

Répartition des nombres premiers

Ferdinand Jacobé de Naurois

Table des matières

I Définitions et notations	1
II Méthodes élémentaires pour l'estimation de $\pi(n)$	2
1 Théorème de raréfaction de Legendre	2
2 Encadrements de Tchebychev	3
3 Théorèmes de Mertens	6
a) Le premier et le second théorème de Mertens	6
b) Le troisième théorème de Mertens	8
4 Si $\pi(n) \sim c \frac{n}{\ln(n)}$, alors $c = 1$	13
5 Théorème des nombres premiers par Erdős et Selberg	13
a) La formule de Selberg	13
b) $a + A = 2$ via la formule de Selberg	20
c) Le lemme d'Erdős	21
d) La conclusion de Selberg	26
III Méthodes élémentaires pour l'infinité des $\mathbb{P} \cap A$, où $A \subset \mathbb{N}$	28
1 Postulat de Bertrand	28
2 Théorème de Brun	30
IV Application de l'analyse complexe à l'étude des nombres premiers	34
1 Théorème des nombres premiers	34
a) Préliminaires sur la fonction θ	34
b) Un théorème taubérien d'analyse complexe	36
c) La fonction ζ sur la droite $\Re(z) = 1$ et la conclusion	38
2 Théorème de la progression arithmétique de Dirichlet	41
a) Caractères des groupes abéliens finis	41
b) Preuve de Dirichlet	43
c) Estimation des fonctions L au voisinage de 1	46
V Bibliographie	51

I Définitions et notations

Dans tout ce développement, on notera p_n le n -ième nombre premier, pour tout $n \in \mathbb{N}^*$. On dénotera par la lettre $\mathbb{P}$ l'ensemble des nombres premiers.

Pour tout $x \in \mathbb{R}$ on note $\mathbb{P}_x = \mathbb{P} \cap]-\infty, x]$.

Définition 1

La fonction π de comptage des nombres premiers est définie, pour tout $x \in \mathbb{R}$, par :

$$\pi(x) = |\mathbb{P}_x| = \sum_{p \in \mathbb{P}_x} 1$$

Enfin, la lettre p désignera toujours un nombre premier.

II Méthodes élémentaires pour l'estimation de $\pi(n)$

1 Théorème de raréfaction de Legendre

On commence par un résultat élémentaire découlant des méthodes de cribles, à peine plus évoluées que celles employées par Eratosthène.

Lemme 1 - Crible de Legendre

Soit $n \in \mathbb{N}$ avec $n \geq 2$. On note $p_1, \dots, p_k$ les nombres premiers inclus dans $[1, \sqrt{n}]$. Alors, on a :

$$\pi(n) - \pi(\sqrt{n}) = -1 + \sum_{d|p_1 \dots p_k} \mu(d) \left\lfloor \frac{n}{d} \right\rfloor$$

Démonstration

Théorème 1 - Théorème de raréfaction de Legendre

Pour n au voisinage de $+\infty$, on a :

$$\pi(n) = o(n)$$

Démonstration

On note $(p_n)_{n \geq 1}$ la suite croissante des nombres premiers. On désigne de plus par ϕ la fonction d'Euler. Commençons par démontrer le fait suivant :

$$\prod_{i=1}^n \left(1 - \frac{1}{p_i}\right) \xrightarrow{n \rightarrow +\infty} 0 \quad (*)$$

Soit donc $n \in \mathbb{N}^*$. On a, par développement en série géométrique, le développement du produit étant justifié car tous les termes sont positifs :

$$\prod_{i=1}^n \frac{1}{1 - \frac{1}{p_i}} = \prod_{i=1}^n \left(\sum_{k=0}^{+\infty} \frac{1}{p_i^k} \right) = \sum_{k_1, \dots, k_n \in \mathbb{N}} \frac{1}{p_1^{k_1} \dots p_n^{k_n}}$$

Maintenant, tous les entiers inférieurs ou égaux à n ont tous leurs facteurs premiers parmi $p_1, \dots, p_n$ et donc la somme ci dessus est minorée par $\sum_{k=1}^n \frac{1}{k}$. Ce minorant tendant vers $+\infty$ quand n tend vers $+\infty$, on en déduit bien la limite (*).

Montrons alors à l'aide de ce résultat que : $\frac{\pi(n)}{n} \xrightarrow{n \rightarrow +\infty} 0$.

Soit donc $\epsilon > 0$. On dispose d'après (*) de $N > 0$ tel que :

$$\prod_{i=1}^N \left(1 - \frac{1}{p_i}\right) \leq \frac{\epsilon}{2}$$

Dès lors, soit $n \geq 1$. On note r le reste de la division euclidienne de n par $q = p_1 \dots p_N$. Il vient alors, comme $n + p - r \geq n$:

$$\pi(n) \leq \pi(n + q - r) \leq 1 + \phi(n + q - r)$$

(en utilisant le fait que $\phi(a) \geq \pi(a) - 1$ pour tout $a \geq 1$, puisque les nombres premiers inférieurs à a sont premiers avec a à l'exception peut être de a lui-même).

On a donc, en utilisant la formule classique pour le calcul de ϕ :

$$\frac{\pi(n)}{n} \leq \frac{\phi(n + q - r)}{n} \leq \frac{n + p - r}{n} \prod_{p|n+q-r} \left(1 - \frac{1}{p}\right)$$

où le produit porte sur les nombres premiers divisant $n + q - r$. Or, par définition de r , $p_1, \dots, p_N$ divisent tous $n + q - r$. Et donc on a :

$$\frac{\pi(n)}{n} \leq \frac{n + p - r}{n} \prod_{p|n+q-r} \left(1 - \frac{1}{p}\right) \leq \frac{n + p - r}{n} \prod_{i=1}^N \left(1 - \frac{1}{p_i}\right) \leq \frac{n + p - r}{n} \frac{\epsilon}{2} \leq \frac{n + p}{n} \frac{\epsilon}{2}$$

Pour n assez grand, ce dernier majorant est lui-même majoré par ϵ , ce qui conclut la preuve du théorème de raréfaction.

2 Encadrements de Tchebychev

On va commencer par montrer un lemme de majoration, qui s'avérera bien utile dans la suite :

Lemme 2 - Majoration de la primorielle

Soit $n \in \mathbb{N}^*$. On a :

$$\prod_{p \in \mathbb{P}_n} p \leq 4^n$$

Démonstration

Pour tout $n \in \mathbb{N}^*$, on note :

$$P_n = \prod_{p \in \mathbb{P}_n} p$$

Il est clair que, pour tout $n \in \mathbb{N}^*$, le produit : $\frac{P_{2n+1}}{P_{n+1}} = \prod_{n+2 \leq p \leq 2n+1} p$ divise $\binom{2n+1}{n}$. Dès lors, pour tout $n \in \mathbb{N}^*$, on a :

$$\frac{P_{2n+1}}{P_{n+1}} \leq \binom{2n+1}{n} \leq \frac{1}{2} \left(\binom{2n+1}{n} + \binom{2n+1}{n+1} \right) \leq \frac{1}{2} 2^{2n+1} = 4^n$$

Montrons alors par récurrence forte sur $n \in \mathbb{N}^*$ que pour tout $n \in \mathbb{N}^*$, on a $P_n \leq 4^n$. L'initialisation pour $n = 1$ et $n = 2$ est immédiate. Soit donc $n \geq 3$ tel que pour tout $k \in \llbracket 1, n-1 \rrbracket$, $P_k \leq 4^k$. On distingue deux cas.

Si n est impair avec $n = 2m + 1$, alors par le point précédent et avec l'hypothèse de récurrence forte, on a :

$$P_n \leq 4^m P_{m+1} \leq 4^{m+m+1} = 4^n$$

Si n est pair avec $n = 2m$, alors comme $n \geq 3$, on a (en utilisant l'hypothèse de récurrence au rang $n-1$) :

$$P_n = P_{2m} = P_{2m-1} \geq 4^{2m-1} \geq 4^n$$

Ceci conclut la récurrence. On a donc montré que pour tout $n \in \mathbb{N}^*$, $P_n \leq 4^n$.

Théorème 2 - Majoration de $\pi(n)$ par Tchebychev

On a, pour tout $n \in \mathbb{N}$ tel que $n \geq 2$:

$$\pi(n) \leq e \frac{n}{\ln n}$$

Démonstration

On commence par appliquer le lemme précédent. Soit donc $n \in \mathbb{N}$ avec $n \geq 2$, on a :

$$4^n \geq P_n = \prod_{p \in \mathbb{P}_n} p \geq \pi(n)!$$

D'où, en passant au logarithme :

$$2n \ln(2) \geq \ln(\pi(n)!) \quad (*)$$

Soit maintenant $k \in \mathbb{N}$. On a :

$$\ln(k!) = \sum_{i=1}^n \ln(k) \geq \sum_{i=1}^k \int_{i-1}^i \ln(t) dt = \int_0^k \ln(t) dt = [t \ln(t) - t]_0^k = k(\ln(k) - 1)$$

De (*), on déduit alors que :

$$2n \ln(2) \geq \pi(n)(\ln(\pi(n)) - 1) \quad (**)$$

On considère la fonction ϕ définie par :

$$\begin{aligned} \varphi : \mathbb{R}_+^* &\rightarrow \mathbb{R} \\ x &\mapsto x(\ln(x) - 1) \end{aligned}$$

On a alors la minoration :

$$\varphi\left(e \frac{n}{\ln n}\right) = e \frac{n}{\ln n} \left(\ln \left(e \frac{n}{\ln n} \right) - 1 \right) = e \frac{n}{\ln n} (\ln(n) - \ln(\ln(n))) = en \left(1 - \frac{\ln(\ln(n))}{\ln(n)} \right)$$

Or, la fonction $x \mapsto \frac{\ln(x)}{x}$ admet pour maximum $\frac{1}{e}$, d'où :

$$\varphi\left(e \frac{n}{\ln n}\right) \geq en \left(1 - \frac{1}{e} \right) \geq (e-1)n \geq 2 \ln(2)n$$

En utilisant la relation (**) on a donc :

$$\varphi\left(e \frac{n}{\ln n}\right) \geq \varphi(\pi(n))$$

La stricte croissance de φ permet alors de conclure.

Théorème 3 - Minoration de $\pi(n)$ par Tchebychev

On a pour tout $n \in \mathbb{N}$ tel que $n \geq 2$:

$$\ln(2) \frac{n}{\ln n} \leq \pi(n)$$

Démonstration

Pour tout $n \geq 2$, on note $\mu_n = \text{ppcm}(1, \dots, n)$.

- Commençons par montrer que pour tout $n \in \mathbb{N}$ tel que $n \geq 2$, pour tout $m \in \llbracket 1, n \rrbracket$, $m \binom{n}{m}$ divise μ_n .

Soit donc $n \geq 2$. Soit $m \in \llbracket 1, n \rrbracket$, on note :

$$I_{n,m} = \int_0^1 t^{m-1} (1-t)^{n-m} dt$$

En développant selon le binôme de Newton, il vient :

$$\begin{aligned} I_{n,m} &= \int_0^1 t^{m-1}(1-t)^{n-m} dt = \int_0^1 t^{m-1} \sum_{k=0}^{n-m} \binom{n-m}{k} (-t)^k dt \\ &= \sum_{k=0}^{n-m} \binom{n-m}{k} (-1)^k \int_0^1 t^{m+k-1} dt = \sum_{k=0}^{n-m} \binom{n-m}{k} (-1)^k \frac{1}{m+k} \end{aligned}$$

Et donc en réduisant au même dénominateur, on obtient qu'il existe $\alpha \in \mathbb{Z}$ tel que :

$$I_{n,m} = \frac{\alpha}{\mu_n} \quad (*)$$

Comme clairement, $I_{n,m} > 0$, on a même $\alpha \in \mathbb{N}^*$.

Posons à présent :

$$P_n = \sum_{m=1}^n \binom{n-1}{m-1} I_{n,m} X^{m-1}$$

Il vient alors, pour tout $x \in \mathbb{R} \setminus \{1\}$:

$$\begin{aligned} P_n(x) &= \sum_{m=1}^n \binom{n-1}{m-1} I_{n,m} x^{m-1} = \sum_{m=1}^n \binom{n-1}{m-1} \int_0^1 t^{m-1} (1-t)^{n-m} x^{m-1} dt \\ &= \int_0^1 \sum_{m=1}^n \binom{n-1}{m-1} (xt)^{m-1} (1-t)^{n-m} dt = \int_0^1 \sum_{m=0}^{n-1} \binom{n-1}{m} (xt)^m (1-t)^{n-1-m} dt \\ &= \int_0^1 (xt + (1-t))^{n-1} dt = \int_0^1 ((x-1)t + 1)^{n-1} dt = \frac{1}{n(x-1)} [((x-1)t + 1)^n]_0^1 \\ &= \frac{x^n - 1}{n(x-1)} = \frac{1}{n} \sum_{k=1}^n x^k \end{aligned}$$

Et donc par rigidité des polynômes et identification des coefficients, on a pour tout $m \in \llbracket 1, n \rrbracket$:

$$\binom{n-1}{m-1} I_{n,m} = \frac{1}{n}$$

i.e.

$$I_{n,m} = \frac{1}{m \binom{n}{m}}$$

En identifiant cette relation avec (*), on obtient :

$$\mu_n = \alpha m \binom{n}{m}$$

On a donc bien montré que pour tout $n \geq 2$, tout $m \in \llbracket 1, n \rrbracket$, $m \binom{n}{m}$ divise μ_n .

• Avec ce lemme, on va pouvoir conclure. Soit donc $n \geq 2$. On sait que $n \binom{2n+1}{n} = n \binom{2n+1}{n+1}$ divise μ_{2n+1} et que $(n+1) \binom{2n+1}{n+1}$ divise également μ_{2n+1} . Comme n et $n+1$ sont premiers entre eux, on en déduit aisément que $n(n+1) \binom{2n+1}{n+1} = n(2n+1) \binom{2n}{n}$ divise μ_{2n+1} .

On en déduit les minoration successives :

$$\mu_{2n+1} \geq n(2n+1) \binom{2n}{n} \geq n \sum_{k=0}^{2n} \binom{2n}{k} \geq n \sum_{k=0}^{2n} \binom{2n}{k} = n 4^n \geq 2^{2n+1} \quad (*)$$

Car en effet, pour tout $k \in \llbracket 0, n \rrbracket$, $n! \leq k!(2n-k)!$ par majoration terme à terme, si bien que $\binom{2n}{n} \geq \binom{2n}{k}$.

Or, comme $\mu_{2n+2} \geq \mu_{2n+1}$, on a également, si $n \geq 4$, en utilisant les inégalités (*) :

$$\mu_{2n+2} \geq \mu_{2n+1} \geq n 2^{2n} \geq 4 \cdot 2^{2n} \geq 2^{2n+2}$$

Si bien que pour tout $n \geq 9$, on a $\mu_n \geq 2^n$.

Et donc, pour tout $n \geq 9$, on a les minoration successives :

$$2^n \leq \mu_n = \prod_{p \in \mathbb{P}_n} p^{\lfloor \log_p(n) \rfloor} \leq \prod_{p \in \mathbb{P}_n} p^{\log_p(n)} = n^{\pi(n)}$$

Soit, en passant au logarithme :

$$\ln(2) \frac{n}{\ln n} \leq \pi(n)$$

Ceci restant vrai pour $n \in \llbracket 2, 8 \rrbracket$, on a prouvé le théorème.

3 Théorèmes de Mertens

On va avoir besoin dans la suite d'introduire une nouvelle fonction, plus facile à manier que π .

Définition 2

La fonction γ est définie pour tout $x \in \mathbb{R}$ par :

$$\gamma(x) = \sum_{p \in \mathbb{P}_x} \frac{\ln(p)}{p}$$

a) Le premier et le second théorème de Mertens

Le premier théorème de Mertens est le suivant :

Théorème 4 - Premier théorème de Mertens (die Grossehilfsatz)

Pour $n \in \mathbb{N}$ au voisinage de $+\infty$, on a :

$$\gamma(n) = \ln(n) + O(1)$$

Démonstration

Soit $n \in \mathbb{N}$ avec $n \geq 2$. Soit $p \in \mathbb{P}$. En utilisant la formule de Legendre, on a les encadrements :

$$\frac{n}{p} - 1 \leq \left\lfloor \frac{n}{p} \right\rfloor \leq v_p(n!) = \sum_{k=1}^{+\infty} \left\lfloor \frac{n}{p^k} \right\rfloor \leq \sum_{k=1}^{+\infty} \frac{n}{p^k} = \frac{n}{p} \frac{p}{p-1} = \frac{n}{p} + \frac{n}{p(p-1)}$$

En remarquant que : $n! = \prod_{p \in \mathbb{P}_n} p^{v_p(n!)}$; on en déduit l'encadrement de $\ln(n!)$ suivant :

$$n\gamma(n) - \sum_{p \in \mathbb{P}_n} \ln(p) \leq \ln(n!) = \sum_{p \in \mathbb{P}_n} v_p(n!) \ln(p) \leq n\gamma(n) + n \sum_{p \in \mathbb{P}_n} \frac{\ln(p)}{p(p-1)}$$

Ce qui se réécrit :

$$-n \sum_{p \in \mathbb{P}_n} \frac{\ln(p)}{p(p-1)} + \ln(n!) \leq n\gamma(n) \leq \sum_{p \in \mathbb{P}_n} \ln(p) + \ln(n!)$$

En utilisant le lemme de majoration de la primorielle, ainsi que l'estimation classique $\ln(n!) = n \ln(n) - n + O(1)$, on peut préciser cet encadrement pour n au voisinage de $+\infty$:

$$-n \sum_{p \in \mathbb{P}_n} \frac{\ln(p)}{p(p-1)} + n \ln(n) - n + O(1) \leq n\gamma(n) \leq n \ln(4) + n \ln(n) - n + O(1)$$

Or la série $\sum \frac{\ln(k)}{k(k-1)}$ converge, donc :

$$\sum_{p \in \mathbb{P}_n} \frac{\ln(p)}{p(p-1)} = O(1)$$

Et l'encadrement devient donc :

$$-nO(1) + n \ln(n) - n + O(1) \leq n\gamma(n) \leq n \ln(4) + n \ln(n) - n + O(1)$$

On conclut alors en divisant par n que, pour n au voisinage de $+\infty$, on a :

$$\gamma(n) = \ln(n) + O(1)$$

Et voici le second :

Théorème 5 - Second théorème de Mertens

Il existe une constante réelle M telle que, au voisinage de $+\infty$, on ait :

$$\sum_{p \in \mathbb{P}_n} \frac{1}{p} = \ln(\ln(n)) + M + O\left(\frac{1}{\ln(n)}\right)$$

M est par définition la constante de Meissel-Mertens.

Démonstration

• On considère la suite $(u_n)_{n \geq 3}$ définie par :

$$u_n = \sum_{k=2}^{n-1} \frac{1}{k \ln(k)} - \ln(\ln(n))$$

Développons $u_{n+1} - u_n$ au voisinage de $+\infty$. Il vient :

$$\begin{aligned} u_{n+1} - u_n &= \frac{1}{n \ln(n)} - \ln\left(\frac{\ln(n+1)}{\ln(n)}\right) = \frac{1}{n \ln(n)} + \ln\left(1 + \frac{\ln(n+1) - \ln(n)}{\ln(n)}\right) \\ &= \frac{1}{n \ln(n)} - \ln\left(1 + \frac{\ln(1 + \frac{1}{n})}{\ln(n)}\right) = \frac{1}{n \ln(n)} - \ln\left(1 + \frac{\frac{1}{n} - \frac{1}{2n^2} + o(\frac{1}{n^2})}{\ln(n)}\right) \\ &= \frac{1}{n \ln(n)} - \left(\frac{\frac{1}{n} - \frac{1}{2n^2} + o(\frac{1}{n^2})}{\ln(n)}\right) + \frac{1}{2} \left(\frac{\frac{1}{n} - \frac{1}{2n^2} + o(\frac{1}{n^2})}{\ln(n)}\right)^2 + o\left(\left(\frac{\frac{1}{n} - \frac{1}{2n^2} + o(\frac{1}{n^2})}{\ln(n)}\right)^2\right) \\ &= \frac{1}{2n^2 \ln(n)} + o\left(\frac{1}{n^2 \ln(n)}\right) \end{aligned}$$

Et donc par le lien suite-série, la suite (u_n) converge vers une constante $l \in \mathbb{R}$. On peut préciser le développement. Pour tout $n \geq 3$ au voisinage de $+\infty$, on a par le théorème de sommation des relations de comparaison sur les restes :

$$u_n - l = \sum_{k=n}^{+\infty} (u_k - u_{k+1}) = \sum_{k=n}^{+\infty} O\left(\frac{1}{2k^2 \ln(k)}\right) = \sum_{k=n}^{+\infty} O\left(\frac{1}{k \ln(k)^2}\right) = \sum_{k=n}^{+\infty} O\left(\frac{1}{\ln(k)} - \frac{1}{\ln(k+1)}\right) = O\left(\frac{1}{\ln(n)}\right)$$

• Notons $\mathbf{1}_{\mathbb{P}}$ la fonction de $\mathbb{R}$ dans $\mathbb{R}$ qui prend la valeur 1 en chaque élément de $\mathbb{P}$, et qui vaut 0 partout ailleurs.

