# Théorème de la progression arithmétique de Dirichlet

Gilles Auriol
auriolg@free.fr — http ://auriolg.free.fr

# Présentation

Depuis Euclide, on sait qu'il existe une infinité de nombres premiers. Naturellement, on peut se demander si étant donnés $a$ et $b$ premiers entre eux, il existe une infinité de nombres premiers de la forme $an + b$ (si $a$ et $b$ ne sont pas premiers entre eux, il est clair qu'aucun des nombres $an + b$ ne sera premier).

Euler résolut de façon purement algébrique la question dans le cas des nombres de la forme $an + 1$. La démonstration de cette proposition fera l'objet de la première section de ce mémoire. Plus tard, en 1835, Dirichlet démontra le théorème dans toute sa généralité, par des méthodes analytiques. La preuve classique passe par l'analyse complexe ; nous présentons ici une variante utilisant l'analyse réelle, tirée de [Cha03]. Auparavant, il nous faudra prouver quelques résultats de théorie des groupes et des propriétés élémentaires sur la fonction $\zeta$ de Riemann.

# Table des matières



# 1 Un cas particulier du théorème de Dirichlet

Dans cette section nous allons démontrer par une méthode purement algébrique l'existence d'une infinité de nombres premiers de la forme $\lambda n + 1, n \in \mathbb{N}^*$.

## 1.1 Polynômes cyclotomiques

**1.1 Définition (Racines primitives de l'unité dans $\mathbb{C}$).** — *Soit $m \in \mathbb{N}^*$. L'ensemble $\mathbb{U}_m = \{z \in \mathbb{C}/z^m = 1\}$ des racines $m$-ièmes de l'unité dans $\mathbb{C}$ est un groupe cyclique d'ordre $m$. On appelle* racine primitive *$m$-ième de l'unité tout générateur de $\mathbb{U}_m$, c'est-à-dire tout élément $\xi$ de $\mathbb{U}_m$ tel que $\xi^d \neq 1$ pour $1 \leqslant d < m$. On notera $\mathcal{P}_m(\mathbb{C})$ l'ensemble des racines primitives $m$-ièmes de l'unité.*

**1.2 Remarque.** — L'application $\overline{k} \mapsto \exp\left(\frac{2i\pi k}{m}\right)$ est un isomorphisme de groupes entre $\mathbb{Z}/m\mathbb{Z}$ et $\mathbb{U}_m$.

D'après les résultats classiques sur les groupes cycliques, il en résulte immédiatement la

**1.3 Proposition.** — *Soit $m \in \mathbb{N}^*$. Soit $\xi$ une racine primitive $m$-ième de l'unité dans $\mathbb{C}$. Alors les racines primitives $m$-ièmes de l'unité sont les $\xi^k$ avec $1 \leqslant k \leqslant m$ et $k$ premier avec $m$, donc $\mathcal{P}_m(\mathbb{C})$ a pour cardinal $\varphi(m)$ où $\varphi$ désigne l'indicatrice d'Euler.*

**1.4 Définition (Polynôme cyclotomique).** — *Soit $m \in \mathbb{N}^*$. On appelle $m$-ième* polynôme cyclotomique *le polynôme*

$$\Phi_m(X) = \prod_{\xi \in \mathcal{P}_m(\mathbb{C})} (X - \xi).$$

*Il est unitaire, de degré $\varphi(m)$.*

**1.5 Lemme.** — *Soit $m \in \mathbb{N}^*$. Les $\mathcal{P}_d(\mathbb{C})$, $d$ décrivant l'ensemble des diviseurs de $m$ dans $\mathbb{N}^*$, forment une partition de $\mathbb{U}_m$.*

**Preuve.** — Si $d$ divise $m$, $\mathcal{P}_d(\mathbb{C}) \subset \mathbb{U}_d \subset \mathbb{U}_m$. Chaque racine $m$-ième de l'unité dans $\mathbb{C}$ a un unique ordre qui est un diviseur de $m$ d'après le théorème de Lagrange ; autrement dit chaque élément de $\mathbb{U}_m$ appartient à un et un seul des $\mathcal{P}_d(\mathbb{C})$, $d$ diviseur de $m$. ∎

On déduit ce résultat la proposition suivante.

**1.6 Proposition.** — *Soit $m \in \mathbb{N}^*$. On a*

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

Notons au passage l'égalité amusante $m = \sum_{d|m} \varphi(d)$ obtenue en comparant les degrés.

Une propriété importante des polynômes cyclotomiques est d'être à coefficients entiers. Pour démontrer ce résultat, nous avons besoin d'un lemme.

**1.7 Lemme.** — *Soit $P, A, B$ trois éléments non nuls de $\mathbb{Q}[X]$. On suppose que $P \in \mathbb{Z}[X]$, que $P = AB$, et que $P$ et $A$ sont unitaires. Alors $A$ et $B$ appartiennent à $\mathbb{Z}[X]$.*

**Preuve.** — Il est que clair que $B$ est lui aussi unitaire. Notons

$$A(X) = X^n + \sum_{i=0}^{n-1} a_i X^i,$$

les $a_i \in \mathbb{Q}$. Pour chaque $i$, notons $a_i = \frac{p_i}{q_i}$, où $p_i \in \mathbb{Z}$ et $q_i \in \mathbb{N}^*$ sont premiers entre eux. Soit $q$ un multiple commun à $q_0, \ldots, q_{n-1}$. Alors

$$A(X) = X^n + \frac{1}{q} \sum_{i=0}^{n-1} z_i X^i,$$

les $z_i \in \mathbb{Z}$. Quitte à diviser $z_0, \ldots, z_{n-1}$ et $q$ par $\mathrm{PGCD}(z_0, \ldots, z_{n-1}, q)$, on peut supposer que $\mathrm{PGCD}(z_0, \ldots, z_{n-1}, q) = 1$.
Notant

$$A_1(X) = qX^n + \sum_{i=0}^{n-1} z_i X^i,$$

on a $A_1(X) \in \mathbb{Z}[X]$, $A(X) = \dfrac{1}{q} A_1(X)$, et le polynôme $A_1(X)$ est primitif. De même il existe $r \in \mathbb{N}^*$ tel que $B(X) = \dfrac{1}{r} B_1(X)$, où le polynôme $B_1(X) \in \mathbb{Z}[X]$ est primitif. Il vient $qrP = A_1 B_1$, et d'après le lemme de Gauss (le produit de deux polynômes primitifs est primitif), le polynôme $A_1 B_1$ est primitif. Or $\gamma(qrP) = qr\gamma(P) = qr$ car $P$ est unitaire. Donc $qr = 1$, d'où $q = r = 1$. Ainsi $A = A_1 \in \mathbb{Z}[X]$ et $B = B_1 \in \mathbb{Z}[X]$. ∎

