LE THÉORÈME DE DIRICHLET

Le théorème de la progression arithmétique

SABIR ILYASS

28 Mars 2021

Introduction:

Dans ce livre on sert à montrer l'un des plus grands résultats sur les nombres premiers, tout le monde sait qu'est-ce qu'un nombre premier, ils s'agitent des entiers qui n'admettent qu'exactement deux diviseurs positifs (1 et lui-même), mais l'importance des nombres premiers se cache derière sa répartition dans l'ensemble des nombres premiers, et plusieurs mathématiciens sont s'interesser à cette fameuse problèmatique, on sait d'après Euclide qui a montré que les nombres premiers sont infinis,mais malheureusement le problématique reste encore sans une grande précision, plusieurs résultats sont apparisent de temps en temps avec le grand développement des mathématiques, et je cite un résultat qui a été démontré en XIX$^{\text{éme}}$ siècle, après une concentration des efforts des mathématiciens en vue de démontrer le théorème des nombres premiers, conjecturé pa GAUSS; si $\pi(n)$ désigne le nombre d'entiers premiers inférieurs ou égaux à n, alors

$$\pi(n) \underset{n\to+\infty}{\sim} \frac{n}{\log(n)}$$

plusieurs démonstrations sont proposées pour montrer ce résultat (franchement je connut une seule démonstration qui utilise quelques propriétés de la fonction Zeta de REIMANN).

Puisque $\frac{n}{\log(n)} \underset{n\to+\infty}{\to} 0$,on notera alors la raréfaction des nombres premiers à l'infini

La recherche des nouveaux nombres premiers est une activité qui n'intéresse pas seulement les mathématiciens, puisque ces applications ne sont pas limitées seulement en mathématiques, notamment les informaticiens utilisent des algorithmes de cryptage des données pour trouver des nouveaux nombres premiers, et beaucoup de grands nombres premiers connus sont des nombres de Mersenne

$M_p = 2^p - 1$, où p est premier, En 1644, Mersenne affirma que M_p étant premier pour les valeurs $p = 2, 3, 5, 7, 13, 17, 19, 31, 67, 127, 257$ et composé pour les autres valeurs de p premier inférieur à 257. Mais en 1806, Pevasin t Seelhoff démontrèrent que M_{61} étant premier. En 1876, Lucas établit une méthode efficace pour tester la primalité de M_p (et prouva ainsi que M_{127} était premier), En septembre 2006 le 44-ième nombre de Mersenne premier a été découvert : il s'agit de $M_{32582657}$ et il possède 9802358 chiffres, et les nombres de Mersenne premiers sont pourtant rares: 51 sont connus début 2020. Leur recherche fait l'objet d'un projet de calcul collaboratif, le projet-GIMPS. On ne sait pas s'il existe une infinité de nombres de Mersenne premiers.

Si vous êtes intéressé, je vous conseille fortement de chercher quelques résultats sur les nombres de Mersenne, notamment le test de primalité de Lucas-Lehmer...,vous trouverez beaucoup de jolis résultats sur ce sujet.

Passant maintenant à notre résultat de ce livre : le théorème de la progression arithmétique de Dirichlet, je n'entre pas dans le contexte historique ici, et je le laissais après, puisque pour moi le contexte historique est important d'être indiqué seulement en introduction, bref, le **théorème de la progression arithmétique**, s'énonce de la façon suivante :

✠✠✠✠✠✠✠✠✠✠

Pour tout entier n non nul et tout entier m premier avec n, il existe une infinité de nombres premiers congrus à m modulo$n$ (c'est-à-dire de la forme $m + a.n$ avec a entier).

✠✠✠✠✠✠✠✠✠✠

Ce théorème est une généralisation du théorème d'Eulide sur les nombres premiers. Sa première démonstration, due au mathématicien allemand Gustav Lejeune Dirichlet en 1838, fait appel aux résultats de l'arithmétique modulaire et à ceux de la théorie analytique des nombres. La première démonstration « élémentaire » est due à Atle Selberg en 1949.

SABIR ILYASS.

Remerciements

Je tiens à remercier ma merveilleuse mère, mon père, mes frères et ma sœur pour votre aide très aimable. vous m'avez toujours encouragé, vous m'avez donné la force tout au long de ma vie.

Merci à tous mes amis et amies, notamment mon ami BOUAZAOUI ABDLLAH qui m'a beaucoup aidé plusieurs fois. Merci infiniment de votre soutien, et d'être toujours à mon côté chaque fois que j'ai besoin de vous.

Le livre est dédié à vous tous.

Table des matières

.Résumé.....8
.Histoire.....9

.Notations and definitions 12
.l'objectif principale:.....14

.Quelques exemples et premiers résultats:.....15

.Le premier théorème de Mertens.....21

.Quelques résultats sur les groupes finis.....27

.La démonstration du théorème de Dirichlet.....31

.Généralisations.....56

Résumé

Dans ce livre, je vais donner la preuve d'un résultat fondamental autour des nombres premiers, on sait d'après le théorème d'Euclide qu'il y a une infinité des nombres premiers, et il est très facile de montrer ce résultat (je ne donnerai pas la preuve de ce résultat ici car ce n'est pas l'objectif principal de ce livre, mais si quelqu'un veut en voir la preuve, vous pouvez visiter le site suivant : https://www.cantorsparadise.com/how-to-prove-the-infinity-of-primes-9ccfbe9bdd6a).

l'une des plus grandes questions des mathématiques est : comment les nombres premiers sont répartis dans le groupe entier

Malgré le grand développement que les mathématiques ont atteint, nous ne pouvons pas en savoir beaucoup sur la distribution des nombres premiers, où il existe de nombreuses conjectures qui n'ont pas encore été prouvées, comme la conjecture de Goldbach, l'hypothèse de Reimann sur la fonction ZETA . . .

Cependant, cela ne veut pas dire que nous ne savons rien de la distribution des nombres premiers; Il y a donc beaucoup de merveilleux résultats sur les nombres premiers, bien qu'ils ne soient pas beaucoup, mais cela fournit une réponse partielle sur la problématique de la distribution des nombres premiers.

Et l'un des plus beaux résultats sur les nombres premiers est le théorème de Dirichlet, qui stipule que pour tout $(a,b) \in \mathbb{N}^\star \times \mathbb{N}^\star$ premiers entre eux, il existe une infinité de nombres premiers de la forme $a.n+b$ avec a un entier.
Autrement dit:$\forall (a,b) \in \mathbb{N}^\star \times \mathbb{N}^\star$ premiers entre eux, on a:

$$\#\{n \in \mathbb{N} / a.n+b \text{ est premier}\} = +\infty$$

À la fin, je dirai que l'étude des nombres premiers et de leur distribution est très importante pour l'avancement des mathématiques, de l'informatique et aussi de la physique. . .

Histoire :

[1]L'intérêt pour les nombres premiers est ancien et omniprésent dans l'histoire des mathématiques. Euclide y consacre le livre VII de ses éléments. On peut aussi citer les travaux de Sun Zi, établissant vers l'an -300, dans son manuel Sunzi Suanjing, une première version du théorème des restes chinois et surtout Qin Jiushao qui, dans son Traité mathématique en neuf section (1247), en développe une version suffisamment sophistiquée pour dépasser le niveau européen du xvii^{e} siècle. George Sarton le considère comme l'un des plus grands mathématiciens de tous les temps.

Le xvii^{e} siècle est celui où les mathématiques européennes, et particulièrement françaises, se réapproprient le savoir de l'Antiquité et l'apport de la civilisation arabe. En 1621, Claude-Gaspard Bachet de Méziriactraduit en latin les Arithmétiques de Diophante d'Alexandrie. Pierre de Fermat l'annote.

Au xviii^{e} siècle, Leonhard Euler résout plusieurs équations diophantiennes laissées ouvertes par le siècle précédent. On peut citer ses travaux sur le théorème des deux carrés de Fermat ou son attaque du « dernier théorème de Fermat » pour le cas $n=3$. Dans ce domaine, il se montre particulièrement adroit en résolvant pour la première fois des problèmes ouverts depuis parfois plus d'un siècle.

En 1735, à la suite d'une étude pour la résolution du problème de Mengoli, Euler étudie des produits infinis. Deux ans plus tard, il utilise une étrange formule maintenant nommée produit eulérien. Son écriture en série est celle de la fonction ζ de Riemann. Elle offre la première information statistique sur la distribution des nombres premiers.