Soit maintenant $n \geq 2$. On a, en effectuant une transformation d'Abel :

$$\begin{aligned}
\sum_{p \in \mathbb{P}_n} \frac{1}{p} &= \sum_{k=2}^n \frac{\mathbf{1}_{\mathbb{P}}(n)}{n} = \frac{1}{2} + \sum_{k=3}^n \frac{1}{\ln(k)} \frac{\ln(k) \mathbf{1}_{\mathbb{P}}(k)}{k} = \frac{1}{2} + \sum_{k=3}^n \frac{1}{\ln(k)} (\gamma(k) - \gamma(k-1)) \\
&= \frac{1}{2} + \sum_{k=3}^n \left(\frac{\gamma(k)}{\ln(k)} - \frac{\gamma(k-1)}{\ln(k-1)} + \gamma(k-1) \left(\frac{1}{\ln(k-1)} - \frac{1}{\ln(k)} \right) \right) \\
&= \frac{1}{2} + \frac{\gamma(n)}{\ln(n)} - \frac{\gamma(2)}{\ln(2)} + \sum_{k=3}^n \left(\gamma(k-1) \left(\frac{1}{\ln(k-1)} - \frac{1}{\ln(k)} \right) \right) \\
&= \frac{\gamma(n)}{\ln(n)} + \sum_{k=2}^{n-1} \frac{\gamma(k) \ln(1 + \frac{1}{k})}{\ln(k) \ln(k+1)} \quad (*)
\end{aligned}$$

Or, pour k au voisinage de $+\infty$, on a en utilisant le premier théorème de Mertens :

$$\frac{\gamma(k) \ln(1 + \frac{1}{k})}{\ln(k) \ln(k+1)} = \frac{(\ln(k) + O(1))(\frac{1}{k} + O(\frac{1}{k^2}))}{\ln(k) \ln(k+1)} = \frac{1}{k \ln(k+1)} + O\left(\frac{1}{k \ln(k) \ln(k+1)}\right) = \frac{1}{k \ln(k)} + O\left(\frac{1}{k \ln(k)^2}\right)$$

Et donc par comparaison avec une série de Bertran, la série :

$$\sum \left(\frac{\gamma(k) \ln(1 + \frac{1}{k})}{\ln(k) \ln(k+1)} - \frac{1}{k \ln(k)} \right)$$

converge, et son reste R_n vérifie, au voisinage de $+\infty$:

$$R_n = \sum_{k=n}^{+\infty} \left(\frac{\gamma(k) \ln(1 + \frac{1}{k})}{\ln(k) \ln(k+1)} - \frac{1}{k \ln(k)} \right) = \sum_{k=n}^{+\infty} O\left(\frac{1}{k \ln(k)^2}\right) = \sum_{k=n}^{+\infty} O\left(\frac{1}{\ln(k)} - \frac{1}{\ln(k+1)}\right) = O\left(\frac{1}{\ln(n)}\right)$$

Et donc en utilisant l'expression (*), on obtient l'existence de $l' \in \mathbb{R}$ tel que pour $n \geq 3$:

$$\sum_{p \in \mathbb{P}_n} \frac{1}{p} = \frac{\gamma(n)}{\ln(n)} + \sum_{k=2}^{n-1} \left(\frac{\gamma(k) \ln(1 + \frac{1}{k})}{\ln(k) \ln(k+1)} - \frac{1}{k \ln(k)} \right) + \sum_{k=2}^{n-1} \frac{1}{k \ln(k)} = \frac{\gamma(n)}{\ln(n)} + (l' - R_n) + (u_n + \ln(\ln(n)))$$

Avec l'estimation de R_n , le calcul effectué sur (u_n) ainsi que le premier théorème de Mertens, on obtient alors :

$$\sum_{p \in \mathbb{P}_n} \frac{1}{p} = \ln(\ln(n)) + l + l' + O\left(\frac{1}{\ln(n)}\right)$$

Ce qui achève la preuve.

On remarque immédiatement qu'on peut remplacer n par un réel positif r dans l'énoncé du second théorème de Mertens, puisque pour r réel au voisinage de $+\infty$, on a $\ln(\ln(r)) - \ln(\ln(\lfloor r \rfloor)) = \ln\left(1 + \frac{O(1)}{\ln(r)}\right) = O\left(\frac{1}{\ln(r)}\right)$

b) Le troisième théorème de Mertens

On arrive enfin au troisième théorème de Mertens, qui se présente comme un produit eulérien. Pour le démontrer, on fera appel à la définition de fonction ζ de Riemann sur $]1, +\infty[$. Il est donc temps d'introduire cette définition :

Définition 3

Pour tout réel s strictement supérieur à 1, on pose :

$$\zeta(s) = \sum_{n=0}^{+\infty} \frac{1}{n^s}$$

Et de prouver la formule du produit eulérien pour ζ :

Lemme 3

Soit $s > 1$ réel. On a :

$$\prod_{p \in \mathbb{P}_n} \left(1 - \frac{1}{p^s}\right)^{-1} \xrightarrow{n \rightarrow +\infty} \zeta(s)$$

Ce qu'on notera :

$$\zeta(s) = \prod_{p \in \mathbb{P}} \left(1 - \frac{1}{p^s}\right)^{-1}$$

Démonstration

Soit $s > 1$.

• Pour tout entier strictement positif k , on note $\text{Fac}(k)$ l'ensemble des facteurs premiers de k , et pour tout $p \in \mathbb{P}$, on note $v_p(k)$ la valuation p -adique de k , et $v(k) = \max\{v_p(k) | p \in \mathbb{P}\}$.

Soit $n \in \mathbb{N}^*$. Pour tout $\epsilon > 0$, on peut trouver $N \in \mathbb{N}^*$ tel que :

$$\prod_{p \in \mathbb{P}_n} \left(1 - \frac{1}{p^s}\right)^{-1} \leq \epsilon + \prod_{p \in \mathbb{P}_n} \left(\sum_{v=0}^N p^{-vs}\right) = \epsilon + \sum_{\substack{\text{Fac}(k) \subset \mathbb{P}_n \\ v(k) \leq N}} \frac{1}{k^s} \leq \epsilon + \zeta(s)$$

Où l'indice de sommation varie sur les éléments de $\mathbb{N}^*$ dont tous les facteurs premiers sont inférieurs ou égaux à n , et dont les valuations p -adiques où $p \in \mathbb{P}$ sont toutes inférieures ou égales à N .

Ceci étant vrai pour tout $\epsilon > 0$, on a la majoration suivante, valable pour tout $n \in \mathbb{N}^*$:

$$\prod_{p \in \mathbb{P}_n} \left(1 - \frac{1}{p^s}\right)^{-1} \leq \zeta(s) =$$

Minorons maintenant le produit.

Soit $n \in \mathbb{N}^*$. On a :

$$\prod_{p \in \mathbb{P}_n} \left(1 - \frac{1}{p^s}\right)^{-1} \geq \prod_{p \in \mathbb{P}_n} \left(\sum_{v=0}^n p^{-vs}\right) = \sum_{\substack{\text{Fac}(k) \subset \mathbb{P}_n \\ v(k) \leq n}} \frac{1}{k^s} \geq \sum_{k=1}^n \frac{1}{k^s}$$

La dernière inégalité découlant du théorème fondamental de l'arithmétique et du fait que tous les entiers entre 1 et n ont uniquement des facteurs premiers inférieurs ou égaux à n et des valuations p -adiques inférieures à n pour tout nombre premier p (en effet, pour tout $k \in \llbracket 1, n \rrbracket$ et tout nombre premier p on a : $p^{v_p(k)} \leq k$ d'où $v_p(k) \leq \log_p(k) \leq \log_2(k) \leq k \leq n$).

On a donc montré pour tout $n \in \mathbb{N}^*$ l'encadrement :

$$\sum_{k=1}^n \frac{1}{k^s} \leq \prod_{p \in \mathbb{P}_n} \left(1 - \frac{1}{p^s}\right)^{-1} \leq \zeta(s)$$

Ce qui prouve le lemme.

Forts de cette formule de produit eulérien, on peut enfin énoncer et prouver le troisième de Mertens :

Théorème 6 - Troisième théorème de Mertens

Pour tout $n \geq 2$, on a au voisinage de $+\infty$ l'équivalent :

$$\prod_{p \in \mathbb{P}_n} \left(1 - \frac{1}{p}\right) \sim \frac{e^{-\gamma}}{\ln(n)}$$

où γ désigne la constante d'Euler-Mascheroni.

Démonstration

• On a, pour p au voisinage de $+\infty$ le développement limité : $e^{\frac{1}{p}}(1 - \frac{1}{p}) = (1 + \frac{1}{p} + O(\frac{1}{p^2}))(1 - \frac{1}{p}) = 1 + O(\frac{1}{p^2})$

Dès lors, par un passage au logarithme, le produit infini portant sur les nombres premiers : $\prod e^{\frac{1}{p}}(1 - \frac{1}{p})$ converge vers une constante réelle m , et on a d'après le second théorème de Mertens l'équivalent au voisinage de $+\infty$:

$$\prod_{p \in \mathbb{P}_n} \left(1 - \frac{1}{p}\right) = e^{-\ln(\ln(n)) - M + o(1)} \prod_{p \in \mathbb{P}_n} e^{\frac{1}{p}} \left(1 - \frac{1}{p}\right) \sim \frac{e^{-M} m}{\ln(n)}$$

Notons que cette formule reste valable en remplaçant $n \in \mathbb{N}^*$ par $r \in \mathbb{R}^*$. En effet, le terme de gauche prend la même valeur en r et en $\lfloor r \rfloor$, et on a clairement $\ln(r) \sim \ln(\lfloor r \rfloor)$.

Il s'agit donc d'évaluer la constante m vérifiant :

$$e^M \ln(r) \prod_{p \in \mathbb{P}_r} \left(1 - \frac{1}{p}\right) \xrightarrow{r \rightarrow +\infty} m$$

• On va commencer par rapprocher le produit qui nous occupe des produits eulériens plus généraux pour la fonction γ , qui eux sont convergents. Par définition de m en effectuant le changement de variable $r = e^{1/t}$, on a pour t au voisinage de 0^+ :

$$m \sim e^M \frac{1}{t} \prod_{p \in \mathbb{P}_{e^{1/t}}} (1 - p^{-1}) = e^M \frac{\zeta(1+t)}{t} \prod_{p \in \mathbb{P}_{e^{1/t}}} \frac{1 - p^{-1}}{1 - p^{-1-t}} \prod_{\substack{p \in \mathbb{P} \\ p > e^{1/t}}} \frac{1}{1 - p^{-1-t}}$$

Or, classiquement, on a pour t au voisinage de 0 :

$$\left| \zeta(1+t) - \frac{1}{t} \right| = \sum_{k=1}^{+\infty} \left(\frac{1}{k^{1+t}} - \int_k^{k+1} \frac{1}{x^{1+t}} dx \right) \leq \sum_{k=1}^{+\infty} \left(\frac{1}{k^{1+t}} - \frac{1}{(k+1)^{1+t}} \right) = O(1)$$

Si bien que l'expression précédente se simplifie en :

$$m \sim e^M \prod_{p \in \mathbb{P}_{e^{1/t}}} \frac{1 - p^{-1}}{1 - p^{-1-t}} \prod_{\substack{p \in \mathbb{P} \\ p > e^{1/t}}} \frac{1}{1 - p^{-1-t}}$$

Et donc, en posant pour tout réel positif x , $f(x) = \ln(1+x) - x$, on a :

$$\begin{aligned} \ln(m) &= M - \sum_{p \in \mathbb{P}_{e^{1/t}}} \ln \left(\frac{1 - p^{-1-t}}{1 - p^{-1}} \right) - \sum_{\substack{p \in \mathbb{P} \\ p > e^{1/t}}} \ln(1 - p^{-1-t}) + o(1) \\ &= M - \sum_{p \in \mathbb{P}_{e^{1/t}}} \ln \left(1 + \frac{p^{-1} - p^{-1-t}}{1 - p^{-1}} \right) - \sum_{\substack{p \in \mathbb{P} \\ p > e^{1/t}}} \ln(1 - p^{-1-t}) + o(1) \\ &= M - \sum_{p \in \mathbb{P}_{e^{1/t}}} \ln \left(1 + \frac{1 - p^{-t}}{p - 1} \right) - \sum_{\substack{p \in \mathbb{P} \\ p > e^{1/t}}} \ln(1 - p^{-1-t}) + o(1) \\ &= M - \sum_{p \in \mathbb{P}_{e^{1/t}}} \frac{1 - p^{-t}}{p - 1} + \sum_{p \in \mathbb{P}_{e^{1/t}}} f \left(\frac{1 - p^{-t}}{p - 1} \right) + \sum_{\substack{p \in \mathbb{P} \\ p > e^{1/t}}} p^{-1-t} + \sum_{\substack{p \in \mathbb{P} \\ p > e^{1/t}}} f(p^{-1-t}) + o(1) \end{aligned}$$

Majorons les deux sommes faisant intervenir f , en remarquant que, classiquement, pour tout réel positif x , on a $0 \leq f(x) \leq \frac{x^2}{2} \leq x^2$, et en utilisant l'inégalité de convexité élémentaire $1 - k^{-t} \leq t \ln(k)$ valable pour tout $k > 1$ et $t \geq 0$. On a d'une part :

$$0 \leq \sum_{p \in \mathbb{P}_{e^{1/t}}} f \left(\frac{1 - p^{-t}}{p - 1} \right) \leq \sum_{2 \leq k \leq e^{1/t}} \frac{(1 - k^{-t})^2}{(k - 1)^2} \leq \sum_{2 \leq k \leq e^{1/t}} \frac{(t \ln(k))^2}{(k - 1)^2} \leq t^2 \sum_{k=2}^{+\infty} \frac{\ln(k)^2}{(k - 1)^2} = O(t^2)$$

Et d'autre part :

$$0 \leq \sum_{\substack{p \in \mathbb{P} \\ p > e^{1/t}}} f(p^{-1-t}) \leq \sum_{k > e^{1/t}} k^{-2-2t} \leq k^{-2} \sum_{k \lfloor e^{1/t} \rfloor}^{+\infty} k^{-2t} = \frac{k^{-2-\lfloor e^{1/t} \rfloor} = o(1)}{1 - k^{-2}}$$

Donc ces deux sommes tendent vers 0 quant t tend vers 0. Donc pour t au voisinage de 0, on a l'estimation :

$$\ln(m) = M - \sum_{\substack{p \in \mathbb{P} \\ p > e^{1/t}}} \frac{1-p^{-t}}{p-1} + \sum_{\substack{p \in \mathbb{P} \\ p > e^{1/t}}} p^{-1-t} + o(1)$$

De plus, en remarquant que pour tout $t > 0$, on a :

$$0 \leq \sum_{p \in \mathbb{P}_{e^{1/t}}} \left(\frac{1-p^{-t}}{p-1} - \frac{1-p^{-t}}{p} \right) = \sum_{p \in \mathbb{P}_{e^{1/t}}} \frac{1-p^{-t}}{p(p-1)} \leq t \sum_{p \in \mathbb{P}_{e^{1/t}}} \frac{\ln(p)}{p(p-1)} \leq t \sum_{k=2}^{+\infty} \frac{\ln(k)}{k(k-1)}$$

On obtient finalement une forme très simple :

$$\ln(m) = M - \sum_{\substack{p \in \mathbb{P} \\ p > e^{1/t}}} \frac{1-p^{-t}}{p} + \sum_{\substack{p \in \mathbb{P} \\ p > e^{1/t}}} p^{-1-t} + o(1) \quad (*)$$

• Posons :

$$A(t) = \sum_{\substack{p \in \mathbb{P} \\ p > e^{1/t}}} \frac{1-p^{-t}}{p} \quad \text{et} \quad B(t) = \sum_{\substack{p \in \mathbb{P} \\ p > e^{1/t}}} p^{-1-t}$$

Et tâchons d'estimer B et A au voisinage de 0. On a pour tout $t > 0$, par une interversion de somme finie et d'intégrale :

$$\begin{aligned} A(t) &= \sum_{p \in \mathbb{P}_{e^{1/t}}} \frac{t}{p} \int_1^p \frac{dx}{x^{t+1}} = t \int_1^{e^{1/t}} \sum_{x < p \leq e^{1/t}} \frac{dx}{px^{t+1}} = t \int_1^{e^{1/t}} \frac{1}{x^{t+1}} \left(\sum_{x < p \leq e^{1/t}} \frac{1}{p} \right) dx \\ B(t) &= \sum_{\substack{p \in \mathbb{P} \\ p > e^{1/t}}} \frac{t}{p} \int_p^{+\infty} \frac{dx}{x^{1+t}} = t \int_{e^{1/t}}^{+\infty} \sum_{e^{1/t} < p \leq x} \frac{dx}{px^{t+1}} = t \int_{e^{1/t}}^{+\infty} \frac{1}{x^{t+1}} \left(\sum_{e^{1/t} < p \leq x} \frac{1}{p} \right) dx \end{aligned}$$

Et donc, en utilisant le second théorème de Mertens et le développement classique de la série harmonique, il vient :

$$\begin{aligned} A(t) &= t \int_1^{e^{1/t}} \frac{1}{x^{t+1}} \left(\ln \ln(e^{1/t}) - \ln \ln(x) + O\left(\frac{1}{\ln(x)}\right) \right) dx = t \int_1^{e^{1/t}} \frac{1}{x^{t+1}} \left(\sum_{\ln(x) < k \leq \frac{1}{t}} \frac{1}{k} + O\left(\frac{1}{\ln(x)}\right) \right) dx \\ &= t \sum_{0 < k \leq \frac{1}{t}} \frac{1}{k} \int_1^{e^k} \frac{dx}{x^{t+1}} + t \int_1^{e^{1/t}} \frac{1}{x^{t+1}} O\left(\frac{1}{\ln(x)}\right) dx = \sum_{1 \leq k \leq \frac{1}{t}} \frac{1-e^{-tk}}{k} + t \int_1^{e^{1/t}} \frac{1}{x^{t+1}} O\left(\frac{1}{\ln(x)}\right) dx \\ B(t) &= t \int_{e^{1/t}}^{+\infty} \frac{1}{x^{t+1}} \left(\ln \ln(x) - \ln \ln(e^{1/t}) + O(e^{-1/t}) \right) dx = t \int_{e^{1/t}}^{+\infty} \frac{1}{x^{t+1}} \left(\sum_{\frac{1}{t} < k \leq \ln(x)} \frac{1}{k} + O(e^{-1/t}) \right) dx \\ &= t \sum_{k > \frac{1}{t}} \frac{1}{k} \int_{e^k}^{+\infty} \frac{dx}{x^{t+1}} + t \int_{e^{1/t}}^{+\infty} \frac{O(e^{-1/t})}{x^{t+1}} dx = \sum_{k > \frac{1}{t}} \frac{e^{-kt}}{k} + t \int_{e^{1/t}}^{+\infty} \frac{O(e^{-1/t})}{x^{t+1}} dx \end{aligned}$$

Il s'agit maintenant d'évaluer les restes qui apparaissent sous forme d'intégrales. On sait qu'il existe des constantes positives C, D, E telles que pour tout $t > 0$, on ait :

$$\begin{aligned} \left| t \int_1^{e^{1/t}} \frac{1}{x^{t+1}} O\left(\frac{1}{\ln(x)}\right) dx \right| &\leq Dt + Ct \int_2^{e^{1/t}} \frac{1}{x^{t+1} \ln(x)} dx = Dt + Ct \left[\ln\left(\frac{1}{t}\right) - \ln(\ln(2)) \right] + Ct^2 \int_2^{e^{1/t}} \frac{\ln(\ln(x))}{x^{t+1}} dx \\ &= O(t \ln(t)) + Ct^2 \int_2^{e^{1/t}} \frac{Ex}{x^{t+1}} dx = O(t \ln(t)) + CEt^2 \int_2^{e^{1/t}} \frac{dx}{x} \\ &= O(t \ln(t)) + CEt^2 (\ln(e^{1/t}) - \ln(2)) = O(t \ln(t)) = o(1) \end{aligned}$$

Et de même :

$$\left| t \int_{e^{1/t}}^{+\infty} \frac{O(e^{-1/t})}{x^{t+1}} dx \right| \leq Cte^{-1/t} \left(\frac{1}{t} (e^{1/t})^{-t} \right) \leq Ce^{-1-1/t} = o(1)$$

Si bien que finalement, en repartant de l'expression (*) et en utilisant nos estimations de A et B :

$$\begin{aligned} \ln(m) &= M - A(t) + B(t) + o(1) = M - \sum_{1 \leq k < 1/t} \frac{1 - e^{-tk}}{k} + \sum_{k > 1/t} \frac{e^{-tk}}{k} + o(1) \\ &= M - \sum_{1 \leq k < 1/t} \frac{1}{k} + \sum_{k=1}^{+\infty} \frac{e^{-tk}}{k} = M - \ln \left(\left\lfloor \frac{1}{t} \right\rfloor \right) - \gamma + o(1) - \ln(1 - e^{-t}) + o(1) \\ &= M - \gamma + \ln \left(\frac{1 - e^{-t}}{t} \right) + o(1) = M - \gamma + o(1) \end{aligned}$$

Et donc finalement, on a $m = e^{M-\gamma}$. Et donc en remplaçant cette valeur dans l'estimation du produit trouvée au début de la preuve, on obtient le troisième théorème de Mertens :

$$\prod_{p \in \mathbb{P}_n} \left(1 - \frac{1}{p} \right) \sim \frac{e^{-\gamma}}{\ln(n)}$$

Forêts de ce résultat, on peut sans grand effort en déduire d'autres similaires :

Corollaire 1

Pour tout $n \leq 2$, on a au voisinage de $+\infty$ l'équivalent :

$$\prod_{p \in \mathbb{P}_n} \left(1 + \frac{1}{p} \right) \sim \frac{6e^{\gamma}}{\pi^2} \ln(n)$$

Démonstration

En effet, pour tout $n \leq 2$, on a au voisinage de $+\infty$ les équivalents suivants, en utilisant d'une part le lemme du produit eulérien, et d'autre part le troisième théorème de Mertens :

$$\prod_{p \in \mathbb{P}_n} \left(1 + \frac{1}{p} \right) = \frac{\prod_{p \in \mathbb{P}_n} \left(1 - \frac{1}{p^2} \right)}{\prod_{p \in \mathbb{P}_n} \left(1 - \frac{1}{p} \right)} \sim \frac{\ln(n)}{\zeta(2)e^{-\gamma}} = \frac{6e^{\gamma}}{\pi^2} \ln(n)$$

Un corollaire du troisième théorème de Mertens donne également une expression de la constante de Meissel-Mertens :

Corollaire 2

En notant M la constante de Meissel-Mertens, on a :

$$M = \gamma + \sum_{p \in \mathbb{P}} \left(\ln \left(1 - \frac{1}{p} \right) + \frac{1}{p} \right)$$

Démonstration

En effet, en reprenant les notations de la démonstration du troisième théorème de Mertens, on a par définition de m :

$$m = \prod_{p \in \mathbb{P}} e^{\frac{1}{p}} \left(1 - \frac{1}{p} \right)$$

Et le résultat prouvé est :

$$\ln(m) = M - \gamma$$

Il suffit donc de passer au logarithme dans la définition de m pour conclure.

4 Si $\pi(n) \sim c \frac{n}{\ln(n)}$, alors $c = 1$

Ce fait, qui porte le nom de Théorème de Tchebychev, est en fait une conséquence du second théorème de Mertens.

Théorème 7 - Théorème de Tchebychev

Si il existe une constante réelle c telle que pour $n \geq 2$ au voisinage de $+\infty$, on ait :

$$\pi(n) \sim c \frac{n}{\ln(n)}$$

alors $c = 1$.