**1.8 Proposition.** — *Pour tout $n \in \mathbb{N}^*$, on a $\Phi_n(X) \in \mathbb{Z}[X]$.*

**Preuve.** — On procède par récurrence sur $n \in \mathbb{N}^*$. Pour $n = 1$, c'est clair puisque $\Phi_1(X) = X - 1$. Supposons la propriété vraie jusqu'au rang $n - 1$, où $n \geqslant 2$. Posons

$$F(X) = \prod_{d|n,\, d<n} \Phi_d(X).$$

Par hypothèse de récurrence $F(X) \in \mathbb{Z}[X]$. $F(X)$ est clairement unitaire. Le polynôme $X^n - 1$ est un polynôme unitaire de $\mathbb{Z}[X]$. L'égalité $X^n - 1 = F(X)\Phi_n(X)$ montre d'abord que $\Phi_n(X) \in \mathbb{Q}[X]$ par division euclidienne de $X^n - 1$ par $F(X)$ dans $\mathbb{Q}[X]$, puis, en appliquant le lemme précédent, que $\Phi_n(X) \in \mathbb{Z}[X]$. Ainsi la propriété est vraie au rang $n$. ∎

**1.9 Remarque.** — Le calcul des premiers polynômes cyclotomiques laisse à penser que les coefficients sont dans $\{-1, 0, 1\}$. Il n'en est rien, le premier contre-exemple est fourni par $\Phi_{105}(X)$ dont deux des coefficients sont $-2$.

## 1.2 Une infinité de nombres premiers de la forme $\lambda n + 1, n \in \mathbb{N}^*$

**1.10 Théorème (Cas particulier du théorème de Dirichlet).** — *Soit $n \in \mathbb{N}^*$ fixé.*

1. *Si un nombre premier $p$ divise $\Phi_n(a)$, où $a$ est un entier, mais aucun $\Phi_d(a)$ où $d$ décrit l'ensemble des diviseurs stricts de $n$, alors $p \equiv 1\,[n]$.*
2. *Il existe une infinité de nombre premiers de la forme $\lambda n + 1, n \in \mathbb{N}^*$.*

**Preuve.** — 1) Si $p$ divise $\Phi_n(a)$, $p$ divise $a^n - 1$, soit $(\overline{a})^n = \overline{1}$ dans $\mathbb{F}_p$, soit $\overline{a} \in \mathbb{F}_p^*$ et l'ordre $\omega$ de $\overline{a}$ dans $\mathbb{F}_p^*$ divise $n$. Comme

$$a^\omega - 1 = \prod_{d|\omega} \Phi_d(a),$$

si $\omega < n$, il existe $d$ diviseur strict de $n$ tel que $p$ divise $\Phi_d(a)$, ce qui est exclu. Ainsi $\omega = n$, et puisque $\overline{a}$ est d'ordre $n$ dans le groupe $\mathbb{F}_p^*$ d'ordre $p - 1$, d'après le théorème de Lagrange, on a $n | p - 1$, c'est-à-dire $p \equiv 1\,[n]$.

2) Soit $N \in \mathbb{N}^*$. Posons $a = 3N!$, alors $\Phi_n(a)$ est un entier et

$$|\Phi_n(a)| = \prod_{\substack{\mathrm{PGCD}(k,n)=1 \\ 1 \leqslant k \leqslant n}} |a - \exp\left(\frac{2ik\pi}{n}\right)| \geqslant \prod_{\substack{\mathrm{PGCD}(k,n)=1 \\ 1 \leqslant k \leqslant n}} (a - 1) \geqslant 2^{\varphi(n)} \geqslant 2.$$

Soit $p$ un diviseur premier de $\Phi_n(a)$.

Si $p \leqslant N$, alors $p$ divise $a$, donc divise tout entier de la forme $\sum_{i=1}^{k} z_i a^i$, avec $z_i \in \mathbb{Z}$, et en particulier $p$ divise $\Phi_n(a) - \Phi_n(0)$. Par suite $p$ divise $\Phi_n(0) = \pm 1$, ce qui est absurde. Ainsi $p > N$.

Supposons qu'il existe $\delta$ diviseur de strict de $n$ tel que $p$ divise $\Phi_\delta(a)$. Comme

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

$\overline{a}$ est racine de multiplicité $\geqslant 2$ du polynôme $X^n - \overline{1}$ de $\mathbb{F}_p[X]$. Ceci contredit que le fait que le polynôme $X^n - \overline{1}$ et sa dérivée $\overline{n}X^{n-1}$ sont premiers entre eux dans $\mathbb{F}_p[X]$, comme le prouve l'égalité de Bezout

$$\frac{1}{\overline{n}} X \overline{n} X^{n-1} - (X^n - \overline{1}) = \overline{1}.$$

Ainsi $p$ divise $\Phi_n(a)$ mais aucun des $\Phi_d(a)$ où $d$ est un diviseur strict de $n$. Par le premier point, $p \equiv 1\,[n]$.
En résumé, $\forall N \in \mathbb{N}^*, \exists p$ premier tel que $p > N$ et $p \equiv 1\,[n]$, ce qui traduit exactement qu'il existe une infinité de nombres premiers de la forme $\lambda n + 1, n \in \mathbb{N}^*$. ∎

# 2 Caractères des groupes abéliens finis

Nous allons étudier les homomorphismes d'un groupe abélien fini dans $\mathbb{C}^*$. Après s'être intéressés aux propriétés de ces homomorphismes et avoir muni leur ensemble d'une structure de groupe, nous verrons les relations dites d'orthogonalité, qui seront utilisées dans la démonstration du théorème de Dirichlet. Enfin nous définirons les caractères de Dirichlet.

## 2.1 Premières propriétés des caractères et dual d'un groupe

**2.1 Définition (Caractère).** — *Soit $G$ un groupe. Un homomorphisme multiplicatif $\chi : G \to \mathbb{C}^*$ est appelé* caractère. *Le caractère $\chi_0$ tel que $\chi_0(a) = 1$ pour tout $a \in G$ est dit caractère trivial.*

Notons que pour tout $a \in G$, on a que $|\chi(a)| = 1$, puisque part le théorème de Lagrange, en posant $n = |G|$, on a $a^n = e$ d'où $1 = \chi(e) = \chi(a^n) = \chi(a)^n$.

