

Théorème de la progression arithmétique et angles des premiers de Gauss

Deux exposés de 1 h 30 dans le cadre de la semaine « *Autour de l'analyse harmonique de Fourier* » pour les élèves de 2^{nde} année à l'École Normale Supérieure, septembre 2022.

GAËTAN CHENEVIER

gaetan.chenevier@math.cnrs.fr

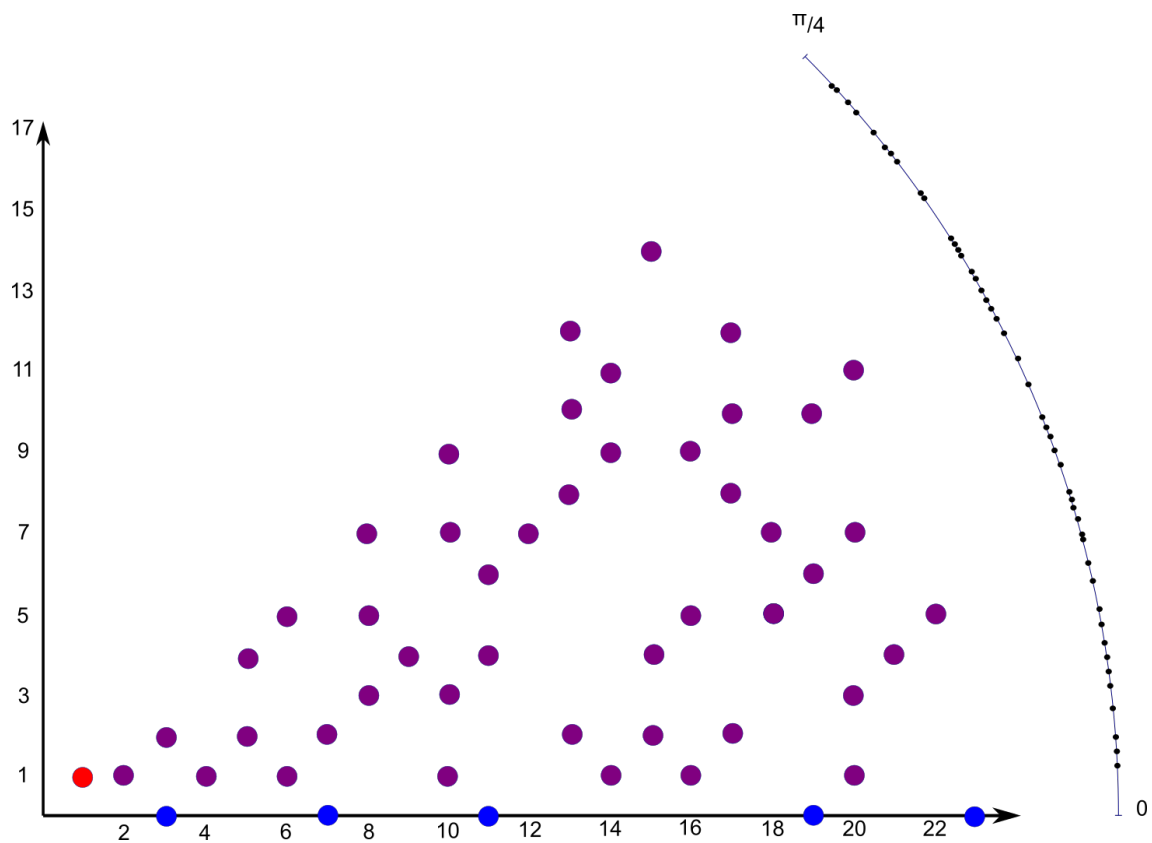


FIGURE 1. Les premiers π de $\mathbb{Z}[i]$ avec $0 \leq \text{Im } \pi \leq \text{Re } \pi$ et $|\pi| \leq 23$.

INTRODUCTION

Dans cette série de deux exposés, on se propose de démontrer deux résultats fameux de la théorie des nombres, respectivement dûs à Gustav Dirichlet (1805-1859) et Erich Hecke (1887-1947), où l’analyse harmonique joue un rôle. Ces deux résultats sont en fait les deux cas particuliers les plus “simples” d’une conjecture générale d’actualité en théorie des nombres (conjectures *à la Sato-Tate* [SER68]).

Dirichlet fut « élève » de Fourier et Poisson lors de son passage à Paris entre 1822 et 1826. Bien que passionné par la théorie des nombres, son premier résultat majeur est son critère de convergence ponctuelle des séries de Fourier (1829), qu’il a par exemple appliqué plus tard à la détermination (du “signe”) des sommes de Gauss générales, et il a d’autres contributions fameuses en analyse, par exemple sur l’équation de Laplace. Dans le premier exposé, on se propose d’expliquer sa démonstration du *théorème de la progression arithmétique*, considérée depuis comme le point de départ de la *théorie analytique des nombres*. Hecke fut lui élève de Hilbert (aussi descendant de Dirichlet), et l’un des pionniers de la théorie des formes modulaires. Dans le second exposé, on se propose de démontrer un cas particulier d’un de ses résultats concernant *l’équirépartition des angles des premiers de Gauss*.

Dans ces deux démonstrations, l’analyse de Fourier soit *discrète* sur les groupes abéliens finis $(\mathbb{Z}/n\mathbb{Z})^\times$, soit sur le cercle unité S^1 , joue un rôle important. Un autre ingrédient est la notion de *fonction L* : ce sont des séries de Dirichlet dont les propriétés analytiques gouvernent en fait les énoncés en question. La formule de Poisson, issue de l’analyse harmonique réelle, s’applique de manière assez magique à ces dernières, et explique une de leurs symétries les plus profondes : nous verrons en Annexes B et C des instances de ce phénomène. Les prérequis pour ce texte sont les cours d’algèbre [ALG] et d’analyse complexe [AC] de première année, et les cours d’analyse de la semaine d’analyse harmonique. L’énoncés de [AC] sur les séries de Dirichlet qui seront nécessaires sont aussi rappelés en Annexe A.

Je remercie mes étudiants Yoël Dadoun, Léo Gratien, Jules Mas et Xuan-Kien Phung, pour des discussions passées qui ont bien profité à l’écriture de ce texte.

TABLE DES MATIÈRES

| | |
|---|----|
| 1. Le théorème de la progression arithmétique | 2 |
| 2. Démonstration du théorème : réductions eulériennes | 4 |
| 3. Fin de la démonstration : preuve de $L(1, \chi) \neq 0$. | 7 |
| 4. Angles des premiers de Gauss | 8 |
| 5. Réduction à une assertion de convergence | 9 |
| 6. Fonctions L de Hecke de $\mathbb{Z}[i]$ | 10 |
| 7. Prolongement analytique des $L_m(s)$ à $\operatorname{Re} s > 1/2$ | 13 |
| Annexe A. Rappels sur les séries de Dirichlet | 14 |
| Annexe B. Équation fonctionnelle de ζ , suivant Riemann | 16 |
| Annexe C. Équations fonctionnelles des L_m , suivant Hecke | 17 |
| Références | 19 |

1. LE THÉORÈME DE LA PROGRESSION ARITHMÉTIQUE

On sait depuis Euclide qu'il existe une infinité de nombres premiers. En fait, toute progression arithmétique ayant deux termes consécutifs premiers entre eux contient une infinité de nombres premiers :

Théorème 1.1. (Dirichlet, 1837) *Si a et b sont des entiers premiers entre eux, alors il existe une infinité de nombres premiers p vérifiant $p \equiv a \pmod{b}$.*

Cet énoncé avait été au moins conjecturé par Legendre dans ses recherches de démonstration de la loi de réciprocité quadratique. Il est clair à la lecture des *Disquisitiones Arithmeticae* que Gauss aurait rêvé d'en avoir une démonstration, tant ces dernières regorgent d'ingéniosité pour en contourner l'utilisation. C'est pourquoi Gauss considérait cet énoncé comme l'un des plus difficiles et importants de l'époque. Il en existe des démonstrations élémentaires à la *Euclide* dans quelques cas particuliers de a et b , par exemple pour $b = 4$:

Proposition 1.2. (Euler) *Le Théorème 1.1 est vrai dans le cas particulier $b = 4$.*

DÉMONSTRATION — Supposons d'abord $a \equiv -1 \pmod{4}$. Pour $n \geq 2$ on pose $f(n) = n! - 1$. Les facteurs premiers de $f(n)$ sont $> n$, donc impairs (congrus à $\pm 1 \pmod{4}$), et on a $f(n) \equiv -1 \pmod{4}$: donc $f(n)$ a un facteur premier $\equiv -1 \pmod{4}$ et $> n$.

Considérons enfin $a \equiv 1 \pmod{4}$. Pour $n \geq 2$ on regarde $f(n) = (n!)^2 + 1$. Tout facteur premier p de $f(n)$ est $> n$, impair, et -1 est un carré modulo p , donc on a $p \equiv 1 \pmod{4}$ d'après un résultat classique d'Euler. \square

Remarque 1.3. *En élaborant ce type d'arguments, Euler a démontré le Théorème 1.1 sous l'hypothèse¹ $a \equiv 1 \pmod{b}$. Des démonstrations élémentaires dans cet esprit existent aussi sous l'hypothèse $a^2 \equiv 1 \pmod{b}$ (Schur), mais pas en général (voir [MT06]). Le cas $(a, b) = (2, 5)$ échappe par exemple à ces méthodes.*

Le résultat démontré par Dirichlet est en fait plus précis que le Théorème 1.1, en ce sens qu'il quantifie l'infinité en question. Le point de départ de Dirichlet est le résultat suivant, dû à Euler, que l'on peut voir comme une forme quantitative de l'infinité des nombres premiers. On notera \mathcal{P} l'ensemble des nombres premiers.

Proposition 1.4. (Euler) *Pour s réel tendant vers 1^+ on a*

$$\sum_{p \in \mathcal{P}} \frac{1}{p^s} = -\log(s-1) + O(1).$$

En particulier, la somme des $1/p$ avec p premier, qui majore le terme de gauche, diverge (Euler). En fait, la divergence de la suite $\sum_{p \leq n} 1/p$ est très lente (en $\log \log n$), de sorte qu'avec un ordinateur on a plutôt l'impression que la série converge !

On supposera le lecteur familier avec les propriétés élémentaires des séries de Dirichlet démontrées dans le cours d'analyse complexe [AC] (rappelées dans l'annexe A), et notamment de la fonction ζ de Riemann. Pour $s \in \mathbb{C}$ avec $\operatorname{Re} s > 1$, c'est la série absolument convergente $\zeta(s) = \sum_{n \geq 1} \frac{1}{n^s}$. Elle se prolonge méromorphiquement à

1. Voir par exemple les exercices du chapitre 2 du cours d'algèbre [ALG].

Re $s > 0$ avec pour unique pôle $s = 1$, simple de résidu 1. Pour Re $s > 1$, on a d'après Euler un développement en produit infini absolument convergent

$$(1) \quad \zeta(s) = \prod_{p \in \mathcal{P}} \frac{1}{1 - p^{-s}},$$

incarnation analytique du théorème fondamental de l'arithmétique.