Démonstration

Supposons l'existence de $c \in \mathbb{R}$ tel que pour $n \geq 2$ au voisinage de $+\infty$, on ait :

$$\pi(n) \sim c \frac{n}{\ln(n)}$$

Soit alors $n \geq 2$. On a, en conservant la notation $\mathbf{1}_{\mathbb{P}}$ introduite dans la section précédente :

$$\begin{aligned} \sum_{p \in \mathbb{P}_n} \frac{1}{p} &= \sum_{k=2}^n \frac{\mathbf{1}_{\mathbb{P}}(k)}{k} = \sum_{k=2}^n \frac{\pi(k) - \pi(k-1)}{k} = \sum_{k=2}^n \left(\frac{\pi(k)}{k} - \frac{\pi(k-1)}{k-1} + \pi(k-1) \left(\frac{1}{k-1} - \frac{1}{k} \right) \right) \\ &= \frac{\pi(n)}{n} + \sum_{k=1}^{n-1} \frac{\pi(k)}{k(k+1)} \end{aligned}$$

Alors, on a pour k au voisinage de $+\infty$:

$$\frac{\pi(k)}{k(k+1)} \sim \frac{c}{k \ln(k)}$$

Ceci étant le terme générale d'une série positive divergente, le théorème de sommation des équivalents s'applique. Il vient alors, pour n au voisinage de $+\infty$:

$$\sum_{p \in \mathbb{P}_n} \frac{1}{p} = \frac{\pi(n)}{n} + \sum_{k=1}^{n-1} \frac{\pi(k)}{k(k+1)} = \sum_{k=1}^{n-1} \frac{c}{k \ln(k)} + o\left(\sum_{k=1}^{n-1} \frac{1}{k \ln(k)}\right)$$

Or, un calcul déjà effectué dans la preuve du second théorème de Mertens montre que :

$$\sum_{k=1}^{n-1} \frac{1}{k \ln(k)} = \ln(\ln(n)) + o(\ln(\ln(n)))$$

Si bien que :

$$\sum_{p \in \mathbb{P}_n} \frac{1}{p} = c \ln(\ln(n)) + o(\ln(\ln(n)))$$

On conclut par le second théorème de Mertens.

5 Théorème des nombres premiers par Erdős et Selberg

a) La formule de Selberg

On définit la fonction θ , plus facile à estimer que la fonction π , de la façon suivante :

Définition 4

Pour tout $x \geq 0$, on pose :

$$\theta(x) = \sum_{p \leq x} \ln(p)$$

où la somme est prise sur les entiers inférieurs ou égaux à p .

L'intérêt de la fonction θ est qu'un équivalent de θ suffit à obtenir un équivalent de π , comme le montre le lemme suivant.

Lemme 4

On a, pour x qui tend vers $+\infty$:

$$\frac{\theta(x)}{\pi(x) \ln(x)} \xrightarrow{x \rightarrow +\infty} 1$$

Démonstration

Soit $\epsilon > 0$. On a pour tout $x \geq 1$, les sommes étant prises sur les nombres premiers :

$$\ln(x^{1-\epsilon})(\pi(x) - \pi(x^{1-\epsilon})) \sum_{x^{1-\epsilon} < p \leq x} \ln(p) \leq x \leq \theta(x) = \sum_{p \leq x} \ln(p) \leq \ln(x)\pi(x)$$

Or, on a clairement pour $x \rightarrow +\infty$ l'estimation suivante, avec les encadrements de Tchebychev :

$$\pi(x^{1-\epsilon}) = O\left(\frac{x^{1-\epsilon}}{\ln(x)}\right) = o\left(\frac{x}{\ln(x)}\right) = o(\pi(x))$$

Et donc l'encadrement ci dessus devient, après division par $\ln(x)\pi(x)$:

$$(1 - \epsilon)(1 + o(1)) \leq \frac{\theta(x)}{\ln(x)\pi(x)} \leq 1$$

Ceci conclut la preuve du lemme.

Voici la formule de Selberg :

Théorème 8

Pour x au voisinage de $+\infty$, on a :

$$\theta(x) \ln(x) + \sum_{p \leq x} \theta\left(\frac{x}{p}\right) \ln(p) = 2x \ln(x) + O(x \ln(\ln(x)))$$

où la somme est évidemment prise sur les nombres premiers.

La démonstration repose sur l'estimation de deux manières différentes de la somme $S(x)$ définie ci-dessous.

Définition 5

Pour tout $x \geq 1$, on pose :

$$S(x) = \sum_{1 \leq n \leq x} \sum_{d|n} \mu(d) \ln \left(\frac{x}{d} \right)^2$$

où μ est la fonction de Moebius définie sur $\mathbb{N}^*$ par :

$$\begin{aligned} \mu(n) &= 0 \quad \text{si } n \text{ est divisible par un carré parfait autre que } 1 \\ \mu(p_1 \dots p_r) &= (-1)^r \quad \text{si } p_1, \dots, p_r \text{ sont des nombres premiers distincts} \\ \mu(1) &= 1 \end{aligned}$$

On estime de deux manières cette somme au voisinage de $+\infty$, et on identifie les deux estimations pour obtenir la formule de Selberg.

Voici la première manière dont Selberg estime la somme $S(x)$:

Lemme 5

Pour x au voisinage de $+\infty$, on a :

$$S(x) = \theta(x) \ln(x) + \sum_{p \leq x} \theta \left(\frac{x}{p} \right) \ln(p) + O(x \ln(\ln(x)))$$

Démonstration

On va regarder de près la valeur de chacun des termes n de la somme. Commençons par le cas où n a au moins 3 facteurs premiers. Soit donc n un entier qui contient $r \geq 3$ facteurs premiers. On note $n = p_1^{a_1} \dots p_r^{a_r}$ où les p_i sont premiers distincts et où les a_i sont dans $\mathbb{N}^*$. Il vient alors, comme $\mu(d)$ s'annule dès que d est divisible par p_i^2 pour un certain i :

$$\begin{aligned} \sum_{d|n} \mu(d) \ln \left(\frac{x}{d} \right)^2 &= \sum_{d|p_1 \dots p_r} \mu(d) \ln \left(\frac{x}{d} \right)^2 = \sum_{I \subset \llbracket 1, r \rrbracket} (-1)^{|I|} \ln \left(n \prod_{i \in I} \frac{1}{p_i} \right)^2 = \sum_{I \subset \llbracket 1, r \rrbracket} (-1)^{|I|} \left(\ln(n) - \sum_{i \in I} \ln(p_i) \right)^2 \\ &= \sum_{I \subset \llbracket 1, r \rrbracket} (-1)^{|I|} \ln(n)^2 - \ln(n) \sum_{I \subset \llbracket 1, r \rrbracket} (-1)^{|I|} \sum_{i \in I} \ln(p_i) + \sum_{I \subset \llbracket 1, r \rrbracket} (-1)^{|I|} \sum_{i, j \in I} \ln(p_i) \ln(p_j) \\ &= -\ln(n) \sum_{i=1}^r \ln(p_i) \left(\sum_{\substack{I \subset \llbracket 1, r \rrbracket \\ i \in I}} (-1)^{|I|} \right) + \sum_{i=1}^r \ln(p_i)^2 \left(\sum_{\substack{I \subset \llbracket 1, r \rrbracket \\ i \in I}} (-1)^{|I|} \right) + \sum_{\substack{1 \leq i, j \leq r \\ i \neq j}} \ln(p_i) \ln(p_j) \left(\sum_{\substack{I \subset \llbracket 1, r \rrbracket \\ i, j \in I}} (-1)^{|I|} \right) \end{aligned}$$

Maintenant, comme $r \geq 3$, les trois sommes portant sur $|I|$ sont nulles et donc finalement :

$$\sum_{d|n} \mu(d) \ln \left(\frac{x}{d} \right)^2 = 0$$

Dès lors, on a le calcul suivant de la somme ci-dessus dans le cas général :

$$\sum_{d|n} \mu(d) \ln \left(\frac{x}{d} \right)^2 = \begin{cases} \ln(x)^2 & \text{si } n = 1 \\ -\ln(p)^2 + 2 \ln(x) \ln(p) & \text{si } n = p^h \text{ avec } p \text{ premier, } h \geq 1 \\ 2 \ln(p) \ln(q) & \text{si } n = p^h q^k \text{ avec } p, q \text{ premiers distincts et } k, h \geq 1 \\ 0 & \text{sinon} \end{cases}$$

Et donc on a, pour $x \geq 1$:

$$S(x) = \ln(x)^2 + \sum_{p^h \leq x} -\ln(p)^2 + 2 \ln(x) \ln(p) + 2 \sum_{\substack{p^h q^k \leq x \\ p < q}} \ln(p) \ln(q) \quad (*)$$

où dans les indices de sommations, les entiers p et q sont premiers distincts, et $h, k \in \mathbb{N}^*$.

Dans cette expression de S , les entiers qui ne sont pas de la forme p ou pq (avec p, q premiers distincts) fournissent une contribution en $O(x)$. En effet, on a d'une part, pour x au voisinage de l'infini :

$$\begin{aligned} \left| \sum_{\substack{p \in \mathbb{P}, h \geq 2 \\ p^h \leq x}} -\ln(p)^2 + 2\ln(x)\ln(p) \right| &\leq 3\ln(x) \sum_{\substack{p \in \mathbb{P}, h \geq 2 \\ p^h \leq x}} \ln(p) \\ &\leq 3\ln(x) \sum_{p \leq \sqrt{x}} \ln(p) \sum_{\substack{h \geq 2 \\ p^h \leq x}} 1 \leq 3\ln(x) \sum_{p \leq \sqrt{x}} \ln(p) \frac{\ln(x)}{\ln(p)} = O(\sqrt{x} \ln(x)^2) \end{aligned}$$

Et d'autre part, toujours pour x au voisinage de $+\infty$:

$$\begin{aligned} \sum_{\substack{p^h q^k \leq x \\ p < q \\ h \geq 2 \text{ ou } k \geq 2}} \ln(p) \ln(q) &\leq 2 \sum_{\substack{p^h \leq x \\ h \geq 2}} \ln(p) \sum_{q \leq \frac{x}{p^h}} \ln(q) + \sum_{\substack{p^h q^k \leq x \\ p < q \\ h \geq 2 \text{ et } k \geq 2}} \ln(p) \ln(q) \\ &\leq 2 \sum_{p \leq \sqrt{x}} \ln(p) \sum_{2 \leq h \leq \frac{\ln(x)}{\ln(p)}} \theta\left(\frac{x}{p^h}\right) + \sum_{p, q \leq \sqrt{x}} \ln(p) \ln(q) \sum_{h \leq \frac{\ln(x)}{\ln(p)}} \sum_{k \leq \frac{\ln(x)}{\ln(q)}} 1 \\ &\leq C_1 \sum_{p \leq \sqrt{x}} \sum_{h \geq 2} \ln(p) \frac{x}{p^h} + \sum_{p, q \leq \sqrt{x}} \ln(x)^2 \leq C_1 x \sum_{n \geq 2} \sum_{h \geq 2} \frac{\ln(n)}{n^h} + \ln(x)^2 \pi(\sqrt{x})^2 \end{aligned}$$

Où on a utilisé le lemme 4 et les majorations de Tchebychev pour obtenir $\theta(x) = O(x)$. Maintenant, on constate aisément que la famille $\left(\frac{\ln(n)}{n^h}\right)_{n, h \geq 2}$ est sommable : on a en effet :

$$\sum_{n \geq 2} \sum_{h \geq 2} \frac{\ln(n)}{n^h} = \sum_{n \geq 2} \ln(n) \sum_{h \geq 2} \frac{1}{n^h} = \sum_{n \geq 2} \frac{\ln(n)}{n^2 - n} = \sum_{n \geq 2} O(\ln(n) n^{-2})$$

Et donc avec les majorations de Tchebychev, la majoration ci-dessus devient asymptotiquement :

$$\sum_{\substack{p^h q^k \leq x \\ p < q \\ h \geq 2 \text{ ou } k \geq 2}} \ln(p) \ln(q) = O(x)$$

Et donc on peut ré-écrire la formule asymptotique (*) sous la forme :

$$S(x) = \sum_{p \leq x} (-\ln(p)^2 + 2\ln(x)\ln(p)) + 2 \sum_{\substack{pq \leq x \\ p < q}} \ln(p) \ln(q) + O(x) \quad (**)$$

où p et q dans la deuxième somme sont des nombres premiers distincts.

Évaluons ces deux sommes.

En premier lieu, on a :

$$\sum_{p \leq x} (-\ln(p)^2 + 2\ln(x)\ln(p)) = \ln(x) \sum_{p \leq x} \ln(p) + \sum_{p \leq x} \ln(p) \ln\left(\frac{x}{p}\right) = \ln(x)\theta(x) + \sum_{p \leq x} \ln(p) \ln\left(\frac{x}{p}\right)$$

Avec :

$$\begin{aligned} \sum_{p \leq x} \ln(p) \ln\left(\frac{x}{p}\right) &\leq \sum_{p \leq \frac{x \ln(\ln(x))}{\ln(x)}} \ln(p) \ln\left(\frac{x}{p}\right) + \sum_{p \leq x} \ln(p) \ln\left(\frac{\ln(x)}{\ln(\ln(x))}\right) \\ &\leq \sum_{p \leq \frac{x \ln(\ln(x))}{\ln(x)}} \ln(p) \ln(x) + \sum_{p \leq x} \ln(p) \ln(\ln(x)) \leq \ln(x)\theta\left(\frac{x \ln(\ln(x))}{\ln(x)}\right) + \ln(\ln(x))\theta(x) \end{aligned}$$

Avec les majorations de Tchebychev et le lemme 4, on a $\theta(x) = O(x)$ et donc ce dernier majorant est un $O(\ln(\ln(x)))$. On obtient donc pour x au voisinage de $+\infty$:

$$\sum_{p \leq x} (-\ln(p)^2 + 2\ln(x)\ln(p)) = \ln(x)\theta(x) + O(x\ln(\ln(x))) \quad (1)$$

Il est temps d'évaluer la deuxième somme de la formule (**). On a :

$$2 \sum_{\substack{pq \leq x \\ p < q}} \ln(p)\ln(q) = \sum_{pq \leq x} \ln(p)\ln(q) - \sum_{p \leq \sqrt{x}} \ln(p)^2 = \sum_{p \leq x} \theta\left(\frac{x}{p}\right) \ln(p) + O(\sqrt{x}\ln(x)^2) \quad (2)$$

Avec (1) et (2), la formule asymptotique (**) devient alors :

$$S(x) = \theta(x)\ln(x) + \sum_{p \leq x} \theta\left(\frac{x}{p}\right) \ln(p) + O(x\ln(\ln(x)))$$

C'est bien ce qu'il fallait démontrer.

Passons maintenant à la seconde estimation de Selberg.

Lemme 6

Pour x au voisinage de $+\infty$, on a :

$$S(x) = 2x\ln(x) + O(x)$$

Démonstration

La suite de terme général $u_n = \frac{1}{n} + \ln(n) - \ln(n+1)$ vérifie $u_n = O\left(\frac{1}{n^2}\right)$, et donc la série des u_n converge et son reste est en $O\left(\frac{1}{n}\right)$ à l'infini. On en déduit aisément l'existence d'une constante absolue c_1 telle que pour x tendant vers $+\infty$:

$$\sum_{m \leq x} \frac{1}{m} = \ln(x) + c_1 + O\left(\frac{1}{x}\right) = \ln(x) + c_1 + O\left(\frac{1}{x^{\frac{1}{4}}}\right)$$

En observant que $\frac{1}{2}(\ln(n+1)^2 - \ln(n)^2) = \frac{\ln(n)}{n} + O\left(\frac{\ln(n)}{n^2}\right)$ et en sommant les relations de comparaisons, et par une simple estimation du reste, on obtient de même l'existence d'une constante c_2 telle que :

$$\sum_{m \leq x} \frac{\ln(m)}{m} = \frac{1}{2}\ln(x)^2 + c_2 + O\left(\frac{1}{x^{\frac{1}{4}}}\right)$$

Si maintenant $\tau(m)$ désigne le nombre de diviseurs de m , on a :

$$\begin{aligned} \sum_{m \leq x} \frac{\tau(m)}{m} &= \sum_{m \leq x} \sum_{d|m} \frac{1}{d} = \sum_{ab \leq x} \frac{1}{ab} = \sum_{1 \leq a \leq x} \frac{1}{a} \sum_{1 \leq b \leq \frac{x}{a}} \frac{1}{b} = \sum_{1 \leq a \leq x} \frac{1}{a} \ln\left(\frac{x}{a}\right) + \frac{c_1}{a} + \frac{1}{a} O\left(\frac{a^{\frac{1}{4}}}{x^{\frac{1}{4}}}\right) \\ &= \ln(x) \sum_{1 \leq a \leq x} \frac{1}{a} - \sum_{1 \leq a \leq x} \frac{\ln(a)}{a} + \sum_{1 \leq a \leq x} \frac{c_1}{a} + \sum_{1 \leq a \leq x} O\left(\frac{1}{a^{\frac{3}{4}}x^{\frac{1}{4}}}\right) \\ &= \ln(x)^2 + c_1 \ln(x) + O\left(\frac{\ln(x)}{x}\right) - \frac{1}{2}\ln(x)^2 - c_2 + O\left(\frac{1}{x^{\frac{1}{4}}}\right) + c_1 \ln(x) + c_1^2 + O\left(\frac{1}{x^{\frac{1}{4}}}\right) \\ &= \frac{1}{2}\ln(x)^2 + 2c_1 \ln(x) + c_1^2 - c_2 + O\left(\frac{1}{x^{\frac{1}{4}}}\right) \end{aligned}$$

Et donc on dispose de constantes c_3 et c_4 telles que :

$$\ln(x)^2 = 2 \sum_{m \leq x} \frac{\tau(m)}{m} + c_3 \sum_{m \leq x} \frac{1}{m} + c_5 + O\left(\frac{1}{x^{\frac{1}{4}}}\right) \quad (*)$$

Ensuite, on peut ré-écrire $S(x)$ ainsi :

$$S(x) = \sum_{n \leq x} \sum_{d|n} \mu(d) \ln \left(\frac{x}{d} \right)^2 = \sum_{d \leq x} \mu(d) \ln \left(\frac{x}{d} \right)^2 \sum_{\substack{1 \leq n \leq x \\ d|n}} 1 = \sum_{1 \leq d \leq x} \mu(d) \ln \left(\frac{x}{d} \right)^2 \left\lfloor \frac{x}{d} \right\rfloor$$

On voudrait se débarrasser de la partie entière. Or, on a :

$$\sum_{1 \leq d \leq x} \mu(d) \ln \left(\frac{x}{d} \right)^2 \left(\left\lfloor \frac{x}{d} \right\rfloor - \frac{x}{d} \right) = O \left(\sum_{1 \leq d \leq x} (\ln(x) - \ln(d))^2 \right)$$

Avec :

$$\begin{aligned} \sum_{1 \leq d \leq x} (\ln(x) - \ln(d))^2 &= \lfloor x \rfloor \ln(x)^2 + \sum_{1 \leq d \leq x} \ln(d)^2 - 2 \ln(x) \sum_{1 \leq d \leq x} \ln(d) \\ &= x \ln(x)^2 + \int_1^x \ln(t)^2 dt - 2 \ln(x) \int_1^x \ln(t) dt + O(x) \\ &= 2x \ln(x)^2 - 2(\ln(x) + 1) \int_1^x \ln(t) dt + O(x) = 2x \ln(x)^2 - 2(\ln(x) + 1)(x \ln(x) - x) + O(x) = O(x) \end{aligned}$$

Et donc l'erreur commise en oubliant la partie entière est en $O(x)$. On a donc au voisinage de $+\infty$:

$$S(x) = x \sum_{1 \leq d \leq x} \frac{\mu(d)}{d} \ln \left(\frac{x}{d} \right)^2 + O(x)$$

Posons $y = \frac{x}{d}$ dans la suite. Avec l'expression (*) de $\log(y)^2$ trouvée précédemment en fonction de τ , on obtient :

$$\begin{aligned} \frac{S(x)}{x} &= \sum_{1 \leq d \leq x} \frac{\mu(d)}{d} \left(2 \sum_{1 \leq m \leq y} \frac{\tau(m)}{m} + c_3 \sum_{1 \leq m \leq y} \frac{1}{m} + c_5 + O \left(\frac{1}{y^{\frac{1}{4}}} \right) \right) \\ &= \sum_{1 \leq d \leq x} \sum_{1 \leq m \leq x} \frac{2\mu(d)\tau(m)}{md} + c_3 \sum_{1 \leq d \leq x} \sum_{1 \leq m \leq x} \frac{\mu(d)}{dm} + c_4 \sum_{1 \leq d \leq x} \frac{\mu(d)}{d} + \sum_{1 \leq d \leq x} O \left(\frac{1}{d^{\frac{3}{4}} x^{\frac{1}{4}}} \right) \\ &= 2 \sum_{1 \leq n \leq x} \frac{1}{n} \sum_{d|n} \mu(d) \tau \left(\frac{n}{d} \right) + c_3 \sum_{1 \leq n \leq x} \frac{1}{n} \sum_{d|n} \mu(d) + c_4 \sum_{1 \leq d \leq x} \frac{\mu(d)}{d} + O(1) \end{aligned}$$

Maintenant, avec le formalisme de la convolution de Dirichlet, en notant $1_{\mathbb{N}}$ la fonction constante égale à 1 et δ la fonction qui vaut 1 en 0 et est nulle partout ailleurs (élément neutre pour la convolution de Dirichlet), on a classiquement : $\delta = 1_{\mathbb{N}} * \mu$ et $1_{\mathbb{N}} * 1_{\mathbb{N}} = \tau$ donc $\mu * \tau = \mu * 1_{\mathbb{N}} * 1_{\mathbb{N}} = 1_{\mathbb{N}}$. La formule ci dessus devient donc :

$$\frac{S(x)}{x} = 2 \sum_{1 \leq n \leq x} \frac{1}{n} + c_3 + c_4 \sum_{1 \leq d \leq x} \frac{\mu(d)}{d} + O(1) = 2 \ln(x) + c_4 \sum_{1 \leq d \leq x} \frac{\mu(d)}{d} + O(1)$$

Reste donc à montrer que la somme des $\frac{\mu(d)}{d}$ est bornée. Pour ceci, on observe que si p est la fonction partie entière sur $\mathbb{R}$, on a par inversion de Moebius, pour tout $x \in \mathbb{R}$:

$$p(x) = \sum_{n \leq x} 1_{\mathbb{N}} \left(\frac{x}{n} \right) \quad \text{donc :} \quad 1 = 1_{\mathbb{N}}(x) = \sum_{n \leq x} \mu(n) p \left(\frac{x}{n} \right) = \sum_{n \leq x} \left(\frac{x \mu(n)}{n} + O(1) \right)$$

d'où :

$$x \sum_{n \leq x} \frac{\mu(n)}{n} + O(x) = 1$$

Ce qui fournit bien le caractère borné de la somme $\sum_{n \leq x} \frac{\mu(n)}{n}$.

