus } v_p(n!)\geqslant 1 \text{ pour tout } p\leqslant n.$$

Ainsi en prenant le logarithme de cette expression on a

$$\log(n!) = \sum_{p \leqslant n} v_p(n!) \log(p).$$

On évalue les deux cotés de cette identité. Considérons la partie de gauche

$$\log(n!) = \sum_{k \leqslant n} \log k.$$

Cette dernière somme peut être évaluée en la comparant avec l' intégrale

$$\int_1^n \log t \, dt = n \log n - n + 1$$

(voir le chapitre suivant) et on trouve

$$\log(n!) = \sum_{k \leqslant n} \log k = n \log n - n + O(\log n). \tag{2.2}$$

Ainsi, on obtient que

$$\sum_{p \leqslant n} v_p(n!) \log(p) = n \log n - n + O(\log n).$$

Nous avons maintenant besoin d'évaluer la valuation $v_p(n!)$. Soit k un entier, la valuation $v_p(k)$ (le plus grand exposant α tel que p^α divise k) vaut

$$v_p(k) = \max(\alpha \geqslant 0, \ p^\alpha | k) = \sum_{\substack{\alpha \geqslant 1 \\ p^\alpha | k}} 1$$

et donc (intervertissant les sommations) on a

$$v_p(n!) = \sum_{1 \leqslant k \leqslant n} v_p(k) = \sum_{1 \leqslant k \leqslant n} \sum_{\substack{\alpha \geqslant 1 \\ p^\alpha | k}} 1 = \sum_{\alpha \geqslant 1} \sum_{\substack{1 \leqslant k \leqslant n \\ p^\alpha | k}} 1 = \sum_{\alpha \geqslant 1} [\frac{n}{p^\alpha}],$$

avec

$$x \mapsto [x] = \sum_{1 \leqslant k \leqslant x} 1 = x - \{x\}$$

désignant la fonction *partie entière* de x ($\{x\}$ désigne la *partie fractionnaire*) ; on a utilisé les identités

$$\sum_{\substack{1 \leqslant k \leqslant n \\ p^\alpha | k}} 1 = \sum_{1 \leqslant k' \leqslant n/p^\alpha} 1 = [\frac{n}{p^\alpha}].$$

On a donc

$$\sum_{p \leqslant n} \log p \sum_{\substack{\alpha \geqslant 1 \\ p^\alpha \leqslant n}} [\frac{n}{p^\alpha}] = n \log n - n + O(\log n). \tag{2.3}$$

Evaluons la somme

$$\sum_{\substack{\alpha \geqslant 1 \\ p^\alpha \leqslant n}} [\frac{n}{p^\alpha}];$$

comme $[x] \leqslant x$, cette somme est majorée par

$$\sum_{\substack{\alpha \geqslant 1 \\ p^\alpha \leqslant n}} [\frac{n}{p^\alpha}] \leqslant \sum_{\alpha \geqslant 1} \frac{n}{p^\alpha} = \frac{n}{p(1 - 1/p)} = \frac{n}{p}(1 + O(\frac{1}{p})) = \frac{n}{p} + O(\frac{n}{p^2})$$

On a donc

$$n\log n - n + O(\log n) \leqslant n \sum_{p\leqslant n} \log p(\frac{1}{p} + O(\frac{1}{p^2})) = n \sum_{p\leqslant n} \frac{\log p}{p} + O(n)$$

car

$$\sum_{p\leqslant n} \frac{\log p}{p^2} = O(1);$$

on a donc, divisant par n

$$\sum_{p\leqslant n} \frac{\log p}{p} \geqslant \log n + O(1)$$

ce qui montre encore que l'ensemble des nombres premiers est infini.

2.1. Le coefficient binomial. Cette approche ne permet cependant pas d'obtenir la fonction de comptage des nombres premiers : le problème est que le "poids" $v_p(n!)$ varie beaucoup quand p varie entre 2 et n. Pour y remédier, Chebycheff considère à la place de l'entier $n!$, le coefficient du binome $C_{2n}^n = (2n!)/(n!)^2$:

Par (2.2), on voit d'abord que

$$\log C_{2n}^n = (2n\log 2n - 2n + O(\log n)) - 2(n\log n - n + O(\log n)) = (\log 4)n + O(\log 2n).$$

Remarque 2.5. On peut obtenir cette formule asymptotique de manière plus élémentaire : on a

$$\sum_{k=0}^{2n} C_{2n}^k = (1+1)^{2n}$$

et on sait bien que parmi les $2n+1$ termes de cette somme, C_{2n}^n est le plus grand. Ainsi

$$\frac{(1+1)^{2n}}{2n+1} \leqslant C_{2n}^n \leqslant (1+1)^{2n}$$

donc prenant le log, on obtient

$$\log C_{2n}^n = 2n(\log 2) + O(\log n).$$

Remarquons que C_{2n}^n est divisible par tous les nombres premiers de l'intervalle $]n, 2n]$: on a donc

$$\log(C_{2n}^n) = \sum_{p\leqslant 2n} v_p(C_{2n}^n)\log p \geqslant \sum_{n<p\leqslant 2n} \log p. \tag{2.4}$$

Posant

$$\theta(x) := \sum_{p\leqslant x} \log p,$$

on obtient que pour tout $n \geqslant 2$

$$\theta(2n) - \theta(n) \leqslant (\log 2)2n.$$

Etant donné un nombre réel $x \geqslant 2$, il existe toujours un entier pair $2n$ tel que $0 \leqslant x - 2n \leqslant 2$; utilisant le fait que

$$0 \leqslant \theta(x) - \theta(2n) \leqslant 2\log(2x), 0 \leqslant \theta(x/2) - \theta(n) \leqslant 2 \leqslant x,$$

on voit que pour tout $x \geqslant 2$

$$\theta(x) - \theta(x/2) \leqslant (\log 2)x + O(\log x).$$

et utilisant cette inégalité avec $x, x/2, x/4, \ldots$ etc, ($O(\log x)$ fois) on en déduit que

$$\begin{aligned}\theta(x) &= \sum_{k\geqslant 0}\theta(x/2^k)-\theta(x/2^{k+1}) \leqslant \sum_{0\leqslant k\ll \log x}(\log 2)\frac{x}{2^k}\\ &\leqslant (2\log 2)x+O(\log^2 x).\end{aligned}$$

On en deduit facilement une majoration pour $\pi(x)$ avec le bon ordre de grandeur : on a

$$\pi(x)=\sum_{p\leqslant x}1=\sum_{p\leqslant x^{1/2}}1+\sum_{x^{1/2}<p\leqslant x}1,$$

le premier terme est majoré par $x^{1/2}$ alors que le second terme vérifie

$$\sum_{x^{1/2}<p\leqslant x}1\leqslant\frac{1}{\log(x^{1/2})}\sum_{x^{1/2}<p\leqslant x}\log p=\frac{2}{\log x}(\theta(x)-\theta(x/2))\leqslant 2(\log 4)\frac{x}{\log x}+O(\log x)$$

et donc

$$\pi(x)\leqslant 2(\log 4)\frac{x}{\log x}+O(x^{1/2}).$$

Remarque 2.6. Par un argument un peu plus élaboré (intégration par parties, voir le chapître suivant), on peut montrer que

$$\pi(x)\leqslant(\log 4)\frac{x}{\log x}(1+O(\frac{1}{\log x})),\ x\to+\infty.$$

2.2. Minoration. Pour obtenir une minoration, il nous faut être plus précis sur la valeur de $v_p(C_{2n}^n)$: on a

$$v_p(C_{2n}^n)=v_p(2n!)-2v_p(n!)=\sum_{\alpha\geqslant 1}[\frac{2n}{p^\alpha}]-2[\frac{n}{p^\alpha}]=\sum_{\alpha\geqslant 1}\varpi(\frac{n}{p^\alpha})$$

avec

$$\varpi(x):\ x\to[2x]-2[x]=2\{x\}-\{2x\}.$$

Cette fonction est periodique de période 1 et vaut

$$\varpi(x)=\begin{cases}0 & x\in[0,1/2[\\ 1 & x\in[1/2,1[.\end{cases}$$

En particulier, elle varie donc beaucoup moins que la fonction $x\mapsto[x]$. Observant que, pour $p\leqslant 2n$ le nombre de terme non nuls de la somme

$$\sum_{\alpha\geqslant 1}\varpi(\frac{n}{p^\alpha})$$

est borné par $\log 2n/\log p$ et comme $\varpi(n/p^\alpha)\leqslant 1$, on obtient la majoration

$$\log C_{2n}^n=(\log 4)n+O(\log n)=\sum_{p\leqslant 2n}\log p\sum_{\alpha\geqslant 1}\varpi(\frac{n}{p^\alpha})\leqslant\sum_{p\leqslant 2n}\log p\frac{\log 2n}{\log p}=(\log 2n)\pi(2n). \tag{2.5}$$

Ainsi, on obtient la minoration

$$(\log 2)\frac{2n}{\log 2n}+O(1)\leqslant\pi(2n)$$

et plus généralement, pour tout entier $x\geqslant 2$

$$(\log 2)\frac{x}{\log x}(1+O(\frac{1}{\log x}))\leqslant\pi(x).$$

On en déduit également une minoration pour la fonction $\theta(x)$:

$$\theta(x) = \sum_{p\leqslant x^{1/2}} \log p + \sum_{x^{1/2}<p\leqslant x} \log p \geqslant (\log x^{1/2})(\pi(x)-\pi(x^{1/2})+O(x^{1/2}\log x) = \frac{1}{2}\log x\pi(x)+O(x^{1/2}\log x)$$

et donc

$$\theta(x) \geqslant \frac{\log 2}{2} x(1+O(\frac{1}{\log x})) \tag{2.6}$$

On a donc montré l'existence de constantes $0<c<C$ telles que pour tout $x\geqslant 2$

$$cx \leqslant \theta(x) \leqslant Cx,\ c\frac{x}{\log x} \leqslant \pi(x) \leqslant C\frac{x}{\log x}. \tag{2.7}$$

□

Remarque 2.7. Avec un peu plus de soin, on peut montrer que les constances c et C peuvent être prises arbitrairement proches de $\log 2$ et $2\log 2$ respectivement au moins quand x est assez grand (cf. Exercice 2.8).

On déduit du théorème de Chebycheff l'estimation asymptotique suivante

Théorème (Mertens). *On a*

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

Preuve. Revenons à (2.3) : pour $n\geqslant 2$,

$$\sum_{p\leqslant n} \log p \sum_{1\leqslant\alpha,\ p^\alpha\leqslant n} [\frac{n}{p^\alpha}] = n\log n - n + O(\log n).$$

La contribution des $\alpha\geqslant 2$ au terme de gauche est bornée par

$$\sum_{p\leqslant n} \log p \sum_{\substack{2\leqslant\alpha,\\ p^\alpha\leqslant n}} [\frac{n}{p^\alpha}] \leqslant \sum_{p\leqslant n} \log p \sum_{2\leqslant\alpha} \frac{n}{p^\alpha} \ll n \sum_{p\leqslant n} \frac{\log p}{p^2} = O(n).$$

Considérant le reste et écrivant $[n/p] = n/p + O(1)$ on obtient

$$\sum_{p\leqslant n} \log p \frac{n}{p} + O(\sum_{p\leqslant n} \log p) = n\log n - n + O(\log n) + O(n).$$

et donc par la majoration de Chebycheff $\sum_{p\leqslant n}\log p = O(n)$, on trouve que

$$\sum_{p\leqslant n} \log p \frac{n}{p} = n\log n + O(n).$$

On conclut en divisant cette dernière égalité par n. □

3. La méthode de Nair

En 19 ? ?, a donné une version trés élégante de la minoration de $\pi(x)$ dans la méthode de Chebycheff : Soit $n\geqslant 1$ un entier, on note d_n le ppcm des entiers $1,2,\ldots,n$:

$$d_n = [1,2,\ldots,n-1,n].$$

Soit I_n, l'integrale

$$I_n = \int_0^1 x^n(1-x)^n dx.$$

Développant cette integrale, on voit que c'est une somme de nombres rationnels dont les dénominateurs sont des entiers compris entre 1 et $2n+1$, ainsi $I_n.d_{2n+1}$ est un entier non-nul (car I_n, intégrale d'une fonction positive non-nulle, est non-nulle), ainsi $I_n.d_{2n+1} \geqslant 1$ et donc

$$I_n^{-1} \leqslant d_{2n+1}.$$

D'autre part comme $0 \leqslant x(1-x) \leqslant 1/4$ pour $x \in [0,1]$ on a $I_n \leqslant 4^{-n}$ soit $d_{2n+1} \geqslant 4^n$. On a

$$\log d_{2n+1} = \sum_{p \leqslant 2n+1} \log p \, v_p(d_{2n+1})$$

avec

$$v_p(d_{2n+1}) = \max_{m=1\ldots 2n+1} v_p(m) = \max_{m=1\ldots 2n+1} \sum_{k \geqslant 1,\ p^k | m} 1 = \sum_{k \geqslant 1,\ p^k \leqslant 2n+1} 1 = [\frac{\log 2n+1}{\log p}].$$

Ainsi

$$\log(d_{2n+1}) = \psi(2n+1)$$

avec

$$\psi(x) = \sum_{p \leqslant x} \log p [\frac{\log x}{\log p}].$$

On a donc, pour tout $n \geqslant 1$,

$$\psi(2n+1) \geqslant \log(4^n) = (\log 2).2n$$

et comme

$$\psi(2n+1) \leqslant \sum_{p \leqslant 2n+1} \log p \frac{\log 2n+1}{\log p} = \pi(2n+1)\log(2n+1),$$

on a pour tout $x \geqslant 2$,

$$\pi(2n+1) \geqslant \log 2 \frac{2n}{\log(2n+1)}$$

dont on déduit que pour tout $x \geqslant 2$

$$\pi(x) \geqslant \log 2 \frac{x}{\log x}(1 + O(\frac{1}{\log x})).$$

Exercice(s) 2.8. En remplaçant $x^{1/2}$ part une autre valeur dans les découpages

$$\pi(x) = \sum_{p \leqslant x^{1/2}} 1 + \sum_{x^{1/2} < p \leqslant x} 1,\ \theta(x) = \sum_{p \leqslant x^{1/2}} \log p + \sum_{x^{1/2} < p \leqslant x} \log p$$

montrer que

$$\log 2 + o(1) \leqslant \frac{\pi(x)}{x/\log x},\ \frac{\theta(x)}{x} \leqslant 2\log 2 + o(1),\ x \to +\infty.$$

CHAPITRE 3

Sommation de fonctions arithmétiques

Dans ce chapitre, on va donner quelques méthodes de base pour évaluer des sommes sur les entiers. Les termes de ces sommes sont appellées fonctions arithmétiques.

Définition 3.1. *Une fonction arithmétique est une fonction à valeurs complexes de l'ensemble des entiers positifs, $f : \mathbb{N}_{\geqslant 1} \to \mathbb{C}$. On note $\mathscr{A}$ le* **C***-espace vectoriel des fonctions arithmétiques.*

Exemple(s) 3.2. (1) La fonction constante égale à 1

$$1 : n \to 1,$$

(2) La "fonction de Dirac" en 1

$$\delta : n \mapsto \begin{cases} 1, & n = 1 \\ 0 & n \neq 1 \end{cases},$$

(3) La fonction caractéristique de l'ensemble des nombres premiers,

$$1_{\mathscr{P}} : n \mapsto \begin{cases} 1, & n = p \in \mathscr{P} \\ 0 & n \notin \mathscr{P} \end{cases},$$

(4) Cette même fonction pondérée par log,

$$\log.1_{\mathscr{P}} : n \mapsto \log(n) 1_{\mathscr{P}}(n);$$

(5) La fonction de *von Mangolt*,

$$\Lambda : n \mapsto \begin{cases} \log p, & n = p^{\alpha},\ \alpha \geqslant 1 \\ 0 & n \neq p^{\alpha} \end{cases}$$

Bien que d'apparence artificielle, cette dernière fonction apparait naturellement dans l'étude des nombres premiers et joue un rôle fondamental.

Définition 3.3. *Soit f une fonction arithmétique, la* fonction sommatoire *de f est la fonction définie sur $\mathbb{R}_{\geqslant 0}$ par*

$$x \mapsto M_f(x) = \sum_{1 \leqslant n \leqslant x} f(n).$$

C'est une fonction constante par morceaux et dans ce chapitre, on va donner des mt́hodes pour étudier la question suivante :

Problème. Etant donné une fonction arithmétique f, déterminer le comportement de $M_f(x)$ quand $x \to +\infty$.

Exemple(s) 3.4. (1) $M_1(x) = \sum_{1 \leqslant n \leqslant x} = [x] = x + O(1)$.

(2) $\pi(x) = M_{1_{\mathscr{P}}}(x) = \sum_{p \leqslant x} 1$.

(3) $\theta(x) := M_{1_{\mathscr{P}}.\log}(x) = \sum_{p\leqslant x}\log p$,

(4) $\psi(x) := M_\Lambda(x) = \sum_{1<p^\alpha\leqslant x}\log p$.

En guide d'exemple, on va comparer $\theta(x)$ et $\psi(x)$. Observons d'abord que

$$\theta(x)\leqslant\psi(x);$$

plus précisement, on a

$$\psi(x)=\theta(x)+\sum_{\substack{p^\alpha\leqslant x\\ \alpha\geqslant 2}}\log p.$$

On a

$$\begin{aligned}\sum_{\substack{p^\alpha\leqslant x\\ \alpha\geqslant 2}}\log p &= \sum_{p\leqslant\sqrt{x}}\log p\sum_{\substack{p^\alpha\leqslant x\\ \alpha\geqslant 2}}1\leqslant\sum_{p\leqslant x^{1/2}}\log p[\frac{\log x}{\log p}]\\ &\leqslant\log x\sum_{p\leqslant x^{1/2}}1\ll x^{1/2}\log x\end{aligned}$$

Ainsi

$$\psi(x)=\theta(x)+O(x^{1/2}\log x)$$

On l'a vu que par la méthode de Chebycheff, $\theta(x)\gg x$ (cf. (2.6)) et on en déduit que

$$\Psi(x)\sim\theta(x). \tag{3.1}$$

1. Approximation par une intégrale, Intégration par parties

Si f est la restriction à $\mathbb{N}_{>0}$ d'une fonction continue sur $\mathbb{R}$, $M_f(x)$ est souvent bien approximée par $\int_1^x f(t)dt$. Par exemple si f est *monotone*, on a

Théorème 3.5 (comparaison séries/integrales)**.**

$$M_f(x)=\int_1^x f(t)dt+O(|f(1)|+|f(x)|). \tag{3.2}$$

Preuve. Supposons f croissante ; le résultat se déduit par sommation de l'inégalité pour $n\geqslant 2$:

$$\int_{n-1}^n f(t)dt\leqslant f(n)\leqslant\int_n^{n+1}f(t)dt.$$

□

Par exemple, on a

$$M_{\log}(x)=\sum_{n\leqslant x}\log(n)=\int_1^x\log(t)dt+O(\log(x))=x\log x-x+O(\log x). \tag{3.3}$$

Le résultat suivant permet d'évaluer la fonction sommatoire d'un produit d'une fonction arithmetique quelconque par une fonction "lisse" :

Théorème 3.6 (Integration par partie)**.** *Soit g une fonction arithmétique ; soient $a<b\in\mathbb{R}^+$ et $f:[a,b]\to\mathbf{C}$ une fonction de classe C^1. On a*

$$\begin{aligned}M_{fg}(b)-M_{fg}(a)=\sum_{a<n\leqslant b}f(n)g(n)&=[f(t)M_g(t)]_{t=a}^{t=b}-\int_a^b M_g(t)f'(t)dt\\ &=f(b)M_g(b)-f(a)M_g(a)-\int_a^b f'(t)M_g(t)dt\end{aligned}$$

Preuve. Supposons d'abord que $b = a+1 = n+1 \in \mathbb{N}_{>0}$:

$$[M_g(x)f(x)]_{x=a}^{x=b} - \int_a^b M_g(x)g'(x)dx = M_g(n+1)f(n+1) - M_g(n).f(n) - M_g(n)(f(n+1)-f(n))$$
$$= f(n+1).g(n+1) = M_{fg}(n+1) - M_{fg}(n)$$

par additivité on étend la formule à $a \leqslant b \in N_{>0}$. puis on passe aux a, b réels généraux □

Remarque 3.7. On notera l'analogie entre cette formule et la formule d'integration classique : si f est C^1 et g est continue, on a

$$\int_a^b f(t)g(t)dt = [f(t)G(t)]_a^b - \int_a^b f'(t)G(t)dt$$

où

$$G(x) = \int_1^x g(t)dt$$

est une primitive de g.

Exemple(s) 3.8. On a

$$\begin{aligned}\theta(x) = \sum_{p\leqslant x} \log(p) &= \sum_{2\leqslant n\leqslant x} \log(n)1_{\mathscr{P}}(n)\\ &= \pi(x)\log(x) - \log(2) - \int_2^x \pi(t)\frac{dt}{t}\\ &= \pi(x)\log(x) + O(1) + O(\int_2^x \frac{dt}{\log(t)})\\ &= \pi(x)\log(x) + O(\frac{x}{\log x})\end{aligned}$$

l'avant dernière inégalité résultant du théorème de Chebychef. En particulier comme $\pi(x) \gg x/\log x$ on voit que

$$\theta(x) = \pi(x)\log(x)(1+o(1)).$$

Ainsi par (3.1) on a les équivalence suivantes concernant le TNP :

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

C'est en fait la dernière équivalence que Hadamard-De la Vallée-Poussin ont démontrée dans leur preuve du TNP.

Considérant la fonction arithmétique constante égale à $g = 1$ ($M_1(x) = [x]$), on déduit du lemme d'intégration par parties la formule plus précise suivante liant séries et integrales :

Corollaire 3.9 (Formule d'Euler Mac-Laurin)**.** *Soit f une fonction de classe C^1 sur $\mathbb{R}_{>0}$, et soit*

$$\psi_1(x) := x - [x] - 1/2 = \{x\} - 1/2;$$

on a pour $x > 1$

$$M_f(x) = \int_1^x f(t)dt + \int_1^x \psi_1(t)f'(t)dt + \psi_1(1)f(1) - \psi_1(x)f(x)$$

en particulier

$$|M_f(x) - \int_1^x f(t)dt| \leqslant \int_1^x |f'(t)|dt + |f(1)| + |f(x)|.$$

Remarque 3.10. On a $\psi_1(x) = B_1(\{x\})$ où $B_1(x) = x - 1/2$. Ce polynôme est appellé *premier polynôme de Bernoulli.*

Preuve. Exercice □

Remarque 3.11. L'intéret dans cette formule est que la fonction g n'est pas nécéssairement monotone.

Exercice(s) 3.12. Montrer que

$$M_{\log}(x) = \sum_{n \leqslant x} \log n = x \log x - x + c + O(x^{-1})$$

où c est une certaine constante.

2. Convolution de Dirichlet

La convolution de Dirichlet est une loi de composition sur l'ensemble des fonctions arithmétiques qui rend compte de la structure multiplicative de l'ensemble des entiers.

Soient $f, g \in \mathscr{A}$, on définit $f * g \in \mathscr{A}$ en posant

$$f * g(n) = \sum_{ab=n} f(a)g(b) = \sum_{d|n} f(d)g(n/d).$$

Proposition 3.13. *$(\mathscr{A}, +, *)$ a une structure de $\mathbf{C}$-algèbre commutative, associative, d'élément neutre la fonction δ_1. L'ensemble des éléments inversibles de l'algèbre $\mathscr{A}$, est*

$$\mathscr{A}^\times = \{f \in \mathscr{A},\ f(1) \neq 0\}.$$

Pour $f \in \mathscr{A}^\times$, on note $f^{(-1)}$ son inverse pour la convolution de Dirichlet.

Preuve. On ne vérifiera que certains points, le reste est laissé en exercices :

– Commutativité

$$f * g(n) = \sum_{ab=n} f(a)g(b) = \sum_{ab=n} g(a)f(b) = g * f(n)$$

– Elément neutre :

$$f * \delta_1(n) = \sum_{d|n} f(n/d)\delta_1(d) = f(n/1) = f(n)$$

donc δ_1 est bien l'élément neutre.

– Unités : Si f est inversible d'inverse f^{-1} alors $f * f^{-1}(1) = \delta_1(1) = 1 = f(1)f^{-1}(1)$ donc $f(1) \neq 0$. Soit f t.q. $f(1) \neq 0$ on cherche $g \in \mathscr{A}$ qui vérifie $f * g = \delta_1$, en particulier $f * g(1) = f(1)g(1) = 1$ donc $g(1) = 1/f(1)$. Pour tout $n > 1$

$$f * g(n) = \delta_1(n) = 0 = \sum_{d|n} f(d)g(n/d) = g(n)f(1) + \sum_{d|n, d>1} f(d)g(n/d)$$

donc

$$g(n) = -\frac{1}{f(1)} \sum_{d|n, d>1} f(d)g(n/d)$$

comme $n/d < n$ si $d > 1$, $g(n)$ est determiné par les valeurs de g aux entiers $\leqslant n/2$, on définit g par récurrence.

□

NOTATION. *Si f est une fonction arithmétique et $k \in \mathbb{N}$, on notera la convolution itérée k fois de f sous la forme*

$$f^{(*k)} = f * f * \cdots * f(\ k \text{ fois}),$$

et si f est inversible on étant cette notation aux entiers relatifs de manière évidente : ie.

$$f^{(*-k)} = (f^{(-1)})^{*k}$$

2.1. Exemples.

(1) $1 * 1(n) = \sum_{d|n} 1 =: d(n)$ est le nombre de diviseurs de n.

(2) $1 * 1 * 1(n) = \sum_{abc=n} 1 =: d_3(n)$ est le nombre de représentations de n comme produit de trois entiers et plus généralement

$$d_k(n) := 1^{(*k)}(n) = 1 * \cdots * 1(n) = \sum_{d_1 \ldots d_k = n} 1$$

est le nombre de représentation de n comme produit de k entiers.

(3) On a

$$\log = \Lambda * 1,\ \log(n) = \sum_{d|n} \Lambda(d).$$

En effet si $n = \prod_p p^{\alpha_p}$

$$\log(n) = \log(\prod_p p^{\alpha_p}) = \sum_p \alpha_p \log(p) =$$

$$\sum_p \sum_{1 \leqslant \alpha \leqslant \alpha_p} \log(p) = \sum_{p^\alpha | n} \log(p) = \sum_{d|n} \Lambda(d).$$

2.2. Formule d'inversion de Moebius. La fonction de *Moebius* est par définition l'inverse de la fonction constante 1 :

$$\mu := 1^{(-1)},\ \mu(1) = 1,\ \mu(n) = -\sum_{\substack{d|n \\ d<n}} \mu(d).$$

Dans la section suivante on va montrer que

(1) $\mu(n) = 0$ si n est divisible par un carré $\neq 1$ (ie. il existe p premier t.q. $p^2|n$).

(2) $\mu(n) = (-1)^r$ si n est sans facteurs carrés et à r facteurs premiers : $n = p_1 p_2 \ldots p_r$ avec p_i premiers.

Théorème 3.14 (Formule d'inversion de Moebius)**.** *Soient $f, g \in \mathscr{A}$, les identités suivantes sont équivalentes*

(1) *Pour tout n, $f(n) = \sum_{d|n} g(d)$.*

(2) *Pour tout n, $g(n) = \sum_{d|n} \mu(d) f(n/d)$.*

Preuve. La première identité est équivalente à $f = g * 1$ et la deuxième à $g = f * \mu$ et il est clair que

$$f = g * 1 \Longleftrightarrow f * \mu = g * 1 * \mu \Longleftrightarrow f * \mu = g * (1 * \mu) \Longleftrightarrow f * \mu = g.$$

□

Ainsi on a

$$\Lambda(n) = \sum_{d|n} \mu(d) \log(n/d) = \sum_{d|n} \mu(d) \log(n) - \sum_{d|n} \mu(d) \log(d) = -\sum_{d|n} \mu(d) \log(d).$$

2.3. Exemple : la fonction d'Euler. La fonction φ d'Euler. Par définition

$$\varphi(n) = |(\mathbb{Z}/n\mathbb{Z})^\times|,$$

c'est à dire que $\varphi(n)$ est égal
- au nombre de générateurs du groupe cyclique $\mathbb{Z}/n\mathbb{Z}$.
- au nombre d'éléments de $\mathbb{Z}/n\mathbb{Z}$ d'ordre n exactement.
- au nombre d'entiers $0 \leqslant a \leqslant n-1$ premiers à n.

Dans tout groupe fini G, on a la partition

$$G = \bigsqcup_{d||G|} G_d$$

où G_d est l'ensemble des éléments d'ordre d exactement. Dans un groupe *cyclique* tous les éléments d' ordre donné d engendrent le même groupe cyclique (donc $\simeq \mathbb{Z}/d\mathbb{Z}$) ; on a donc pour $d|n$

$$|(\mathbb{Z}/n\mathbb{Z})_d| = \varphi(d) \ \ et \ \ n = \sum_{d|n} |(\mathbb{Z}/n\mathbb{Z})_d| = \sum_{d|n} \varphi(d) = (1 * \varphi)(n).$$

Ainsi on a les identités de fonctions arithmétiques

$$\mathrm{Id} = 1 * \varphi, \ \ \varphi = \mathrm{Id} * \mu = \sum_{d|n} d\mu(n/d)$$

3. Application au comptage des nombres premiers

Théorème 3.15 (Mertens)**.** *On a*

$$\sum_{n\leqslant x} \frac{\Lambda(n)}{n} = \log(x) + O(1), \ \ \sum_{p\leqslant x} \frac{\log(p)}{p} = \log(x) + O(1) \tag{3.4}$$

$$\sum_{p\leqslant x} \frac{1}{p} = \log\log(x) + O(1). \tag{3.5}$$

Preuve. On a

$$\sum_{\substack{p^\alpha\leqslant x\\ \alpha\geqslant 2}} \frac{\log p}{p^\alpha} = O(1) \text{ et comme } \sum_{n\leqslant x} \frac{\Lambda(n)}{n} = \sum_{p\leqslant x} \frac{\log p}{p} + \sum_{\substack{p^\alpha\leqslant x\\ \alpha\geqslant 2}} \frac{\log p}{p^\alpha},$$

les deux égalités de (3.4) sont équivalentes. La troisième égalité (3.5) résulte de (3.4) par une intégration par parties.

Pour montrer la première partie de (3.4), on évalue de deux manières la somme

$$M_{\log}(x) = \sum_{n\leqslant x} \log(n).$$

D'une part

$$\sum_{n\leqslant x} \log(n) = x\log x + O(x).$$

D'autre part $\log = \Lambda * 1$ et

$$\begin{aligned}\sum_{n\leqslant x} \log(n) &= \sum_{n\leqslant x}\sum_{d|n} \Lambda(d) = \sum_{d\leqslant x} \Lambda(d) \sum_{m\leqslant x/d} 1\\ &= \sum_{d\leqslant x} \Lambda(d)[\frac{x}{d}] = \sum_{d\leqslant x} \Lambda(d)\frac{x}{d} + O(\sum_{d\leqslant x} \Lambda(d))\end{aligned}$$

(on a utilisé que $[x] = x + O(1)$). Par le théorème de Chebycheff

$$\sum_{d\leqslant x} \Lambda(d) = \sum_{p\leqslant x} \log p + \sum_{p\leqslant x^{1/2},}\sum_{p^\alpha\leqslant x} \log p = O(x) + O(x^{1/2}\log x) = O(x)$$

et donc

$$x\log x + O(x) = \sum_{n\leqslant x} \log(n) = x\sum_{d\leqslant x} \frac{\Lambda(d)}{d} + O(x)$$

ce qui donne le résultat en divisant les deux termes par x.