**2.2 Définition (Dual d'un groupe).** — *Soit $\chi_1$ et $\chi_2$ deux caractères d'un groupe abélien fini $G$. On définit le produit $\chi_1\chi_2$ de ces deux caractères en posant $\chi_1\chi_2(a) = \chi_1(a)\chi_2(a)$. L'ensemble des caractères de $G$ muni de cette opération forme un groupe abélien à $|G|$ éléments noté $\widehat{G}$, appelé* dual *de $G$, dont l'élément neutre est $\chi_0$.*

Il est immédiat de vérifier que $\widehat{G}$ est bien un groupe abélien. En effet, pour $\chi_1, \chi_2 \in \widehat{G}$, on a $\chi_1\chi_2(ab) = \chi_1(ab)\chi_2(ab) = \chi_1(a)\chi_1(b)\chi_2(a)\chi_2(b) = \chi_1\chi_2(a)\chi_1\chi_2(b)$, donc $\chi_1\chi_2$ est encore un caractère. L'inverse $\chi_1^{-1}$ de $\chi_1$ est défini par $\chi_1^{-1}(a) = \dfrac{1}{\chi_1(a)}$, ou encore puisque $\chi_1(a)$ est de module 1 par $\chi_1^{-1}(a) = \overline{\chi(a)} = \overline{\chi}(a)$ (la dernière égalité étant juste une notation). Le fait que $\chi_0$ est l'identité de $\widehat{G}$ et que $\widehat{G}$ est commutatif est évident. Enfin que $\widehat{G}$ soit d'ordre $|G|$ résulte du théorème 2.4 ci-dessous.

**2.3 Théorème.** — *Soit $H$ un sous-groupe d'un groupe fini abélien $G$, et supposons que le quotient $G/H$ soit cyclique. Alors chaque caractère de $H$ est la restriction de $[G : H]$ caractères de $G$.*

**Preuve.** — Soit $m = [G : H]$, et soit $aH$ un générateur de $G/H$. Alors $a^m \in H$ et chaque élement de $G$ s'écrit de façon unique $a^j h$ avec $0 \leqslant j \leqslant m-1$ et $h \in H$.

Soit $\chi \in \widehat{H}$ et supposons que $\chi = \widetilde{\chi}|_H$ avec $\widetilde{\chi} \in \widehat{G}$. Posons $\eta = \widetilde{\chi}(a)$. Alors

$$\eta^m = \widetilde{\chi}(a)^m = \widetilde{\chi}(a^m) = \chi(a^m)$$

et pour $0 \leqslant j \leqslant m-1$ et $h \in G$,

$$\widetilde{\chi}(a^j h) = \widetilde{\chi}(a)^j \widetilde{\chi}(h) = \eta^j \chi(h).$$

Ainsi $\widetilde{\chi}$ est déterminé par $\chi$ et $\eta$. Il y a $m$ façons de choisir $\eta$, ce sont les racines $m$-ièmes de $\chi(a^m)$. Vérifions alors que la formule ci-dessous donne bien des caractères de $G$.

Prenons pour $\eta$ une racine $m$-ième de $\chi(a^m)$. Soit $0 \leqslant j, k \leqslant m-1$ et $h, h' \in H$. Alors en utilisant la commutativité de $G$

$$\widetilde{\chi}(a^j h)\widetilde{\chi}(a^k h') = \eta^{j+k}\chi(h)\chi(h') = \eta^{j+k}\chi(hh').$$

Si $j + k \leqslant m-1$, alors

$$\widetilde{\chi}(a^j h)\widetilde{\chi}(a^k h') = \widetilde{\chi}(a^{j+k} hh') = \widetilde{\chi}((a^j h)(a^k h')).$$

Sinon $0 \leqslant j + k - m \leqslant m-1$ et donc

$$\begin{aligned} \widetilde{\chi}(a^j h)\widetilde{\chi}(a^k h') &= \eta^{j+k-m}\eta^m \chi(hh') = \eta^{j+k-m}\chi(a^m)\chi(hh') \\ &= \eta^{j+k-m}\chi(a^m hh') = \widetilde{\chi}(a^{j+k-m}a^m hh') = \widetilde{\chi}((a^j h)(a^k h')). \end{aligned}$$

Ce qui montre que $\widetilde{\chi}$ est un caractère de $G$. ∎

Plus généralement, on peut énoncer

**2.4 Théorème.** — *Soit $H$ un sous-groupe d'un groupe fini abélien $G$. Chaque caractère de $H$ est la restriction de $[G : H]$ caractères de $G$. En particulier $|\widehat{G}| = |G|$.*

**Preuve.** — Soit $G = \langle a_1, \ldots, a_r \rangle$. Posons $H_j = H + \langle a_1, \ldots, a_j \rangle$ pour $0 \leqslant j \leqslant r$. Ainsi $H_0 = H$, $H_r = G, H_j \subset H_{j+1}$ pour $0 \leqslant j \leqslant r-1$ et $H_{j+1}/H_j$ est cyclique. En appliquant le théorème 2.3 il vient qu'un caractère de $H$ est la restriction de

$$\prod_{j=0}^{r-1} [H_{j+1} : H_j] = [G : H]$$

caractères de $G$.

Le groupe trivial n'a qu'un seul caractère, donc en appliquant le résultat à $H = \{e\}$, on obtient $|\widehat{G}| = [G : \{e\}] = |G|$. ∎

**2.5 Remarque (Caractères d'un groupe cyclique).** — Soit $G = \langle a \rangle$ d'ordre $m$. Il est aisé d'exhiber ses caractères. Soit $\psi \in \widehat{G}$. En reprenant la démonstration du théorème 2.3 avec $H = \{e\}$ il vient que $\psi(a)$ est l'une des racines $m$-ièmes de l'unité, donc $\psi(a) = \exp(2\pi ij/m)$ avec $0 \leqslant j \leqslant m-1$. De plus la connaissance de $\psi(a)$ détermine entièrement le caractère, puisque pour tout $0 \leqslant k \leqslant m-1$, on a $\psi(a^k) = \psi(a)^k = \exp(2\pi ijk/m)$. De façon pratique, on retiendra que les caractères de $G$ sont les $\psi_j : a^k \mapsto \exp(2\pi ijk/m)$ pour $0 \leqslant j \leqslant m-1$.

## 2.2 Relations d'orthogonalité des caractères

**2.6 Théorème.** — *Soit $G$ un groupe fini abélien. On a*

$$(i)\ \sum_{g\in G}\chi(g)=\begin{cases}|G| & si\ \chi=\chi_0,\\ 0 & sinon\end{cases}\qquad et\quad (ii)\ \sum_{\chi\in\widehat{G}}\chi(g)=\begin{cases}|G| & si\ g=e,\\ 0 & sinon.\end{cases}$$

**Preuve.** — $(i)$ Remarquons que $\chi$ étant un homomorphisme, son noyau H est un sous-groupe de $G$ et on a l'isomorphisme $G/H\simeq \mathrm{Im}(\chi)$. Comme $\mathrm{Im}(\chi)$ est un sous-groupe fini de $\mathbb{C}^*$, c'est un groupe de racines de l'unité. Le caractère $\chi$ envoie sur chaque racine $d$-ième de l'unité un même nombre d'éléments de $G$. Si $\chi\neq\chi_0$, le groupe quotient $G/H$ a au moins 2 éléments et par l'isomorphisme, il en est de même de $\mathrm{Im}(\chi)$. Ainsi la somme de ses éléments vaut 0. Si $\chi=\chi_0$, le résultat est clair puisque $\chi(g)=1$ pour tout $g\in G$ et $|\widehat{G}|=|G|$.