DÉMONSTRATION — (de la Proposition 1.4) Pour s réel > 1 , on a par (1)

$$\log \zeta(s) = \sum_{p \in \mathcal{P}} -\log(1 - p^{-s}) = \sum_{p, k} \frac{1}{k p^{ks}},$$

une série à termes positifs indexée par les $p \in \mathcal{P}$ et les entiers $k \geq 1$. Séparons les termes avec $k = 1$ et $k \geq 2$ en écrivant $\log \zeta(s) = \sum_{p \in \mathcal{P}} \frac{1}{p^s} + g(s)$. Pour $k \geq 2$ et $p \in \mathcal{P}$ on a trivialement $k p^{-ks} \geq 2 p^{-ks}$ et $1 - p^{-s} \geq 1 - p^{-1} \geq 1/2$, puis

$$0 \leq g(s) \leq \frac{1}{2} \sum_{p \in \mathcal{P}} \frac{p^{-2s}}{1 - p^{-s}} \leq \sum_{p \in \mathcal{P}} p^{-2s} \leq \zeta(2s).$$

La proposition se déduit de $(s - 1)\zeta(s) \rightarrow 1$ et $\zeta(2s) \rightarrow \zeta(2)$ (fini) pour $s \rightarrow 1^+$. \square

Définition 1.5. Soient A une partie de \mathcal{P} et $\delta \in \mathbb{R}$. On dit que A est de densité de Dirichlet δ si on a $\frac{\sum_{p \in A} p^{-s}}{-\log(s-1)} \rightarrow \delta$ quand $s \rightarrow 1^+$.

La proposition d'Euler ci-dessus montre que \mathcal{P} est densité de Dirichlet 1, et qu'en général on a $0 \leq \delta \leq 1$. Il est évident que toute partie finie A est de densité de Dirichlet 0, mais la réciproque est fautive : considérer $A = \{p_1, p_2, \dots\}$ avec $p_i \geq 2^i$ pour tout $i \geq 1$. Une autre notion de densité consisterait à demander que $\frac{|A \cap \{1, \dots, n\}|}{|\mathcal{P} \cap \{1, \dots, n\}|}$ admette une limite pour $n \rightarrow +\infty$. Bien que plus naturelle, cette propriété est plus difficile à établir que celle de Dirichlet (voir [SER70] Ch. IV §4.5), et nous ne l'utiliserons pas dans ce texte. Notre premier but sera de démontrer l'énoncé suivant, entraînant trivialement le Théorème 1.1 en le précisant quantitativement :

Théorème 1.6. (Dirichlet) Soient a, b des entiers premiers entre eux avec $b \geq 1$. L'ensemble des nombres premiers p tels que $p \equiv a \pmod{b}$ est de densité de Dirichlet $\frac{1}{\varphi(b)}$, où φ désigne l'indicatrice d'Euler.

En un sens, cela dit que les classes des nombres premiers ne divisant pas b sont également réparties dans $(\mathbb{Z}/b\mathbb{Z})^\times$ (de cardinal $\varphi(b)$), un phénomène clair empiriquement comme le montre la table suivante pour $b = 4$:

| n | 10 | 100 | 1,000 | 10,000 | 100,000 | 1,000,000 | 10,000,000 | 100,000,000 |
|----------|----|-----|-------|--------|---------|-----------|------------|-------------|
| $N_1(n)$ | 4 | 47 | 495 | 4984 | 49950 | 499798 | 4999452 | 49998748 |
| $N_3(n)$ | 6 | 53 | 505 | 5016 | 50050 | 500202 | 5000548 | 50001252 |

TABLE 1. Parmi les n premiers nombres premiers impairs, $N_i(n)$ sont $\equiv i \pmod{4}$.

Remarque 1.7. (Biais de Tchebychev) *Pour tous les entiers n ci-dessus, on constate suivant Tchebychev que l'on a $N_3(n) > N_1(n)$. C'est empiriquement le cas pour presque tous les entiers n : le premier n avec $N_1(n) > N_3(n)$, découvert par Leech en 1957, est $n = 2946$. Cette observation est encore largement inexplicée : voir [GM04]. cela découlerait de l'hypothèse de Riemann généralisée et de la conjecture « LI ».*

2. DÉMONSTRATION DU THÉORÈME : RÉDUCTIONS EULÉRIENNES

Fixons définitivement un entier $b \geq 1$. On veut montrer

$$(2) \quad \frac{1}{-\log(s-1)} \sum_{p \equiv a \pmod{b}} \frac{1}{p^s} \xrightarrow{s \rightarrow 1^+} \frac{1}{\varphi(b)}, \quad \forall a \in (\mathbb{Z}/b\mathbb{Z})^\times.$$

Il est équivalent de démontrer que l'on a

$$(3) \quad \frac{1}{-\log(s-1)} \sum_{p \in \mathcal{P}, p \nmid b} \frac{f(p)}{p^s} \xrightarrow{s \rightarrow 1^+} \frac{1}{\varphi(b)} \sum_{x \in (\mathbb{Z}/b\mathbb{Z})^\times} f(x), \quad \forall f \in \mathcal{F}((\mathbb{Z}/b\mathbb{Z})^\times).$$

où $\mathcal{F}((\mathbb{Z}/b\mathbb{Z})^\times)$ désigne le \mathbb{C} -espace vectoriel des fonctions $(\mathbb{Z}/b\mathbb{Z})^\times \rightarrow \mathbb{C}$. En effet, la Formule (2) est le cas particulier de (3) où f est la fonction caractéristique $\mathbb{1}_a$ d'un point $a \in (\mathbb{Z}/b\mathbb{Z})^\times$, et (3) se déduit alors de (2) par linéarité. Munissant $\mathcal{F}((\mathbb{Z}/b\mathbb{Z})^\times)$ du produit scalaire hermitien $\langle f, f' \rangle = \frac{1}{\varphi(b)} \sum_{x \in (\mathbb{Z}/b\mathbb{Z})^\times} \overline{f(x)} f'(x)$, notons aussi que le terme $\frac{1}{\varphi(b)} \sum_{x \in (\mathbb{Z}/b\mathbb{Z})^\times} f(x)$, *i.e.* la valeur moyenne de f , n'est autre que $\langle 1, f \rangle$.

Fait 2.1. *La Formule (3) est vraie pour $f = 1$.*

DÉMONSTRATION — C'est la somme des identités (2). On conclut par la Proposition 1.4. En effet, la somme finie des p^{-s} avec p divisant b a une limite quand $s \rightarrow 1$, et donc disparaît quand on divise par $-\log(s-1)$. \square

Il reste à comprendre pourquoi (3) est vraie pour tout f . En cherchant à imiter la Proposition 1.4, Dirichlet est amené à considérer pour $f \in \mathcal{F}((\mathbb{Z}/b\mathbb{Z})^\times)$, la série

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

On utilise l'abus de notation $f(n) := f(n \bmod b)$ si $n \in \mathbb{Z}$ est premier à b , et la convention $f(n) = 0$ si n n'est pas premier à b . Comme f est bornée, cette série de Dirichlet converge absolument pour $\operatorname{Re} s > 1$, et définit donc, comme $\zeta(s)$, une fonction holomorphe de s sur cet ouvert de \mathbb{C} (Lemme A.1). En cherchant à quelle condition $L(s, f)$ admet un produit eulérien, Dirichlet est conduit à s'intéresser aux fonctions f *multiplicatives*, *i.e.* vérifiant $f(mn) = f(m)f(n)$ et $f(1) = 1$, ce qui revient à dire que $f : (\mathbb{Z}/b\mathbb{Z})^\times \rightarrow \mathbb{C}^\times$ est un *caractère* du groupe $(\mathbb{Z}/b\mathbb{Z})^\times$.

Définition 2.2. *Un caractère de Dirichlet modulo b est un caractère du groupe $(\mathbb{Z}/b\mathbb{Z})^\times$, *i.e.* un morphisme de groupes $(\mathbb{Z}/b\mathbb{Z})^\times \rightarrow \mathbb{C}^\times$.*

On notera souvent χ un tel caractère. Nous en avons vu des exemples dans le cours d'algèbre, comme le caractère de Legendre $x \mapsto \left(\frac{x}{b}\right)$, important dans la théorie des carrés modulo b , pour b premier > 2 . Même pour b premier, il faut en général introduire un générateur abstrait de $(\mathbb{Z}/b\mathbb{Z})^\times$ (Gauss) pour tous les décrire.

Exemple 2.3. Le groupe $(\mathbb{Z}/4\mathbb{Z})^\times = \{\pm 1\}$ a deux éléments. Il a exactement deux caractères : le caractère trivial 1 et le caractère χ_4 défini par $\chi_4(n) = 1$ pour $n \equiv 1 \pmod{4}$, et $\chi_4(n) = -1$ pour $n \equiv 3 \pmod{4}$.

Les deux observations importantes de Dirichlet sont alors les suivantes :

Proposition 2.4. (i) Si χ est caractère de $(\mathbb{Z}/b\mathbb{Z})^\times$, alors pour $\operatorname{Re} s > 1$ on a un produit absolument convergent $L(s, \chi) = \prod_{p \in \mathcal{P}} \frac{1}{1 - \chi(p)p^{-s}}$.
(ii) Les caractères de $(\mathbb{Z}/b\mathbb{Z})^\times$ forment une base orthonormée de $\mathcal{F}((\mathbb{Z}/b\mathbb{Z})^\times)$.

DÉMONSTRATION — Si χ est un caractère modulo b , et pour $x \in (\mathbb{Z}/b\mathbb{Z})^\times$, alors $\chi(x) \in \mathbb{C}^\times$ est de module 1 : c'est même une racine de l'unité d'ordre divisant $\varphi(b)$, car on a $x^{\varphi(b)} = 1$. Le (i) se montre alors exactement comme le développement en produit eulérien de $\zeta(s)$ (voir [AC] ou l'Exemple A.6). Le (ii) est un cas particulier d'un énoncé plus généralement valable pour tout groupe abélien fini, déjà vu en cours d'algèbre [ALG, Chap. 3 §2]. \square

L'assertion (ii) est précurseur à la fois de l'analyse de Fourier discrète et de la théorie des représentations des groupes finis. Ainsi, Dirichlet explicite par exemple, pour tout $a \in (\mathbb{Z}/b\mathbb{Z})^\times$, la décomposition à la Fourier

$$\mathbb{1}_a = \frac{1}{\varphi(b)} \sum_{\chi} \overline{\chi(a)} \chi,$$

la somme portant sur les $\varphi(b)$ caractères χ modulo b . La formule exacte a peu d'importance : le point est que par linéarité de (3), il suffit de vérifier (3) pour les caractères $f = \chi$, et même pour χ non trivial par le Fait 2.1.

