Le théorème de la progression arithmétique

Camille LANUEL

année scolaire 2016-2017

encadré par Joël MERKER

Table des matières

1 Introduction

Euclide a prouvé dans les *Éléments* que l'ensemble $\mathcal{P}$ des nombres premiers est de cardinal infini. Il s'agit de l'un des résultats les plus connus sur les nombres premiers, dont de nombreux mystères restent à élucider.

On peut en particulier se poser la question plus précise suivante : étant donné deux entiers a et b, combien de nombres premiers la progression arithmétique :

$$\{an+b\}_{n\in\mathbb{N}} = \{b, a+b, 2a+b, \ldots\}$$

contient-elle ?

Évidemment, si $\text{pgcd}(a,b) \neq 1$, alors tous les $an+b$ sont multiples de $\text{pgcd}(a,b)$ et ne sont donc jamais premiers pour $n \geqslant 1$. Mais lorsque a et b sont premiers entre eux, c'est-à-dire $\text{pgcd}(a,b) = 1$, après quelques études de cas particuliers et de tests numériques, on imagine facilement que cette progression arithmétique contient une infinité de nombres premiers.

On remarque que dans le cas très particulier où $a = 1$ et $b = 0$, on retrouve :

$$\{1 \times n + 0\}_{n\in\mathbb{N}} = \mathbb{N} \supset \mathcal{P}$$

qui satisfait ce que l'on vient d'énoncer.

L'objectif de cet article est alors de prouver, avec des moyens théoriques relativement simples, le *théorème de la progression arithmétique*, aussi appelé *théorème de Dirichlet*, du nom de celui qui le démontra en premier.

Théorème 1.1 (de la progression arithmétique)**.** *Pour tous $a, b \in \mathbb{N}$ premiers entre eux, la progression arithmétique :*

$$\{an+b\}_{n\in\mathbb{N}} = \{b, a+b, 2a+b, \ldots\}$$

contient une infinité de nombres premiers. Autrement dit :

$$\text{Card}\left(\mathcal{P} \cap \{an+b\}_{n\in\mathbb{N}}\right) = +\infty.$$

En termes d'arithmétique modulaire, cela s'écrit :

$$\text{Card}\left(\{p \in \mathcal{P} \colon p \equiv b\,[a]\}\right) = +\infty.$$

Pour illustrer ce théorème, regardons par exemple le cas où $a = 4$ et $b = 1$. Le tableau suivant montre les nombres premiers parmi les 100 premiers termes de la suite arithmétique $(4n+1)_{n\in\mathbb{N}}$.

1	5	9	13	17	21	25	29	33	37
41	45	49	53	57	61	65	69	73	77
81	85	89	93	97	101	105	109	113	117
121	125	129	133	137	141	145	149	153	157
161	165	169	173	177	181	185	189	193	197
201	205	209	213	217	221	225	229	233	237
241	245	249	253	257	261	265	269	273	277
281	285	289	293	297	301	305	309	313	317
321	325	329	333	337	341	345	349	353	357
361	365	369	373	377	381	385	389	393	397

Grâce à la formule suivante démontrée par Euler :

$$\sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_{p \in \mathcal{P}} \frac{1}{1 - \frac{1}{p^s}},$$

valable pour $s > 1$, celui-ci a démontré de manière élémentaire que :

$$\log\left(\frac{1}{s-1}\right) + \mathrm{O}(1) = \sum_{p \in \mathcal{P}} \frac{1}{p^s} \qquad (s \to 1, \Re(s) > 1).$$

La notation O(1) signifie ici qu'il s'agit d'une fonction bornée au voisinage de 1. Plus généralement, si f, g sont deux fonctions, on dit que g *domine* f au voisinage d'un point a, et l'on note alors $f = \mathrm{O}(g)$, lorsqu'il existe $M \in \mathbb{R}^+$ tel que $|f| \leqslant M|g|$ au voisinage de a.

Et par conséquent :

$$\sum_{p \in \mathcal{P}} \frac{1}{p} = \infty,$$

ce qui fournit une autre preuve de l'infinitude des nombres premiers. C'est ce raisonnement d'Euler que Dirichlet est parvenu à généraliser aux progressions arithmétiques qui nous intéressent ici.

Pour prouver le théorème, nous montrerons que :

$$\lim_{s \to 1^+} \sum_{\substack{p \in \mathcal{P} \\ p \equiv b[a]}} \frac{1}{p^s} = \infty.$$

Pour cela, nous introduirons la notion de *caractères* : il s'agit des fonctions multiplicatives $e : G \longrightarrow \mathbb{S}^1$ (c'est-à-dire $e(x \cdot y) = e(x)e(y)$), avec G un groupe commutatif et $\mathbb{S}^1$ le cercle unité de $\mathbb{C}$. Nous étendrons à $\mathbb{Z}$ les caractères du groupe $(\mathbb{Z}/a\mathbb{Z})^*$ des éléments inversibles de $\mathbb{Z}/a\mathbb{Z}$, nous les noterons χ, et nous montrerons que pour tout $s > 1$:

$$\sum_{\substack{p \in \mathcal{P} \\ p \equiv b[a]}} \frac{1}{p^s} = \frac{1}{\varphi(a)} \sum_{p \nmid a} \frac{1}{p^s} + \frac{1}{\varphi(a)} \sum_{\chi \neq \chi_0} \overline{\chi(b)} \sum_{p} \frac{\chi(p)}{p^s},$$

où χ_0 est le caractère trivial défini pour $n \in \mathbb{Z}$ par :

$$\chi_0(n) := \begin{cases} 1 & \text{si } \mathrm{pgcd}(a, n) = 1, \\ 0 & \text{sinon,} \end{cases}$$

et où φ est la *fonction indicatrice d'Euler*, définie pour $a \in \mathbb{N}^*$ par :

$$\varphi(a) := \mathrm{Card}\left(\{1 \leqslant n \leqslant a \colon \mathrm{pgcd}(a, n) = 1\}\right).$$

Afin d'arriver à cette égalité, nous aurons besoin de résultats que nous fournira l'analyse de Fourier sur les groupes abéliens finis, dont traitera la première partie de cet article.

Il suffira alors de montrer que le deuxième terme de droite reste borné lorsque $s \to 1^+$ puisque le premier terme de droite diverge. Pour cela, nous introduirons des logarithmes, et ce que l'on appelle les fonctions L qui nous permettrons de généraliser la formule d'Euler ci-avant. Soulignons que nous n'utiliserons jamais d'analyse complexe.

De plus, la preuve du théorème de la progression arithmétique nous fournira les résultats nécessaires pour montrer la version plus quantitative suivante :

$$\sum_{\substack{p \in \mathcal{P} \\ p \equiv b[a]}} \frac{1}{p^s} = \frac{1}{\varphi(a)} \log\left(\frac{1}{s-1}\right) + \mathrm{O}(1) \qquad (s \to 1, s > 1),$$

qui démontre également l'infinitude des nombres premiers congrus à $b \mod a$. En particulier, on remarque que ce résultat est *indépendant* de b.

Plus précisément, la proportion de nombres premiers congrus à $b \mod a$ tend asymptotiquement vers $1/\varphi(a)$, c'est-à-dire :

$$\lim_{x \to \infty} \frac{\mathrm{Card}\left(\{p \in \mathcal{P} \colon p \leqslant x, p \equiv b\,[a]\}\right)}{\mathrm{Card}\left(\{p \in \mathcal{P} \colon p \leqslant x\}\right)} = \frac{1}{\varphi(a)}.$$

La preuve de cet énoncé est conséquence de ce qui va suivre, et sera laissée en exercice au lecteur.

Au-delà de ce qui sera présenté dans cet article, il existe des résultats qui permettent d'approfondir la réflexion autour du théorème. Ils ne seront cependant pas prouvés ici.

On définit la *fonction de comptage* pour tout $x \in \mathbb{N}$ par :

$$\pi(x) := \mathrm{Card}\left(\{p \in \mathcal{P} \colon p \leqslant x\}\right).$$

Le théorème suivant fut conjecturé par Gauss, dans la marge d'une table logarithmique à l'âge de 15 ou 16 ans selon ses dires, et par Legendre. Ce sont de la Vallée-Poussin et Hadamard qui le démontrèrent indépendamment en 1896, un siècle après la conjecture de Gauss.

Théorème 1.2 (des nombres premiers)**.** *Lorsque $x \to \infty$, on a :*

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

Autrement dit :

$$\lim_{x \to \infty} \frac{\pi(x)\log(x)}{x} = 1.$$

Afin de comprendre ce qu'il en est de la répartition des nombres premiers congrus à $b \mod a$, introduisons la fonction de comptage suivante :

$$\pi(x, a, b) := \mathrm{Card}\left(\{p \in \mathcal{P} \colon p \leqslant x, p \equiv b\,[a]\}\right).$$

Théorème 1.3. *Lorsque $x \to \infty$, on a :*

$$\pi(x,a,b) \sim \frac{1}{\varphi(a)}\pi(x) \sim \frac{1}{\varphi(a)}\frac{x}{\log(x)}$$

et ce, indépendamment de b premier avec a. □

Mentionnons également qu'à notre époque, le problème similaire de démontrer que la progression quadratique :

$$\left\{a + bn + cn^2\right\}_{n\in\mathbb{N}}$$

contient toujours une infinité de nombres premiers lorsque a, b, c sont des entiers premiers entre eux est toujours *ouvert* !

Avant de passer à la suite de cet article, intéressons-nous rapidement à l'historique du théorème de la progression arithmétique.

En 1735, travaillant sur la résolution du problème de Mengoli, Euler introduisit certains produits infinis pour l'étude des fonctions trigonométriques. Deux ans plus tard, Euler découvrit la formule maintenant célèbre, valable pour $s \in \mathbb{C}$ avec $\Re(s) > 1$:

$$\sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_{p\in\mathcal{P}} \frac{1}{1-\frac{1}{p^s}}.$$

Historiquement, il s'agit de la première apparition d'une information statistique sur les nombres premiers ! En effet, en prenant le logarithme, en faisant un développement asymptotique, et en regardant la limite lorsque $s \to 1^+$, on peut montrer que la somme des inverses des nombres premiers :

$$\sum_{p\in\mathcal{P}} \frac{1}{p} = \frac{1}{2} + \frac{1}{3} + \frac{1}{5} + \frac{1}{7} + \frac{1}{11} + \dots$$

est de l'ordre du logarithme de la somme des inverses des nombres entiers. Cette formule est essentielle et nous la démontrerons pour $s \in \mathbb{R}$ dans la suite. Les écritures de séries en produits d'Euler furent par la suite exploitées par Riemann dans son étude de la fonction éponyme définie pour $s \in \mathbb{C}$ avec $\Re(s) > 1$ par :

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

Le théorème de la progression arithmétique fut conjecturé pour la première fois en 1785 par Adrien-Marie Legendre. Il crut le démontrer en 1808, mais un lemme crucial qu'il utilisa dans sa preuve était erroné.