□

4. Fonctions multiplicatives

Définition 3.16. *Une fonction arithmétique f non nulle est multiplicative (resp. complètement multiplicative) si et seulement si elle vérifie :*

- *pour tous $m, n \geqslant 1$ premiers entre eux on a $f(mn) = f(m)f(n)$ (resp. pour tous $m, n \geqslant 1$, $f(mn) = f(m)f(n)$.)*

En particulier, une fonction multiplicative vérifie $f(1) = 1$ et elle est déterminée entièrement par ses valeurs aux puissances de nombres premiers (resp. par ses valeurs aux nombres premiers) : si $n = \prod_{p^{\alpha_p}\|n} p^{\alpha_p}$, on a

$$f(n) = f(\prod_{p^{\alpha_p}\|n} p^{\alpha_p}) = \prod_{p^{\alpha_p}\|n} f(p^{\alpha_p}) \ (resp.\ f(n) = f(\prod_{p^{\alpha_p}\|n} p^{\alpha_p}) = \prod_{p^{\alpha_p}\|n} f(p)^{\alpha_p}.)$$

Proposition 3.17. *Si f et g sont multiplicatives, alors $f * g$ et $f^{(-1)}$ sont multiplicatives.*

Preuve. Si $(m, n) = 1$ alors l'ensemble des diviseurs de mn, $\{d \geqslant 1,\ d|mn\}$ est en bijection avec l'ensemble $\{(d_1, d_2),\ d_1|m,\ d_2|n\}$ des paires de diviseurs de m et n, la bijection est donnée par les deux application réciproques l'une de l'autre

$$d \mapsto ((d, m), (d, n)),\ (d_1, d_2) \mapsto d_1 d_2.$$

etant donné deux fonction multiplicatives, f, g et m, n premiers entre eux on a

$$\begin{aligned} f * g(mn) &= \sum_{d|mn} f(d)g(\frac{mn}{d}) = \sum_{d_1|m,d_2|n}\sum f(d_1d_2)g(\frac{m}{d_1}\frac{n}{d_2}) \\ &= \sum_{d_1|m,d_2|n}\sum f(d_1)f(d_2)g(\frac{m}{d_1})g(\frac{n}{d_2}) = (\sum_{d_1|m} f(d_1)g(\frac{m}{d_1}))(\sum_{d_2|n} f(d_2)g(\frac{n}{d_2})). \end{aligned}$$

De même si $g = f^{(-1)}$, comme $f(1) = 1$, on a pour $m, n > 1$

$$\begin{aligned} g(mn) = f(1)g(mn) &= -\sum_{\substack{d|mn \\ d>1}} f(d)g(\frac{mn}{d}) = -\sum_{\substack{d_1|m,d_2|n \\ d_1d_2>1}}\sum f(d_1)f(d_2)g(\frac{m}{d_1})g(\frac{n}{d_2}) \\ &= -f * g(m)f * g(n) + f(1)g(m)f(1)g(n) = g(m)g(n) \end{aligned}$$

car $f * g(m) = f * g(n) = 0$.

□

Remarque 3.18. Par contre si f est totalement multiplicative, $f^{(-1)}$ ne l'est pas nécéssairement (eg. 1 et μ).

4.1. Exemples. Comme les fonction 1 et Id sont multiplicatives, $\mu = 1^{(-1)}$, ainsi que $d = 1 * 1$, $d_k = d_{k-1} * 1$ ou $\varphi = \mathrm{Id} * \mu$ le sont. Il suffit donc de calculer ces fonctions sur les puissances de nombres premiers : pour $\alpha \geqslant 0$, l'ensemble des diviseurs de p^α est de la forme $\{p^\beta,\ 0 \leqslant \beta \leqslant \alpha\}$. On trouve donc

$$d(p^\alpha) = |\{0 \leqslant \beta \leqslant \alpha\}| = \alpha + 1,$$

et plus généralement

$$d_k(p^\alpha) = |\{(\beta_1, \cdots, \beta_k) \in \mathbb{N}^k,\ \beta_1 + \cdots + \beta_k = \alpha\}| = C_{\alpha+1}^{k-1}.$$

La relation $\mu * 1 = \delta$, donne pour $\alpha \geqslant 1$

$$\mu(1) = 1,\ \sum_{\beta \leqslant \alpha} \mu(p^\beta) = 0$$

dont on déduit

$$\mu(1) = 1,\ \mu(p) = -1,\ \mu(p^\alpha) = 0\ \alpha \geqslant 2.$$

Utilisant l'égalité $\varphi = \mathrm{Id} * \mu$, on obtient alors

$$\varphi(1) = 1,\ \varphi(p^\alpha) = p^\alpha - p^\alpha - 1 = p^\alpha(1 - \frac{1}{p})$$

Ainsi pour $n = \prod_{p^\alpha \| n} p^\alpha$, on obtient

$$d(n) = \prod_{p^\alpha \| n} (\alpha + 1),\ \mu(n) = \prod_{p^\alpha \| n} \mu(p^\alpha),\ \varphi(n) = \prod_{p^\alpha \| n} (p^\alpha - p^{\alpha-1}) = n \prod_{p|n} (1 - \frac{1}{p}).$$

5. Fonctions arithmétiques : Formulaire RAPPEL

f			L(s)
e	$e(n) = \delta_{n=1}$		1
1	$1(n) = 1$		$\zeta(s) = \prod_p (1 - \frac{1}{p^s})^{-1}$
μ	$\mu(p_1 \dots p_r) = (-1)^r,\ \mu(a^2 b) = 0$	$\mu = 1^{(-1)},\ \mu * 1 = e$	$\frac{1}{\zeta(s)} = \prod_p (1 - \frac{1}{p^s})$
log	$\log(n)$		$-\zeta'(s)$
Λ	$\Lambda(n) = \begin{cases} \log p\ si\ n = p^\alpha \\ 0\ sinon \end{cases}$	$\log = 1 * \Lambda,\ \Lambda = \mu * \log$	$-\frac{\zeta'}{\zeta}(s)$
φ	$\varphi(n) = n \prod_{p|n} (1 - \frac{1}{p})$	$\varphi = Id * \mu$	$\frac{\zeta(s+1)}{\zeta(s)}$
d	$d(n) = \lvert\{d \geqslant 1,\ d \mid n\}\rvert$	$d = 1 * 1$	$\zeta^2(s)$

6. Exercices

Exercice(s) 3.19.

(1) Montrer que le TNP equivaut a $p_n \sim n \log n$ où p_n est le n-ième nombre premier.

(2) Donner un équivalent de la somme $\sum_{p \leqslant x} p$ (on admettra le TNP).

Exercice(s) 3.20. Montrer que

$$\sum_{n \leqslant x} \log(n) = x \log x - x + O(\log x),$$

$$TNP \Longleftrightarrow \theta(x) = x(1 + o(1)) \Longleftrightarrow \psi(x) = x(1 + o(1)).$$

Exercice(s) 3.21. Montrer que

$$\sum_{n\leqslant x}\tau(n)=x\log x+O(x)$$

puis que pour $k\geqslant 3$

$$\sum_{n\leqslant x}\tau_k(n)=x\log^{k-1}x+O(x\log^{k-2}x).$$

Exercice(s) 3.22. Montrer que $d=1*1$ et $\mu=1^{(-1))}$ sont multiplicatives et que

$$d(p^\alpha)=\alpha+1,\ \mu(p)=-1,\ \mu(p^\alpha)=0\ si\ \alpha\geqslant 2.$$

Exercice(s) 3.23. Montrer que $\sum_{p|n}\frac{\log p}{p}=O(\log\log n)$ (on pourra remarquer que $x\to\log x/x$ est décroissante).

Exercice(s) 3.24.

– On définit la fonction d'Euler $\varphi:=\mathrm{Id}*\mu$. Montrer que φ est multiplicative et que

$$\varphi(p^\alpha)=(p-1)p^{\alpha-1}=p^\alpha(1-\frac{1}{p}).$$

– Montrer que $\varphi(q)=|(\mathbb{Z}/q\mathbb{Z})^\times|=|\{1\leqslant a\leqslant q,\ (a,q)=1\}|$ (on utilisera la formule suivante qu'on démontrera

$$\delta_{(a,q)=1}=\sum_{d|a,\ d|n}\mu(d)\ ).$$

Exercice(s) 3.25. Montrer que $\sum_n\mu(n)/n^2=6/\pi^2$ puis que

$$\sum_n\varphi(n)=\frac{6}{\pi^2}x^2(1+o(1))$$

Exercice(s) 3.26. Soit A l'ensemble des entiers n tels que $p|n\Rightarrow p\leqslant\sqrt{n}$, On veut étudier la fonction $Q_A(x)=\#A\cap[1,x]$. On note pour tout nombre premier p $B_p=\{p,2p,\dots,(p-1)p\}$.

(1) Montrer que $\mathbb{N}^*-A=\bigcup_p B_p$ et que $B_p\cap B_q=$.

(2) Montrer que $Q_A(x)=[x]-\sum_{p\leqslant x^{1/2}}(p-1)-\sum_{x^{1/2}<p\leqslant x}[\frac{x}{p}]$.

(3) Donner un équivalent de $Q_A(x)$ quand $x\to+\infty$.

Exercice(s) 3.27. Soit SQF l'ensemble des entier sans facteur carrés et $Q(x)=\#SQF\cap[1,x]$.

(1) Montrer que

$$Q(x)=\sum_{n\leqslant x^{1/2}}\mu(n)[\frac{x}{n^2}],$$

et calculer un équivalent de $Q(x)$ quand $x\to+\infty$.

(2) Généraliser ceci au cas des entiers k-libres : n est k libre ssi $\forall\ p,\ p^k\not| n$.

Exercice(s) 3.28. Montrer que la probabilité que deux entiers soient premiers entre eux est $6/\pi^2$.

Exercice(s) 3.29. Pour $k\geqslant 1$ entier on pose $D_k(n)=\sum_{d|n}d^k0(1*\mathrm{Id}^k)(n)$.

(1) Montrer que $D_k(uv)\leqslant D_k(u)D_k(v)$.

(2) Montrer que pour tout nombre premier p $D_k(p^l) \leqslant k^l$ et que la série $\sum_{l\geqslant 0} \frac{D_k(p^l)}{p^l}$ converge.

(3) Montrer que $\sum_{n\leqslant x} \frac{D_k(n)}{n} = O_k(\prod_{k<p\leqslant x} (1-\frac{k}{p})^{-1}$ et en déduire la majoration

$$\sum_{n\leqslant x} D_k(n) = O_k(x\log^{k-1} x).$$

Exercice(s) 3.30. Pour $n = p_1^{a_1} p_2^{a_2} \dots p_k^{a_k}$, on pose $\alpha(n) = a_1 a_2 \dots a_n$.

(1) Montrer que $L(\alpha, s) = \sum_{n\geqslant 1} \frac{\alpha(n)}{n^s}$ converge absolument pour $\Re e s > 2$ et que dans ce domaine, on a l'égalité

$$L(\alpha, s) = \zeta(s) \frac{\zeta(2s)\zeta(3s)}{\zeta(6s)}$$

(2) En déduire que l'abscisse de convergence absolue de $L(\alpha, s)$ est 1.

(3) On note β, la fonction arithmétique définie par $1 * \beta = \alpha$. Montrer que β est multiplicative, calculer $\beta(p)$.

(4) Calculer sa série L associée,

$$L(\beta, s) = \sum_{n\geqslant 1} \frac{\beta(n)}{n^s},$$

puis montrer que l'abscisse de convergence absolue de $L(\beta, s)$ vaut $1/2$.

(5) En déduire par une IPP que

$$\sum_{n\leqslant y} |\beta(n)| = O(y^{3/4}).$$

(6) En utilisant la décomposition $\alpha(n) = (1 * \beta)(n) = \sum_{d|n} \beta(d)$ montrer l'équivalent

$$\sum_{n\leqslant x} \alpha(n) = \frac{\zeta(2)\zeta(3)}{\zeta(6)} x + O(x^{3/4})$$

Exercice(s) 3.31. Montrer que pour $\Re e s > 1$, on a

$$\zeta(s) = \sum_{n\geqslant 1} \frac{1}{n^s} = \int_1^\infty [t]\, t^s \frac{dt}{t}$$

et en écrivant $t = [t] + \{t\}$ montrer que

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

se prolonge en une fonction holomorphe dans le domaine $\Re e s > 0$.

CHAPITRE 4

Série de Dirichlet

1. Rappel sur les séries entières

Etant donné une suite à valeurs complexes $\mathbf{a} = (a_n)_{n\geqslant 0}$, sa série entière associée est la série

$$F(\mathbf{a}, q) = \sum_{n\geqslant 0} a_n q^n.$$

Soit ρ son rayon de convergence qu'on suppose strictement positif (en particulier $|a_n| = o((\frac{1.01}{\rho})^n),\ n \to +\infty$). La série $F(\mathbf{a}, q)$ définit alors une fonction holomorphe dans le disque ouvert $\{q \in \mathbf{C},\ |q| < \rho\}$ et la donnée de cette fonction détermine la suite $\mathbf{a}$ (formules de Cauchy). Soit $\mathbf{b} = (b_n)$ est un autre suite dont la série entière associée

$$F(\mathbf{b}, q) = \sum_{n\geqslant 0} b_n q^n$$

est de rayon de convergence $\rho' > 0$ alors le produit $F(\mathbf{a}, q)F(\mathbf{b}, q)$ définit une série entière de rayon de convergence $\rho'' \geqslant \min(\rho, \rho')$

$$F(\mathbf{c}, q) = F(\mathbf{a}, q)F(\mathbf{b}, q) = \sum_{n\geqslant 0} c_n q^n,\ c_n = \sum_{l+m=n} a_l b_m.$$

Ce type de relation ouvre la porte à l'étude de problèmes arithmétiques par des voies analytiques : par exemple, consiérons $\mathbf{a} = (r_\square(n))_{n\geqslant 0}$:

$$a_n = r_\square(n) = |\{m \in \mathbb{Z},\ m^2 = n\}| = \begin{cases} 2 & \text{si } n \text{ est un carré,} \\ 0 & \text{sinon} \end{cases};$$

sa série associée est

$$F(q) = 1 + 2\sum_{m\geqslant 1} q^{m^2}$$

et son rayon de convergence vaut 1. Les puissances de cette série sont de la forme ($k \geqslant 1$)

$$F(q)^k = \sum_{n\geqslant 0} r_k(n) q^n$$

où

$$r_k(n) = |\{(m_1, \cdots, m_k) \in \mathbb{Z},\ m_1^2 + \cdots + m_k^2 = n\}|,$$

est le nombre de manières de représenter n comme somme de k carrés d'entiers. La fonction $F(q)$ admet des propriétés analytique qui permettent d'étudier le comportement de ces nombres de représentations. D'autre part, comme on va le voir plus loin, cette fonction (à un changement de variable près) est fortement liée à la fonction ζ de Riemann.

2. Séries de Dirichlet

Les séries de Dirichlet sont aux fonctions arithmétiques ce que les séries entières sont aux suites numériques. Soit f une fonction arithmétique, *la série de Dirichlet associée à* f est la série de la variable complexe s

$$s \mapsto L(f,s) = \sum_{n\geqslant 1} \frac{f(n)}{n^s}.$$

On va s'intéresser aux propriétés analytique de telles séries. Encore faut-il qu'elles convergent pour au moins une valeur de s : supposons que ce soit le cas, alors $f(n)/n^s \to 0,\ n \to +\infty$ et donc

$$|f(n)| = O(n^\sigma),\ \text{avec } \sigma = \Re e s.$$

Réciproquement si pour un certain $A \in \mathbb{R}$

$$|f(n)| = O(n^A) \tag{4.1}$$

alors pour $\sigma > A+1$

$$\sum_{n\geqslant 1} \frac{|f(n)|}{n^\sigma} = O(\sum_{n\geqslant 1} \frac{n^A}{n^\sigma}) < +\infty,$$

ie. la série converge absolument (en particulier elle converge)pour tout s tel que $\Re s > A+1$.

Définition 4.1. *Une fonction arithmétique $f : \mathbb{N}_{\geqslant 1} \to \mathbf{C}$ est à croissance polynomiale si elle satisfait à l'une des conditions équivalentes suivantes*

– *Il existe une constante $A \in \mathbb{R}$ (dépendant de f) telle que $|f(n)| = O(n^A)$.*

– *Il existe $\sigma \in \mathbb{R}$ tel que la série $L(f,\sigma)$ soit absolument convergente.*

Dans ce cas on note

$$\sigma_f = \inf\{\sigma \in \mathbb{R},\ L(f,\sigma) \text{ converge absolument}\} \in \mathbb{R} \cup \{-\infty\};$$

La quantité σ_f est appelée abscisse de convergence absolue de $L(f,s)$.

L'abscisse de convergence absolue est l' analogue pour les série de dirichlet du rayon de convergence pour une série entière :

Proposition 4.2. *Soit f une fonction arithmétique à croissance polynomiale et σ_f son abscisse de convergence absolue. Pour tout $\sigma > \sigma_f$, la série $L(f,s)$ converge absolument uniformément dans le demi-plan $\{s \in \mathbf{C},\ \Re s \geqslant \sigma\}$ et définit une fonction holomorphe dans le demi-plan $\{s \in \mathbf{C},\ \Re s > \sigma_f\}$; dans ce domaine, la dérivée de $L(f,s)$ est la série de Dirichlet de la fonction arithmétique*

$$-\log.f : n \mapsto -\log(n)f(n),\ \textit{i.e. } L(f,s)' = L(-f.\log,s) = \sum_n \frac{-\log(n)f(n)}{n^s}$$

dont l'abscisse de convergence absolue vaut σ_f.

Preuve. Soit $\sigma > \sigma_f$, alors uniformément pour $\Re s \geqslant \sigma$ on a

$$\frac{|f(n)|}{|n^s|} \leqslant \frac{|f(n)|}{n^\sigma}$$

et donc la série de fonctions holomorphes $\sum_{n\geqslant 1} \frac{f(n)}{n^s}$ est uniformément absolument majorée par la série absolument convergente $\sum_{n\geqslant 1} \frac{|f(n)|}{n^\sigma}$, et donc converge uniformément sur $\Re e s \geqslant \sigma$

et définit donc une fonction holomorphe sur $\Re es > \sigma$. Il résulte des formules de Cauchy que la dérivée $L(f,s)'$ est donnée par la série des dérivées, à savoir

$$\sum_{n\geqslant 1} f(n)(n^{-s})' = \sum_n \frac{-\log(n)f(n)}{n^s} = L(-f.\log, s),$$

cette série de Dirichlet est donc convergente pour s tel que $\Re es > \sigma_f$. Appliquant ce raisonnement à la fonction arithmétique $n \mapsto |f(n)|$ on voit que $L(-f.\log, s)$ est absolument convergente pour $\Re es > \sigma_f$: $\sigma_{-f.\log} \leqslant \sigma_f$. D'autre part, comme $f(n)\log(n) \geqslant f(n),\ n \geqslant 3$, $\sigma_{-f.\log} \geqslant \sigma_f$ d'ou l'égalité. □

Le lemme suivant est très utile : il montre qu'une fonction arithmétique à croissance polynomiale est déterminée par sa série de Dirichlet :

Lemme 4.3. *Soient f, g deux fonctions arithmétiques à croissance polynomiale. On suppose que pour tout s contenu dans un ouvert (non-vide) du demi-plan $\{s,\ \Re es > \max(\sigma_f, \sigma_g)\}$ on a $L(f,s) = L(g,s)$ alors $f = g$.*

Preuve. Quitte à remplacer f par $f - g$ on peut supposer que $g = 0$ et que $L(f,s) = 0$ pour s dans un ouvert du demi-plan $\{s,\ \Re es > \sigma_f\}$. comme cette fonction est holomorphe, elle est identiquement nulle dans ce demi-plan. Quitte à remplacer f par

$$f \times \mathrm{Id}^{-(\sigma_f+1)} :\ n \mapsto f(n)n^{-(\sigma_f+1)}$$

on peut supposer que $\sigma_f \leqslant -1$ et en particulier que $f(n) = O(1)$. Suposons $f \not\equiv 0$ et soit n_0 le plus petit entier tel que $f(n) \neq 0$; on a pour $\Re es > 2$

$$0 = \sum_{n\geqslant n_0} \frac{f(n)}{n^s} = \frac{f(n_0)}{n_0^s}\Big(1 + \frac{n_0^s}{f(n_0)} \sum_{n\geqslant n_0+1} \frac{f(n)}{n^s}\Big).$$

Comme f est bornée, on voit (en comparant avec une intégrale) que pour $\Re es > 2$

$$\sum_{n\geqslant n_0+1} \frac{f(n)}{n^s} = O\Big(\frac{1}{(n_0+1)^{\Re s-1}}\Big)$$

et donc

$$0 = 1 + \frac{n_0^s}{f(n_0)} \sum_{n\geqslant n_0+1} \frac{f(n)}{n^s} = 1 + O\Big(\frac{1}{Res-1}\Big)$$

qui donne une contracdiction quand $\Re s \to +\infty$. □

L'intéret principal de l'introduction des séries de Dirichlet est le suivant

Théorème 4.4. *Soient $f, g \in \mathscr{A}$ avec $\sigma_f, \sigma_g < \infty$, alors $\sigma_{f*g} \leqslant \max(\sigma_f, \sigma_g)$ et pour $\Re s > \max(\sigma_f, \sigma_g)$*

$$L(f*g, s) = L(f,s)L(g,s).$$

Preuve. Soit $\Re s > \max(\sigma_f, \sigma_g)$ alors (toutes les identités et inversions de sommations sont justifiées par le fait qu'on somme des termes positifs)

$$\begin{aligned}
\sum_{n\geqslant 1} \frac{|f*g(n)|}{|n^s|} &= \sum_{n\geqslant 1} \frac{|\sum_{ab=n} f(a)g(b)|}{n^{\Re s}} \\
&\leqslant \sum_{n\geqslant 1} \frac{\sum_{ab=n} |f(a)||g(b)|}{(ab)^{\Re s}} \\
&= \sum_{a,b\geqslant 1} \frac{|f(a)||g(b)|}{(ab)^{\Re s}} = \sum_a \frac{|f(a)|}{a^{\Re s}} \sum_{b\geqslant 1} \frac{|g(b)|}{b^{\Re s}} < \infty
\end{aligned}$$

donc $\sigma_{f*g} \leqslant \max(\sigma_f, \sigma_g)$; de plus pour $\Re s > \max(\sigma_f, \sigma_g)$ par convergence absolue on peut regrouper les termes arbitrairement ce qui donne

$$L(f,s)L(g,s) = L(f*g,s).$$

□

Corollaire 4.5. *Supposons que f est inversible (pour la convolution de Dirichlet) et que $\sigma_f, \sigma_{f^{(-1)}} < +\infty$ alors pour $\Re s > \max(\sigma_f, \sigma_{f^{-1}})$ on a*

$$L(f,s)L(f^{(-1)},s) = 1.$$

En particulier, $L(f,s)$ ne s'annule pas dans le demi-plan $\{\Re s > \max(\sigma_f, \sigma_{f^{-1}})\}$.

Exercice(s) 4.6. Montrer que si $\sigma_f \neq \sigma_g$, $\sigma_{f*g} = \max(\sigma_f, \sigma_g)$.

2.1. Exemples. Pour $f \equiv 1$ on a

$$L(1,s) = \sum_{n\geqslant 1} \frac{1}{n^s} = \zeta(s),\ \sigma_1 = 1.$$

La fonction de Moebius est l'inverse de la fonction 1 ; on a vu que $|\mu(n)| \leqslant 1$ et donc $\sigma_\mu \geqslant 1$. De plus on a

$$\sum_{n\geqslant 1} \frac{|\mu(n)|}{n} \geqslant \sum_{p\geqslant 2} \frac{1}{p} = \infty$$

donc $\sigma_\mu = 1$; on voit donc que pour $\Re es > 1$, $\zeta(s)$ ne s'annule pas et que

$$L(\mu,s) = \sum_n \frac{\mu(n)}{n^s} = \frac{1}{\zeta(s)}.$$

– Soit d la fonction nombre de diviseurs : on a $d = 1*1$ et donc $\sigma_d \leqslant 1$ (en fait comme $d(n) \geqslant 1$, $\sigma_d = 1$) et pour $\Re s > 1$, on a

$$L(d,s) = \zeta(s)^2.$$

– La fonction d'Euler φ vaut $\mu * \mathrm{Id}$ et comme $\sigma_{\mathrm{Id}} = 2$ et $\sigma_\mu = 1$, $\sigma_\varphi \leqslant 2$ (par l'exercice précédent $\sigma_\varphi = 2$) et pour $\Re es > 2$, on a

$$L(\varphi,s) = L(\mu,s)L(\mathrm{Id},s) = \frac{\zeta(s-1)}{\zeta(s)}.$$

– La fonction de von Mangoldt $\Lambda = \log * \mu$ et donc

$$L(\Lambda,s) = L(\log,s)L(\mu,s) = -\frac{\zeta'(s)}{\zeta(s)}.$$

On a $\sigma_\Lambda \leqslant 1$ et comme la série $\sum_{n\geqslant 1} \frac{\Lambda(n)}{n}$ diverge, $\sigma_\Lambda = 1$. Comme $\zeta(s)$ ne s'annule pas pour $\Re es > 1$, son logarithme $\log\zeta(s)$ est bien définit -à une constante additive près- et holomorphe sur ce demi-plan et sa dérivée (la dérivée logarithmique) vaut précisèment

$$(\log\zeta(s))' = \mathrm{dlog}\zeta(s) = -\frac{\zeta'(s)}{\zeta(s)}.$$

3. Séries de Dirichlet et fonctions multiplicatives

Théorème 4.7. *Soit $f \in \mathscr{A}$ une fonction multiplicative et croissance polynomiale, alors pour tout $\sigma > \sigma_f$ on a,*

(1) *pour tout p premier la série*

$$L_p(f,s) := \sum_{\alpha \geqslant 0} \frac{f(p^\alpha)}{p^{\alpha s}}$$

converge absolument uniformément dans le demi-plan $\Re s \geqslant \sigma$; on l'appelle le facteur local de f en p.

(2) *De plus on a*

$$L(f,s) = \prod_p L_p(f,s) (= \lim_{P \to +\infty} \prod_{p \leqslant P} L_p(f,s))$$

et la convergence est uniforme dans ce demi-plan.

(3) *De façon plus précise, si on note $L^{>P}(f,s) = \lim_{P' \to +\infty} \prod_{P < p \leqslant P'} L_p(f,s)$ alors quand $P \to +\infty$*

$$L^{>P}(f,s) \to 1$$

uniformément dans tout demi-plan $\Re s \geqslant \sigma$, $\sigma > \sigma_f$.

(4) *Réciproquement, si f est une fonction arithmetique telle que $\sigma_f < \infty$ et $f(1) = 1$ et si $L(f,s)$ vérifie*

$$L(f,s) = \prod_p L_p(f,s) (= \lim_{P \to +\infty} \prod_{p \leqslant P} L_p(f,s))$$

pour $s \gg 1$ alors f est multiplicative.

Preuve. (1) Soit $\Re s \geqslant \sigma$, alors

$$\sum_{\alpha \geqslant 0} |f(p^\alpha)| / |p^{\alpha s}| \leqslant \sum_n |f(n)| / n^\sigma < \infty,$$

d'où la convergence absolue uniforme de $L_p(f,s)$.

(2) Pour $P \geqslant 2$, notons

$$p_1 < p_2 < \cdots < p_k \leqslant P$$

l'ensemble des nombres premiers $\leqslant P$, alors

$$\prod_{p \leqslant P} L_p(f,s) = \sum_{\alpha_1, \ldots, \alpha_k \geqslant 0} \frac{f(p_1^{\alpha_1}) \ldots f(p_k^{\alpha_k})}{(p_1^{\alpha_1} \ldots p_k^{\alpha_k})^s} = \sum_{\alpha_1, \ldots, \alpha_k \geqslant 0} \frac{f(p_1^{\alpha_1} \ldots p_k^{\alpha_k})}{(p_1^{\alpha_1} \ldots p_k^{\alpha_k})^s} = \sum_{\substack{n \geqslant 1 \\ p \mid n \Rightarrow p \leqslant P}} \frac{f(n)}{n^s}$$

ainsi un entier qui n'est pas dans la somme précédente a au moins un diviseur premier $> P$ et est donc $> P$:

$$|L(f,s) - \prod_{p \leqslant P} L_p(f,s)| \leqslant \sum_{n > P} |f(n)| / n^\sigma \to 0, \ P \to +\infty$$

avec convergence uniforme.

(3) On va maintenant montrer que quand $P \to +\infty$,

$$L^{>P}(f,s) := \prod_{p > P} L_p(f,s)$$

tend vers 1 uniformément dans tout demi-plan $\Re s \geqslant \sigma > \sigma_f$. On a $\prod_{p > P} L_p(f,s)$ est la série de Dirichlet de la fonction multiplicative f_P qui vaut 0 si n a un facteur premier $\leqslant P$ et $f(n)$

sinon (pour $n=1$, $f(1)=1$ car 1 n'a pas de facteur premier et en particulier aucun facteur premier $\leqslant P$). Il est clair que $\sigma_{f_P} < \sigma_f$. On a

$$\prod_{p>P} L_p(f,s) = \sum_{\substack{n \\ p|n \to p>P}} \frac{f(n)}{n^s} = 1 + \sum_{\substack{n>1 \\ p|n \to p>P}} \frac{f(n)}{n^s}$$

et donc

$$|\prod_{p>P} L_p(f,s) - 1| \leqslant \sum_{\substack{n>1 \\ p|n \to p>P}} \frac{|f(n)|}{n^\sigma} \leqslant \sum_{n>P} \frac{|f(n)|}{n^\sigma} \to 0.$$

(4) Réciproquement, soit $\widetilde{f}$ l'unique fonction multiplicative définie par

$$\widetilde{f}(n) = \prod_{p^\alpha \| n} f(p^\alpha).$$

Alors $\sigma_{\widetilde{f}} \leqslant \sigma_f + 1$: en effet pour $\sigma > \sigma_f$, $|f(n)|/n^\sigma = o(1)$ et donc pour n assez grand (disons $n \geqslant N$) $|f(n)|/n^\sigma < 1$; on en déduit que

$$\frac{\widetilde{f}(n)}{n^\sigma} = \prod_{p^\alpha \| n} \frac{f(p^\alpha)}{p^{\alpha\sigma}} = \prod_{\substack{p^\alpha \| n \\ p^\alpha \leqslant N}} \frac{f(p^\alpha)}{p^{\alpha\sigma}} \prod_{\substack{p^\alpha \| n \\ p^\alpha > N}} \frac{f(p^\alpha)}{p^{\alpha\sigma}} = O(1)$$

et donc que $L(\widetilde{f},s)$ converge absolument pour $\Re s > \sigma + 1$ et alors

$$L(\widetilde{f},s) = \prod_p L_p(\widetilde{f},s) = \prod_p L_p(f,s).$$

On a donc pour $\Re s$ assez grand

$$L(\widetilde{f},s) = \sum_n \frac{\widetilde{f}(n)}{n^s} = L(f,s) = \sum_n \frac{f(n)}{n^s};$$

cela implique par le Lemme 4.3 que pour tout $n \geqslant 1$, $f(n) = \tilde{f}(n)$. □

Corollaire 4.8. *Si f est completement multiplicative, pour $\Re s > \sigma_f$, on a*

$$L(f,s) = \prod_p (1 - \frac{f(p)}{p^s})^{-1}$$

Ces résultats de factorisation en produit Eulérien permettent une première localisation des zéros de $L(f,s)$:

Proposition 4.9. *Soit $f \in \mathscr{A}^\times$ une fonction multiplicative. Soit $\sigma > \sigma_f$; le nombre de facteurs locaux $L_p(f,s)$ qui ont un zero dans le demi-plan $\Re e s \geqslant \sigma$ est fini et les zeros de $L(f,s)$ dans ce demi-plan sont exactement les zeros des facteurs locaux $L_p(f,s)$. Plus précisément, il existe P tel que*

$$\prod_{p>P} L_p(f,s) = \frac{L(f,s)}{\prod_{p<P} L_p(f,s)}$$

ne s'annule pas pour $\Re e s \geqslant \sigma$. Ainsi les zéros de $L(f,s)$ dans le demi-plan de convergence absolue sont exactement les zéros des facteurs locaux $L_p(f,s)$.