Proposition 2.5. Soit χ un caractère non trivial de $(\mathbb{Z}/b\mathbb{Z})^\times$. On a l'annulation $\sum_{x \in (\mathbb{Z}/b\mathbb{Z})^\times} \chi(x) = 0$. De plus, $L(s, \chi)$ converge uniformément sur tout compact de $\operatorname{Re} s > 0$, et définit donc une fonction holomorphe de s dans cette région.

DÉMONSTRATION — La première identité est la relation d'orthogonalité $\langle 1, \chi \rangle = 0$, qui vaut par la Proposition 2.4. On aussi peut la justifier directement comme suit. Pour $S = \sum_{x \in (\mathbb{Z}/b\mathbb{Z})^\times} \chi(x)$ et $t \in (\mathbb{Z}/b\mathbb{Z})^\times$, on constate $\chi(t)S = S$ par changement de variable $x \mapsto tx$ dans le groupe $(\mathbb{Z}/b\mathbb{Z})^\times$, et donc $S = 0$ si $\chi(t) \neq 1$. Cette annulation montre que la suite des sommes partielles $S_n = \sum_{k=1}^n \chi(k)$ ne prend qu'un nombre fini de valeurs ; elle est donc bornée. Une simple transformation d'Abel montre $\sum_{n=1}^N \chi(n)n^{-s} = S_N N^{-s} + \sum_{n=1}^{N-1} S_n (n^{-s} - (n+1)^{-s})$, et on conclut par l'inégalité $|n^{-s} - (n+1)^{-s}| \leq |s|n^{-\operatorname{Re} s - 1}$ (voir le Lemme A.1 pour des détails). \square

Dirichlet porte alors naturellement son attention sur la quantité

$$L(1, \chi) = \sum_{n \geq 1} \frac{\chi(n)}{n},$$

une série convergente pour $\chi \neq 1$, mais non absolument convergente. Le dernier ingrédient de sa démonstration est alors le suivant :

Théorème 2.6. Pour tout caractère χ de $(\mathbb{Z}/b\mathbb{Z})^\times$ avec $\chi \neq 1$, on a $L(1, \chi) \neq 0$.

Par exemple, la non-annulation de $L(1, \chi_4)$ est élémentaire :

$$L(1, \chi_4) = \sum_{n=0}^{\infty} \left(\frac{1}{4n+1} - \frac{1}{4n+3} \right) = \sum_{n=0}^{\infty} \frac{2}{(4n+1)(4n+3)} > 0$$

(cette somme vaut même $\arctan 1 = \frac{\pi}{4}$). Nous reportons à la section suivante la démonstration de ce théorème clé, et montrons d'abord comment il permet de conclure.

Proposition 2.7. *Le Théorème 2.6 entraîne le Théorème 1.6.*

DÉMONSTRATION — Nous allons en fait montrer que pour un caractère χ modulo b non trivial, la série $\sum_{p \in \mathcal{P}} \frac{\chi(p)}{p^s}$ admet une limite quand $s \rightarrow 1^+$. D'après l'annulation $\sum_x \chi(x) = 0$ (Proposition 2.5), cela entraîne (3) pour $f = \chi$, ce qu'il restait à démontrer par le Fait 2.1 et la Proposition 2.4 (ii).

Fixons s réel > 1 et supposons d'abord que χ ne prend que des valeurs réelles. Comme $\chi(x)$ est une racine de l'unité pour tout $x \in (\mathbb{Z}/b\mathbb{Z})^\times$, cela signifie $\chi(x) = \pm 1$ pour tout x (c'est le cas de χ_4 par exemple). Dans ce cas on a $1 - \chi(p)p^{-s} > 0$ pour tout p et donc $L(s, \chi) \geq 0$. Comme dans la preuve d'Euler, en prenant le logarithme du développement eulérien de $L(s, \chi)$ on a :

$$(4) \quad \log L(s, \chi) = \sum_{p \in \mathcal{P}} -\log(1 - \chi(p)p^{-s}) = \sum_{p,k} \frac{\chi(p)^k}{kp^{ks}},$$

puis $\log L(s, \chi) = \sum_{p \in \mathcal{P}} \frac{\chi(p)}{p^s} + g(s, \chi)$ avec $g(s, \chi) := \sum_{p,k \geq 2} \frac{\chi(p)^k}{kp^{ks}}$. Cette dernière série converge absolument comme pour $\zeta(s)$, pour $\operatorname{Re} s > 1/2$: on la majore trivialement par $g(s, 1)$ puis $\zeta(2s)$ comme dans la démonstration de la Proposition 1.4. En faisant tendre s vers 1^+ , on a $L(1, \chi) \geq 0$ par continuité, et donc $L(1, \chi) > 0$ par hypothèse, et on conclut $\sum_{p \in \mathcal{P}} \frac{\chi(p)}{p^s} \rightarrow \log L(1, \chi) - g(1, \chi)$.

Pour un χ général, l'idée est la même mais il faut prendre garde que $L(s, \chi)$ n'est pas un nombre réel. Il faut donc faire attention au sens que l'on donne à son logarithme et justifier une assertion du style de l'équation (4). C'est un détail que l'on peut régler comme suit. Notons $\log : \mathbb{C} \setminus \mathbb{R}_{\leq 0} \rightarrow \mathbb{C}$ le logarithme principal, vérifiant comme on le sait $-\log(1 - z) = \sum_{n \geq 1} \frac{z^n}{n}$ pour $|z| < 1$. Considérons la série

$$\mathcal{L}(s, \chi) := \sum_{p \in \mathcal{P}} -\log(1 - \chi(p)p^{-s}) = \sum_{p,k} \frac{\chi(p)^k}{kp^{ks}}.$$

Elle est clairement absolument convergente, donc holomorphe, sur l'ouvert $\Omega = \{s \in \mathbb{C}, \operatorname{Re} s > 1\}$, et satisfait $e^{\mathcal{L}(s, \chi)} = L(s, \chi)$ sur Ω . D'autre part, par l'hypothèse $L(1, \chi) \neq 0$, il existe un disque ouvert D de centre 1 sur lequel la fonction holomorphe $L(s, \chi)$ ne s'annule pas, et donc² admet un logarithme complexe dans D , *i.e.* une fonction holomorphe $f(s)$ sur D vérifiant $e^{f(s)} = L(s, \chi)$. Sur l'ouvert connexe $D \cap \Omega$, les deux logarithmes $f(s)$ et $\mathcal{L}(s, \chi)$ de $L(s, \chi)$ diffèrent d'une constante dans $2i\pi\mathbb{Z}$. Quitte à soustraire cette constante à f , on peut supposer $f(s) = \mathcal{L}(s, \chi)$ sur $D \cap \Omega$, et en particulier $\mathcal{L}(s, \chi) \xrightarrow{s \rightarrow 1} f(1)$. Le reste de la démonstration est inchangé. \square

2. Considérer simplement pour f une primitive de $L'(s, \chi)/L(s, \chi)$ sur D .

3. FIN DE LA DÉMONSTRATION : PREUVE DE $L(1, \chi) \neq 0$.

Dans sa démonstration du Théorème 2.6, Dirichlet se ramène d'abord au cas $\chi^2 = 1$, pour lequel il donne une formule *exacte* pour $L(1, \chi)$, sa célèbre *formule du nombre de classes*, rendant sa non nullité évidente. La démonstration qui suit, plus simple, est différente et ne distingue pas ces deux cas. Nous renvoyons à [IR90, Ch. 16], [DAV80, Chap. 1] ou [SER70, Chap. 4] pour des expositions dans le même esprit.

Fixons χ un caractère de $(\mathbb{Z}/b\mathbb{Z})^\times$ avec $b \geq 1$. Notons d le plus petit entier ≥ 1 tel que $\chi^d = 1$, c'est-à-dire l'ordre de χ dans le groupe des caractères de $(\mathbb{Z}/b\mathbb{Z})^\times$. On considère le produit

$$F(s) = L(s, 1)L(s, \chi)L(s, \chi^2) \cdots L(s, \chi^{d-1}).$$

Chaque $L(s, \chi^i)$ avec $1 \leq i < d$ est holomorphe sur $\operatorname{Re} s > 0$. Pour $i = 0$, on a

$$L(s, 1) = \sum_{(n,b)=1} \frac{1}{n^s} = \prod_{p \nmid b} \frac{1}{1 - p^{-s}} = \zeta(s) \prod_{p|b} (1 - p^{-s}),$$

qui est méromorphe sur $\operatorname{Re} s > 0$ avec pour unique pôle $s = 1$, qui est simple (de résidu $\prod_{p|b} (1 - p^{-1})$). Supposant $d > 1$ et $L(1, \chi) = 0$, ce zéro de $L(s, \chi)$ compense le pôle simple de $L(s, 1)$ en $s = 1$, de sorte que $F(s)$ est holomorphe sur $\operatorname{Re} s > 0$. Nous allons aboutir à une contradiction en donnant une seconde expression de $F(s)$.

Lemme 3.1. *Pour $\operatorname{Re} s > 1$ on a $F(s) = \prod_{p \nmid b} \frac{1}{(1 - \chi(p)p^{-s})^{d/f_p}}$, où f_p est l'ordre de la racine de l'unité $\chi(p)$.*

DÉMONSTRATION — Par l'hypothèse $\chi^d = 1$, on a $\chi(p)^d = 1$ pour $p \nmid b$, et $\chi(p) = 0$ pour $p|b$. Pour $\xi \in \mathbb{C}^\times$ avec $\xi^d = 1$, et disons ξ d'ordre f , on a la formule évidente $\prod_{i=0}^{d-1} (1 - \xi^i T) = (1 - T^f)^{d/f}$. On conclut par le produit eulérien des $L(s, \chi^i)$ (dans un produit absolument convergent, l'ordre des termes du produit n'importe pas.) \square

Ainsi, pour $\operatorname{Re} s > 1$ la fonction $F(s)$ est une série de Dirichlet à coefficients ≥ 0 . Comme on a vu qu'elle se prolonge holomorphiquement à $\operatorname{Re} s > 0$, lemme de Landau (voir [AC] ou le Cor. A.4) assure que *cette série de Dirichlet converge pour tout réel $s > 0$* . Mais chaque série de Dirichlet $\frac{1}{(1 - \chi(p)p^{-s})^{d/f_p}}$ ayant un coefficient d'indice p^d qui est ≥ 1 , on en déduit

$$F(1/d) \geq \sum_{p \nmid b} \frac{1}{p} = +\infty,$$

en contradiction avec $F(1/d) < +\infty$. \square

4. ANGLES DES PREMIERS DE GAUSS

Soit p un nombre premier $\equiv 1 \pmod{4}$. On sait depuis Fermat et Gauss qu'il existe deux uniques entiers $a > b$ positifs tels que $p = a^2 + b^2$. Le nombre complexe $a + bi$ s'écrit alors de manière unique sous la forme

$$a + bi = \sqrt{p} e^{i\theta_p} \text{ avec } \theta_p \in]0, \frac{\pi}{4}[.$$

| p | 5 | 13 | 17 | 29 | 37 | 41 | 53 | 61 | 73 | 89 | 97 | 101 | 109 | 113 | 137 |
|-------------------------|------|------|------|------|------|------|------|------|------|------|------|------|------|------|------|
| $\frac{4}{\pi}\theta_p$ | 0.59 | 0.75 | 0.31 | 0.48 | 0.21 | 0.86 | 0.35 | 0.88 | 0.46 | 0.71 | 0.53 | 0.13 | 0.37 | 0.92 | 0.44 |

TABLE 2. Premières valeurs de $\frac{4}{\pi}\theta_p$, à 10^{-2} près.