En 1775, Euler énonce le théorème pour une suite arithmétique de premier terme 1.

1. Histoire : https://fr.wikipedia.org/wiki/Th%C3%A9or%C3%A8me_de_la_progression_arithm%C3%A9tique

Dix ans plus tard, Adrien-Marie Legendre énonce le théorème de la progression arithmétique dans le cas général. Il croit le démontrer en 1808, via un lemme (faux), qui affirmait qu'étant donnés deux entiers m et n premiers entre eux, et k nombres premiers impairs ne divisant pas n, il existe au moins un entier j compris (au sens large) entre 1 et p_k (le $k-i$ème nombre premier, à partir de $p_1=2$) tel que $-m+j.n$ ne soit divisible par aucun de ces k nombres premiers.

En 1801, Carl Friedrich Gauss publie ses célèbres Disquisitiones arithmeticae. Il offre les bases d'une théorie algébrique des nombres, que l'on appelle arithmétique modulaire. Son livre analyse les propriétés de $\mathbb{Z}/n\mathbb{Z}$ et, pour démontrer la loi de réciprocité quadratique, développe un cas particulier de caractère d'un groupe fini : le symbole de Legendre.

En 1837, Dirichlet démontre une première version de son théorème de la progression arithmétique, en supposant que n est premier. Il démontre l'année suivante le cas où n n'est pas premier et en 1841, généralise la démonstration aux entiers de Gauss.

La démonstration est d'un intérêt considérable en arithmétique. Elle relie la nouvelle théorie de Gauss aux idées, apparemment si éloignées, d'Euler. Il enrichit de plus chacune des deux branches.

L'apport algébrique pour la théorie des nombres consiste essentiellement dans le développement de l'analyse harmonique. Dirichlet a travaillé sur les découvertes de Joseph Fourier (1768-1830). Pour la démonstration de son théorème, il utilise les mêmes méthodes, cette fois pour un groupe abélien fini. Jacobi dit de lui : « En appliquant les séries de Fourier à la théorie des nombres, Dirichlet a récemment trouvé des résultats atteignant les sommets de la perspicacité humaine 12 ». La théorie des caractères d'un groupe fini pour le cas abélien est pratiquement complète.

Son apport en analyse est non moins innovateur. À chaque caractère, il associe un produit infini analogue à celui d'Euler. Il montre l'équivalence de ces produits à des séries, maintenant nommé série L de Dirichlet dont un cas particulier est la fonction ζ de Riemann. L'essentiel de la démonstration consiste alors à déterminer si l'unité est oui ou non une racine de ces séries. On reconnait là, l'analogie profonde avec l'hypothèse de Riemann. Cet article marque la naissance d'une nouvelle branche des mathématiques : la théorie analytique des nombres avec ses outils fondamentaux : les produits eulériens, ou les séries L de Dirichlet et son intime relation avec l'arithmétique modulaire.

Johann Peter Gustav Lejeune Dirichlet
(13 février 1805, Düren 5 mai 1859, Göttingen) est un mathématicien prussien qui apporta de profondes contributions à la théorie des nombres, en créant le domaine de la théorie analytique des nombres et à la théorie des séries de Fourier. On lui doit d'autres avancées en analyse mathématique. On lui attribue la définition formelle moderne d'une fonction.[2]

2. Johann Peter Gustav Lejeune Dirichlet : https://fr.wikipedia.org/wiki/Johann_Peter_Gustav_Lejeune_Dirichlet

Notations et définitions :

- $\mathbb{N}$: l'ensemble des nombres entiers naturels.
- $\mathbb{N}^\star$: l'ensemble des nombres entiers naturels sauf 0.
- $\mathbb{Z}$: l'ensembles des entiers relatifs
- $\mathbb{R}$: l'ensemble des nombres réels.
- $\mathbb{C}$: l'ensemble des nombres complexes.
- $\mathcal{P}$: l'ensemble des nombres premiers.
- $\mathcal{P}^+$: l'ensemble des nombres premiers positifs.
- $\mathbb{Z}[X]$: l'ensemble des polynômes à coefficients dans $\mathbb{Z}$.
- $\mathbb{C}[X]$: l'ensemble des polynômes à coefficients dans $\mathbb{C}$.
- Les symboles n, m (respectivement x) désigneront des nombres entiers (respectivement, un nombre réel) >1.
- Le symbole p désignera toujours un nombre premier.
- On désigne par $v_p(n)$ la plus grande puissance, éventuellement nulle, de p divisant n.
- L'entier $[x]$ désigne la partie entière de x.
- Pour tout entiers $a, b \in \mathbb{N}$, on note $a \wedge b$ le plus grand commun diviseur de ces deux entiers.
- Si f, g sont deux fonctions numériques définies au voisinage de $+\infty$, l'écriture $f = O(g)$ signifie que f est produit de g par une fonction bornée au voisinage de $+\infty$.
- De même, si $(u_n)_{n\in\mathbb{N}}$ et $(v_n)_{n\in\mathbb{N}}$ sont deux suites à valeurs complexes, l'écriture $u_n = O(v_n)$ signifie que la suite u_n est produit de la suite v_n par une suite bornée au voisinage de $+\infty$.
- La notation $\sum_{d/n} u_d$ désigne la somme des u_d étendue aux entiers $d>1$ divisant n.

- On désigne par log le logarithme népérien.
- On se donne un entier non nul N fixé une fois pour toutes. On note G(N) le groupe multiplicatif des éléments inversibles de l'anneau $\mathbb{Z}/N\mathbb{Z}$.
- Pour tout fonction $f : \mathbb{N} \to \mathbb{C}$, on dit que f est arithmétique, si pour tout $n, m \in \mathbb{N}$, premiers entre eux, on a $f(n.m) = f(n)f(m)$

l'objectif principale:

On veut montrer le résultat suivant :

Pour tout $(a,b)\in\mathbb{N}^\star\times\mathbb{N}^\star$ premiers entre eux, on a une infinité de nombres premiers qui s 'écrivent sous la forme: $a.n+b$, avec $a\in\mathbb{N}$

$\star\star\star\star\star\star\star\star\star\star\star\star\star\star\star\star\star\star\star\star$

Remarque 1.

Soit $(a,b)\in\mathbb{N}^\star\times\mathbb{N}^\star$, si a et b ne sont pas premiers entre eux,$(a\wedge b>1)$,Alors on a pour tout entier $n\in\mathbb{N}$:

$$a.n+b=a\wedge b\left(\frac{a}{a\wedge b}n+\frac{b}{a\wedge b}\right)$$

Donc, par définition d'un nombre premier, on peut trouver au plus un nombre permier de la forme $a.n+b=a\wedge b\left(\frac{a}{a\wedge b}n+\frac{b}{a\wedge b}\right)$

On en déduit que la condition a et b sont premiers entre eux est une condition nécessaire pour que le résultat soit vrai, on va montrer donc la suite que cette condition est suffisante.

$\star\star\star\star\star\star\star\star\star\star\star\star\star\star\star\star\star\star\star\star$

Quelques exemples et premiers résultats

Avant de commancer d'attaquer la démonstration de notre théorème principale de ce livre, on va commancer par voir quelques exemples qui montre la validité de ce théorème pour des cas particuliers.

Exemple 1 :

On sait d'après le lemme d'Euclide qu'il existe une infinité de nombres premiers, et puisque les nombres premiers sont tous impairs sauf 2, alors il existe une infinité de nombres premiers de la forme : $2n+1$, avec $n \in \mathbb{N}$.

Donnons maintenant une question

Question 1:

Existe-il une infinité de nombres premiers congrus à 3 modulo 4 ?

Réponse.

Raisonnons par l'absurde, et supposons qu'il n'en existe qu'un nombre fini n, Notons-les $p_1, \ldots, p_n$, et considérons l'entier $N = 4.p_1 \ldots p_n - 1 \geqslant 2$

Aucun des p_k ne divise N, puisque N est impair et ses diviseurs premiers ne sont pas dans l'ensemble $\{p_1, \ldots, p_n\}$, donc ils ne sont pas congrus à 3 modulo 4, par imparité et le primabilité, tous les diviseurs premiers de N sont congus à 1 modulo 4, et donc N est congru à 1 modulo 4. Or, manifestement, N est congru à 3 modulo 4, ce qui est contradictoire.