Preuve. Soit $\sigma > \sigma_f$; on a vu que si p est assez grand, pour tout s avec $\Re es \geqslant \sigma$

$$|L_p(f,s) - 1| \leqslant 1/2$$

ainsi le nombre de facteurs locaux qui s'annulent dans le demi-plan $\Re es \geqslant \sigma$ est fini. D'autre part, on a vu prècèdemment que si P est assez grand et $\Re es \geqslant \sigma$ $|L^{>P}(f,s)-1| \leqslant \sum_{n>P} \frac{|f(n)|}{n^\sigma} < 1/2$ donc $L_{>P}(f,s)$ ne s'annule pas dans le demi-plan $\Re s \geqslant \sigma$. □

3.1. Exemples. Pour $\Re s > 1$,

$$\zeta(s) = \sum_{n\geqslant 1} \frac{1}{n^s} = \prod_p (1 - \frac{1}{p^s})^{-1}, \sum_{n\geqslant 1} \frac{\mu(n)}{n^s} = \prod_p (1 - \frac{1}{p^s}) = 1/\zeta(s);$$

$\zeta(s)$ ne s'annule pas pour $\Re s > 1$.

$$\Re s > 1, \sum_{n\geqslant 1} \frac{\tau(n)}{n^s} = \zeta(s)^2 = \prod_p (1 - \frac{1}{p^s})^{-2},$$

$$L(\tau^{(-1)}, s) = \zeta(s)^{-2} = \prod_p (1 - \frac{2}{p^s} + \frac{1}{p^{2s}}).$$

$$\Re s > 2, \sum_{n\geqslant 1} \frac{\varphi(n)}{n^s} = \frac{\zeta(s-1)}{\zeta(s)} = \prod_p (\frac{1-p^{-s}}{1-p^{1-s}}) = \prod_p (1 + \sum_{\alpha\geqslant 1} (1 - \frac{1}{p}) \frac{p^\alpha}{p^{\alpha s}})$$

4. Les séries L

Les séries de Dirichlet qui apparaisent le plus souvent en théorie des nombres sont liés à des séries de la forme suivante qu'on appellera "séries L". Entre autres propriété les séries L, sont des séries de Dirichlet de la forme suivante : soit $d \geqslant 1$ un entier et $\pi = (\pi_p)_p = ((V_p, \Phi_p))_p$ une suite (indexée par les nombres premiers) de paires formées de

(1) un $\mathbf{C}$-espace vectoriel V_p de dimension d,

(2) un endomorphisme $\Phi_p : V_p \to V_p$; ces valeurs propres sont notées $\{\chi_{p,i},\ i = 1 \cdots, d\}$.

On associe à chaque paire π_p, un polynôme de degré $\leqslant d$ qui vérifie $P_p(0) = 1$

$$P(\pi_p, X) := \det(\mathrm{Id}_{V_p} - X\Phi_p) = \prod_{i=1}^{d} (1 - \chi_{p,i} X),$$

(c'est une sorte de "polynôme caractéristique" de l'endomorphisme Φ_p) et un facteur local

$$L(\pi_p, s) := P(\pi_p, p^{-s})^{-1} = \prod_{i=1}^{d} (1 - \frac{\chi_{p,i}}{p^s})^{-1},\ s \in \mathbf{C}$$

qui définit une fonction méromorphe sur $\mathbf{C}$.

On fait l'hypothèse suivante concernant les valeurs propres des Φ_p :

Il existe $A \in \mathbb{R}$ telle que pour tout p et tout $i = 1, \cdots, d$ $|\chi_{p,i}| \leqslant p^A$.

Alors, pour chaque p, la série entière $P(\pi_p, X)^{-1}$ converge pour $|X| < p^{-A}$ et écrivant son développement de Taylor

$$P(\pi_p, X)^{-1} = \sum_{\alpha\geqslant 0} \lambda_\pi(p^\alpha) X^\alpha;$$

on a

$$\lambda_\pi(1) = P(\pi_p, 0) = 1,\ \lambda_\pi(p^\alpha) = \sum_{\alpha_1 + \cdots + \alpha_d = \alpha} \chi_{p,1}^{\alpha_1} \times \cdots \times \chi_{p,d}^{\alpha_d}$$

et pour $\Re s > A$, on a

$$L(\pi_p, s) = \sum_{\alpha \geqslant 0} \lambda_\pi(p^\alpha) p^{-\alpha s}.$$

Considérons le fonction multiplicative définie par

$$\lambda_\pi(n) = \prod_{p^{\alpha_p} \| n} \lambda_\pi(p^{\alpha_p}).$$

On a la

Proposition 4.10. *La fonction multiplicative $n \to \lambda_\pi(n)$ est a croissance polynomiale et sa série de Dirichlet associaée est*

$$L(\pi, s) = \sum_{n \geqslant 1} \frac{\lambda_\pi(n)}{n^s} = \prod_p L(\pi_p, s)$$

et son abscisse de convergence absolue vérifie

$$\sigma_\pi \leqslant A + 1$$

et cette fonction ne s'annule pas pour $\Re s > A + 1$.

Preuve. On a

$$|\lambda_\pi(p^\alpha)| \leqslant \sum_{\alpha_1 + \cdots + \alpha_d = \alpha} |\chi_{p,1}|^{\alpha_1} \times \cdots \times |\chi_{p,d}|^{\alpha_d} \leqslant p^A \sum_{\alpha_1 + \cdots + \alpha_d = \alpha} 1 = p^A d_d(p^\alpha)$$

avec $d_d(n) = 1^{(*d)}(n)$ est la fonction diviseurs d'ordre d. On a donc

$$|\lambda_\pi(n)| = |\prod_{p^{\alpha_p} \| n} \lambda_\pi(p^{\alpha_p})| \leqslant n^A d_d(n)$$

et comme la'abscisse de convergence de la série L de la fonction $n \to d_d(n)$ vaut 1 (car $L(d_d, s) = L(1, s)^d = \zeta(s)^d$), la série $L(\pi, s)$ converge absoluement pour $\Re s > A+1$. Cette fonction ne s'annule pas pour $\Re s > A + 1$ car d'après la Prop. 4.9, ses seuls zéros possible dans ce demi-plan sont ceux des facteur locaux

$$L(\pi_p, s) = \prod_{i=1}^{d} (1 - \frac{\chi_{p,i}}{p^s})^{-1}$$

qui ne s'annulent pas sur $\mathbf{C}$. □

4.1. Dérivé logarithmique d'une série L. étant donné f une fonction méromorphe sur un ouvert $\Omega \subset \mathbf{C}$, la *dérivée logarithmique* de f est la fonction

$$\mathrm{dlog} f : s \mapsto \frac{f'(s)}{f(s)}.$$

Cette fonction est méromorphe sur Ω et l'ensemble de ses poles est formé de la réunion des zéros et des poles de f. En effet, il résulte de la règle de Leibniz

$$(f \times g)' = f' \times g + f \times g'$$

que

$$\mathrm{dlog}(f \times g) = \frac{f' \times g + f \times g'}{f \times g} = \mathrm{dlog} f + \mathrm{dlog} g. \tag{4.2}$$

En particulier si ρ est un zéro ou un pôle de f, on peut écrire

$$f(s) = (s - \rho)^{m_\rho} g(s)$$

pour $m_\rho \in \mathbb{Z}$ (c'est l'ordre de f en ρ) et $g(s)$ une fonction holomorphe au voisinage de ρ et ne s'annulant pas en ρ. On a donc au voisinage de ρ

$$\mathrm{dlog} f(s) = \frac{m_\rho}{s-\rho} + \mathrm{dlog} g(s)$$

qui est une fonction méromorphe avec un pôle simple en $s=\rho$ de résidu m_ρ (l'ordre de f en s_0).

On va appliquer cette construction à la série $L(\pi,s)$ et on va notamment voir que la propriété d'additivité (4.2) "passe" au produit Eulérien.

Théorème 4.11. *Soit $L(\pi,s)$ comme ci-dessus, la fonction $\mathrm{dlog} L(\pi,s)$ est holomorphe pour $\Re e > A+1$ et, pour $\Re s > A+1$, on a l'identité suivante :*

$$-\mathrm{dlog} L(\pi,s) = -\frac{L'(\pi,s)}{L(\pi,s)} = L(\Lambda_\pi,s) = \sum_{n\geqslant 1} \frac{\Lambda_\pi(n)}{n^s},$$

$$\Lambda_\pi(n) = \begin{cases} \log p(\chi_{p,1}^\alpha + \cdots + \chi_{p,d}^\alpha) & si\ n = p^\alpha,\ \alpha \geqslant 1 \\ 0 & sinon. \end{cases}$$

Preuve. On a

$$|\Lambda_\pi(n)| \leqslant d\Lambda(n) n^A$$

donc la série $L(\Lambda_\pi,s)$ converge absolument pour $\Re s > A+1$ et définit une fonction holomorphe dans ce demi-plan.

Soit $P \geqslant 2$, on a pour s contenu dans un compact K du demi-plan $\{\Re s > A+1\}$

$$L(\pi,s) = \prod_{p\leqslant P} L(\pi_p,s) \prod_{p>P} L(\pi_p,s) = L^{\leqslant P}(\pi,s) L^{>P}(\pi,s)$$

et donc

$$\mathrm{dlog} L(\pi,s) = \mathrm{dlog} L^{\leqslant P}(\pi,s) + \mathrm{dlog} L^{>P}(\pi,s)$$

Comme $L^{>P}(\pi,s) \to 1$ uniformément sur K quand $P \to +\infty$ on a

$$\mathrm{dlog} L^{>P}(\pi,s) \to 0$$

et donc

$$\mathrm{dlog} L(\pi,s) = \lim_{P\to\infty} \mathrm{dlog} L^{\leqslant P}(\pi,s) = \lim_{P\to\infty} \sum_{p\leqslant P} \mathrm{dlog} L(\pi_p,s).$$

On a

$$\mathrm{dlog} L(\pi_p,s) = \mathrm{dlog} \prod_{i=1}^d (1-\frac{\chi_{p,i}}{p^s})^{-1} = -\sum_{i=1}^d \mathrm{dlog}(1-\frac{\chi_{p,i}}{p^s}) = -\sum_{i=1}^d \log p \frac{\chi_{p,i}}{p^s(1-\frac{\chi_{p,i}}{p^s})}$$

$$= -\sum_{\alpha\geqslant 1} \frac{\log p}{p^{\alpha s}} \sum_{i=1}^d \chi_{p,i}^\alpha = -\sum_{\alpha\geqslant 1} \frac{\Lambda_\pi(p^\alpha)}{p^{\alpha s}},$$

en utilisant l'identité valable pour $\Re s > A+1$

$$\frac{\chi_{p,i}}{p^s(1-\frac{\chi_{p,i}}{p^s})} = \sum_{\alpha\geqslant 1} \frac{\chi_{p,i}^\alpha}{p^{\alpha s}}.$$

Ainsi

$$\mathrm{dlog} L(\pi,s) = -L(\Lambda_\pi,s)$$

□

5. Fonctions arithmétiques : Formulaire RAPPEL

f			L(s)
e	$e(n) = \delta_{n=1}$		1
1	$1(n) = 1$		$\zeta(s) = \prod_p (1 - \frac{1}{p^s})^{-1}$
μ	$\mu(p_1 \dots p_r) = (-1)^r,\ \mu(a^2 b) = 0$	$\mu = 1^{(-1)},\ \mu * 1 = e$	$\frac{1}{\zeta(s)} = \prod_p (1 - \frac{1}{p^s})$
$\log$	$\log(n)$		$-\zeta'(s)$
Λ	$\Lambda(n) = \begin{cases} \log p \ \ si\ \ n = p^\alpha \\ 0\ \ sinon \end{cases}$	$\log = 1 * \Lambda,\ \Lambda = \mu * \log$	$-\frac{\zeta'}{\zeta}(s)$
φ	$\varphi(n) = n \prod_{p\mid n} (1 - \frac{1}{p})$	$\varphi = Id * \mu$	$\frac{\zeta(s+1)}{\zeta(s)}$
d	$d(n) = \lvert\{d \geqslant 1,\ d\mid n\}\rvert$	$d = 1 * 1$	$\zeta^2(s)$

6. Exercices

Exercice(s) 4.12.

(1) Montrer que le TNP equivaut a $p_n \sim n \log n$ où p_n est le n-ième nombre premier.

(2) Donner un équivalent de la somme $\sum_{p \leqslant x} p$ (on admettra le TNP).

Exercice(s) 4.13. Montrer que

$$\sum_{n \leqslant x} \log(n) = x \log x - x + O(\log x),$$

$$TNP \Longleftrightarrow \theta(x) = x(1 + o(1)) \Longleftrightarrow \psi(x) = x(1 + o(1)).$$

Exercice(s) 4.14. Montrer que

$$\sum_{n \leqslant x} \tau(n) = x \log x + O(x)$$

puis que pour $k \geqslant 3$

$$\sum_{n \leqslant x} \tau_k(n) = x \log^{k-1} x + O(x \log^{k-2} x).$$

Exercice(s) 4.15. Montrer que $d = 1 * 1$ et $\mu = 1^{(-1))}$ sont multiplicatives et que

$$d(p^\alpha) = \alpha + 1,\ \mu(p) = -1,\ \mu(p^\alpha) = 0\ \ si\ \ \alpha \geqslant 2.$$

Exercice(s) 4.16. Montrer que $\displaystyle\sum_{p \mid n} \frac{\log p}{p} = O(\log\log n)$ (on pourra remarquer que $x \to \log x / x$ est décroissante).

Exercice(s) 4.17.

– On définit la fonction d'Euler $\varphi := \mathrm{Id} * \mu$. Montrer que φ est multiplicative et que

$$\varphi(p^\alpha) = (p-1)p^{\alpha-1} = p^\alpha (1 - \frac{1}{p}).$$

– Montrer que $\varphi(q) = \lvert(\mathbb{Z}/q\mathbb{Z})^\times\rvert = \lvert\{1 \leqslant a \leqslant q,\ (a,q) = 1\}\rvert$ (on utilisera la formule suivante qu'on démontrera

$$\delta_{(a,q)=1} = \sum_{d \mid a,\ d \mid n} \mu(d)\ ).$$

Exercice(s) 4.18. Montrer que $\sum_n \mu(n)/n^2 = 6/\pi^2$ puis que

$$\sum_n \varphi(n) = \frac{6}{\pi^2} x^2 (1 + o(1))$$

Exercice(s) 4.19. Soit A l'ensemble des entiers n tels que $p|n \Rightarrow p \leqslant \sqrt{n}$, On veut étudier la fonction $Q_A(x) = \#A \cap [1,x]$. On note pour tout nombre premier p $B_p = \{p, 2p, \dots, (p-1)p\}$.

(1) Montrer que $\mathbb{N}^* - A = \bigcup_p B_p$ et que $B_p \cap B_q =$.

(2) Montrer que $Q_A(x) = [x] - \sum_{p \leqslant x^{1/2}} (p-1) - \sum_{x^{1/2} < p \leqslant x} [\frac{x}{p}]$.

(3) Donner un équivalent de $Q_A(x)$ quand $x \to +\infty$.

Exercice(s) 4.20. Soit SQF l'ensemble des entier sans facteur carrés et $Q(x) = \#SQF \cap [1,x]$.

(1) Montrer que
$$Q(x) = \sum_{n \leqslant x^{1/2}} \mu(n) [\frac{x}{n^2}],$$
et calculer un équivalent de $Q(x)$ quand $x \to +\infty$.

(2) Généraliser ceci au cas des entiers k-libres : n est k libre ssi $\forall\ p,\ p^k \not| n$.

Exercice(s) 4.21. Montrer que la probabilité que deux entiers soient premiers entre eux est $6/\pi^2$.

Exercice(s) 4.22. Pour $k \geqslant 1$ entier on pose $D_k(n) = \sum_{d|n} d^k 0(1 * \mathrm{Id}^k)(n)$.

(1) Montrer que $D_k(uv) \leqslant D_k(u) D_k(v)$.

(2) Montrer que pour tout nombre premier p $D_k(p^l) \leqslant k^l$ et que la série $\sum_{l \geqslant 0} \frac{D_k(p^l)}{p^l}$ converge.

(3) Montrer que $\sum_{n \leqslant x} \frac{D_k(n)}{n} = O_k(\prod_{k < p \leqslant x} (1 - \frac{k}{p})^{-1}$ et en déduire la majoration
$$\sum_{n \leqslant x} D_k(n) = O_k(x \log^{k-1} x).$$

Exercice(s) 4.23. Pour $n = p_1^{a_1} p_2^{a_2} \dots p_k^{a_k}$, on pose $\alpha(n) = a_1 a_2 \dots a_n$.

(1) Montrer que $L(\alpha, s) = \sum_{n \geqslant 1} \frac{\alpha(n)}{n^s}$ converge absolument pour $\Re es > 2$ et que dans ce domaine, on a l'égalité
$$L(\alpha, s) = \zeta(s) \frac{\zeta(2s)\zeta(3s)}{\zeta(6s)}$$

(2) En déduire que l'abscisse de convergence absolue de $L(\alpha, s)$ est 1.

(3) On note β, la fonction arithmétique définie par $1 * \beta = \alpha$. Montrer que β est multiplicative, calculer $\beta(p)$.

(4) Calculer sa série L associée,
$$L(\beta, s) = \sum_{n \geqslant 1} \frac{\beta(n)}{n^s},$$
puis montrer que l'abscisse de convergence absolue de $L(\beta, s)$ vaut $1/2$.

(5) En déduire par une IPP que
$$\sum_{n \leqslant y} |\beta(n)| = O(y^{3/4}).$$

(6) En utilisant la décomposition $\alpha(n) = (1 * \beta)(n) = \sum_{d|n} \beta(d)$ montrer l'équivalent

$$\sum_{n \leqslant x} \alpha(n) = \frac{\zeta(2)\zeta(3)}{\zeta(6)} x + O(x^{3/4})$$

Exercice(s) 4.24. Montrer que pour $\Re es > 1$, on a

$$\zeta(s) = \sum_{n \geqslant 1} \frac{1}{n^s} = \int_1^\infty [t] t^s \frac{dt}{t}$$

et en écrivant $t = [t] + \{t\}$ montrer que

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

se prolonge en une fonction holomorphe dans le domaine $\Re es > 0$.

CHAPITRE 5

Le Théorème de la Progression Arithmétique

Définition 5.1. *Une progression arithmétique est un sous-ensemble non-vide de $\mathbb{Z}$ vérifiant la propriété suivante : il existe un entier positif $q > 0$ tel que la distance entre deux entiers consécutifs de cet ensemble est toujours q. L'entier q s'appelle le module de la progression arithmétique.*

Il est facile de voir que les progressions arithmétiques de module q sont de la forme

$$L_{q,a} = a + q\mathbb{Z} \subset \mathbb{Z}.$$

où a est un entier. Remarquons que si $a \equiv a'(q)$, on a $L_{q,a} = L_{q,a'}$. Ainsi les progression arithmetique de module q sont indexées par les classes de congruence modulo q (ie. par l'anneau $\mathbb{Z}/q\mathbb{Z}$) ; il y en a donc q.

Ainsi n appartient à $L_{q,a}$ ssi $n \equiv a(q)$. Ainsi la classe $\overline{a}$ de a modulo q est appellée *classe* de la progression arithmetique. On écrira indifférement $L_{q,a}$ ou $L_{q,\overline{a}}$ et par abus de language, on parlera pour l'entier a de la classe de la progression arithmétique.

Comme $L_{q,a}$ est infini il est naturel de se demander si son intersection avec les nombres premiers $\mathscr{P}$, l'est aussi : c'est presque toujours le cas

Théorème (de la progression arithmétique de Dirichlet, TPA). *Soient $a, q > 0$ deux entiers premiers entre eux, alors l'ensemble*

$$\mathscr{P}_{q,a} = \mathscr{P} \cap L_{q,a}$$

est infini ; autrement dit, il existe une infinité de nombres premiers $p \equiv a (\bmod q)$ (ie. de la forme $p = qk + a$ avec $k \in \mathbb{Z}$).

Remarque 5.2. La condition "*a et q premiers entre eux*" est nécessaire. En effet, si $(a, q) \neq 1$ alors il n'y a au plus un seul p premier de la forme $qn + a$ (la seule possibilité est $p = (a, q)$). En d'autres termes, les classes de congruences contenant une infinité de nombres premiers sont exactement celles de $(\mathbb{Z}/q\mathbb{Z})^\times$.

Dans la lignée du TNP, on peut poser des question plus précise sur la densité de l'ensemble $\mathscr{P}_{q,a}$. On pose donc

$$\pi(x; q, a) := |\mathscr{P}_{q,a} \cap [1, x]| = |\{p \leqslant x,\ p \equiv a(q)\}| = \sum_{p \equiv a(q)} 1$$

la fonction de comptage de cet ensemble. Au début du 20ème siècle, Landau a montré la généralisation suivant du TNP :

Théorème (Landau). *Soient a, q premiers entre eux alors*

$$\pi(x; q, a) = \frac{1}{\varphi(q)} \pi(x)(1 + o(1)) = \frac{1}{\varphi(q)} \frac{x}{\log x}(1 + o(1)).$$

Si $p > q$, alors p se trouve nécessairement dans l'une des progression arithmetiques dont la classe est première à q. Le Théorème de Dirichlet dit que chacune des classes de congruence dans $(\mathbb{Z}/q\mathbb{Z})^\times$ est atteinte une infinité de fois. Le Théorème de Landau dit que la proportion asymptotique de nombres premiers tombant dans une telle classe de congruence ne dépend pas de cette classe : asymptotiquement il n'y a pas de classe "privilégiée"). Dans ce chapitre on ne montrera pas le théorème de Landau mais plus simplement l'analogue du Thm de Mertens

Théorème 5.3. *On a pour a, q premiers entre eux et $x \to +\infty$*

$$\sum_{\substack{n \leqslant x \\ n \equiv a(q)}} \frac{\Lambda(n)}{n} = \frac{1}{\varphi(q)} \log(x) + O(1), \quad \sum_{\substack{p \leqslant x \\ p \equiv a(q)}} \frac{\log(p)}{p} = \frac{1}{\varphi(q)} \log(x) + O(1) \tag{5.1}$$

$$\sum_{\substack{p \leqslant x \\ p \equiv a(q)}} \frac{1}{p} = \frac{1}{\varphi(q)} \log\log(x) + O(1). \tag{5.2}$$

La méthode (due à Dirichlet) consistera à trouver une expression "agréable" du point de vue analytique de la condition de congruence

$$n \equiv a(q)$$

puis à la convertir dans la sommation sur les nombres premiers. Le point crucial est la structure de *groupe* (abélien) de l'ensemble $(\mathbb{Z}/q\mathbb{Z})^\times$.

1. Caractères d'un groupe abélien fini

Soit G un groupe abélien fini ; on note e l'élément neutre. Soit

$$\mathscr{C}(G) = \mathbf{C}^G = \{f : G \mapsto \mathbf{C}\},$$

l'espace vectoriel des fonctions de G dans $\mathbf{C}$. C'est un espace vectoriel (et même une algèbre avec la multiplication de deux fonctions) complexe de dimension $|G|$, dont une $\mathbf{C}$-base est donnée par l'ensemble

$$\mathscr{B}_0 = \{\delta_g,\ g \in G\},\ \delta_g(g') = \begin{cases} 1, & g' = g \\ 0, & g' \neq g \end{cases}.$$

On a en effet pour $f \in \mathscr{C}(G)$, la décomposition

$$f = \sum_g f(g)\delta_g,$$

et il est facile de voir que $\mathscr{B}_0$ est libre.

L'espace $\mathscr{C}(G)$ est munis d'un produit scalaire hermitien

$$\langle f, f' \rangle := \frac{1}{|G|} \sum_{g \in G} f(g)\overline{f'}(g) \tag{5.3}$$

pour lequel la base $\mathscr{B}_0$ est orthogonale :

$$\langle \delta_g, \delta'_g \rangle = \frac{1}{|G|} \delta_{g=g'} = \frac{1}{|G|} \times \begin{cases} 1 & \text{si } g = g' \\ 0 & \text{si } g \neq g' \end{cases}.$$

Bien entendu ces considérations sont valables pour un ensemble fini quelconque. Cependant, pour G un groupe abélien, $\mathscr{C}(G)$ possède un base orthonormée canonique provenant de la structure de groupe de G.

Comme G est un groupe, il agit sur lui-même par translations. Cette action induit une action de G sur $\mathscr{C}(G)$: à chaque élément g de G on associe l'endomorphisme $T_g \in \mathrm{End}(\mathscr{C}(G))$ défini par

$$T_g : \ f \to T_g f : g' \to T_g f(g') := f(gg').$$

On vérifie facilement que

$$T_g \circ T_{g'} = T_{gg'}, \ T_e = \mathrm{Id}_{\mathscr{C}(G)},$$

dont on déduit que T_g est inversible, d'inverse

$$(T_g)^{-1} = T_{g^{-1}}$$

et donc l'application

$$T : g \mapsto T_g$$

définit en fait un morphisme de groupes

$$T : G \mapsto \mathrm{Aut}(\mathscr{C}(G)).$$

De plus comme G est abélien, les éléments de $T_g, \ g \in G$ commutent entre eux :

$$T_g \circ T_{g'} = T_{gg'} = T_{g'g} = T_{g'} \circ T_g.$$

De plus, on a

$$\langle T_g f, T_g f' \rangle = \frac{1}{|G|} \sum_{g' \in G} f(gg')\overline{f'}(gg') = \frac{1}{|G|} \sum_{g \in G} f(g)\overline{f'}(g) = \langle f, f' \rangle.$$

Ainsi $\{T_g, \ g \in G\}$ est un ensemble d'isométries (pour le produit scalaire hermitien (5.3)) qui commutent entre elles deux à deux. On rappelle le théorème spectral :

Théorème (théorème spectral). *Soit $(V, \langle \ , \ \rangle)$ un espace hermitien de dimension finie et $\mathscr{T} \subset \mathrm{End}(V)$ un ensemble d'endomorphismes autoadjoints commutant entre eux deux à deux, alors il existe une base orthonormée de V formée de vecteurs propres de tous les éléments de $\mathscr{T}$.*

Dans le cas présent, le théorème spectral implique que $\mathscr{C}(G)$ possède une base orthonormée formée de vecteus propres des T_g : la preuve du théorème suivant implique qu'à normalisation et permutation près une telle base est unique :

Théorème 5.4. *Il existe une unique base orthonormée $\widehat{G} = \{\chi\}$ de $\mathscr{C}(G)$ formée de vecteurs propres de tous les T_g qui vérifient $\chi(e) = 1$ pour tout $\chi \in \widehat{G}$. On a l'égalité*

$$\widehat{G} = \mathrm{Hom}_{\mathbb{Z}}(G, \mathbf{C}^\times)$$

où $\mathrm{Hom}_{\mathbb{Z}}(G, \mathbf{C}^\times)$ désigne l'ensemble des morphismes de groupes de G vers $\mathbf{C}^\times$. Cet ensemble est un groupe : le groupe des caractères de G, ou encore le dual de G.

Preuve. L'ensemble $\{T_g, \ g \in G\}$ est une famille d'opérateur hermitiens et donc autoadjoints qui commutent deux à deux. Par le théorème spectral cette famille est diagonalisable dans une base orthonormée.

Soit $\{\psi\}$ une telle base : les ψ sont donc vecteurs propres (non-nuls) de tous les T_g et on a pour tout g,

$$T_g \psi(x) = \psi(gx) = \chi_\psi(g)\psi(x), \tag{5.4}$$

où $\chi_\psi(g)$ désigne la valeur propre de T_g associée au vecteur propre ψ. On associe donc à tout ψ, une fonction $\chi_\psi \in \mathscr{C}(G)$ définie par

$$\chi_\psi : g \to \chi_\psi(g).$$

On a

$$T_e\psi = \mathrm{Id}(\psi) = \chi_\psi(e)\psi = \psi,$$
$$T_g \circ T_{g'}\psi = T_{gg'}\psi = \chi_\psi(g)\chi_\psi(g')\psi = \chi_\psi(gg')\psi$$
$$T_g^{-1}\psi = T_{g^{-1}}\psi = \chi_\psi(g^{-1})\psi = (\chi_\psi(g))^{-1}\psi,$$

ainsi (comme $\psi \not\equiv 0$), on a pour tout $g, g' \in G$

$$\chi_\psi(e) = 1,\ \chi_\psi(gg') = \chi_\psi(g)\chi_\psi(g'),\ \chi_\psi(g^{-1}) = \chi_\psi(g)^{-1}.$$

En d'autre termes χ_ψ est un morphisme de groupes de G dans $\mathbf{C}^\times$. Notons également que comme G est fini, on a, par le théoréme de Lagrange, pour tout $\chi \in \mathrm{Hom}(G, \mathbf{C}^\times)$,

$$\chi(g^{|G|}) = \chi(e) = 1 = \chi(g)^{|G|}$$

et donc χ est à valeurs dans $\mu_{|G|}$ l'ensemble des racnes $|G|$-iémes de l'unité. En particulier $\chi_\psi(g)$ est un nombre complexe de module 1 pour tout g et

$$\langle \chi_\psi, \chi_\psi \rangle = \frac{1}{|G|}\sum_{g\in G} \chi_\psi(g)\overline{\chi_\psi(g)} = \frac{1}{|G|}\sum_{g\in G} 1 = 1. \tag{5.5}$$

Comme ψ est non-nulle, soit g' tel que $\psi(g') \neq 0$, par (7.2), on a pour tout g, $\psi(g) = \chi_\psi(g)\psi(e)$ et comme $\psi \not\equiv 0$, $\psi(e) \neq 0$, ainsi

$$\chi_\psi(g) = \frac{1}{\psi(e)}\psi(g) \ \Rightarrow\ \chi_\psi = \frac{1}{\psi(e)}\psi$$

ie. χ_ψ appartient au sous-espace $\mathbf{C}.\psi$ engendré par ψ. Comme les χ_ψ sont tous non-nuls ($\chi_\psi(e) = 1$), la famille $\{\chi_\psi\} =: \widehat{G}$ est une base orthonormée de $\mathscr{C}(G)$ qui est contenue dans $\mathrm{Hom}(G, \mathbf{C}^\times)$. Montrons qu'en fait tout élément de $\mathrm{Hom}(G, \mathbf{C}^\times)$ appartient à $\{\chi_\psi\}$:

Inversement soit $\psi \in \mathrm{Hom}(G, \mathbf{C}^\times)$; alors ψ appartient a $\mathscr{C}(G)$ et comme $\psi \not\equiv 0$ ($\psi(e) = 1$), il existe $\chi \in \widehat{G}$ tel que $\langle \psi, \chi \rangle \neq 0$. Alors, on a pour tout g,

$$0 \neq \langle \psi, \chi \rangle = \langle T_g\psi, T_g\chi \rangle = \frac{1}{|G|}\sum_{g'\in G} \psi(gg')\overline{\chi}(gg') = \psi(g)\overline{\chi}(g)\langle \psi, \chi \rangle;$$

ainsi pour tout g, $\psi(g)\overline{\chi}(g) = 1$ c'est à dire $\psi(g) = \chi(g)$. Ceci montre que

$$\widehat{G} = \mathrm{Hom}(G, \mathbf{C}^\times).$$

□

1.1. Propriétés des caractères. On extrait de la preuve précédente les propriétés importantes suivantes.

1.1.1. *Structure de groupe.* L'ensemble $\widehat{G} = \mathrm{Hom}(G, \mathbf{C}^\times)$ à une structure naturelle de groupe (on l'appelle le groupe dual de G) via la multiplication des fonctions : pour $\chi, \chi' \in \widehat{G}$ on définit

$$\chi.\chi' : g \mapsto \chi(g)\chi'(g),\ \chi^{-1} : g \mapsto \chi(g)^{-1};$$

$\chi.\chi'$ et χ^{-1} sont évidemment des caractères. L'élément neutre de $\widehat{G}$ est la fonction constante égale à 1, qu'on note

$$\chi_0 : g \mapsto 1$$

et qu'on appelle *le caractère trivial.*

Dit autrement, et de façon pédante, $\widehat{G}$ est un sous-groupe du groupe des unités de l'algèbre $\mathscr{C}(G)$ munie de la multiplication des fonctions, $f, f' \in \mathscr{C}(G)$:

$$f.f' : g \mapsto f(g)f'(g).$$

1.1.2. *Unitarité.* On a montré que

$$|\widehat{G}| = \dim \mathscr{C}(G) = |G|;$$

en particulier (Théorème de Lagrange) pour tout $\chi \in \widehat{G}$, $\chi^{|G|} = \chi_0$ c'est à dire que pour tout $g \in G$

$$\chi(g)^{|G|} = 1,$$

autrement dit, les caractères sont à valeurs dans le groupe des racines $|G|$-ièmes de l'unité

$$\mu_{|G|} = \{\zeta \in \mathbf{C},\ \zeta^{|G|} = 1\}.$$

On dit qu'ils sont *unitaires*. En particulier pour tout g

$$\chi(g)^{-1} = \overline{\chi(g)},\ \textit{i.e.}\ \chi^{-1} = \overline{\chi}$$

le conjugué complexe de χ.