En reprenant l'expression de $\frac{S(x)}{x}$ ci-dessus, on arrive bien à :

$$S(x) = 2x \ln(x) + O(x)$$

Démonstration

On commence par montrer les trois formules asymptotiques suivantes :

$$\sum_{n \leq x} \frac{\mu(n)}{n} = O(1) \quad \sum_{n \leq x} \frac{\mu(n)}{n} \ln\left(\frac{x}{n}\right) = O(1) \quad \sum_{n \leq x} \frac{\mu(n)}{n} \ln\left(\frac{x}{n}\right)^2 = 2 \ln(x) + O(1) \quad (*)$$

Pour la première, on obtient aisément par inversion de Moebius :

$$\lfloor x \rfloor = \sum_{n \leq x} 1 \text{ d'où } 1 = \sum_{n \leq x} \mu(n) \left\lfloor \frac{x}{n} \right\rfloor = x \sum_{n \leq x} \frac{\mu(n)}{n} + O(x)$$

ce qui donne le résultat voulu. Pour la seconde, une simple estimation intégrale donne une constante C telle que :

$$\sum_{n \leq x} \frac{x}{n} = x \ln(x) + Cx + O(1)$$

Et en appliquant la formule d'inversion de Moebius à la fonction identité, on obtient :

$$x = \sum_{n \leq x} \mu(n) \sum_{m \leq \frac{x}{n}} \frac{\left(\frac{x}{n}\right)}{m} = \sum_{n \leq x} \mu(n) \left(\frac{x}{n} \ln\left(\frac{x}{n}\right) + \frac{Cx}{n} + O(1) \right) = x \sum_{n \leq x} \frac{\mu(n)}{n} \ln\left(\frac{x}{n}\right) + Cx \sum_{n \leq x} \frac{\mu(n)}{n} + O(x)$$

Et donc en utilisant la première estimation sur $\sum \frac{\mu(n)}{n}$, on obtient la seconde.

Reste à montrer la troisième estimation. Pour cela, on écrit, à l'aide d'une comparaison somme intégrale :

$$\begin{aligned} \sum_{n \leq x} \frac{x}{n} \ln\left(\frac{x}{n}\right) &= x \ln(x) \sum_{n \leq x} \frac{1}{n} - x \sum_{n \leq x} \frac{\ln(n)}{n} = x \ln(x)^2 + Cx \ln(x) + O(\ln(x)) - x \left(\frac{1}{2} \ln(x)^2 + D + O\left(\frac{\ln(x)}{x}\right) \right) \\ &= \frac{x}{2} \ln(x)^2 + Ax \ln(x) + Bx + O(\ln(x)) \end{aligned}$$

où A, B, C, D sont des constantes. Alors, à nouveau par inversion de Moebius sur la fonction $x \mapsto x \ln(x)$:

$$x \ln(x) = \sum_{n \leq x} \mu(n) \sum_{m \leq \frac{x}{n}} \frac{x}{nm} \ln\left(\frac{x}{nm}\right) = \sum_{n \leq x} \mu(n) \left(\frac{1}{2} \frac{x}{n} \ln\left(\frac{x}{n}\right)^2 + \frac{x}{n} \ln\left(\frac{x}{n}\right) + B \frac{x}{n} + O\left(\ln\left(\frac{x}{n}\right)\right) \right)$$

En utilisant les deux premières estimations, on obtient :

$$x \ln(x) = \frac{x}{2} \sum_{n \leq x} \frac{\mu(n)}{n} \ln\left(\frac{x}{n}\right) + O(x)$$

Ce qui montre la troisième estimation. Ainsi, on a démontré les trois formules asymptotiques (*).

Avec ces trois estimations, on est maintenant en mesure de calculer $S(x)$ assez précisément. Il vient :

$$S(x) = \sum_{n \leq x} \sum_{d|n} \mu(d) \ln\left(\frac{x}{d}\right)^2 = \sum_{d \leq x} \mu(d) \ln\left(\frac{x}{d}\right)^2 \sum_{\substack{1 \leq n \leq x \\ d|n}} 1 = \sum_{1 \leq d \leq x} \mu(d) \ln\left(\frac{x}{d}\right)^2 \left\lfloor \frac{x}{d} \right\rfloor$$

On voudrait se débarrasser de la partie entière. Or, on a :

$$\sum_{1 \leq d \leq x} \mu(d) \ln\left(\frac{x}{d}\right)^2 \left(\left\lfloor \frac{x}{d} \right\rfloor - \frac{x}{d} \right) = O\left(\sum_{1 \leq d \leq x} (\ln(x) - \ln(d))^2 \right)$$

Avec :

$$\begin{aligned} \sum_{1 \leq d \leq x} (\ln(x) - \ln(d))^2 &= \lfloor x \rfloor \ln(x)^2 + \sum_{1 \leq d \leq x} \ln(d)^2 - 2 \ln(x) \sum_{1 \leq d \leq x} \ln(d) \\ &= x \ln(x)^2 + \int_1^x \ln(t)^2 dt - 2 \ln(x) \int_1^x \ln(t) dt + O(x) \\ &= 2x \ln(x)^2 - 2(\ln(x) + 1) \int_1^x \ln(t) dt + O(x) = 2x \ln(x)^2 - 2(\ln(x) + 1)(x \ln(x) - x) + O(x) = O(x) \end{aligned}$$

Et donc l'erreur commise en oubliant la partie entière est en $O(x)$. On a donc au voisinage de $+\infty$:

$$S(x) = x \sum_{1 \leq d \leq x} \frac{\mu(d)}{d} \ln \left(\frac{x}{d} \right)^2 + O(x)$$

Dès lors, en utilisant la troisième estimation (*), il vient :

$$S(x) = x \sum_{1 \leq n \leq x} \frac{\mu(n)}{n} \ln \left(\frac{x}{n} \right)^2 + O(x) = x (2 \ln(x) + O(1)) + O(x)$$

Ceci prouve finalement la formule asymptotique :

$$S(x) = 2x \ln(x) + O(x)$$

Finalement, en identifiant les deux estimations de $S(x)$ données par les deux lemmes précédents, on obtient exactement la formule asymptotique de Selberg :

$$\theta(x) \ln(x) + \sum_{p \leq x} \theta \left(\frac{x}{p} \right) \ln(p) = 2x \ln(x) + O(x \ln(\ln(x))) \quad (1)$$

On note que cette formule implique également la seconde formule dite de "symétrie" de Selberg :

$$\sum_{p \leq x} \ln(p)^2 + \sum_{pq \leq x} \ln(p) \ln(q) = 2x \ln(x) + o(x \ln(x)) \quad (2)$$

En effet, on a d'une part :

$$\sum_{p \leq x} \theta \left(\frac{x}{p} \right) \ln(p) = \sum_{pq \leq x} \ln(p) \ln(q)$$

Et d'autre part, on a les estimations (qui utilisent les estimations de Tchebychev), pour tout $\epsilon > 0$:

$$\sum_{p \leq x} \ln(p)^2 \leq \theta(x) \ln(x) \leq \theta(x^{1-\epsilon}) \ln(x) + \sum_{x^{1-\epsilon} \leq p \leq x} \ln(p)^2 \frac{1}{1-\epsilon} \leq o(\ln(x)x) + \frac{1}{1-\epsilon} \sum_{p \leq x} \ln(p)^2$$

b) $a + A = 2$ via la formule de Selberg

Selberg est ensuite parvenu à tirer une conséquence très intéressante de la formule asymptotique qui porte son nom. Pour l'énoncé, on introduit les nombres suivants :

Définition 6

On définit les nombres suivants :

$$a = \liminf_{x \rightarrow +\infty} \frac{\pi(x) \ln(x)}{x} = \liminf_{x \rightarrow +\infty} \frac{\theta(x)}{x}$$

$$A = \limsup_{x \rightarrow +\infty} \frac{\pi(x) \ln(x)}{x} = \limsup_{x \rightarrow +\infty} \frac{\theta(x)}{x}$$

On remarque que ces définitions sont cohérentes en vertu de l'équivalent obtenu précédemment :

$$\theta(x) \sim \ln(x) \pi(x)$$

De plus, les encadrements de Tchebychev réalisés précédemment montrent que :

$$\ln(2) \leq a \leq A \leq e$$

Enfin, une remarque triviale mais importante est que, pour montrer le théorème des nombres premiers, il suffit de prouver que $a = A = 1$.

Or, Selberg parvient en quelque sorte à effectuer la moitié du travail puisqu'il démontre l'égalité suivante :

Proposition 1

Avec les notations précédentes, on a :

$$a + A = 2$$

Démonstration

Prenons x qui tend vers $+\infty$ avec $\theta(x) = Ax + o(x)$. Alors, la formule asymptotique de Selberg donne :

$$\sum_{p \leq x} \theta\left(\frac{x}{p}\right) \ln(p) = (2 - A)x \ln(x) + o(x \ln(x))$$

Mais le membre de gauche est minoré asymptotiquement par :

$$\sum_{p \leq x} \theta\left(\frac{x}{p}\right) \ln(p) \geq \sum_{p \leq x} \left(a \frac{x}{p} + o\left(\frac{x}{p}\right)\right) \ln(p) \geq ax \ln(x) + o(x \ln(x))$$

en utilisant la Grossenhilfsatz de Mersenne. On en déduit $a \leq 2 - A$. De la même façon, en prenant cette fois x tendant vers $+\infty$ de sorte que $\theta(x) = ax + o(x)$, on obtient $A \geq 2 - a$. Et donc on a bien $a + A = 2$. En utilisant l'égalité $a + A = 2$ et la borne $a \geq \ln(2)$, on en déduit au passage un raffinement sur la borne de A :

Corollaire 3

On a :

$$A \leq 2 - \ln(2) (\simeq 1.31)$$

c) Le lemme d'Erdős

Voici le résultat qu'est parvenu à prouver Erdős quelques temps après la publication de la formule de Selberg.

Proposition 2

Pour tout $c > 0$, il existe $\delta(c) > 0$ tel qu'on ait pour x assez grand :

$$\theta((1+c)x) - \theta(x) > \delta(c)x$$

On raisonne par l'absurde. On suppose donc l'existence de $c > 0$ tel qu'il existe des x arbitrairement grands tels que le quotient $\frac{\theta((1+c)x) - \theta(x)}{x}$ soit arbitrairement petit. On note S l'ensemble des constantes qui vérifient ceci, et C sa borne sup (les bornes de Tchebychev assurent aisément que S est majoré). On va démontrer que $C \in S$.

Montrons d'abord un petit lemme :

Lemme 7

Pour x, y au voisinage de $+\infty$ vérifiant $x \leq y$, on a :

$$\theta(y) - \theta(x) \leq 2(y - x) + o(y)$$

Démonstration

La formule de symétrie de Selberg donne immédiatement :

$$\sum_{x < p \leq y} \ln(p)^2 \leq 2y \ln(y) - 2x \ln(x) + o(y \ln(y))$$

Supposons dans un premier temps que $x > \frac{y}{\ln(y)^2}$. Dans ce cas, on a $\ln(x) = (1 + o(1)) \ln(y)$ et pour les nombres premiers p entre x et y , on a $\ln(p) = (1 + o(1)) \ln(y)$. En divisant les deux côtés de l'inégalité ci-dessus par $\ln(y)$, on a donc :

$$\sum_{x < p \leq y} \ln(p)(1 + o(1)) \leq 2y - 2x \frac{\ln(x)}{\ln(y)} + o(y)$$

Puis :

$$\theta(y) - \theta(x) + o(\theta(y)) \leq 2y - 2x \frac{\ln(x)}{\ln(y)} + o(y) \leq 2(y - x) + o(y)$$

qui est la formule recherchée. Dans le cas où au contraire, on a $x \leq \frac{y}{\ln(y)^2}$, on a alors avec des inégalités de Tchebychev et le cas précédent :

$$\begin{aligned} \theta(y) - \theta(x) &\leq \theta(y) - \theta\left(\frac{y}{\ln(y)^2}\right) + \theta\left(\frac{y}{\ln(y)^2}\right) \leq \theta(y) - \theta\left(\frac{y}{\ln(y)^2}\right) + o(y) \\ &\leq 2\left(y - \frac{y}{\ln(y)^2}\right) + o(y) \leq 2(y - x) + o(y) \end{aligned}$$

en utilisant le fait que $x = o(y)$ dans ce second cas. Ceci conclut la preuve du lemme.

Prenons maintenant un $\epsilon > 0$, et $c \in S$ vérifiant $c > C - \frac{\epsilon}{2}$. Pour x tendant vers $+\infty$ en parcourant les valeurs pour lesquelles $\theta(x(1+c)) - \theta(x) = o(x)$, on a :

$$\theta((1+C)x) - \theta((1+c)x) + \theta((1+c)x) - \theta(x) \leq 2(C-c)x + o(x) = \epsilon x + o(x)$$

Et donc comme ϵ est arbitraire, ceci prouve que $C \in S$. Ainsi, $C > 0$ est la plus grande valeur pour laquelle on a pour des valeurs de x arbitrairement grandes :

$$\theta((1+C)x) - \theta(x) = o(x)$$

(on note que cette formule n'est pas vraie pour tout x tendant vers $+\infty$ mais seulement pour un ensemble non majoré de valeurs de x , qu'on va noter dans la suite Ω)

Maintenant, pour x tendant vers $+\infty$ en restant dans Ω , on a par la formule de symétrie de Selberg :

$$\sum_{x \leq p \leq (1+C)x} \ln(p)^2 + \sum_{x \leq pq \leq (1+C)x} \ln(p) \ln(q) = 2Cx \ln(x) + o(x \ln(x))$$

Maintenant, on a évidemment, quand x tend vers $+\infty$ en restant dans Ω :

$$\sum_{x \leq p \leq (1+C)x} \ln(p)^2 \leq \ln((1+C)x)(\theta((1+C)x) - \theta(x)) = o(x \ln(x))$$

Et donc en combinant les deux résultats ci-dessus, il vient :

$$\begin{aligned} \sum_{x < pq \leq (1+C)x} \ln(p) \ln(q) &= 2Cx \ln(x) + o(x \ln(x)) \\ \text{d'où : } \sum_{p \leq (1+C)x} \ln(p) \left(\theta\left(\frac{x(1+C)}{p}\right) - \theta\left(\frac{x}{p}\right) \right) &= 2Cx \ln(x) + o(x \ln(x)) \end{aligned}$$

On a maintenant besoin d'un nouveau lemme :

Lemme 8

Pour x tendant vers $+\infty$ en restant dans Ω , on a :

$$\theta\left(\frac{x(1+C)}{p}\right) - \theta\left(\frac{x}{p}\right) = \frac{2Cx}{p} + o\left(\frac{x}{p}\right)$$

pour tous les nombres premiers $p \leq x(1+C)$ hors d'un ensemble $\mathcal{P}_x$ vérifiant :

$$\sum_{p \in \mathcal{P}_x} \frac{\ln(p)}{p} = o(\ln(x))$$

Démonstration

On raisonne par l'absurde. Si le lemme est faux, alors on dispose pour $x \in \Omega$ d'ensembles $\mathcal{P}_x$ et de $b_1, b_2 > 0$ tels que :

$$\theta\left(\frac{x(1+C)}{p}\right) - \theta\left(\frac{x}{p}\right) \leq (2C - b_1)\frac{x}{p} + o\left(\frac{x}{p}\right) \quad \text{pour } x \in \mathcal{P}_x$$

$$\sum_{p \in \mathcal{P}_x} \frac{\ln(p)}{p} \geq b_2 \ln(x) + o(\ln(x))$$

(en effet, pour la première inégalité, elle est forcément dans ce sens car le lemme 7 interdit une inégalité inversée avec un b_1 de signe opposé)

Dès lors, on a les estimations, avec la Grossenhilfsatz et le lemme 7 :

$$\begin{aligned} & \sum_{p \leq (C+1)x} \left(\theta\left(\frac{x(1+C)}{p}\right) - \theta\left(\frac{x}{p}\right) \right) \ln(p) \\ & \leq \sum_{p \leq (C+1)x ; p \notin \mathcal{P}_x} \left(\theta\left(\frac{x(1+C)}{p}\right) - \theta\left(\frac{x}{p}\right) \right) \ln(p) + \sum_{p \in \mathcal{P}_x} \left(\theta\left(\frac{x(1+C)}{p}\right) - \theta\left(\frac{x}{p}\right) \right) \ln(p) \\ & \leq \sum_{p \leq (C+1)x ; p \notin \mathcal{P}_x} \left(\frac{2C}{p}x + o\left(\frac{x}{p}\right) \right) \ln(p) + \sum_{p \in \mathcal{P}_x} \left((2C - b_1)\frac{x}{p} + o\left(\frac{x}{p}\right) \right) \ln(p) \\ & \leq 2Cx \ln(x) - b_1 b_2 x \ln(x) + o(x \ln(x)) \end{aligned}$$

Ceci contredit l'estimation qui précède le lemme, et donc conclut par l'absurde.

Dans la suite, on note conformément aux conventions de l'énoncé du lemme, $\mathcal{P}_x$ l'ensemble des p qui vérifient :

$$\sum_{p \in \mathcal{P}_x} \frac{\ln(p)}{p} = o(\ln(x))$$

On a donc pour p hors de $\mathcal{P}_x$ et x tendant vers $+\infty$ en restant dans Ω :

$$\theta\left(\frac{x(1+C)}{p}\right) - \theta\left(\frac{x}{p}\right) = \frac{2Cx}{p} + o\left(\frac{x}{p}\right)$$

Les éléments de $\mathcal{P}_x$ seront appelés les premiers "mauvais" et les autres les "bons" (notion qui dépend de x).

Supposons maintenant qu'on dispose d'une liste $p_1 < \dots < p_k$ de nombres premiers tous bons relativement à des x arbitrairement grands, tels que $10p_1 < p_k < 100p_1$ et $(1+C)(1+t)^2 p_i >$

$p_{i+1} > (1+t)p_i$ pour tout $1 \leq i \leq k-1$, où $t > 0$ est petit devant C , à fixer plus tard. On définit des intervalles :

$$I_i = \left[\frac{x}{p_i}; \frac{x}{p_i}(1+C) \right]$$

Si pour un certain i , on a $I_i \cap I_{i+1} \neq \emptyset$, alors par hypothèse, on a :

$$\frac{x}{p_{i+1}}(1+t) < \frac{x}{p_i} \leq \frac{x}{p_{i+1}}(1+C)$$

On montre alors dans ce cas que :

$$\theta\left(\frac{x}{p_i}\right) - \theta\left(\frac{x}{p_{i+1}}\right) = 2\left(\frac{x}{p_i} - \frac{x}{p_{i+1}}\right) + o\left(\frac{x}{p_i}\right) \quad (*)$$

En effet, si cette égalité est fausse, avec le lemme 7, on a pour des valeurs de x arbitrairement grandes dans Ω et pour $c_1 > 0$:

$$\theta\left(\frac{x}{p_i}\right) - \theta\left(\frac{x}{p_{i+1}}\right) < (2 - c_1)\left(\frac{x}{p_i} - \frac{x}{p_{i+1}}\right)$$

En combinant ceci avec le fait que p_{i+1} est bon relativement à x , on obtient :

$$\theta\left(\frac{x(1+C)}{p_{i+1}}\right) - \theta\left(\frac{x}{p_i}\right) > (2C + 2 - c_1)\frac{x}{p_{i+1}} - (2 - c_1)\frac{x}{p_i}$$

En prenant $c_2 > 0$ tel que $\frac{c_1+c_2}{p_{i+1}} < \frac{c_1-c_2}{p_i}$ (ce qui est possible indépendamment de x et i au vu du contrôle entre p_i et p_{i+1} imposé par t) on obtient :

$$\theta\left(\frac{x(1+C)}{p_{i+1}}\right) - \theta\left(\frac{x}{p_i}\right) > (2 + c_2)\left(\frac{x}{p_{i+1}}(1+C) - \frac{x}{p_i}\right)$$

Ceci contredit le résultat du lemme 7 et donc on a prouvé par l'absurde l'égalité (*) ci-dessus par l'absurde. En la combinant avec le fait que p_i est bon, on obtient si $I_i \cap I_{i+1} \neq \emptyset$:

$$\theta\left(\frac{x}{p_i}(1+C)\right) - \theta\left(\frac{x}{p_{i+1}}\right) = 2\left(\frac{x}{p_i}(1+C) - \frac{x}{p_{i+1}}\right) + o\left(\frac{x}{p_i}\right)$$

Alors, d'après les hypothèses sur les p_i et comme t est petit devant C , on a, si $I_i \cap I_{i+1} = \emptyset$ et pour x assez grand, en utilisant le fait que les p_i et p_{i+1} sont bons et que $\frac{x}{p_{i+1}}(1+C) < \frac{x}{p_i}$:

$$\begin{aligned} \theta\left(\frac{x}{p_i}(1+C)\right) - \theta\left(\frac{x}{p_{i+1}}\right) &> \theta\left(\frac{x}{p_i}(1+C)\right) - \theta\left(\frac{x}{p_i}\right) + \theta\left(\frac{x}{p_{i+1}}(1+C)\right) - \theta\left(\frac{x}{p_{i+1}}\right) \\ &> 2Cx\left(\frac{1}{p_i} - \frac{1}{p_{i+1}}\right) > 1.9\left(\frac{x}{p_i}(1+C) - \frac{x}{p_{i+1}}\right) \end{aligned}$$

A COMPLETER!!!

En sommant les deux dernières inégalités de 1 à k selon que $I_i \cap I_{i+1} = \emptyset$ ou non, on obtient aisément :

$$\theta\left(\frac{x}{p_1}(1+C)\right) - \theta\left(\frac{x}{p_k}\right) > 1.9\left(\frac{x}{p_1}(1+C) - \frac{x}{p_k}\right)$$

Mais par le choix des relations entre p_1 et p_k (à savoir $10p_1 < p_k < 100p_k$) ceci devient facilement :

$$\theta\left(\frac{x}{p_1}(1+C)\right) > 1.6\frac{x}{p_1}(1+C)$$

Ceci étant valable pour des valeurs de x arbitrairement grandes, on obtient $A \geq 1.6$, ce qui est absurde et donc prouve le lemme d'Erdős.

Il reste à montrer qu'on peut effectivement choisir une liste de premiers bons $p_1 \leq \dots \leq p_k$ tels que $10p_1 < p_k < 100p_1$ et $(1+C)(1+t)^2 p_i > p_{i+1} > (1+t)p_i$ pour tout $i \in \llbracket 1, k-1 \rrbracket$ pour $t > 0$ petit devant C . On considère un entier B très grand devant 1, à préciser éventuellement plus tard, et :

$$r \in \left[\left[0; \left\lfloor \frac{\ln(x)}{2\ln(B)} \right\rfloor - 1 \right] \right]$$

de sorte que $I_r = \llbracket B^{2r}, B^{2r+1} \rrbracket$ soit inclus dans $\llbracket 0, x \rrbracket$. On démontre d'abord que I_r contient un premier bon pour toutes les valeurs de r sauf $o(\ln(x))$ d'entre elles.