De la même manière, on peut montrer qu'il existe une infinité de nombre premiers de la forme $4n+1$, et bien beaucoup d'autres...

Pasons une question plus forte :

Question 2:

Existe-il une infinité de nombres premiers de la forme :$3n+1$,et une infinité de nombres premiers de la forme : $4n+15$ (Nous l'avons déjà mentionné), et une infinité de nombres premiers de la forme : $5n+1$...

De manière générale,pour un entier $\lambda \in \mathbb{N}^\star$, Existe-il une infinité de nombres premiers de la forme :$\lambda n+1$

Réponse.

La réponse est OUI, mais il faut montrer ca, En se basans sur une méthode due au Leonard Euler qui à utilisé les polynôme cyclotomique pour montrer ce résultat (qu'on pourra le vu comme une version faible du théorème de la progression arithmétique de Dirichlet

Commancans par définir les polynômes cyclotomiques:

Définition 1 .

Soit $n \in \mathbb{N}^\star$, on définie le n-ième polynôme cyclotomique par :

$$\Phi_n = \prod_{\substack{1 \leqslant k \leqslant n \\ k \wedge n = 1}} \left(X - e^{\frac{2i.k\pi}{n}} \right)$$

Théorème 1.

Pour tout $n \in \mathbb{N}^\star$, on a : $\Phi_n \in \mathbb{Z}[X]$

Démonstration. (Théorème 1) □

Soit $n \in \mathbb{N}^\star$,

Montrons que $X^n - 1 = \prod_{d|n} \Phi_d$. On sait que : $X^n - 1 = \prod_{l=1}^{n} \left(X - e^{\frac{2i.k\pi}{n}} \right)$

Notons pour tout entier $d \geqslant 1$, R_d :l'ensemble des racines primitives d-ièmes de l'unité et $\mathbb{U}_d$ l'ensemble des racines d-ièmes de l'unité.

On a, par définition, $\Phi_n = \prod_{\xi \in R_n} (X - \xi)$. Si $\xi \in \mathbb{U}_n$, l'ordre de ξ est un diviseur d de n ett alors $\xi \in R_d$

Par conséquent $\mathbb{U}_n$ est une réunion disjointe des R_d pour $d|n$, d'où il résulte

$$X^n - 1 = \prod_{\xi \in R_n} (X - \xi) = \prod_{d|n} \left(\prod_{\xi \in R_d} (X - \xi) \right) = \prod_{d|n} \Phi_d$$

Nous allons établir que Φ_n est à coefficients entiers par récurrence sur $n \geqslant 1$ en utilisant le résultat suivant:

Lemme 1.

Soient A et B deux polynômes à coefficients entiers, B étant non nul unitaire. Alors Q et R, le quotient et le reste de la division euclidienne de A par B dans $\mathbb{C}[X]$ sont aussi à coefficients entiers.

Démonstration. (Le lemme 1) □

On a la division euclidienne est invariant par extension de corps alors $Q, R \in \mathbb{Q}[X]$.
On a : $A = B.Q + R$
On définit l'application $\mathcal{C}: \mathbb{Z}[X] \to \mathbb{Z}$ par

$$\forall P = \sum_{n=0}^{N} a_n X^n \in \mathbb{Z}[X], \mathcal{C}(P) = \bigwedge_{n=0}^{N} a_n$$

On a pour: $P = \sum_{n=0}^{N} a_n X^n, Q = \sum_{n=0}^{M} b_n X^n \in \mathbb{Z}[X]$

On a par définition de $\mathcal{C}$, $\frac{P}{\mathcal{C}(P)}, \frac{Q}{\mathcal{C}(Q)} \in \mathbb{Z}[X]$, et les coefficients de P (resp. de $\frac{Q}{\mathcal{C}(Q)}$) sont premiers entre eux.

On a pour tout entier premier p: p ne divise pas tout les coefficients de $\frac{P}{\mathcal{C}(P)}$ (resp. de $\frac{Q}{\mathcal{C}(Q)}$), alors on a dans $\mathbb{Z}/P\mathbb{Z}[X]$, $\frac{P}{\mathcal{C}(P)} \neq 0$ et $\frac{Q}{\mathcal{C}(Q)} \neq 0$.

Or $\mathbb{Z}/p\mathbb{Z}$ est un corps, alors l'anneau $\mathbb{Z}/p\mathbb{Z}[X]$ est intègre,

Alors dans $\mathbb{Z}/p\mathbb{Z}[X]$ on a $\frac{P}{\mathcal{C}(P)}.\frac{Q}{\mathcal{C}(Q)} \neq 0$, et donc p ne divise pas tout les coefficients de $\frac{P}{\mathcal{C}(P)}.\frac{Q}{\mathcal{C}(Q)}$,et donc ne divise pas $\mathcal{C}\left(\frac{P}{\mathcal{C}(P)}.\frac{Q}{\mathcal{C}(Q)}\right)$,et ceci pour tout nombre premier p

Alors $\mathcal{C}\left(\frac{P}{\mathcal{C}(P)}.\frac{Q}{\mathcal{C}(Q)}\right) = 1$ par suite $\mathcal{C}(P.Q) = \mathcal{C}(P)\mathcal{C}(Q)$

Soit $b \in \mathbb{N}^\star$, un entier tel que $b.Q, b.R \in \mathbb{Z}[X]$, on a alors :

$$b.A = (b.B)Q + b.R$$

Donc

$$\mathcal{C}(b.A - b.R) = \mathcal{C}(B(b.Q)) = \mathcal{C}((B))\mathcal{C}(b.Q) = \mathcal{C}(b.Q)$$

Avec B et A sont unitaires, alors Q est unitaire aussi, et donc le coefficient dominant de $b.Q$ est b, en particulier : $\mathcal{C}(b.Q)|b$, donc $\frac{b}{\mathcal{C}(b.Q)} \in \mathbb{N}$

De même on montre que $b|\mathcal{C}(b.Q)$, donc $\mathcal{C}(b.Q) = b$
Ainsi : $Q = \frac{b.Q}{\mathcal{C}(b.Q)} \in \mathbb{Z}[X]$, par suite $R = A - B.Q \in \mathbb{Z}[X]$

D'où le résultat.

Etablissons maintenant par récurrence sur n que Φ_n est à coefficients entiers

*C'est vrai pour $n=1$ (par définition)

*Si $n \geqslant 2$, Φ_n est le quotient dans $\mathbb{C}[x]$ de X^n-1 par B, où B est égal au produit des Φ_d, où d est un diviseur strict de n.

Si on suppose la propriété vraie pour les entiers inférieurs ou égal à $n-1$, chacun de ces Φ_d est à coefficients entièrs et unitaire par définition, donc B est aussi à coefficients entiers et unitaire, En vertu de lemme 1, Φ_n est à coefficients entiers.

Soit p un nombre premier qui divise $\Phi_n(a)$, où $a \in \mathbb{Z}$, mais ne divise aucun $\Phi_d(a)$, où d décrit l'ensemble des diviseur stricts de n.

Soit $a \in \mathbb{Z}$,

Comme p divise $\Phi_n(a)$, il divise aussi : a^n-1, Ainsi, l'ordre de $\overline{a}$ dans le groupe multiplicatif $(\mathbb{Z}/p\mathbb{Z})^\star$ divise n, Montrons que cet ordre est exactement n, $d<n$, on a dans $\mathbb{Z}/p\mathbb{Z}$

$$\overline{a}^d - 1 = \prod_{d'|d} \overline{\Phi_{d'}(a)}$$

Or, si d' divise d, d' divise aussi n et par hypothèse sur p, $\overline{\Phi_{d'}(a)} \neq 0$, Comme $\mathbb{Z}/p\mathbb{Z}$ est un coprs, le produit de ces éléments non nuls est également non nul,, si bien que $\overline{a}^d \neq 1$. L'ordre de $\overline{a}$ est donc n. Comme cet ordre divise $p-1$ d'après le théorème de Lagrange, p est de la forme $\lambda n+1 \quad$ avec $\lambda \in \mathbb{N}$.

Montrons maintenant que pour $n \geqslant 1$ fixé, il existe une infinité de nombres premiers de la forme : $\lambda n+1 \quad$ avec $\lambda \in \mathbb{N}$.