En 1835, Dirichlet prouva le cas où a est premier, et démontra le cas général l'année suivante. En 1841, il généralisa sa preuve à l'ensemble des *entiers de Gauss* :

$$\mathbb{Z}(i) := \{a + ib \colon a, b \in \mathbb{Z}\}.$$

Les démonstrations de Dirichlet sont d'un intérêt considérable en arithmétique. L'apport algébrique pour la théorie des nombres consiste essentiellement en un développement de l'Analyse Harmonique, car Dirichlet avait déjà travaillé sur les découvertes de Joseph Fourier, et pour la démonstration de son théorème il utilisa des méthodes très analogues, cette fois-ci sur des groupes abéliens, i.e. commutatifs, finis, au lieu du groupe abélien géométrique $\mathbb{S}^1 := \{e^{i\theta} : \theta \in \mathbb{R}\}$. Jacobi aurait écrit au sujet de Dirichlet :

> « En appliquant les séries de Fourier à la théorie des nombres, Dirichlet a récemment trouvé des résultats atteignant les sommets de la perspicacité humaine. »

Dans les mémoires mathématiques de Dirichlet, la théorie des caractères d'un groupe fini pour le cas abélien est pratiquement complète.

De la Vallée Poussin démontra le Théorème 1.3, qui est la version quantitative du théorème, conjecturée par Dirichlet et Legendre, qui entrevoyaient expérimentalement l'équirépartition des nombres premiers dans les classes modulo a. Ce théorème généralise le théorème de Dirichlet, de la même manière que ce dernier généralise le théorème d'Euclide.

En 1998, Ivan Soprounov ([2]) l'a redémontré en seulement quatre pages (!), grâce aux raccourcis mis au point par Donald J. Newman ([1]) en 1980 dans sa preuve remarquablement simple du théorème des nombres premiers, encore contractée par Don Zagier ([4]) en 1997 à l'occasion du centième anniversaire du théorème des nombres premiers.

Références

[1] Newman, D.J. : *Simple analytic proof of the prime number theorem*, Amer. Math. Monthly **87** (1980), 693–696.

[2] Soprounov, I. : *A short proof of the prime number theorem for arithmetic progressions*, 4 pages, academic.csuohio.edu/soprunov/pdf/primes.pdf/

[3] Stein, E. ; Shakarchi, R. : *Fourier analysis. An introduction.* Princeton Lectures in Analysis, 1. Princeton University Press, Princeton, NJ, 2003. xvi+311 pp.

[4] Zagier, D. : *Newman's short proof of the Prime Number Theorem*, Amer. Math. Monthly **104** (1997), no. 8, 705–708.

2 Séries de Fourier sur des groupes abéliens finis

Cette partie a pour but d'établir des résultats fondamentaux pour la preuve du théorème de Dirichlet.

2.1 Analyse de Fourier sur $\mathbb{Z}(n)$

Pour $n \in \mathbb{N}^*$, l'ensemble $\{z \in \mathbb{C} \colon z^n = 1\}$ des racines n-ièmes de l'unité est exactement :

$$\mathbb{Z}(n) := \left\{\exp\left(\tfrac{2ik\pi}{n}\right) \colon\ k \in [\![0, n-1]\!]\right\}.$$

Lemme 2.1. *L'ensemble $\mathbb{Z}(n)$ est un groupe multiplicatif abélien fini, de cardinal n.*

Preuve. En effet, $(\mathbb{Z}(n), \times)$ est un sous-groupe du groupe abélien $(\mathbb{C}, \times)$, car on a $1 \in \mathbb{Z}(n)$, et car si $z, z' \in \mathbb{Z}(n)$, alors $(zz')^n = z^n z'^n = 1 \times 1 = 1$. □

On abrège dorénavant $\zeta = \exp\left(\frac{2ik\pi}{n}\right)$.

Proposition 2.1. *On a $\mathbb{Z}(n) \simeq \mathbb{Z}/n\mathbb{Z}$ via l'isomorphisme :*

$$k \mod n \ \longleftrightarrow\ \zeta^k. \qquad \square$$

Dans la suite, on identifiera donc $\mathbb{Z}(n)$ et $\mathbb{Z}/n\mathbb{Z}$.

Soit E un $\mathbb{C}$-espace-vectoriel. On dit qu'une fonction $f : E \times E \longrightarrow \mathbb{C}$ est un *produit hermitien* lorsque :

1. $\forall\, x, y, z \in E, \forall\, a \in \mathbb{C}, f(ax+y, z) = af(x, z) + f(y, z)$ (linéaire par rapport à la première variable) ;
2. $\forall\, x, y, z \in E, \forall\, a \in \mathbb{C}, f(x, ay + z) = f(x, z) + \overline{a} f(y, z)$ (anti-linéaire par rapport à la seconde variable) ;
3. $\forall\, x, y \in E, f(y, x) = \overline{f(x, y)}$ (à symétrie hermitienne) ;
4. $\forall\, x \in E, f(x, x) \geqslant 0$ (positive), et $f(x, x) = 0 \Leftrightarrow x = 0$ (définie).

Il s'agit de l'équivalent pour E du produit scalaire sur un $\mathbb{R}$-espace-vectoriel. Un *espace hermitien* est alors un $\mathbb{C}$-espace-vectoriel (souvent de dimension finie) et muni d'un produit hermitien que l'on note dorénavant $\langle ., . \rangle$. On définit sa norme associée par : $\|x\| := \sqrt{\langle x, x \rangle}$, voir [3] pour les fondements.

Soit maintenant $V := \{F : \mathbb{Z}(n) \longmapsto \mathbb{C}\}$. C'est un espace hermitien, de dimension n, que l'on munit du produit hermitien défini par :

$$\langle F, G \rangle = \sum_{k=0}^{n-1} F(k)\, \overline{G(k)}.$$

Soient aussi, pour tout $l \in [\![0, n-1]\!]$, les fonctions définies par :

$$e_l(k) = \exp\left(\frac{2ikl\pi}{n}\right) = \zeta^{kl} \qquad (\forall\, k \in [\![0, n-1]\!]).$$

Proposition 2.2. *La famille* $\{e_0, \dots, e_{n-1}\}$ *est une base orthogonale de* V*. Plus précisément, on a :*

$$\langle e_m, e_l \rangle = n\,\delta_{m,l} \qquad (\forall\, m,l \in [\![0,n-1]\!]).$$

Il s'agit de l'équivalent pour $\mathbb{Z}(n)$ de $\left\{x \longmapsto \exp(2i\pi nx)\right\}_{n\in\mathbb{N}}$ pour le cercle.

Preuve. On a :

$$\langle e_m, e_l \rangle = \sum_{k=0}^{n-1} \zeta^{mk}\,\overline{\zeta^{lk}} = \sum_{k=0}^{n-1} \zeta^{(m-l)k},$$

donc si $m \neq l$, alors :

$$\langle e_m, e_l \rangle = \frac{1-(\zeta^{m-l})^n}{1-\zeta^{m-l}} = \frac{1-1}{1-\zeta^{m-l}} = 0,$$

et si $l = m$, alors :

$$\langle e_m, e_m \rangle = \sum_{k=0}^{n-1} 1 = n.$$

Ainsi $\langle e_m, e_l \rangle = n\,\delta_{m,l}$. De plus, $\operatorname{Card}\{e_0, \dots, e_{n-1}\} = n = \dim V$, donc cette famille forme bien une base orthogonale de V. □

On définit, pour tout $l \in [\![0, n-1]\!]$:

$$e_l^* := \frac{1}{\sqrt{n}}\, e_l.$$

Alors on a, pour tout $F \in V$:

$$F = \sum_{k=0}^{n-1} \langle F, e_k^* \rangle\, e_k^*,$$

et aussi :

$$\|F\|^2 = \sum_{k=0}^{n-1} |\langle F, e_k^* \rangle|^2.$$

On peut ainsi définir, pour $F \in V$, et $k \in [\![0, n-1]\!]$, le *k-ième coefficient de Fourier de* F par :

$$\begin{aligned} a_k(F) &= \frac{1}{n} \sum_{l=0}^{n-1} F(l) \exp\left(-\frac{2ikl\pi}{n}\right) \\ &= \frac{1}{n}\langle F, e_k \rangle = \frac{1}{\sqrt{n}}\langle F, e_k^* \rangle. \end{aligned}$$

Il en découle aisément le théorème fondamental suivant, qui fournit les formules d'inversion de Fourier et de Plancherel-Parseval sur $\mathbb{Z}(n)$.

Théorème 2.1. *Soient $F \in V$ et $l \in [\![0, n-1]\!]$. Alors :*

$$F(l) = \sum_{k=0}^{n-1} a_k(F) \exp\left(-\frac{2ikl\pi}{n}\right),$$

et aussi :

$$\sum_{k=0}^{n-1} |a_k(F)|^2 = \frac{1}{n} \sum_{k=0}^{n-1} |F(k)|^2. \qquad \square$$

2.2 Analyse de Fourier sur des groupes abéliens finis

On veut maintenant généraliser ce que l'on vient de faire à tous les groupes abéliens finis.

2.2.1 Le groupe $\mathbb{Z}^*(a)$

Cet exemple est crucial pour la preuve du théorème de Dirichlet. Soit $a \in \mathbb{N}^*$. On note $\mathbb{Z}^*(a)$ l'ensemble des inversibles (ou unités) de $\mathbb{Z}(a)$, vu comme $\mathbb{Z}/a\mathbb{Z}$. Alors $(\mathbb{Z}^*(a), \times)$ est un groupe abélien.