Si on prend B assez grand, les estimations de Tchebychev permettent de s'assurer que : $\theta(Bx) - \theta(x) > cx$ pour $c > 0$ constante et x assez grand. Dès lors, on a :

$$\sum_{p \in I_r} \frac{\ln(p)}{p} > B^{-2r-1} \sum_{p \in I_r} \ln(p) = B^{-2r-1} (\theta(BB^{2r}) - \theta(B^{2r})) > \frac{c}{B}$$

Si on avait $c_1 \ln(x)$ intervalles ne contenant aucun premier bon, on aurait alors en sommant leurs contributions avec la formule ci-dessus :

$$\sum_{p \leq x \text{ mauvais}} \frac{\ln(p)}{p} > \frac{cc_1}{B} \ln(x)$$

Ceci contredit la définition des premiers mauvais. Ainsi, on a montré que tous les I_r sauf peut-être $o(\ln(x))$ d'entre eux contiennent un nombre premier bon pour x assez grand.

Maintenant, supposons que r contienne un premier bon, et notons $p_1(r)$ le plus petit d'entre eux. On suppose qu'on dispose d'une liste $p_1(r) < \dots < p_i(r)$ de premiers bons tels que $10p_1(r) < p_i < 100p_1(r)$ et $(1+C)(1+t)^2 p_j > p_{j+1} > (1+t)p_j$ et que cette liste ne peut pas être étendue à $p_{i+1} > p_i$ vérifiant les mêmes conditions. Alors, l'intervalle :

$$J_r(i) = [p_i(r)(1+t), p_i(r)(1+C)(1+t)^2] \subset I_r$$

ne contient aucun nombre premier bon. Il vient alors, avec la définition de C comme la plus grande constante telle que $\theta((1+C)x) - \theta(x) = o(x)$ pour des x arbitrairement grands :

$$\sum_{p \in J_r(i)} \ln(p) > \eta p_i(r)(1+C)(1+t)^2$$

pour x assez grand, où η est une constante absolue. Dès lors, on a :

$$\sum_{p \in J_r(i)} \frac{\ln(p)}{p} > \frac{1}{p_i(r)(1+C)(1+t)^2} \sum_{p \in J_r(i)} \ln(p) > \eta$$

Maintenant, si on prend $B > 100$, on a très largement $p_i(r)(1+C)(1+t)^2 < B^{2r+2}$ et donc les intervalles $J_r(i)$ où r et i varient ne se coupent pas. Alors, en sommant sur r la minoration ci-dessus pour les $J_r(i)$ ne contenant que des premiers pas bons, comme le nombre de r tels que $p_1(r)$ soit bien défini est au moins $\frac{\ln(x)}{4\ln(B)}$ (car on a vu que les intervalles I_r ne contenant que des premiers mauvais sont en un nombre $o(\ln(x))$), on obtient :

$$\sum_{p \leq x(C+1); \text{ mauvais}} \frac{\ln(p)}{p} > \frac{\eta \ln(x)}{4 \ln(B)}$$

Ceci contredit le lemme sur la faible densité des nombres premiers mauvais, et établit donc le lemme d'Erdős.

d) La conclusion de Selberg

Durant les deux jours qui suivent la publication de ce dernier lemme d'Erdős, Selberg est parvenu à démontrer le théorème des nombres premiers. On rappelle qu'il suffit pour cela d'obtenir l'équivalent $\theta(x) \sim x$.

Voici comment Selberg procède pour démontrer le :

Théorème 9

On a au voisinage de $+\infty$ l'équivalent :

$$\pi(x) \sim \frac{x}{\ln(x)}$$

On rappelle qu'on a démontré que, si a est la limite inférieure du quotient $\frac{\theta(x)}{x}$ et A sa limite supérieure, on a $a + A = 2$.

Selberg commence par démontrer un petit lemme :

Lemme 9

Soit x tendant vers $+\infty$ tel que $\theta(x) = Ax + o(x)$. Alors, pour tous les nombres premiers $p \leq x$ sauf peut être un ensemble $\mathcal{P}_x$ vérifiant :

$$\sum_{p \in \mathcal{P}_x} \frac{\ln(p)}{p} = o(\ln(x))$$

on a :

$$\theta\left(\frac{x}{p}\right) = a\frac{x}{p} + o\left(\frac{x}{p}\right)$$

Démonstration

Raisonnons par l'absurde en supposant que le lemme est faux. Alors quitte à extraire sur x , on dispose d'un ensemble $\mathcal{P}_x$ de premiers $\leq x$ et de constantes $b_1, b_2 > 0$ telles que pour p dans $\mathcal{P}_x$, on ait :

$$\begin{aligned} \sum_{p \in \mathcal{P}_x} \frac{\ln(p)}{p} &= b_1 \ln(x) \\ \theta\left(\frac{x}{p}\right) &> (a + b_2)\frac{x}{p} + o\left(\frac{x}{p}\right) \end{aligned}$$

Alors, comme $a + A = 2$, la formule asymptotique de Selberg donne (avec la Grossenhilfsatz) :

$$\begin{aligned} ax \ln(x) + o(x \ln(x)) &= \sum_{p \leq x} \theta\left(\frac{x}{p}\right) \ln(p) \geq \sum_{p \in \mathcal{P}_x} \theta\left(\frac{x}{p}\right) \ln(p) + \sum_{p \notin \mathcal{P}_x} \theta\left(\frac{x}{p}\right) \ln(p) \\ &> b_1(a + b_2) \ln(x) + (1 - b_1)a \ln(x) + o(\ln(x)) \end{aligned}$$

d'où $a > a + b_1 b_2$ qui est manifestement absurde. Ceci prouve le lemme. On conserve les notations du lemme : $\mathcal{P}_x$ est un ensemble de nombres premiers tel que :

$$\sum_{p \in \mathcal{P}_x} \frac{\ln(p)}{p} = o(\ln(x))$$

et pour p hors de $\mathcal{P}_x$, on a :

$$\theta\left(\frac{x}{p}\right) = a \frac{x}{p} + o\left(\frac{x}{p}\right)$$

Il démontre ensuite un second lemme utile dans la suite :

Lemme 10

Avec ces mêmes notations, on note p_1 le plus petit premier hors de $\mathcal{P}_x$, de sorte que :

$$\theta\left(\frac{x}{p_1}\right) = a \frac{x}{p_1} + o\left(\frac{x}{p_1}\right)$$

(p_1 dépend évidemment de x)

Alors pour tout $\epsilon > 0$, on a pour x assez grand : $p_1 < x^\epsilon$, et pour tous les nombres premiers $p_j < \frac{x}{p_1}$ sauf peut-être pour un ensemble $\mathcal{Q}_x$ vérifiant :

$$\sum_{p \in \mathcal{Q}_x} \frac{\ln(p)}{p} = o(\ln(x))$$

on a :

$$\theta\left(\frac{x}{p_1 p_j}\right) = A \frac{x}{p_1 p_j} + o\left(\frac{x}{p_1 p_j}\right)$$

Démonstration

La démonstration est identique à celle du lemme précédent, en échangeant A et a et en utilisant le résultat (qui découle de la définition de p_1) :

$$\theta\left(\frac{x}{p_1}\right) = a \frac{x}{p_1} + o\left(\frac{x}{p_1}\right)$$

Pour la première moitié du lemme, on remarque que tous les premiers inférieurs à x sont dans $\mathcal{P}_x$ et donc sont dans $\mathcal{P}_x$, ainsi on a $\theta(p_1) = o(\ln(x))$ soit $\ln(p_1) = o(\ln(x))$ qui fournit bien asymptotiquement $p_1 < x^\epsilon$.

Venons-en à la preuve du théorème des nombres premiers. On suppose par l'absurde que $A > a$. Soit p_i un nombre premier hors de $\mathcal{P}_x$, de sorte que :

$$\theta\left(\frac{x}{p_i}\right) = a \frac{x}{p_i} + o\left(\frac{x}{p_i}\right)$$

Soit également p_j un tel nombre premier hors de $\mathcal{P}_x$. Supposons que $\frac{x}{p_1 p_j} < \frac{x}{p_i}$. Il vient alors : $\theta\left(\frac{x}{p_1 p_j}\right) \leq \theta\left(\frac{x}{p_i}\right)$ et donc avec le lemme précédent et la formule rappelée ci-dessus :

$$A \frac{x}{p_1 p_j} \leq a \frac{x}{p_i} + o\left(\frac{x}{p_i}\right)$$

Et donc pour $0 < \delta < \frac{A}{a} - 1$ quelconque, pour x assez grand, ceci prouve que p_j n'est pas dans l'intervalle :

$$I_i = \left[\frac{p_i}{p_1}, \frac{p_i}{p_1} \left(\frac{A}{a} - \delta \right) \right]$$

Et donc cet intervalle ne contient que des nombres premiers dans $\mathcal{P}_x$: les "mauvais". Or, on a en posant $c = \frac{A}{a} - \delta > 1$, avec le lemme d'Erdős :

$$\sum_{p \in I_i} \frac{\ln(p)}{p} > \frac{1}{\frac{p_i c}{p_1}} \left(\theta\left(\frac{c p_i}{p_1}\right) - \theta\left(\frac{p_i}{p_1}\right) \right) > \delta(c) \frac{1}{c}$$

Maintenant, comme dans la preuve du lemme d'Erdős, on construit $c' \ln(x)$ tels intervalles I_i deux à deux disjoints (où $c' > 0$), et on obtient donc finalement :

$$\sum_{p \in \mathcal{P}_x} \frac{\ln(p)}{p} > \frac{c' \delta(c)}{c} \ln(x)$$

Ceci est manifestement absurde, et prouve donc par contradiction que $a \geq A$. Comme on sait que $a + A = 2$, on conclut que $a = A = 2$: le théorème des nombres premiers est prouvé.

III Méthodes élémentaires pour l'infinité des $\mathbb{P} \cap A$, où $A \subset \mathbb{N}$

Dans cette partie, nous allons étudier des exemples de résultats d'existence de nombres premiers vérifiant certaines propriétés, toujours en employant exclusivement des méthodes élémentaires.

1 Postulat de Bertrand

Le Postulat de Bertrand, démontré par Tchebychev, s'énonce en ces termes :

Théorème 10 - Postulat de Bertrand

Soit $n \in \mathbb{N}$ avec $n \geq 2$. Il existe au moins un nombre premier p tel que :

$$n < p < 2p$$

Démonstration

• Soit $n \geq 2$.

Par la formule du binôme, ainsi que le fait déjà démontré à l'occasion de la preuve du théorème 3 selon lequel pour tout k , $\binom{2n}{n} \geq \binom{2n}{k}$, on a :

$$4^n = 2 + \sum_{k=1}^{2n-1} \binom{2n}{k} \leq 2 + (2n-1) \binom{2n}{n} \leq 2n \binom{2n}{n}$$

Pour tout $p \in \mathbb{P}$, notons v_p la valuation p -adique de $\binom{2n}{n}$. On écrit alors :

$$\binom{2n}{n} = P_1 P_2 P_3 P_4$$

où :

$$P_1 = \prod_{\substack{p \in \mathbb{P} \\ 1 < p \leq \sqrt{2n}}} p^{v_p} ; \quad P_2 = \prod_{\substack{p \in \mathbb{P} \\ \sqrt{2n} < p \leq \frac{2n}{3}}} p^{v_p} ; \quad P_3 = \prod_{\substack{p \in \mathbb{P} \\ \frac{2n}{3} < p \leq n}} p^{v_p} ; \quad P_4 = \prod_{\substack{p \in \mathbb{P} \\ n < p < 2n}} p^{v_p}$$

Pour minorer P_4 , on va tâcher de majorer P_1 , P_2 et P_3 . On va pour cela devoir estimer les v_p . Par la formule de Legendre, on a pour tout $p \in \mathbb{P}$:

$$v_p = \sum_{k=1}^{+\infty} \left[2 \frac{n}{p^k} \right] - 2 \left[\frac{n}{p} \right]$$

Posons pour tous $k \in \mathbb{N}^*$, $p \in \mathbb{P}$: $u_k(p) = \left[2 \frac{n}{p^k} \right] - 2 \left[\frac{n}{p} \right]$

• Majoration de P_1 .

Soit p premier inférieur ou égal à $\sqrt{2n}$. Chaque terme $u_k(p)$ vaut soit 0, soit 1 selon la position de la partie fractionnaire de $\frac{n}{p^k}$ par rapport à $\frac{1}{2}$. De plus, pour tout k tel que $2 \frac{n}{p^k} < 1$, $u_k(p)$ est nul. Donc finalement, on a :

$$v_p = \sum_{k=1}^{\left\lfloor \frac{\ln(2n)}{\ln(p)} \right\rfloor} u_k(p) \leq \left\lfloor \frac{\ln(2n)}{\ln(p)} \right\rfloor \leq \frac{\ln(2n)}{\ln(p)}$$

Et donc $p^{v_p} \leq 2n$, et finalement, $P_1 \leq (2n)^{\sqrt{2n}}$.

• Majoration de P_2 .

Soit p premier, avec $\sqrt{2n} < p < \frac{2n}{3}$. Pour tout $k \geq 2$, on a : $0 < \frac{n}{p^k} < \frac{2n}{p^k} < 1$ et donc $u_k(p) = 0$. Donc $v_p = u_1(p)$. Donc finalement :

$$P_2 \leq \prod_{\substack{p \in \mathbb{P} \\ \sqrt{2n} < p \leq \frac{2n}{3}}} p \leq \prod_{p \in \mathbb{P}_{\frac{2n}{3}}} p = \prod_{p \in \mathbb{P}_{\lfloor \frac{2n}{3} \rfloor}} p \leq 4^{\lfloor \frac{2n}{3} \rfloor} \leq 4^{\frac{2n}{3}}$$

En utilisant le lemme de majoration de la primorielle.

• Majoration de P_3 .

En fait, on a $P_3 = 1$. En effet, soit p premier tel que $\frac{2n}{3} < p \leq n$. Alors, on a :

$$u_1(p) = \left[2 \frac{n}{p} \right] - 2 \left[\frac{n}{p} \right] = 2 - 2 = 0$$

et les autres $u_k(p)$ sont nuls pour les mêmes raisons que dans la majoration de P_2 .

• En réunissant tous ces résultats, on obtient :

$$4^n \leq 2n \binom{2n}{n} = 2n P_1 P_2 P_3 P_4 \leq (2n)^{1+\sqrt{2n}} 4^{\frac{2n}{3}} P_4$$

i.e.

$$P_4 \geq \frac{4^{\frac{n}{3}}}{(2n)^{1+\sqrt{2n}}}$$

En posant $2n = 2^{2t}$, l'inégalité devient :

$$\ln(P_4) > \frac{t 2^t \ln(2)}{3} \left(\frac{2^t}{t} - 6(1 + 2^{-t}) \right)$$

Si on fait l'hypothèse selon laquelle $n \leq 600$, on a $2^{2t} > 2^{10}$ d'où $t > 5$ puis $\frac{2^t}{t} > \frac{2^5}{5} > 6(1 + 2^{-5}) > 6(1 + 2^{-t})$ et donc $\ln(P_4) > 0$. Donc $P_4 > 1$, ce qui prouve le résultat dès lors que $n \leq 600$.

On conclut alors en vérifiant manuellement le résultat pour tout $n \in \llbracket 2, 600 \rrbracket$.

2 Théorème de Brun

Le théorème de Brun, qui est à rapprocher de la conjecture des nombres premiers jumeaux, donne, par une méthode de crible, une majoration du nombre de nombres premiers jumeaux. On va devoir, pour énoncer ce théorème, fixer quelques notations supplémentaires :

Définition 7

La fonction π de comptage des nombres premiers jumeaux est définie, pour tout $x \in \mathbb{R}$, par :

$$\pi_2(x) = \sum_{\substack{p \in \mathbb{P}_x \\ p+2 \in \mathbb{P}}} 1$$

On commence par prouver un lemme fondamental dans la mise en place des techniques de crible.

Lemme 11

Soient $n \in \mathbb{N}^*$ et $a_1, \dots, a_n \in [0, 1]$. On note pour tout $k \in \llbracket 0, n \rrbracket$:

$$\sigma_k = \sum_{1 \leq i_1 < \dots < i_k \leq n} a_{i_1} \dots a_{i_k}$$

avec la convention $\sigma_0 = 1$.

Alors, pour tout k impair et tout l pair dans $\llbracket 0, n \rrbracket$, on a :

$$\sigma_0 - \sigma_1 + \dots - \sigma_k \leq \prod_{i=1}^n (1 - a_i) \leq \sigma_0 - \sigma_1 + \dots + \sigma_l$$

Démonstration

Montrons le résultat par récurrence sur $n \in \mathbb{N}^*$. Le résultat étant clair pour $n = 1$, fixons $n \in \mathbb{N}^*$ tel que la propriété soit vérifiée et montrons-la pour $n + 1$.

Soient donc $a_1, \dots, a_{n+1}$ $n + 1$ éléments de $[0, 1]$. Pour tout $p \in \llbracket 0, n + 1 \rrbracket$, pour tout $k \in \llbracket 0, p \rrbracket$, on notera :

$$\sigma_k^{(p)} = \sum_{1 \leq i_1 < \dots < i_p \leq n} a_{i_1} \dots a_{i_k} \leq p$$

Soient alors k impair et l pair dans $\llbracket 0, n \rrbracket$. Supposons pour l'instant $k < n + 1$ et $l < n + 1$. Alors, on a par hypothèse de récurrence :

$$\sigma_0^{(n)} - \sigma_1^{(n)} + \dots - \sigma_k^{(n)} \leq \prod_{i=1}^n (1 - a_i) \leq \sigma_0^{(n)} - \sigma_1^{(n)} + \dots + \sigma_l^{(n)}$$

D'où, en multipliant par $1 - a_{n+1}$ qui est positif, on a successivement :

$$\begin{aligned}
\sum_{i=0}^k (1 - a_{n+1})(-1)^i \sigma_i^{(n)} &\leq \prod_{i=1}^{n+1} (1 - a_i) \leq \sum_{i=0}^l (1 - a_{n+1})(-1)^i \sigma_i^{(n)} \\
\sigma_0 + \sum_{i=0}^{k-1} (-1)^{i+1} \left(a_{n+1} \sigma_i^{(n)} + \sigma_{i+1}^{(n)} \right) - (-1)^k a_{n+1} \sigma_k^{(n)} &\leq \prod_{i=1}^{n+1} (1 - a_i) \leq \sigma_0 + \sum_{i=0}^{l-1} (-1)^{i+1} \left(a_{n+1} \sigma_i^{(n)} + \sigma_{i+1}^{(n)} \right) - (-1)^l a_{n+1} \sigma_l^{(n)} \\
\sigma_0 + \sum_{i=0}^{k-1} (-1)^{i+1} \sigma_{i+1}^{(n+1)} + a_{n+1} \sigma_k^{(n)} &\leq \prod_{i=1}^{n+1} (1 - a_i) \leq \sigma_0 + \sum_{i=0}^{l-1} (-1)^{i+1} \sigma_{i+1}^{(n+1)} - a_{n+1} \sigma_l^{(n)} \\
\sum_{i=0}^k (-1)^i \sigma_i^{(n+1)} + a_{n+1} \sigma_k^{(n)} &\leq \prod_{i=1}^{n+1} (1 - a_i) \leq \sum_{i=0}^l (-1)^i \sigma_i^{(n+1)} - a_{n+1} \sigma_l^{(n)} \\
\sum_{i=0}^k (-1)^i \sigma_i^{(n+1)} &\leq \prod_{i=1}^{n+1} (1 - a_i) \leq \sum_{i=0}^l (-1)^i \sigma_i^{(n+1)}
\end{aligned}$$

Ceci restant clairement vrai quand $k = n + 1$ ou $l = n + 1$ car :

$$\sum_{i=0}^{n+1} (-1)^i \sigma_i^{(n+1)} = \prod_{i=1}^{n+1} (1 - a_i)$$

on a bien démontré le lemme par récurrence sur n .

On est maintenant en mesure d'énoncer et de démontrer le théorème de Brun :

Théorème 11

Pour $n \in \mathbb{N}$, $n \geq 2$, on a au voisinage de $+\infty$ la majoration :

$$\pi_2(n) = O\left(\frac{n \ln(\ln(n))^2}{\ln(n)^2}\right)$$

Démonstration

Fixons un très grand entier $n \in \mathbb{N}^*$, et un entier $y < n$ dont on précisera le choix plus tard.

• Pour tout nombre premier p , posons $A_p = \{k \in \llbracket 1, n \rrbracket \mid p \text{ divise } k \text{ ou } k + 2\}$ Clairement, si un certain $k > y$ est dans un des A_p pour $p < y$ (ce qui impose $p < k$), alors l'un ou l'autre des nombres k et $k + 2$ n'est pas premier. On en déduit directement la majoration :

$$\pi_2(n) \leq y + \left(x - \left| \bigcup_{p \in \mathbb{P}_y} A_p \right| \right)$$

• Soit maintenant l un entier pair inférieur ou égal à y . Pour tout ensemble E , on note $\mathbf{1}_E$ la fonction indicatrice de E qui prend la valeur 1 en tout élément de E , et 0 partout ailleurs. Alors, pour tout $x \in \llbracket 1, n \rrbracket$, on a :

$$(\mathbf{1}_{\bigcup_{p \in \mathbb{P}_y} A_p})(x) = 1 - (\mathbf{1}_{\bigcap_{p \in \mathbb{P}_y} \llbracket 1, n \rrbracket \setminus A_p})(x) = 1 - \prod_{p \in \mathbb{P}_y} (\mathbf{1}_{\llbracket 1, n \rrbracket \setminus A_p})(x) = 1 - \prod_{p \in \mathbb{P}_y} (1 - \mathbf{1}_{A_p}(x))$$

D'où, d'après le lemme et comme l est pair, on a (où les produits sont pris sur les nombres premiers) :

$$(\mathbf{1}_{\bigcup_{p \in \mathbb{P}_y} A_p})(x) \geq \sum_{i=1}^l (-1)^{i+1} \left(\sum_{p_1 < \dots < p_i \leq y} \mathbf{1}_{A_{p_1}}(x) \dots \mathbf{1}_{A_{p_i}}(x) \right) = \sum_{i=1}^l (-1)^{i+1} \left(\sum_{p_1 < \dots < p_i \leq y} \mathbf{1}_{A_{p_1} \cap \dots \cap A_{p_i}}(x) \right)$$

En sommant cette relation pour tout $x \in \llbracket 1, n \rrbracket$, on obtient :

$$\left| \bigcup_{p \in \mathbb{P}_y} A_p \right| \geq \sum_{i=1}^l (-1)^{i+1} \left(\sum_{p_1 < \dots < p_i < y} \left| \bigcap_{j=1}^i A_{p_j} \right| \right)$$

- Tâchons maintenant d'estimer les termes : $\left| \bigcap_{j=1}^i A_{p_j} \right|$.