Raisonnons par l'absurde et supposons qu'il existe qu'un nombre fini d'entiers premiers congrus à 1 modulo n, soit p_1,..., p_q .La question précédente, si on arrive à trouver a et p vérifiant les hypothèses, assure que p est congru à 1 modulo n

Ce sera insuffisant pour aboutir à une contradiction, p pouvant être alors un des p_i. Pour éviter cela, on va changer n en $N = n.p_1 \ldots p_q$ Si p est congru à 1 modulo N, p ne peut être un des p_i et pourtant, il est congru à 1 modulo n

Il faut donc trouver $a \in \mathbb{Z}$ et p premier, tels que p divise $\Phi_N(a)$, mais aucun des $\Phi_d(a)$, pour $d|N, d<N$. On note $B = \prod_{d|N, d<N} \Phi_d$. Le problème est donc de trouver $a \in \mathbb{Z}$ et p premier tels que p divise $\Phi_N(a)$,et ne divise pas $B(a)$

Puisque les deux polynômes B et Φ_N sont scindés sur $\mathbb{C}$ et n'ont aucune racine commune, alors ils sont premiers entre eux dans $\mathbb{C}[X]$, donc dans $\mathbb{Q}[X]$, puisque ces polynômes sont à coefficients rationnels et que le pgcd est invariant par extension de corps.

D'après le théorème de Bezout, il existe donc un coupl $(U, V) \in \mathbb{Q}[X]^2$ tel que $U\Phi_N + \mathrm{VB} = 1$. Il existe $a \in \mathbb{Z}$ tel que $U' = a.U$ et $V' = a.V$ appartient à $\mathbb{Z}[X]$

Comme $\Phi_N \neq 0$ et $\Phi_N \neq \pm 1$. On peut même choisir a tel que $\Phi_N(a) \neq 0$ et $\Phi_N(a) \neq \pm 1$, étant donnée l'infinité de $a \in \mathbb{Z}$ vérifiant $a.U \in \mathbb{Z}[X]$ et $a.V \in \mathbb{Z}[X]$

On a donc $a = U'\Phi_N + V'B$ et en particulier $a = U'(a)\Phi_N(a) + V'(a)B(a)$ $(\star)$

Soit p un nombre premier divisant $\Phi_N(a)$, Alors p divise $a^N - 1$, car Φ_N divise $X^N - 1$ dans $\mathbb{Z}[X]$. Dans $\mathbb{Z}/p\mathbb{Z}$, $\overline{a}^N = 1$, et donc $\overline{a}$ est inversible, ce qui signifie que a est premier avec p. si p divise $B(a)$, il diviserait a, d'après $(\star)$, ce qui est exclu.

On est donc dans les hypothèses: p est congru à 1 modulo N, et donc modulo n, avec p forcément distincr des p_i, pour $1 \leqslant i \leqslant q$, C'est la contradiction voulue.

$\star\star\star\star\star\star\star\star\star\star\star\star\star\star\star\star\star\star\star$

Après avoir donné quelques exemples, je laisse le lecteur, s'il veut vérifier le résultat pour d'autres exemples, sinon je pense que nous sommes prêts à passer au cas général, nous commencerons tout d'abord par quelques définitions et quelques premiers résultats et théorèmes.

Je vous encourage à lire le livre jusqu'à la fin, et si vous maîtrisez bien la théorie des groupes finis, l'étude des fonctions de Dirichlets, et les fonctions arithmétiques usuels, vous pouvez aller directement à la preuve du théorème principal de notre livre (à la page).

N.B : Si vous trouvez des erreurs de Francais ou de mathématiques ou bien si vous avez des questions et/ou des suggestions, envoyez-moi un mail à ilyasssabir7@gmail.com

$\star\star\star\star\star\star\star\star\star\star\star\star\star\star\star\star\star\star\star$

Le premier théorème de Mertens

Avant de démontrer le théorème de Mertens, on est besoin de montrer le théorème de Legendre qui s'éconce comme ceci :

Théorème 2.(théorème de Legendre)
soit $n \in \mathbb{N}^\star$, Pour tout nombre premier p on a:

$$v_p(n!) = \sum_{k=1}^{+\infty} \left[\frac{n}{p^k} \right]$$

Démonstration. (Théorème 2) □

Soit $n \in \mathbb{N}^\star$, et p premier, on note $n_0 = \max \left\{ k \in \mathbb{N}, \frac{n}{p^k} \geqslant 1 \right\}$ [3]
En réalité $\sum_{k=1}^{+\infty} \left[\frac{n}{p^k} \right]$ est fini, puisque $\forall k \geqslant n_0 + 1 \left[\frac{n}{p^k} \right] = 0$
Et on a alors : $\sum_{k=1}^{+\infty} \left[\frac{n}{p^k} \right] = \sum_{k=1}^{n_0} \left[\frac{n}{p^k} \right]$
On commence par montrer tout d'abord le lemme suivant:

Lemme.2
Soit $(a, b) \in \mathbb{N}^\star \times \mathbb{N}$, le nombre des multiples de a dans $[\![1, b]\!]$ est : $\left[\frac{b}{a} \right]$

Démonstration. (Lemme 1) □

Soit $(a, b) \in \mathbb{N}^\star \times \mathbb{N}$,
Si $b < a$:
On a aucune multiple de a entre 1 et b,donc le nombre des multiple de a dans $[\![1, b]\!]$ est : $0 = \left[\frac{b}{a} \right]$

3. n_0 existe puisque $\frac{n}{p^k} \underset{k \to +\infty}{\longrightarrow} 0$ et $n > 0$

Si $b \geqslant a$:

Soit $x \in [\![1, b]\!]$,tel que a divise x, alors $\exists k \in \mathbb{N}^\star \, x = k.a$

On a $1 \leqslant k.a \leqslant b$,donc $0 < \frac{1}{a} \leqslant k \leqslant \frac{b}{a}$, donc $1 \leqslant k \leqslant \left[\frac{b}{a}\right]$,

Et inversement, pour tout entier $1 \leqslant k \leqslant \left[\frac{b}{a}\right]$, on a $a \leqslant a.k \leqslant a.\left[\frac{b}{a}\right] \leqslant b$, avec $k.a$ est un multiple de a

Alors le nombre des multiples de a dans $[\![1, b]\!]$ est : $\left[\frac{b}{a}\right]$

Pour tout nombre premier p , on a:

$$v_p(n!) = v_p\left(\prod_{k=1}^{n} k\right) = \sum_{k=1}^{n} v_p(k)$$

On note pour tout $i \in [\![0, n_0]\!]$, $A_i = \{k \in [\![1, n]\!] / \, p^i \text{ divise } k \text{ et } p^{i+1} \text{ ne divise pas } k\}$

On a bien $(A_i)_{0 \leqslant i \leqslant n_0}$ est une partition de $[\![1, n]\!]$ (par construction), donc

$$v_p(n!) = \sum_{i=0}^{n_0} \left(\sum_{k \in A_i} v_p(k) \right)$$

Or $\forall i \in [\![0, n_0]\!], \forall k \in A_i \, p^i$ divise k et p^{i+1} ne divise pas k , donc

$$\forall i \in [\![0, n_0]\!], \forall k \in A_i \, v_p(k) = i$$

D'où

$$v_p(n!) = \sum_{i=0}^{n_0} i.\#(A_i) = \sum_{i=1}^{n_0} i.\#(A_i)$$

Or, pour tout $i \in [\![1, n_0]\!]$,On a :

$$A_i = \{k \in [\![1, n]\!] / \, p^i \text{ divise } k \text{ et } p^{i+1} \text{ ne divise pas } k\}$$

Ainsi

$$A_i = \{k \in [\![1, n]\!] / \, p^i \text{ divise } k \, \} \backslash \{k \in [\![1, n]\!] / \, p^{i+1} \text{ divise } k \, \}$$

Puisque $\{k \in [\![1,n]\!] / p^{i+1} \text{ divise } k\} \subset \{k \in [\![1,n]\!] / p^i \text{ divise } k\}$,Alors

$$\#A_i = \#\{k \in [\![1,n]\!] / p^i \text{ divise } k\} \backslash - \#\{k \in [\![1,n]\!] / p^{i+1} \text{ divise } k\}$$