1.1.3. *Relations d'orthogonalité.*

Proposition 5.5. *On a :*

$$\delta_{\chi=\chi'} = \frac{1}{|G|} \sum_{g' \in G} \chi(g')\overline{\chi'}(g') \tag{5.6}$$

$$\delta_{g=g'} = \frac{1}{|G|} \sum_{\chi \in G} \overline{\chi}(g)\chi(g') \tag{5.7}$$

Preuve. La première relation est la relation d'orthogonalité (5.5) :

$$\langle \chi, \chi' \rangle = \delta_{\chi=\chi'}.$$

Pour montrer la seconde relation considérons la decomposition de δ_g dans la base $\widehat{G}$:

$$\delta_g = \sum_{\chi} \langle \delta_g, \chi \rangle \chi = \frac{1}{|G|} \sum_{\chi} (\sum_{g' \in G} \delta_g(g')\overline{\chi}(g')).\chi = \frac{1}{|G|} \sum_{\chi} \overline{\chi}(g)\chi \tag{5.8}$$

évaluant cette identité en g', on obtient la relation (5.7). □

Remarque 5.6. L'expression (5.8) est la *décomposition de Fourier* de la fonction δ_g. C'est cette expression qui va nous être utile dans la suite.

1.2. Caractères d'un groupe cyclique. Soit $G =< g >$ un groupe cyclique de générateur g ; notons q son ordre ; un caractère χ de g est complètement déterminé par sa valeur en g, $\chi(g)$: pour tout $g' \in G$, on pose $g' = g^m$, $m \in \mathbb{Z}$ et $\chi(g') = \chi(g)^m$. Notons que cela ne dépend pas du choix de $m \in \mathbb{Z}$: si $g' = g^{m'}$ alors $m' \equiv m (\mathrm{mod}\, q)$ et

$$\chi(g^{m'}) = \chi(g)^m \chi(g)^{m'-m} = \chi(g^m)$$

car $\chi(g)$ est une racine q-ième de l'unité. Ainsi toute racine q-ième de l'unité ζ définit de manière unique un caractère de G en posant

$$\chi(g^m) = \zeta^m.$$

En d'autre termes on a la

Proposition 5.7. *Soit G un groupe cyclique d'ordre q. Le choix d'un générateur de G détermine un isomorphisme entre le groupe des racines q-ièmes de l'unité et le groupe $\widehat{G}$. Cet isomorphisme est donné par*

$$\zeta \in \mu_q \mapsto \chi : g^m \to \chi(g^m) := \zeta^m.$$

Dans le cas du groupe $\mathbb{Z}/q\mathbb{Z}$, les caractères (dits caractères additifs) sont donnés explicitement par les fonctions

$$\psi_n : x(\bmod q) \mapsto \mathrm{e}(n\frac{x}{q}).$$

Notons que ψ_n ne dépend que de la classe de n modulo q et

$$n(\bmod q) \mapsto \psi_n$$

est l'isomorphisme recherché.

Remarque 5.8. Notons que μ_q est un groupe cyclique d'ordre q engendré par l'exponentielle complexe

$$\zeta_q = \mathrm{e}(\frac{1}{q}),\ \mathrm{e}(x) := \exp(2\pi i x).$$

On a donc

$$\widehat{G} \simeq \mu_q \simeq \mathbb{Z}/q\mathbb{Z} \simeq G.$$

Notons que c'est isomorphisme n'est pas canonique car il dépend du choix du générateur g. On va voir (dans les exercices), plus généralement, que pour tout groupe abélien G, on a $G \simeq \widehat{G}$.

2. Caractères de Dirichlet

On va maintenant appliquer cette théorie aux groupes multiplicatifs $(\mathbb{Z}/q\mathbb{Z})^\times$.

Définition 5.9. *Soit $q \geqslant 1$ un entier ; les caractères du groupe abélien $(\mathbb{Z}/q\mathbb{Z})^\times$ sont appelés caractères de Dirichlet de module q. Le caractère trivial (la fonction constante égale à 1) sera noté χ_0.*

2.1. Fonction arithmétique associé à un caractère de Dirichlet. Soit $\chi \in \widehat{(\mathbb{Z}/q\mathbb{Z})^\times}$ un caractère. On prolonge cette fonction par zero en une fonction sur $\mathbb{Z}/q\mathbb{Z}$ puis on la prolonge en une fonction sur $\mathbb{Z}$ en la composant avec la réduction modulo q :

$$\chi(n) = \begin{cases} \chi(n \bmod q), & (n,q) = 1 \\ 0 & (n,q) > 1. \end{cases}$$

Par abus de langage, la fonction arithmétique ainsi obtenue sera encore appelée "caractère de Dirichlet". En particulier χ définit une fonction arithmétique, périodique de période q, qui s'annule sur les entiers non-premiers à q ; c' est une fonction arithmétique complètement multiplicative :

$$\forall m, n \in \mathbb{Z},\ \chi(mn) = \chi(m)\chi(n).$$

Les relations d'orthogonalité (5.6) et (5.7) s'écrivent alors

$$\delta_{\chi=\chi'} = \frac{1}{\varphi(q)} \sum_{a \bmod q} \chi(a)\overline{\chi'}(a) \tag{5.9}$$

Pour $(ab, q) = 1$,

$$\delta_{a \equiv b \bmod q} = \frac{1}{\varphi(q)} \sum_{\chi} \overline{\chi}(a)\chi(b). \tag{5.10}$$

On considère alors la série de Dirichlet associée à cette fonction

$$L(\chi, s) := \sum_{n \geqslant 1} \frac{\chi(n)}{n^s}.$$

Comme $|\chi(n)| \leqslant 1$, cette série est absolument convergente pour $\Re e s > 1$ et dans ce domaine, on a

$$L(\chi, s) = \prod_p (1 - \frac{\chi(p)}{p^s})^{-1}.$$

On obtient ainsi une série L au sens de la section 4. Dasn ce cas precis $V_p = \mathbf{C}$ et l'endomorphisme $\Phi_p : x \to \chi(p)x$ est la multiplication par le scalaire $\chi(p)$.

Proposition 5.10. *Soit $\chi \bmod q$ un caractère de Dirichlet.*

– *Si $\chi = \chi_0$, on a pour $\Re e s > 1$,*

$$L(\chi_0, s) = \prod_{p|q} (1 - \frac{1}{p^s})\zeta(s)$$

qui admet un prolongement holomorphe au demi-plan $\Re e s > 0$.

– *Si $\chi \neq \chi_0$, la série $L(\chi, s)$ converge uniformément sur les compacts du demi-plan $\Re e s > 0$ et définit donc une fonction holomorphe dans ce domaine. Plus précisement on a pour $\Re e s > 0$*

$$\sum_{1 \leqslant n \leqslant X} \frac{\chi(n)}{n^s} = L(\chi, s) + O(\frac{q|s|}{\sigma} X^{-\sigma}). \tag{5.11}$$

Preuve. Si $\chi = \chi_0$, alors

$$L(\chi_0, s) = \prod_p (1 - \frac{\chi_0(p)}{p^s})^{-1} = \prod_{p,\ (p,q)=1} (1 - \frac{1}{p^s})^{-1} = \prod_{p|q} (1 - \frac{1}{p^s})\zeta(s).$$

L'énoncé résulte du prolongement méromorphe de ζ au demi-plan $\Re s > 0$ (cf. l'exercice 4.24).

Si χ est non trivial, on a pour tout intervalle I de longueur q exactement

$$\sum_{n \in I} \chi(n) = 0$$

en effet I étant de longueur q contient exactement une fois chaque classe de $\mathbb{Z}/q\mathbb{Z}$ et l'égalité résulte de la relation d'orthogonalité (5.9) en prenant $\chi' = \chi_0$. Ainsi pout tout t, on a

$$|M_\chi(t)| \leqslant q.$$

Par intégration par partie, on a alors

$$\sum_{1 \leqslant n \leqslant X} \frac{\chi(n)}{n^s} = X^{-s} M_\chi(X) - 1 + s \int_1^X M_\chi(t) t^{-s-1} dt.$$

Comme $M_\chi(t)$ est bornée, pour $\sigma = \Re e s > 0$, le premier terme tend vers 0 et l'intégrale est absolument convergente ; ainsi la série converge. Par le même argument, on a

$$\begin{aligned} L(\chi, s) - \sum_{1 \leqslant n \leqslant X} \frac{\chi(n)}{n^s} = \sum_{n > X} \frac{\chi(n)}{n^s} &= \left[M_\chi(t) t^{-s}\right]_X^\infty + s \int_X^\infty M_\chi(t) t^{-s-1} dt \\ &\ll q X^{-\sigma} + \frac{|s|}{\sigma} q X^{-\sigma} \to 0,\ X \to +\infty \end{aligned}$$

ce qui démontre (5.11). Cette majoration montre que $\sum_{1 \leqslant n \leqslant X} \frac{\chi(n)}{n^s}$ converge uniformément vers $L(\chi, s)$ sur les compacts du demi-plan $\Re e s > 0$. On en déduit l'holomorphie de $L(\chi, s)$ dans ce domaine. □

3. Début de la preuve du Théorème 5.3

Par des arguments élémentaires il suffit de prouver la première identité : on a par (5.10)

$$\sum_{\substack{n\leqslant x\\ n\equiv a(q)}} \frac{\Lambda(n)}{n} = \frac{1}{\varphi(q)} \sum_{\chi(q)} \overline{\chi}(a) S_\chi(x) \tag{5.12}$$

avec

$$S_\chi(x) = \sum_{n\leqslant x} \frac{\chi(n)}{n} \Lambda(n).$$

Si $\chi = \chi_0$,

$$S_{\chi_0}(x) = \sum_{\substack{n\leqslant x\\ (n,q)=1}} \frac{\Lambda(n)}{n} = \sum_{n\leqslant x} \frac{\Lambda(n)}{n} - \sum_{p|q} \log p \sum_{\substack{\alpha\geqslant 1\\ p^\alpha\leqslant x}} \frac{1}{q^\alpha} = \log(x) + O_q(1)$$

et donc la contribution de ce terme à la somme (5.12) est en

$$\log(x) + O_q(1).$$

Pour conclure il suffit de montrer que pour tout $\chi \neq \chi_0$,

$$S_\chi(x) = \sum_{n\leqslant x} \frac{\chi(n)}{n} \Lambda(n) = O_q(1).$$

Pour calculer $S_\chi(x)$, on considère la somme

$$T_\chi(x) = \sum_{n\leqslant x} \log(n) \frac{\chi(n)}{n};$$

par integration par partie et utilisant le fait que $M_\chi(x)$ est bornée si $\chi \neq \chi_0$, on voit que

$$T_\chi(x) = O(1).$$

D'autre part, utilisant l'égalité $\log = 1 * \Lambda$, on a

$$\begin{aligned} T_\chi(x) &= \sum_{a\leqslant x} \frac{\chi(a)}{a} \Lambda(a) \sum_{b\leqslant x/a} \frac{\chi(b)}{b} \\ &= \sum_{a\leqslant x} \frac{\chi(a)}{a} \Lambda(a) \big(L(\chi,1) + O(\frac{a}{x})\big) \\ &= L(\chi,1) S_\chi(x) + O(1) \end{aligned}$$

par la majoration de Chebycheff. Ainsi si on montre que

$$L(\chi,1) \neq 0,$$

on aura

$$S_\chi(x) = O(1), \tag{5.13}$$

se qui concluera la preuve du Théorème 5.3. La non-annulation de $L(\chi,s)$ en $s=1$ est le point clef de la preuve du Théorème de Dirichlet ; elle sera montrée dans la prochaine Section

4. Non-annulation des fonctions L de Dirichlet au point 1

Théorème 5.11 (Dirichlet)**.** *Soit $\chi(\mathrm{mod}\, q)$ un caractère non-trivial, alors*

$$L(\chi, 1) \neq 0.$$

On va donner deux preuves de ce théorème : l'une n'utilisant que de l'analyse réelle, l'autre passant par l'analyse complexe. Quelque soit la preuve une point clef est l'utilisation d'argument de positivité.

4.1. Preuve par l'analyse complexe. L'idée est la suivante : on considère le produit de toutes les fonctions L de Dirichlet

$$\prod_{\chi(q)} L(\chi, s) = L(\chi_0, s) \prod_{\chi \neq \chi_0} L(\chi, s) = L_q(s).$$

C'est une série de Dirichlet (celle de la fonction multiplicative $n \mapsto a_q(n)$ obtenue comme convolée des caractères de module q),

$$L_q(s) = \sum_{n \geqslant 1} \frac{a_q(n)}{n^s}$$

et on va voir que les coefficients $a_q(n)$ sont positifs ou nuls pour tout $n \geqslant 1$; on va également montrer que pour n premier avec q,

$$a_q(n^{\varphi(q)}) \geqslant 1.$$

On en déduit que l'abscisse de convergence σ_q de a_q vérifie $\sigma_q \geqslant 1/\varphi(q)$ (on a a priori $\sigma_q \leqslant 1$ car a_q est la convolée de fonctions arithmétiques d'abscisses de convergence égales à 1) : en effet, pour $\sigma = 1/\varphi(q)$

$$\sum_{n \geqslant 1} a_q(n)/n^\sigma \geqslant \sum_{\substack{m \geqslant 1 \\ (m,q)=1}} a_q(m^{\varphi(q)})/m^{\varphi(q)\sigma} \geqslant \sum_{\substack{m \geqslant 1 \\ (m,q)=1}} 1/m = +\infty.$$

Par la proposition 5.10, $L_q(s)$ admet un prolongement méromorphe au demi-plan $\Re s > 0$ dont le seul pùle possible dans ce domaine est en $s = 1$. Si on suppose maintenant qu'il existe un caractère χ tel que $L(\chi, s)$ s'annule en $s = 1$, comme le pùle de $L(\chi_0, s)$ en 1 est simple, la fonction $L(s)$ sera holomorphe en $s = 1$ et donc dans tout le demi-plan $\{s,\ \Re s > 0\}$. Le Lemme de Landau ci-dessous, l'holomorphie de $L_q(s)$ dans le demi-plan $\{s,\ \Re s > 0\}$ et le fait que les $a_q(n)$ sont positifs ou nuls implique alors que l'abscisse de convergence de $L_q(s)$ est en fait $\leqslant 0$, contradiction !

Lemme 5.12 (Landau)**.** *Soit*

$$L(s) = \sum_{n \geqslant 1} \frac{f(n)}{n^s}$$

une série de Dirichlet d'abscisse de convergence σ_f finie et dont les coefficients $f(n)$ sont positifs ou nuls ; alors $L(s)$ n'admet pas de prolongement holomorphe au voisinage du point σ_f.

Preuve. Quitte a remplacer $L(s)$ par $L(s - \sigma_f)$ on peut supposer $\sigma_f = 0$. Supposons que $L(s)$ admette un prolongement holomorphe dans un disque ouvert D centré en $\sigma_f = 0$ alors $L(s)$ et toutes ses dérivées definissent des fonctions holomorphes dans le domaine $D \cup \{s,\ \mathrm{Re}\, s > 0\}$. Remarquons que l'on a

$$\sum_{n \geqslant 1} f(n) = L(0).$$

C'est une conséquence du théorème de convergence monotone et on rappelle l'argument ci-dessous : comme on a $f(n) \geqslant 0$, la fonction

$$\sigma \in]0,1] \mapsto L(\sigma) = \sum_{n \geqslant 1} f(n)/n^{\sigma}$$

est décroissante et est majorée par sa limite quand $\sigma \to 0^+$ qui est $L(0)$. D'autre part pour tout $N \geqslant 1$,

$$\sum_{n \leqslant N} f(n) = \lim_{\sigma \to 0^+} \sum_{n \leqslant N} f(n)/n^{\sigma} \leqslant \lim_{\sigma \to 0^+} L(\sigma) = L(0),$$

ce qui montre la convergence de la somme précédente. On calcule la limite en notant que pour tout $\sigma > 0$, on a

$$L(\sigma) = \sum_{n \geqslant 1} f(n)/n^{\sigma} \leqslant \sum_{n \geqslant 1} f(n),$$

et en faisant tendre σ vers 0. Considérons la dérivée d'ordre k de $L(s)$: pour $\Re s > 0$ elle est donnée par

$$L(s)^{(k)} = (-1)^k \sum_{n \geqslant 1} \frac{f(n)(\log n)^k}{n^s}.$$

Comme $f(n)(\log n)^k$ est positif ou nul, le même argument que précédemment donne que

$$(-1)^k \sum_{n \geqslant 1} f(n)(\log n)^k = L^{(k)}(0).$$

Soit $\sigma < 0$ et contenu dans D, $L(\sigma)$ se calcule par son développement de Taylor en 0 :

$$L(\sigma) = \sum_{k \geqslant 0} \frac{L^{(k)}(0)}{k!} \sigma^k = \sum_{k \geqslant 0} \frac{(-\sigma)^k}{k!} \sum_{n \geqslant 1} f(n)(\log n)^k.$$

Comme $(-\sigma)^k \geqslant 0$ les terme de cette double somme sont positifs ou nuls et on peut les permuter :

$$L(\sigma) = \sum_{n \geqslant 1} f(n) \sum_{k \geqslant 0} \frac{(-\sigma \log n)^k}{k!} = \sum_{n \geqslant 1} f(n) \exp(-\sigma \log n) = \sum_{n \geqslant 1} \frac{f(n)}{n^{\sigma}}.$$

Ainsi la série $L(s)$ convergerait pour un $\sigma < 0$ ce qui contredit le fait que $\sigma_f = 0$. □

4.2. Positivité des $a_q(n)$. La fonction $n \mapsto a_q(n)$ étant multiplicative, il suffit de montrer que $a_q(p^k) \geqslant 0$ pour p premier et $k \geqslant 0$. Il suffit donc de montrer que les coefficients de

$$L_{q,p}(s) = \prod_{\chi} L_p(\chi, s) = \prod_{\chi} (1 - \chi(p) p^{-s})^{-1} = \sum_{k \geqslant 1} \frac{a_q(p^k)}{p^{ks}}$$

sont positifs ou nuls. Si p divise q, $L_{q,p}(s) = 1$; on peut donc supposer que p est premier avec q. Posant $z = p^{-s}$ (de sorte que $|z| < 1$ si $\Re s > 0$), on considère la série entière (convergente)

$$E(z) = \prod_{\chi} (1 - \chi(p) z)^{-1} = \sum_{k \geqslant 0} a_q(p^k) z^k.$$

Prenant le logarithme, on a

$$\begin{aligned} \log(E(z)) &= \sum_{\chi} \log((1 - \chi(p) z)^{-1}) = \sum_{\chi} \sum_{k \geqslant 1} \chi(p)^k \frac{z^k}{k} = \sum_{\chi} \sum_{k \geqslant 1} \chi(p^k) \frac{z^k}{k} \\ &= \sum_{k \geqslant 1} \frac{z^k}{k} \sum_{\chi} \chi(p^k) = \sum_{\substack{k \geqslant 1 \\ p^k \equiv 1 (q)}} \varphi(q) \frac{z^k}{k}. \end{aligned}$$

On voit donc que $\log(E(z))$ est un série entière à coefficient positifs ou nuls ; comme

$$E(z) = \exp(\log(E(z))) = 1 + \log(E(z)) + \frac{\log(E(z))^2}{2} + \cdots + \frac{(\log(E(z)))^l}{l!} + \ldots$$

on voit que les coefficients de $E(z)$ sont eux aussi positifs ou nuls. Notons également que pour $k = \varphi(q)$,

$$p^{\varphi(q)} \equiv 1(q)$$

car (théorème de Lagrange) l'ordre d'un élément d'un groupe (ici $p(\mathrm{mod}\, q)$) divise toujours l'ordre du groupe (ici $(\mathbb{Z}/q\mathbb{Z})^\times$). On voit donc que le coefficient d'ordre $\varphi(q)$ de $\log(E(z))$ vaut 1 et on en déduit que le coefficient d'ordre $\varphi(q)$ de $E(z)$ est $\geqslant \frac{1}{\varphi(q)!}$. Cela permettrait déjà d'en déduire que l'abscisse de convergence de $L_q(s)$ est $\geqslant 1/\varphi(q)$.

On va faire un peu mieux et calculer complètement $L_q(s)$. Soit e_p l'ordre de $p(\mathrm{mod}\, q)$ dans $(\mathbb{Z}/q\mathbb{Z})^\times$, on a

$$\log(E(z)) = \frac{\varphi(q)}{e_p} \sum_{k\geqslant 1} \frac{p^{e_p k}}{k} = \frac{\varphi(q)}{e_p} \log((1 - z^{e_p})^{-1}) = \log((1 - z^{e_p})^{-\frac{\varphi(q)}{e_p}})$$

et donc

$$E(z) = \frac{1}{(1 - z^{e_p})^{\frac{\varphi(q)}{e_p}}} = (1 + z^{e_p} + z^{2e_p} + \ldots)^{\frac{\varphi(q)}{e_p}},$$

et

$$L_{q,p}(s) = \frac{1}{(1 - \frac{1}{p^{e_p s}})^{\frac{\varphi(q)}{e_p}}} = \sum_{k\geqslant 0} \frac{a_q(p^k)}{p^{ks}}.$$

On en déduit que les $a_q(p^k)$ sont des *entiers positifs ou nuls* tels que $a_q(p^k) \geqslant 1$ si k est un multiple de $\varphi(q)$ et donc que pour tout entier n premier avec q,

$$a_q(n^{\varphi(q)}) \geqslant 1.$$

4.3. Preuve élémentaire. Dans cette section on donne une autre preuve du théorème de non-annulation de Dirichlet qui n'utilise pas l'analyse complexe. Cette preuve est due à H. Iwaniec. Rappelons qu'on veut montrer que si χ est non-trivial $L(\chi, 1) \neq 0$.

La preuve se subdivise en deux cas suivant que χ est un caractère réel (ie. $\chi(\mathbb{Z}) \subset \mathbb{R}$ ce qui équivaut au fait que χ est d'ordre 2, $\chi^2 = \chi_0$) ou non. Soit χ un caractère non trivial, on considère à nouveau la somme

$$S_\chi(x) = \sum_{n\leqslant x} \frac{\chi(n)}{n} \Lambda(n)$$

qui a été évaluée dans la section3 : on a vue en cette occasion que

$$L(\chi, 1) \neq 0 \Longrightarrow S_\chi(x) = O_q(1).$$

On évalue cette somme d'une manière différente : utilisant que $\Lambda = \mu * \log$, on a

$$\begin{aligned} S_\chi(x) &= \sum_{n\leqslant x} \frac{\chi(n)}{n} \sum_{a|n} \mu(a) \log(n/a) = \sum_{n\leqslant x} \frac{\chi(n)}{n} \sum_{a|n} \mu(a)(\log(n) - \log a) \\ &= \sum_{n\leqslant x} \frac{\chi(n)}{n} \sum_{a|n} \mu(a)(-\log a) \end{aligned}$$

car $\sum_{a|n}\mu(a)\log(n) = \log(n)\delta_{n=1} = 0$. Utilisant de plus que $\sum_{a|n}\mu(a)\log(x) = \delta_{n=1}\log(x)$, on obtient

$$\begin{aligned}
S_\chi(x) &= -\log(x) + \sum_{n\leqslant x}\frac{\chi(n)}{n}\sum_{a|n}\mu(a)(\log x - \log a)\\
&= -\log(x) + \sum_{n\leqslant x}\frac{\chi(n)}{n}\sum_{a|n}\mu(a)\log\frac{x}{a}\\
&= -\log(x) + \sum_{a\leqslant x}\frac{\chi(a)}{a}\mu(a)\log\frac{x}{a}\sum_{b\leqslant x/a}\frac{\chi(b)}{b}\\
&= -\log(x) + \sum_{a\leqslant x}\frac{\chi(a)}{a}\mu(a)\log\frac{x}{a}(L(\chi,1) + O(\frac{a}{x}))\\
&= -\log(x) + L(\chi,1)\sum_{a\leqslant x}\frac{\chi(a)}{a}\mu(a)\log\frac{x}{a} + O(1)
\end{aligned}$$

car $\sum_{a\leqslant x}|\chi(a)\mu(a)|\log\frac{x}{a} = O(x)$. Ainsi, si $L(\chi,1) = 0$, on a

$$S_\chi(x) = -\log(x) + O(1).$$

Rappelons que si $\chi = \chi_0$, on a

$$S_{\chi_0}(x) = \log x + O(1)$$

et ainsi on obtient utilisant les résultats de la section (3)

$$S_\chi(x) = \delta_\chi\log(x) + O(1) \text{ avec } \delta_\chi = \begin{cases} 1 & \text{si } \chi = \chi_0\\ 0 & \text{si } \chi \neq \chi_0,\ L(\chi,1)\neq 0\\ -1 & \text{si } \chi\neq\chi_0,\ L(\chi,1) = 0\end{cases}.$$

On a (par (5.10)) $\delta_{n\equiv 1(q)} = \frac{1}{\varphi(q)}\sum_{\chi(q)}\chi(n)$ et donc

$$\sum_{\substack{n\leqslant x\\ n\equiv 1(q)}}\frac{\Lambda(n)}{n} = \frac{1}{\varphi(q)}\sum_\chi S_\chi(x) = \frac{\log x}{\varphi(q)}\sum_{\chi(q)}\delta_\chi + O(1).$$

Comme

$$\sum_{\substack{n\leqslant x\\ n\equiv 1(q)}}\frac{\Lambda(n)}{n} \geqslant 0$$

on voit que

$$\sum_\chi \delta_\chi = 1 + \sum_{\chi\neq\chi_0}\delta_\chi \geqslant 0$$

et donc que

$$\sum_{\chi\neq\chi_0}\delta_\chi \geqslant -1.$$

Donc dans l'ensemble $\{\chi\neq\chi_0\}$, il y a au plus UN χ tel que $\delta_\chi = -1$ (ie. tel que $L(\chi,1) = 0$). Maintenant si $\chi\neq\chi_0$ est un caractère non-réel (ie. $\chi\neq\overline{\chi}$) alors si on avait $L(\chi,1) = 0$, on aurait aussi $L(\overline{\chi},1) = \overline{L(\chi,1)} = 0$ ce qui contredit la remarque précédente. Ainsi

$$\textit{pour } \chi\neq\overline{\chi},\ \textit{on a } L(\chi,1)\neq 0.$$

4.4. Le cas χ réel. On voit que l'argument précédent ne s'applique pas si $\chi = \overline{\chi}$ (ou ce qui revient au même si $\chi^2 = \chi_0$). Dans ce cas là, on utilise un argument différent :

Soit $\tau_\chi = 1 * \chi$. On considère la somme

$$U_\chi(x) = \sum_{n \leqslant x} \frac{(1*\chi)(n)}{n^{1/2}}.$$

On remarque, d'une part que τ_χ est multiplicative et que d'autre part, pour p premier et $\alpha \geqslant 0$,

$$\tau_\chi(p^\alpha) = 1 + \chi(p) + \chi(p^2) + \cdots + \chi(p^\alpha) = 1 + \chi(p) + \chi(p)^2 + \cdots + \chi(p)^\alpha \geqslant 0$$

car $\chi(p) = \pm 1$; de plus, si α est pair, alors $\tau_\chi(p^\alpha) \geqslant 1$.

On en déduit que pour tout n

$$\tau_\chi(n) \geqslant 0, \ \tau_\chi(n^2) \geqslant 1.$$

Il en résulte que

$$U_\chi(x) \geqslant \sum_{n^2 \leqslant x} \frac{1}{\sqrt{n^2}} = \frac{1}{2}\log(x) + O(1).$$

D'autre part on évalue $U_\chi(x)$ d'une manière similaire à précédement avec une variante appelée *méthode de l'hyperbole* : soit $1 \leqslant y < x$ un paramètre (on va prendre $y = x^{1/2}$), on a

$$\begin{aligned} U_\chi(x) &= \sum_{ab \leqslant x} \frac{\chi(a)}{(ab)^{1/2}} = \sum_{a \leqslant y} \sum_{b \leqslant x/a} \cdots + \sum_{a > y} \sum_{b \leqslant x/a} \cdots \\ &= \sum_{a \leqslant y} \frac{\chi(a)}{a^{1/2}} \Big(2(\frac{x}{a})^{1/2} + c + O((\frac{a}{x})^{1/2}) \Big) + \sum_{1 \leqslant b \leqslant x/y} \frac{1}{b^{1/2}} \sum_{y < a \leqslant x/b} \frac{\chi(a)}{a^{1/2}} \end{aligned}$$

En effet (le démontrer) on a

$$\sum_{n \leqslant x} n^{-1/2} = 2x^{1/2} + c + O(x^{-1/2})$$

avec c une constante absolue. On a (cf. (5.11))

$$\sum_{a \leqslant y} \frac{\chi(a)}{a} = L(\chi, 1) + O(1/y)$$

et

$$\sum_{y < a \leqslant x/b} \frac{\chi(a)}{a^{1/2}} = L(\chi, 1/2) + O((x/b)^{-1/2}) - L(\chi, 1/2) + O(y^{-1/2}) = O((x/b)^{-1/2}) + O(y^{-1/2})$$

et ainsi

$$U_\chi(x) = 2x^{1/2} L(\chi, 1) + O(x^{1/2}/y) + O(y/x^{1/2}) + cL(\chi, 1/2) + O(y^{-1/2}) + O(x^{1/2}/y).$$

Prenant $y = x^{1/2}$, on obtient

$$\log x + O(1) \leqslant U_\chi(x) = 2x^{1/2} L(\chi, 1) + O(1)$$

et donc en faisant tendre x vers $+\infty$, on a $L(\chi, 1) \neq 0$. □

5. Exercices

Exercice(s) 5.13. $\widehat{G}$ est un groupe abélien, on peut donc considérer son groupe des caractères $\widehat{\widehat{G}}$: montrer que l'application $G \to C(\widehat{G})$

$$g \to \tilde{g} : \chi \to \chi(g)$$

a son image dans $\widehat{\widehat{G}} = \mathrm{Hom}_{\mathbb{Z}}(\widehat{G}, \mathbf{C}^{\times})$ et est un isomorphisme.