On s'intéresse, suivant Hecke, à la répartition des angles θ_p dans le segment $[0, \frac{\pi}{4}]$ quand le nombre premier $p \equiv 1 \pmod{4}$ varie. Hecke a démontré dans [HEC20] le résultat remarquable suivant :

Théorème 4.1. (Hecke, 1920)

- (i) La suite des θ_p est dense dans $[0, \frac{\pi}{4}]$.
- (ii) Mieux, elle y est équirépartie : si p_n désigne le n -ème nombre premier $\equiv 1 \pmod{4}$, et si $I \subset [0, \frac{\pi}{4}]$ est un intervalle de longueur ℓ , on a

$$\frac{1}{N} |\{n \leq N \mid \theta_{p_n} \in I\}| \xrightarrow{N \rightarrow +\infty} \frac{4}{\pi} \ell.$$

On se propose dans ce qui suit de démontrer la première assertion, ainsi qu'une variante de la seconde. La figure ci-dessous illustre bien ces résultats :

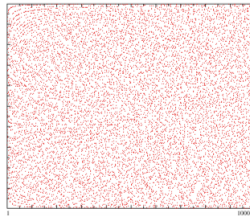


FIGURE 2. Ensemble des couples (n, θ_{p_n}) pour $n \leq 10^4$.

Les questions ci-dessus sont particulièrement intéressantes du point de vue de l'arithmétique de l'anneau $\mathbb{Z}[i]$ des *entiers de Gauss*. Nous avons vu en cours d'algèbre [ALG, Chap. 7] que $\mathbb{Z}[i]$ est un anneau euclidien pour la *norme* $N(z) = |z|^2$, et en particulier factoriel. Le lien avec les sommes de deux carrés est bien entendu la formule $N(a + bi) = a^2 + b^2$. On rappelle que le groupe des inversibles de $\mathbb{Z}[i]$, constitué des éléments de norme 1, est

$$\mathbb{Z}[i]^\times = \{1, i, -1, -i\} \simeq \mathbb{Z}/4\mathbb{Z}$$

Rappelons que les irréductibles de $\mathbb{Z}[i]$, aussi appelés *premiers de Gauss*, sont de trois types. Dans chacun des cas, on ne donnera qu'un élément parmi ses 4 associés.³ Il y a d'abord l'irréductible $1 + i$, de norme 2. Ensuite, il y a les nombres premiers

3. On rappelle que deux éléments z et z' de $\mathbb{Z}[i]$ sont dits *associés*, ce que l'on note $z \sim z'$, si l'on a $z' = uz$ avec $u \in \mathbb{Z}[i]^\times$, c'est-à-dire $z' = \pm z$ ou $z' = \pm iz$.

$p \equiv 3 \pmod{4}$ usuels, de norme p^2 , qui restent irréductibles dans $\mathbb{Z}[i]$. Enfin, pour tout nombre premier $p \equiv 1 \pmod{4}$, disons écrit $p = a^2 + b^2$ avec $a > b > 0$, on a

$$(5) \quad p = \pi \bar{\pi} \quad \text{avec } \pi = a + bi,$$

et π et $\bar{\pi}$ sont deux irréductibles non associés.⁴ Ainsi, la question de comprendre les θ_p est équivalente à celle de comprendre les arguments – ou *angles* – des premiers de Gauss. Bien sûr, seuls ceux du troisième type sont mystérieux, ce qu'illustre bien la Figure 1! (Voir aussi [GWW98] pour d'autres illustrations intéressantes sur les premiers de Gauss).

Remarque 4.2. *On conjecture que pour essentiellement toute droite $D \subset \mathbb{C}$ passant par au moins deux points de $\mathbb{Z}[i]$, alors D contient une infinité de premiers de Gauss. Si D a pour équation $ax - by = c$, avec $a, b, c \in \mathbb{Z}$ et a, b premiers entre eux, la condition exacte sur (a, b, c) devrait être que $a^2 + b^2$ soit premier avec c . Cependant, on ne sait le démontrer pour aucune droite, exceptées bien sûr $x = 0$ et $y = 0$. Par exemple, on ne sait pas s'il existe une infinité de nombres premiers de la forme $n^2 + 1$ (cas $y = 1$), ou de la forme $2n^2 - 2n + 1$ (cas $y = x - 1$).*

5. RÉDUCTION À UNE ASSERTION DE CONVERGENCE

La démonstration par Hecke du Théorème 4.1 peut être vue comme un développement de celle par Dirichlet du théorème de la progression arithmétique. Pour $m \in \mathbb{Z}$, et disons s réel > 1 , considérons la série de Dirichlet

$$D_m(s) = \sum_{p \equiv 1 \pmod{4}} \frac{\cos(m \theta_p)}{p^s}.$$

C'est une série absolument convergente, majorée par $\zeta(s)$. Le théorème clé à démontrer est le suivant :

Théorème 5.1. (Hecke) *Pour $m \equiv 0 \pmod{4}$, la fonction $D_m(s)$ admet une limite quand $s \rightarrow 1^+$, sauf pour $m = 0$, auquel cas on a $D_0(s) \sim -\frac{1}{2} \log(s - 1)$.*

L'assertion sur D_0 est bien sûr un cas particulier du théorème de Dirichlet, et exprime le fait que « la moitié des nombres premiers sont $\equiv 1 \pmod{4}$ ». On a aussi $D_m = D_{-m}$. La démonstration du théorème ci-dessus pour $m > 0$ constituera l'essentiel du travail. Admettons-le pour l'instant et concluons.

Corollaire 5.2. *Soit f une fonction continue $[0, \frac{\pi}{4}] \rightarrow \mathbb{R}$. On a*

$$-\frac{2}{\log(s-1)} \sum_{p \equiv 1 \pmod{4}} \frac{f(\theta_p)}{p^s} \xrightarrow{s \rightarrow 1^+} \frac{4}{\pi} \int_0^{\frac{\pi}{4}} f(x) dx.$$

DÉMONSTRATION — Notons $D(s, f)$ le terme de gauche et $I(f) = \frac{4}{\pi} \int_0^{\frac{\pi}{4}} f(x) dx$ celui de droite. Pour $f(x) = \cos(mx)$ on a $I(f) = 0$ pour $m \neq 0$, et $I(f) = 1$ pour $m = 0$. Le résultat découle donc du Théorème 5.1 pour un tel f . Par linéarité, il vaut donc aussi pour toute fonction du sous-espace

$$\mathcal{A} := \sum_{m \in 4\mathbb{Z}} \mathbb{R} \cos(mx)$$

4. Les 8 irréductibles de $\mathbb{Z}[i]$ divisant p dans (5) sont donc $\pm\pi, \pm i\pi, \pm\bar{\pi}, \pm i\bar{\pi}$. Leurs arguments sont les $\pm\theta_p \pmod{\frac{\pi}{2}\mathbb{Z}}$. Ils correspondent aux 8 couples $(u, v) \in \mathbb{Z}^2$ avec $p = u^2 + v^2$, à savoir $(\pm a, \pm b)$ et $(\pm b, \pm a)$.

de la \mathbb{R} -algèbre \mathcal{C} des fonctions continues $[0, \frac{\pi}{4}] \rightarrow \mathbb{R}$. Mais ce sous-espace en est manifestement une sous-algèbre qui sépare les points (considérer $\cos 4x$) ; il est donc dense dans \mathcal{C} pour la norme sup. sur $[0, \frac{\pi}{4}]$, par Stone-Weierstrass. (Noter ici le raisonnement manifestement à la Fourier !)

Soit f une fonction continue arbitraire sur $[0, \frac{\pi}{4}]$. Fixons $\epsilon > 0$. On peut donc trouver $P \in \mathcal{A}$ tel que $|P - f|_\infty < \epsilon$. Pour s réel > 1 on a

$$D(s, f) - I(f) = D(s, f - P) + (D(s, P) - I(P)) - I(f - P)$$

Mais on a $|I(f - P)| \leq \epsilon$, $|D(s, f - P)| \leq \epsilon D(s, 1)$ et $D(s, P) - I(P)$ tend vers 0 quand s tend vers 1. Comme $D(s, 1)$ tend vers 1 (cas $f = 1$), on en déduit

$$\limsup_{s \rightarrow 1^+} |D(s, f) - I(f)| \leq 2\epsilon.$$

Comme cela vaut pour tout $\epsilon > 0$, la limite supérieure ci-dessus est donc 0. \square

Nous pouvons maintenant démontrer la densité des θ_p .

DÉMONSTRATION — (du Théorème 4.1 (i)) Soient S un intervalle dans $[0, \frac{\pi}{4}]$ et f une fonction continue ≥ 0 , non nulle, et à support dans cet intervalle. On a donc $I(f) > 0$. D'après le corollaire, cela entraîne $f(\theta_p) \neq 0$ (et donc $\theta_p \in S$) pour une infinité de $p \equiv 1 \pmod{4}$, sinon le terme de gauche (alors une somme finie) tendrait vers 0. \square

Le Corollaire 5.2 est la variante promise de l'équirépartition des θ_p .