Donc :

$$\#A_i = \left[\frac{n}{p^i}\right] - \left[\frac{n}{p^{i+1}}\right]$$

Ainsi

$$\boxed{v_p(n!) = \sum_{i=1}^{n_0} i.\left(\left[\frac{n}{p^i}\right] - \left[\frac{n}{p^{i+1}}\right]\right) = \sum_{k=1}^{n_0}\left[\frac{n}{p^k}\right] = \sum_{k=1}^{+\infty}\left[\frac{n}{p^k}\right]}$$

Théorème 3. (la formule de Mertens)

On a pour tout $x > 1$,

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

Démonstration. (théorème 3) □

Soit $x > 2$, notons $n = [x]$
On a

$$n! = \prod_{p \leqslant x} p^{v_p(n!)}$$

Donc :

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

Et pour tout nombre premier $p \leqslant x$, on a d'après le théorème de Legendre:

$$\frac{n}{p} - 1 < \left[\frac{n}{p}\right] < v_p(n!) = \sum_{k=1}^{+\infty}\left[\frac{n}{p^k}\right] \leqslant \sum_{k=1}^{+\infty}\frac{n}{p^k} = \frac{n}{p-1} = \frac{n}{p} + \frac{n}{p(p-1)}$$

Donc

$$n\sum_{p \leqslant x}\left(\frac{\log(p)}{p} - \frac{\log(p)}{n}\right) \leqslant \log(n!) = \sum_{p \leqslant x} v_p(n!)\log(p) \leqslant n\sum_{p \leqslant x}\left(\frac{\log(p)}{p} + \frac{\log(p)}{p(p-1)}\right)$$

Donc:

$$\frac{\log(n!)}{n}-\sum_{p\leqslant x}\frac{\log(p)}{p(p-1)}-\log(x)\leqslant\sum_{p\leqslant x}\frac{\log(p)}{p}-\log(x)$$

Et

$$\sum_{p\leqslant x}\frac{\log(p)}{p}-\log(x)\leqslant\frac{\log(n!)}{n}-\log(x)+\sum_{p\leqslant x}\frac{\log(p)}{n}$$

Avec :

$$\sum_{p\leqslant x}\frac{\log(p)}{n}=\frac{1}{n}\log\left(\prod_{p\leqslant x}p\right)=\frac{1}{n}\log\left(\prod_{p\leqslant n}p\right)$$

Or, on a pout tout entier $m\geqslant 0\quad 2\times 4^m=(1+1)^{2m+1}=\sum_{k=0}^{2m+1}\binom{2m+1}{k}$

Donc

$$\binom{2m+1}{m}=\frac{1}{2}\left[\binom{2m+1}{m}+\binom{2m+1}{m+1}\right]\leqslant\frac{1}{2}\sum_{k=0}^{2m+1}\binom{2m+1}{k}=4^m$$

Pour tout nombre premier $m+1<p\leqslant 2m+1$, on a p divise $(2m+1)!$, alors p divise : $m!(m+1)!\binom{2m+1}{m}$

Avec $p>m+1$,alors p ne divise ni $m!$ ni $(m+1)!$, d'où d'après le lemme de GAUSS p divise $\binom{2m+1}{m}$

Donc : $\prod_{m+1<p\leqslant 2m+1}p$ divise $\binom{2m+1}{m}$

Ainsi :

$$\prod_{m+1<p\leqslant 2m+1}p\leqslant\binom{2m+1}{m}\leqslant 4^m$$

Montrons maintenant par récurrence que pour tout $m\in\mathbb{N}^\star$, on a: $\prod_{p\leqslant m}p\leqslant 4^m$

Pour $m=1$, on a $\prod_{p\leqslant m}p=\prod_{p\leqslant 1}p=1\leqslant 4=4^m$

Soit $m\in\mathbb{N}^\star$, supposons que $\forall k\in[\![1,m]\!]\ \prod_{p\leqslant k}p\leqslant 4^k$,et montrons que $\prod_{p\leqslant m+1}p\leqslant 4^{m+1}$

Si $m+1$ n'est pas premier, on a alors :

$$\prod_{p\leqslant m+1}p\leqslant\prod_{p\leqslant m}p\leqslant 4^m\leqslant 4^{m+1}$$

Si $(m+1)$ est premier,

Si $m=1$, on a $\prod_{p\leqslant m+1}p=2\leqslant 4^2=4^{m+1}$

Si $m>1$, on a $(m+1)$ est impair, donc $\exists k_0\in[\![1,m]\!]\ m+1=2k_0+1$

On a alors :

$$\prod_{p\leqslant m+1}p=\prod_{p\leqslant 2k_0+1}p=\prod_{p\leqslant k_0+1}p\prod_{k_0+1<p\leqslant 2k_0+1}p\leqslant 4^{k_0}\times 4^{k_0+1}=4^{m+1}$$

D'où pour tout $m\in\mathbb{N}^\star$: $\prod_{p\leqslant m}p\leqslant 4^m$

Par suite :

$$\sum_{p\leqslant x}\frac{\log(p)}{n}=\frac{1}{n}\log\left(\prod_{p\leqslant x}p\right)=\frac{1}{n}\log\left(\prod_{p\leqslant n}p\right)\leqslant\frac{1}{n}\log(4^n)=\log(4)$$

Et on a:

$$\sum_{p\leqslant x}\frac{\log(p)}{p(p-1)}\leqslant\sum_{2\leqslant k\leqslant n}\frac{\log(k)}{k(k-1)}$$

Comme $\frac{\log(k)}{\sqrt{k}}\underset{k\to+\infty}{\longrightarrow}0$, alors $\frac{\log(k)}{k(k-1)}=o\left(\frac{1}{\sqrt{k}(k-1)}\right)$, avec $\frac{1}{\sqrt{k}(k-1)}\underset{k\to+\infty}{\sim}\frac{1}{k^{3/2}}$ et $\sum_{k\geqslant 2}\frac{1}{k^{3/2}}$ converge

Alors $\sum_{k\geqslant 2}\frac{1}{\sqrt{k}(k-1)}$ converge, et par suite $\sum_{k\geqslant 2}\frac{\log(k)}{k(k-1)}$ converge.

On a donc par positivité des termes:

$$\sum_{p\leqslant x}\frac{\log(p)}{p(p-1)}\leqslant\sum_{2\leqslant k\leqslant n}\frac{\log(k)}{k(k-1)}\leqslant\sum_{k=2}^{+\infty}\frac{\log(k)}{k(k-1)}<+\infty$$

D'où

$$\frac{\log(n!)}{n}-\sum_{k=2}^{+\infty}\frac{\log(k)}{k(k-1)}-\log(x)\leqslant\sum_{p\leqslant x}\frac{\log(p)}{p}-\log(x)\leqslant\frac{\log(n!)}{n}-\log(x)+\log(4)$$

D'après la formule de stirling [4] :

$$\frac{\log(n!)}{n} = \log(n) - 1 + O\left(\frac{\log(n)}{n}\right)$$

Donc :

$$\frac{\log(n!)}{n} - \log(x) = \log\left(\frac{n}{x}\right) - 1 + O\left(\frac{\log(n)}{n}\right)$$

Avec $n \leqslant x < n+1$, donc $1 - \frac{1}{x} < \frac{n}{x} \leqslant 1$

On a donc : $\log\left(1 - \frac{1}{x}\right) \leqslant \log\left(\frac{n}{x}\right) \leqslant 0$

On a $\exists N_1 \in \mathbb{N},\ \exists M > 0\ \forall m \geqslant N_1 \left|O\left(\frac{\log(m)}{m}\right)\right| \leqslant M.\frac{\log(m)}{m}$

Donc $\forall x \geqslant N_1$, ona $n \geqslant N_1$, on a :

$$\left|\frac{\log(n!)}{n} - \log(x)\right| \leqslant 1 + \left|\log\left(\frac{n}{x}\right)\right| + M\frac{\log(n)}{n} \leqslant 1 + \log\left(\frac{x}{x-1}\right) + M.\frac{\log(n)}{n}$$

Donc:

$$\left|\frac{\log(n!)}{n} - \log(x)\right| \leqslant 1 + \left|\log\left(\frac{n}{x}\right)\right| + M\frac{\log(n)}{n} \leqslant 1 + \log\left(\frac{x}{x-1}\right) + M$$

Comme $\log\frac{x}{x-1} \underset{x\to+\infty}{\to} 0$, alors $\exists \eta > 0, \forall x \geqslant \eta\ \ \log\frac{x}{x-1} \leqslant 1$

Pour $N = \max(N_1, [\eta] + 1)$, on a pour tout $x \geqslant N$:

$$\left|\frac{\log(n!)}{n} - \log(x)\right| \leqslant 2 + M$$

Donc pour tout $x \geqslant \eta$, on a

$$-\sum_{k=2}^{+\infty} \frac{\log(k)}{k(k-1)} - 2 - M \leqslant \sum_{p\leqslant x} \frac{\log(p)}{p} - \log(x) \leqslant 2 + M + \log(4)$$

Par suite

$$\left|\sum_{p\leqslant x} \frac{\log(p)}{p} - \log(x)\right| \leqslant 2 + M + \max\left(\log(4), \sum_{k=2}^{+\infty} \frac{\log(k)}{k(k-1)}\right)$$

4. formule de Stirling : https://fr.wikipedia.org/wiki/Formule_de_Stirling

D'où

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

✠✠✠✠✠✠✠✠✠✠✠

La théorie des groupes finis est très importante plus que vous croyez, elle a beaucoup d'applications en théorie des nombres, analyse complexe, et la physique, et l'informatique théoriques ...