$(ii)$ Le résultat est acquis pour $g=e$ car dans ce cas $\chi(e)=1$ pour tout caractère $\chi$. Si $g\neq e$, considérons le sous-groupe $H=\langle g\rangle$. Il est cyclique d'ordre $n\geqslant 2$, son dual $\widehat{H}$ est aussi d'ordre $n$, et si $\psi(g)=1$ pour tout $\psi\in H$, il vient que $\psi(g^k)=1$ pour tout $0\leqslant k\leqslant n-1$, donc $\widehat{H}$ est trivial, ce qui contredit $n\geqslant 2$. Il existe donc $\psi_1\in\widehat{H}$ tel que $\psi_1(g)\neq 1$. Par suite il existe $\chi_1\in\widehat{G}$ tel que $\chi_1(g)\neq 1$, par prolongement de $\psi_1$ à $G$ (théorème 2.4). Finalement puisque $\chi\mapsto\chi_1\chi$ est une permutation de $\widehat{G}$,

$$\sum_{\chi\in\widehat{G}}\chi(g)=\sum_{\chi\in\widehat{G}}\chi_1\chi(g)=\chi_1(g)\sum_{\chi\in\widehat{G}}\chi(g)$$

et donc $\displaystyle\sum_{\chi\in\widehat{G}}\chi(g)=0$ vu le choix $\chi_1(g)\neq 1$. ∎

## 2.3 Caractères de Dirichlet

Soit $N\in\mathbb{N}^*$. On note $(\mathbb{Z}/N\mathbb{Z})^*$ le groupe des entiers inversibles modulo $N$. L'ordre de ce groupe est $\varphi(N)$, et $\overline{a}$ appartient à $(\mathbb{Z}/N\mathbb{Z})^*$ si et seulement si $a$ et $N$ sont premiers entre eux.

Un caractère de Dirichlet modulo $N$ est un caractère du groupe $(\mathbb{Z}/N\mathbb{Z})^*$ que l'on étend en une fonction définie sur $\mathbb{Z}$ en posant

$$\chi(a)=\begin{cases}\chi(\overline{a}) & \text{si } a \text{ et } N \text{ sont premiers entre eux,}\\ 0 & \text{sinon.}\end{cases}$$

La fonction ainsi définie est multiplicative. En effet si $a$ et $b$ sont premiers à $N$ alors $ab$ l'est aussi, et la multiplicativité résulte de la définition du caractère. si $a$ ou $b$ n'est pas premier à $N$ le produit $ab$ n'est pas non plus premier à $N$ et on a bien $\chi(a)\chi(b)=\chi(ab)=0$. De plus elle est $N$-périodique.

On note $X_N$ l'ensemble des caractères de Dirichlet modulo $N$ et $\chi_0$ le caractère trivial étendu. Il y a $\varphi(N)$ caractères de Dirichlet.

# 3 La fonction $\zeta$ de Riemann

La fonction $\zeta$ peut être définie sur le corps des complexes, mais nous nous contenterons ici d'une définiton dans un cadre réel.

**3.1 Définition (Fonction $\zeta$ de Riemann).** — *Soit $s$ un nombre réel. On pose $\zeta(s)=\displaystyle\sum_{n=1}^{+\infty}\frac{1}{n^s}$ quand cette série converge.*

Pour $s \leqslant 0$, la série diverge grossièrement, on peut donc supposer $s > 0$. Dans ce cas

$$\frac{1}{n^s} > \int_n^{n+1} \frac{\mathrm{d}t}{t^s} > \frac{1}{(n+1)^s},$$

donc

$$\sum_{n=1}^{M} \frac{1}{n^s} > \int_1^M \frac{\mathrm{d}t}{t^s} > \sum_{n=2}^{M+1} \frac{1}{n^s}. \tag{1}$$

et la série converge si et seulement si $\displaystyle\int_1^{+\infty} \frac{\mathrm{d}t}{t^s}$ converge. On a alors le résultat suivant.

**3.2 Théorème.** — *La série $\zeta(s)$ converge si et seulement si $s > 1$. Dans ce cas*

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

*En particulier*

$$\lim_{s \to 1^+} (s-1)\zeta(s) = 1.$$

**Preuve.** — On a

$$\int_1^N \frac{\mathrm{d}t}{t^s} = \begin{cases} \dfrac{1 - N^{1-s}}{s-1} & \text{si } s \neq 1, \\ \ln N & \text{si } s = 1, \end{cases}$$

donc l'intégrale $\displaystyle\int_1^{+\infty} \frac{\mathrm{d}t}{t^s}$ converge vers $\dfrac{1}{s-1}$ si et seulement si $s > 1$. En passant à la limite dans (**??**), il vient

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

d'où

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

En multipliant par $s - 1$ et en faisant tendre $s$ vers $1^+$, on a le résultat souhaité. ∎

Nous prouvons maintenant la formule d'Euler pour la fonction $\zeta$ qui fait le lien avec les nombres premiers.

**3.3 Théorème (Développement eulérien).** — *Soit $s > 1$. Alors*

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

*où le produit est pris sur les entiers premiers.*

**Preuve.** — Soit $M$ un entier naturel. Alors

$$\prod_{p \leqslant M} \left(1 - \frac{1}{p^s}\right)^{-1} = \prod_{p \leqslant M} \sum_{m=0}^{+\infty} \frac{1}{p^{ms}} = \sum_{n \in A_M} \frac{1}{n^s}$$

où $A_M$ est l'ensemble des entier naturel dont aucun des facteurs premiers n'excède $M$. Puisque $A_M$ contient tous les entiers $n \leqslant M$, il vient

$$\sum_{n=1}^{M} \frac{1}{n^s} \leqslant \prod_{p \leqslant M} \left(1 - \frac{1}{p^s}\right)^{-1} \leqslant \zeta(s).$$

En faisant tendre $M$ vers $+\infty$, on a le résultat souhaité. ∎

# 4 L-fonctions de Dirichlet

Dans la suite, $N$ désignera un entier $\geqslant 1$.

**4.1 Définition (L-fonction de Dirichlet).** — *Soit $\chi \in X_N$ et $s \in \mathbb{R}$. On définit la* L-fonction de Dirichlet *$L(s,\chi)$ par $L(s,\chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}$ quand cette série converge.*

Avant de regarder des conditions pour que les L-fonctions convergent, nous allons prouver un lemme qui nous servira plusieurs fois.