Fixons donc $i \in \llbracket 1, l \rrbracket$ et $p_1, \dots, p_i$ des nombres premiers strictement inférieurs à y . Notons que pour tout $m \in \llbracket 1, n \rrbracket$, d'après le théorème des restes chinois, la condition $m \in A_{p_1} \cap \dots \cap A_{p_i}$ dépend uniquement du reste de m modulo $p_1 \dots p_i$, et que toujours par le théorème des restes chinois, il y a exactement 2^i restes possibles pour m pour être dans $A_{p_1} \cap \dots \cap A_{p_i}$ (en effet, pour tout $j \in \llbracket 1, i \rrbracket$, on peut choisir $m \equiv 0$ ou $m \equiv -2$ modulo p_j).

Effectuons la division euclidienne de n par $p_1 \dots p_i$: $n = qp_1 \dots p_i + r$. Alors par la remarque précédente, pour tout $k \in \llbracket 0, q-1 \rrbracket$, l'ensemble $\llbracket kp_1 \dots p_i + 1, (k+1)p_1 \dots p_i \rrbracket$ contient exactement 2^i éléments de $A_{p_1} \cap \dots \cap A_{p_i}$. On en déduit que :

$$\left| \llbracket 1, qp_1 \dots p_i \rrbracket \cap \bigcap_{j=1}^i A_{p_j} \right| = q2^i$$

Et donc en notant :

$$R(p_1, \dots, p_i) = \left| \llbracket qp_1 \dots p_i + 1, n \rrbracket \cap \bigcap_{j=1}^i A_{p_j} \right|$$

On a d'une part, par le même raisonnement que précédemment sur $\llbracket qp_1 \dots p_i + 1, n \rrbracket$: $0 \leq R(p_1, \dots, p_i) \leq 2^i$.

Et d'autre part :

$$\left| \bigcap_{j=1}^i A_{p_j} \right| = q2^i + R(p_1, \dots, p_i)$$

Et donc :

$$\left| \bigcap_{j=1}^i A_{p_j} \right| = \frac{n2^i}{p_1 \dots p_i} + T(p_1, \dots, p_i)$$

où $-2^i \leq T(p_1, \dots, p_i) \leq 2^i$.

- Des deux points précédents, il découle la majoration :

$$\begin{aligned} n - \left| \bigcup_{p \in \mathbb{P}_y} A_p \right| &\leq x + \sum_{i=1}^l (-1)^i \left(\sum_{p_1 < \dots < p_i < y} \left| \bigcap_{j=1}^i A_{p_j} \right| \right) = n + \sum_{i=1}^l (-1)^i \left(\sum_{p_1 < \dots < p_i < y} \frac{n2^i}{p_1 \dots p_i} + T(p_1, \dots, p_i) \right) \\ &\leq n \sum_{i=0}^l (-1)^i \left(\sum_{p_1 < \dots < p_i < y} \frac{2^i}{p_1 \dots p_i} \right) + \sum_{i=1}^l (-1)^i \left(\sum_{p_1 < \dots < p_i < y} T(p_1, \dots, p_i) \right) \\ &\leq n \sum_{i=0}^l (-1)^i \left(\sum_{p_1 < \dots < p_i < y} \frac{2^i}{p_1 \dots p_i} \right) + \sum_{i=1}^l \left(\sum_{p_1 < \dots < p_i < y} 2^i \right) \\ &\leq n \sum_{i=0}^l (-1)^i \left(\sum_{p_1 < \dots < p_i < y} \frac{2^i}{p_1 \dots p_i} \right) + 2^l \sum_{i=1}^l \binom{\pi(y)}{i} \leq n \sum_{i=0}^l (-1)^i \left(\sum_{p_1 < \dots < p_i < y} \frac{2^i}{p_1 \dots p_i} \right) + 2^l \pi(y)^l \\ &\leq n \sum_{i=0}^l (-1)^i \left(\sum_{p_1 < \dots < p_i < y} \frac{2^i}{p_1 \dots p_i} \right) + y^l \end{aligned}$$

Et donc, du lemme utilisé au rang $l-1$ qui est impair, ainsi que de la première majoration montrée sur π_2 , on déduit

enfin :

$$\begin{aligned}
\pi_2(n) &\leq y + \left(x - \left| \bigcup_{p \in \mathbb{P}_y} A_p \right| \right) \leq y + n \sum_{i=0}^l (-1)^i \left(\sum_{p_1 < \dots < p_i < y} \frac{2^i}{p_1 \dots p_i} \right) + y^l \\
&\leq y + y^l + n \sum_{i=0}^{l-1} (-1)^i \left(\sum_{p_1 < \dots < p_i < y} \frac{2^i}{p_1 \dots p_i} \right) + n \sum_{p_1 < \dots < p_l < y} \frac{2^l}{p_1 \dots p_l} \\
&\leq y + y^l + n \prod_{p \in \mathbb{P}_y} \left(1 - \frac{2}{p} \right) + n \sum_{p_1 < \dots < p_l < y} \frac{2^l}{p_1 \dots p_l} \\
&\leq y + y^l + n \prod_{p \in \mathbb{P}_y} \left(1 - \frac{1}{p} \right)^2 + \frac{n}{l!} \left(\sum_{p \in \mathbb{P}_y} \frac{2}{p} \right)^l
\end{aligned}$$

Les théorème de Mertens vont nous permettre d'estimer les deux termes restants. Pourvu que y soit assez grand, on a en effet, d'après le deuxième et le troisième théorème de Mertens :

$$\prod_{p \in \mathbb{P}_y} \left(1 - \frac{1}{p} \right)^2 \leq \frac{C}{\ln(y)^2} \quad ; \quad \sum_{p \in \mathbb{P}_y} \frac{1}{p} \leq e^2 \ln \ln(y)$$

où C est une constante positive. Ceci donne l'inégalité pour y assez grand :

$$\pi_2(n) \leq y + y^l + \frac{nC}{\ln(y)^2} + \frac{n2^l e^{2l} \ln(\ln(y))^l}{l!} \leq \pi_2(n) \leq y + y^l + \frac{nC}{\ln(y)^2} + n \left(\frac{2e^2 \ln(\ln(y))}{l} \right)^l$$

Il suffit alors de prendre $y = n^{\frac{1}{100 \ln(\ln(n))}}$ (ce qui assure que $y \xrightarrow{n \rightarrow +\infty} +\infty$ et donc assure que la majoration ci-dessus est valable pour n assez grand) et $l \simeq 4e^2 \ln \ln(n)$ pour conclure : aucun terme de l'expression majorante ne dépasse alors $\frac{Kn \ln \ln(n)^2}{\ln(n)^2}$ où K est une constante réelle positive.

Et voici un très joli corollaire de cette majoration :

Corollaire 4

La série des inverses des nombres premiers jumeaux :

$$\sum_{\substack{p \in \mathbb{P} \\ p+2 \in \mathbb{P}}} \frac{1}{p} + \frac{1}{p+2}$$

converge.

Démonstration

Il s'agit simplement de faire une transformation d'Abel. Notons $C > 0$ une constante réelle telle que pour tout $n \geq 2$, on ait :

$$\pi_2(n) \leq K \frac{n \ln(\ln(n))^2}{\ln(n)^2}$$

Pour tout $n \in \mathbb{N}^*$, on a :

$$\begin{aligned}
\sum_{\substack{p \in \mathbb{P}_n \\ p+2 \in \mathbb{P}}} \frac{1}{p} + \frac{1}{p+2} &\leq 2 \sum_{\substack{p \in \mathbb{P}_n \\ p+2 \in \mathbb{P}}} \frac{1}{p} \leq 2 \sum_{k=2}^n \frac{\pi_2(k) - \pi_2(k-1)}{k} = 2 \sum_{k=2}^n \left(\frac{\pi_2(k)}{k} - \frac{\pi_2(k-1)}{k-1} + \frac{\pi_2(k-1)}{k(k-1)} \right) \\
&\leq 2 \frac{\pi_2(n)}{n} + K \sum_{k=1}^{n-1} \frac{\pi_2(k)}{k(k+1)} \leq 2 + K \sum_{k=2}^n \frac{\ln(\ln(k))}{k \ln(k)^2}
\end{aligned}$$

On conclut en remarquant que :

$$\frac{\ln(\ln(n))}{n \ln(n)^2} = o\left(\frac{1}{n \ln(n)^{\frac{3}{2}}}\right)$$

Qui est le terme général d'une série de Bertran absolument convergente.

IV Application de l'analyse complexe à l'étude des nombres premiers

1 Théorème des nombres premiers

Voici l'énoncé du théorème des nombres premiers :

Théorème 12

On a l'équivalent, au voisinage de $+\infty$:

$$\pi(x) \sim \frac{x}{\ln(x)}$$

Le reste de cette section est dédié à la preuve de ce résultat, qui requiert une bonne dose d'analyse complexe. La preuve qui suit est due à Newman.

a) Préliminaires sur la fonction θ

On définit la fonction θ qui nous sera utile pour l'estimation :

Définition 8

On pose, pour tout $x \geq 0$:

$$\theta(x) = \sum_{p \in \mathbb{P}_x} \ln(p)$$

On a alors les encadrements suivants, pour tout $\epsilon > 0$:

$$(1 - \epsilon) \ln(x) (\pi(x) - \pi(x^{1-\epsilon})) \leq \sum_{x^{1-\epsilon} < p \leq x} \ln(p) = \theta(x) - \theta(x^{1-\epsilon}) \leq \theta(x)$$

$$\theta(x) \leq \pi(x) \ln(x)$$

Et donc pour x au voisinage de $+\infty$:

$$(1 - \epsilon) \ln(x) \pi(x) + O(x) \leq \theta(x) \leq \pi(x) \ln(x)$$

Ceci étant valable pour tout $\epsilon > 0$, on a prouvé le :

Lemme 12

Pour x tendant vers $+\infty$, on a :

$$\frac{\theta(x)}{\pi(x) \ln(x)} \xrightarrow{x \rightarrow +\infty} 1$$

Et donc finalement, on a obtenu qu'il suffit de montrer que $\theta(x) \sim x$ pour prouver le théorème des nombres premiers. Montrons alors un petit lemme d'analyse, qui sera utile pour montrer l'équivalent $\theta(x) \sim x$:

Lemme 13

Soient $a > 0$ et $u : [a, +\infty]$ une fonction croissante telle que l'intégrale :

$$\int_a^{+\infty} \frac{u(x) - x}{x^2} dx$$

converge. Alors, on a l'équivalent au voisinage de $+\infty$:

$$u(x) \sim x$$

Démonstration

On suppose par l'absurde le contraire. Alors, deux situations sont possibles.

• Premier cas : il existe $\lambda > 1$ et une suite strictement croissante $(x_n)_{n \geq 0}$ tendant vers $+\infty$ telle que $u(x_n) \geq \lambda x_n$ pour tout $n \geq 0$. Alors, on a par croissance de u :

$$\int_{x_n}^{\lambda x_n} \frac{u(x) - x}{x^2} dx \geq \int_{x_n}^{\lambda x_n} \frac{u(x_n) - x}{x^2} dx \geq \int_{x_n}^{\lambda x_n} \frac{\lambda x_n - x}{x^2} dx = \lambda - 1 - \ln(\lambda) > 0$$

Ceci est absurde car l'intégrale sur $[a, +\infty]$ converge.

• Deuxième cas : il existe $\mu > 1$ et une suite strictement croissante $(x_n)_{n \geq 0}$ tendant vers $+\infty$ telle que $u(x_n) \leq \mu x_n$ pour tout $n \geq 0$. Alors, on a par croissance de u :

$$\int_{\mu x_n}^{x_n} \frac{u(x) - x}{x^2} dx \leq \int_{\mu x_n}^{x_n} \frac{u(x_n) - x}{x^2} dx \leq \int_{\mu x_n}^{x_n} \frac{\mu x_n - x}{x^2} dx = 1 - \mu + \ln(\mu) < 0$$

Encore une fois, ceci contredit la convergence de l'intégrale. Ceci termine la preuve du lemme d'analyse.

À ce stade, faisons une rapide remarque. On cherche à estimer $\theta(x)$ (plus précisément, à montrer que $\theta(x)$ est équivalent à x en $+\infty$), dont l'exponentielle n'est autre que la primorielle vue au lemme 2. La majoration de la primorielle vue à l'occasion de ce lemme 2 donne dès maintenant une majoration de θ au voisinage de $+\infty$:

$$\theta(x) = O(x)$$

On introduit ensuite une nouvelle fonction ϕ qui nous sera utile pour estimer l'intégrale du lemme 5 (avec $u = \theta$).

Définition 9

Pour tout $s \in \mathbb{C}$ tel que $\Re(s) > 1$, on pose :

$$\phi(s) = \sum_{p \in \mathbb{P}} \frac{\ln(p)}{p^s}$$

On établit alors le lien entre ϕ et la fonction θ (on ne manquera pas de remarquer que dans le lemme qui suit, le membre de gauche pour $s = 1$ est l'intégrale dont il faut montrer qu'elle converge pour pouvoir appliquer le lemme 6) :

Lemme 14

Pour tout $s \in \mathbb{C}$ tel que $\Re(s) > 1$, on a :

$$\phi(s) - \frac{s}{s-1} = s \int_1^\infty \frac{\theta(x) - x}{x^{s+1}} dx$$

Démonstration

Soit $s \in \mathbb{C}$ tel que $\Re(s) > 1$. L'estimation $\theta(x) = O(x)$ assure que l'intégrale :

$$\int_1^\infty \frac{\theta(x) - x}{x^{s+1}} dx$$

converge absolument, donc converge. On a ensuite, en notant $(p_n)_{n \geq 0}$ la suite croissante des nombres premiers :

$$\begin{aligned} \int_1^\infty \frac{\theta(x) - x}{x^{s+1}} dx &= \int_1^\infty \frac{\theta(x)}{x^{s+1}} - \int_1^\infty \frac{1}{x^s} = \int_1^\infty \frac{\theta(x)}{x^{s+1}} - \frac{1}{s-1} = \frac{-1}{s-1} + \sum_{n \geq 1} \int_{p_n}^{p_{n+1}} \frac{1}{x^{s+1}} \sum_{i=1}^n \ln(p_i) dx \\ &= \frac{-1}{s-1} + \sum_{n \geq 1} \frac{1}{s} \left(\frac{1}{p_n^s} - \frac{1}{p_{n+1}^s} \right) \sum_{i=1}^n \ln(p_i) dx = \frac{-1}{s-1} + \frac{1}{s} \sum_{i=0}^{+\infty} \ln(p_i) \sum_{n \geq i} \left(\frac{1}{p_n^s} - \frac{1}{p_{n+1}^s} \right) \\ &= \frac{-1}{s-1} + \frac{1}{s} \sum_{i=0}^{+\infty} \frac{\ln(p_i)}{p_i^s} = \frac{-1}{s-1} + \frac{\phi(s)}{s} \end{aligned}$$

L'interversion de sommes étant justifiée par la positivité de la famille sommée $\left(\ln(p_i) \left(\frac{1}{p_n^s} - \frac{1}{p_{n+1}^s} \right) \right)_{1 \leq i \leq n}$.

b) Un théorème taubérien d'analyse complexe

L'objectif va alors être de montrer, à partir de cette formule, que l'intégrale :

$$\int_1^\infty \frac{\theta(x) - x}{x^2} dx$$

converge, pour pouvoir appliquer le lemme 6. Pour ce faire, on va devoir utiliser des théorèmes taubériens d'analyse complexe. On va maintenant énoncer et démontrer ces théorèmes.

Soit f une fonction bornée sur $[0, +\infty[$ et intégrable sur tout compact de $[0, +\infty[$. On suppose que la fonction g définie sur $\{z \in \mathbb{C} \mid \Re(z) > 0\}$ par :

$$g(z) = \int_0^{+\infty} f(t) e^{-zt} dt$$

est bien définie (i.e. l'intégrale converge) et qu'elle se prolonge en une fonction holomorphe (qu'on note encore g) sur un ouvert Ω de $\mathbb{C}$ contenant le demi-plan fermé : $\{z \in \mathbb{C} \mid \Re(z) \geq 0\}$. Le théorème taubérien à démontrer est le suivant :

Lemme 15

Sous les hypothèses ci-dessus, l'intégrale :

$$\int_0^{+\infty} f(t) dt$$

converge.

Démonstration

On introduit $\lambda, R > 0$ et on considère les fonctions h, u, v définies respectivement sur $\mathbb{C}$, $\mathbb{C} \setminus \{0\}$ et $\Omega \setminus \{0\}$ par :

$$\begin{aligned} h(z) &= \int_0^\lambda f(t) e^{-tz} dt \\ u(z) &= e^{\lambda z} h(z) \left(\frac{1}{z} + \frac{z}{R^2} \right) \\ v(z) &= e^{\lambda z} g(z) \left(\frac{1}{z} + \frac{z}{R^2} \right) \end{aligned}$$

On note également M un majorant de $|f(t)|$ pour $t \geq 0$.

On a par inégalités triangulaires, pour $z \in \mathbb{C}$ tel que $x = \Re(z) < 0$:

$$|e^{\lambda z} h(z)| \leq e^{\lambda x} \int_0^\lambda |f(t)| e^{-xt} dt \leq M e^{\lambda x} \int_0^\lambda e^{-xt} dt = M e^{\lambda x} \frac{e^{-\lambda x} - 1}{-x} \leq \frac{M}{|x|}$$

On va également donner une borne pour $u - v$. On fixe $z \in \mathbb{C}$ avec $|z| = R$ et $x = \Re(z) > 0$. On a :

$$\frac{1}{z} + \frac{z}{R^2} = \frac{\bar{z} + z}{R^2} = \frac{2x}{R^2}$$

et donc :

$$|u(z) - v(z)| = e^{\lambda x} \frac{2x}{R^2} \left| \int_\lambda^{+\infty} f(t) e^{-tz} dt \right| \leq \frac{2x e^{\lambda x}}{R^2} M \int_\lambda^{+\infty} e^{-tx} dt = \frac{2M}{R^2}$$

Soit ensuite $\epsilon \geq 0$ et $D(R, \epsilon)$ la partie du plan définie par les inégalités : $|z| \leq R$ et $\Re(z) > -\epsilon$, et $C(R, \epsilon)$ sa frontière, parcourue une fois dans le sens direct. Comme Ω est ouvert, la distance de $D(R, 0)$ au complémentaire de Ω est non nulle et donc on peut fixer $\alpha \in]0, R[$ tel que $D(R, \epsilon)$ soit contenu dans Ω pour tout $\epsilon \in [0, \alpha]$.

La fonction $v - u$ est méromorphe sur Ω , son seul pôle éventuel se trouvant en 0. Le résidu de ce pôle en 0 est $h(0) - g(0)$, et donc le théorème des résidus donne :

$$2\pi i (g(0) - h(0)) = \int_{C(R, \epsilon)} (v(z) - u(z)) dz$$

On note alors C^+ et C^- les intersections respectives de $C(R, \epsilon)$ avec les demi plans $\Re(z) \geq 0$ et $\Re(z) \leq 0$ respectivement. On note :

$$I^+ = \int_{C^+} (v(z) - u(z)) dz \quad J^- = \int_{C^-} u(z) dz \quad K^- = \int_{C^-} v(z) dz$$

La majoration de $|v - u|$ permet alors d'obtenir :

$$|I^+| \leq \int_{C^+} |v(z) - u(z)| dz \leq \int_{C^+} \frac{2M}{R^2} dz = \frac{2\pi M}{R}$$

Estimons de même J^- . Comme u est holomorphe sur $\mathbb{C} \setminus \mathbb{R}_+$ qui est simplement connexe, on peut remplacer C^- par C'^- , le demi-cercle défini par $\Re(z) < 0$ et $|z| = R$ car C^- et C'^- sont homotopes dans $\mathbb{C} \setminus \mathbb{R}_+$. Dès lors, on a :

$$\begin{aligned} |J^-| &= \left| \int_{C^-} u(z) dz \right| = \left| \int_{C'^-} u(z) dz \right| \leq \int_{C'^-} |u(z)| dz \leq \int_{C'^-} |e^{\lambda z} h(z)| \left| \frac{1}{z} + \frac{z}{R^2} \right| dz \\ &\leq \int_{C'^-} \frac{M}{|\Re(z)|} \frac{\bar{z} + z}{R^2} dz \leq \int_{C'^-} \frac{2M}{R^2} dz = \frac{2\pi M}{R} \end{aligned}$$

Enfin, on majore $|K^-|$. On note $G(R)$ un majorant de $|g(z)|$ sur $D(R, \alpha)$. Alors, on découpe C^- en un segment S et deux petits arcs de cercle C_1 et C_2 . On a :

$$\begin{aligned}
|K^-| &= \left| \int_{C^-} v(z) dz \right| \leq \int_S |v(z)| dz + \int_{C_1} |v(z)| dz + \int_{C_2} |v(z)| dz \\
&\leq G(R) \left(\int_S e^{-\lambda\epsilon} \left| \frac{1}{z} + \frac{z}{R^2} \right| dz + \int_{C_1} \left| e^{\lambda\Re(z)} \left(\frac{2\Re(z)}{R^2} \right) \right| dz + \int_{C_2} \left| e^{\lambda\Re(z)} \left(\frac{2\Re(z)}{R^2} \right) \right| dz \right) \\
&\leq G(R) \left(\int_S e^{-\lambda\epsilon} \left(\frac{1}{\epsilon} + \frac{1}{R} \right) dz + 2 \int_{C_1} \left| \left(\frac{2\Re(z)}{R^2} \right) \right| dz \right) \\
&\leq G(R) \left(2Re^{-\lambda\epsilon} \left(\frac{1}{\epsilon} + \frac{1}{R} \right) + 2 \int_{C_1} \frac{2\epsilon}{R^2} dz \right) \leq 2G(R) \left(e^{-\lambda\epsilon} \left(1 + \frac{R}{\epsilon} \right) + \frac{\epsilon}{R^2} \int_{C_1} dz \right) \\
&\leq 2G(R) \left(e^{-\lambda\epsilon} \left(1 + \frac{R}{\epsilon} \right) + \frac{\pi\epsilon^2}{R^2} \right)
\end{aligned}$$

Finalement, avec l'égalité $2\pi i(g(0) - h(0)) = I^+ + J^- + K^-$ et les majorations des trois intégrales, il vient :

$$2\pi|g(0) - h(0)| \leq \frac{4\pi M}{R} + 2G(R) \left(e^{-\lambda\epsilon} \left(1 + \frac{R}{\epsilon} \right) + \frac{\pi\epsilon^2}{R^2} \right)$$

Et donc pour tout $\eta > 0$, on peut fixer $R > 0$ suffisamment grand pour que $\frac{4\pi M}{R} < \eta$, et en prenant $\epsilon > 0$ tel que $D(R, \epsilon) \subset \Omega$ et $2G(R) \frac{\pi\epsilon^2}{R^2} \leq \eta$, on a alors :

$$2\pi|g(0) - h(0)| \leq 2\eta + 2G(R)e^{-\lambda\epsilon} \left(1 + \frac{R}{\epsilon} \right)$$

Et donc pour λ assez grand :

$$2\pi \left| \int_0^\lambda f(t) dt - g(0) \right| \leq 3\eta$$

Ceci étant valable pour tout $\eta > 0$, on a donc obtenu :

$$\int_0^\lambda f(t) dt \xrightarrow{\lambda \rightarrow +\infty} g(0)$$

Ceci conclut la preuve du lemme.