On va utiliser quelques notions et résultat de cette théorie dans la démonstration du théorème de Dirichlet, c'est pour cela je donnerai quelques résultats autour de cette théorie.

Quelques résultats sur les groupes finis

Définition 2.

Soit G un groupe commutatif fini dont on notera la loi multiplicativement.

On dit qu'un homomorphisme de G dans le groupe multiplicatif $\mathbb{C}^\star$ est un caractère de G. Soient χ et χ' deux caractères de G. Le produit $\chi\chi_0$ est défini par la formule :

$$\chi\chi'(g)=\chi(g)\chi'(g)\text{ pour }g\in G.$$

On note 1 le caractère constant de valeur 1. L'ensemble $\hat{G}$ des caractères de G est ainsi muni d'une loi de groupe d'élément neutre 1.

On note $\hat{\hat{G}}$ le groupe des caract'eres de $\hat{G}$.

On note enfin $\overline{\chi}$ le caractère qui à $g\in G$ associe le conjugué $\overline{\chi(g)}$ de $\chi(g)$.

Pour tout $z\in G$, considérons l'application $\varphi_x\in\hat{\hat{G}}$ définie par:

$$\forall\chi\in\hat{G}\quad\varphi_x(\chi)=\chi(x)$$

Théorème.4

le morphisme : $\begin{cases}G\to\hat{\hat{G}}\\ x\longmapsto\varphi_x\end{cases}$ est injectif

Démonstration. (Théorème 4) □

Soit $x \in G$, $x \neq 1$ et $\mathrm{gr}(x)$ le sous-groupe de G engendré par x. Montrons qu'il existe un caractère χ de $\mathrm{gr}(x)$ tel que $\chi(x) \neq 1$

Comme $\mathrm{gr}(x)$ est cyclique, alors il est isomorphe à $\mathbb{Z}/m\mathbb{Z}$,
où $m = o(x)$: l'ordre de x dans G.
Et comme $\mathbb{Z}/m\mathbb{Z}$ est isomprphe à $\mathbb{U}_m$: le groupe des racines m-ième de l'unité alors $\mathrm{gr}(x)$ est isomorphe à $\mathbb{U}_m$
$x \neq 1$, alors $m \geqslant 2$, et donc il existe un caractère de $\mathbb{U}_m$ qui ne prend la valeur 1 que en 1.
Via l'isomorphisme, on en déduit l'existance d'un caractère χ de $\mathrm{gr}(x)$ qui ne prend la valeur 1 que en 1_G
D'où l'existance d'un caractère χ de $\mathrm{gr}(x)$ tel que $\chi(x) \neq 1$

Soit F la famille des sous-groupes H de G contenant $\mathrm{gr}(x)$ tels que χ se prolonge en un caractère de H. Montrer que F admet un élément G' de cardinal maximal. Supposons $G' \neq G$. Soit y un élément de G qui n'est pas dans G' .
On a
$F = \{H \text{ sous groupe de } G / \mathrm{gr}(x) \subset H \text{ et } \chi \text{ se prolonge en un caractère de } H\}$
Considèrons l'ensemble :

$$A_F = \{\#H \,/\, H \in F\}$$

A_F est une partie de $\mathbb{N}$, comme $\mathrm{gr}(x)$ est un sous groupe de G tel que $\mathrm{gr}(x) \subset \mathrm{gr}(x)$ et χ se prolonge en un caractère de H.
Alors $\mathrm{gr}(x) \in F$, donc $F \neq \varnothing$ par suite $A_F \neq \varnothing$
Puisque G est un groupe fini, alors

$$\forall H \subset F, H \text{ est fini et } \#H \leqslant \#G$$

D'où A_F est une partie de $\mathbb{N}$, non vide majorée
Alors A_F possède un plus grand élément
D'où F admet un élement G' de cardinal maximal
Condidèrons l'ensemble

$$K = \{m \in \mathbb{N}^\star \,/\, y^m \in G'\}$$

K est une partie de $\mathbb{N}$ non vide puisqu'elle contient l'ordre de y (qui est fini puisque G est fini, et $1_G \in G'$)
donc K admet un plus petit élément

d'où l'existance de $n \in \mathbb{N}^\star$ minimal tel que $y^n \in G'$

Soit χ' un caractère de G' prolongeant χ et $a = \chi'(g^n)$

soit b une racine n-eme de a dans $\mathbb{C}$.

Pour tout $m, k \in \mathbb{Z}$, et $g, g' \in G'$, en effectuant la division euclidienne de $m-k$ par n, on a $\exists (q,r) \in \mathbb{Z} \times [\![0, n-1]\!]$ tel que $m-k = q.n+r$

comme $g^n \in G'$ alors $g^{q.n} \in G'$

si $g^m.g = y^k g'$,alors $g^{m-k} = g'.g^{-1} \in G'$, on a alors $g^r = g^{m-k}.g^{-q.n} \in G'$

Alors $r = 0$, (car sinon, on trouve une contraduction avec le caratère minimale de $n \geqslant 1$), donc $g^{m-k} = g'.g^{-1}$

Donc $g^{q.n} = g^{-1}.g'$ donc puisque χ' est un caractère alors:

$$\chi'(g').\chi'(g^{-1}) = \chi'((g^n)^q) = (\chi'(g^n))^q = a^q = b^{m-k}$$

Il vient donc ;

$$\chi'(g')b^k = \chi'(g)b^m$$

Donc, on peut définir χ'' par : $\forall (m,g) \in \mathbb{Z} \times G'$

$$\chi''(g^m g) = b^m \chi'(g)$$

On a donc $\chi''_{/G} = \chi'$,par constuction $\chi''_{/G} = \chi'_{/G} = \chi$

Puisque χ' prolonge χ à G', autrement dit : on peut prolonger χ au groupe engendré par g et G'.

L'hypothèse $G' \neq G$ conduit donc à une absurdité; car le groupe engendré par G' et g est de cardinal strictement supérieur à celui de G', puique $y \notin G'$, et on en déduit que : $G' = G$.

Pour tout $g \in G$ distinct de 1, on dispose d'un caractère χ de G tel que $\chi(g) \neq 1$, donc $\phi_g(\chi) \neq 1$ autrement dit $\phi_g \neq 1$, on en déduit $g \longmapsto \varphi_g$ est injective (puisque ϕ_g est un morphisme)

Théorème 5.

On a pour tout $x \in G$:

$$\sum_{\chi \in \hat{G}} \chi(x) = 0 \text{ si } x \neq 1$$

Et

$$\sum_{\chi \in \hat{G}} \chi(x) = \#\hat{G} \text{ si } x = 1$$

Démonstration. (Théorème 5) □

Soit $(\chi', x) \in \hat{G} \times G$, on a l'application φ: $\begin{cases} \hat{G} \longrightarrow \hat{G} \\ \chi \longmapsto \chi \cdot \chi' \end{cases}$ est bien définie, et bijective.

Alors

$$\sum_{\chi \in \hat{G}} \chi(x) = \sum_{\chi \in \hat{G}} (\chi . \chi')(x)$$

Si $x \neq 1$,on a l'existance d'après ce qui précède de $\chi' \in \hat{G}$ tel que : $\chi'(x) \neq 1$,on a alors :

$$(1 - \chi'(x)) \sum_{\chi \in \hat{G}} \chi(x) = 0$$

Avec $1 - \chi'(x) \neq 0$, alors :

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

Si $x = 1$,on a :

$$\sum_{\chi \in \hat{G}} \chi(x) = \sum_{\chi \in \hat{G}} 1 = \#\hat{G}$$

Théorème 6.