**4.2 Lemme.** — *Soit $\chi \in X_N$ et supposons que $\chi \neq \chi_0$. Posons $a_n = \sum_{j=1}^{n} \chi(j)$. Alors pour tout $n \in \mathbb{N}$, $|a_n| \leqslant N$.*

**Preuve.** — On suppose $N \geqslant 2$, car pour $N = 1$, on ne peut pas trouver de $\chi \neq \chi_0$. Par le théorème 2.6, $\sum_{j=1}^{N} \chi(j) = 0$ pour $N \geqslant 2$. Soit maintenant $n > N$. En effectuant la division euclidienne de $n$ par $N$, il existe $q \in \mathbb{N}$ et $0 \leqslant r < N$ tel que $n = qN + r$, d'où

$$a_n = \sum_{j=1}^{n} \chi(j) = \sum_{j=1}^{N} \chi(j) + \sum_{j=N+1}^{2N} \chi(j) + \cdots + \sum_{j=(q-1)N+1}^{qN} \chi(j) + \sum_{j=qN+1}^{qN+r} \chi(j)$$

Tous les termes du membre de droite sont nuls, sauf le dernier qui peut se réécrire $\sum_{j=1}^{r} \chi(j) = a_r$ par définition du caractère de Dirichlet. Par suite

$$|a_n| = |a_r| \leqslant \sum_{j=1}^{r} |\chi(j)| \leqslant r \leqslant N,$$

comme attendu. ∎

**4.3 Théorème.** — *Soit $\chi \in X_N$. Si $\chi = \chi_0$, la série $L(s,\chi)$ converge pour $s > 1$. Si $\chi \neq \chi_0$, la série converge pour $s > 0$.*

**Preuve.** — Lorsque $\chi = \chi_0$, on a $\chi(n) \in \{0, 1\}$ pour tout $n \in \mathbb{N}$, donc

$$0 \leqslant \sum_{n=1}^{M} \frac{\chi(n)}{n^s} \leqslant \sum_{n=1}^{M} \frac{1}{n^s}$$

et par comparaison à la série $\zeta(s)$, cette série converge pour $s > 1$.
Supposons à présent $\chi \neq \chi_0$. Posons

$$a_0 = 0 \text{ et } a_n = \sum_{j=1}^{n} \chi(j) \text{ si } n \geqslant 1.$$

On a alors $\chi(n) = a_n - a_{n-1}$ pour $n \geqslant 1$, et une transformation d'Abel conduit à

$$\begin{aligned}\sum_{n=1}^{M} \frac{\chi(n)}{n^s} &= \sum_{n=1}^{M} \frac{a_n - a_{n-1}}{n^s} \\ &= \sum_{n=1}^{M} \frac{a_n}{n^s} - \sum_{n=1}^{M} \frac{a_{n-1}}{n^s} \\ &= \sum_{n=1}^{M} \frac{a_n}{n^s} - \sum_{n=1}^{M-1} \frac{a_n}{(n+1)^s} \\ &= \frac{a_M}{M^s} + \sum_{n=1}^{M-1} a_n \left[\frac{1}{n^s} - \frac{1}{(n+1)^s}\right].\end{aligned}$$

Par le lemme 4.2, il existe $A$ tel que $|a_n| \leqslant A$ pour tout $n$. Si $s > 0$, alors $a_M/M^s \to 0$ quand $M \to \infty$ et

$$\sum_{n=1}^{M-1} \left| a_n \left[\frac{1}{n^s} - \frac{1}{(n+1)^s}\right]\right| \leqslant A\left(1 - \frac{1}{M^s}\right)$$

Il en résulte que la série $L(s,\chi)$ converge pour $s > 0$. De plus,

$$L(s,\chi) = \sum_{n=1}^{\infty} a_n \left[\frac{1}{n^s} - \frac{1}{(n+1)^s}\right]$$

Cette formule nous servira un peu plus loin. ∎

A l'instar de la série $\zeta(s)$, la série $L(s,\chi)$ peut s'écrire comme un produit infini. Plus précisément, on dispose du théorème suivant

**4.4 Théorème.** — *Soit $\chi \in X_N$ et $s > 1$. Alors*

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

**Preuve.** — Puisque

$$L(s,\chi) = 1 + \frac{\chi(2)}{2^s} + \frac{\chi(3)}{3^s} + \ldots,$$

on a par exemple

$$\frac{\chi(2)}{2^s} L(s,\chi) = \frac{\chi(2)}{2^s} + \frac{\chi(4)}{4^s} + \frac{\chi(6)}{6^s} + \ldots,$$

d'où en soustrayant membre à membre

$$\left(1 - \frac{\chi(2)}{2^s}\right) L(s,\chi) = 1 + \frac{\chi(3)}{3^s} + \frac{\chi(5)}{5^s} + \ldots$$

On recommence alors le procédé : on a

$$\frac{\chi(3)}{3^s}\left(1 - \frac{\chi(2)}{2^s}\right) L(s,\chi) = \frac{\chi(3)}{3^s} + \frac{\chi(9)}{9^s} + \frac{\chi(15)}{15^s} + \ldots$$

puis en soustrayant ces deux dernières équations

$$\left(1 - \frac{\chi(2)}{2^s}\right)\left(1 - \frac{\chi(3)}{3^s}\right) L(s,\chi) = 1 + \frac{\chi(5)}{5^s} + \frac{\chi(7)}{7^s} + \ldots$$

En itérant ce procédé pour chaque premier $p$, on obtient

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

ce qui est le résultat attendu. ∎

Les deux théorèmes suivants concernent le comportement de $L(s,\chi)$ quand $s \to 1^+$.

**4.5 Théorème.** — *Pour $\chi = \chi_0 \in X_N$, on a*

$$\lim_{s\to 1^+} (s-1)L(s,\chi) = \frac{\varphi(N)}{N}.$$

**Preuve.** — Soit $s > 1$. Puisque $\chi(p) = 0$ si $p|N$ et $\chi(p) = 1$ si $p \nmid N$, on peut écrire par le théorème 4.4

$$L(s,\chi) = \prod_{p\nmid N} \left(1 - \frac{1}{p^s}\right)^{-1} = \prod_p \left(1 - \frac{1}{p^s}\right)^{-1} \prod_{p|N} \left(1 - \frac{1}{p^s}\right),$$

ou encore

$$L(s,\chi) = \zeta(s) \prod_{p|N} \left(1 - \frac{1}{p^s}\right).$$

Mais

$$\lim_{s\to 1^+} (s-1)\zeta(s) = 1,$$

donc

$$\lim_{s\to 1^+} (s-1)L(s,\chi) = \lim_{s\to 1^+} \prod_{p|N} \left(1 - \frac{1}{p^s}\right) = \prod_{p|N} \left(1 - \frac{1}{p}\right) = \frac{\varphi(N)}{N},$$

d'où le résultat. ∎

**4.6 Théorème.** — *Soit $\chi \in X_N$ avec $\chi \neq \chi_0$. On a*

$$L(s,\chi) = L(1,\chi) + O(s-1) \text{ quand } s \to 1^+.$$

**Preuve.** — Soit $1 < s < 2$. Par la preuve du théorème 4.3,

$$L(s,\chi) - L(1,\chi) = \sum_{n=1}^{\infty} a_n \left[\left(\frac{1}{n^s} - \frac{1}{(n+1)^s}\right) - \left(\frac{1}{n} - \frac{1}{n+1}\right)\right]$$