Exemple 2.1. On a : $\mathbb{Z}^*(4) = \{1, 3\}$. De plus, $\mathbb{Z}^*(4) \simeq \mathbb{Z}(2)$ via l'isomorphisme :

$$\begin{cases} (\mathbb{Z}^*(4), \times) & \longleftrightarrow & (\mathbb{Z}(2), +) \\ 1 & \longleftrightarrow & 0, \\ 3 & \longleftrightarrow & 2. \end{cases}$$

Exemple 2.2. On a : $\mathbb{Z}^*(8) = \{1, 3, 5, 7\}$. De plus, $\mathbb{Z}^*(8) \simeq \mathbb{Z}(2) \times \mathbb{Z}(2)$ via l'isomorphisme :

$$\begin{cases} (\mathbb{Z}^*(8), \times) & \longleftrightarrow & (\mathbb{Z}(2) \times \mathbb{Z}(2), +) \\ 1 & \longleftrightarrow & (0, 0), \\ 3 & \longleftrightarrow & (1, 0), \\ 5 & \longleftrightarrow & (0, 1), \\ 7 & \longleftrightarrow & (1, 1). \end{cases}$$

2.2.2 Caractères

Soit G un groupe abélien. Un *caractère* sur G est un morphisme de G vers $(\mathbb{S}^1, \times)$, où $\mathbb{S}^1$ est le cercle unité de $\mathbb{C}$.

Les caractères jouent un rôle crucial pour généraliser la théorie de Fourier aux groupes abéliens finis, puisqu'ils sont l'équivalent, ou l'analogue, des e_l pour $\mathbb{Z}(n)$. En fait, les e_l sont exactement les caractères sur $\mathbb{Z}(n)$.

On note $\widehat{G}$ l'ensemble des caractères sur G, et l'on remarque que $(\widehat{G}, \times)$ est un groupe abélien fini de neutre $\underline{1}$ (le caractère trivial : constant égal à 1).

Exemple 2.3. Voici quelques exemples classiques :

- L'ensemble des caractères de $\mathbb{Z}(n)$ est $\widehat{\mathbb{Z}(n)} = \{e_l\}_{0 \leqslant l \leqslant n-1}$. De plus, l'application $\widehat{\mathbb{Z}(n)} \ni e_l \longmapsto l \in \mathbb{Z}(n)$ est un isomorphisme.
- L'ensemble des caractères de $\mathbb{S}^1$ est $\widehat{\mathbb{S}^1} = \{e_n : z \longmapsto \exp(2i\pi nz)\}_{n\in\mathbb{Z}}$. De plus, l'application $\widehat{\mathbb{S}^1} \ni e_n \longmapsto n \in \mathbb{Z}$ est un isomorphisme.
- L'ensemble des caractères de $\mathbb{R}$ est $\widehat{\mathbb{R}} = \{e_\xi : x \longmapsto \exp(2i\pi x\xi)\}_{\xi\in\mathbb{R}}$. De plus, l'application $\widehat{\mathbb{R}} \ni e_\xi \longmapsto \xi \in \mathbb{R}$ est un isomorphisme.

Nous établissons maintenant un lemme qui sera utile plus tard :

Lemme 2.2. *Soient G un groupe abélien fini et $e : G \longrightarrow \mathbb{C}^*$ une fonction multiplicative i.e. :*

$$e(a \cdot b) = e(a) \times e(b) \qquad (\forall\, a, b \in G).$$

Alors e est un caractère.

Preuve. Il suffit de montrer que e est à valeurs dans $\mathbb{S}^1$. Soit $a \in G$. Comme e est multiplicative, et d'après le théorème de Lagrange, on a $e(a^n) = e(a)^n = e(1_G)$ avec $n = \mathrm{Card}(G)$.

Or, $e(1_G) = e(1_G \cdot 1_G) = e(1_G)^2$, et $e(1_G) \neq 0$ par hypothèse. On en déduit que $e(1_G) = 1$. Ainsi, $|e(a)|^n = 1$, donc $|e(a)| = 1$. □

L'étape suivante consiste à montrer que l'ensemble des caractères sur G forme une base de l'espace vecoriel V des fonctions $G \longrightarrow \mathbb{C}$. Ce résultat est immédiat dans le cas où $G = \mathbb{Z}(n)$, mais ne l'est pas dans le cas général.

2.2.3 Les caractères comme base de l'espace des fonctions complexes

Soit $V := \{f : G \longrightarrow \mathbb{C}\}$. Il s'agit d'un $\mathbb{C}$-espace-vectoriel de dimension $n := \mathrm{Card}(G)$. On le munit du produit hermitien défini par :

$$\langle F, G \rangle = \frac{1}{n} \sum_{a\in G} f(a)\, \overline{g(a)}.$$

Théorème 2.2. *Les caractères de G forment une famille orthonormée.*

Preuve. Soit $e \in \widehat{G}$. Alors :

$$\langle e, e\rangle = \frac{1}{n} \sum_{a\in G} e(a)\, \overline{e(a)} = \frac{1}{n} \sum_{a\in G} |e(a)|^2 = \frac{n}{n} = 1.$$

Il reste à montrer que si $e' \neq e$, alors $\langle e, e'\rangle = 0$. Pour cela, on utilise le lemme suivant :

Lemme 2.3. *Si $e \neq \underline{1}$, alors $\sum_{a\in G} e(a) = 0$.*

Preuve. Soit $b \in G$ tel que $e(b) \neq 1$ (qui existe par hypothèse). Alors comme $bG = G$, on a :

$$e(b) \sum_{a \in G} e(a) = \sum_{a \in G} e(ba) = \sum_{a \in G} e(a).$$

Puisque $e(b) \neq 1$, on obtient bien $\sum_{a \in G} e(a) = 0$. □

Revenons à la preuve du théorème. On a :

$$\langle e, e' \rangle = \frac{1}{n} \sum_{a \in G} e(a)\, \overline{e'(a)} = \frac{1}{n} \sum_{a \in G} e(a)(e'(a))^{-1}.$$

Or, comme $e' \neq e$, on a $ee'^{-1} \neq \underline{1}$. Le lemme montre alors que $\langle e, e' \rangle = 0$. □

Ainsi, $\widehat{G}$ forme une famille libre et orthonormée de V. En fait, il s'agit plus précisément une base orthonormée de V.

Théorème 2.3. *Les caractères d'un groupe abélien fini G forment une base orthonormée de l'espace des fonctions $G \longrightarrow \mathbb{C}$.*

Preuve. Il existe plusieurs preuves de ce théorème. L'une d'entre elles utilise le théorème de structure, vu en cours d'algèbre : un groupe abélien fini non vide est isomorphe à un produit de groupes cycliques de la forme $\mathbb{Z}(n)$. Puisque $\widehat{\mathbb{Z}(n)} \simeq \mathbb{Z}(n)$ (cf. Exemple 2.3) et que le groupe des caractères d'un produit est le produit des groupes de caractères, on obtient $\mathrm{Card}(\widehat{G}) = \mathrm{Card}(G) = \dim V$, ce qui conclut la preuve.

Nous allons cependant prouver le théorème sans utiliser ces résultats. Pour cela, nous utilisons le lemme suivant, qui est une extension du théorème spectral (tout endomorphisme unitaire, i.e. qui conserve le produit scalaire, est diagonalisable).

Lemme 2.4. *Soient $T_1, T_2, \ldots, T_k$ des endomorphismes unitaires, sur un espace vectoriel V, qui commutent deux à deux. Alors $T_1, T_2, \ldots, T_k$ sont codiagonalisables (i.e. diagonalisables dans la même base).*

Preuve. Le lemme se prouve par récurrence sur k, en appliquant le théorème spectral à T_k, puis en codiagonalisant $T_1, \ldots, T_{k-1}$ sur chaque sous-espace propre de T_k. Nous ne développons pas plus cette preuve. □

Nous pouvons maintenant terminer la preuve du Théorème 2.3. Pour tout $a \in G$, on définit :

$$T_a : \left\{ \begin{array}{ccc} V & \longrightarrow & V \\ f & \longmapsto & (x \longmapsto f(ax)). \end{array} \right.$$

Les n applications T_a sont linéaires, commutent deux à deux (car G est abélien) et l'on vérifie aisément qu'elles sont unitaires. Donc d'après le Lemme 2.4, les T_a sont codiagonalisables, et l'on note $(v_1, \ldots, v_n)$ une base de codiagonalisation. Donc :

$$\exists\, \lambda_{i,a} \in \mathbb{C} \colon T_a(v_i) = \lambda_{i,a} v_i \qquad (\forall\, i \in [\![0,n]\!], \forall\, a \in G).$$

Soit $i \in [\![0, n]\!]$. On a $v_i(1) \neq 0$, car sinon, pour tout $a \in G$, on aurait $v_i(a) = v_i(1 \times a) = T_a(v_i)(1) = \lambda_{i,a} v_i(1) = 0$ donc $v_i = \underline{0}$, ce qui est impossible car $(v_1, \dots v_n)$ est libre.

On peut donc définir la fonction :

$$w_i := \frac{v_i}{v_i(1)},$$

et l'on montre de même que w_i ne s'annule jamais. De plus, w_i est multiplicative. En effet, si $a, b \in G$, alors :

$$w_i(ab) = \frac{v_i(ab)}{v_i(1)} = \frac{T_a(v_i)(b)}{v_i(1)} = \frac{\lambda_{i,a} v_i(b)}{v_i(1)}.$$

Or, par définition :

$$\lambda_{i,a} = \frac{T_a(v_i)(1)}{v_i(1)} = \frac{v_i(a)}{v_i(1)},$$

donc $w_i(ab) = w_i(a) w_i(b)$.

Ainsi, d'après le Lemme 2.2, w_i est un caractère, et comme la famille $\{w_i\}_{1 \leqslant i \leqslant n}$ forme une base de V, le théorème est prouvé. □

En particulier, on obtient ainsi $\mathrm{Card}(\widehat{G}) = \dim V = \mathrm{Card}(G)$.

2.2.4 Inversion de Fourier et formule de Plancherel

On rassemble les résultats obtenus précédemment afin de définir les séries de Fourier sur les groupes abéliens finis.