Forts de ce lemme, on va pouvoir montrer la convergence de l'intégrale $\int_a^{+\infty} \frac{\theta(x)-x}{x^2} dx$ et donc conclure.

c) La fonction ζ sur la droite $\Re(z) = 1$ et la conclusion

On considère comme précédemment la fonction ζ définie par :

$$\zeta(s) = \sum_{n=0}^{+\infty} \frac{1}{n^s}$$

pour tout $s \in \mathbb{C}$ tel que $\Re(s) > 1$. La convergence normale sur tout compact de la série assure que la fonction ζ ainsi définie est holomorphe sur le demi plan $\mathcal{P} = \{z \in \mathbb{C} \mid \Re(z) > 1\}$.

On observe alors qu'on a, pour tout $s \in \mathcal{P}$:

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

L'intégrale $\left| \int_n^{n+1} \frac{1}{n^s} - \frac{1}{x^s} dx \right|$ est bornée par $|s|n^{-\Re(s)-1}$ par le théorème des accroissements finis, et donc la fonction ψ définie par :

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

est définie et holomorphe sur le demi-plan $\mathcal{P}_0 = \{z \in \mathbb{C} \mid \Re(z) > 0\}$ comme somme de fonctions holomorphes convergeant normalement sur tout compact. Ceci définit un prolongement holomorphe de ζ à $\mathcal{P}_0$ privé du point 0, prolongement qu'on notera également ζ .

Ensuite, le produit eulérien de la fonction ζ (lemme 3) donne, après avoir pris la dérivée logarithmique (ce qui est légitime, car on a affaire à un produit convergeant normalement sur tout compact) :

$$\forall s \in \mathcal{P}, \quad \frac{\zeta'(s)}{\zeta(s)} = - \sum_{p \in \mathbb{P}} \frac{\ln(p)}{p^s - 1}$$

Pour prolonger analytiquement $\frac{\zeta'}{\zeta}$ à un ouvert contenant $\mathcal{P}$, on a alors besoin du lemme suivant :

Lemme 16

Pour tous $\tau \in \mathbb{R}^*$, $\zeta(\sigma + i\tau)$ est non nul. (Ici, ζ est pris au sens du prolongement à $\mathcal{P}_0$ vu précédemment)

Démonstration

Pour tout $\alpha \in \mathbb{R}$, on a : $3 + 4\cos(\alpha) + \cos(2\alpha) = 3 + 4\cos(\alpha) + 2\cos^2(\alpha) - 1 = 2(\cos(\alpha) - 1)^2 \geq 0$

Dès lors, pour tout $r \in [0, 1[$ et tout $\alpha \in \mathbb{R}$, on a, en notant $\ln$ la détermination principale du logarithme :

$$\begin{aligned} \ln(|1-r|^3 \cdot |1-re^{i\alpha}|^4 \cdot |1-re^{2i\alpha}|) &= 3\ln(|1-r|) + 4\ln(|1-re^{i\alpha}|) + \ln(|1-re^{2i\alpha}|) \\ &= 3\ln(1-r) + 4\Re(\ln(1-re^{i\alpha})) + \Re(\ln(1-re^{2i\alpha})) \\ &= -\Re\left(\sum_{n=1}^{+\infty} \frac{3r^n}{n} + \frac{4r^n e^{ni\alpha}}{n} + \frac{r^n e^{2ni\alpha}}{n}\right) = -\sum_{n=1}^{+\infty} \frac{r^n}{n} (3 + 4\cos(n\alpha) + \cos(2n\alpha)) \leq 0 \end{aligned}$$

Et donc : $|1-r|^3 \cdot |1-re^{i\alpha}|^4 \cdot |1-re^{2i\alpha}| \leq 1$.

Dès lors, soit $\sigma > 1$ et $\tau \in \mathbb{R}$. On a pour tout nombre premier p , avec $r = \frac{1}{p^\sigma} < 1$ et $\alpha = \tau \ln(p)$, on a donc :

$$\left| \left(1 - \frac{1}{p^\sigma}\right)^3 \left(1 - \frac{1}{p^{\sigma+i\tau}}\right)^4 \left(1 - \frac{1}{p^{\sigma+2i\tau}}\right) \right| = |1-r|^3 \cdot |1-re^{i\alpha}|^4 \cdot |1-re^{2i\alpha}| \leq 1$$

d'où :

$$\left| \left(\frac{1}{1 - \frac{1}{p^\sigma}}\right)^3 \left(\frac{1}{1 - \frac{1}{p^{\sigma+i\tau}}}\right)^4 \left(\frac{1}{1 - \frac{1}{p^{\sigma+2i\tau}}}\right) \right| \geq 1$$

En prenant le produit sur tous les nombres premiers, et en utilisant le produit eulérien de la fonction ζ , il vient alors :

$$|\zeta(\sigma)^3 \zeta(\sigma + i\tau)^4 \zeta(\sigma + 2i\tau)| \geq 1 \quad (*)$$

Supposons alors par l'absurde que ζ s'annule en $1 + i\tau$ où τ est un réel non nul. On a alors, comme ζ est holomorphe au voisinage de $1 + i\tau$, pour $\sigma > 1$ tendant vers 1 :

$$\zeta(\sigma + i\tau) = O(\sigma - 1)$$

et comme ζ est continue donc bornée au voisinage de $1 + 2i\tau$, on a pour σ tendant vers 1 :

$$\zeta(\sigma + i\tau) = O(1)$$

Enfin, on a vu que la fonction $s \mapsto \zeta(s) - \frac{1}{s-1}$ se prolonge en une fonction holomorphe, donc continue, au voisinage de 1. On a donc, pour σ qui tend vers 1 :

$$\zeta(\sigma) = O\left(\frac{1}{\sigma - 1}\right)$$

En réunissant les trois dernières estimations, on obtient pour σ tendant vers 1 :

$$\zeta(\sigma)^3 \zeta(\sigma + i\tau)^4 \zeta(\sigma + 2i\tau) = O(\sigma - 1)$$

Ceci contredit la minoration (*) trouvée plus haut, et donc conclut que ζ ne s'annule pas sur $\{1 + i\tau \mid \tau \in \mathbb{R}^*\}$.

On rappelle que la fonction ϕ est définie pour tout $s \in \mathcal{P}$ par :

$$\phi(s) = \sum_{p \in \mathbb{P}} \frac{\ln(p)}{p^s}$$

Alors, pour tout $s \in \mathcal{P}$, on a :

$$\phi(s) + \frac{\zeta'(s)}{\zeta(s)} = \sum_{p \in \mathbb{P}} \ln(p) \left(\frac{1}{p^s} - \frac{1}{p^s - 1} \right) = - \sum_{p \in \mathbb{P}} \frac{\ln(p)}{p^s(p^s - 1)}$$

La série du terme de gauche est une série de fonctions holomorphes qui converge normalement sur tout compact du demi-plan $\mathcal{P}_{1/2} = \{z \in \mathbb{C} \mid \Re(z) > \frac{1}{2}\}$, et donc est holomorphe en la variable s sur ce même demi-plan. Ainsi, la fonction $s \mapsto \phi(s) + \frac{\zeta'(s)}{\zeta(s)}$ se prolonge en une fonction holomorphe sur ce demi-plan $\mathcal{P}_{1/2}$.

Par ailleurs, ζ ne s'annulant en aucun point de la droite $\Re(s) = 1$, la fonction $s \mapsto \frac{\zeta'(s)}{\zeta(s)}$ est bien définie et holomorphe sur un voisinage de $\bar{\mathcal{P}} \setminus \{0\}$. Comme ζ s'écrit $\zeta(s) = \frac{1}{s-1} + \psi(s)$ avec ψ holomorphe sur $\mathcal{P}_0$, $\frac{\zeta'(s)}{\zeta(s)} - \frac{1}{s-1}$ est définie et holomorphe au voisinage de 1. Et donc finalement, la fonction :

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

est définie et holomorphe sur un voisinage de $\bar{\mathcal{P}}$. Comme il en va de même de la fonction $s \mapsto \phi(s) + \frac{\zeta'(s)}{\zeta(s)}$, on a donc enfin montré que la fonction :

$$s \mapsto \phi(s) - \frac{1}{s-1}$$

admet un prolongement holomorphe à un ouvert contenant le demi-plan fermé $\bar{\mathcal{P}} = \{z \in \mathbb{C} \mid \Re(z) \geq 0\}$.

Avec la formule du lemme 7, on en déduit que la fonction :

$$h : s \mapsto \int_1^{+\infty} \frac{\theta(x) - x}{x^{s+1}} dx$$

définie sur le demi-plan $\mathcal{P}$ se prolonge en une fonction holomorphe sur un ouvert contenant le demi-plan fermé $\bar{\mathcal{P}}$. On pose alors naturellement, avec pour objectif d'appliquer le théorème taubérien d'analyse complexe :

$$\forall z \in \mathcal{P}, \quad g(z) = h(z+1) = \int_1^{+\infty} \frac{\theta(x) - x}{x^{z+2}} dx$$

Ce qui précède assure que la fonction g se prolonge en une fonction holomorphe sur un ouvert Ω contenant le demi-plan fermé $\bar{\mathcal{P}}_0 = \{z \in \mathbb{C} \mid \Re(z) \geq 0\}$.

De plus, le changement de variable $x = e^t$ donne, pour tout $z \in \mathbb{C}$ tel que $\Re(z) > 0$:

$$g(z) = \int_0^{+\infty} \frac{\theta(e^t) - e^t}{e^{tz+2t}} e^t dt = \int_0^{+\infty} (\theta(e^t)e^{-t} - 1)e^{-zt} dt$$

De plus, la fonction définie par :

$$f(t) = \theta(e^t)e^{-t} - 1$$

est continue par morceaux et bornée sur $\mathbb{R}^+$ car on sait que $\theta(x) = O(x)$ pour x au voisinage de $+\infty$. Comme g admet un prolongement holomorphe à Ω , toutes les hypothèses sont donc réunies pour appliquer le théorème taubérien du lemme 8 à la fonction f . On en déduit donc que l'intégrale :

$$\int_0^{+\infty} (\theta(e^t)e^{-t} - 1)dt$$

converge, et par le même changement de variable que précédemment, $x = e^t$, on en déduit que l'intégrale :

$$\int_1^{+\infty} \frac{\theta(x) - x}{x^2} dx$$

converge également.

Le lemme 6 assure alors que pour x au voisinage de $+\infty$, on a $\theta(x) \sim x$. Et donc avec le lemme 5, on obtient, pour x au voisinage de $+\infty$:

$$\pi(x) \sim \frac{x}{\ln(x)}$$

Ceci achève la preuve du théorème des nombres premiers.

2 Théorème de la progression arithmétique de Dirichlet

a) Caractères des groupes abéliens finis

Soit G un groupe abélien fini. On notera dans la suite n son cardinal. On définit comme suit les caractères du groupe G :

Définition 10

Un caractère du groupe G est un morphisme de G dans le groupe multiplicatif $\mathbb{C}^*$. L'ensemble des caractères de G sera noté $\hat{G}$.

On notera en particulier χ_0 le caractère trivial, qui prend la valeur 1 en tout point de G .

On a immédiatement quelques propriétés :

Propriétés 1

Soit χ un caractère de G . Alors :

1. χ est à valeurs dans $\mathbb{U}_n$ (le groupes des racines n -ièmes de l'unité)
2. Si $\chi \neq \chi_0$, alors on a :

$$\sum_{g \in G} \chi(g) = 0$$

Et de plus :

$$\sum_{g \in G} \chi_0(g) = |G|$$

3. Pour tout $\chi \in \hat{G}$, χ ne s'annule pas et on a, pour la multiplication des fonctions de G dans $\mathbb{C}$:

$$\chi \bar{\chi} = \chi_0$$

Démonstration

1. C'est une conséquence immédiate du théorème de Lagrange : pour tout $g \in G$, on a $\chi(g)^n = \chi(g^n) = \chi(e) = 1$.
2. On suppose $\chi \neq \chi_0$. Alors, on fixe $g \in G$ tel que $\chi(g) \neq 1$. On a alors, comme $x \mapsto gx$ est une permutation de G :

$$\sum_{x \in G} \chi(x) = \sum_{x \in G} \chi(gx) = \chi(g) \sum_{x \in G} \chi(x)$$

d'où le résultat. Le cas de $\chi = \chi_0$ est évident.

3. Découle immédiatement de 1.

On peut également observer que l'ensemble $\hat{G}$ est naturellement muni d'une structure de groupe :

Propriété 1

La multiplication des fonctions de G dans $\mathbb{C}^*$ fait de $\hat{G}$ un groupe.

Démonstration

On montre que l'ensemble $\hat{G}$ est un sous groupe du groupe des fonctions de G dans $\mathbb{C}^*$.

D'une part, comme pour tout $x \in G$ et tout $\chi \in \hat{G}$, on a $\chi(x)^n = 1$, on a $\chi(x) \neq 0$. Donc $\hat{G}$ est bien un sous-ensemble de $(\mathbb{C}^*)^G$.

Si χ_1 et χ_2 sont deux caractères de G , alors on a pour tous $x, y \in G$:

$$(\chi_1 \chi_2)(xy) = \chi_1(xy) \chi_2(xy) = \chi_1(x) \chi_1(y) \chi_2(x) \chi_2(y) = (\chi_1 \chi_2)(x) (\chi_1 \chi_2)(y)$$

Donc $\chi_1 \chi_2 \in \hat{G}$. On montre de même que $\frac{1}{\chi_1}$ est dans $\hat{G}$.

Enfin, $\hat{G}$ contient χ_0 , l'élément neutre du groupe $(\mathbb{C}^*)^G$.

On munit alors l'espace des fonctions de G dans $\mathbb{C}$ du produit hermitien défini par :

$$\forall f, g \in \mathbb{C}^G, \quad \langle f, g \rangle = \frac{1}{|G|} \sum_{x \in G} f(x) \overline{g(x)}$$

(la vérification qu'il s'agit bien d'un produit hermitien est immédiate)

On a alors le résultat :

Proposition 3

La famille $(\chi)_{\chi \in \hat{G}}$ est orthonormée pour le produit hermitien $\langle, \rangle$.

Démonstration

On a pour tous χ_1, χ_2 , on a :

$$\langle \chi_1, \chi_2 \rangle = \frac{1}{|G|} \sum_{x \in G} (\chi_1 \overline{\chi_2})(x)$$

Et donc si $\chi_1 \neq \chi_2$, on a $\chi_1 \overline{\chi_2} \neq \chi_0$ et donc le deuxième point des propriétés des caractères assure que $\langle \chi_1, \chi_2 \rangle = 0$.

Si au contraire $\chi_1 = \chi_2$, alors on a $\chi_1 \overline{\chi_2} = \chi_0$ et donc $\langle \chi_1, \chi_2 \rangle = 1$.

Ainsi, la famille des caractères de G est une famille libre de l'espace des fonctions de G dans $\mathbb{C}$. On va montrer qu'en fait, elle est même une base de $\mathbb{C}^G$.

Théorème 13

L'ensemble des caractères de G forme une base de $\mathbb{C}^G$.

Démonstration

On sait déjà que les éléments de $\hat{G}$ forment une famille orthonormée pour le produit hermitien $\langle, \rangle$, donc libre. Reste à montrer qu'elle est génératrice. Pour cela, on montre que $\text{Vect}(\hat{G})^\perp = \{0\}$, c'est à dire que la seule fonction f orthogonale à tous les caractères au sens de $\langle, \rangle$ est la fonction nulle. Pour ce faire, on effectue un léger détour par la théorie des représentations des groupes finis.

Soit donc $f : G \rightarrow \mathbb{C}$ une fonction orthogonale à tous les caractères de $\bar{G}$. On considère l'algèbre de groupe $\mathbb{C}[G]$ (c'est à dire les combinaisons linéaires formelles d'éléments de G à coefficients dans $\mathbb{C}$, munies des opérations d'algèbres naturelles induites par celles de G). Alors, pour tout $g \in G$, on note :

$$\begin{aligned} \phi_g : \mathbb{C}[G] &\rightarrow \mathbb{C}[G] \\ \sum_{x \in G} a_x x &\mapsto \sum_{x \in G} a_x (gx) \end{aligned}$$

ϕ_g permute les éléments de G qui forment une base de $\mathbb{C}[G]$, et donc ϕ_g est une application linéaire (immédiat) inversible de $\mathbb{C}[G]$ dans lui-même. On note ceci : $\phi_g \in \text{GL}(\mathbb{C}[G])$. De plus, on a clairement pour tous $g, h \in G$: $\phi_g \circ \phi_h = \phi_{gh}$ et donc l'application :

$$\phi : g \mapsto \phi_g$$

est un morphisme de G dans $\text{GL}(\mathbb{C}[G])$. Ce morphisme est, en théorie des représentations, ce qu'on appelle la "représentation régulière de G ". Maintenant, la famille $(\phi_g)_{g \in G}$ est commutative car ϕ est un morphisme et G est abélien, et tous les ϕ_g sont diagonalisables car ils vérifient $\phi_g^n = \text{id}$. Dès lors, la famille $(\phi_g)_{g \in G}$ est co-diagonalisable (on le prouve en raisonnant par récurrence, et en remarquant que les espaces propres d'un élément de cette famille sont laissés stables par les autres éléments).

Ainsi, comme $\mathbb{C}[G]$ est de dimension $n = |G|$, on dispose d'une base $(e_1, \dots, e_n)$ dans laquelle toutes les matrices des ϕ_g sont diagonales. Mais alors, notons pour tout $g \in G$ et tout $i \in \llbracket 1, n \rrbracket$: $\phi_g(e_i) = \chi_i(g)e_i$ où $\chi_i(g)$ est un complexe. Le fait que pour tous $g, h \in G$, $\phi_{gh} = \phi_g \phi_h$ se traduit par les égalités :

$$\forall g, h \in G, \quad \forall i \in \llbracket 1, n \rrbracket, \quad \chi_i(gh) = \chi_i(g)\chi_i(h)$$

et comme $\phi_e = \text{id}$, on a $\chi_i(e) = 1$ pour tout i . On en déduit finalement que les χ_i sont des caractères du groupe G . Dès lors, par définition de f , on a pour tout $i \in \llbracket 1, n \rrbracket$:

$$\sum_{g \in G} \overline{f(g)} \phi_g(e_i) \sum_{g \in G} \overline{f(g)} \chi_i(g) e_i = 0$$

Et donc comme $(e_1, \dots, e_n)$ est une base de $\mathbb{C}[G]$, l'endomorphisme :

$$T = \sum_{g \in G} \overline{f(g)} \phi_g$$

est nul. On évalue T en l'élément neutre de G , qui est aussi un élément de $\mathbb{C}[G]$:

$$0 = T(e) = \sum_{g \in G} \overline{f(g)} \phi_g(e) = \sum_{g \in G} \overline{f(g)} g$$

Comme les éléments de G forment une base de G , ceci conclut que f est nulle. Ceci achève la preuve.

b) Preuve de Dirichlet

Dans cette section, on va utiliser les résultats qui précèdent sur les caractères des groupes finis pour démontrer le théorème de Dirichlet :

Théorème 14

Soient a, b deux entiers premiers entre eux. Alors l'ensemble :

$$\{ak + b \mid k \in \mathbb{N}\}$$

contient une infinité de nombres premiers.

Dans toute la suite de cette section, on fixe $a, b \leq 1$ deux entiers premiers entre eux. On note $G = (\mathbb{Z}/a\mathbb{Z})^\times$ muni de la multiplication. On considère ensuite dans G la fonction 1_b définie par :

$$\forall \bar{k} \in G, \quad 1_b(\bar{k}) = 1 \text{ si } \bar{k} = \bar{b}, \quad 0 \text{ sinon.}$$

Au vue de la section précédente qui montre que l'ensemble des caractères de G forment une base orthonormée de $\mathbb{C}^G$, on a la décomposition :

$$1_b = \sum_{\chi \in \hat{G}} \langle \chi, 1_b \rangle \chi$$

Pour toute fonction $f : G \mapsto \mathbb{C}$, on dispose alors d'une fonction $f_* : \mathbb{Z} \mapsto \mathbb{C}$ définie par $f_* = f \circ p$ où p est la projection canonique de $\mathbb{Z}$ dans $\mathbb{Z}/a\mathbb{Z}$, et en convenant que $f_*(x) = 0$ si x n'est pas premier avec a . On peut alors écrire :

$$1_{b*} = \sum_{\chi \in \hat{G}} \langle 1_b, \chi \rangle \chi_* = \frac{1}{\phi(a)} \sum_{\chi \in G} \overline{\chi(\bar{b})} \chi_*$$

où ϕ est la fonction d'Euler : $\phi(a)$ est le cardinal du groupe G .

Dans la suite, on écrira souvent par abus de notation χ au lieu de χ_* .

Donnons ensuite les définitions des séries L de Dirichlet, qui seront très utiles dans la suite :

Définition 11

Soit $\chi \in \hat{G}$. Alors, pour tout $s \in \mathbb{C}$ tel que $\Re(s) > 1$, on définit :

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

Pour chaque $\chi \in \hat{G}$, ceci définit une fonction holomorphe sur le demi-plan $\mathcal{P} = \{s \in \mathbb{C} \mid \Re(s) > 1\}$ (car c'est la somme d'une série de fonctions holomorphe convergeant normalement sur tout compact de $\mathcal{P}$).

Comme pour la fonction ζ de Riemann, on a le produit eulérien :

Proposition 4

Pour tout caractère χ de G , pour tout $s \in \mathcal{P}$, on a :

$$L(s, \chi) = \prod_{p \in \mathbb{P}} \frac{1}{1 - \frac{\chi(p)}{p^s}}$$

Démonstration

Comme χ est borné, la famille $(\chi(p)p^{-s})_{p \in \mathbb{P}}$ est sommable en vertu du calcul effectué pour le produit eulérien de la fonction ζ . On en déduit, avec les théorèmes sur les produits de familles sommables :

$$\begin{aligned} \prod_{p \in \mathbb{P}} \frac{1}{1 - \frac{\chi(p)}{p^s}} &= \prod_{p \in \mathbb{P}} \sum_{k=0}^{+\infty} \frac{\chi(p)^k}{p^{sk}} = \prod_{p \in \mathbb{P}} \sum_{k=0}^{+\infty} \frac{\chi(p^k)}{p^{sk}} = \sum_{\substack{p_1 < \dots < p_r \in \mathbb{P} \\ a_1, \dots, a_r \geq 1}} \frac{\chi(p_1^{a_1}) \dots \chi(p_r^{a_r})}{p_1^{a_1 s} \dots p_r^{a_r s}} \\ &= \sum_{\substack{p_1 < \dots < p_r \in \mathbb{P} \\ a_1, \dots, a_r \geq 1}} \frac{\chi(p_1^{a_1} \dots p_r^{a_r})}{p_1^{a_1 s} \dots p_r^{a_r s}} = \sum_{n=1}^{+\infty} \frac{\chi(n)}{n^s} = L(s, \chi) \end{aligned}$$

Ceci conclut.