On a pour tout $\chi \in \hat{G}$:

$$\sum_{g \in G} \chi(g) = 0 \text{ si } \chi \neq 1$$

Et

$$\sum_{g \in G} \chi(g) = \#G \text{ si } \chi = 1$$

Démonstration. (Théorème 6) □

Si $\chi \neq 1$, soit $y \in G$ tel que $\chi(y) \neq 1$, et on a l'application $g \in G \rightarrow g.y \in G$ est bijective, alors :

$$\sum_{g \in G} \chi(g) = \sum_{g \in G} \chi(g.y) = \left(\sum_{g \in G} \chi(g) \right) \chi(y)$$

D'où

$$(1-\chi(y))\left(\sum_{g\in G}\chi(g)\right)=0$$

Avec $1-\chi(y)\neq 0$, alors $\sum_{g\in G}\chi(g)=0$

Si $\chi\neq 1$, on a $\sum_{g\in G}\chi(g)=\sum_{g\in G}1=\#G$

Théorème 7.

le morphisme $\begin{cases} G\to\hat{\hat{G}} \\ x\longmapsto\varphi_x \end{cases}$ est bijectif

Démonstration. (Théorème 7) □

On a:

$$\sum_{(\chi,x)\in\hat{G}\times G}\chi(x)=\sum_{\chi\in\hat{G}}\sum_{x\in G}\chi(x)=\sum_{\chi\in\hat{G}\setminus\{1\}}\sum_{x\in G}\chi(x)+\sum_{x\in G}1(x)=\#G$$

D'autre part :

$$\sum_{(\chi,x)\in\hat{G}\times G}\chi(x)=\sum_{x\in G}\sum_{\chi\in\hat{G}}\chi(x)=\sum_{x\in G\setminus\{1\}}\sum_{\chi\in\hat{G}}\chi(x)+\sum_{\chi\in\hat{G}}\chi(1)=\#\hat{G}$$

On en déduit que $\#\hat{G}=\#G$,donc $\#\hat{\hat{G}}=\#G$

Puisque le morphisme $\begin{cases} G\to\hat{\hat{G}} \\ x\longmapsto\varphi_x \end{cases}$ est injective alors ce morphisme est bijective (isomorphisme de groupe).

✠✠✠✠✠✠✠✠✠✠

La démonstration du théorème de Dirichlet

On va utiliser plusieurs fois une transformée qui connut sous le nom de sommation d'ABEL.

On commence par la donnée et la décomnstration de cette formule .

Puis on définit quelques fonctions arithmétiques et on donne quelques propositions sur ces fonctions.

Théorème 8.(la formule de sommation d'ABEL)

Soit $\sum_{n\geqslant 1} u_n$, $\sum_{n\geqslant 1} v_n$ deux séries de nombres complexes. Soit $U_n = \sum_{k=1}^{n} u_k$ la somme partielle, on a:

$$\sum_{k=1}^{n} u_k v_k = \sum_{i=1}^{n-1} (v_i - v_{i+1}) U_i + v_n U_n$$

Démonstration. (Théorème 8) □

Méthode 1: on a pour tout $n \geqslant 1$,

$$\sum_{k=1}^{n} u_k v_k = \sum_{k=1}^{n} u_k (v_k - v_n) + v_n \sum_{k=1}^{n} u_k = \sum_{k=1}^{n} u_k \left(\sum_{i=k}^{n-1} (v_i - v_{i+1}) \right) + v_n U_n$$

Donc

$$\sum_{k=1}^{n} u_k v_k = \sum_{k=1}^{n} \sum_{i=k}^{n-1} u_k (v_i - v_{i+1}) + v_n U_n = \sum_{i=1}^{n-1} \sum_{k=1}^{i} u_k (v_i - v_{i+1}) + v_n U_n$$

Ainsi

$$\boxed{\sum_{k=1}^{n} u_k v_k = \sum_{i=1}^{n-1} (v_i - v_{i+1}) \left(\sum_{k=1}^{i} u_k \right) + v_n U_n = \sum_{i=1}^{n-1} (v_i - v_{i+1}) U_i + v_n U_n}$$

Méthode 2 : Notons pour tout suite $(a_n)_{n\in\mathbb{N}}$,pour tout $n \in \mathbb{N}$

$$\Delta a_n = a_{n+1} - a_n$$

On a pour tout $k \in \mathbb{N}$

$$\Delta (U.v)_k = U_{k+1} v_{k+1} - U_k v_k = \begin{vmatrix} U_{k+1} & U_k \\ v_k & v_{k+1} \end{vmatrix} = \begin{vmatrix} u_{k+1} & U_k \\ -\Delta v_k & v_{k+1} \end{vmatrix}$$

Ainsi

$$\Delta (U.v)_k = u_{k+1} v_{k+1} + U_k \Delta v_k$$

En sommant de 1 à $n-1$

$$\sum_{k=1}^{n-1}\Delta(U.v)_k=\sum_{k=1}^{n-1}u_{k+1}v_{k+1}+\sum_{k=1}^{n-1}U_k\Delta v_k$$

D'où

$$U_{n-1}.v_{n-1}-U_1.v_1=\sum_{k=1}^{n-1}u_{k+1}v_{k+1}+\sum_{k=1}^{n-1}U_k(v_{k+1}-v_k)$$

Ainsi :

$$\boxed{\sum_{k=1}^{n}u_kv_k=\sum_{i=1}^{n-1}(v_i-v_{i+1})U_i+v_nU_n}$$

Définition 3.(la fonction de Möbius) [5]

Soit $n\in\mathbb{N}^\star$, On note $\mu(n)$ l'entier défini par :

$$\mu(n)=\begin{cases}0 & \text{si } n \text{ est divisible par le carré d'un nombre premier}\\ (-1)^r & \text{si } r \text{ est le nombre de facteurs premiers distincts de } n\text{, } n \text{ non divisible par le carr\'e d'un nombre premier}\end{cases}$$

Proposition 1.

pour tout $n\neq 1$, on a l'égalité

$$\sum_{d/n}\mu(d)=0$$

Démonstration. (Proposition 1) □

Méthode 1 : soit $n=\prod_{i=1}^{m}p_i^{a_i}$ la décomposition en facteurs premiers de n,

De plus si $d\in\mathbb{N}$, alors :

d/n et $\mu(d)\neq 0$ si et seulement si $d=\prod_{i\in J}p_i^{a_i}$ with $J\subset[\![1,m]\!]$ et alors $\mu(d)=(-1)^{\#J}$, on en déduit que

$$\boxed{\sum_{d/n}\mu(d)=\sum_{J\subset[\![1,m]\!]}(-1)^{\#J}=(1-1)^m=0}\ (\text{car } m>0)$$

5. https://fr.wikipedia.org/wiki/Fonction_de_M%C3%B6bius#:~:text=En%20math%C3%A9matiques%2C%20la%20fonction%20de,des%20branches%20diff%C3%A9rentes%20des%20math%C3%A9matiques.