Soient $f \in V = \{g : G \longrightarrow \mathbb{C}\}$ et $e \in \widehat{G}$. On définit le *coefficient de de Fourier de f par rapport à e* par :

$$\hat{f}(e) := \langle f, e \rangle = \frac{1}{n} \sum_{a \in G} f(a)\, \overline{e(a)},$$

et sa *série de Fourier* par :

$$\mathcal{F} f := \sum_{e \in \widehat{G}} \hat{f}(e)\, e.$$

Comme les caractères forment une base orthonormée de V, on obtient :

$$f = \sum_{e \in \widehat{G}} \langle f, e \rangle e = \mathcal{F} f.$$

Pour résumer :

Théorème 2.4. *Soit G un groupe abélien fini. Les caractères de G forment une base orthonormée de l'espace hermitien $V = \{f : G \longrightarrow \mathbb{C}\}$ muni du produit hermitien défini par :*

$$\langle f, g\rangle = \frac{1}{n}\sum_{a\in G} f(a)\,\overline{g(a)}.$$

En particulier, toute fonction de V est égale à sa transformée de Fourier :

$$f = \sum_{e\in\widehat{G}} \hat{f}(e)e$$

avec

$$\hat{f}(e) = \langle f, e\rangle \qquad (\forall\, f \in V).$$

Pour finir, voici la formule de Plancherel-Parseval pour les groupes abéliens finis :

Théorème 2.5.

$$\|f\|^2 := \sum_{e\in\widehat{G}} |\hat{f}(e)|^2.$$

Preuve. Il suffit d'écrire :

$$\|f\|^2 = \langle f, f\rangle = \langle \sum_{e\in\widehat{G}} \hat{f}(e)e, f\rangle = \sum_{e\in\widehat{G}} \hat{f}(e)\langle e, f\rangle = \sum_{e\in\widehat{G}} \hat{f}(e)\overline{\hat{f}(e)} = \sum_{e\in\widehat{G}} |\hat{f}(e)|^2.$$

□

3 La preuve du théorème de Dirichlet

Nous pouvons maintenant passer à la preuve du *théorème de la progression arithmétique* :

Si a et b sont premiers entre eux, alors il existe une infinité de nombres premiers congrus à $b \mod a$.

3.1 Quelques résultats utiles

Il s'agit ici d'énoncer quelques résultats d'arithmétique qui seront essentiels dans la preuve du théorème. La plupart de ces énoncés a déjà été vue en cours, notamment celui d'algèbre, et ne sera donc pas démontrée. Seuls les résultats dont la preuve est importante ou qui n'ont pas été vus en cours seront prouvés.

Théorème 3.1. *Soient $a, b \in \mathbb{Z}$ avec $b \neq 0$. Alors il existe un unique couple d'entiers (q, r) appelés respectivement quotient et reste tels que :*

$$a = bq + r$$

et avec :

$$0 \leqslant r < |b|.$$ □

Théorème 3.2. *Soient $a, b \in \mathbb{Z}$. Alors il existe $u, v \in \mathbb{Z}$ tels que :*

$$au + bv = \text{pgcd}(a, b).$$

De plus, a et b sont premiers entre eux si et seulement si il existe $u, v \in \mathbb{Z}$ tels que :

$$au + bv = 1. \qquad \square$$

Théorème 3.3. *Soient $a, b, c \in \mathbb{Z}$. Si $a \mid bc$ et si $\text{pgcd}(a, b) = 1$, alors $a \mid c$.* $\square$

Il en découle :

Lemme 3.1. *Si p est premier et si $p \mid a_1 a_2 \dots a_n$, alors $p \mid a_i$ pour un certain indice i.* $\square$

Théorème 3.4 (Théorème fondamental de l'arithmétique)**.** *Tout entier naturel non nul admet une factorisation en nombres premiers, unique à l'ordre des facteurs près.* $\square$

Théorème 3.5. *Il y a une infinité de nombres premiers.*

Nous allons prouver ce théorème, car le raisonnement utilisé nous sera essentiel pour la suite.

La preuve la plus classique se fait par l'absurde : on suppose qu'il y a un nombre fini de nombres premiers $p_1, \dots, p_n$ puis on construit un nombre premier qui n'est pas dans la liste $\{p_1, \dots, p_n\}$.

Il est intéressant de remarquer qu'un raisonnement similaire permet de montrer qu'il y a une infinité de nombres premiers congrus à $3 \mod 4$ (théorème de Dirichlet dans le cas où $a = 4$ et $b = 3$).

En effet, supposons qu'il y en a un nombre fini. On les numérote dans l'ordre croissant en excluant 3 :

$$p_1 = 7, p_2 = 11, \dots, p_n.$$

On considère alors :

$$N = 4p_1 p_2 \dots p_n + 3.$$

N est congru à $3 \mod 4$, mais n'est pas premier car $N > p_n$. De plus, l'un de ses facteurs premiers, noté p, doit être congru à $3 \mod 4$ puisque tous les nombres premiers, excepté 2, sont soit congrus à $1 \mod 4$ soit congrus à $3 \mod 4$, et le produit de deux nombres congrus à $1 \mod 4$ est congru à $1 \mod 4$. Or, $p \notin \{p_1, \dots, p_n\}$ car sinon on aurait $p \mid N - 4p_1 \dots p_n = 3$ donc $p = 3$, mais $3 \nmid N$. Donc ceci contredit l'hypothèse que $3, p_1, \dots, p_n$ sont les seuls nombres premiers congrus à $3 \mod 4$. Il y en a donc une infinité.

Cependant, un tel argument ne permet pas de montrer qu'il y a un nombre infini d'entiers premiers congrus à $1 \mod 4$.

Revenons au Théorème 3.5. Nous allons le prouver en montrant le lemme suivant qui donne immédiatement le résultat, et qui nous sera également utile dans la suite.

Lemme 3.2. *La série $\sum_{p\in\mathcal{P}} 1/p$ diverge.*

Preuve. On procède par l'absurde : supposons que cette série converge. Alors il existe $k \in \mathbb{N}$ tel que :

$$\sum_{n=k+1}^{\infty} \frac{1}{p_n} < \frac{1}{2}$$

lorsque l'on numérote les nombres premiers par ordre croissant : $\mathcal{P} = \{p_0, p_2, \ldots\}$.

On pose alors $Q = p_0 p_1 \ldots p_k$. Soit $n \in \mathbb{N}^*$. Alors $1 + nQ$ a ses facteurs premiers parmi $\{p_{k+1}, p_{k+2}, \ldots\}$, car si $i \leqslant k$ alors p_i ne divise pas $1+nQ$, sinon il diviserait $1 = 1 + nQ - nQ$.

Donc, pour pour tout $r \geqslant 1$, on a :

$$\sum_{n=1}^{r} \frac{1}{1+nQ} \leqslant \sum_{t=1}^{\infty} \left(\sum_{n=k+1}^{\infty} \frac{1}{p_n} \right)^t,$$

car chaque terme de la somme de droite apparaît dans la somme de gauche par unicité de la décomposition en facteurs premiers et par développement multinomial. Or, $\sum_{n=k+1}^{\infty} 1/p_n < 1/2$ et $\sum_{t\geqslant 1} 1/2^t$ converge, donc :

$$\limsup_r \sum_{n=1}^{r} \frac{1}{1+nQ} < \infty.$$

Mais cela est faux car $\sum_{n\geqslant 1} 1/(1+nQ)$ diverge, puisque $1/(1+nQ) \sim 1/nQ$ et $\sum_{n\geqslant 1} 1/n$ diverge. Il s'agit d'une contradiction, donc l'hypothèse de départ est fausse, d'où $\sum_{p\in\mathcal{P}} 1/p$ diverge. □

Nous allons maintenant nous intéresser à la fonction zêta de Riemann et à son produit d'Euler. Pour commencer, voici quelques rappels sur les produits infinis.

Soit $(A_n)_{n\in\mathbb{N}}$ une suite réelle. On définit alors :

$$\prod_{n=0}^{\infty} A_n := \lim_{N\to\infty} \prod_{n=0}^{N} A_n$$

lorsque la limite existe. Pour étudier les produits infinis, il est naturel d'utiliser le logarithme afin de transformer des produits en sommes. Le lemme suivant nous sera donc utile.

Lemme 3.3. *Le logarithme satisfait les propriétés suivantes pour tout $x > 0$:*

1. $\exp(\log(x)) = x$;
2. *Si* $|x| < 1/2$, *alors* $\log(1+x) = x + E(x)$ *où* $|E(x)| \leqslant x^2$;
3. *Si* $|x| < 1/2$, *alors* $|\log(1+x)| \leqslant 2|x|$. □

Il en découle le résultat suivant :

Proposition 3.1. *Si $A_n = 1 + a_n$ et si $\sum_{n\in\mathbb{N}} |a_n|$ converge, alors $\prod_{n\in\mathbb{N}} A_n$ converge.*

De plus, si $a_n \neq 1$ pour tout n, alors $\prod_{n\in\mathbb{N}} 1/(1-a_n)$ converge.

Preuve. L'énoncé se montre en passant au logarithme puis en utilisant le lemme précédent. Nous ne développons pas plus cette preuve. □

Nous pouvons maintenant introduire la *fonction zêta*, définie pour tout $s > 1$ par :

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

On peut montrer que ζ est bien définie en la comparant avec des intégrales, mais nous ne le ferons pas ici. De plus, $\sum 1/n^s$ est uniformément convergente sur chaque intervalle de la forme $[s_0, +\infty[$ pour $s_0 > 1$, donc ζ est continue sur $]1, +\infty[$.

Le résultat suivant est une formule clé :

Théorème 3.6.

$$\zeta(s) = \prod_{p\in\mathcal{P}} \frac{1}{1-\frac{1}{p^s}} \qquad (\forall\, s > 1).$$

Preuve. Soit $N \in \mathbb{N}$. Pour M suffisamment grand, par unicité de la décomposition en facteurs premiers, on a :

$$\begin{aligned}
\sum_{n=1}^{N} \frac{1}{n^s} &\leqslant \prod_{\substack{p\in\mathcal{P}\\ p\leqslant N}} \left(1 + \frac{1}{p^s} + \frac{1}{p^{2s}} + \ldots + \frac{1}{p^{Ms}}\right) \\
&\leqslant \prod_{\substack{p\in\mathcal{P}\\ p\leqslant N}} \sum_{k=0}^{\infty} \left(\frac{1}{p^s}\right)^k = \prod_{\substack{p\in\mathcal{P}\\ p\leqslant N}} \frac{1}{1-\frac{1}{p^s}} \\
&\leqslant \prod_{p\in\mathcal{P}} \frac{1}{1-\frac{1}{p^s}}.
\end{aligned}$$

Donc, lorsque $N \to +\infty$, on obtient :

$$\zeta(s) \leqslant \prod_{p\in\mathcal{P}} \frac{1}{1-\frac{1}{p^s}}.$$

De même, si $M \in \mathbb{N}$, par le théorème fondamental de l'arithmétique, on a :

$$\prod_{\substack{p\in\mathcal{P}\\ p\leqslant N}} \left(1 + \frac{1}{p^s} + \frac{1}{p^{2s}} + \ldots + \frac{1}{p^{Ms}}\right) \leqslant \zeta(s).$$

Alors on obtient :

$$\prod_{p\in\mathcal{P}} \frac{1}{1-\frac{1}{p^s}} \leqslant \zeta(s).$$

□

3.2 Le théorème de Dirichlet

On rappelle que l'on veut montrer que si a et b sont premiers entre eux, alors il existe une infinité de nombres premiers congrus à $b \mod a$. Dirichlet prouva ce théorème en montrant la divergence de la série :

$$\sum_{\substack{p\in\mathcal{P}\\ p\equiv b[a]}} \frac{1}{p}.$$

Dans le suite, la lettre p désignera toujours un nombre premier, et l'on omettra alors de noter « $p \in \mathcal{P}$ ».