Exercice(s) 5.14. Montrer que si G est cyclique, $G \simeq \widehat{G}$ (on calculera $\widehat{\mathbb{Z}/n\mathbb{Z}}$). Montrer que $\widehat{G_1 \times G_2} \simeq \widehat{G_1} \times \widehat{G_2}$. En déduire que pour tout groupe abélien fini $G \simeq \widehat{G}$.

Exercice(s) 5.15. Soit $F \in \mathscr{C}(G)$, la *transformée de Fourier* $\widehat{f}$ *de* F *est la fonction de* $\widehat{G} \to \mathbf{C}$ *définie par*

$$\widehat{f}(\chi) = \langle F, \chi \rangle = \frac{1}{|G|} \sum_g F(g)\overline{\chi}(g).$$

– *Montrer que (formule d'inversion de Fourier)*

$$F = \sum_{\chi} \widehat{f}(\chi).\chi.$$

– *Que vaut* $\widehat{\widehat{f}}$ *?*

Exercice(s) 5.16. (Induction/Restriction) Soit $H < G$ un sous groupe de G,
– montrer que si χ est un caractère de G alors $\chi_{|H}$ est un caractère de H.
– Soit $res_{|H}$ l'application (restriction à H). Montrer que $\ker res_{|H}$ peut s'identifier à $\widehat{G/H}$.
– Montrer que $\mathrm{res}_{|H}$ est surjective : ie. pour tout $\chi' \in \hat{H}$, il existe $\chi \in \widehat{G}$ qui prolonge χ'. Pour cela on considérera la fonction

$$F(g) = \sum_{\chi \in \widehat{G}} \chi(g).$$

Calculer cette fonction. Soit χ' un caractère de H. Montrer que

$$\sum_{h \in H} \overline{\chi'}(h)F(h) = |\{\chi \in \widehat{G},\ \chi_{|H} = \chi'\}|.$$

On a donc la suite exacte

$$1 \to \widehat{G/H} \to \widehat{G} \to \hat{H} \to 1$$

qui est duale de la suite

$$1 \to H \to G \to G/H \to 1.$$

Exercice(s) 5.17. Soit $q \geqslant 1$ et $\zeta_q(s) = \prod_{\chi(q)} L(\chi, s) = \sum_{n \geqslant 1} \frac{r_q(n)}{n^s}$. Montrer que $r_q(n) \geqslant 0$. Pour cela on pourra d'abord montrer que c'est le cas de la série de Dirichlet $-\frac{\zeta_q'(s)}{\zeta_q(s)}$.

Exercice(s) 5.18. soient χ_1 et χ_2 deux caractères quadratiques. Montrer que

$$\zeta(s)L(\chi_1, s)L(\chi_2, s)L(\chi_1\chi_2, s)$$

est une série de Dirichlet à coefficients positifs.

Exercice(s) 5.19. Soit $\chi(q)$ un caractère non-trivial, montrer que pour $\sigma = \Re es \in]0, 1]$,

$$L(\chi, s) \ll (q|s|)^{1-\sigma} \log(2q|s|),\ L'(\chi, s) \ll (q|s|)^{1-\sigma} \log^2(2q|s|)$$

CHAPITRE 6

Le théorème des nombres premiers dans les progressions arithmétiques (d'après Newman)

Dans ce chapitre on va donner une preuve du théorème de la progression arithmétique sous sa forme "forte" ; cette preuve est une adaptation de la preuve élégante du théorème des nombres premiers de Newman.

Théorème 6.1. *Soit $a, q \geqslant 1$ des entiers premiers entre eux, on a pour $x \to \infty$*

$$\pi(x; q, a) = \sum_{\substack{p \leqslant x \\ p \equiv a \,(\mathrm{mod}\, q)}} 1 = \frac{1}{\varphi(q)} \frac{x}{\log x}(1 + o_q(1)).$$

De manière équivalente, quand $x \to +\infty$,

$$\psi(x; q, a) = \sum_{\substack{n \leqslant x \\ n \equiv a \,(\mathrm{mod}\, q)}} \Lambda(n) = \frac{1}{\varphi(q)} x(1 + o_q(1)).$$

En particulier, en prenant $q = 1$, on obtient

Théorème 6.2 (Théorème des nombres premiers)**.** *On a pour $x \to \infty$*

$$\pi(x) = \sum_{p \leqslant x} 1 = \frac{x}{\log x}(1 + o(1)),$$

$$\psi(x) = \sum_{n \leqslant x} \Lambda(n) = x(1 + o(1)).$$

Ce théorème est conséquence du théorème de non-annulation suivant :

Théorème 6.3. *Soit $\chi \,(\mathrm{mod}\, q)$ un caractère de Dirichlet (trivial ou non), alors $L(\chi, s)$ ne s'annule pas pour $\Re s = 1$.*

1. Le Théorème 6.3 implique le Théorème 6.1

Il suffit de démontrer la seconde équivalence. Pour $\Re s > 1$, on a

$$L(\Lambda.\delta_{a \,(\mathrm{mod}\, q)}, s) = \sum_{n \equiv a \,(\mathrm{mod}\, q)} \frac{\Lambda(n)}{n^s} = \frac{1}{\varphi(q)} \sum_{\chi \,(\mathrm{mod}\, q)} \overline{\chi}(a)(-\frac{L'(\chi, s)}{L(\chi, s)}).$$

Pour chaque χ la série

$$-\frac{L'(\chi, s)}{L(\chi, s)} = \sum_{n \geqslant 1} \frac{\Lambda(n)\chi(n)}{n^s}$$

se prolonge méromorphiquement au demi-plan $\{s,\ \Re s > 0\}$ avec des pôles simples aux points ρ où $L(\chi, s)$ s'annule ou bien à un pôle et de résidu

$$\mathrm{res}_{s=\rho} -\frac{L'(\chi, s)}{L(\chi, s)} = -\mathrm{ord}_{s=\rho} L(\chi, s).$$

En particulier, comme $L(\chi, s)$ ne s'annule pas sur la droite $\Re s = 1$ (par le Théorème 6.3), $-\frac{L'(\chi,s)}{L(\chi,s)}$ n'a pas de pole sur cette droite sauf si $\chi = \chi_0$ est le caratère trivial, auquel cas $-\frac{L'(\chi_0,s)}{L(\chi_0,s)}$ a un unique pole simple en $s = 1$ de résidu 1.

En particulier $L(\Lambda.\delta_{a(\mathrm{mod}\, q)}, s)$ se prolonge méromorphiquement à $\{\Re s > 0\}$ et est holomorphe dans le demi-plan $\Re s \geqslant 1$ sauf au point $s = 1$ où elle admet un pole simple de résidu $\frac{1}{\varphi(q)}$.

Rappelons que par Chebycheff

$$\psi(x; q, a) \leqslant \psi(x) \ll x$$

et donc, par integration par partie, on a pour $\Re s > 1$

$$L(\Lambda.\delta_{a(\mathrm{mod}\, q)}, s) = [\psi(t; q, a)t^{-s}]_1^\infty - \int_1^\infty \psi(t; q, a)(t^{-s})' dt = -s\int_1^\infty \psi(t; q, a)t^{-s}\frac{dt}{t},$$

par ailleurs pour $\Re s > 1$,

$$\frac{1}{\varphi(q)}\frac{1}{s-1} = -\frac{1}{\varphi(q)}\int_1^\infty t^{-s} dt$$

et donc

$$L(\Lambda.\delta_{a(\mathrm{mod}\, q)}, s) - \frac{1}{\varphi(q)}\frac{s}{s-1} = -s\int_1^\infty [\psi(t; q, a) - \frac{t}{\varphi(q)}]t^{-s}\frac{dt}{t}.$$

Par la discussion précédente la partie de gauche admet une limite finie quand $s \to 1$ et on voudrait en déduire que cette limite est égale au terme de droite évalué en $s = 1$, ie. en déduire que l'intégrale

$$-\int_1^\infty [\psi(t; q, a) - \frac{t}{\varphi(q)}]\frac{dt}{t^2}$$

converge (et est finie) et (par le critère de convergence de Cauchy) pour tout $x \geqslant 1$ et $\lambda \geqslant 1$ on a

$$\lim_{x\to\infty}\int_x^{\lambda x} [\psi(t; q, a) - \frac{t}{\varphi(q)}]\frac{dt}{t^2} = 0.$$

Cela résulte du Lemme suivant appliqué à la fonction $f(t)$ à support dans $[1, +\infty[$ donnée par

$$f(t) = \frac{1}{t}[\psi(t; q, a) - \frac{t}{\varphi(q)}],$$

(par Chebycheff cette fonction est bornée) :

Lemme 6.4. *Soit $f(t)$ une fonction bornée, nulle au voisinage de 0, localement intégrable et telle que sa transformée*

$$F(s) = \int_0^\infty f(t)t^{-s} dt$$

admette un prolongement analytique dans un voisinage du demi-plan $\{s,\ \Re s \geqslant 1\}$ (comme f est bornée $F(s)$ admet un prolongement analytique évident à $\{s,\ \Re s > 1\}$), alors l'intégrale

$$\int_0^\infty f(t)\frac{dt}{t}$$

converge et vaut $F(1)$

Etant donné $\lambda > 1$, supposons qu'il existe une suite $x_n \to \infty$ telle que $\psi(x_n; q, a) \geqslant \frac{\lambda x_n}{\varphi(q)}$, on aura (comme $\psi(t; q, a)$ est croissante)

$$\int_{x_n}^{\lambda x_n} [\psi(t; q, a) - \frac{t}{\varphi(q)}] \frac{dt}{t^2} \geqslant \frac{1}{\varphi(q)} \int_{x_n}^{\lambda x_n} [\lambda x_n - t] \frac{dt}{t^2} = \frac{1}{\varphi(q)} \int_1^{\lambda} \frac{\lambda - t}{t} \frac{dt}{t} > 0.$$

de même, si il existe une suite $x_n \to \infty$ telle que $\psi(x_n; q, a) \leqslant \frac{x_n}{\lambda \varphi(q)}$, on aura

$$\int_{x_n/\lambda}^{x_n} [\psi(t; q, a) - \frac{t}{\varphi(q)}] \frac{dt}{t^2} \leqslant \frac{1}{\varphi(q)} \int_{x_n/\lambda}^{x_n} [x_n/\lambda - t] \frac{dt}{t^2} = \frac{1}{\varphi(q)} \int_{1/\lambda}^{1} \frac{1/\lambda - t}{t} \frac{dt}{t} < 0.$$

Cela montre que

$$\psi(x; q, a) \sim \frac{x}{\varphi(q)}.$$

□

2. Preuve du Théorème 6.3

On sait déjà que $L(\chi, 1) \neq 0$, il suffit donc de montrer que pour tout $t \in \mathbb{R} - \{0\}$ et tout χ

$$L(\chi, 1 + it) \neq 0.$$

L'idée (due à Hadamard et de la Vallée-Poussin) ressemble à la stratégie utilisée pour démontrer la non-annulation de $L(\chi, s)$ en $s = 1$. On construit une série L dont les coefficients sont positifs ou nuls mais qui est holomorphe (voir s'annule) en $s = 1$ si d'aventure $L(\chi, 1 + it) = 0$; on en déduit une contradiction. Le (sempiternel [1]) exemple d'une telle fonction est le suivant

Lemme 6.5. *Soit*

$$L_{it}(s) = \zeta_q^3(s)(\zeta_q(s + it)\zeta_q(s - it))^2 \zeta_q(s + 2it)\zeta_q(s - 2it).$$

alors les coefficients de la série de Dirichlet $-\frac{L'}{L}(s)$ *sont positifs ou nuls.*

Preuve. On a pour $\Re s > 1$

$$-\frac{L'}{L}(s) = \sum_{n \geqslant 1} \frac{\Lambda_q(n)}{n^s} [3 + 2(n^{-it} + n^{it}) + (n^{-2it} + n^{2it})] = \sum_{n \geqslant 1} \frac{\Lambda_q(n)}{n^s} (1 + n^{-it} + n^{it})^2$$

avec $\Lambda_q(n)$ définit par

$$\sum_{n \geqslant 1} \frac{\Lambda_q(n)}{n^s} = -\frac{\zeta_q'}{\zeta_q}(s) = \sum_{\chi \,(\mathrm{mod}\, q)} -\frac{L'(\chi, s)}{L(\chi, s))}$$

$$= \sum_{\chi \,(\mathrm{mod}\, q)} \sum_{n \geqslant 1} \frac{\Lambda(n)\chi(n)}{n^s} = \sum_{n \geqslant 1} \varphi(q)\delta(n \equiv 1 \,(\mathrm{mod}\, q)) \frac{\Lambda(n)}{n^s},$$

soit

$$\Lambda_q(n) = \varphi(q)\delta(n \equiv 1 \,(\mathrm{mod}))\Lambda(n) \geqslant 0.$$

Comme $n^{-it} + n^{it} \in \mathbb{R}$, $(1 + n^{-it} + n^{it})^2 \geqslant 0$ et les coefficients de $-L'/L$ sont positifs ou nuls. □

Supposons que $L(\chi, 1 + it) = 0$ alors

$$\zeta_q(1 + it) = 0 = \overline{\zeta_q(1 + it)} = \zeta_q(1 - it)$$

1. comme dirait P. Deligne

et donc $L(s)$ s'annule en $s=1$ à l'ordre $m \geqslant 2\times 2-3=1$ et $\frac{-L'}{L}(s)$ à un pôle simple en $s=1$ de résidu $-m$ et donc

$$-1 \geqslant -m \lim_{s\to 1+}(s-1)\frac{-L'}{L}(s) = \lim_{s\to 1+}(s-1)\sum_{n\geqslant 1}\frac{\Lambda_q(n)}{n^s}(1+n^{-it}+n^{it})^2 \geqslant 0,$$

contradiction.

Remarque 6.6. La preuve que nous venons de donner de la non-annulation de $L(\chi,1+it)$ est "globale" : elle utilise le produit $\zeta_q(s)=\prod_\chi L(\chi,s)$ et les propriťés de positivité de ses coefficients et montre la non-annulation de toutes les valeurs $L(\chi,1+it)$ en même temps.

Si la paire (χ,it) n'est pas invariante par conjugason complexe,

$$\overline{(\chi,it)} = (\overline{\chi},-it) \neq (\chi,it)$$

on peut montrer la non-annulation de manière individuelle en considérant la fonction

$$L(\chi_0,s)^3(L(\chi,s+it)L(\overline{\chi},s-it))^2L(\chi^2,s+2it)L(\overline{\chi}^2,s-2it)$$

qui si $L(\chi,1+it)=0$, s'annulera à l'ordre au moins 1 en $s=1$. En revanche cette méthode ne fonctionne pas si

$$(\overline{\chi},-it) = (\chi,it)$$

c'est à dire si $\chi^2=\chi_0$ et $t=0$. Dans ce cas la méthode précédente ne donne rien car

$$L(\chi^2,s+2it) = L(\chi_0,s)$$

à un pôle en $s=1$.

CHAPITRE 7

Caractères de Dirichlet

Dans ce chapître on va discuter en details la structure de groupe de l'ensemble des caractères de Dirichlet.

1. Notion de caractère primitif

Soit χ un caractère de Dirichlet de module q et q' un multiple de q ; on a une application de rèduction modulo q

$$\mathrm{red}_q : \begin{array}{ccc} (\mathbb{Z}/q'\mathbb{Z})^\times & \mapsto & (\mathbb{Z}/q\mathbb{Z})^\times \\ a(\mathrm{mod}\, q') & \to & a(\mathrm{mod}\, q) \end{array}$$

et on peut former un nouveau caractère de Dirichlet de module q' en composant χ avec red_q :

$$\chi'(a(\mathrm{mod}\, q')) := \chi(\mathrm{red}_q(a)) = \chi(a(\mathrm{mod}\, q)).$$

On notera encore χ' l'extension à $\mathbb{Z}$ ce ce caractère en une fonction totalement multiplicative :

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

Il est clair qu'un tel caractère χ' ne peut pas Ãªtre considèrè comme vraiment "nouveau" et on dira qu'il est *non-primitif* ou encore qu'il est *induit* par le caractère χ. Dans le cas inverse, on dèfinit

Définition 7.1. *Un caractère $\chi(\mathrm{mod}\, q)$ qui n'est induit par aucun caractère de module $q'|q$ avec $q' \neq q$ est dit* primitif.

On a la proposition suivante dont la preuve estlaissèe en exercice :

Proposition 7.2. *Soit $q \geqslant 1$ et χ un caractère de Dirichlet de module q. Il existe un unique q^* divisant q et un unique caractère primitif χ^* de module q^* qui induit χ. L'entier q^* est appelè conducteur de χ.*

Dans la suite, on aura besoin de la caractèrisation suivante des caractères primitifs :

Proposition 7.3. *Un caractère $\chi(\mathrm{mod}\, q)$ est primitif si et seulement si pour tout $d|q$, $d < q$, la restriction de χ au sous-groupe*

$$\ker(\mathrm{red}_d) = \{x(\mathrm{mod}\, q),\ x \equiv 1(\mathrm{mod}\, d)\}$$

est une caractère non-trivial.

Preuve. Supposons que $\chi = \chi_d \circ \mathrm{red}_d$ pour $d < q$ divisant q alors χ restreint à $\ker(\mathrm{red}_d)$ est constant ègal à 1.

Rèciproquement, soit $d|q$, $d < q$ et supposons que $\chi_{|\ker(\mathrm{red}_d)}$ est constant ègal à 1 pour $d|q$; on dèfinit un caractère de module d en posant pour $x \in (\mathbb{Z}/d)^\times$

$$\chi_d(x) = \chi(\tilde{x})$$

pour $\tilde{x} \in (\mathbb{Z}/q)^\times$ tel que $\mathrm{red}_d(\tilde{x}) = x$. Cette dèfinition ne dèpend pas du choix de $\tilde{x}$ car si $\mathrm{red}_d(\tilde{x}')$ alors $\tilde{x}' = \tilde{x}y$avec y
$equiv1(d)$ et donc $\chi(\tilde{x}) = \chi(\tilde{x}')$. Il est clair que χ est induit par χ_d donc χ n'est pas primitif. □

2. Sommes de Gauss.

Soit $\chi(\mathrm{mod}\, q)$ un caractères et $n \in \mathbb{Z}$ un entier ; ce dernier dèfinit un caractère *additif* du groupe $\mathbb{Z}/q$ via

$$x \mapsto \exp(2\pi i \frac{nx}{q}) = \mathrm{e}(\frac{nx}{q}).$$

La somme de Gauss associèe à n est dèfinie par

$$\tau_\chi(n) = \sum_{x(\mathrm{mod}\, q)} \chi(x)\mathrm{e}(\frac{nx}{q}).$$

Si $n = 1$, on la note $\tau_\chi := \tau_\chi(1)$.

Théorème 7.4. *On a*

$$\overline{\tau_\chi(n)} = \tau_{\overline{\chi}}(-n). \tag{7.1}$$

Pour $(n, q) = 1$,

$$\tau_\chi(n) = \overline{\chi}(n)\tau_\chi \tag{7.2}$$

de plus, si χ *est primitif, cette égalité est valable pour tout* n *(dans ce cas, si* $(n, q) \neq 1$, $\tau_\chi(n) = 0$*). Pour* χ *primitif, on a*

$$|\tau_\chi|^2 = \chi(-1)\tau_\chi\tau_{\overline{\chi}} = q. \tag{7.3}$$

Preuve. On a

$$\overline{\tau_\chi(n)} = \sum_{x(q)} \overline{\chi(x)}\overline{\mathrm{e}(\frac{nx}{q})} = \sum_{x(q)} \overline{\chi(x)}\mathrm{e}(-\frac{nx}{q}).$$

Supposons que $(n, q) = 1$ et soit $\overline{n} \in (\mathbb{Z}/q)^\times$ un inverse de$n$ modulo q ($n\overline{n} \equiv 1(\mathrm{mod}\, q)$), l'application $x(q) \to nx(q)$ est un homèomorphisme de $(\mathbb{Z}/q)^\times$ et faisant le changement de variable $x \to x' = nx$ ($x = \overline{n}x'$), on obtient

$$\tau_\chi(n) = \sum_{x'(\mathrm{mod}\, q)} \chi(\overline{n}x')\mathrm{e}(\frac{x'}{q}) = \chi(\overline{n})\tau_{\overline{\chi}}.$$

Supposons que χ est primitif et que $(n, q) > 1$ et posons $n' = n/(n, q)$, $q' = q/(n, q) < q$ de sorte que $(n', q') = 1$, on a

$$\tau_\chi(n) = \sum_{x(\mathrm{mod}\, q)} \chi(x)\mathrm{e}(\frac{n'x'}{q});$$

notons que la valeur de $\mathrm{e}(\frac{n'x'}{q})$ ne dèpend que de la rèduction de x modulo q', aussi on dècompose $(\mathbb{Z}/q)^\times$ en classes modulo le sous-groupe $\ker(\mathrm{red}_{q'})$:

$$(\mathbb{Z}/q)^\times = \bigsqcup_{x'} x'\ker(\mathrm{red}_{q'});$$

ainsi

$$\tau_\chi(n) = \sum_{x'} \chi(x') \sum_{y \in \ker(\mathrm{red}_{q'})} \chi(y)\mathrm{e}(\frac{n'x'y'}{q}) = \sum_{x'} \chi(x')\mathrm{e}(\frac{n'x''}{q}) \sum_{y \in \ker(\mathrm{red}_{q'})} \chi(y) = 0$$

car le caractère $\chi_{|\ker(\mathrm{red}_{q'})}$ est non-trivial d'après la proposition 7.3 ; cela termine la preuve de (7.2).

On dèmontre maintenant (7.3) : soit χ un caractère primitif,

$$|\tau_\chi|^2 = \sum_{x,x'(q)} \chi(x)\overline{\chi}(x')\mathrm{e}(\frac{x-x'}{q}) = \sum_{x,x'(q)} \chi(x/x')\mathrm{e}(\frac{x-x'}{q}) = \sum_{z(q)} \chi(z) \sum_{x'\in(\mathbb{Z}/q)^\times} \mathrm{e}(\frac{(z-1)x'}{q}).$$

La somme sur x' est une somme de Ramanujan qui vaut

$$q \sum_{\substack{d|q \\ d|z-1}} \frac{\mu(d)}{d}.$$

On obtient donc

$$|\tau_\chi|^2 = q \sum_{d|q} \frac{\mu(d)}{d} \sum_{z\equiv 1(d)} \chi(z).$$

Comme χ est primitif, la dernière somme est nulle si $d < q$ (Proposotion 7.3), et on obtient (7.3). □

Dans la section suivante, on va calculer la valeur de la somme de Gauss pour les caractères quadratiques primitifs.

3. La structure du groupe $(\mathbb{Z}/q)^\times$

Dasn cette section on va dècrire la structure du groupe abèlien fini $(\mathbb{Z}/q)^\times$, c'est à dire dèterminer sa dècomposition en produit de groupes cycliques.

3.1. Le théorème des restes chinois. Le théorème des restes chinois permet de rèduire l'ètude de la structure de l'anneau $\mathbb{Z}/q\mathbb{Z}$ à celle des anneaux $\mathbb{Z}/p_i^{\alpha_i}\mathbb{Z}$ où $q = \prod_i p_i^{\alpha_i}$ est la dècomposition de q en produit de puissances de nombres premiers.

Théorème 7.5. *(théorème Chinois des Restes) L'application*

$$\begin{aligned} \mathrm{red}: \quad \mathbb{Z}/q\mathbb{Z} &\mapsto \prod_i \mathbb{Z}/p_i^{\alpha_i}\mathbb{Z}, \\ n(\mathrm{mod}\, q) &\mapsto (n(\mathrm{mod}\, p_i^{\alpha_i}))_i \end{aligned}$$

est un isomorphisme ; en particulier elle induit un isomorphisme au niveau des groupes des unitès (ie. des èlèments inversibles) des anneaux respectifs

$$\mathrm{red}: \ (\mathbb{Z}/q)^\times \simeq \prod_i (\mathbb{Z}/p_i^{\alpha_i})^\times.$$

Preuve. Il est clair que red est un morphisme d'anneaux ; de plus red est injectif : si $n(\mathrm{mod}\, q)$ est dans ker(red) alors pour tout i $n \equiv 0(p_i^{\alpha_i})$ donc $n \equiv 0(q)$. Comme les deux anneaux sont de mÃªme cardinal c'est un isomorphisme. □

Remarque 7.6. L'inverse de l'isomorphisme précédent est obtenu de la manière suivante : notons $q_i = q/p_i^{\alpha_i}$ alors q_i est premier à $p_i^{\alpha_i}$, soit $\overline{q_i}$ son inverse $\mathrm{mod}\, p_i^{\alpha_i}$:

$$q_i\overline{q_i} \equiv 1(\mathrm{mod}\, p_i^{\alpha_i}).$$

Soit $(n_i)_i \in \prod_i \mathbb{Z}/p_i^{\alpha_i}\mathbb{Z}$ alors (vèrifier que c'est bien dèfini)

$$\mathrm{red}^{-1}((n_i)_i) = \sum_i n_i q_i \overline{q_i} \ (\mathrm{mod}\, q).$$

Remarque 7.7. On a vu que si G_1, G_2 sont deux groupes abèliens finis, on a un isomorphisme des groupes de caractères

$$\widehat{G_1} \times \widehat{G_2} \simeq \widehat{G_1 \times G_2}.$$

L'isomorphisme ètant donnè par

$$(\chi_1, \chi_2) \mapsto \chi_1.\chi_2 : (g_1, g_2) \mapsto \chi_1(g_1)\chi_2(g_2).$$

En particulier

$$\widehat{(\mathbb{Z}/q)^\times} \simeq \prod_i \widehat{(\mathbb{Z}/p_i^{\alpha_i})^\times}.$$

Dans le cas prèsent les isomorphismes inverses l'un de l'autre sont donnès par

$$\chi(q) \mapsto \chi \circ \mathrm{red}^{-1} \ \in \prod_i \widehat{(\mathbb{Z}/p_i^{\alpha_i})^\times} \quad (\chi_i(p_i^{\alpha_i}))_i \mapsto \prod_i \chi_i \circ \mathrm{red} \ \in \widehat{(\mathbb{Z}/q)^\times}$$

Ainsi pour obtenir tous les caractères de Dirichlet de module q, il suffit de factoriser q en $q = \prod_i p_i^{\alpha_i}$ et de multiplier ensemble des caractères χ_i de modules $p_i^{\alpha_i}$. De mÃªme pour obtenir les caractères *primitifs*, on multiplie ensemble des caractères χ_i *primitifs* de modules $p_i^{\alpha_i}$ (s'ils existent).

On se ramène ainsi où cas $q = p^\alpha$ avec $\alpha \geqslant 1$ et p premier.

3.2. Structure de $(\mathbb{Z}/p)^\times$. On commence par rappeler le cas bien connu où $\alpha = 1$

Théorème 7.8. *Soit p un nombre premier, l'anneau $\mathbb{Z}/p\mathbb{Z}$ est un corps (notè $\mathbb{F}_p$) et $(\mathbb{Z}/p)^\times = \mathbb{F}_p^\times$ est un groupe cyclique d'ordre $p-1$.*

Preuve. Comme p est premier,

$$a (\mathrm{mod}\, p) \neq 0 \Leftrightarrow p \nmid a \Leftrightarrow (a, p) = 1$$

donc $\mathbb{F}_p^\times = \mathbb{Z}/p\mathbb{Z} - \{0\}$ est un corps. Comme $\mathbb{F}_p^\times$ est un groupe d'ordre $p-1$ on a pour tout $a \in \mathbb{F}_p^\times$

$$a^{p-1} = 1$$

et donc pour tout $a \in \mathbb{F}_p$,

$$a^p = a;$$

en d'autre termes pour tout $n \in \mathbb{Z}$

$$n^p \equiv n (\mathrm{mod}\, p), \tag{7.4}$$

il s'agit bien sÃ»r du petit théorème de Fermat...

Montrons que $\mathbb{F}_p^\times$ est cyclique : soit $a \in \mathbb{F}_p^\times$ un èlèment d'ordre maximal q : on a

$$a^q = 1$$

avec $q | p-1$; notons que les èlèments du sous-groupe engendrè par a vèrifient la mÃªme équation

$$X^q - 1 = 0.$$

et il y a q tels èlèments ; comme un polynùme de degrè q dans un corps à au plus q racine, le groupe engendrè par a est exactement l'ensemble de racine de $X^q - 1$.

Supposons $q < p-1$ et soit b qui n'appartient pas au sous-groupe engendrè par a ; quitte à remplacer b par une puissance convenable de b, on peut supposer que b est d'ordre premier r ; alors nècessairement $r | q$ car sinon ab serait d'ordre rq ce qui contredirait la maximalitè de q. Alors b vèrifie $b^q = 1$; cela contredit le fait que l'ensemble des racine de $X^q - 1$ est $a^{\mathbb{Z}}$. $\square$

3.2.1. *Racines primitives modulo p.* L'ensemble des générateurs du groupe cyclique

$$(\mathbb{Z}/p)^\times \simeq \mathbb{Z}/p-1$$

sont appellèes les *racines primitives modulo p* : c'est à dire les classes de congruences $a(\mathrm{mod}\, p)$ vèrifiant

$$a^{p-1} = 1(\mathrm{mod}\, p),\ a^d \neq 1(\mathrm{mod}\, p),\ d|p-1,\ d < p-1.$$

Leur nombre est le nombre de générateurs de $\mathbb{Z}/p-1$ et vaux donc $|(\mathbb{Z}/p-1)^\times| = \varphi(p-1)$ que l'on obtient en dècomposant $p-1$ en facteurs premiers.

En particulier, on voit qu'il n'y a pas de formule vraiment simple pour calculer ce nombre ; de mÃªme il n'y a pas de mèthode vraiment simple pour trouver les racines primitives modulo p (bien sÃ»r il suffirait a priori d'en trouver une, puis de calculer les puissances de celle-ci à des exposants premiers à $p-1$ pour obtenir les autres). En tout cas il est nècèssaire de disposer au moins de la dècomposition de $p-1$ en facteurs premiers.

La conjecture la plus cèlèbre concernant les racines primitives est la suivante :

Conjecture 7.9 (E. Artin)**.** *Soit a un entiers $\neq -1$ et qui n'est pas un carrè parfait, alors il existe une infinitè de p tels que $a(\mathrm{mod}\, p)$ est une racine primitive.*

A ce jour, les meilleurs résultats en direction de cette conjecture sont dus à Gupta-Murty et Heath-Brown.