Corollaire 5.3. *Pour tout $0 \leq a < b \leq \frac{\pi}{4}$, on a*

$$-\frac{2}{\log(s-1)} \sum_{p \equiv 1 \pmod{4} \text{ et } \theta_p \in [a, b]} \frac{1}{p^s} \xrightarrow{s \rightarrow 1^+} \frac{4}{\pi}(b-a)$$

DÉMONSTRATION — Fixons $\epsilon > 0$ assez petit. Choisissons deux fonctions $f, g \in \mathcal{C}$ avec $0 \leq f, g \leq 1$ (par exemple affines par morceaux) telles que : la fonction f vaut 1 sur $[a, b]$ et 0 hors de $[0, \frac{\pi}{4}] \cap [a - \epsilon, b + \epsilon]$, la fonction g vaut 0 hors de $[a, b]$ et 1 sur $[a + \epsilon, b - \epsilon]$. Notons $F(s)$ le terme de gauche de l'énoncé. On a $D(s, g) \leq F(s) \leq D(s, f)$. Le Corollaire 5.2 appliqué à f et g implique donc

$$\frac{4}{\pi}(b-a-2\epsilon) \leq I(g) \leq \liminf_{s \rightarrow 1^+} F(s) \leq \limsup_{s \rightarrow 1^+} F(s) \leq I(f) \leq \frac{4}{\pi}(b-a+2\epsilon),$$

ce qui conclut en faisant tendre maintenant ϵ vers 0. \square

6. FONCTIONS L DE HECKE DE $\mathbb{Z}[i]$

NOTATIONS : Pour $z \in \mathbb{C}^\times$, il sera commode de poser $e(z) = z/|z|$ (son "angle" vu comme nombre complexe de module 1), de sorte que l'on a la décomposition polaire $z = |z|e(z)$ et $e(zz') = e(z)e(z')$ pour tout $z, z' \in \mathbb{C}^\times$. Notons aussi \mathcal{N} l'ensemble des éléments *non nuls* de $\mathbb{Z}[i]$ modulo la relation d'association⁵, et $\mathcal{Q} \subset \mathcal{N}$ le sous-ensemble des éléments irréductibles.

5. Autrement dit, on a $\mathcal{N} = (\mathbb{Z}[i] \setminus \{0\}) / \mathbb{Z}[i]^\times$.

Fixons $m \in \mathbb{Z}$ avec $m \equiv 0 \pmod{4}$. Pour $z \in \mathcal{N}$ les éléments $N(z)$ et $e(z^m) = e(z)^m$ de \mathbb{C}^\times sont bien définis. Il y a donc un sens à poser

$$L_m(s) = \sum_{z \in \mathcal{N}} \frac{e(z)^m}{N(z)^s}$$

(fonctions L de Hecke). C'est une série de Dirichlet, que l'on peut aussi écrire

$$L_m(s) = \sum_{n \geq 1} \frac{h_m(n)}{n^s} \quad \text{avec} \quad h_m(n) = \sum_{z \in \mathcal{N} \mid N(z)=n} e(z)^m.$$

Les éléments de \mathcal{N} de norme ≤ 9 étant $1, 1+i, 2, 2 \pm i, 2(1+i)$ et 3 , on a

$$L_m(s) = 1 + \frac{(-1)^{m/4}}{2^s} + \frac{1}{4^s} + \frac{2 \cos(m \theta_5)}{5^s} + \frac{(-1)^{m/4}}{8^s} + \frac{1}{9^s} + \dots$$

avec $\theta_5 = \arctan \frac{1}{2}$. On a de plus clairement $|h_m(n)| \leq h_0(n)$ et

$$h_0(n) = \frac{1}{4} |\{(a, b) \in \mathbb{Z}^2 \mid a^2 + b^2 = n\}|.$$

L'estimation triviale $h_0(n) = O(\sqrt{n})$ pour $n \rightarrow +\infty$ montre que $L_m(s)$ converge absolument pour $\operatorname{Re} s > 1 + 1/2$. On peut faire mieux :

Lemme 6.1. *La série $L_m(s)$ est absolument convergente pour $\operatorname{Re} s > 1$, et définit une fonction holomorphe de s dans ce demi-plan. De plus, elle y admet un développement en produit infini (« développement eulérien ») absolument convergent*

$$L_m(s) = \prod_{\pi \in \mathcal{Q}} \frac{1}{1 - e(\pi)^m N(\pi)^{-s}}.$$

Étant donné la description de \mathcal{Q} rappelée en Section 4, le produit ci-dessus est aussi

$$(6) \quad \frac{1}{1 - (-1)^{\frac{m}{4}} 2^{-s}} \prod_{p \equiv 3 \pmod{4}} \frac{1}{1 - p^{-2s}} \prod_{p \equiv 1 \pmod{4}} \frac{1}{1 - e^{im\theta_p} p^{-s}} \frac{1}{1 - e^{-im\theta_p} p^{-s}}.$$

DÉMONSTRATION — Soit $\sigma := \operatorname{Re} s$. Pour $\pi \in \mathcal{Q}$ et $\sigma > 1$ on constate, en développant la série géométrique, $1 + \left| \frac{1}{1 - e(\pi)^m N(\pi)^{-s}} - 1 \right| \leq \frac{1}{1 - N(\pi)^{-\sigma}}$ pour $\pi \in \mathcal{Q}$. On a de plus

$$\prod_{\pi \in \mathcal{Q}} \frac{1}{1 - N(\pi)^{-\sigma}} = \frac{1}{1 - 2^{-\sigma}} \prod_{p \equiv 3 \pmod{4}} \frac{1}{1 - p^{-2\sigma}} \prod_{p \equiv 1 \pmod{4}} \frac{1}{(1 - p^{-\sigma})^2} \leq \zeta(\sigma) L(\sigma, \chi_4),$$

la dernière inégalité venant de $1 - p^{-2\sigma} = (1 - p^{-\sigma})(1 + p^{-\sigma})$. Cela montre la convergence absolue du produit infini pour $\sigma > 1$. L'identité de l'énoncé, et la convergence absolue de $L_m(s)$ pour $\sigma > 1$, s'en déduisent par factoriabilité de $\mathbb{Z}[i]$ et multiplicativité de N et e , comme pour $\zeta(s)$ (imiter la preuve du Lemme A.5). \square

Remarque 6.2. *La proposition ci-dessus montre que l'on a $h_m(ab) = h_m(a)h_m(b)$ pour a et b premiers entre eux, ainsi que $h_m(2^k) = (-1)^{mk/4}$, $h_m(p^k) = 1$ pour $p \equiv 3 \pmod{4}$, et $h_0(p^k) = k + 1$ pour $p \equiv 1 \pmod{4}$. C'est un exercice que d'en déduire que pour tout $\epsilon > 0$ et tout m , on a $h_m(n) = O(n^\epsilon)$ quand $n \rightarrow +\infty$.*

Une autre conséquence immédiate de la Formule (6), de la factorisation $1 - p^{-2s} = (1 - p^{-s})(1 + p^{-s})$ et des produits eulériens de $\zeta(s)$ et $L(s, \chi_4)$ est :

Corollaire 6.3. *On a $L_0(s) = \zeta(s)L(s, \chi_4)$. En particulier, $L_0(s)$ se prolonge méromorphiquement à $\operatorname{Re} s > 0$, avec $s = 1$ pour unique pôle, simple de résidu $L(1, \chi_4)$.*

Pour $m \neq 0$, et de manière un peu analogue au $L(s, \chi)$ pour $\chi \neq 1$, un phénomène de type « série alternée » fait que la série $L_m(s)$ converge à gauche de $\operatorname{Re} s > 1$:

Proposition 6.4. *Pour $m \neq 0$, la série $L_m(s)$ converge uniformément sur tout compact de $\operatorname{Re} s > 1/2$; c'est donc une fonction holomorphe de s sur ce demi-plan.*

Nous reportons au paragraphe suivant la démonstration de cette proposition. En fait, en imitant une des deux démonstrations de Riemann du prolongement analytique de $\zeta(s)$, Hecke démontre même que $L_m(s)$ se prolonge analytiquement à \mathbb{C} tout entier, et vérifie une équation fonctionnelle reliant s et $1 - s$: nous renvoyons aux annexes B et C pour ces bonus importants mais qui ne serviront pas ici.

DÉMONSTRATION — (La Proposition 6.4 implique le Théorème 5.1.) On suppose $\operatorname{Re} s > 1$ et on regarde :

$$\mathcal{L}_m(s) := \sum_{\pi \in \mathcal{Q}} -\log(1 - e(\pi)^m N(\pi)^{-s}) = \sum_{\pi \in \mathcal{Q}, k \geq 1} \frac{e(\pi)^{mk}}{k N(\pi)^{ks}}.$$

Pour $p \equiv 1 \pmod{4}$ et $p = \pi\bar{\pi}$, on a $e(\pi)^{mk} + e(\bar{\pi})^{mk} = 2 \cos(mk\theta_p)$. On a donc

$$\begin{aligned} \mathcal{L}_m(s) &= 2D_m(s) + g_m(s), \text{ avec} \\ g_m(s) &= \sum_{k \geq 1} \frac{(-1)^{mk/4}}{k2^{ks}} + \sum_{p \equiv 3 \pmod{4}, k \geq 1} \frac{1}{kp^{2ks}} + \sum_{p \equiv 1 \pmod{4}, k \geq 2} \frac{2 \cos(mk\theta_p)}{kp^{ks}}. \end{aligned}$$

On a déjà vu que $D_m(s)$ est absolument convergente pour $\operatorname{Re} s > 1$, et la série $g_m(s)$ est absolument convergente pour $\operatorname{Re} s > 1/2$ par le même argument que dans la preuve de la Proposition 1.4. Par exponentiation on a en outre, pour $\operatorname{Re} s > 1$

$$\exp \mathcal{L}_m(s) = L_m(s).$$

En raisonnant exactement comme dans la démonstration de la Proposition 2.7, il suffit alors de démontrer le théorème suivant ! \square

Théorème 6.5. *On a $L_m(1) \neq 0$ pour $m \neq 0$.*

La démonstration un peu astucieuse suivante est inspirée de celle du théorème des nombres premiers par Hadamard et La Vallée Poussin.

DÉMONSTRATION — Nous allons utiliser l'inégalité suivante (!)

$$(7) \quad \operatorname{Re}(4e^{i\theta} + e^{2i\theta} + 3) = 4 \cos \theta + \cos 2\theta + 3 = 2(\cos \theta + 1)^2 \geq 0, \quad \forall \theta \in \mathbb{R}.$$

Appliquée à chacun des éléments $e(\pi)^{mk} =: e^{i\theta}$ pour $k \geq 1$ et $\pi \in \mathcal{Q}$, elle montre que pour s réel > 1 on a $\operatorname{Re}(4\mathcal{L}_m(s) + \mathcal{L}_{2m}(s) + 3\mathcal{L}_0(s)) \geq 0$ et donc

$$(8) \quad |L_m(s)^4 L_{2m}(s) L_0(s)^3| \geq 1, \quad \forall s > 1$$

par exponentiation. D'après le Corollaire 6.3, la série de Dirichlet $L_0(s)$ se prolonge méromorphiquement sur $\operatorname{Re} s > 0$, avec $s = 1$ pour unique pôle, qui est simple. D'après la Proposition 6.4, les fonctions $L_m(s)$ et $L_{2m}(s)$ sont holomorphes sur $\operatorname{Re} s > 1/2$. Si $L_m(1) = 0$, la fonction $L_m(s)^4 L_{2m}(s) L_0(s)^3$ est donc holomorphe sur $\operatorname{Re} s > 1/2$, et s'annule en $s = 1$, contredisant (8). \square

Remarque 6.6. *Le même argument redémontre aussi $L(1, \chi) \neq 0$ pour $\chi^2 \neq 1$.*

7. PROLONGEMENT ANALYTIQUE DES $L_m(s)$ À $\operatorname{Re} s > 1/2$

Pour démontrer la Proposition 6.4, on peut supposer $m > 0$ par l'identité $L_m = L_{-m}$ (considérer $z \mapsto \bar{z}$). Il suffit de prouver que pour r réel > 0 on a

$$(9) \quad \sum_{z \in \mathbb{Z}[i], |z| \leq r} z^m = O(r^{1+m}), \quad r \rightarrow +\infty.$$

En effet, pour $\operatorname{Re} s > 1 + \frac{m}{2}$ on a $4L_m(s - \frac{m}{2}) = \sum_{z \in \mathbb{Z}[i]} \frac{z^m}{N(z)^s}$. La majoration (9) pour $r = \sqrt{n}$ et le Lemme A.1 (ii) montrent que la série $L_m(s - \frac{m}{2})$ converge uniformément sur tout compact de $\operatorname{Re} s > \frac{1+m}{2}$, ce que l'on voulait démontrer.