Avant de faire la preuve dans le cas général, revenons au cas où $a = 4$ et $b = 1$, qui illustre parfaitement le raisonnement général.

Soit χ le caractère sur $\mathbb{Z}^*(4)$ défini par $\chi(1) = 1$ et $\chi(3) = -1$. On l'étend sur $\mathbb{Z}$ tout entier par :

$$\chi(n) : \begin{cases} 0 & \text{si } n \text{ est pair,} \\ 1 & \text{si } n \equiv 1[4], \\ -1 & \text{si } n = 3[4]. \end{cases}$$

On remarque que χ est une fonction multiplicative sur $\mathbb{Z}$ entier. On définit alors, pour $s > 1$:

$$L(s,\chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s} = 1 - \frac{1}{3^s} + \frac{1}{5^s} - \frac{1}{7^s} + \dots$$

Alors on remarque que $L(1,\chi)$ est également bien définie comme série alternée de terme général tendant vers 0. On a :

$$L(1,\chi) = 1 - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} + \dots$$

et $L(1,\chi) \neq 0$. De plus, comme χ est multiplicative, on a la formule suivante, qui est la généralisation du Théorème 3.6, que nous prouverons dans la suite :

$$L(s,\chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s} = \prod_p \frac{1}{1 - \frac{\chi(p)}{p^s}} \qquad (\forall\, s > 1).$$

En passant au logarithme , on obtient :

$$\log L(s,\chi) = \sum_p \frac{\chi(p)}{p^s} + \mathrm{O}(1).$$

Donc, lorsque $s \to 1^+$, et comme $L(1,\chi) \neq 0$, on en déduit que :

$$\sum_{p\equiv 1[4]} \frac{1}{p^s} - \sum_{p\equiv 3[4]} \frac{1}{p^s}$$

est bornée près de 1. Or, $\sum_p 1/p^s$ diverge lorsque $s \to 1^+$, donc :

$$\sum_p \frac{1}{p^s} + \sum_{p\equiv 1[4]} \frac{1}{p^s} - \sum_{p\equiv 3[4]} \frac{1}{p^s} = 2\sum_{p\equiv 1[4]} \frac{1}{p^s}$$

diverge lorsque $s \to 1^+$. Ainsi,

$$\sum_{p\equiv 1[4]} \frac{1}{p}$$

diverge, ce qui prouve bien qu'il y a une infinité de nombres premiers congrus à 1 mod 4.

3.2.1 Analyse de Fourier, caractères de Dirichlet et simplification du problème

Soit $G := \mathbb{Z}^*(a)$. Le cardinal de G est le nombre d'entiers naturels plus petits que a qui sont premiers avec a. Ceci définit l'*indicatrice d'Euler*, notée φ. On a donc $\mathrm{Card}(G) = \varphi(a)$.

Soit δ_b la *fonction caractéristique de* $b \mod a$ définie par :

$$\delta_b : \begin{cases} G & \longrightarrow & \mathbb{C} \\ n & \longmapsto & \begin{cases} 1 & \text{si } n \equiv b\,[a], \\ 0 & \text{sinon.} \end{cases} \end{cases}$$

Alors, d'après le Théorème 2.4, on a :

$$\delta_b = \sum_{e\in\widehat{G}} \widehat{\delta_b}(e)\, e,$$

où $\widehat{\delta_b}(e) = \frac{1}{\mathrm{Card}(G)} \sum_{m\in G} \delta_b(m)\,\overline{e(m)} = \frac{1}{\varphi(a)}\,\overline{e(b)}$. Donc :

$$\delta_b = \frac{1}{\varphi(a)} \sum_{e\in\widehat{G}} \overline{e(b)}\, e.$$

On peut étendre δ_b à $\mathbb{Z}$ en posant $\delta_b(m) = 0$ si $\mathrm{pgcd}(a, m) \neq 1$. De la même manière, on peut étendre un caractère $e \in \widehat{G}$ à $\mathbb{Z}$ en posant :

$$\chi(m) = \begin{cases} e(m \mod a) & \text{si } \mathrm{pgcd}(a, m) = 1, \\ 0 & \text{sinon.} \end{cases}$$

Ces fonctions s'appellent les *caractères de Dirichlet modulo* a. Dans la suite, comme a est fixé, on écrira plus simplement « caractères de Dirichlet ». On note χ_0 l'extension à $\mathbb{Z}$ du caractère trivial, et ainsi, on a $\chi_0(m) = 1$ si $\mathrm{pgcd}(a, m) = 1$ et 0 sinon. On remarque que les caractères de Dirichlet sont multiplicatifs sur tout $\mathbb{Z}$. On peut alors résumer ces résultats avec le lemme suivant :

Lemme 3.4. *Les caractères de Dirichlet sont multiplicatifs sur $\mathbb{Z}$. De plus :*

$$\delta_b(m) = \frac{1}{\varphi(a)} \sum_{\chi} \overline{\chi(b)}\, \chi(m) \qquad (\forall\, m \in \mathbb{Z}),$$

où la somme porte sur tous les caractères de Dirichlet. □

Grâce à ce lemme, on obtient :

$$\sum_{p \equiv b[a]} \frac{1}{p^s} = \sum_{p} \frac{\delta_b(p)}{p^s} = \frac{1}{\varphi(a)} \sum_{\chi} \overline{\chi(b)} \sum_{p} \frac{\chi(p)}{p^s}.$$

Ainsi, il suffit de connaître le comportement de $\sum_p \chi(p)/p^s$ lorsque $s \to 1^+$. En fait, on peut différencier le cas $\chi = \chi_0$ du cas $\chi \neq \chi_0$. On a alors :

$$\begin{aligned}\sum_{p \equiv b[a]} \frac{1}{p^s} &= \frac{1}{\varphi(a)} \sum_{p} \frac{\chi_0(p)}{p^s} + \frac{1}{\varphi(a)} \sum_{\chi \neq \chi_0} \overline{\chi(b)} \sum_{p} \frac{\chi(p)}{p^s} \\ &= \frac{1}{\varphi(a)} \sum_{p \nmid a} \frac{1}{p^s} + \frac{1}{\varphi(a)} \sum_{\chi \neq \chi_0} \overline{\chi(b)} \sum_{p} \frac{\chi(p)}{p^s}.\end{aligned}$$

En effet, $\chi_0(p) = 1$ si et seulement si $\operatorname{pgcd}(a, p) = 1$, c'est-à-dire si et seulement si $p \nmid a$. Or, il n'y a qu'un nombre fini d'entiers premiers qui ne divisent pas a, donc la somme de gauche a le même comportement que $\sum_p 1/p^s$ lorsque $s \to 1^+$, donc elle diverge d'après le Lemme 3.2. Ainsi, cela montre qu'il suffit d'établir le théorème suivant pour conclure la preuve.

Théorème 3.7. *Si $\chi \neq \chi_0$, alors $\sum_p \chi(p)/p^s$ reste bornée lorsque $s \to 1^+$.*

Pour prouver ce résultat, nous allons introduire les fonctions L. On a prouvé le Théorème 3.6 qui affirme que :

$$\zeta(s) = \sum_{n=0}^{\infty} \frac{1}{n} = \prod_{p \in \mathcal{P}} \frac{1}{1 - \frac{1}{p^s}} \qquad (\forall\, s > 1).$$

En fait, Dirichlet observa une formule analogue pour ce que l'on appelle les *fonctions L* définies, pour $s > 1$ et χ un caractère de Dirichlet, par :

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

Théorème 3.8. *Pour $s > 1$, on a :*

$$L(s, \chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s} = \prod_{p} \frac{1}{1 - \frac{\chi(p)}{p^s}}.$$

En admettant ce théorème pour l'instant, en prenant le logarithme, on obtient :

$$\begin{aligned}\log L(s,\chi) &= -\sum_p \log\left(1-\frac{\chi(p)}{p^s}\right)\\ &= -\sum_p \left(-\frac{\chi(p)}{p^s}+\mathrm{O}\left(\frac{1}{p^{2s}}\right)\right)\\ &= \sum_p \frac{\chi(p)}{p^s}+\mathrm{O}(1).\end{aligned}$$

Si $L(1,\chi)$ est fini et non nul, alors $\log L(s,\chi)$ est borné lorsque $s\to 1^+$ et l'on en déduit que $\sum_p \chi(p)/p^s$ l'est.

Il reste alors à :

- Prouver le Théorème 3.8, ce qui nécessitera l'utilisation du logarithme complexe ;
- Justifier le passage au logarithme de la formule ;
- Montrer que $L(s,\chi)$ est fini et non nul lorsque $\chi\neq\chi_0$, ce qui suffit car nous verrons que $L(s,\chi)$ est continue lorsque $s\to 1^+$.

3.2.2 Logarithmes

Afin de prouver le Théorème 3.8, nous allons définir deux logarithmes : l'un pour les nombres complexes de la forme $1/(1-z)$ avec $|z|<1$, et l'autre pour les fonctions L.

On définit, pour tout $z\in\mathbb{C}$ tel que $|z|<1$:

$$\log_{(1)}\left(\frac{1}{1-z}\right)=\sum_{k=1}^{\infty}\frac{z^k}{k}.$$

On note que $\log_{(1)}(w)$ est défini si $\Re(w)>1/2$, et d'après le développement en série entière de $\log(1+x)$ avec $x\in\,]-1,1[$, $\log_{(1)}$ est une extension du logarithme réel $\log(x)$ quand $x>1/2$.