En appliquant le théorème des accroissements finis à $s \mapsto n^{-s} - (n+1)^{-s}$ de dérivée

$$s \mapsto \frac{\ln(n+1)}{(n+1)^s} - \frac{\ln n}{n^s},$$

il existe $s_n \in ]1; s[$ tel que

$$L(s,\chi) - L(1,\chi) = (s-1) \sum_{n=1}^{\infty} a_n \left[\frac{\ln(n+1)}{(n+1)^{s_n}} - \frac{\ln n}{n^{s_n}}\right].$$

Une nouvelle application du théorème des accroissements finis à la fonction $x \mapsto \dfrac{\ln x}{x^{s_n}}$ de dérivée

$$x \mapsto \frac{1 - s_n \ln x}{x^{s_n+1}}$$

donne un réel $b_n$ tel que $n < b_n < n+1$ avec

$$L(s,\chi) - L(1,\chi) = (s-1)\sum_{n=1}^{\infty} a_n \left( \frac{1 - s_n \ln b_n}{b_n^{s_n+1}} \right).$$

En appelant $A$ un majorant de la suite bornée $(|a_n|)$, on a

$$\left| a_n \left( \frac{1 - s_n \ln b_n}{b_n^{s_n+1}} \right) \right| \leqslant A \frac{1 + s_n \ln(n+1)}{n^{s_n+1}} \leqslant A \frac{1 + 2\ln(n+1)}{n^2}.$$

Posons

$$C = A \sum_{n=1}^{\infty} \frac{1 + 2\ln(n+1)}{n^2}.$$

Admettons provisoirement que cette série converge. On a alors

$$|L(s,\chi) - L(1,\chi)| \leqslant C(s-1),$$

pour $1 < s < 2$, ce qui démontre le théorème.

Pour voir que $C$ converge, remarquons d'abord que $\ln(n+1) \leqslant \ln(2n) \leqslant \ln 2 + \ln n$ pour $n \geqslant 1$. Posons $f(x) = \dfrac{\ln x}{\sqrt{x}}$ pour $x \geqslant 1$. On a $f(x) \geqslant 0$ et

$$f'(x) = \frac{2 - \ln x}{2x^{3/2}},$$

d'où $f'(x) > 0$ pour $1 \leqslant x < e^2$ et $f'(x) < 0$ pour $x > e^2$. Ainsi $f$ admet un maximum en $e^2$, c'est-à-dire $f(x) \leqslant f(e^2)$ pour tout $x \geqslant 1$, soit encore

$$\frac{\ln x}{\sqrt{x}} \leqslant \frac{2}{e}.$$

Par suite,

$$0 < \frac{1 + 2\ln(n+1)}{n^2} \leqslant \frac{1 + 2\ln 2 + 2\ln n}{n^2} \leqslant \frac{1 + 2\ln 2}{n^2} + \frac{4}{en^{3/2}}$$

pour tout entier naturel $n \geqslant 1$. On en déduit que $C$ converge puisque le dernier terme de cette inégalité est le terme général d'une série qui converge vers $(1 + 2\ln 2)\zeta(2) + \dfrac{4}{e}\zeta(\dfrac{3}{2})$. ∎

Nous allons maintenant montrer que $Ł(s,\chi) \neq 0$ pour tout $\chi \neq \chi_0$. Avant cela prouvons un lemme.

**4.7 Lemme.** — *Pour tout $s > 1$ on a*

$$\prod_{\chi \in X_N} L(s,\chi) > 1.$$

**Preuve.** — En utilisant le théorème 4.4, on a

$$\prod_{\chi \in X_N} L(s,\chi) = \prod_{p} \prod_{\chi \in X_N} \left( 1 - \frac{\chi(p)}{p^s} \right)^{-1}.$$

Si $p$ et $N$ sont premiers entre eux

$$\left( 1 - \frac{\chi(p)}{p^s} \right)^{-1} = 1.$$

Sinon $\chi(p) \neq 0$ pour tout $\chi \in X_N$. Soit $H$ le sous-groupe de $(\mathbb{Z}/N\mathbb{Z})^*$ engendré par $\overline{p}$ et $r$ son ondre. Il vient par le théorème 2.3

$$\prod_{\chi \in X_N} \left(1 - \frac{\chi(p)}{p^s}\right)^{-1} = \prod_{\psi \in \widehat{H}} \left(1 - \frac{\psi(p)}{p^s}\right)^{-\varphi(N)/r}.$$

Puisque $H$ est cyclique d'ordre $r$ engendré par $\overline{p}$, ses caractères sont les $\psi_j : \overline{p}^k \mapsto \exp(2\pi ijk/r)$ pour $0 \leqslant j \leqslant r-1$ (voir remarque 2.5). Ainsi $\psi_j(\overline{p}) = \exp(2\pi ij/r)$, donc

$$\prod_{\psi \in \widehat{H}} \left(1 - \frac{\chi(p)}{p^s}\right) = \prod_{j=0}^{r-1} \left(1 - \frac{\exp(2\pi ij/r)}{p^s}\right) = \frac{1}{p^{sr}} \prod_{j=0}^{r-1} (p^s - \exp(2\pi ij/r)) = \frac{1}{p^{sr}}(p^{sr} - 1) < 1,$$

d'où

$$\prod_{\chi \in X_N} \left(1 - \frac{\chi(p)}{p^s}\right)^{-1} = \left(1 - \frac{1}{p^{rs}}\right)^{-\varphi(n)/r} > 1,$$

ce qui termine la preuve. ∎

**4.8 Théorème.** — *Soit $\chi \in X_N$, avec $\chi \neq \chi_0$. Alors*

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

**Preuve.** — Supposons dans un premier temps que $\chi$ est à valeurs complexes. Les trois caractères $\chi_0$, $\chi$ et $\overline{\chi}$ sont distincts. Si $L(1, \chi) = 0$, on a

$$L(1, \overline{\chi}) = \sum_{n=1}^{\infty} \frac{\overline{\chi(n)}}{n} = \overline{\sum_{n=1}^{\infty} \frac{\chi(n)}{n}} = \overline{L(1, \chi)} = 0.$$

Par les théorèmes 4.5 et 4.6, $L(s, \chi_0) = O(1/(s-1))$, $L(s, \chi) = O(s-1)$ et $L(s, \overline{\chi}) = O(s-1)$ quand $s \to 1^+$. Ainsi

$$\lim_{s \to 1^+} L(s, \chi_0) L(s, \chi) L(s, \overline{\chi}) = 0,$$

mais le théorème 4.3 donne

$$\lim_{s \to 1^+} \prod_{\substack{\psi \in X_N \\ \psi \neq \chi_0, \chi, \overline{\chi}}} L(s, \psi) = \prod_{\substack{\psi \in X_N \\ \psi \neq \chi_0, \chi, \overline{\chi}}} L(1, \psi),$$

d'où

$$\lim_{s \to 1^+} \prod_{\psi \in X_N} L(s, \psi) = 0,$$

ce qui contredit le lemme.