3.3. Structure de $(\mathbb{Z}/p^\alpha)^\times$. On a le théorème de structure suivant :

Théorème 7.10. *Soit p premier, on a les isomorphismes de groupes suivants :*
– *pour $p = 2$ et $\alpha \geqslant 2$*

$$(\mathbb{Z}/2)^\times = \{1\}, (\mathbb{Z}/2^\alpha)^\times \simeq (\mathbb{Z}/4)^\times \times \mathbb{Z}/2^{\alpha-2} \simeq \mathbb{Z}/2 \times \mathbb{Z}/2^{\alpha-2};$$

– *pour $p > 2$ et $\alpha \geqslant 1$*

$$(\mathbb{Z}/p^\alpha)^\times \simeq \mathbb{F}_p^\times \times \mathbb{Z}/p^{\alpha-1} \simeq \mathbb{Z}/(p-1) \times \mathbb{Z}/p^{\alpha-1}.$$

Preuve. Soit $n \in \mathbb{Z}$, notons

$$[n] : \begin{array}{ccc} (\mathbb{Z}/p^\alpha)^\times & \to & (\mathbb{Z}/p^\alpha)^\times \\ a & \to & a^n \end{array},$$

l'homomorphisme d'èlèvation à la puissance n.

3.3.1. *Le cas $p > 2$.* On a $|(\mathbb{Z}/p^\alpha)^\times| = (p-1)p^{\alpha-1}$, comme $p-1$ et $p^{\alpha-1}$ sont premiers entre eux, il existe $a, b \in \mathbb{Z}$ tels que

$$a(p-1) + bp^{\alpha-1} = 1;$$

ainsi, pour tout $x \in (\mathbb{Z}/p^\alpha)^\times$, on a

$$x = x^{a(p-1)} x^{bp^{\alpha-1}} =: uv; \tag{7.5}$$

notons que par le théorème de Lagrange

$$u^{p^{\alpha-1}} = x^{a(p-1)p^{\alpha-1}} = 1,\ v^{p-1} = x^{b(p-1)p^{\alpha-1}} = 1.$$

Ains tout èlèment $x \in (\mathbb{Z}/p^\alpha)^\times$ se dècompose en le produit d'un èlèment de $\ker[p^{\alpha-1}]$ et de $\ker[p-1]$. En d'autres termes, on a un morphisme de groupes

$$\begin{array}{ccc} (\mathbb{Z}/p^\alpha)^\times & \to & \ker[p^{\alpha-1}] \times \ker[p-1] \\ x & \to & (x^{a(p-1)}, x^{bp^{\alpha-1}}) \end{array}$$

qui est injectif par (7.5). Ce morphisme est surjectif : ètant donnè $(u,v)\in\ker[p^{\alpha-1}]\times\ker[p-1]$, on a par (7.5)

$$u=u^{a(p-1)}u^{bp^{\alpha-1}}=u^{a(p-1)},\ \ v=v^{a(p-1)}v^{bp^{\alpha-1}}=v^{bp^{\alpha-1}}.$$

Remarque 7.11. Ce resultat est un cas particulier de la proposition générale suivante (la dèmontrer)

Proposition. *Soit G un groupe abèlien fini (qu'on notera multiplicativement) d'ordre rs avec r et s premiers entre eux, alors G est isomorphe au produit de ses deux sous-groupes*

$$G[r]=\{g\in G,\ g^r=e_G\},\quad G[s]=\{g\in G,\ g^s=e_G\}$$

et ceux-ci sont d'ordre r et s respectivement.

Montrons maintenant que

$$\ker[p^{\alpha-1}]\simeq\mathbb{Z}/p^{\alpha-1},\ \ker[p-1]\simeq(\mathbb{Z}/p)^\times\simeq\mathbb{Z}/(p-1).$$

Tout d'abord, par le petit théorème de Fermat, on a pour tout $a\in(\mathbb{Z}/p^\alpha)^\times$

$$[p]a=a^p\equiv a(\operatorname{mod}p).$$

En particulier pour $u\in\ker[p^{\alpha-1}]$,

$$1=[p^{\alpha-1}]u=[p]^{\alpha-1}u\equiv u(\operatorname{mod}p)$$

et donc

$$\ker[p^{\alpha-1}]\subset(\mathbb{Z}/p^\alpha)^{(1)}=:\{a\in(\mathbb{Z}/p^\alpha)^\times,\ a\equiv 1(\operatorname{mod}p)\}=\{1+pb,\ b\in\mathbb{Z}/p^{\alpha-1}\mathbb{Z}\}=\ker(\mathrm{red}_p).$$

Montrons l'inclusion inverse : pour $b\in\mathbb{Z}$,

$$[p](1+bp)=(1+bp)^p=1+p^2b+\sum_{k=2}^{p-1}C_p^k(pb)^k+p^pb^p=1+bp^2+p^3c,\ c\in\mathbb{Z};$$

en effet, si $2\leqslant k\leqslant p-1$, l'entier $C_p^k=\frac{p}{k(p-k)}$ est divisible par p. Substituant b par bp dans l'égalité précédente, on obtient en itèrant

$$[p^{\alpha-1}](1+pb)=[p]^{\alpha-1}(1+pb)=1+p^\alpha b'\equiv 1(\operatorname{mod}p^\alpha).$$

Ce qui montre l'égalité

$$\ker[p^{\alpha-1}]\subset(\mathbb{Z}/p^\alpha)^{(1)}.$$

En particulier $\ker[p^{\alpha-1}]$ est d'ordre $p^{\alpha-1}$. Notons ègalement que le calcul précédent montre que si b est premier à p

$$[p^{\alpha-2}](1+pb)=[p]^{\alpha-2}(1+pb)=1+p^{\alpha-1}b'\ \text{avec}\ b'\equiv b(\operatorname{mod}p);$$

ainsi $1+pb(\operatorname{mod}p^\alpha)$ est exactement d'ordre $p^{\alpha-1}$, c'est donc un générateur du groupe $\ker[p^{\alpha-1}]$.

Considèrons la restriction de l'application red_p à $\ker[p-1]$. Cette application est injective car son noyau vaut $\ker[p-1]\cap\ker(\mathrm{red}_p)=\ker[p-1]\cap\ker[p^{\alpha-1}]=\{1\}$ et comme elle est surjective car

$$(\mathbb{Z}/p)^\times=\mathrm{red}_p((\mathbb{Z}/p^\alpha)^\times)=\mathrm{red}_p(\ker[p-1]\cap\ker[p^{\alpha-1}])=\mathrm{red}_p(\ker[p-1])$$

puisque $\ker[p^{\alpha-1}]=\ker(\mathrm{red}_p)$.

3.4. Le cas $p=2$. Soit $\alpha \geqslant 2$; tout èlèment a de $(\mathbb{Z}/2^\alpha)^\times$ s'ècrit de manière unique sous la forme

$$\pm 1 + 4b = \pm 1(1 \mp 4b),\ b \in \mathbb{Z}/2^{\alpha-2},$$

avec $\pm 1 = 1$ si $a \equiv 1 (\mathrm{mod}\, 4)$ et -1 si $a \equiv -1 (\mathrm{mod}\, 4)$. Cela montre que l'on a

$$\mathbb{Z}/2^{\alpha-2} = \{\pm 1\} \times (\mathbb{Z}/2^\alpha)^{(2)}$$

avec $(\mathbb{Z}/p^\alpha)^{(2)}$ le sous-groupe d'ordre $2^{\alpha-2}$

$$(\mathbb{Z}/p^\alpha)^{(2)} =: \{a \in (\mathbb{Z}/2^\alpha)^\times,\ a \equiv 1 (\mathrm{mod}\, 2^2)\} = \ker(\mathrm{red}_4).$$

Montrons que $(\mathbb{Z}/p^\alpha)^{(2)}$ est cyclique et engendrè par tout èlèment de la forme $a = 1+4b (\mathrm{mod}\, p^\alpha)$ avec $(b,2)=1$. En effet, pour $b \in \mathbb{Z}$, on a

$$[2](1+4b) = (1+4b)^2 = 1 + 8b + 16b^2.$$

En particulier

$$[2^{\alpha-2}](1+4b) \equiv 1 (\mathrm{mod}\, 2^\alpha)$$

et si b est impair

$$[2^{\alpha-3}](1+4b) \equiv 1 + 2^{\alpha-1} b \not\equiv 1 (\mathrm{mod}\, 2^\alpha),$$

c'est à dire que pour b impair $1+4b$ engendre un groupe cyclique d'ordre $2^{\alpha-2}$. □

4. Caractères quadratiques.

On va utiliser le théorème de structure précédent pour dèterminer les caractères de Dirichlet d'ordre 2 (ie. les caractères non-triviaux à valeur dans $\{1,-1\}$).

Par les arguments de la première section, on peut se restreindre au cas où $q = p^\alpha$. Il s'agit donc de dèterminer les sous-groupes d'ordre 2 de $\widehat{(\mathbb{Z}/p^\alpha)^\times}$ qui est un produit d'un ou deux groupes cycliques. On sait par ailleurs qu'un groupe cyclique admet un sous-groupe d'ordre 2 si et seulement si il est d'ordre pair et ce sous-groupe est alors unique.

Si $p=2$, on a

$$(\mathbb{Z}/p^\alpha)^\times \simeq (\mathbb{Z}/4)^\times \times \ker[2^{\alpha-2}] \simeq \mathbb{Z}/2 \times \mathbb{Z}/2^{\alpha-2}$$

admet un caractère d'ordre 2 si $\alpha = 2$ et trois caractères d'ordre 2 si $\alpha \geqslant 3$.

De mÃªme, si $p > 2$,

$$(\mathbb{Z}/p^\alpha)^\times \simeq (\mathbb{Z}/p)^\times \times \ker[p^{\alpha-1}] \simeq \mathbb{Z}/(p-1) \times \mathbb{Z}/p^{\alpha-1}$$

admet un unique caractère d'ordre 2.

Rappelons ègalement que si $\beta \geqslant \alpha$ et si χ est un caractère de module p^α, on obtient un caractère de module p^β en composant avec la rèduction modulo p^α, $\chi' = \chi \circ \mathrm{red}_{p^\alpha}$; le caractère obtenu est de mÃªme ordre.

On va maintenant construire ces caractères :

Le groupe $(\mathbb{Z}/4)^\times \simeq \mathbb{Z}/2\mathbb{Z}$ admet exactement un caractère d'ordre 2 que l'on note χ_4 : c'est l'unique caractère non-trivial (et primitif) de $(\mathbb{Z}/4)^\times$ et il vaut -1 en $3 (\mathrm{mod}\, 4)$: en d'autres termes

$$\chi_4(a) = (-1)^{\frac{a-1}{2}}.$$

Le groupe $(\mathbb{Z}/8)^\times \simeq (\mathbb{Z}/4)^\times \times (\mathbb{Z}/8)^{(2)}$ admet trois caractères d'ordre 2 :

(1) celui obtenu en composant le caractère χ_4 avec la reduction modulo 4 : $\chi_4 \circ \mathrm{red}_4$; il n'est pas primitif et par abus de notation on le note encore χ_4.

(2) Le caractère notè χ_8 qui dans l'isomorphisme précédent est trivial sur le premier facteur et non-trivial sur $(\mathbb{Z}/8)^{(2)}$: ce caractère est primitif et on a $\chi_8(1) = \chi_8(7) = 1$, $\chi_8(3) = \chi_8(5) = -1$, où encore

$$\chi_8(a) = (-1)^{\frac{a^2-1}{8}}.$$

(3) le produit $\chi_4\chi_8$.

Pour $\alpha \geqslant 4$, on a vu qu'on dispose exactement de 3 caractères. Comme les caractères obtenus par $\chi_4, \chi_8, \chi_4\chi_8$ en composant avec la rèduction modulo 8 sont au nombre de trois on les a tous et ils sont tous non primitifs.

4.1. Le cas $p > 2$: le symbole de Legendre. Si $p > 2$, l'unique caractère d'ordre deux de $(\mathbb{Z}/p^\alpha)^\times$ est obtenu à partir de l'unique caractère d'ordre deux de $(\mathbb{Z}/p)^\times$ en composant avec la rèduction modulo p. Ce dernier –qui est primitif– est appelè *symbole de Legendre* et est notè $\chi_p(a)$ ou $\left(\frac{a}{p}\right)$.

Théorème 7.12. *Soit*

$$(\mathbb{F}_p^\times)^2 = [2].\mathbb{F}_p^\times = \{x^2,\ x \in \mathbb{F}_p^\times\}$$

l'ensemble des carrès de $\mathbb{F}_p^\times$, alors

$$\left(\frac{a}{p}\right) = \begin{cases} 1 \ \ si \ \ a \in \mathbb{F}_p^{\times 2} \\ -1 \ \ si \ \ a \notin \mathbb{F}_p^{\times 2} \end{cases}$$

et on a la formule "analytique" suivante

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod p$$

Preuve. le noyau de l'application $[2] : x \mapsto x^2$ est l'ensemble des racines du polynùme

$$X^2 - 1 = (X-1)(X+1)$$

et vaut donc $\{1, -1\}$. Ainsi $(\mathbb{F}_p^\times)^2$ est l'unique sous-groupe d'incide 2 de $\mathbb{F}_p^\times$ et donc le noyau de $\left(\frac{\cdot}{p}\right)$. Ainsi $\left(\frac{\cdot}{p}\right)$ vaut nècèssairement -1 sur le complèmentaire de $\mathbb{F}_p^{\times 2}$. Pour la formule, on note que par (7.4) tout $a \in (\mathbb{Z}/p)^\times$ est racine du polynùme de $\mathbb{F}_p[X]$

$$X^{p-1} - 1 = (X^{\frac{p-1}{2}} - 1)(X^{\frac{p-1}{2}} + 1)$$

et que $\mathbb{F}_p^{\times 2}$ est l'ensemble des racines du premier facteur (si $a = b^2$, $a^{\frac{p-1}{2}} = b^{p-1} = 1$) ; ainsi $\mathbb{F}_p^\times - \mathbb{F}_p^{\times 2}$ est l'ensemble des racines du deuxième facteur. □

Etendons le caractère de Legendre à $\mathbb{Z}$ de la manière usuelle,

$$\left(\frac{n}{p}\right) = \begin{cases} \left(\frac{n \bmod p}{p}\right) & \text{si } (n,p) = 1, \\ 0 & \text{sinon ;} \end{cases}$$

on a donc

Corollaire 7.13. *Soit $p > 2$ premier et $\Delta \in \mathbb{Z}$, on a*

$$\left(\frac{\Delta}{p}\right) = \begin{cases} 1 \ \ si \ \Delta \pmod p \ \ est \ un \ carrè \ non\text{-}nul \ dans \ \mathbb{F}_p^\times \\ -1 \ \ si \ \Delta \pmod p \ \ n'est \ pas \ un \ carrè \ dans \ \mathbb{F}_p^\times \\ 0 \ \ si \ \Delta \equiv 0 \pmod p; \end{cases}$$

en particulier, le nombre de racines distinctes dans $\mathbb{F}_p$ *du polynome* aX^2+bX+c *est*

$$1+\left(\frac{\Delta}{p}\right),\ \Delta=b^2-4ac.$$

4.2. Caractères quadratiques de module quelconque. Les caractères quadratiques de module $q=\prod_i p_i^{\alpha_i}$ sont obtenus par la recette dècrite dans la section §3.1 en multipliant entre eux des caractères quadratiques de modules $p_i^{\alpha_i}$. Si on se restreint aux caractères *primitifs* tous les modules ne sont pas possibles car chaque χ_i doit Ãªtre primitif. Ainsi les seules possibilitès sont

(1) $q=\prod_i p_i$, p_i impair : $\chi(.)=\prod_i(\frac{\cdot}{p_i})$.

(2) $q=4\prod_i p_i$, p_i impair : $\chi(.)=\chi_4(.)\prod_i(\frac{\cdot}{p_i})$.

(3) $q=8\prod_i p_i$, p_i impair : $\chi(.)=\chi_8(.)\prod_i(\frac{\cdot}{p_i})$ ou bien $\chi=\chi_4\chi_8(.)\prod_i(\frac{\cdot}{p_i})$.

5. la loi de réciprocité quadratique

Le caractère de Legendre permet de dèterminer si un entier donnè Δ est un carrè modulo un nombre premier impair p. Un point tout a fait remarquable conjecturè par Euler et Legendre et dèmontrè par Gauss est que, pour $\Delta\neq 0$ fixè la condition

$$\Delta \textit{ est un carrè modulo } p$$

se traduit en une condition *de congruence sur* p modulo un entier qui ne dèpend que de Δ. En particulier, on pourra compter asymptotiquement le nombre de p satisfaisant une telle condition grÃ¢ce au théorème de la progression arithmètique. Ce principe s'appelle une *loi de rèciprocitè* car il permet d'exprimer une condition de congruence modulo p par une condition de congruence sur p lui-mÃªme.

L'exemple le plus simple d'un tel principe est le cas de l'entier $\Delta=-1$:

Théorème 7.14 (La loi de réciprocité quadratique (cas de $\Delta=-1$))**.** *Soit* p *impair, alors* -1 *est un carrè modulo* p *si et seulement si* $p\equiv 1 \pmod 4$. *De manière èquivalente, on a l'égalité*

$$\left(\frac{-1}{p}\right)=\chi_4(p).$$

Preuve. Avec la dernière formulation, la preuve est évidente puisque par la formule analytique

$$\left(\frac{-1}{p}\right)=(-1)^{\frac{p-1}{2}}=\chi_4(p).$$

□

La loi de rèciprocitè quadratique dèmontrèe par Gauss traite du cas où $\Delta=q$ est un nombre premier et comme ci-dessus on peut l'exprimer en terme de caractères.

Théorème 7.15 (La loi de réciprocité quadratique (cas de $\Delta=2$))**.** *Soit* p *impair, alors* 2 *est un carrè modulo* p *si et seulement si* $p\equiv 1,7 \pmod 8$. *De manière èquivalente, on a l'égalité*

$$\left(\frac{2}{p}\right)=\chi_8(p).$$

Théorème 7.16 (La loi de réciprocité quadratique (cas de $\Delta=q$ premier impair))**.** *Soit* p,q *deux nombres premiers impairs, on a l'égalité*

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right)=(-1)^{\frac{p-1}{2}\frac{q-1}{2}};$$

de manière èquivalente

$$(\frac{q}{p}) = (\frac{\chi_4(p)p}{q}).$$

5.1. Preuve de la loi de rèciprocitè quadratique. Soit p premier impair et soit q qui est, ou bien ègal à 8, ou bien est un nombre premier impair. Soit $\omega = \exp(\frac{2\pi i}{q})$. On va effectuer des calculs dans l'anneau d'entiers $\mathbb{Z}[\omega] \subset \mathbf{C}$ et plus prècisement modulo l'idèal principal $p\mathbb{Z}[\omega]$. Notons que $\omega^q = 1$ donc l'application $x \mapsto \omega^x$ dèfinit un caractère du groupe abèlien $(\mathbb{Z}/q\mathbb{Z}, +)$ à valeur dans $\mathbb{Z}[\omega]^\times \subset \mathbf{C}^\times$. Considèrons la somme de Gauss

$$\tau_q := \sum_{x \in (\mathbb{Z}/q)^\times} \chi_q(x)\omega^x \in \mathbb{Z}[\omega].$$

On a d'une part

$$\tau_q^2 = \sum_{x,y \in (\mathbb{Z}/q)^\times} \chi_q(xy)\omega^{x+y} = \sum_{x,y \in (\mathbb{Z}/q)^\times} \chi_q(x/y)\omega^{x+y}$$

car $\chi_q(y) = \chi_q(1/y)$, le charactère χ_q ètant à valeurs dans $\{-1, 1\}$. Posons $z = x/y$, on obtient

$$\tau_q^2 = \sum_{z \in (\mathbb{Z}/q)^\times} \chi_q(z) \sum_{x \in (\mathbb{Z}/q)^\times} \omega^{x(1+1/z)}.$$

Si q est premier et $z \neq -1$

$$\sum_{x \in (\mathbb{Z}/q)^\times} \omega^{x(1+1/z)} = \sum_{x \in \mathbb{Z}/q} \omega^{x(1+1/z)} - 1 = -1$$

(par orthogonalitè des caractères : $x \mapsto \omega^{x(1+1/z)}$ dèfinit un caractère non-trivial du groupe $\mathbb{Z}/q$) alors que si $z = -1$,

$$\sum_{x \in (\mathbb{Z}/q)^\times} \omega^{x(1+1/z)} = \sum_{x \in (\mathbb{Z}/q)^\times} 1 = q - 1.$$

Utilisant le fait que $\sum_{z \in (\mathbb{Z}/q)^\times} \chi_q(z) = 0$ (par orthogonalitè des caractères), on en déduit que

$$\tau_q^2 = \chi_q(-1)q.$$

Un calcul explicite montrer que la mÃªme égalité est vraie pour $q = 8$ (et $\chi_8(-1) = 1$).

Calculons maintenant τ_q^p ou plutùt $\tau_q^p \pmod{p\mathbb{Z}[\omega]}$. Notons que si on a $A, B \in \mathbb{Z}[\omega]$,

$$(A+B)^p = A^p + \sum_{k=1}^{p-1} C_p^k A^{p-k} B^k + B^p \equiv A^p + B^p \pmod{p\mathbb{Z}[\omega]}$$

car $C_p^k \in p\mathbb{Z}$ si $1 \leqslant k \leqslant p-1$. On en déduit que

$$\tau_q^p \equiv \sum_{x \in (\mathbb{Z}/q)^\times} \chi_q(x)^p \omega^{xp} \equiv \sum_{x \in (\mathbb{Z}/q)^\times} \chi_q(x)\omega^{xp} \pmod{p\mathbb{Z}[\omega]}$$

faisont le changement de variable $z = px$ dans $(\mathbb{Z}/q)^\times$ (car p est premier a q), on obtient

$$\tau_q^p \equiv \sum_{z \in (\mathbb{Z}/q)^\times} \chi_q(z/p)\omega^z \equiv \chi_q(1/p)\tau_q \equiv \chi_q(p)\tau_q \pmod{p\mathbb{Z}[\omega]}.$$

Ainsi on obtient

$$\tau_q^p = \tau_q \tau_q^{2.\frac{p-1}{2}} = \tau_q \chi_q(-1)^{\frac{p-1}{2}} q^{\frac{p-1}{2}} \equiv \chi_q(p)\tau_q \pmod{p\mathbb{Z}[\omega]}.$$

Multipliant cette égalité par τ_q on obtient

$$q\chi_q(-1)^{\frac{p-1}{2}} q^{\frac{p-1}{2}} \equiv \chi_q(p)q \pmod{p\mathbb{Z}[\omega]}.$$

En d'autres termes, p divise l'entier $q(\chi_q(-1)^{\frac{p-1}{2}} q^{\frac{p-1}{2}} - \chi_q(p))$ dans $\mathbb{Z}[\omega]$. Cependant comme $\mathbb{Z}[\omega] \cap \mathbb{Q} = \mathbb{Z}$ ($\mathbb{Z}[\omega]$ est intègralement clos), on voit que p divise l'entier $q(\chi_q(-1)^{\frac{p-1}{2}} q^{\frac{p-1}{2}} - \chi_q(p))$ dans $\mathbb{Z}$:

$$\chi_q(p) \equiv \chi_q(-1)^{\frac{p-1}{2}} \left(\frac{q}{p}\right) \pmod{p}$$

et donc $\chi_q(p) = \chi_q(-1)^{\frac{p-1}{2}} \left(\frac{q}{p}\right)$ cela dèmontre le résultat en notant que $\left(\frac{8}{p}\right) = \left(\frac{2}{p}\right)$. □

Exercice(s) 7.17. Soit Δ un entier qui n'est pas un carrè parfait (pas de la forme d^2 pour $d \in \mathbb{N}$), montrer que

$$\sum_{\substack{p \leqslant X \\ \Delta \text{ est un carrè modulo } p}} \frac{\log p}{p} = \frac{1}{2} \log X + O(1).$$

On utilisera la loi de rèciprocitè quadratique.

Méthode d'analyse complexe

CHAPITRE 8

Le mémoire de Riemann

Il y a 150 ans, en 1859, Riemann publia sont célèbre mémoire *Uber die anzahl....* : dans ce mémoire, Riemann jette les bases de l'étude des propriétés analytiques de la fonction "dzeta"

$$\zeta(s) = \sum_{n\geqslant 1} \frac{1}{n^s} = \prod_p (1 - \frac{1}{p^s})^{-1},\ \Re s > 1 \tag{8.1}$$

en tant que fonction de la variable complexe et la relation entre celles ci et le problème du comptage des nombres premiers.

Ainsi, Riemann mentionne un formule "explicite", démontrèe plus tard par von Mangolt reliant la fonction sommatoire de la fonction Λ,

$$M_\Lambda(x) = \sum_{n\leqslant x} \Lambda(n)$$

à une somme sur les zéros de $\zeta(s)$. une formule asymptotique pour $M_\Lambda(x)$ quand $x \to +\infty$. Riemann montre que les zéros "non-triviaux" de ζ sont en nombre infini et donne une formula asymptotique de leur nombre. C'est également à cette occasion qu'il formule sa célèbre hypothèse *l'hypothèse de Riemann* qui prédit que les zéros non-triviaux sont tous situé sur la droite $\Re es = 1/2$. La preuve de cette hypothèse est un des problèmes les plus important des mathématiques : pour sa résolution, l'Institut américain Clay à promis une récompense de 1000000 USD à son auteur.

Prolongement analytique. *La fonction $\zeta(s)$ admet un prolongement méromorphe à $\mathbf{C}$. Elle est holomorphe partout sauf en $s = 1$, ou elle admet un pùle simple de résidu égal à* 1

Equation fonctionnelle. *Soit*

$$\Lambda(s) := \zeta_\infty(s)\zeta(s) \text{ avec } \zeta_\infty(s) = \pi^{-s/2}\Gamma(s/2).$$

Alors $\Lambda(s)$ admet un prolongement analytique à $\mathbf{C}$ avec deux poles simples en $s = 0, 1$ et vérifie pour $s \neq 0, 1$

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

Dans cet énoncé, $\Gamma(s)$ désigne la fonction Γ d'Euler

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

On a vu que, compte-tenu de la factorisation en produit eulérien (8.1), $\zeta(s)$ ne s'annule pas pour $\Re s > 1$. Comme $\Gamma(s)$ ne s'annule pas sur $\mathbf{C}$, on déduit de l'équation fonctionnelle précèdente que $\Lambda(s)$ ne s'annule pas pour $\Re s < 0$ ou $\Re s > 1$. En revanche comme $\Gamma(s/2)$ a des pôles simple aux entiers négatifs pairs, $\zeta(s)$ s'annule à l'ordre 1 en $s = -2, -4, \ldots$. Ces zéros sont appelés les *zéros triviaux de ζ*, et les zéros non-triviaux de ζ sont les zéros de $\Lambda(s)$ et ils sont contenus dans la bande critique

$$\{s \in \mathbf{C},\ \Re s \in [0, 1]\}.$$

Riemann a donné une formule asymptotique pour les compter :

Comptage des Zeros. *Pour $T \geqslant 0$, soit*

$$N(T) = |\{\rho = \beta + it,\ \zeta(\rho) = 0,\ \beta \in [0,1],\ |t| \leqslant T\}|$$

le nombre de zéros non-triviaux de hauteur $\leqslant T$. On a

$$N(T) = \frac{T}{\pi}\log(\frac{T}{2\pi}) + O(\log(2+|T|)).$$

Cette formule de comptage peut être déduite de la formule suivante qui relie les zeros de ζaux nombres premiers :

Formule explicite. *Soit $f \in \mathscr{C}_c^\infty(\mathbb{R}_{>0})$ et*

$$\widetilde{f}(s) = \int_0^{+\infty} f(x)x^s\frac{dx}{x}$$

sa transformée de Mellin. Soit $\check{f}(x) = x^{-1}f(x^{-1})$. On a l'identité

$$\sum_{n\geqslant 1}(f(n)+\check{f}(n))\Lambda(n) = \widetilde{f}(1) + \frac{1}{2\pi i}\int_{(1/2)}\big(\frac{\zeta'_\infty}{\zeta_\infty}(s) + \frac{\zeta'_\infty}{\zeta_\infty}(1-s)\big)\widetilde{f}(s)ds - \sum_{\substack{\zeta(\rho)=0\\ \Re\rho\in[0,1]}}\widetilde{f}(\rho).$$

Dans ce chapître et les suivants nous établissons les différents points du mémoire de Riemann en les généralisant aux fonctions L des caractères de Dirichlet.

CHAPITRE 9

L'équation fonctionnelle

1. Quelques transformations intégrales

La théorie de Fourier décrit la structure de l'espaces des fonctions sur la droite rélle $\mathbb{R}$ en tentant compte du fait que $(\mathbb{R},+)$ est un groupe commutatif pour l'addition. Elle permet d'écrire les fonctions [1] de $\mathbb{R}$ comme "combinaison linéaire" de fonctions adaptées à la structure de groupe, les *caractère* dont nous avons rencontrer des examples quand nous avons parlé des groupes abéliens finis.

1.1. Les caractères de $\mathbb{R}$.

Définition 9.1. *Soit $(G,+)$ un groupe abélien topologique (un groupe abélien muni d'une structure d'espace topologique pour laquelle l'addition $+:(x_1,x_2)\to x_1+x_2$ et l'inversion $[-1]:x\to -x$ sont continues), l'ensemble des caractères de G est l'ensemble $\mathrm{Hom}_c(G,\mathbf{C}^\times)$ des homomorphismes de groupes continus de G vers $(\mathbf{C}^\times,\times)$. C'est ensemble est un groupe commutatif pour la multiplication des fonctions.*

Un caractère est unitaire si il est à valeurs dans le cercle unité $\mathbf{C}^{(1)}=\{z\in\mathbb{C}^\times,\ |z|=1\}$. On note $\widehat{\mathbb{C}}$ the sous-groupe des caractères unitaires.

Remarque 9.2. Si G est compact alors tout caractère est unitaire : soit ψ un caractère alors $\psi(G)$ est un sous-groupe compact de $\mathbb{C}^\times$ et est donc contenu dans $\mathbb{C}^{(1)}$ (s'il existe $z\in\psi(G)$ tel que $|z|\neq 1$ alors pour tout $n\in\mathbb{Z}$, $z^n\in\psi(G)$ mais $z^n\to 0$ ou $+\infty$ suivant que $|z|<1$ ou $|z|>1$.)

Théorème 9.3. *L'application*

$$y\in\mathbf{C}\mapsto\psi_y:x\mapsto e(xy)$$

est un isomorphisme de groupes

$$(\mathbf{C},+)\simeq\mathrm{Hom}_c(\mathbb{R},\mathbb{C}^\times).$$

la restriction de cette application à $\mathbb{R}$ est un isomorphisme de groupes

$$(\mathbb{R},+)\simeq\widehat{\mathbb{R}}.$$

Démonstration. Il est clair que cette application est un morphisme de groupes injectif : si y est tel que pour tout x, $x\mapsto e(xy)=1$ alors y doit être nul car sa dérivée (en x) vaut $2\pi iye(xy)=0$. Montrons qu'ell est surjective : soit $\psi\in\mathrm{Hom}_c(\mathbb{R},\mathbb{C}^\times)$ et

$$\Psi(x)=\int_0^x\psi(t)dt$$

sa primitive (ψ est continue donc intégrable), on a

$$\Psi(x+y)=\int_{0,x+y}\psi(t)dt=\int_{0,x}\psi(t)dt+\int_{0,y}\psi(x+t)dt=\Psi(x)+\psi(x)\Psi(y).$$

1. au moins celles qui sont suffisament régulières

Fixons y tel que $\Psi(y) \neq 0$ (un tel y existe sinon $\Psi'(y) = \psi(y) = 0$ ce qui est impossible), on dédui de l'identité précédente que $x \mapsto \psi(x)$ est dérivable et que

$$\psi(x+y) = \psi(x)\psi(y) = \psi(x) + \psi'(x)\Psi(y)$$

et donc

$$\frac{\psi'(x)}{\psi(x)} = \frac{\psi(y)-1}{\Psi(y)}$$

et donc posant $u = \frac{\psi(y)-1}{\Psi(y)}$ on voit que

$$\psi(x) = C\exp(ux)$$

et de plus on a $C = 1$ en évaluant l'égalité précédente en $x = 0$.