Proposition 3.2. *La fonction* $\log_{(1)}$ *satisfait pour tout* $z\in\mathbb{C}$ *:*

1. *Si* $|z|<1$*, alors :*

$$\exp\left(\log_{(1)}\left(\frac{1}{1-z}\right)\right)=\frac{1}{1-z}.$$

2. *Si* $|z|<1$*, alors :*

$$\log_{(1)}\left(\frac{1}{1-z}\right)=z+E_1(z),$$

avec $|E_1(z)|\leqslant|z|^2$ *si* $|z|<1/2$.

3. Si $|z| < 1/2$, alors :

$$\left|\log_{(1)}\left(\frac{1}{1-z}\right)\right| \leqslant 2|z|.$$

Preuve. Pour (1), il suffit d'écrire $z = re^{i\theta}$ avec $0 \leqslant r < 1$, puis de dériver par rapport à r l'expression :

$$(1 - re^{i\theta}) \exp\left(\sum_{k=0}^{\infty} \frac{(re^{i\theta})^k}{k}\right).$$

Nous ne développons pas plus la preuve. Les assertions (2) et (3) sont conséquence de (1). □

On peut en déduire le résultat suivant sur les produits infinis :

Proposition 3.3. *Soit $(a_n)_{n\in\mathbb{N}} \subset \mathbb{C}$. Si $\sum_{n\in\mathbb{N}} a_n$ converge et $a_n \neq 1$ pour tout $n \in \mathbb{N}$, alors le produit :*

$$\prod_{n\in\mathbb{N}} \frac{1}{1-a_n}$$

converge et est non nul.

Preuve. Il suffit de regarder :

$$\log_{(1)}\left(\prod_{n\in\mathbb{N}} \frac{1}{1-a_n}\right),$$

et d'utiliser la proposition précédente. □

Nous pouvons maintenant prouver le Théorème 3.8 qui affirme :

$$L(s,\chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s} = \prod_{p} \frac{1}{1 - \frac{\chi(p)}{p^s}}.$$

Preuve. On note Π le membre de droite, et l'on définit pour tout $N \in \mathbb{N}^*$:

$$S_N = \sum_{n\leqslant N} \frac{\chi(n)}{n^s},$$

ainsi que :

$$\Pi_N = \prod_{p\leqslant N} \frac{1}{1 - \frac{\chi(p)}{p^s}}.$$

Le produit $\Pi = \lim_{n\to\infty} \Pi_N$ converge d'après la proposition précédente. En effet, en posant $a_n = \chi(p_n)/{p_n}^s$, où p_n désigne le n-ième nombre premier, alors comme $s > 1$, $\sum_{n\in\mathbb{N}} a_n$ converge.

On définit également, pour tous $N \in \mathbb{N}^*$ et $M \in \mathbb{N}$:

$$\Pi_{N,M} = \prod_{p \leqslant N} \left(1 + \frac{\chi(p)}{p^s} + \ldots + \frac{\chi(p^M)}{p^{Ms}}\right).$$

Soit $\varepsilon > 0$. Alors pour N assez grand, on a de manière évidente :

$$|S_N - L(s,\chi)| < \varepsilon,$$

ainsi que :

$$|\Pi_N - \Pi| < \varepsilon.$$

De plus, pour M et N suffisamment grands, on a également :

$$|S_N - \Pi_{N,M}| < \varepsilon,$$

et aussi :

$$|\Pi_{N,M} - \Pi_N| < \varepsilon.$$

En effet, par le théorème fondamental de l'arithmétique, et comme les caractères sont multiplicatifs, pour M assez grand, tous les termes de S_N sont annulés par $\Pi_{N,M}$. Il ne reste alors qu'un somme de termes de la forme $\chi(p^k)/p^{ks}$ où $p^k \geqslant N+1$. On peut alors majorer cette somme par un reste de $\sum 1/n^s$ qui est donc plus petit que ε pour N assez grand, d'où $|S_N - \Pi_{N,M}| < \varepsilon$. L'inégalité $|\Pi_{N,M} - \Pi_N| < \varepsilon$ vient du fait que chaque série $\sum_n \chi(p^n)/p^{ns}$ converge.

Ainsi, par inégalité triangulaire, on obtient :

$$|L(s,\chi) - \Pi| \leqslant |L(s,\chi) - S_N| + |S_N - \Pi_{N,M}| + |\Pi_{N,M} - \Pi_N| + |\Pi_N - \Pi| < 4\varepsilon,$$

d'où le résultat. □

3.2.3 Étude des fonctions L

Il s'agit maintenant d'étudier le comportement des fonctions L, en particulier lorsque $s \to 1^+$. En réalité, celui-ci dépend de si oui ou non χ est trivial.

Dans le cas où $\chi = \chi_0$, on a le résultat suivant :

Proposition 3.4. *Soit χ_0 le caractère de Dirichlet trivial, i.e. :*

$$\chi_0(n) = \begin{cases} 1 & \textit{si } \operatorname{pgcd}(a,n) = 1, \\ 0 & \textit{sinon}, \end{cases} \qquad (\forall\, n \in \mathbb{Z}).$$

Soit $a = {p_1}^{\alpha_1} {p_2}^{\alpha_2} \ldots {p_n}^{\alpha_n}$ la décomposition en facteurs premiers de a. Alors :

$$L(s,\chi_0) = \left(1 - \frac{1}{{p_1}^s}\right)\left(1 - \frac{1}{{p_2}^s}\right)\ldots\left(1 - \frac{1}{{p_n}^s}\right)\zeta(s).$$

Par conséquent, $\lim_{s \to 1^+} L(s,\chi_0) = +\infty$.

Preuve. Il suffit de remarquer que si $p \in \mathcal{P}$, alors :

$$\left(1 - \frac{1}{p^s}\right)\zeta(s) = \sum_{p \nmid n} \frac{1}{n^s} = \sum_{\mathrm{pgcd}(p,n)=1} \frac{1}{n^s}.$$

On applique ceci successivement à $p_1, \ldots, p_n$, puis on utilise la divergence de $\zeta(s)$ lorsque $s \to 1^+$. □

Lorsque $\chi \neq \chi_0$, le comportement de $L(s,\chi)$ est moins évident, mais satisfait tout de même des propriétés remarquables.

Proposition 3.5. *Si $\chi \neq \chi_0$, alors la série :*

$$\sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}$$

converge pour $s > 0$ et l'on note cette somme $L(s,\chi)$.

De plus, la fonction L ainsi définie satisfait les propriétés suivantes :

1. *La fonction $L(\cdot,\chi)$ est continûment dérivable sur $]0,+\infty[$.*
2. *Il existe $c, c' > 0$ tels que :*

$$L(s,\chi) \overset{+\infty}{=} 1 + \mathrm{O}(e^{-cs}),$$

ainsi que :

$$L'(s,\chi) \overset{+\infty}{=} \mathrm{O}(e^{-c's}).$$

Preuve. Pour prouver cette proposition, nous allons utiliser le lemme suivant :

Lemme 3.5. *Si $\chi \neq \chi_0$, alors on a :*

$$\left|\sum_{k=1}^{k} \chi(n)\right| \leqslant a \qquad (\forall\, k \in \mathbb{N}^*).$$

Preuve. Tout d'abord, on a d'après le Lemme 2.3 page 11 :

$$\sum_{n=1}^{a} \chi(n) = 0,$$

On écrit ensuite la division de k par a : $k = aq + r$ avec $0 \leqslant r < a$. Ainsi :

$$\begin{aligned}\sum_{n=1}^{k} \chi(n) &= \sum_{n=1}^{a} \chi(n) + \sum_{n=a+1}^{2a} \chi(n) + \ldots + \sum_{n=(q-1)a+1}^{qa} \chi(n) + \sum_{n=qa}^{aq+r} \chi(n) \\ &= 0 + 0 + \ldots + 0 + \sum_{n=qa}^{aq+r} \chi(n).\end{aligned}$$

Donc puisque $r < a$ et $|\chi(n)| \leqslant 1$, on obtient bien le résultat. □

Nous pouvons donc prouver la proposition. On pose $s_0 = 0$ et :

$$s_N := \sum_{n=1}^{N} \chi(n)$$

pour tout entier $N \geqslant 1$.

On sait que $L(s,\chi)$ est définie pour $s > 1$ par la série $\sum_{n=1}^{\infty} \chi(n)/n^s$ qui converge absolument et uniformément sur $]\delta, +\infty[$ pour tout $\delta > 1$. Il en est de même pour la série dérivée terme à terme. Donc $L(\cdot,\chi)$ est continûment dérivable sur $]1, +\infty[$.

Pour étendre ce résultat à $]0, +\infty[$, on fait la transformation d'Abel suivante :

$$\sum_{n=1}^{N} \frac{\chi(n)}{n^s} = \sum_{n=1}^{N} \frac{s_n - s_{n-1}}{n^s} = \sum_{n=1}^{N-1} s_n \left(\frac{1}{n^s} - \frac{1}{(n+1)^s} \right) + \frac{s_N}{N^s}.$$

Puis, en appliquant l'inégalité des accroissements finis à $x \longmapsto x^{-s}$ entre n et $n+1$ ainsi que le lemme précédent, on obtient :

$$\left| s_n \left(\frac{1}{n^s} - \frac{1}{(n+1)^s} \right) \right| \leqslant asn^{-s-1}.$$

Ainsi, $\sum s_n(1/n^s - 1/(n+1)^s)$ converge uniformément sur $]0, +\infty[$. Donc $L(\cdot,\chi)$ est continue sur $]0, +\infty[$.

Pour prouver que $L(\cdot,\chi)$ est continûment dérivable, il suffit de dériver terme à terme, et les mêmes arguments montrent le résultat.

Ensuite, on observe que :

$$|L(s,\chi) - 1| = \left| \sum_{n=2}^{\infty} \frac{\chi(n)}{n^s} \right| \leqslant \sum_{n=2}^{\infty} \frac{1}{n^s} = 2^{-s} \sum_{n=2}^{\infty} \left(\frac{2}{n} \right)^s \leqslant 2^{-s} \sum_{n=2}^{\infty} \frac{2^2}{n^2}$$

pour s assez grand. Étant donné que $\sum 2^2/n^2 = \mathrm{O}(1)$, pour $c = \log(2)$, on obtient bien $L(s,\chi) \overset{+\infty}{=} 1 + \mathrm{O}(e^{-cs})$. On procède de même pour montrer que $L'(s,\chi) \overset{+\infty}{=} \mathrm{O}(e^{-c's})$. □

Comme $L(t,\chi) \neq 0$ pour tout $t > 1$ d'après le Théorème 3.8 et la Proposition 3.3, et comme $L'(t,\chi)/L(t,\chi) = \mathrm{O}(e^{-ct})$ d'après ce qui précède, nous sommes maintenant en mesure de définir un logarithme pour les fonctions L. Soient $\chi \neq \chi_0$ et $s > 1$. On définit :

$$\log_{(2)} L(s,\chi) := -\int_s^{\infty} \frac{L'(t,\chi)}{L(t,\chi)} dt.$$

Attention : la notation $\log_{(2)}$ ne doit pas être confondue avec celle du logarithme en base 2, notée $\log_2$!