Passons maintenant au cas difficile, lorsque $\chi$ est à valeurs réelles, donc dans $\{-1, 0, 1\}$. On introduit la série de Lambert

$$f(x) = \sum_{d=1}^{+\infty} \frac{\chi(d) x^d}{1 - x^d}.$$

qui converge pour $0 < x < 1$ par comparaison à la série de terme général $u_d = \dfrac{x^d}{1 - x^d}$. En effet

$$\frac{u_{d+1}}{u_d} = x \frac{1 - x^d}{1 - x^{d+1}} < 1$$

car $1-x^{d+1} > 1-x^d$ pour $0<x<1$ et le critère de d'Alembert permet de conclure. On peut écrire $f$ sous la forme

$$f(x) = \sum_{d=1}^{+\infty} \chi(d) \sum_{t=1}^{+\infty} x^{dt} = \sum_{n=1}^{+\infty} x^n \sum_{d|n} \chi(d) = \sum_{n=1}^{+\infty} c_n x^n$$

où $c_n = \sum_{d|n} \chi(d)$. Nous allons montrer par récurrence sur $n \geqslant 1$ que $c_n \geqslant 0$. Il est clair que $c_1 = \chi(1) = 1$. Si $n \geqslant 2$, on a $n = p^k m$ où $p$ est premier, $k > 0$ et $p \nmid m$. Alors

$$c_n = \sum_{d|p^k m} \chi(d) = \sum_{j=0}^{k} \sum_{r|m} \chi(p^j r) = \sum_{j=0}^{k} \sum_{r|m} \chi(p)^j \chi(r) = c_m \sum_{j=0}^{k} \chi(p)^j.$$

Ainsi

$$c_n = \begin{cases} (k+1)c_m & \text{si } \chi(p) = 1, \\ c_m & \text{si } \chi(p) = 0, \\ c_m & \text{si } \chi(p) = -1 \text{ et } k \text{ est pair}, \\ 0 & \text{si } \chi(p) = -1 \text{ et } k \text{ est impair}. \end{cases}$$

ce qui montre que si $c_m \geqslant 0$, alors $c_n \geqslant 0$. En remarquant que $c_1 = 1$, on a aussi $c_{p^{2k}} \geqslant 1$ pour tout $k \geqslant 0$ et donc la série $\sum_{r=1}^{+\infty} c_r$ diverge. Pour tout $M \geqslant 1$,

$$\limsup_{x \to 1^-} f(x) \geqslant \lim_{x \to 1^-} \sum_{n=1}^{M} c_n x^n = \sum_{n=1}^{M} c_n.$$

Par suite $f(x) \to +\infty$ quand $x \to 1^-$.

Supposons que $L(1, \chi) = 0$. Alors

$$-f(x) = \frac{L(1,\chi)}{1-x} - f(x) = \sum_{n=1}^{+\infty} \chi(n) \left[ \frac{1}{n(1-x)} - \frac{x^n}{1-x^n} \right].$$

Posons

$$b_n(x) = \frac{1}{n(1-x)} - \frac{x^n}{1-x^n}$$

Alors pour $0 < x < 1$,,

$$\begin{aligned} (1-x)(b_n(x) - b_{n+1}(x)) &= \frac{1}{n} - \frac{1}{n+1} - \left[ \frac{x^n(1-x)}{1-x^n} - \frac{x^{n+1}(1-x)}{1-x^{n+1}} \right] \\ &= \frac{1}{n(n+1)} - \frac{x^n(1-x)^2}{(1-x^n)(1-x^{n+1})}. \end{aligned}$$

En utilisant l'inégalité $\dfrac{a+b}{2} \geqslant \sqrt{ab}$, il vient

$$\frac{1-x^n}{1-x} = \sum_{j=0}^{n-1} = \frac{1}{2} \sum_{j=0}^{n-1} (x^j + x^{n-1-j}) \geqslant n x^{\frac{n-1}{2}}.$$

En remplaçant $n$ par $n+1$, on a $\dfrac{1-x^{n+1}}{1-x} \geqslant (n+1)x^{\frac{n}{2}}$, d'où la minoration

$$(1-x)(b_n(x)-b_{n+1}(x)) \geqslant \frac{1-\sqrt{x}}{n(n+1)}$$

qui montre que la suite $(b_n(x))$ est décroissante pour $0<x<1$.

Posons $a_m = \sum_{j=1}^{m} \chi(j)$ pour $m \geqslant 0$ et $a_0 = 0$. Par le lemme 4.2, cette suite est bornée, soit $A$ tel que $|a_m| \leqslant A$ pour tout $m$. Alors

$$\sum_{n=1}^{M} \chi(n)b_n(x) = \sum_{n=1}^{M}(a_n - a_{n-1})b_n(x) = A_M b_M(x) + \sum_{n=1}^{M-1} a_n(b_n(x)-b_{n+1}(x)).$$

Quand $M \to +\infty$, $B_M(x) \to 0$, donc

$$-f(x) = \sum_{n=1}^{+\infty} a_n(b_n(x)-b_{n+1}(x)).$$

Il vient alors

$$|f(x)| \leqslant \sum_{n=1}^{+\infty} |a_n|(b_n(x)-b_{n+1}(x)) \leqslant A\sum_{n=1}^{+\infty}(b_n(x)-b_{n+1}(x)) = Ab_1(x) = A,$$

ce qui montre que $f$ est bornée pour $0<x<1$ et contredit le fait que $f(x) \to +\infty$ quand $x \mapsto 1^-$. Ainsi nous ne pouvons avoir $L(1,\chi)=0$. ∎

# 5 Preuve du théorème de Dirichlet

Maintenant que les propriétés essentielles des L-fonctions de Dirichlet sont établies, nous allons montrer le théorème de Dirichlet.

**5.1 Théorème.** — *Soit* $\psi(s) = \sum_p \dfrac{1}{p^s}$ *où la somme est prise sur tout les nombres premiers* $p$. *Cette série est convergente pour* $s>1$, *et* $\psi(s) = -\ln(s-1) + O(1)$ *quand* $s \to 1^+$.