Pour montrer (9), nous allons étudier ce type de sommes dans leur contexte naturel. On se place pour cela dans le plan euclidien \mathbb{R}^2 , dont on note D le disque unité fermé, et on pose $Z_r = (\frac{1}{r}\mathbb{Z}^2) \cap D$ pour r réel > 0 . Le résultat ci-dessous est une variante d'un résultat classique de Gauss (cas $f = 1$). L'identité (9) se déduit du cas $f(z) = z^m$ avec $m \neq 0$, pour lequel on a $\int_D f = \int_0^1 dr \int_0^{2\pi} e^{im\theta} d\theta = 0$.

Proposition 7.1. *Soient U un voisinage ouvert de D dans \mathbb{C} et $f : U \rightarrow \mathbb{C}$ une fonction de classe \mathcal{C}^1 . On a $\sum_{z \in Z_r} f(z) = r^2 \int_D f + O(r)$ quand $r \rightarrow +\infty$.*

DÉMONSTRATION — Posons $C = [0, 1]^2$. Les parties de \mathbb{R}^2 de la forme $z + C$, avec $z \in \mathbb{Z}^2$, sont deux à deux disjointes. Posons $E_r = \coprod_{z \in Z_r} (z + \frac{1}{r}C)$ et $D_r = \{z \in \mathbb{R}^2, |z| \leq r\}$. On a les inclusions

$$(10) \quad D \subset E_r \subset D_{1 + \frac{\sqrt{2}}{r}}.$$

En effet, la seconde résulte immédiatement de l'inégalité triangulaire. Pour la première, on constate que pour tout $(x, y) \in D$, et pour $(m, n) := ([rx], [ry]) \in \mathbb{Z}^2$, on a $\frac{1}{r}(m, n) \in Z_r$ et $r(x, y) - (m, n) \in C$.

Considérons d'abord le cas particulier $f = 1$, pour lequel la somme de l'énoncé est $|Z_r|$. Notons $\operatorname{vol}(A)$ la mesure (ou *aire*) d'une partie borélienne $A \subset \mathbb{R}^2$. On a $\operatorname{vol}(E_r) = \frac{|Z_r|}{r^2}$, et par les inclusions (10), $\operatorname{vol}(E_r) = \operatorname{vol}(D) + \operatorname{vol}(E_r \setminus D)$ et

$$(11) \quad \operatorname{vol}(E_r \setminus D) \leq \operatorname{vol}(D_{1 + \frac{\sqrt{2}}{r}} \setminus D) = O(1/r),$$

ce qui termine la démonstration pour $f = 1$. Pour un f général, quitte à rétrécir U on peut supposer $U = D_{1 + \frac{\sqrt{2}}{r_0}}$ pour un certain $r_0 > 1$, et que f et sa différentielle df sont bornées sur U par une constante $M > 0$. Pour $r > r_0$, on a $D \subset E_r \subset U$ puis

$$\frac{1}{r^2} \sum_{z \in Z_r} f(z) - \int_D f = \sum_{z \in Z_r} \int_{z + \frac{1}{r}C} (f(z) - f) + \int_{E_r \setminus D} f.$$

On a d'une part $|\int_{E_r \setminus D} f| \leq M \operatorname{vol}(E_r \setminus D) = O(1/r)$ par (11). D'autre part, pour $z \in Z_r$ et $w \in z + \frac{1}{r}C$ on a les inégalités $|f(z) - f(w)| \leq M|z - w| \leq M\frac{\sqrt{2}}{r}$, puis la majoration

$$\sum_{z \in Z_r} \int_{z + \frac{1}{r}C} |f(z) - f| \leq M \frac{\sqrt{2}}{r} \sum_{z \in Z_r} \int_{z + \frac{1}{r}C} 1 = O\left(\frac{1}{r}\right)$$

par le cas $f = 1$, ce qui conclut. □

ANNEXE A. RAPPELS SUR LES SÉRIES DE DIRICHLET

On regroupe dans cette annexe les quelques vérifications analytiques que nous avons laissées de côté dans le corps du texte (mais déjà vues dans le cours d'analyse complexe). On rappelle qu'une *série de Dirichlet* est une série de la forme

$$f(s) = \sum_{n \geq 1} \frac{a_n}{n^s},$$

avec les a_n dans \mathbb{C} . On la verra en général comme une fonction de la variable complexe ou réelle s . La fonction $\zeta(s)$ de Riemann en est un exemple fameux pour $\operatorname{Re} s > 1$ (cas $a_n = 1$), mais c'est aussi le cas de nombreuses fonctions rencontrées dans ce texte. On rappelle que pour $n \geq 1$ et $s \in \mathbb{C}$ on a $n^s := e^{s \log n}$. En particulier, n^s est une fonction entière de s qui ne s'annule pas sur \mathbb{C} . On a de plus

$$|n^s| = e^{\sigma \log n} = n^\sigma \text{ pour } \sigma = \operatorname{Re} s,$$

une quantité croissante de σ . Pour $r \in \mathbb{R}$ on pose $\mathcal{D}_r = \{s \in \mathbb{C} \mid \operatorname{Re} s > r\}$.

Lemme A.1. (i) Si la suite a_n est bornée, alors $\sum_{n \geq 1} \frac{a_n}{n^s}$ converge normalement sur \mathcal{D}_r pour tout $r > 1$. En particulier, elle définit une fonction holomorphe de s sur \mathcal{D}_1 .

(ii) Si la suite des sommes partielles $A_n = \sum_{k=1}^n a_k$ vérifie $A_n = O(n^r)$ pour un certain réel r , alors $\sum_{n \geq 1} \frac{a_n}{n^s}$ converge uniformément sur tout compact de \mathcal{D}_r . En particulier, elle définit une fonction holomorphe s sur \mathcal{D}_r .

DÉMONSTRATION — Montrons le (i). Si $|a_n| \leq M$ et $s \in \mathcal{D}_r$, on a $|a_n n^{-s}| \leq M n^{-r}$, et on conclut par l'inégalité bien connue $\sum_{n \geq 2} \frac{1}{n^r} \leq \int_1^\infty \frac{dt}{t^r} = 1/(r-1)$ pour $r > 1$. Pour le (ii), on pose $A_0 = 0$ et on écrit (transformation d'Abel)

$$\sum_{n=1}^N \frac{a_n}{n^s} = \frac{A_N}{N^s} + \sum_{n=1}^{N-1} A_n \left(\frac{1}{n^s} - \frac{1}{(n+1)^s} \right).$$

Par accroissements finis appliqués à $t \mapsto t^{-s}$ sur $[n, n+1]$ on a $|\frac{1}{n^s} - \frac{1}{(n+1)^s}| \leq \frac{|s|}{n^{\operatorname{Re} s + 1}}$, de sorte que par le (i), la série ci-dessus converge uniformément sur le compact $\operatorname{Re} s \geq r'$ et $|s| \leq C$, pour tout $C > 0$ et $r' > r$. \square

Ce lemme et l'assertion (2.5) montrent que $L(s, \chi)$ converge normalement sur \mathcal{D}_r pour tout $r > 1$, et uniformément sur tout compact de \mathcal{D}_0 pour $\chi \neq 1$.

Proposition A.2. La fonction $\zeta(s)$ se prolonge méromorphiquement à \mathcal{D}_0 , avec un unique pôle en $s = 1$, qui est simple de résidu 1.

DÉMONSTRATION — Soit $s \in \mathcal{D}_1$. L'identité $\frac{1}{s-1} = \int_1^\infty \frac{dt}{t^s}$ permet d'écrire

$$\zeta(s) = \frac{1}{s-1} + \sum_{n \geq 1} \int_n^{n+1} \left(\frac{1}{n^s} - \frac{1}{t^s} \right) dt.$$

Mais on a $|\int_n^{n+1} (\frac{1}{n^s} - \frac{1}{t^s}) dt| \leq \sup_{n \leq t \leq n+1} |\frac{1}{n^s} - \frac{1}{t^s}| \leq \frac{|s|}{n^{1+\operatorname{Re} s}}$, donc la série de fonctions ci-dessus (holomorphes sur \mathcal{D}_0) converge normalement sur tout compact de \mathcal{D}_0 . \square

Lemme A.3. (Landau) Soient $f(s) = \sum_{n \geq 1} a_n n^{-s}$ une série de Dirichlet à coefficients a_n réels ≥ 0 , et $\sigma \in \mathbb{R}$ tel que f converge absolument sur \mathcal{D}_σ . Si f se prolonge analytiquement sur un voisinage de σ dans \mathbb{C} , il existe $\sigma' < \sigma$ tel que $f(\sigma')$ converge.

DÉMONSTRATION — Quitte à remplacer $f(s)$ par $f(s + \sigma)$, soit encore a_n par $a_n n^{-\sigma}$ (toujours ≥ 0), on peut supposer $\sigma = 0$. Pour $N \geq 1$ on pose $f_N(s) = \sum_{n=1}^N a_n n^{-s}$. Pour tous entiers $k \geq 0, N \geq 1$, et tout réel $s > 0$, on a les inégalités

$$(12) \quad (-1)^k f^{(k)}(s) = \sum_{n \geq 1} a_n (\log n)^k n^{-s} \geq (-1)^k f_N^{(k)}(s) \geq 0,$$

d'abord par la convergence normale susmentionnée, puis par positivité des a_n .