□

Corollaire 9.4. *L'application*

$$n \in \mathbb{Z} \mapsto \psi_n : x \mapsto e(nx)$$

est un isomorphisme de groupes

$$(\mathbb{Z}, +) \simeq \mathrm{Hom}_c(\mathbb{R}/\mathbb{Z}, \mathbb{C}^\times) = \widehat{\mathbb{R}/\mathbb{Z}}.$$

Démonstration. L'égalité $\mathrm{Hom}_c(\mathbb{R}/\mathbb{Z}, \mathbb{C}^\times) = \widehat{\mathbb{R}/\mathbb{Z}}$ tient au fait que $\mathbb{R}/\mathbb{Z}$ est compact (cf. la remarque ci-dessus). Soit $\psi \in \widehat{\mathbb{R}/\mathbb{Z}}$ alors ψ définit un caractère unitaire sur $\mathbb{R}$ qui vaut 1 sur $\mathbb{Z}$ et est donc de la forme $\psi(x) = e(nx)$ avec $n \in \mathbb{R}$. Comme $\psi(1) = 1 = \exp(2\pi i n)$ on a que $n \in \mathbb{Z}$. Le reste suit. □

1.2. La transformée de Fourier.

1.3. La classe de Schwartz. On dit qu'une fonction $f : \mathbb{R} \to \mathbf{C}$ appartient à la classe de Schwartz, $\mathscr{S}(\mathbb{R})$, si $f \in \mathscr{C}^\infty(\mathbb{R})$ et que f et toutes ses dérivées sont à décroissance rapide : c'est à dire, pour tout $A \geqslant 0$ et tout entier $j \geqslant 0$

$$f^{(j)}(x) \ll_{j,N} (1+|x|)^{-A}.$$

1.4. Transformée de Fourier. On note $e(x) := \exp(2\pi i x)$; soit $f \in \mathscr{S}(\mathbb{R})$, la transformée de Fourier de f est la fonction

$$\widehat{f} : \ y \to \int_{\mathbb{R}} f(x)e(xy)dx.$$

Comme f est a décroissance rapide, on voit que l'intégrale précédente converge absolument uniformement sur $\mathbb{R}$ et qu'elle définit une fonction infiniment dérivable et ses dérivées valent

$$\widehat{f}^{(j)}(y) = \int_{\mathbb{R}} (2\pi i x)^j f(x)e(xy)dx = \widehat{M^j f}(y), \ \textit{avec} \ Mf : x \to (2\pi i x)f(x). \tag{9.1}$$

Notons également que par intégration par parties, on a pour $y \neq 0$

$$\widehat{f}(y) = -\frac{1}{2\pi i y}\int f'(x)e(xy)dx = -\frac{1}{2\pi i y}\widehat{f'}(y), \tag{9.2}$$

et en itérant, on obtient pour tout $j \geqslant 1$

$$\widehat{f}(y) = (-\frac{1}{2\pi i y})^j \widehat{f^{(j)}}(y).$$

Ce calcul est justifié par la décroissance rapide des dérivées de f. Ainsi pour $|y| \geqslant 1$, on a pour tout $j \geqslant 0$

$$\widehat{f}(y) \ll_j |y|^{-j} \int |f^{(j)}(x)| dx \ll_{j,f} |y|^{-j},$$

ainsi $\widehat{f}(y)$ est à décroissance rapide. Comme pour tout $j \geqslant 0$, $M^j f \in \mathscr{S}(\mathbb{R})$, en utilisant (9.1), on voit que ses dérivées la sont également : en d'autres termes

Proposition 9.5. *la transformée de Fourier envoie $\mathscr{S}(\mathbb{R})$ dans $\mathscr{S}(\mathbb{R})$.*

1.4.1. *Comportement de la transformée de Fourier par translations.* Soit $h \in \mathbb{R}$, on note $[+h]$ l'action de "translation par h" sur l'espace des fonctions sur $\mathbb{R}$

$$[+h]f : x \mapsto f(x+h).$$

L'espace de Schwartz, $\mathscr{S}(\mathbb{R})$, est invariant par $[+h]$ et vérifie (par changement de variable) la formule suivante

$$\widehat{[+h]f}(y) = e(-hy)\widehat{f}(y).$$

En particulier en considerant la transformée de Fourier du quotient

$$\frac{[+h]f(x) - f(x)}{h} = \frac{f(x+h) - f(x)}{h}$$

et en passant Ĺa limite, on obtient (9.2)

$$\widehat{f'}(y) = (-2\pi i y)\widehat{f}(y). \tag{9.3}$$

et pour tout $j \geqslant 0$

$$\widehat{f^{(j)}}(y) = (-2\pi i y)^j \widehat{f}(y). \tag{9.4}$$

1.4.2. *Comportement de la transformée de Fourier par homothéties.* Soit $\lambda \in \mathbb{R}^\times$, on note $[\times\lambda]$ l' "homothétie de rapport λ" sur l'espace des fonctions sur $\mathbb{R}$

$$[\times\lambda]f : x \mapsto f(\lambda x).$$

Alors, par changement de variable, on a pour $f \in \mathscr{S}(\mathbb{R})$,

$$\widehat{[\times\lambda]f}(y) = \frac{1}{|\lambda|}\widehat{f}(y/\lambda) = \frac{1}{|\lambda|}[\times\lambda]\widehat{f}(y).$$

1.4.3. *Formule d'inversion de Fourier.* C'est l'un des résultat les plus important de la théorie de la transformée de Fourier : pour $f \in \mathscr{S}(\mathbb{R})$

$$\widehat{\widehat{f}} = f_{-1}, ie.\ \widehat{\widehat{f}}(x) = f(-x) \tag{9.5}$$

1.4.4. *Transformée de la Gausienne.* Soit $f(x) = \mathrm{e}^{-\pi x^2}$ alors

$$\widehat{f}(y) = f(y). \tag{9.6}$$

Rappelons comment on peut en déduire la formule d'inversion de Fourier :

1.5. Formule de Poisson.

Proposition 9.6. *Soit $f \in \mathscr{S}(\mathbb{R})$ une fonction dans la classe de Schwartz. On a la formule de Poisson : pour $u \in \mathbb{R}$*

$$\sum_{n\in\mathbb{Z}} f(n+u) = \sum_{n\in\mathbb{Z}} \widehat{f}(n)e(-nu).$$

Preuve. Posons

$$f_{\mathbb{Z}}(u) := \sum_{n\in\mathbb{Z}} f(n+u).$$

Comme $f \in \mathscr{S}(\mathbb{R})$, la série qui définit $f_{\mathbb{Z}}$ converge uniformement ainsi que la série construite à partir des dérivées de f : on en déduit que $f_{\mathbb{Z}} \in \mathscr{C}^{\infty}(\mathbb{R})$. De plus $f_{\mathbb{Z}}$ est périodique de période 1. Ainsi par décomposition de Fourier on a

$$f_{\mathbb{Z}}(u) = \sum_{n\in\mathbb{Z}} c_{f_{\mathbb{Z}}}(n)e(nu)$$

avec

$$\begin{aligned} c_{f_{\mathbb{Z}}}(n) &= \int_0^1 f_{\mathbb{Z}}(u)e(-nu)du = \int_0^1 (\sum_{m\in\mathbb{Z}} f(n+u))e(-nu)du \\ &= \int_0^1 (\sum_{m\in\mathbb{Z}} f(m+u)e(-n(u+m)))du = \sum_{m\in\mathbb{Z}} \int_0^1 f(m+u)e(-n(u+m))du \\ &\sum_{m\in\mathbb{Z}} \int_m^{m+1} f(u)e(-nu)du = \widehat{f}(-n) \end{aligned}$$

□

On va utiliser cette formule pour analyser la fonction sommatoire d'une fonction dans les progressions arithmétiques :

Corollaire 9.7. *Soit $q, a \in \mathbb{Z}$, $q \neq 0$, on a*

$$\sum_{n\equiv a \,(\mathrm{mod}\, q)} f(n) = \frac{1}{q} \sum_{m\in\mathbb{Z}} \widehat{f}(\frac{n}{q})e(\frac{-an}{q}).$$

Preuve. On a

$$\begin{aligned} \sum_{n\equiv a \,(\mathrm{mod}\, q)} f(n) &= \sum_{n\in\mathbb{Z}} f(qn+a) = \sum_{n\in\mathbb{Z}} f(q(n+\frac{a}{q})) = \sum_{n\in\mathbb{Z}} [\times q]f(n+\frac{a}{q}) \\ &= \sum_{n\in\mathbb{Z}} \widehat{[\times q]f}(n)e(-\frac{an}{q}) = \frac{1}{q}\sum_{n\in\mathbb{Z}} \widehat{f}(\frac{n}{q})e(-\frac{an}{q}). \end{aligned}$$

□

2. Transformée de Mellin

Soit $f \in \mathscr{C}^{\infty}(\mathbb{R}_{\geqslant 0})$ une fonction qui quand $x \to +\infty$ est à décroissance rapide ainsi que toutes ses dérivés ; la transformée de Mellin de f est définie pour $\Re s > 0$ par

$$\widetilde{f}(s) = \int_{\mathbb{R}_{>0}} f(x)x^s d^{\times}x.$$

Dans cette égalité, on a posé

$$d^{\times}x := \frac{dx}{x};$$

notons que cette mesure est invariante par les translation de $(\mathbb{R}_{>0}, \times)$ $x \mapsto yx$. L'integrale $\widetilde{f}(s)$ converge en 0 car $\Re s > 0$ et en ∞ car f décroit rapidement. La convergence est uniforme sur les compacts de $\Re s > 0$ et définit une fonction holomorphe de s. Notons que si f vérifie $f(x) = O(x^N)$ (quand $x \to 0$) alors $\widetilde{f}(s)$ définit une fonction holomorphe pour $\Re s > -N$.

Par intégration par parties, on a

$$\widetilde{f}'(s) = -(s-1)\widetilde{f}(s-1). \tag{9.7}$$

En particulier comme $\widetilde{f}'(s)$ est définie pour $\Re s > 0$, cela définit par prolongement analytique $\widetilde{f}(s)$ pour $\Re s > -1$ avec un pole simple en $s = 0$ de résidu $-\widetilde{f}'(1) = -\int_0^\infty f'(y)dy = f(0)$. En itérant, on obtient le prologement méromorphe de $\widetilde{f}(s)$ sur $\mathbf{C}$ avec des poles au plus simple en $s = -n$, $n \in \mathbb{N}$. Si de plus f s'annule en 0 alors $\widetilde{f}(s)$ est holomorphe pour $\Re s > -1$ et plus généralement, si toutes ses dérivées de f jusqu'à l'ordre $n \geqslant 0$ s'annulent en 0 alors $\widetilde{f}(s)$ est holomorphe pour $\Re s > -(n+1)$.

Par ailleurs l'itération de (9.7) implique

$$\widetilde{f}(s) = \frac{(-1)^n}{s(s+1)\dots(s+n-1)}\widetilde{f^{(n)}}(s+n)$$

implique que pour tout $n \geqslant 0$, $|\Re s| \leqslant \sigma$ et $|\Im s| \geqslant 1$ on a

$$|\widetilde{f}(s)| \ll_{\sigma,f} \frac{1}{(|s|)^n}. \tag{9.8}$$

2.1. Exemple : la fonction Γ. La fonction Γ est par définition la transformée de Mellin de la fonction $x \mapsto \exp(-x)$:

$$\Gamma(s) := \widetilde{e^{-x}}(s) = \int_0^\infty e^{-x} x^s d^\times x.$$

Cette fonction vérifie pour $\Re s > 0$

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

Ainsi $\Gamma(s)$ admet un prolongement holomorphe à $\mathbf{C}$ avec des poles en $s = -n$, $n \in \mathbb{N}$ de résidus $(-1)^n/n!$.

2.2. Homotheties. Soit $\lambda > 0$, on a

$$\widetilde{f_\lambda}(s) = \lambda^{-s}\widetilde{f}(s).$$

2.3. Transformée de Mellin et Transformée de Fourier. Soit $f \in \mathscr{C}_c^\infty(\mathbb{R}_{>0})$, on définit $g \in \mathscr{C}_c^\infty(\mathbb{R})$ par changement de variable

$$f(y) = g(\log y),\ g(x) = f(\exp(x))$$

En particulier $\widetilde{f}(s)$ définit une fonction holomorphe sur $\mathbf{C}$. On a, posant $s = \sigma + it$

$$\begin{aligned}\widetilde{f}(s) &= \int_0^\infty g(\log y)\exp(s\log y)dy/y = \int_{-\infty}^{+\infty} g(x)\exp(sx)dx \\ &= \int_{-\infty}^{+\infty} g(x)\exp(\sigma x)e(\frac{xt}{2\pi})dx = \widehat{g\exp(\sigma x)}(\frac{t}{2\pi}).\end{aligned}$$

En particulier, utilisant (9.5), on obtient

$$\int_{\mathbb{R}} \widetilde{f}(\sigma + it)dt = \int_{\mathbb{R}} \widehat{g\exp(\sigma x)}(\frac{t}{2\pi})dt = 2\pi g\exp(0) = 2\pi f(1)$$

que l'on peut encore écrire

$$\frac{1}{2\pi i}\int_{(\sigma)} \widetilde{f}(s)ds = f(1).$$

Remplaçant f par f_y, on obtient la *Formule d'inversion de Mellin* : pour tout $y>0$ et tout $\sigma\in\mathbb{R}$

$$\frac{1}{2\pi i}\int_{(\sigma)} \widetilde{f}(s)y^{-s}ds = f(y).$$

Notons que cette formule reste valable pour tout $f\in\mathscr{S}(\mathbb{R})$ si on suppose que $\sigma>0$.

3. L'équation fonctionnelle de la fonction ζ de Riemann

THÉORÈME. *Soit*

$$\Lambda(s)=\zeta_\infty(s)\zeta(s)\ \ \zeta_\infty(s)=\pi^{-s/2}\Gamma(s/2),\ \Re s>1.$$

Cette fonction se prolonge méromorphiquement à $\mathbf{C}$*, est holomorphe sur holomorphe sur* $\mathbf{C}-\{0,1\}$ *et a des pôles simples en* $s=0,1$ *; elle vérifie l'équation fonctionelle*

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

En particulier, la fonction $\zeta(s)=\sum_{n\geqslant 1}\frac{1}{n^s}$*,* $\Re s>1$ *se prolonge en une fonction méromorphe sur* $\mathbf{C}$*, holomorphe sur* $\mathbf{C}-\{1\}$*, avec un pôle simple en* $s=1$ *de résidu* 1*. Elle vérifie l'équation fonctionnelle*

Preuve. La deuxième partie concernant $\zeta(s)$ résulte de la première et du fait que $\zeta_\infty(s)$ ne s'annule pas sur $\mathbf{C}$ et a un pôle simple en $s=0$. Le principe de la preuve de la première partie consiste à faire apparaître la série $\zeta(s)$, via la propriété d'invariance par homothétie de la transformée de Mellin §2.2. Plus précisément soit $f\in\mathscr{S}(\mathbb{R})$ et $\Re s>1$, on a pour tout $n\geqslant 1$,

$$\widetilde{f_n}(s)=\widetilde{f}(s)n^{-s}$$

et donc

$$\widetilde{f}(s)\zeta(s)=\sum_{n\geqslant 1}\widetilde{f_n}(s)=\sum_{n\geqslant 1}\int_{\mathbb{R}_{>0}} f(nx)x^s d^\times x=\int_{\mathbb{R}_{>0}}(\sum_{n\geqslant 1} f(nx))x^s d^\times x.$$

Dans la derniére égalité, l'intervertion de la somme et de l'intégrale est justifiée car pour tout $x>0$ et tout $A\geqslant 2$

$$\sum_{n\geqslant 1}|f(nx)|\ll_A \sum_{n\geqslant 1}(1+nx)^{-A}\ll_A \min(x^{-1},x^{-A})$$

comme on le voit en distinguant les cas $x<1$ et $x\geqslant 1$; ainsi la double somme est absolument uniformément convergente dans toute bande verticale $\{s\in\mathbf{C},\ \Re e s\in[a,b]\}$ avec $1<a\leqslant b$.

En fait l'intégrale précédente est absolument convergente en $+\infty$ pour tout $s\in\mathbf{C}$ mais pourrait diverger en 0 si $\Re s<1$. On subdivise donc l'intégrale en deux intégrales

$$\int_{\mathbb{R}_{>0}}\cdots=\int_0^1\cdots+\int_1^\infty\cdots$$

Dans la première, on fait le changement de variable $x\leftrightarrow 1/x$, on obtient alors

$$\widetilde{f}(s)\zeta(s)=\int_1^\infty(\sum_{n\geqslant 1} f(n/x))x^{-s}d^\times x+\int_1^\infty(\sum_{n\geqslant 1} f(nx))x^s d^\times x.$$

Supposons f paire ; on a alors

$$\sum_{n\geqslant 1} f(n/x)=\frac{1}{2}\sum_{n\in\mathbb{Z}} f(n/x)-\frac{1}{2}f(0)$$

appliquant la formule de Poisson au premier terme et appliquant §**??** avec $\lambda = 1/x$, on obtient

$$\sum_{n\geqslant 1} f(n/x) = \frac{1}{2}(\widehat{f}(0)x - f(0)) + x\sum_{n\geqslant 1}\widehat{f}(nx).$$

On a

$$\int_1^\infty \frac{1}{2}(\widehat{f}(0)x - f(0))x^{-s}d^\times x = -\frac{1}{2}(\frac{\widehat{f}(0)}{1-s} + \frac{f(0)}{s})$$

et donc

$$\widetilde{f}(s)\zeta(s) = -\frac{1}{2}(\frac{\widehat{f}(0)}{1-s} + \frac{f(0)}{s}) + \int_1^\infty (\sum_{n\geqslant 1} f(nx))x^s d^\times x + \int_1^\infty (\sum_{n\geqslant 1}\widehat{f}(nx))x^{1-s}d^\times x. \tag{9.9}$$

Comme f et $\widehat{f}$ sont à décroissance rapide quand $x \to +\infty$, on a pour tout $A \geqslant 0$ et tout $x \geqslant 1$

$$\sum_{n\geqslant 1} f(nx),\ \sum_{n\geqslant 1}\widehat{f}(nx) \ll_A x^{-A}$$

et les deux intégrales précédentes convergent absolument et uniformément dans tout bande verticale $\{s \in \mathbf{C},\ \Re e s \in [a,b]\}$, avec $a < b \in \mathbb{R}$; ces integrales définissent donc des fonctions holomorphes sur $\mathbf{C}$. Ainsi la fonction

$$s \mapsto \widetilde{f}(s)\zeta(s)$$

admet un prolongement méromorphe à $\mathbf{C}$, holomorphe sur $\mathbf{C} - \{0,1\}$ et avec au plus deux pôles simples en $s = 0, 1$.

D'autre part si on remplace f par $\widehat{f}$ et s par $1-s$ dans l'identité précédente et qu' on utilise que

$$\widehat{\widehat{f}}(x) = f(-x) = f(x),$$

on obtient une *equation fonctionnelle*

Théorème 9.8. *Soit $f \in \mathscr{S}(\mathbb{R})$, paire, alors la fonction définie pour $\Re s > 1$*

$$s \to \tilde{f}(s)\zeta(s)$$

admet un prolongement mésomorphe à $\mathbf{C}$ avec au plus deux pôles simples en $s = 0, 1$ de résidus en $s = 0,\ s = 1$

$$-f(0)/2,\ \hat{f}(0)/2$$

et vérifie l'équation fonctionnelle

$$\widetilde{f}(s)\zeta(s) = \widetilde{\widehat{f}}(1-s)\zeta(1-s).$$

En particulier, si f est telle que $\widehat{f} = f$, on obtient

$$\widetilde{f}(s)\zeta(s) = \widetilde{f}(1-s)\zeta(1-s).$$

Un exemple d'une telle fonction est la *Gausienne*

$$f(x) = \exp(-\pi x^2) \tag{9.10}$$

qui vérifie

$$\widetilde{f}(s) = \frac{1}{2}\pi^{-s/2}\widetilde{\exp(-y)}(s/2) = \frac{1}{2}\pi^{-s/2}\Gamma(s/2).$$

□

4. Fonctions L de Dirichlet

On considère maintenant le cas des fonctions L de Dirichlet. Soit $\chi(q)$ un caractère de Dirichlet de module $q>1$, on veut ètudier lespropriétés analytiques de sa fonction L. Notons d'abord que si $\chi(q)$ est induit par le caractère primitif $\chi^*(q^*)$ alors

$$L(\chi,s)=\prod_{p|q}(1-\frac{\chi^*(p)}{p^s})L(\chi^*,s) \tag{9.11}$$

et donc les propriétés analytiques de $L(\chi,s)$ se déduisent facilement de celles de $L(\chi^*,s)$. Dans la suite on va supposer que χ est primitif et non-trivial.

Théorème 9.9. *soit $\chi(q)$ un caractère primitif non-trivial. Posons*

$$L_\infty(\chi,s)=\begin{cases}\pi^{-s/2}\Gamma(s/2) & si\ \chi\ est\ pair\\ \pi^{-(s+1)/2}\Gamma(\frac{s+1}{2}), & si\ \chi\ est\ impair.\end{cases}$$

et

$$\Lambda(\chi,s):=q^{s/2}L_\infty(\chi,s)L(\chi,s);$$

alors $\Lambda(\chi,s)$ admet un prolongement holomorphe à $\mathbf{C}$ et vérifie l'équation fonctionnelle

$$\Lambda(\chi,s)=\varepsilon(\chi)\Lambda(\overline{\chi},1-s) \tag{9.12}$$

avec

$$\varepsilon(\chi)=\begin{cases}\frac{\tau_\chi}{\sqrt{q}} & si\ \chi\ est\ pair\\ i\frac{\tau_\chi}{\sqrt{q}} & si\ \chi\ est\ impair\end{cases}$$

et

$$\tau_\chi=\sum_{a(q)}\chi(a)\mathrm{e}(\frac{a}{q})$$

désigne la somme de Gauss.

Preuve. Soit $f\in\mathscr{S}(\mathbb{R})$; on supposera que f est de même paritè que χ. Comme on a pour $\Re es>1$ (utilisant que $|\chi(n)|\leqslant 1$)

$$\widetilde{f}(s)L(\chi,s)=\sum_{n\geqslant 1}\chi(n)\widetilde{f_n}(s)=\int_{\mathbb{R}>0}(\sum_{n\geqslant 1}\chi(n)f(nx))x^s d^\times x.$$

On sèpare l'intégrale en deux parties

$$\widetilde{f}(s)L(\chi,s)=\int_{\mathbb{R}_{>0}}\cdots=\int_0^1\cdots+\int_1^\infty\cdots$$

et la seconde intégrale définit une fonction holomorphe sur $\mathbf{C}$. Par changement de variable $x\leftrightarrow 1/x$, on a

$$\int_0^1\cdots=\int_1^\infty(\sum_{n\geqslant 1}\chi(n)f(n/x))x^{-s}d^\times x$$

Pour tout $x>0$, la fonction $n\mapsto\chi(n)f(n/x)$ est paire et vaut 0 en $n=0$, on a donc

$$\sum_{n\geqslant 1}\chi(n)f(n/x)=\frac{1}{2}\sum_{n\in\mathbb{Z}}\chi(n)f(n/x).$$

On voudrait appliquer la formule de Poisson ; pour cela, on utilise le fait que $n\mapsto\chi(n)$ ne dèpend que de la classe de congruence $n(\mathrm{mod}\,q)$:

$$\sum_{n\in\mathbb{Z}}\chi(n)f(n/x)=\sum_{a(q)}\chi(a)\sum_{n\equiv a(q)}f(n/x)=\sum_{a(q)}\chi(a)\sum_{m\in\mathbb{Z}}f(\frac{q}{x}(m+\frac{a}{q})).$$

Par la formule de Poisson, on a

$$\sum_{m\in\mathbb{Z}} f(\frac{q}{x}(m+\frac{a}{q})) = \sum_{m\in\mathbb{Z}} \widehat{f_{\frac{q}{x}}}(m)\mathrm{e}(-\frac{am}{q}) = \frac{x}{q}\sum_{m\in\mathbb{Z}} \widehat{f}(\frac{x}{q}m)\mathrm{e}(-\frac{am}{q})$$

et

$$\sum_{n\in\mathbb{Z}} \chi(n)f(n/x) = \frac{x}{q}\sum_{m\in\mathbb{Z}} \widehat{f}(\frac{x}{q}m)\sum_{a(q)} \chi(a)\mathrm{e}(-\frac{am}{q}) = \frac{x}{q}\sum_{m\in\mathbb{Z}} \widehat{f}(\frac{x}{q}m)\tau_\chi(-m).$$

Comme χ est primitif, on a

$$\tau_\chi(-m) = \chi(-1)\overline{\chi}(m)\tau_\chi$$

et donc

$$\sum_{n\in\mathbb{Z}} \chi(n)f(n/x) = \frac{x}{q}\chi(-1)\tau_\chi\sum_{m\in\mathbb{Z}} \widehat{f}(\frac{x}{q}m)\overline{\chi}(m) = 2\frac{x}{q}\chi(-1)\tau_\chi\sum_{m\geqslant 1} \widehat{f}(\frac{x}{q}m)\overline{\chi}(m).$$

On obtient finalement

$$\int_0^1 \cdots = \frac{\chi(-1)\tau_\chi}{q}\int_1^\infty (\sum_{n\geqslant 1} \widehat{f}(\frac{xn}{q})\overline{\chi}(n))x^{1-s}d^\times x$$

Comme $\widehat{f}$ est à décroissance rapide, cette intégrale converge absolument et uniformement sur les compacts de $\mathbf{C}$ et définit une fonction holomorphe sur $\mathbf{C}$. Ainsi

$$\widetilde{f}(s)L(\chi,s) = \int_1^\infty (\sum_{n\geqslant 1} \chi(n)f(nx))x^s d^\times x + \frac{\chi(-1)\tau_\chi}{q}\int_1^\infty (\sum_{n\geqslant 1} \widehat{f}(\frac{xn}{q})\overline{\chi}(n))x^{1-s}d^\times x$$

admet un prolongement analytique au plan complexe.

Dans l'égalité précédente, remplaçons f par $(\widehat{f})_{1/q}$, χ par $\overline{\chi}$ et s par $1-s$; la transformée de $(\widehat{f})_{1/q}$ vaut

$$q(\widehat{\widehat{f}})_q(x) = qf(-qx) = \chi(-1)qf(qx)$$

et on on obtient donc

(9.13)

$$q^s\widetilde{\widehat{f}}(s)L(\overline{\chi},1-s) = \int_1^\infty (\sum_{n\geqslant 1} \widehat{f}(n\frac{x}{q})\overline{\chi}(n))x^{1-s}d^\times x + \tau_{\overline{\chi}}\int_1^\infty (\sum_{n\geqslant 1} \chi(n)f(nx))x^s d^\times x = \frac{q}{\chi(-1)\tau_\chi}\widetilde{f}(s)L(\chi,s);$$

ici, on a utilisé l'égalité $\tau_{\overline{\chi}} = \chi(-1)q/\tau_\chi$ qui résulte de (14.3). Ainsi on obtient l'équation fonctionnelle

$$q^{s/2}L(\chi,s)\widetilde{f}(s) = \frac{\tau_\chi}{q^{1/2}}q^{\frac{1-s}{2}}L(\overline{\chi},1-s)\widetilde{\widehat{f}}(1-s). \tag{9.14}$$

Prenons

$$f(x) = \begin{cases} e^{-\pi x^2}, & \text{si } \chi(-1)=1, \\ (e^{-\pi x^2})' = -2\pi x e^{-\pi x^2}, & \text{si } \chi(-1)=-1. \end{cases} \tag{9.15}$$

On a (utiliser (9.3))

$$\widehat{f}(x) = \begin{cases} f(x), & \text{si } \chi(-1)=1, \\ if(x), & \text{si } \chi(-1)=-1, \end{cases}$$

et, pour les transformées de Mellin, on a

$$\widetilde{f}(s) = \begin{cases} \frac{1}{2}\pi^{-s/2}\Gamma(\frac{s}{2}), & \text{si } \chi(-1)=1, \\ = -\frac{s-1}{2}\pi^{-\frac{s-1}{2}}\Gamma(\frac{s-1}{2}) = -\pi\pi^{-\frac{s+1}{2}}\Gamma(\frac{s+1}{2}), & \text{si } \chi(-1)=-1. \end{cases}$$

On déduit de ces identités et de (9.14) l'équation fonctionnelle (9.12)

CHAPITRE 10

La factorisation d'Hadamard

Dans ce chapître, on établit un formule (dite de factorisation de Hadamard) qui exprime les fonctions $L(\chi, s)$ comme un produit infini indexè par leurs zéros. En fait cette factorisation est valable pour un classe très générale de fonctions holomorphe : celles d'ordre $\leqslant 1$.

1. Fonctions d'ordre borné

Définition 10.1. *Soit $\alpha \geqslant 0$, Une fonction $f : s \to f(s)$ holomorphe sur $\mathbf{C}$ est dite d'ordre borné si il existe une constante $\alpha \geqslant 0$ telle que, pour tout $s \in \mathbf{C}$ et tout $\varepsilon > 0$, on a*

$$|f(s)| \ll_{\varepsilon,f} \exp(|s|^{\alpha+\varepsilon}).$$

On dira que f est d'ordre $\leqslant \alpha$. On dira que f est d'ordre α, si elle est d'ordre $\leqslant \alpha$ mais pas d'ordre $\leqslant \alpha'$ pour tout $\alpha' < \alpha$.

Exemple(s) 10.2. Un polynôme est une fonction d'ordre 0.

La fonction exponentielle $s \to \exp(s)$ est d'ordre 1.

Plus généralement, une fonction de la forme $s \to \exp(P(s))$ avec P un polynùme est d'ordre $\deg P$.

Le dernier exemple est une fonction d'ordre $\alpha = \deg(P)$ qui ne s'annule pas sur $\mathbf{C}$; on a la rèciproque suivante :

Lemme 10.3. *Une fonction d'ordre $\leqslant \alpha$ qui ne s'annule pas sur $\mathbf{C}$ est de la forme*

$$f(s) = \exp(P(s))$$

avec P un polynùme de degrè $\leqslant \alpha$.