Dès lors, comme le produit est absolument convergent sur le demi-plan $\mathcal{P}$, on peut dériver logarithmiquement. On obtient :

Proposition 5

Soit $\chi \in \hat{G}$. On a pour tout $s \in \mathcal{P}$:

$$\frac{L'(s, \chi)}{L(s, \chi)} = - \sum_{p \in \mathbb{P}} \frac{\chi(p) \ln(p)}{p^s - \chi(p)}$$

Démonstration

On peut dériver logarithmiquement terme à terme car le produit infini de fonctions holomorphes converge uniformément sur les compacts. Il vient alors, pour tout $s \in \mathcal{P}$, en notant DL l'opérateur dérivée logarithmique :

$$DL(L(s, \chi)) = -DL \left(\prod_{p \in \mathbb{P}} \left(1 - \frac{\chi(p)}{p^s} \right) \right) = - \sum_{p \in \mathbb{P}} DL \left(1 - \frac{\chi(p)}{p^s} \right) = - \sum_{p \in \mathbb{P}} \frac{-\chi(p)p^{-s}(-\ln(p))}{1 - \chi(p)p^{-s}}$$

Soit, après simplification :

$$\frac{L'(s, \chi)}{L(s, \chi)} = - \sum_{p \in \mathbb{P}} \frac{\chi(p) \ln(p)}{p^s - \chi(p)}$$

Pour tout caractère χ , définissons alors $\psi(s, \chi)$ par :

Définition 12

Pour tout $\chi \in \hat{G}$, tout $s \in \mathcal{P}$, on pose :

$$\psi(s, \chi) = \sum_{p \in \mathbb{P}} \frac{\chi(p) \ln(p)}{p^s}$$

Ceci définit clairement une fonction holomorphe sur $\mathcal{P}$ (car on a à nouveau convergence normale d'une série de fonctions holomorphes sur tous les compacts de $\mathcal{P}$).

De plus avec la proposition 3, on a pour tout s tel que $\Re(s) > 1$:

$$\frac{L'(s, \chi)}{L(s, \chi)} + \psi(s) = \sum_{p \in \mathbb{P}} \chi(p) \ln(p) \left(\frac{1}{p^s} - \frac{1}{p^s - \chi(p)} \right) = \sum_{p \in \mathbb{P}} \frac{-\chi(p)^2 \ln(p)}{p^s(p^s - \chi(p))}$$

Cette série de fonctions holomorphes converge normalement sur tout compact du demi-plan $\{s \in \mathbb{C} \mid \Re(s) > \frac{1}{2}\}$, et donc définit une fonction holomorphe sur ce demi-plan. On en déduit le :

Lemme 17

Soit $\chi \in \hat{G}$. La fonction :

$$s \mapsto \psi(s, \chi) + \frac{L'(s, \chi)}{L(s, \chi)}$$

se prolonge en une fonction holomorphe sur tout le demi-plan d'équation $\Re(s) > \frac{1}{2}$.

Puis, on obtient aisément la formule suivante :

Lemme 18

Soit $s \in \mathcal{P}$. Il existe une fonction θ holomorphe sur le demi-plan $\{s \in \mathbb{C} \mid \Re(s) > \frac{1}{2}\}$ telle que :

$$\sum_{\substack{p \in \mathbb{P} \\ p \equiv b \pmod{a}}} \frac{\ln(p)}{p^s} = \theta(s) - \frac{1}{\phi(a)} \sum_{\chi \in \hat{G}} \overline{\chi(b)} \frac{L'(s, \chi)}{L(s, \chi)}$$

Démonstration

Soit $s \in \mathcal{P}$.

$$\sum_{\substack{p \in \mathbb{P} \\ p \equiv b \pmod{a}}} \frac{\ln(p)}{p^s} = \sum_{p \in \mathbb{P}} \frac{\ln(p)}{p^s} 1_b(p) = \sum_{p \in \mathbb{P}} \frac{\ln(p)}{p^s} \frac{1}{\phi(a)} \sum_{\chi \in \hat{G}} \overline{\chi(b)} \chi(p) = \frac{1}{\phi(a)} \sum_{\chi \in \hat{G}} \overline{\chi(b)} \psi(s, \chi)$$

en échangeant une somme finie avec une somme infinie.

On conclut en utilisant le lemme qui précède, sur le prolongement holomorphe de la fonction :

$$s \mapsto \psi(s, \chi) + \frac{L'(s, \chi)}{L(s, \chi)}$$

La fonction L associée à χ_0 n'est autre que la fonction :

$$s \mapsto \zeta(s) \prod_{\substack{p \in \mathbb{P} \\ p|a}} \left(1 - \frac{1}{p^s}\right)$$

Les estimations de la fonction ζ aux alentours du point $s = 1$ effectuées dans la section sur le théorème des nombres premiers montrent qu'alors, pour s tel que $\Re(s) > 1$, au voisinage de 1, on a l'estimation :

$$\sum_{\substack{p \in \mathbb{P} \\ p \equiv b \pmod{a}}} \frac{\ln(p)}{p^s} = \frac{1}{\phi(a)} \frac{1}{s-1} - \sum_{\chi \neq \chi_0} \overline{\chi(b)} \frac{L'(s, \chi)}{L(s, \chi)} + O(1)$$

Il s'agit donc de montrer que, pour tout caractère non trivial χ , on a pour $s \in \mathcal{P}$ tendant vers 1 l'estimation :

$$\frac{L'(s, \chi)}{L(s, \chi)} = O(1) \quad (*)$$

En effet, avec de telles estimations, on obtiendra alors que, pour $s \in \mathcal{P}$ tendant vers 1 :

$$\sum_{\substack{p \in \mathbb{P} \\ p \equiv b \pmod{a}}} \frac{\ln(p)}{p^s} = \frac{1}{\phi(a)} \frac{1}{s-1} + O(1)$$

ce qui impose clairement l'existence d'une infinité de nombres premiers congrus à b modulo a . Les estimations (*) sont l'objet de la section suivante.

c) Estimation des fonctions L au voisinage de 1

Soit χ un caractère non trivial de G .

Le caractère borné des somme partielles du caractère évalué en les entiers permet d'effectuer une sommation d'Abel, qui donne le résultat suivant :

Proposition 6

Soit $\chi \in \hat{G}$ un caractère non trivial de G . La fonction $s \mapsto L(s, \chi)$ se prolonge en une fonction holomorphe sur le demi-plan $\mathcal{P}_0 = \{s \in \mathbb{C} \mid \Re(s) > 0\}$.

Démonstration

On note pour tout $m \in \mathbb{N}$:

$$A_m = \sum_{k=1}^m \chi(k)$$

avec la convention $A_0 = 0$. Alors, la suite A_m est a -périodique, en vertu de la propriété 2 des caractères vues précédemment :

$$\sum_{g \in G} \chi(g) = 0$$

Dès lors, A_m est bornée par une constante M . Une sommation d'Abel donne alors, pour tout $s \in \mathcal{P}$:

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

Soit :

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

Comme la suite $(A_n)_{n \geq 0}$ est bornée, cette série converge normalement sur le demi-plan $\{s \in \mathbb{C} \mid \Re(s) > 0\}$. Elle définit donc un prolongement holomorphe de la fonction $s \mapsto L(s, \chi)$ sur ce demi-plan.

Dans la suite, on notera toujours L ce prolongement analytique au demi-plan $\mathcal{P}_0$.

Ainsi, pour démontrer que $\frac{L'(s, \chi)}{L(s, \chi)}$ est bornée au voisinage de 1, il suffit de montrer que le prolongement analytique de $L(s, \chi)$ ne s'annule pas en $s = 1$. C'est l'objet de la suite de cette section.

On vérifie que $L(1, \chi)$ est non nul séparément pour les caractères réels et pour les caractères non réels, qu'on définit comme suit :

Définition 13

Un caractère $\chi \in \hat{G}$ est dit "réel" si il est à valeurs dans $\mathbb{R}$.

On commence par démontrer que $L(1, \chi)$ est non nul dans le cas où χ est un caractère non réel.

On prouve pour cela le :

Lemme 19

Soit $s > 1$ un réel. Alors, on a :

$$\prod_{\chi \in \hat{G}} L(s, \chi) \geq 1$$

le produit étant réel.

Démonstration

Soit $s > 1$. On a, en notant $\ln$ la détermination principale du logarithme :

$$\begin{aligned} \prod_{\chi \in \hat{G}} L(s, \chi) &= \exp \left(\sum_{\chi \in \hat{G}} \ln \left(\prod_{p \in \mathbb{P}} \left(1 - \frac{\chi(p)}{p^s} \right) \right) \right) = \exp \left(\sum_{\chi \in \hat{G}} \sum_{p \in \mathbb{P}} \ln \left(1 - \frac{\chi(p)}{p^s} \right) \right) \\ &= \exp \left(\sum_{\chi \in \hat{G}} \sum_{p \in \mathbb{P}} \sum_{k=1}^{+\infty} \frac{\chi(p)^k}{k p^{ks}} \right) = \exp \left(\sum_{p \in \mathbb{P}} \sum_{k=1}^{+\infty} \frac{1}{k p^{ks}} \sum_{\chi \in \hat{G}} \chi(p^k) \right) \end{aligned}$$

Reste à montrer que le terme dans l'exponentielle est réel positif. Ceci est une conséquence du fait suivant :
Pour tout entier q , on a :

$$\sum_{\chi \in \hat{G}} \chi(q) \geq 0$$

En effet, si q n'est pas premier avec a , c'est évident. Si au contraire q est premier avec a , alors deux cas se présentent.
· Si $\chi(q) = 1$ pour tout χ , alors il n'y a rien à faire.
· Dans le cas contraire, on dispose de $\chi_1 \in \hat{G}$ tel que $\chi_1(q) \neq 1$. Alors, comme $\chi \rightarrow \chi_1 \chi$ est une permutation du groupe $\hat{G}$, on a :

$$\chi_1(q) \sum_{\chi \in \hat{G}} \chi(q) = \sum_{\chi \in \hat{G}} (\chi_1 \chi)(q) = \sum_{\chi \in \hat{G}} \chi(q)$$

Et donc la somme est nulle.

Ceci termine la preuve du lemme.

On peut en déduire le résultat de non annulation dans le cas où χ est non réel.

Proposition 7

Si $\chi \in \hat{G}$ est un caractère non réel, alors $L(1, \chi) \neq 0$.

Démonstration

Supposons par l'absurde que $L(1, \chi) = 0$. Alors $s \mapsto L(s, \bar{\chi})$ s'annule également en $s = 1$, et comme les fonctions L des caractères non triviaux sont holomorphes au voisinage de 1, on a pour s au voisinage de 1 :

$$L(s, \chi) L(s, \bar{\chi}) = O((s-1)^2)$$

Comme χ et $\bar{\chi}$ sont deux distincts de G et comme les fonctions L associées aux caractères non triviaux sont bornées au voisinage de 1, on en déduit l'estimation pour $s > 1$ au voisinage de 1 :

$$\prod_{\chi_1 \neq \chi_0} L(s, \chi_1) = O((s-1)^2)$$

En utilisant l'estimation effectuée plus tôt de la fonction L associée au caractère trivial au voisinage de 1, on en déduit :

$$\prod_{\chi_1 \in \hat{G}} L(s, \chi_1) = O(s-1)$$

Ceci contredit la minoration du produit ci-dessus démontrée dans le lemme précédent, et donc conclut par l'absurde.

On va maintenant se pencher sur le cas des caractères réels. On fixe dans toute la suite $\chi \in \hat{G}$ un caractère réel. On commence par définir une somme qu'on va estimer de deux manières différentes.

Définition 14

Pour tout $N \in \mathbb{N}^*$, posons :

$$S_N = \sum_{\substack{1 \leq n, m \\ nm \leq N}} \frac{\chi(n)}{(nm)^{\frac{1}{2}}}$$

On donne tout d'abord une minoration de S_N :

Lemme 20

S_N tend vers $+\infty$ quand N tend vers $+\infty$.

Démonstration

Soit $N \in \mathbb{N}^*$. On évalue S_N en regroupant les termes selon les valeurs de nm :

$$S_N = \sum_{\substack{1 \leq n, m \\ nm \leq N}} \frac{\chi(n)}{(nm)^{\frac{1}{2}}} = \sum_{l=1}^N \frac{1}{\sqrt{l}} \sum_{k|l} \chi(k)$$

Maintenant, soit $l \in \mathbb{N}^*$. On écrit $l = p_1^{a_1} \dots p_r^{a_r}$ où les p_i sont premiers distincts et les a_i sont des entiers. Il vient alors, comme χ est complètement multiplicative :

$$\sum_{k|l} \chi(k) = \prod_{i=1}^r \sum_{k|p_i^{a_i}} \chi(k) = \prod_{i=1}^r \sum_{j=0}^{a_i} \chi(p_i)^j$$

Comme χ est réel, il prend des valeurs dans $\{-1, 1\}$ et donc les sommes ci-dessus vérifient :

$$\text{si } a_i \text{ est pair alors : } \sum_{j=0}^{a_i} \chi(p_i)^j \geq 1$$

$$\text{si } a_i \text{ est impair alors : } \sum_{j=0}^{a_i} \chi(p_i)^j \geq 0$$

Et donc comme l est pair si et seulement si les a_i sont tous des carrés, on en déduit :

$$\text{si } l \text{ est un carré alors : } \sum_{k|l} \chi(k) \geq 1$$

$$\text{si } l \text{ n'est pas un carré alors : } \sum_{k|l} \chi(k) \geq 0$$

Dès lors, l'expression de S_N ci dessus donne :

$$S_N \geq \sum_{\substack{l \leq N \\ l \text{ carré parfait}}} \frac{1}{\sqrt{l}} \geq \sum_{m \leq \sqrt{N}} \frac{1}{m}$$

Cette minoration suffit pour conclure.

On donne également une minoration de S_N faisant intervenir $L(1, \chi)$.

Lemme 21

On a pour N au voisinage de $+\infty$ l'estimation :

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

Démonstration

Soit $N \geq 1$. On découpe la somme S_N de la façon suivante :

$$S_N = \sum_{\substack{1 \leq n, m \\ nm \leq N}} \frac{\chi(n)}{\sqrt{nm}} = S_1 + S_2$$

où, par définition :

$$S_1 = \sum_{1 \leq m \leq N^{\frac{1}{2}}} \sum_{N^{\frac{1}{2}} < n \leq \frac{N}{m}} \frac{\chi(n)}{(nm)^{\frac{1}{2}}}$$

$$S_2 = \sum_{1 \leq n \leq N^{\frac{1}{2}}} \sum_{1 \leq m \leq \frac{N}{n}} \frac{\chi(n)}{(nm)^{\frac{1}{2}}}$$

Montrons alors l'existence d'une constante C ne dépendant que de χ telle que pour tous $b \geq a \geq 1$, on ait :

$$\left| \sum_{n=a}^b \frac{\chi(n)}{n^{\frac{1}{2}}} \right| \leq \frac{C}{a^{\frac{1}{2}}} \quad \left| \sum_{n=a}^b \frac{\chi(n)}{n} \right| \leq \frac{C}{a} \quad (**)$$

Pour cela, on note à nouveau $A_n = \sum_{k=0}^n \chi(k)$ pour tout $n \geq 1$ et on écrit :

$$\sum_{n=a}^b \frac{\chi(n)}{n^{\frac{1}{2}}} = \frac{\chi(a)}{a^{\frac{1}{2}}} + \sum_{n=a+1}^b \frac{A_n - A_{n-1}}{n^{\frac{1}{2}}} = \frac{\chi(a)}{a^{\frac{1}{2}}} + \frac{A_b}{b^{\frac{1}{2}}} - \frac{A_a}{a^{\frac{1}{2}}} + \sum_{n=a+1}^b A_{n-1} \left(\frac{1}{(n-1)^{\frac{1}{2}}} - \frac{1}{n^{\frac{1}{2}}} \right)$$

En notant M une borne pour les sommes partielles A_n , on obtient aisément par inégalité triangulaire :

$$\left| \sum_{n=a}^b \frac{\chi(n)}{n^{\frac{1}{2}}} \right| \leq \frac{1+2M}{a^{\frac{1}{2}}} + M \sum_{n=a+1}^b \left(\frac{1}{(n-1)^{\frac{1}{2}}} - \frac{1}{n^{\frac{1}{2}}} \right) \leq \frac{1+3M}{a^{\frac{1}{2}}}$$

On raisonne exactement de la même manière pour la second somme sans les puissances $\frac{1}{2}$ et on obtient finalement les bornes (**).

On peut dès lors borner S_1 . Il vient, pour N tendant vers $+\infty$:

$$|S_1| \leq \sum_{1 \leq m \leq N^{\frac{1}{2}}} \frac{1}{m^{\frac{1}{2}}} \left| \sum_{N^{\frac{1}{2}} < n \leq \frac{N}{m}} \frac{\chi(n)}{n^{\frac{1}{2}}} \right| \leq \sum_{1 \leq m < N^{\frac{1}{2}}} \frac{1}{m^{\frac{1}{2}}} \frac{C}{N^{\frac{1}{4}}} \leq \frac{1}{N^{\frac{1}{4}}} \int_0^{N^{\frac{1}{2}+1}} \frac{1}{x^{\frac{1}{2}}} dx = O(1)$$

Avant d'estimer S_2 , il va nous falloir étudier de près la somme $\sum_{k=1}^n \frac{1}{k^{\frac{1}{2}}}$. On note pour tout $n \in \mathbb{N}^*$:

$$u_n = -2\sqrt{n} + \sum_{k=1}^n \frac{1}{k^{\frac{1}{2}}}$$

Il vient alors, pour $n \in \mathbb{N}^*$ tendant vers $+\infty$:

$$u_n - u_{n-1} = \frac{1}{\sqrt{n}} + 2(\sqrt{n-1} - \sqrt{n}) = \frac{1}{\sqrt{n}} + 2\sqrt{n} \left(\sqrt{1 - \frac{1}{n}} - 1 \right) = \frac{1}{\sqrt{n}} + 2\sqrt{n} \left(\frac{-1}{2n} + O\left(\frac{1}{n^2}\right) \right) = O\left(\frac{1}{n^{\frac{3}{2}}}\right)$$

Donc par le lien suite série, la suite (u_n) converge vers une constante c et on a :

$$u_n - c = \sum_{k \geq n+1} u_k - u_{k-1} = \sum_{k \geq n+1} O\left(\frac{1}{k^{\frac{3}{2}}}\right) = O\left(\frac{1}{n^{\frac{1}{2}}}\right)$$

On a donc obtenu le développement limité pour n au voisinage de $+\infty$:

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

On peut maintenant estimer S_2 . Il vient :

$$\begin{aligned}
S_2 &= \sum_{1 \leq n \leq N^{\frac{1}{2}}} \frac{\chi(n)}{n^{\frac{1}{2}}} \sum_{1 \leq m \leq \frac{N}{n}} \frac{1}{m^{\frac{1}{2}}} = \sum_{1 \leq n \leq N^{\frac{1}{2}}} \frac{\chi(n)}{n^{\frac{1}{2}}} \left(2 \left(\frac{N}{n} \right)^{\frac{1}{2}} + c + O \left(\left(\frac{n}{N} \right)^{\frac{1}{2}} \right) \right) \\
&= 2N^{\frac{1}{2}} \sum_{1 \leq n \leq N^{\frac{1}{2}}} \frac{\chi(n)}{n} + 2c \sum_{1 \leq n \leq N^{\frac{1}{2}}} \frac{\chi(n)}{n^{\frac{1}{2}}} + \sum_{1 \leq n \leq N^{\frac{1}{2}}} O \left(\frac{1}{N^{\frac{1}{2}}} \right) \\
&= 2N^{\frac{1}{2}} L(1, \chi) - 2N^{\frac{1}{2}} \sum_{n > N^{\frac{1}{2}}} \frac{\chi(n)}{n^{\frac{1}{2}}} + O(1) = 2N^{\frac{1}{2}} L(1, \chi) + O(1)
\end{aligned}$$

Finalement, on a donc obtenu pour N au voisinage de $+\infty$:

$$S_N = S_1 + S_2 = 2N^{\frac{1}{2}} L(1, \chi) + O(1)$$

On en déduit aisément la non annulation de $L(1, \chi)$:

Proposition 8

Si χ est un caractère réel, alors $L(1, \chi) \neq 0$.

Démonstration

En effet, avec les notations des deux derniers lemmes, si $L(1, \chi)$ était nul, alors le lemme précédent assurerait que (S_N) est borné, ce qui contredit le lemme 13. On en déduit par l'absurde que $L(1, \chi)$ est non nul.

Ainsi, on a montré que pour $\chi \in \hat{G}$ un caractère non trivial, $L(1, \chi)$ est non nul. Dès lors, la remarque faite à l'issue de la proposition 4 assure que pour tout caractère non trivial, la fonction :

$$s \mapsto \frac{L'(s, \chi)}{L(s, \chi)}$$

est bornée au voisinage de 1.

Dès lors, avec le lemme 11 et les estimations de la fonction ζ au voisinage de 1, on obtient l'estimation pour $s \in \mathcal{P}$ tendant vers 1 :

$$\sum_{\substack{p \in \mathbb{P} \\ p \equiv b \pmod{a}}} \frac{\ln(p)}{p^s} = \frac{1}{\phi(a)} \frac{1}{s-1} + O(1)$$

Ceci achève la preuve du théorème de la progression arithmétique de Dirichlet.

V Bibliographie

1. Oaux X-ENS Algèbre 1, Francinou, Gianella, Nicolas, 2014
2. Franz Mertens, Ein Beitrag zur analytischen Zahlentheorie, Journal für die reine und angewandte Mathematik, 1874
3. Bernard Tessler, Crible de Brun, Séminaire Delange-Pisot-Poitou - Théorie des nombres, tome7, no2 (1965-1966).
4. Capes Externe, Mathématiques 2, session 2008

5. Concours ENS Ulm, Mathématiques 1, session 1993
6. Les Nombres premiers, entre l'ordre et le chaos, Gérald Tenenbaum, Michel Mendès France
7. Problèmes d'Analyse pour l'Agrégation, François Rouvière, 1999