Supposons que f se prolonge analytiquement au voisinage de 0, et donc sur un disque ouvert de centre 1 et de rayon $1 + 2\epsilon$ pour un certain $\epsilon > 0$. Par Cauchy, on a convergence absolue de la série de Taylor $S := \sum_{k \geq 0} \frac{f^{(k)}(1)}{k!} (-\epsilon - 1)^k$, puis

$$S = \sum_{k \geq 0} \frac{(-1)^k f^{(k)}(1)}{k!} (1 + \epsilon)^k \geq \sum_{k \geq 0} \frac{(-1)^k f_N^{(k)}(1)}{k!} (1 + \epsilon)^k = f_N(-\epsilon)$$

pour tout $N \geq 1$ par l'inégalité (12). En faisant tendre N vers l'infini, on en déduit $\sum_{n \geq 1} a_n n^\epsilon \leq S$, ce que l'on voulait démontrer. \square

Corollaire A.4. (mêmes hypothèses) Si f se prolonge analytiquement à $\mathcal{D}_{\sigma'}$ pour un réel $\sigma' < \sigma$, alors $f(s)$ converge absolument pour tout $s \in \mathcal{D}_{\sigma'}$.

DÉMONSTRATION — Notons $a \in \mathbb{R}$ la borne inférieure dans $\{-\infty\} \cup \mathbb{R}$ de l'ensemble des réels s tels que $f(s)$ converge (nécessairement absolument). On a $a \leq \sigma$ et $f(s)$ converge absolument sur \mathcal{D}_a . Mais si l'on suppose $\sigma' < a$, le lemme de Landau appliqué au point a contredit la définition de a : on a donc $a \leq \sigma'$. \square

Faisons maintenant quelques rappels sur les produits infinis. Soit b_n une suite de nombres réels positifs (ou $+\infty$). La suite $\prod_{i=1}^n (1 + b_i)$ croît avec l'entier n , et on note

$$\prod_{n \geq 1} (1 + b_n) \in \mathbb{R}_{>0} \cup \{+\infty\}$$

sa limite. On dit que le produit des $1 + b_n$ est convergent si $\prod_n (1 + b_n) < +\infty$. Il est clair que l'on a $\prod_n (1 + b_n) \geq \sum_n b_n$, et l'inégalité $1 + x \leq e^x$ pour $x \geq 0$ assure même que $\sum_n b_n < +\infty$ si, et seulement si, $\prod_n (1 + b_n) < +\infty$.

Supposons maintenant $b_n \in \mathbb{C}$. On dit que le produit des $1 + b_n$ est absolument convergent si $\prod_n (1 + |b_n|) < +\infty$. Dans ce cas, la finitude de $\sum_n |b_n|$ montre par critère de Cauchy que la suite $\prod_{i=1}^n (1 + b_i)$ converge quand $n \rightarrow \infty$ vers un nombre complexe noté $\prod_i (1 + b_i)$. Elle entraîne de plus que pour toute bijection σ de \mathbb{N} , on a l'égalité $\prod_i (1 + b_{\sigma(i)}) = \prod_i (1 + b_i)$. Ces propriétés ne sont pas sans rappeler celles des familles sommables. Un produit eulérien est un produit infini absolument convergent indexé par les nombres premiers (qu'il n'est donc pas nécessaire de numéroter).

Lemme A.5. (Euler) Soit $(a_n)_{n \geq 1}$ une suite de nombres complexes vérifiant $a_1 = 1$ et $a_{mn} = a_m a_n$ si m et n sont premiers entre eux. Soient $s \in \mathbb{C}$ et $\sigma = \operatorname{Re}(s)$. Les conditions suivantes sont équivalentes :

- (i) $\prod_p (\sum_{i \geq 0} \frac{|a_{p^i}|}{p^{i\sigma}}) < +\infty$, le produit étant pris sur tous les nombres premiers p ,
(ii) $\sum_{n \geq 1} \frac{|a_n|}{n^\sigma} < +\infty$.

Si elles sont satisfaites, on a l'égalité $\sum_{n \geq 1} \frac{a_n}{n^s} = \prod_p (\sum_{i \geq 0} \frac{a_{p^i}}{p^{is}})$, cette série et ce produit étant absolument convergents.

DÉMONSTRATION — Soient $N \geq 1$ un entier et S_N l'ensemble des entiers ≥ 1 dont tous les facteurs premiers sont $\leq N$. La propriété de multiplicativité de (a_n) , et l'existence et unicité de la décomposition d'un entier en facteurs premiers, montrent

$$\prod_{p \leq N} (\sum_{i \geq 0} \frac{|a_{p^i}|}{p^{i\sigma}}) = \sum_{n \in S_N} \frac{|a_n|}{n^\sigma}$$

(un égalité dans $\mathbb{R}_{\geq 0} \cup \{+\infty\}$). En faisant tendre N vers $+\infty$, on en déduit que l'on a $\prod_p (\sum_{i \geq 0} \frac{|a_{p^i}|}{p^{i\sigma}}) = \sum_{n \geq 1} \frac{|a_n|}{n^\sigma}$, puis l'équivalence de (i) et (ii). Supposons ces assertions sont satisfaites. Par factorialité de \mathbb{Z} et multiplicativité de (a_n) on a alors

$$\prod_{p \leq N} (\sum_{i \geq 0} \frac{a_{p^i}}{p^{is}}) = \sum_{n \in S_N} \frac{a_n}{n^s},$$

et on conclut en faisant tendre $N \rightarrow \infty$. \square

Exemple A.6. Si χ est un caractère de Dirichlet, et si on pose $a_n := \chi(n)$, l'hypothèse (ii) est satisfaite pour $\operatorname{Re} s > 1$, et on a en outre $\sum_{i \geq 1} \frac{\chi(p^i)}{p^{is}} = \frac{1}{1 - \chi(p)p^{-s}}$ pour tout p , de sorte que le Lemme A.5 entraîne la Formule (1) et la Proposition 2.4.

ANNEXE B. ÉQUATION FONCTIONNELLE DE ζ , SUIVANT RIEMANN

Dans ce complément, annoncé dans l'introduction, nous exposons une des deux démonstrations de Riemann du prolongement méromorphe de $\zeta(s)$ à \mathbb{C} tout entier, ainsi que de son équation fonctionnelle. On rappelle la fonction Γ d'Euler, définie pour $\operatorname{Re} s > 0$ par l'intégrale absolument convergente

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

Elle admet un prolongement méromorphe à \mathbb{C} vérifiant $\Gamma(s+1) = s\Gamma(s)$. On sait que $\Gamma(s)$ ne s'annule pas sur \mathbb{C} et a pour pôles (simples) les entiers ≤ 0 .

Théorème B.1. La fonction $\Lambda(s) := \pi^{-s/2} \Gamma(s/2) \zeta(s)$ se prolonge méromorphiquement à \mathbb{C} tout entier et y vérifie $\Lambda(1-s) = \Lambda(s)$. De plus, elle a pour uniques pôles $s = 1$ et $s = 0$, qui sont simples et de résidus respectifs 1 et -1 .

Le point de départ de Riemann est l'identité, pour $\operatorname{Re} s > 1$ et $n \geq 1$,

$$(13) \quad \pi^{-\frac{s}{2}} n^{-s} \Gamma(s/2) = \int_0^\infty e^{-n^2 \pi t} t^{\frac{s}{2}} \frac{dt}{t}.$$

un simple changement de variable dans $\Gamma(s/2)$. Cela pousse à considérer la fonction $\vartheta : \mathbb{R}_{>0} \rightarrow \mathbb{R}$ définie par $\vartheta(t) = \sum_{n \in \mathbb{Z}} e^{-\pi t n^2}$. La convergence est triviale : on a même

$$(14) \quad |\vartheta(t) - 1| \leq 2 \sum_{n=1}^\infty e^{-\pi t n} = \frac{2e^{-\pi t}}{1 - e^{-\pi t}}, \quad \forall t > 0.$$

En particulier, on a $\vartheta(t) = 1 + O(e^{-\pi t})$ pour $t \rightarrow +\infty$, et $\vartheta(t) = O(\frac{1}{t})$ pour $t \rightarrow 0^+$. Poursuivant l'idée de départ (13), on considère pour $s \in \mathbb{C}$, l'intégrale

$$(15) \quad I(s) = \int_0^\infty (\vartheta(t) - 1)t^{s/2} \frac{dt}{t}$$

(une *transformée de Mellin*). Les estimées ci-dessus montrent qu'elle converge absolument pour tout s au voisinage de $t = \infty$, et pour $\operatorname{Re} s > 2$ au voisinage de $t = 0$. Ainsi, $I(s)$ est une fonction holomorphe de s sur ce dernier demi-plan. En développant brutalement ϑ en série, et en intervertissant somme et intégrale (loisible, car tout est absolument convergent), l'identité (13) montre

$$(16) \quad I(s) = 2\Lambda(s), \quad \operatorname{Re} s > 2.$$

Nous allons prolonger $I(s)$ sur \mathbb{C} en étudiant les propriétés de $\vartheta(t)$ au voisinage de 0. La clé de la démonstration est suivante :

Lemme B.2. (Identité de Poisson) *On a $\vartheta(1/t) = \sqrt{t}\vartheta(t)$, $\forall t > 0$.*

DÉMONSTRATION — Pour toute fonction de Schwarz sur \mathbb{R} , rappelons que l'on a

$$\sum_{n \in \mathbb{Z}} f(n) = \sum_{n \in \mathbb{Z}} \widehat{f}(n) \quad \text{avec} \quad \widehat{f}(\xi) := \int_{\mathbb{R}} f(x)e^{-2i\pi x\xi} dx \quad \text{pour} \quad \xi \in \mathbb{R}$$

(*formule sommatoire de Poisson*). Mais dans le cas de la gaussienne $f_t(x) = e^{-\pi tx^2}$, où $t > 0$ est un paramètre réel, on sait depuis Gauss que l'on a $\widehat{f}_1 = f_1$ puis $\widehat{f}_t = \frac{1}{\sqrt{t}}f_{1/t}$, de sorte que l'identité ci-dessus est exactement celle de l'énoncé. \square

L'identité de Poisson montre, pour $\operatorname{Re} s > 2$,

$$\begin{aligned} \int_0^1 (\vartheta(t) - 1)t^{\frac{s}{2}} \frac{dt}{t} &= \int_1^\infty (\vartheta(1/t) - 1)t^{-\frac{s}{2}} \frac{dt}{t} = \int_1^\infty (\sqrt{t}\vartheta(t) - 1)t^{-\frac{s}{2}} \frac{dt}{t} \\ &= \int_1^\infty (\vartheta(t) - 1)t^{\frac{1-s}{2}} \frac{dt}{t} + \int_1^\infty (\sqrt{t} - 1)t^{-\frac{s}{2}} \frac{dt}{t}. \end{aligned}$$

Mais on a $\int_1^\infty (\sqrt{t} - 1)t^{-\frac{s}{2}} \frac{dt}{t} = \frac{2}{s-1} - \frac{2}{s}$, et donc par (15) et (16) :

$$(17) \quad \Lambda(s) = \frac{1}{2}I(s) = \frac{1}{2} \int_1^\infty (\vartheta(t) - 1)(t^{\frac{s}{2}} + t^{\frac{1-s}{2}}) \frac{dt}{t} + \frac{1}{s-1} - \frac{1}{s}.$$