Preuve. Puisque $f(s)$ ne s'annule pas, la fonction logarithme $g(s) = \log(f(s))$ est bien définie et holomorphe sur $\mathbf{C}$. Considèrons son développement de Taylor en $s = 0$

$$g(s) = \sum_{n \geqslant q0} c_n s^n$$

on va montrer que $c_n = 0$ si $n > \alpha$ ce qui donnera le résultat. On a pour $R > 0$ (formules de Cauchy)

$$c_n = \frac{1}{R^n} \int_{[0,1]} g(R.\mathrm{e}(x))\mathrm{e}(-nx)dx.$$

Par hypothèse, on a

$$\Re g(s) = \log|f(s)| \leqslant C_{\varepsilon,f} R^{\alpha+\varepsilon}, \ |s| \leqslant R;$$

supposons que l'on ait la majoration plus forte

$$|g(s)| \ll_{\varepsilon,f} R^{\alpha+\varepsilon}, \ |s| \leqslant R,$$

alors, on aurait

$$|c_n| \ll_{\varepsilon,f} R^{\alpha+\varepsilon-n}$$

qui impliquerais la conclusion recherchée. Malheureusement on ne dispose que d'une majoration le la partie réelle de de $g(s)$; cela va nous obliger à quelques contortions : on dècompose c_n en sa partie réelle et sa partie imaginaire, $c_n = a_n + ib_n$. Posant $s = R.\mathrm{e}(x)$ on a

$$\Re g(s) = \sum_{n\geqslant 0} a_n R^n \cos(2\pi nx) - \sum_{n\geqslant 1} b_n R^n \sin(2\pi nx)$$

et ainsi

$$a_n R^n = 2\int_{[0,1]} \Re g(s)\cos(2\pi nx)dx$$

et donc

$$|a_n|R^n \leqslant 2\int_{[0,1]} |\Re g(R.\mathrm{e}(x))|dx = 2\int_{[0,1]} \big(|\Re g(R.\mathrm{e}(x))| + \Re g(R.\mathrm{e}(x))\big)\,dx - 2a_0,$$

en effet

$$2\int_{[0,1]} \Re g(R.\mathrm{e}(x))dx = 2a_0.$$

On note que

$$|\Re g(R.\mathrm{e}(x))| + \Re g(R.\mathrm{e}(x)) = 2\max(0, \Re g(R.\mathrm{e}(x))) \leqslant C_{\varepsilon,f} R^{\alpha+\varepsilon}$$

et donc, pour $n > \alpha$

$$|a_n| \leqslant (R^{\alpha+\varepsilon-n} + 2|a_0|R^{-n}) \to 0 \;\; R \to +\infty.$$

Le même raisonnement (en remplaçant $\cos(2\pi nx)$ par $\sin(2\pi nx)$) montre que pour $n > \alpha$, $b_n = 0$ et ainsi $c_n = 0$. □

Remarque 10.4. Notons que la conclusion du Lemme 10.3 reste valide si la condition suivante (et a priori plus faible) sur f est satisfaite :

Il existe une suite de réels positifs $(R_n)_{n\geqslant 0}$ *vérifiant* $R_n \to +\infty$, $n \to +\infty$ *et telle que pour tout* $n \geqslant 0$, *tout* $\varepsilon > 0$, *et tout* $s \in \mathbf{C}$ *de module* $|s| = R_n$, *on ait*

$$f(s) \ll_{f,\varepsilon} \exp(|s|^{\alpha+\varepsilon}).$$

En fait, par le principe du maximum, cette dernière condition implique que f est d'ordre au plus α.

2. Première estimation des zéros

Pour $R > 0$, notons

$$Z(f,R) := \{\rho \in \mathbf{C},\ f(\rho) = 0,\ |\rho| \leqslant R\} \subset Z(f) := \{\rho \in \mathbf{C},\ f(\rho) = 0\},$$

l'ensemble des zéros de f contenus dans le disque de rayon R et l'ensemble de tous les zéros de f dans $\mathbf{C}$. Dans la suite, la convention suivante sera commode : ètant donnè $k : Z(f) \to \mathbf{C}$ une fonction définie sur $Z(f)$, les expressions

$$\text{"}\sum_{\rho\in Z(f,R)} k(\rho)\text{"},\ \text{"}\prod_{\rho\in Z(f,R)} k(\rho)\text{"}$$

seront utilisèes comme raccourcit pour la somme et le produit suivant

$$\sum_{\rho\in Z(f,R)} m(\rho)k(\rho),\quad \prod_{\rho\in Z(f,R)} k(\rho)^{m(\rho)}$$

où $m(\rho)$ est l'ordre d'annulation de f en ρ (ou encore la *multiplicité* de ρ). En particulier, la notation

$$N(f,R) := \sum_{\rho\in Z(f,R)} 1$$

dèsignera le nombre de zéros de f de module $\leqslant R$ *comptè avec multiplicité.*

Théorème 10.5. *Soit f une fonction d'ordre $\leqslant \alpha$; pour tout R, et tout $\varepsilon > 0$, on a la majoration*

$$N(f,R) \ll_{\varepsilon,f} R^{\alpha+\varepsilon}.$$

En particulier la série

$$\sum_{\rho \in Z(f)} \frac{1}{1+|\rho|^{\alpha+\varepsilon}}$$

converge.

La preuve utilise la formule suivante :

Proposition (formule de Jensen)**.** *Soit $R > 0$ et f une fonction holomorphe dans un voisinage du disque $\{s \in \mathbf{C},\ |s| \leqslant R\}$. Supposons que f ne s'annule ni en 0 ni sur le cercle de rayon R, $\{s \in \mathbf{C},\ |s| = R\}$; on a l'égalité*

$$\int_{[0,1]} \log|f(R.\mathrm{e}(t))/f(0)|dt = \log\prod_{\rho}\frac{R}{|\rho|} = \sum_{\rho}\log\frac{R}{|\rho|}$$

où ρ parcourt l'ensemble des zéros de f de module $\leqslant R$ (comptès avec multiplicité).

Preuve. On factorise $f(s)$ en

$$f(s) = F(s)\prod_{\rho}(s-\rho)$$

avec $F(s)$ une fonction holomorphe et ne s'annulant pas pour $|s| \leqslant R$. On a alors

$$\log|f(s)/f(0)| = \log|F(s)/F(0)| + \sum_{\rho}\log|(s-\rho)/\rho|$$

et il suffit de montrer l'égalité de l'ènoncè pour chaque terme de la somme ci-dessus. Pour le premier terme on a $\log|F(s)/F(0)| = \Re\log F(s)/F(0)$ et $\log F(s)/F(0)$ est une fonction holomorphe au voisinage du disque de rayon R et qui s'annule au point $s = 0$, le fait que $\int_{[0,1]}\log(F(R.\mathrm{e}(t))/F(0))dt = 0$ résulte du théorème des rèsidus. Pour les autre termes on remarque que

$$\log|(R\mathrm{e}(t)-\rho)/\rho| = \log(R/|\rho|) + \log|1-\frac{\overline{\rho}}{R}\mathrm{e}(t)|$$

et le fait que $\int_{[0,1]}\log|1-\frac{\overline{\rho}}{R}\mathrm{e}(t)|dt = 0$ résulte du fait que la fonction $s \to \log(1-\frac{\overline{\rho}}{R}s)$ est une fonction holomorphe au voisinage du disque unitè s'annulant en 0. □

Preuve. (du théorème 10.5) On peut toujours supposer que $f(0) \neq 0$ quitte à remplacer $f(s)$ par $f(s)/s^m$ pour $m \geqslant 0$ un entier convenable (la nouvelle fonction reste d'ordre $\leqslant \alpha$). Soit $R > 0$, quitte à remplacer R par R' avec $R' - R \in [0,1]$, on peut supposer que f ne s'annule pas sur le cercle de rayon $2R$. Soit $\rho \in Z(f,R)$ alors $\log(2R/|\rho|) \geqslant \log 2$ et donc la formule de Jensen nous donne alors que

$$(\log 2)N(f,R) \leqslant \sum_{|\rho|\leqslant R}\log(2R/|\rho|) \leqslant \sum_{|\rho|<2R}\log(2R/|\rho|) = \int_{[0,1]}\log|f(2R.\mathrm{e}(t))/f(0)|dt.$$

Comme f est d'ordre $\leqslant \alpha$, cette dernière intègrale est majorée par $\ll_{\varepsilon} (2R)^{\alpha+\varepsilon}$ pour tout $\varepsilon > 0$. □

Théorème 10.6 (Factorisation de Hadamard)**.** *Soit $f(s)$ une fonction holomorphe d'ordre au plus 1 telle que $f(0) \neq 0$, alors on a*

$$f(s) = A\exp(bs) \prod_{\rho \in Z(f)} (1 - \frac{s}{\rho})\mathrm{e}^{s/\rho}$$

avec $A = f(0)$, $b = f'(0)/f(0)$ et le produit est uniformément convergent sur les compacts de $\mathbf{C}$.

Preuve. soit $K \subset \mathbf{C}$ un compact ; $K \cap Z(f)$ est fini et pour $s \in K$ et $\rho \notin K$ un zéro, on a

$$(1 - \frac{s}{\rho})\mathrm{e}^{s/\rho} = 1 + O_K(\frac{1}{|\rho|^2}).$$

Comme la série $\sum_\rho \frac{1}{|\rho|^2}$ converge, on en déduit la convergence du produit infini uniformément sur tout compact de $\mathbf{C}$.

Considèrons le produit infini

$$h(s) = \prod_{\rho \in Z(f)} (1 - \frac{s}{\rho})\mathrm{e}^{s/\rho};$$

par construction la fonction $f(s)/h(s)$ est holomorphe et ne s'annule pas sur $\mathbf{C}$. Nous allons maintenant montrer que le quotient est une fonction d'ordre au plus 1, d'après le Lemme 10.3, cela impliquera que $f(s)/h(s) = \exp(a + bs)$ et on pourra conclure. Plus prècisèment nous allons montrer que f/h vérifie la condition de la Remarque 10.4.

D'après le théorème 10.5, il existe n_0 tel que pour tout $n \geqslant n_0$, il existe $R_n \in [n, n+1[$ vérifiant pour tout zéro $\rho \in Z(f)$

$$||\rho| - R_n| \geqslant 1/(4n^2). \tag{10.1}$$

En effet il suffit de dècomposer l'anneau d'épaisseur 1

$$\{s \in \mathbf{C},\ |s| \in [n, n+1[\}$$

en $2(n+1)^2$ sous-anneaux disjoints d'èpaisseur $1/(2(n+1)^2)$. Si chacun de ces anneaux contenait un zéro de f, le disque de rayon $n+1$ contiendrait au moins $\geqslant 2(n+1)^2$ zéros ce qui contredirait le théorème 10.5 pour n assez grand...

Soit $n \geqslant n_0 + 100$ et s tel que $|s| = R_n$, on veut minorer $|h(s)|$, pour cela il suffit de majorer

$$\log(|h(s)|^{-1}) = -\sum_\rho \log|(1 - \frac{s}{\rho})e^{s/\rho}|$$

et on dècompose la somme en trois parties

$$\log(|h(s)|^{-1}) = -\sum_{|\rho| \leqslant |s|-1} \cdots - \sum_{|\rho|-|s| \in]-1,1]} \cdots - \sum_{|\rho| \geqslant |s|+1} \cdots$$

Soit ρ apparaissant dans le premier terme, on a

$$-\log|(1 - \frac{s}{\rho})e^{s/\rho}| = -\log|1 - \frac{s}{\rho}| - \Re(\frac{s}{\rho}) \leqslant \log R_n + \frac{|s|}{|\rho|}$$

et donc le premier terme est majoré par

$$\sum_{|\rho| \leqslant R_n - 1} \log R_n + \frac{R_n}{|\rho|} \ll_\varepsilon N(f, R_n)\log R_n + \sum_{|\rho| \leqslant R_n - 1} \frac{R_n^{1+\varepsilon}}{|\rho|^{1+\varepsilon}} \ll_\varepsilon R_n^{1+\varepsilon};$$

Dans cette majoration on a utilisé le fait que pour $\varepsilon > 0$

$$|\frac{R_n}{\rho}| \geqslant 1 \Rightarrow |\frac{R_n}{\rho}|^{1+\varepsilon} \geqslant |\frac{R_n}{\rho}|.$$

Le second terme est majoré en valeur absolue par

$$\sum_{|\rho|-|s|\in]-1,1]} \log(R_n^3) \ll_{\varepsilon,f} R_n^{1+\varepsilon}.$$

car pour de tels ρ, on a par (10.1)

$$R_n^{-3} \ll |(1-\frac{s}{\rho})e^{s/\rho}| \ll 1$$

Le troisième terme est majoré en valeur absolue par

$$\sum_{|\rho|\geqslant 1+R_n} \log(1+O(\frac{|s|^2}{|\rho|^2})) = \sum_{|\rho|\geqslant 1+R_n} R_n^2/|\rho|^2 \leqslant R_n^{1+\varepsilon} \sum_{|\rho|\geqslant 1+R_n} 1/|\rho|^{1+\varepsilon} \ll_\varepsilon R_n^{1+\varepsilon}$$

(comme $|s|/|\rho| < 1$ on l'obtient en prenant le dévelopement de Taylor $(1-s/\rho)e^{s/\rho} = 1 + O(|s|^2/|\rho|^2)$). Ainsi, on obtient la majoration

$$|h(s)|^{-1} \ll_{\varepsilon,f} \exp(R_n^{1+\varepsilon}),$$

pour tout $\varepsilon > 0$.

Il existe donc une suite $(R_n)_{n\geqslant 0}$, $R_n \to +\infty$ telle que tout n, tout $\varepsilon > 0$ et s de module R_n, on ait

$$|f(s)/h(s)| \ll_\varepsilon \exp(R_n^{1+\varepsilon}).$$

Par la Remarque 10.4, on obtient que (comme $f(s)/h(s)$ ne s'annule pas sur $\mathbf{C}$)

$$f(s)/h(s) = \exp(a+bs)$$

pour $a, b \in \mathbf{C}$.

Notons que pour tout ρ

$$(1-\frac{s}{\rho})\mathrm{e}^{s/\rho}_{|s=0} = 1,\ \frac{d}{ds}(1-\frac{s}{\rho})\mathrm{e}^{s/\rho}_{|s=0} = 0$$

et donc

$$h(0) = 1, h'(0) = 0,\ \mathrm{e}^a = f(0),\ b = f'(0)/\mathrm{e}^a = f'(0)/f(0).$$

□

Le théorème de factorisation admet le corollaire suivant :

Corollaire 10.7. *Pour tout $s \in \mathbf{C} - Z(f)$, on a*

$$d\log f(s) := \frac{f'(s)}{f(s)} = b + \sum_{\rho\in Z(f)} \frac{1}{\rho} - \frac{1}{\rho - s}.$$

De plus la convergence de la série de droite est uniforme sur les compacts $K \subset \mathbf{C}$, tels que $K \cap Z(f) = \emptyset$.

Preuve. Par convergence uniforme du produit infini sur les compacts, on a (par les formules de Cauchy)

$$f'(s) = bf(s) + A\exp(bs)\sum_\rho ((1-\frac{s}{\rho})\mathrm{e}^{s/\rho})' \prod_{\rho'\neq\rho} (1-\frac{s}{\rho'})\mathrm{e}^{s/\rho'} = bf(s) + A\exp(bs)h(s)\sum_\rho \frac{((1-\frac{s}{\rho})\mathrm{e}^{s/\rho})'}{(1-\frac{s}{\rho})\mathrm{e}^{s/\rho}}$$

et donc pour tout $s \notin Z(f)$

$$\frac{f'(s)}{f(s)} = b + \sum_\rho \frac{((1-\frac{s}{\rho})\mathrm{e}^{s/\rho})'}{(1-\frac{s}{\rho})\mathrm{e}^{s/\rho}} = b + \sum_{\rho\in Z(f)} \frac{1}{\rho} - \frac{1}{\rho - s}.$$

Comme pour $s \neq \rho$

$$\frac{1}{\rho} - \frac{1}{\rho - s} = O_{s,s-\rho}(\frac{1}{|\rho|^2})$$

la série converge uniformément sur les compacts qui évitent $Z(f)$. $\square$

CHAPITRE 11

Les formules explicites

On va appliquer la théorie précédente à la fonction holomorphe

$$\xi(s) := s(1-s)\zeta_\infty(s)\zeta(s).$$

Proposition 11.1. *Cette fonction est d'ordre au plus* 1.

Preuve. Par l'équation fonctionnelle, on a

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

on peut donc supposer que $\Re e s > 1/2$; par (9.9) et (9.10) on a

$$\xi(s) = -1 + 2s(1-s)\int_1^\infty (\sum_{n\geqslant 1} \mathrm{e}^{-\pi n^2 x^2}) x^s d^\times x + 2s(1-s)\int_1^\infty (\sum_{n\geqslant 1} \mathrm{e}^{-\pi n^2 x^2}) x^{1-s} d^\times x. \tag{11.1}$$

Pour $x \geqslant 1$, on a $\sum_{n\geqslant 1} \mathrm{e}^{-\pi n^2 x^2} \ll \mathrm{e}^{-\pi x^2}$ et pour $\sigma \geqslant 1/2$

$$\int_1^\infty (\sum_{n\geqslant 1} \mathrm{e}^{-\pi n^2 x^2}) x^s d^\times x \ll \int_1^\infty \mathrm{e}^{-\pi x^2} x^\sigma d^\times x \ll \pi^{-\sigma/2}\Gamma(\frac{\sigma}{2}) \ll_\varepsilon \exp(|s|^{1+\varepsilon}).$$

d'autre part, on a pour pour $\sigma \geqslant 1/2$

$$\int_1^\infty (\sum_{n\geqslant 1} \mathrm{e}^{-\pi n^2 x^2}) x^{1-s} d^\times x \ll 1$$

et cela conclut la preuve. □

1. Application au comptage des zéros de ζ.

Rappelons que l'ensemble $Z(\xi)$ de zéros de $\xi(s)$ est précisément l'ensemble des zéros non-triviaux de $\zeta(s)$ (les zéros que ne sont pas des entiers négatifs pairs). Notons que par les équations fonctionnelles, le fait que $\Gamma(s)$ ne s'annule pas sur $\mathbf{C}$ et le fait que ζ ne s'annule pas pour $\Re s > 1$, on a

$$Z(\xi) \subset \{s,\ \Re s \in [0,1]\}.$$

On utilisera la notation générique suivante pour un tel zéro

$$\rho = \beta + i\gamma,\ \beta \in [0,1],\ \gamma \in \mathbb{R}.$$

Prenant la dérivée logarithmique on voit que

$$\frac{\xi'}{\xi}(s) = \frac{1}{s} + \frac{1}{s-1} + \frac{\zeta'_\infty}{\zeta_\infty}(s) + \frac{\zeta'}{\zeta}(s) = b + \sum_{\rho\in Z(\xi)} \frac{1}{\rho} - \frac{1}{\rho - s}. \tag{11.2}$$

Notons que

$$\xi(s) = \overline{\xi(\overline{s})}:$$

Cela ce voit en considérant la représentation intégrale (11.1) et en observant que pour $s \in \mathbf{C}$ et $x \in \mathbb{R}_{>0}$, on a $\overline{x^{\overline{s}}} = x^s$. Il en résulte que le multi-ensemble $Z(\xi)$ est stable par la conjugaison complexe ($\rho \mapsto \overline{\rho}$ préserve l'ensemble des zéros ainsi que leur multiplicité). Ainsi

$$\sum_{\rho \in Z(\xi)} \frac{1}{\rho} - \frac{1}{\rho - s} = \frac{1}{2}\Big(\sum_{\rho \in Z(\xi)} \frac{1}{\rho} + \frac{1}{\overline{\rho}} - \frac{1}{\rho - s} + \frac{1}{\overline{\rho} - s}\Big).$$

Dans cette dernière somme isolons les termes $1/\rho + 1/\overline{\rho}$: on a

$$\frac{1}{\rho} + \frac{1}{\overline{\rho}} = \frac{2\beta}{|\rho|^2}, \ \beta \in [0,1]$$

et donc

$$\sum_{\rho \in Z(\xi)} \frac{1}{\rho} + \frac{1}{\overline{\rho}} \ll \sum_{\rho} \frac{1}{|\rho|^2} < \infty.$$

Il en résulte que la série

$$\frac{1}{2}\Big(\sum_{\rho \in Z(\xi)} \frac{1}{s-\rho} - \frac{1}{s - \overline{\rho}}\Big)$$

est uniformément convergente sur les compacts de $\mathbf{C} - Z(\xi)$.

On a donc montré

Proposition 11.2. *On a pour tout $s \notin Z(\xi)$,*

$$-\frac{\zeta'}{\zeta}(s) = \frac{1}{s} + \frac{1}{s-1} + \sum_{\rho \in Z(\xi)}^{*} \frac{1}{s-\rho} + \frac{\zeta'_\infty}{\zeta_\infty}(s) + O(1).$$

Dans cette sommation, on a fait la convention que l'on a regroupé les termes de la somme suivant les paires $(\rho, \overline{\rho})$:

$$\sum_{\rho \in Z(\xi)} \frac{1}{s-\rho} = \frac{1}{2} \sum_{\rho \in Z(\xi)} \frac{1}{s-\rho} + \frac{1}{s - \overline{\rho}}$$

On va maintenant se servir de cette identité pour compter plus finement les zéros de ξ : posont

$$N(T) = |\{\rho = \beta + i\gamma \in Z(\xi), \ |\gamma| \leqslant T\}|$$

Corollaire 11.3. *Pour tout $T \geqslant 1$,*

$$N(T+1) - N(T) = O(\log(2+T))$$

et

$$N(T) = O(T \log(T+1)).$$

Démonstration. Soit $s = 2 + iT$, on a (cf. les exercices)

$$\frac{\zeta'_\infty}{\zeta_\infty}(s) = O(\log(2 + |T|))$$

ainsi (avec la convention précédente concernant la sommation)

$$\sum_{\rho \in Z(\xi)} \frac{1}{\rho - s} = O(\log(2 + |T|))$$

Prenons la partie réelle de cette identité : on a ($\beta \in [0,1]$)

$$\Re\Big(\frac{1}{\rho - s}\Big) = \frac{2-\beta}{|s-\rho|^2} \geqslant \frac{1}{|2-\beta|^2 + |\gamma - T|^2} \geqslant \frac{1}{4 + |\gamma - T|^2} \geqslant \frac{1}{5}\delta_{|\gamma - T| \leqslant 1}$$

et donc

$$N(T+1)-N(T-1) \leqslant 10\sum \Re(\frac{1}{\rho-s}) = O(\log(2+T)).$$

La deuxième partie se déduit par intégration par parties □

2. Les formules explicites de Weil

Dans cette section on démontre la formule

Formule explicite. *Soit* $f \in \mathscr{C}_c^\infty(\mathbb{R}_{>0})$ *et*

$$\widetilde{f}(s) = \int_0^{+\infty} f(x)x^s \frac{dx}{x}$$

sa transformée de Mellin. Soit $\check{f}(x) = x^{-1}f(x^{-1})$. *On a l'identité*

$$\sum_{n\geqslant 1}(f(n)+\check{f}(n))\Lambda(n) = \tilde{f}(1)+\tilde{f}(0)+\frac{1}{2\pi i}\int_{(1/2)}\big(\frac{\zeta'_\infty}{\zeta_\infty}(s)+\frac{\zeta'_\infty}{\zeta_\infty}(1-s)\big)\widetilde{f}(s)ds - \sum_{\substack{\rho\in Z(\xi)\\ \beta\in[0,1]}}\widetilde{f}(\rho).$$

Preuve. On calcule de deux manières différentes l'intégrale

$$\frac{1}{2\pi i}\int_{(3/2)}\tilde{f}(s)d\log\xi(s)ds$$

Pour $\Re es > 1$ on a

$$d\log\xi(s) = \frac{1}{s}+\frac{1}{s-1}+d\log\zeta_\infty(s)-\sum_{n\geqslant 1}\frac{\Lambda(n)}{n^s}$$

si bien d'en intervertissant les sommations, on obtient grâce à la formule d'inversion de Mellin

$$\frac{1}{2\pi i}\int_{(3/2)}\tilde{f}(s)d\log\xi(s)ds = \frac{1}{2\pi i}\int_{(2)}(\frac{1}{s}+\frac{1}{s-1}+\frac{\zeta'_\infty}{\zeta_\infty}(s))\widetilde{f}(s)ds - \sum_{n\geqslant 1}\Lambda(n)\frac{1}{2\pi i}\int_{(2)}\tilde{f}(s)n^{-s}ds$$

$$= \frac{1}{2\pi i}\int_{(3/2)}(\frac{1}{s}+\frac{1}{s-1}+\frac{\zeta'_\infty}{\zeta_\infty}(s))\widetilde{f}(s)ds - \sum_{n\geqslant 1}\Lambda(n)f(n).$$

On va maintenant calculer cette intégrale par déformation de contour.

Soit $T>0$ et R_T le rectangle dont les sommets sont en $3/2\pm iT$ et $-1/2\pm iT$; par ailleurs on peut choisir T aussi grand qu'on veut de sorte que

$$\forall \rho\in Z(\xi),\ |T\pm\gamma| \gg \frac{1}{\log(T+2)}$$

On a (l'intégration se faisant dans le sens inverse des aiguilles d'une montre)

$$\frac{1}{2\pi i}\int_{R_T}\tilde{f}(s)d\log\xi(s)ds = \sum_{\substack{\zeta(\rho)=0,\\ \sigma\in[0,1],\ |t|\leqslant T}}\operatorname{res}_{s=\rho}\tilde{f}(s)d\log(\xi(s)) = \sum_{\substack{\zeta(\rho)=0,\\ \sigma\in[0,1],\ |t|\leqslant T}}\tilde{f}(\rho).$$

Quand $T\to+\infty$ les intégrales le long des segments horizontaux tendent vers 0. On obtient donc

$$\sum_{\substack{\zeta(\rho)=0,\\ \sigma\in[0,1]}}\tilde{f}(\rho) = \frac{1}{2\pi i}\int_{(3/2)}\cdots - \frac{1}{2\pi i}\int_{(-1/2)}\cdots$$

(observons que la série converge car $\tilde{f}(s) \ll (1+|\Im s|)^{-A}$ pour tout $A\gg 0$ par (9.8)).

On effectue alors le changement de variable $s \leftrightarrow 1-s$ et on utilise l'équation fonctionnelle

$$d\log\xi(s) = -d\log\xi(1-s)$$

qui donne

$$\sum_{\substack{\zeta(\rho)=0,\\ \sigma\in[0,1]}} \tilde{f}(\rho) = \frac{1}{2\pi i}\int_{(3/2)} (\tilde{f}(s)+\tilde{f}(1-s))d\log\xi(s)ds$$

$$= \frac{1}{2\pi i}\int_{(3/2)} (\frac{1}{s}+\frac{1}{s-1}+\frac{\zeta'_\infty}{\zeta_\infty}(s))(\tilde{f}(s)+\tilde{f}(1-s))ds - \sum_{n\geqslant 1}\Lambda(n)(f(n)+\check{f}(n))$$

A reste à calculer

$$\frac{1}{2\pi i}\int_{(3/2)} (\frac{1}{s}+\frac{1}{s-1})(\tilde{f}(s)+\tilde{f}(1-s))ds = \tilde{f}(1)+\tilde{f}(0)+\frac{1}{2\pi i}\int_{(1/2)} (\frac{1}{s}+\frac{1}{s-1})(\tilde{f}(s)+\tilde{f}(1-s))ds$$

par décalage de contour (on passe un pole en $s=1$ de residu $\tilde{f}(1)+\tilde{f}(0)$). Faisant le changement de variable $s\leftrightarrow 1-s$ on obtient

$$\frac{1}{2\pi i}\int_{(1/2)} (\frac{1}{s}+\frac{1}{s-1})(\tilde{f}(s)+\tilde{f}(1-s))ds = --\frac{1}{2\pi i}\int_{(1/2)} (\frac{1}{1-s}-\frac{1}{s})(\tilde{f}(1-s)+\tilde{f}(s))ds = 0$$

□

On montre maintenant comment une région sans zéros convenable implique le Théorème des nombres premiers avec un terme d'erreur explicite : dans le chapitre suivant on montrera le

Théorème 11.4 (Hadamard/de la Vallée-Poussin)**.** *Il existe $c>0$ telle que $\zeta(s)$ ne s'annule pas dans la région ($s=\sigma+it$)*

$$\sigma \geqslant 1-\frac{c}{\log(2+|t|)}.$$

Corollaire 11.5. *Il existe $C>0$, telle que pour $f\in C_c^\infty(\mathbb{R}_{>0})$ et $X\geqslant 2$*

$$\sum_{n\geqslant 1}\Lambda(n)f(\frac{n}{X}) = X\int_{\mathbb{R}} f(x)dx + O_f(X\exp(-C\sqrt{\log X})).$$

Démonstration. Soit $f_X(x)=f(x/X)$, on a

$$\tilde{f}_X(s) = \tilde{f}(s)X^s$$

et la formule explicite donne pour X assez grand (de sorte que $f(Xn)=0$ si $n\geqslant 1$)

$$\sum_{n\geqslant 1}\Lambda(n)f(\frac{n}{X}) = X\int_{\mathbb{R}} f(x)dx + \int_{\mathbb{R}} f(x)\frac{dx}{x} + \frac{1}{2\pi i}\int_{(1/2)} \Big(\frac{\zeta'_\infty}{\zeta_\infty}(s)+\frac{\zeta'_\infty}{\zeta_\infty}(1-s)\Big)\widetilde{f}(s)X^s ds$$

$$-\sum_{\substack{\zeta(\rho)=0\\ \Re\rho\in[0,1]}} \widetilde{f}(\rho)X^\rho.$$

Le second terme est un $O_f(1)$, le troisième est bornée par $O_f(X^{1/2})$ (car $|X^s|=X^{1/2}$ pour $\Re s=1/2$) et pour le troisième on a (écrivant $\rho=\beta+i\gamma$)

$$\sum_{\substack{\zeta(\rho)=0\\ \beta\in[0,1]}} |\widetilde{f}(\beta+i\gamma)|X^\beta \leqslant X\sum_{\substack{\zeta(\rho)=0\\ \beta\in[0,1]}} |\widetilde{f}(\beta+i\gamma)|X^{-\frac{c}{\log(2+|\gamma|)}} = X\sum_{\substack{\zeta(\rho)=0\\ \beta\in[0,1]}} |\widetilde{f}(\beta+i\gamma)|e^{-\frac{c\log X}{\log(2+|\gamma|)}}.$$

On fait la décomposition

$$\sum_{\substack{\zeta(\rho)=0\\ \Re\rho\in[0,1]}} \cdots = \sum_{\substack{\rho\\ \log(2+|\gamma|)\leqslant\sqrt{\log X}}} \cdots + \sum_{\substack{\rho\\ \log(2+|\gamma|)>\sqrt{\log X}}} \cdots$$

Le premier terme set majoré par

$$\ll \exp(-c\sqrt{\log X}) \sum_{\substack{\zeta(\rho)=0\\ \beta\in[0,1]}} |\widetilde{f}(\beta+i\gamma)| \ll \exp(-c\sqrt{\log X})$$

et le second par

$$\ll \sum_{\substack{\rho\\ \log(2+|\gamma|)>\sqrt{\log X}}} |\widetilde{f}(\beta+i\gamma)| \ll \exp(-\sqrt{\log X}),$$

en utilisant le fait que

$$|\widetilde{f}(\beta+i\gamma)| \ll (1+|\gamma|)^{-2}$$

quand $\gamma\to\infty$. □

Remarque 11.6. Le corollaire précédent "compte" les nombres premiers p dans une fenÂtre de taille $\sim X$ quand ceux-ci sont pondérés par $\log p.f(p/X)$ où f est une fonction (lisse a support compact) fixée. Ce choix a permit d'utiliser la décroissance rapide de $|\widetilde{f}(\beta+i\gamma)|$ qui résulte de la méthode d'intégration par partie appliquée deux fois à la transformée de Mellin. La constante implicite dans le terme $O_f(X\exp(-C\sqrt{\log X}))$ dépend donc directement de la taille de f et de ses deux premières dérivées. En choisissant des fonctions f convenables qui peuvent dépendre de X, on peut par des argument d'approximation, remplacer le terme $f(n/X)$ par la fonction caractéristique de l'intervalle $[1,X]$ et obtenir

$$\sum_{n\leqslant X}\Lambda(n) = X + O(X\exp(-C'\sqrt{\log X})),$$

avec $C'>0$ une constante absolue ce qui est la formulation originale du Théorème des Nombres Premiers. Ces argument relève de l'analyse classique et pas de la théorie analytique de la fonction ζ ; pour cette raison nous avons préfère donner la version ci-dessus qui contient toutes les idées éssentielles.