**Preuve.** — Soit $s>1$. La série $\psi(s)$ converge par comparaison à la série $\zeta(s)$. En utilisant le développement eulérien de $\zeta(s)$, il vient

$$\ln\zeta(s) = -\sum_p \ln\left(1-\frac{1}{p^s}\right) = \sum_p \sum_{m=1}^{+\infty} \frac{1}{mp^{ms}} = \psi(s) + \omega(s)$$

où on a posé

$$\omega(s) = \sum_p \sum_{m=2}^{+\infty} \frac{1}{mp^{ms}}.$$

Mais

$$\begin{aligned} 0 < \omega(s) &< \sum_p \sum_{m=2}^{+\infty} \frac{1}{2p^{ms}} = \frac{1}{2}\sum_p \frac{1}{p^{2s}}\left(1-\frac{1}{p^s}\right)^{-1} = \frac{1}{2}\sum_p \frac{1}{(p^s-1)p^s} \\ &< \frac{1}{2}\sum_p \frac{1}{(p-1)p} < \frac{1}{2}\sum_{m=2}^{+\infty} \frac{1}{(m-1)m} = \frac{1}{2}. \end{aligned}$$

Il en résulte que $\psi(s) = \ln \zeta(s) + O(1)$ quand $s \to 1^+$. Mais pour $s > 1$, on a

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

et donc

$$-\ln(s-1) < \ln \zeta(s) < \ln s - \ln(s-1)$$

puis $\ln \zeta(s) = -\ln(s-1) + O(1)$ quand $s \to 1^+$. Par conséquent $\psi(s) = -\ln(s-1) + O(1)$ quand $s \to 1^+$. ∎

**5.2 Théorème.** — *Soit $\chi \in X_N$, avec $\chi \neq \chi_0$. On définit $\psi_\chi(s) = \sum_p \frac{\chi(p)}{p^s}$ où la somme est prise sur tout les nombres premiers $p$. Cette série est convergente pour $s > 1$, et $\psi_\chi(s) = O(1)$ quand $s \to 1^+$.*

**Preuve.** — La série $\psi_\chi(s)$ est convergente par comparaison à la série $\psi(s)$ du théorème 5.1. Soit $s > 1$. Par le développement d'Euler de $L(s, \chi)$ en produit (théorème 4.4), nous avons

$$\ln L(s,\chi) = -\sum_p \ln\left(1 - \frac{\chi(p)}{p^s}\right) = \sum_p \sum_{m=1}^{+\infty} \frac{\chi(p^m)}{mp^{ms}} = \psi_\chi(s) + \omega_\chi(s)$$

où

$$\omega_\chi(s) = \sum_p \sum_{m=2}^{+\infty} \frac{\chi(p^m)}{mp^{ms}}.$$

Mais $|\omega_\chi(s)| \leqslant \omega(s)$, où $\omega$ désigne la fonction du théorème précédent, donc $\omega_\chi(s) = O(1)$ quand $s \to 1^+$. Comme $L(1,\chi) \neq 0$ et $\lim_{s\to 1^+} L(s,\chi) = L(1,\chi)$, il vient que $\ln L(s,\chi) = O(1)$ quand $s \to 1^+$ puis que $\psi_\chi(s) = O(1)$ quand $s \to 1^+$. ∎

Introduisons une définition.

**5.3 Définition (Densité de Dirichlet).** — . *Soit $X$ un sous-ensemble des nombres premiers. On appelle* densité de Dirichlet *de cet ensemble la limite*

$$\lim_{s\to 1^+} \frac{-1}{\ln(s-1)} \sum_{p\in X} \frac{1}{p^s}$$

*lorsqu'elle existe.*

D'après le théorème 5.1, l'ensemble de tous les nombres premiers a pour densité de Dirichlet 1. Un ensemble fini de nombres premiers a pour densité 0, donc un ensemble de densité non nulle est infini.

Nous pouvons maintenant énoncer le théorème tant attendu.

**5.4 Théorème (de Dirichlet).** — *Soit $N$ un entier naturel et $a$ un entier premier à $N$. Alors l'ensemble*

$$P_{a,N} = \{p \text{ premier et } p \equiv a\,[N]\}$$

*a pour densité de Dirichlet $\frac{1}{\varphi(N)}$. En particulier $P_{a,N}$ est infini, c'est-à-dire il existe une infinité de nombres premiers congrus à $a$ modulo $N$.*

**Preuve.** — Posons pour tout $\chi \in X_N$ et $s > 1$

$$\psi_\chi(s) = \sum_p \frac{\chi(p)}{p^s}.$$

Si $\chi \neq \chi_0$, on a vu dans le théorème 5.2 que $\psi_\chi(s) = O(1)$ quand $s \to 1^+$. Pour $\chi = \chi_0$, on a

$$\psi_{\chi_0}(s) = -\sum_{p|N} \frac{1}{p^s} + \sum_p \frac{1}{p^s}.$$

D'après le théorème 5.1, $\displaystyle\sum_p \frac{1}{p^s} = -\ln(s-1) + O(1)$ quand $s \to 1^+$, donc

$$\psi_{\chi_0} = -\ln(s-1) + O(1)$$

quand $s \to 1^+$.

Soit $a$ premier à $N$. Considérons

$$\theta_a(s) = \sum_{\chi \in X_N} \overline{\chi(a)}\psi_\chi(s) = \sum_{\chi \in X_n} \overline{\chi(a)} \sum_p \frac{\chi(p)}{p^s} = \sum_p \frac{1}{p^s} \sum_{\chi \in X_N} \overline{\chi(a)}\chi(p).$$

Soit $b$ un entier naturel tel que $ab \equiv 1\,[N]$. Alors $\chi(b) = \overline{\chi(a)}$ et par le théorème 2.6 $(ii)$

$$\sum_{\chi \in X_N} \overline{\chi(a)}\chi(p) = \sum_{\chi \in X_N} \chi(bp) = \begin{cases} \varphi(N) & \text{si } bp \equiv 1\,[N], \\ 0 & \text{sinon.} \end{cases}$$

Comme $bp \equiv 1\,[N]$ si et seulement si $p \equiv a\,[N]$, il vient

$$\theta_a(s) = \varphi(N) \sum_{p \in P_{a,N}} \frac{1}{p^s}.$$

Mais

$$|\theta_a(s)| \leqslant \sum_{\chi \in X_N} |\overline{\chi(a)}||\psi_\chi(s)| = \sum_{\chi \in X_N} |\psi_\chi(s)|,$$

d'où

$$\theta_a(s) = -\ln(s-1) + O(1)$$

et donc $P_{a,N}$ a pour densité de Dirichlet $\dfrac{1}{|X_N|} = \dfrac{1}{\varphi(N)}$. ∎

# Références


[Cha03] Chapman, R., *Dirichlet's theorem, a real variable approach*. 2003. Disponible à l'adresse `www.maths.ex.ac.uk/~rjc/rjc.html`.

[Goz97] Gozard, Y., *Théorie de Galois*. Ellipses, 1997.

[Ser70] Serre, J.-P., *Arithmétique*. PUF, 1970.