Proposition 3.6. *Pour $\chi \neq \chi_0$ et $s > 1$, $\log_{(2)} L(s,\chi)$ satisfait :*

$$\exp(\log_{(2)} L(s,\chi)) = L(s,\chi),$$

ainsi que :

$$\log_{(2)} L(s,\chi) = \sum_p \log_{(1)} \left(\frac{1}{1 - \frac{\chi(p)}{p^s}} \right).$$

Preuve. Pour la première égalité, il suffit de dériver $\exp(-\log_{(2)} L(s,\chi))L(s,\chi)$ par rapport à s. Pour la seconde, il suffit de regarder l'exponentielle de chaque membre. □

On peut maintenant justifier le passage au logarithme de la page 18. En effet, d'après les propriétés de $\log_{(1)}$, on a :

$$\sum_p \log_{(1)} \left(\frac{1}{1 - \frac{\chi(p)}{p^s}} \right) = \sum_p \frac{\chi(p)}{p^s} + \mathrm{O}\left(\sum_p \frac{1}{p^{2s}} \right) = \sum_p \frac{\chi(p)}{p^s} + \mathrm{O}(1).$$

Donc si $L(1,\chi) \neq 0$ lorsque $\chi \neq \chi_0$, alors $\log_{(2)} L(s,\chi)$ reste borné lorsque $s \to 1^+$. Ainsi, d'après la relation entre les deux logarithmes, on déduit que $\sum_p \chi(p)/p^s$ l'est également, ce qui est le résultat souhaité. Il reste donc à montrer que $L(1,\chi) \neq 0$ pour $\chi \neq \chi_0$.

3.2.4 Non nullité de $L(1,\chi)$

Nous allons maintenant prouver le résultat crucial suivant :

Théorème 3.9. *Si $\chi \neq \chi_0$, alors $L(1,\chi) \neq 0$.*

Preuve. Nous allons prouver ce théorème en distinguant deux cas : les caractères réels et les caractères complexes.

Le cas des caractères complexes

Il s'agit du cas le plus facile. On procède par l'absurde en utilisant deux lemmes.

Lemme 3.6. *Si $s > 1$, alors :*

$$\prod_\chi L(s,\chi) \geqslant 1,$$

où le produit porte sur l'ensemble des caractères de Dirichlet. En particulier, ce produit est réel.

Preuve. D'après la Proposition 3.6, pour tout $s > 1$, on a :

$$L(s,\chi) = \exp\left(\sum_p \log_{(1)} \left(\frac{1}{1 - \frac{\chi(p)}{p^s}} \right) \right).$$

De plus, comme les caractères sont multiplicatifs, on en déduit :

$$\begin{aligned}\prod_{\chi} L(s,\chi) &= \exp\left(\sum_{\chi}\sum_{p} \log_{(1)}\left(\frac{1}{1-\frac{\chi(p)}{p^s}}\right)\right)\\ &= \exp\left(\sum_{\chi}\sum_{p}\sum_{k=1}^{\infty}\frac{\chi(p)^k}{kp^{ks}}\right)\\ &= \exp\left(\sum_{p}\sum_{k=1}^{\infty}\sum_{\chi}\frac{\chi(p^k)}{kp^{ks}}\right).\end{aligned}$$

Or, en appliquant le Lemme 3.4 page 20 avec $b = 1$, on obtient :

$$\sum_{\chi}\chi(p^k) = \varphi(a)\delta_1(p^k).$$

Donc comme $\delta_1 \geqslant 0$, on en déduit :

$$\prod_{\chi} L(s,\chi) = \exp\left(\varphi(a)\sum_{p}\sum_{k=1}^{\infty}\frac{\delta_1(p^k)}{kp^{ks}}\right) \geqslant 1.$$

□

Lemme 3.7. *Les fonctions L satisfont les propriétés suivantes :*

1. *Si $L(1,\chi) = 0$, alors $L(1,\overline{\chi}) = 0$.*
2. *Si $\chi \neq \chi_0$ et si $L(1,\chi) = 0$, alors pour tout $s \in [1,2]$:*
$$|L(s,\chi)| \leqslant C|s-1|.$$
3. *Pour tout $s \in]1,2]$:*
$$|L(s,\chi_0)| \leqslant \frac{C}{|s-1|}.$$

Preuve. 1. C'est immédiat car $L(1,\overline{\chi}) = \overline{L(1,\chi)}$.

2. Il s'agit de l'inégalité des accroissements finis puisque $L(\cdot,\chi)$ est continûment dérivable sur $]0,+\infty[$ lorsque $\chi \neq \chi_0$.

3. D'après la Proposition 3.4 on a :
$$L(s,\chi_0) = \left(1-\frac{1}{{p_1}^s}\right)\left(1-\frac{1}{{p_2}^s}\right)\ldots\left(1-\frac{1}{{p_n}^s}\right)\zeta(s).$$
De plus, $\zeta(s)$ satisfait une inégalité similaire à (3) obtenue en la comparant avec l'intégrale de $t \longmapsto t^{-s}$.

□

Maintenant, supposons que $L(1,\chi)=0$ pour un caractère complexe $\chi \neq \chi_0$. Alors $L(1,\overline{\chi})=0$. Comme $\overline{\chi} \neq \chi$ puisque χ est complexe, le produit $\prod_{\chi'} L(s,\chi')$ comprend au moins deux termes qui se comportent au plus comme $|s-1|$ lorsque $s \to 1^+$. Puisque seul le terme en χ_0 diverge comme $1/|s-1|$, on en déduit que le produit tend vers 0 lorsque $s \to 1^+$, ce qui est absurde car le Lemme 3.6 affirme qu'il est plus grand que 1, d'où $L(s,\chi) \neq 0$.

Le cas des caractères réels

On commence par comparer des sommes avec l'intégrale correspondante.

Proposition 3.7. *Soit $n \in \mathbb{N}$, alors :*

$$\sum_{k=1}^{n} \frac{1}{k} = \int_1^n \frac{\mathrm{d}x}{x} + \mathrm{O}(1) = \log(n) + \mathrm{O}(1).$$

Plus précisément, il existe une constante γ appelée constante d'Euler, telle que :

$$\sum_{k=1}^{n} \frac{1}{k} = \log(n) + \gamma + \mathrm{O}\left(\frac{1}{n}\right).$$

Preuve. Il suffit de prouver la seconde partie, qui se fait en posant :

$$\gamma_k := \frac{1}{k} - \int_k^{k+1} \frac{\mathrm{d}x}{x}$$

puis en sommant. Nous ne nous attardons pas plus sur cette preuve. □

Proposition 3.8. *Soit $n \in \mathbb{N}$. Alors :*

$$\sum_{k=1}^{n} \frac{1}{\sqrt{k}} = 2\sqrt{n} + c + \mathrm{O}\left(\frac{1}{\sqrt{n}}\right).$$

Preuve. Il s'agit du même principe que pour la proposition précédente. □

Soient $F\colon \mathbb{N}^* \times \mathbb{N}^* \longrightarrow \mathbb{R}$ et $N \in \mathbb{N}^*$. On peut calculer la somme :

$$S_N := \sum_{mn \leqslant N} F(m,n)$$

grâce à ces trois méthodes de sommation :

a) le long des hyperboles :

$$S_N = \sum_{k=1}^{N} \left(\sum_{mn=k} F(m,n) \right);$$

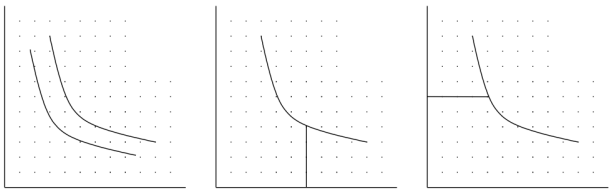
b) verticalement :

$$S_N = \sum_{m=1}^{N} \left(\sum_{n=1}^{N/m} F(m,n) \right);$$

c) horizontalement :

$$S_N = \sum_{n=1}^{N} \left(\sum_{m=1}^{N/n} F(m,n) \right).$$

La figure suivante illustre ces trois méthodes de sommation :



Nous voulons sommer selon tous les points situés en-dessous de la courbe d'équation $nm = N$ (il s'agit de l'hyperbole que l'on retrouve sur chaque graphe). Dans la méthode (a), on somme selon les hyperboles d'équation $nm = k$, dans la méthode (b), selon les droites verticales d'équation $m = k$, et dans la méthode (c), selon les droites horizontales d'équation $n = k$, et ce pour tout $1 \leqslant k \leqslant N$.

Soit $\chi \neq \chi_0$. On pose, pour tous entiers $m, n \geqslant 1$:

$$F(m,n) := \frac{\chi(n)}{\sqrt{mn}},$$

ainsi que S_N définie comme précédemment pour $N \in \mathbb{N}^*$.

Proposition 3.9. *La somme S_N vérifie :*

1. *Il existe une constante $c > 0$ telle que $S_N \geqslant c \log N$.*
2. *De plus, $S_N = 2\sqrt{N} L(1,\chi) + \mathrm{O}(1)$.*

Pour conclure la preuve du théorème de Dirichlet, il suffit alors de prouver cette proposition. En effet, en supposant que $L(1,\chi) = 0$, les assertions (1) et (2) sont incompatibles. Donc si la proposition est vraie, cela montre par l'absurde que $L(1,\chi) \neq 0$.