L'intégrale ci-dessus est manifestement absolument convergente pour tout $s \in \mathbb{C}$. C'est donc une fonction entière de s , trivialement invariante par $s \mapsto 1-s$, de sorte que le terme de droite des égalités (17) fournit le prolongement cherché (l'assertion sur ses pôles est évidente). Cela termine la démonstration du Théorème B.1. \square

ANNEXE C. ÉQUATIONS FONCTIONNELLES DES L_m , SUIVANT HECKE

Expliquons maintenant comment Hecke généralise la méthode de l'Annexe B pour démontrer le résultat suivant (on rappelle que l'on a $L_m = L_{-m}$) :

Théorème C.1. *Pour $m \geq 0$, la fonction $\Lambda_m(s) := \pi^{-s-\frac{m}{2}} \Gamma(s + \frac{m}{2}) L_m(s)$ se prolonge méromorphiquement à \mathbb{C} tout entier et vérifie $\Lambda_m(1-s) = \Lambda_m(s)$. Elle est en fait holomorphe sur \mathbb{C} , sauf pour $m = 0$ auquel cas elle a pour uniques pôles $s = 1$ et $s = 0$, qui sont simples et de résidus respectifs $\frac{1}{4}$ et $-\frac{1}{4}$.*

Hecke considère pour cela la *fonction thêta harmonique* :

$$\vartheta_m(t) = \sum_{z \in \mathbb{Z}[i]} z^m e^{-t\pi|z|^2}, \quad t \in \mathbb{R}_{>0}.$$

Pour $m = 0$, on convient que z^m vaut 1 pour tout $z \in \mathbb{C}$. La série $\vartheta_m(t)$ est absolument convergente, de la forme $\delta_{m,0} + \sum_{n \geq 1} 4h_m(n) n^{m/2} e^{-n\pi t}$ avec $h_m(n) = O(\sqrt{n})$ et $\delta_{i,j}$ le symbole de Kronecker. On vérifie de plus aisément la majoration :⁶

$$(18) \quad \vartheta_m(t) = \delta_{m,0} + O(e^{-\pi t}) \quad \text{pour } t \rightarrow +\infty,$$

Proposition C.2. *Pour tout réel $t > 0$, on a $\vartheta_m(1/t) = t^{m+1}\vartheta_m(t)$.*

Pour démontrer cette identité, identifions le plan euclidien standard \mathbb{R}^2 et avec \mathbb{C} (muni de $|z|^2$) par la bijection usuelle $(x, y) \mapsto x + iy$. La formule de Poisson dans \mathbb{R}^2 s'écrit alors, pour toute fonction f dans l'espace de Schwartz sur \mathbb{C} ,

$$\sum_{z \in \mathbb{Z}[i]} f(z) = \sum_{z \in \mathbb{Z}[i]} \widehat{f}(z) \quad \text{avec} \quad \widehat{f}(w) = \int_{\mathbb{C}} f(z) e^{-i\pi(z\bar{w} + \bar{z}w)} \frac{1}{2} |dz d\bar{z}|.$$

(Le terme $\frac{1}{2}|dz d\bar{z}|$ est juste une autre notation pour $dx dy$.) Fixons un réel $t > 0$ et considérons la fonction de Schwartz $f_{m,t} : \mathbb{C} \rightarrow \mathbb{C}$, $z \mapsto z^m e^{-t\pi|z|^2}$. La Proposition C.2 résulte immédiatement de la formule de Poisson appliquée à $f_{m,t}$, et du :

Lemme C.3. *Pour tout réel $t > 0$ on a $\widehat{f_{m,t}} = \frac{1}{t^{1+m}} f_{m,1/t}$.*

DÉMONSTRATION — Montrons d'abord $f_{m,1} = \widehat{f_{m,1}}$ (cas $t = 1$). Pour $m = 0$, $f_{0,1}$ est la gaussienne euclidienne standard $e^{-\pi(x^2+y^2)}$ sur \mathbb{R}^2 . On sait donc, depuis Gauss, que l'on a $\widehat{f_{0,1}} = f_{0,1}$, c'est-à-dire

$$e^{-\pi w\bar{w}} = \int_{\mathbb{C}} e^{-\pi|z|^2} e^{-i\pi(z\bar{w} + \bar{z}w)} \frac{1}{2} |dz d\bar{z}|.$$

Appliquons à cette identité m fois l'opérateur différentiel $\frac{\partial}{\partial \bar{w}} = \frac{1}{2}(\frac{\partial}{\partial x} + i\frac{\partial}{\partial y})$ du cours d'analyse complexe, ce qui est bien sûr loisible. On en déduit, pour tout $w \in \mathbb{C}$,

$$(-\pi)^m f_{m,1}(w) = (-i\pi)^m \widehat{f_{m,1}}(w),$$

et on conclut car $m \equiv 0 \pmod{4}$. On en déduit l'énoncé par un simple changement de variables $w \mapsto w/\sqrt{t}$ et $z \mapsto z\sqrt{t}$. \square

DÉMONSTRATION — (Du Théorème C.1) On rappelle que l'on a $\Gamma(s) = \int_0^\infty e^{-t} t^{s-1} dt$ pour $\operatorname{Re} s > 0$. Par changement de variable $t' = \pi t|z|^2$, avec $z \neq 0$, on a l'identité :

$$(19) \quad \int_0^\infty e^{-\pi t|z|^2} t^{s+\frac{m}{2}} \frac{dt}{t} = (\pi|z|^2)^{-s-m/2} \Gamma(s + \frac{m}{2}), \quad \text{pour tout } z \in \mathbb{C}^\times.$$

6. Par récurrence sur l'entier $k \geq 0$, il existe un unique polynôme $P_k \in \mathbb{Z}[x]$ vérifiant $\sum_{n \geq 0} n^k x^n = \frac{P_k(x)}{(1-x)^{k+1}}$ pour $|x| < 1$ (appliquer $x \frac{\partial}{\partial x}$). On a $P_0 = 1$, et la relation de récurrence $P_{k+1}(x) = x(1-x)P_k'(x) + (k+1)xP_k(x)$ montre que P_k est de degré k , $P_k(1) = k! \neq 0$, et aussi $P_k(0) = 0$ et $P_k'(0) = 1$ pour $k > 0$. On conclut en prenant $x = e^{-\pi t}$ et $k > \frac{1+m}{2}$.

Supposons d'abord $m > 0$. Dans ce cas, il n'y a pas de contribution de $z = 0$ dans $\vartheta_m(t)$. On a la majoration (18) pour $t \rightarrow +\infty$, puis $\vartheta_m(t) = O(t^{-1-m}e^{-\pi/t})$ par l'identité de Poisson (Proposition C.2) pour $t \rightarrow 0^+$. L'intégrale

$$I_m(s) := \int_0^\infty \vartheta_m(t) t^{s+\frac{m}{2}} \frac{dt}{t}$$

est donc absolument convergente et holomorphe pour $s \in \mathbb{C}$. En développant $\vartheta_m(t)$ en série, et utilisant l'identité (19), on constate pour $\operatorname{Re} s > 1$

$$I_m(s) = \pi^{-s-\frac{m}{2}} \Gamma\left(s + \frac{m}{2}\right) \sum_{z \in \mathbb{Z}[i] \setminus \{0\}} \frac{z^m}{|z|^{2s+m}} = 4 \pi^{-s-\frac{m}{2}} \Gamma\left(s + \frac{m}{2}\right) L_m(s) = 4 \Lambda_m(s)$$

L'interversion série-intégrale est loisible pour $\operatorname{Re} s > 1$ car la série ci-dessus est alors absolument convergente : on a montré le prolongement analytique de Λ_m à \mathbb{C} tout entier ! Mieux, on a aussi

$$\int_0^1 \vartheta_m(t) t^{s+\frac{m}{2}} \frac{dt}{t} = \int_1^\infty \vartheta_m(1/t) t^{-s-\frac{m}{2}} \frac{dt}{t} = \int_1^\infty \vartheta_m(t) t^{1-s+\frac{m}{2}} \frac{dt}{t}$$

par changement de variable $t \mapsto 1/t$ et l'identité $\vartheta_m(1/t) = t^{1+m} \vartheta_m(t)$, et donc

$$I_m(s) = \int_1^\infty \vartheta_m(t) (t^{s+\frac{m}{2}} + t^{1-s+\frac{m}{2}}) \frac{dt}{t} = I_m(1-s), \quad \forall s \in \mathbb{C},$$

puis $\Lambda_m(s) = \Lambda_m(1-s)$ pour tout $s \in \mathbb{C}$. Le cas $m = 0$ se traite de manière similaire en prenant garde au terme $z = 0$ dans ϑ_0 comme dans le cas de $\zeta(s)$. Nous laissons au lecteur le soin de montrer que l'on a la formule

$$4 \Lambda_0(s) = \int_1^\infty (\vartheta_0(t) - 1) (t^s + t^{1-s}) \frac{dt}{t} + \frac{1}{s-1} - \frac{1}{s},$$

l'intégrale ci-dessus étant absolument convergente pour tout $s \in \mathbb{C}$. \square

Remarque C.4. Pour $m = 0$, le théorème résulterait aussi de la formule $L_0(s) = \zeta(s)L(s, \chi_4)$ (Corollaire 6.3), du prolongement analytique de $L(s, \chi_4)$ à \mathbb{C} et de son équation fonctionnelle $L(s, \chi_4) = L(1-s, \chi_4)$.

RÉFÉRENCES

- [ALG] G. Chenevier, *Algèbre, Cours de 1ère année à l'ENS* (2022).
- [AC] A. Mézard, *Analyse complexe, Cours de 1ère année à l'ENS* (2022).
- [DAV80] H. Davenport, *Multiplicative number theory*, Springer GTM 74 (1980).
- [GWW98] E. Gethner, S. Wagon & B. Wick, *A Stroll Through the Gaussian Primes*, The American Mathematical Monthly 105 (4), 327–337 (1998).
- [GM04] A. Granville & G. Martin, *Prime number races* (2004).
- [HEC20] E. Hecke, *Eine neue Art von Zetafunktion und ihre Beziehungen zur Verteilung der Primzahlen*, Math. Z. 6, 11–51 (1920).
- [IR90] K. Ireland & M. Rosen, *A classical introduction to modern number theory*, Springer GTM 84 (1990).
- [MT06] R. Murty & N. Thain, *Primes in certain arithmetic progressions*, Funct. Approx. Comment. Math. 35, 249–259 (2006).
- [SER68] J.-P. Serre, Appendice au chapitre 1 du livre *Abelian ℓ -adic Representations and Elliptic Curves*, Mc Gill University lecture notes, Addison Wesley (1968).
- [SER70] J.-P. Serre, *Cours d'arithmétique*, P.U.F., Paris (1970).