Preuve. On commence par sommer le long des hyperboles (méthode (a)) :

$$S_N = \sum_{k=1}^{N} \left(\sum_{mn=k} F(m,n) \right) = \sum_{k=1}^{N} \left(\sum_{mn=k} \frac{\chi(n)}{\sqrt{mn}} \right) = \sum_{k=1}^{N} \left(\frac{1}{\sqrt{k}} \sum_{n|k} \chi(n) \right).$$

Pour prouver (1), il suffit de montrer le lemme suivant :

Lemme 3.8. *Pour tout $\chi \neq \chi_0$, on a :*

$$\sum_{n|k} \chi(n) \geqslant \begin{cases} 0 & \text{pour tout } k, \\ 1 & \text{si } k \text{ est un carré.} \end{cases}$$

Preuve. Tout d'abord, si k est une puissance d'un nombre premier, que l'on note $k = p^\alpha$, alors ses diviseurs sont $1, p, \ldots, p^\alpha$. Ainsi, comme χ est multiplicatif :

$$\begin{aligned} \sum_{n|k} \chi(n) &= \chi(1) + \chi(p) + \chi(p^2) + \ldots + \chi(p^\alpha) \\ &= \chi(1) + \chi(p) + \chi(p)^2 + \ldots + \chi(p)^\alpha \\ &= \begin{cases} \alpha + 1 & \text{si } \chi(p) = 1, \\ 1 & \text{si } \chi(p) = -1 \text{ et } \alpha \text{ est pair}, \\ 0 & \text{si } \chi(p) = -1 \text{ et } \alpha \text{ est impair}, \\ 1 & \text{si } \chi(p) = 0, \text{ i.e. si } p \mid a. \end{cases} \end{aligned}$$

Dans le cas général, k s'écrit sous la forme $k = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_r^{\alpha_r}$. Alors ses diviseurs sont tous les $p_1^{\beta_1} p_2^{\beta_2} \ldots p_r^{\beta_r}$ où $0 \leqslant \beta_j \leqslant \alpha_j$ pour tout j. Donc, comme χ est multiplicatif, on obtient :

$$\sum_{n|k} \chi(n) = \prod_{j=1}^{r} \left(\chi(1) + \chi(p_j) + \chi(p_j^2) + \ldots + \chi(p_j^{\alpha_j}) \right).$$

D'après ce qui précède, chaque facteur du produit est positif, et dans le cas où k est un carré, chaque facteur est plus grand que 1 car tous les α_j sont pairs. □

Revenons à la preuve de (1). On a alors d'après la Proposition 3.7 :

$$S_N \geqslant \sum_{l=1}^{\sqrt{N}} \frac{1}{\sqrt{l^2}} = \sum_{l=1}^{\sqrt{N}} \frac{1}{l} \geqslant c \log N.$$

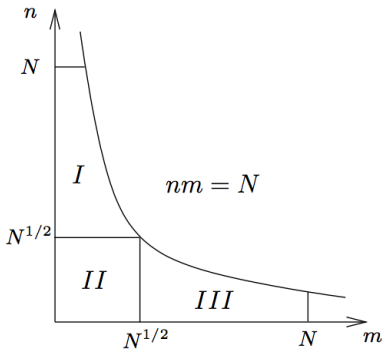
Pour prouver (2), on écrit :

$$S_N = S_I + S_{II} + S_{III},$$

où $S_I = \sum_{m,n \in I} F(m,n)$, et de même pour S_{II} et S_{III}, avec :

$$\begin{aligned} I &= \left\{ 1 \leqslant m < \sqrt{N}, \sqrt{N} < n \leqslant N/m \right\}, \\ II &= \left\{ 1 \leqslant m \leqslant \sqrt{N}, 1 \leqslant n \leqslant \sqrt{N} \right\}, \\ III &= \left\{ \sqrt{N} < m \leqslant N/n, 1 \leqslant n < \sqrt{N} \right\}. \end{aligned}$$

La figure suivante montre ces trois régions :



On évalue S_I en sommant verticalement et $S_{II} + S_{III}$ en sommant horizontalement. Pour cela, on utilise le lemme suivant :

Lemme 3.9. *Pour tous entiers $0 < \alpha < \beta$, on a :*

$$\sum_{n=\alpha}^{\beta} \frac{\chi(n)}{\sqrt{n}} = \mathrm{O}\left(\frac{1}{\sqrt{\alpha}}\right),$$

ainsi que :

$$\sum_{n=\alpha}^{\beta} \frac{\chi(n)}{n} = \mathrm{O}\left(\frac{1}{\alpha}\right).$$

Preuve. La preuve est similaire à celle de la Proposition 3.5 en utilisant une transformation d'Abel puis en effectuant une comparaison avec une intégrale. □

Revenons à la preuve de (2). On a :

$$S_I = \sum_{m=1}^{\sqrt{N}} \frac{1}{\sqrt{m}} \left(\sum_{n=\sqrt{N}+1}^{N/m} \frac{\chi(n)}{\sqrt{n}} \right).$$

Le lemme et la Proposition 3.8 montrent que $S_I = \mathrm{O}(1)$. De plus :

$$\begin{aligned} S_{II} + S_{III} &= \sum_{n=1}^{\sqrt{N}} \left(\frac{\chi(n)}{\sqrt{n}} \sum_{m=1}^{N/n} \frac{1}{\sqrt{m}} \right) \\ &= \sum_{n=1}^{\sqrt{N}} \frac{\chi(n)}{\sqrt{n}} \left(2\sqrt{\frac{N}{n}} + c + \mathrm{O}\left(\sqrt{\frac{N}{n}}\right) \right) \\ &= \underbrace{2\sqrt{N} \sum_{n=1}^{\sqrt{N}} \frac{\chi(n)}{n}}_{A} + \underbrace{c \sum_{n=1}^{\sqrt{N}} \frac{\chi(n)}{\sqrt{n}}}_{B} + \underbrace{\frac{1}{\sqrt{N}} O\left(\sum_{n=1}^{\sqrt{N}} \chi(n) \right)}_{C}. \end{aligned}$$

Or, on peut écrire d'après le lemme :

$$A = 2\sqrt{N}\left(L(1,\chi) - \sum_{n>\sqrt{N}} \frac{\chi(n)}{n}\right) = 2\sqrt{N}\left(L(1,\chi) + \mathrm{O}\left(\frac{1}{\sqrt{N}}\right)\right).$$

Donc $A = 2\sqrt{N}L(1,\chi) + \mathrm{O}(1)$. Le lemme montre également que $B = \mathrm{O}(1)$. De plus, $C = \mathrm{O}(1)$. Ainsi, $S_{II} + S_{III} = 2\sqrt{N}L(1,\chi) + \mathrm{O}(1)$.

On obtient bien :

$$S_N = 2\sqrt{N}L(1,\chi) + \mathrm{O}(1). \qquad \square$$

Cette proposition étant prouvée, la démonstration du théorème de la progression arithmétique est maintenant achevée. $\square$

3.3 Version quantitative du théorème

Nous allons maintenant montrer, comme annoncé dans l'introduction, la formule suivante :

$$\sum_{\substack{p\in\mathcal{P}\\ p\equiv b[a]}} \frac{1}{p^s} = \frac{1}{\varphi(a)}\log\left(\frac{1}{s-1}\right) + \mathrm{O}(1) \qquad (s\to 1, s>1).$$

Tout d'abord, en comparant $\zeta(s)$ et $\int_1^\infty x^{-s}\mathrm{d}x$, on a :

$$\zeta(s) = \frac{1}{s-1} + \mathrm{O}(1) \qquad (s\to 1, s>1).$$

Donc, en passant au logarithme le Théorème 3.6 page 17, on obtient :

$$\sum_{p\in\mathcal{P}} \frac{1}{p^s} = \log\left(\frac{1}{s-1}\right) + \mathrm{O}(1) \qquad (s\to 1, s>1).$$

Ensuite, d'après la formule page 20, on a :

$$\sum_{p\equiv b[a]} \frac{1}{p^s} = \frac{1}{\varphi(a)}\sum_{p\nmid a}\frac{1}{p^s} + \frac{1}{\varphi(a)}\sum_{\chi\neq\chi_0}\overline{\chi(b)}\sum_p \frac{\chi(p)}{p^s}.$$

Puisque le terme de droite est un $\mathrm{O}(1)$, et que $\sum_{p\nmid a} 1/p^s = \sum_p 1/p^s + \mathrm{O}(1)$, on obtient :

$$\sum_{p\equiv b[a]} \frac{1}{p^s} = \frac{1}{\varphi(a)}\sum_p \frac{1}{p^s} + \mathrm{O}(1) \qquad (s\to 1, s>1),$$

et donc, d'après ce qui précède :

$$\sum_{p\equiv b[a]} \frac{1}{p^s} = \frac{1}{\varphi(a)}\log\left(\frac{1}{s-1}\right) + \mathrm{O}(1) \qquad (s\to 1, s>1).$$

C'est bien ce que nous voulons démontrer.

4 Conclusion

Nous avons prouvé le théorème de la progression arithmétique. Ce résultat est en lui-même remarquable car il est bien plus précis que le théorème des nombres premiers. Mais la démonstration que nous venons de faire est bien plus intéressante encore.

Elle fait appel presque entièrement à de l'analyse, et elle illustre donc bien le fait que tous les domaines mathématiques sont reliés entre eux et forment un tout.

Nous avons vu qu'un raisonnement par l'absurde ne nous permet pas de prouver le théorème de la progression arithmétique. Nous avons donc utilisé une autre méthode qui consiste à montrer que la somme des inverses des nombres premiers congrus à $b \mod a$ diverge.

Grâce à la première partie sur l'analyse de Fourier sur $\mathbb{Z}(n)$ et à la généralisation du Théorème 3.6, nous avons pu montrer qu'il suffit de prouver que les fonctions suivantes :

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

introduites par Dirichlet, sont finies et non nulles pour tous $s > 1$ et $\chi \neq \chi_0$ afin de conclure la démonstration.

Il est remarquable de constater que Dirichlet a été conduit à inventer de toutes pièces une théorie absolument nouvelle, la théorie des caractères, aujourd'hui présente dans plusieurs domaines des mathématiques.

Cette théorie, de nature *a priori* algébrique, permet d'appréhender, avec une perspective duale, les groupes des unités modulo un entier a quelconque. Dirichlet a eu la perspicacité d'inscrire les propriétés formelles que satisfont les caractères à l'intérieur de ces séries infinies convergentes, aujourd'hui appelées séries de Dirichlet, lesquelles sont des expressions réellement propres à l'analyse.

Sur le plan épistémologique, l'intérêt de cette magnifique démonstration réside dans la compréhension synthétique d'un problème d'apparence et d'énonciation simples, mais qui, après analyse et approfondissement par plusieurs générations de mathématiciens, s'est avéré requérir des méthodes unitaires.