Méthode 2 :Soit $n \geqslant 2$, d'après le théorème fondamentale de l'arithmétique on a l'existance de $(p_1, \ldots, p_r) \in \mathcal{P}^r$ et $\alpha_1, \ldots, \alpha_r \geqslant 1$ tel que $n = \prod_{i=1}^{r} p_i^{\alpha_i}$

On a

$$\sum_{d/n} \mu(d) = \sum_{k_1=0}^{\alpha_1} \sum_{k_2=0}^{\alpha_2} \cdots \sum_{k_r=0}^{\alpha_r} \mu\left(\prod_{i=1}^{r} p_i^{k_i}\right)$$

Parsuite:

$$\sum_{d/n} \mu(d) = \sum_{\substack{(k_1,\ldots,k_r) \in \prod_{i=1}^{r} [\![0,\alpha_i]\!] \\ \exists i_0 \in [\![1,r]\!] \, k_{i_0} \geqslant 2}} \mu\left(\prod_{i=1}^{r} p_i^{k_i}\right) + \sum_{(k_1,\ldots,k_r) \in [\![0,1]\!]^r} \mu\left(\prod_{i=1}^{r} p_i^{k_i}\right)$$

puisque pour tout $(k_1, \ldots, k_r) \in \prod_{i=1}^{r} [\![0, \alpha_i]\!]$ tel que $\exists i_0 \in [\![1, r]\!] \, k_{i_0} \geqslant 2$

On a $\prod_{i=1}^{r} p_i^{k_i}$ est divisible par $p_{i_0}^2$ alors $\mu\left(\prod_{i=1}^{r} p_i^{k_i}\right) = 0$

D'où

$$\sum_{\substack{(k_1,\ldots,k_r) \in \prod_{i=1}^{r} [\![0,\alpha_i]\!] \\ \exists i_0 \in [\![1,r]\!] \, k_{i_0} \geqslant 2}} \mu\left(\prod_{i=1}^{r} p_i^{k_i}\right) = 0$$

Par suite

$$\sum_{d/n} \mu(d) = \sum_{(k_1,\ldots,k_r) \in [\![0,1]\!]^r} \mu\left(\prod_{i=1}^{r} p_i^{k_i}\right)$$

Pour tout $(k_1, \ldots, k_r) \in [\![0, 1]\!]^r$,on a $\sum_{i=1}^{r} k_i$ est le nombre de facteurs premiers distincts de $\prod_{i=1}^{r} p_i^{k_i}$, et $\prod_{i=1}^{r} p_i^{k_i}$ est non divisible par le carré d'un nombre premier, alors

$$\sum_{d/n} \mu(d) = \sum_{(k_1,\ldots,k_r) \in [\![0,1]\!]^r} (-1)^{\sum_{i=1}^{r} k_i} = \prod_{i=1}^{r} \left(\sum_{k_1=0}^{1} (-1)^{k_i} \right) = (1-1)^r = 0$$

Théorème 9.(la formule d'inversion de Möbius)

Soit H une fonction non nulle de $\mathbb{N}^\star$ dans $\mathbb{C}$ telle que $\forall n, m \in N, H(n.m) = H(n)H(m)$

Et on se donne également deux fonctions F et G de $[1,+\infty[$ dans $\mathbb{C}$ telles que :

$$\forall x>1, G(x)=\sum_{1\leqslant k\leqslant x} F\Big(\frac{x}{k}\Big)H(k)$$

Alors:

$$\forall x>1, F(x)=\sum_{1\leqslant k\leqslant x} \mu(k)G\Big(\frac{x}{k}\Big)H(k)$$

Démonstration. (Théorème 9) □

on a $H(1)=H(1\times 1)=H(1)^2$, et puisque $H\neq 0$ alors $H(1)=1$
et on a pour tout $x\in[1,+\infty[$

$$\sum_{1\leqslant k\leqslant x} \mu(k)G\Big(\frac{x}{k}\Big)H(k)=\sum_{1\leqslant k\leqslant x}\mu(k)\sum_{1\leqslant i\leqslant \frac{x}{k}} F\Big(\frac{x}{i.k}\Big)H(i)H(k)$$

Par suite

$$\sum_{1\leqslant k\leqslant x} \mu(k)G\Big(\frac{x}{k}\Big)H(k)=\sum_{1\leqslant k\leqslant x}\sum_{1\leqslant i\leqslant \frac{x}{k}}\mu(k)F\Big(\frac{x}{i.k}\Big)H(i.k)$$

Ainsi

$$\sum_{1\leqslant k\leqslant x} \mu(k)G\Big(\frac{x}{k}\Big)H(k)=\sum_{1\leqslant k.i\leqslant x}\mu(k)F\Big(\frac{x}{i.k}\Big)H(i.k)$$

Ainsi

$$\sum_{1\leqslant k\leqslant x} \mu(k)G\Big(\frac{x}{k}\Big)H(k)=\sum_{1\leqslant m\leqslant x}\sum_{d/m}\mu(d)F\Big(\frac{x}{m}\Big)H(m)$$

Par suite

$$\sum_{1\leqslant k\leqslant x} \mu(k)G\Big(\frac{x}{k}\Big)H(k)=\sum_{1\leqslant m\leqslant x} F\Big(\frac{x}{m}\Big)H(m)\Big(\sum_{d/m}\mu(d)\Big)$$

Ainsi

$$\sum_{1\leqslant k\leqslant x} \mu(k)G\Big(\frac{x}{k}\Big)H(k)=F(x)H(1)+\sum_{2\leqslant m\leqslant x} F\Big(\frac{x}{m}\Big)H(m)\Big(\sum_{d/m}\mu(d)\Big)$$

D'après la proposition 1, on a pour tout $m \geqslant 2$

$$\sum_{d/m} \mu(d) = 0$$

d'où

$$\boxed{F(x) = \sum_{1 \leqslant k \leqslant x} \mu(k) G\Big(\frac{x}{k}\Big) H(k)}$$

Définition 4.

Soit Λ la fonction de $[1, +\infty[$ dans $\mathbb{R}$ qui à p^n associe $\log(p)$ et qui est nulle sur tous les réels qui ne sont pas des entiers de la forme p^n

Proposition 2.

Pour tout entier $m \geqslant 1$, on a:

$$\Lambda(x) = \sum_{d/m} \mu(d) \log\Big(\frac{m}{d}\Big)$$

Démonstration. (Proposition 2) □

Méthode 1: On applique ce qui précède à $F = \Lambda$ et $H = 1$ (qui est bien multiplicative)

Alors, on a pour tout $x \geqslant 1$, et $k \in \mathbb{N}^\star$ $\Lambda\big(\frac{x}{k}\big)$ est non nul si et seulement si x est un entier de la forme $k.p^n$ avec $n \in \mathbb{N}^\star$, et nécessairement inférieur à $v_p(x)$

d'où

$$G(x) = \sum_{1 \leqslant k \leqslant x} \Lambda\Big(\frac{x}{k}\Big) = 1_{\mathbb{N}}(x) \sum_{p^n \leqslant x} \log(p) = 1_{\mathbb{N}}(x) \sum_{p/x} v_p(x) \log(p) = 1_{\mathbb{N}}(x).\log(x)$$

Et donc

$$\Lambda(x) = \sum_{1 \leqslant k \leqslant x} \mu(k) 1_{\mathbb{N}}\Big(\frac{x}{k}\Big) \log\Big(\frac{x}{k}\Big)$$

En particulier, puisque $\frac{m}{k}$ est un entier si et seulement si k divise m

$$\boxed{\Lambda(x) = \sum_{d/m} \mu(d) \log\Big(\frac{m}{d}\Big)}$$

Méthode 2: pour tout entier $m \in \mathbb{N}^\star$, on a $\Lambda(1) = 0$,
et $\sum_{d/1} \mu(d)\log\left(\frac{1}{d}\right) = \log(1) = 0$

Dans la suite ,on prend $m \geqslant 2$, d'après le théorème fondamentale de l'arithmetique on a l'existance de $p_1, \ldots, p_r \in \mathcal{P}^+$ et $\alpha_1, \ldots, \alpha_r \in \mathbb{N}^\star$ tel que

$$m = \prod_{i=1}^{r} p_i^{\alpha_i}$$

On a alors

$$\sum_{d/m} \mu(d)\log\left(\frac{m}{d}\right) = \sum_{(k_1,\ldots,k_r) \in \prod_{i=1}^{r} [\![0,\alpha_i]\!]} \mu\left(\prod_{i=1}^{r} p_i^{k_i}\right)\log\left(\prod_{i=1}^{r} p_i^{\alpha_i - k_i}\right)$$

Avec $\forall (k_1, \ldots, k_r) \in \prod_{i=1}^{r} [\![0, \alpha_i]\!]\ \exists i_0 \in [\![1, r]\!]\ k_{i_0} \geqslant 2\ \mu\left(\prod_{i=1}^{r} p_i^{k_i}\right) = 0$

Alors

$$\sum_{\substack{(k_1,\ldots,k_r) \in \prod_{i=1}^{r} [\![0,\alpha_i]\!] \\ \exists i_0 \in [\![1,r]\!]\, k_{i_0} \geqslant 2}} \mu\left(\prod_{i=1}^{r} p_i^{k_i}\right)\log\left(\prod_{i=1}^{r} p_i^{\alpha_i - k_i}\right) = 0$$

par suite

$$\sum_{d/m} \mu(d)\log\left(\frac{m}{d}\right) = \sum_{(k_1,\ldots,k_r) \in [\![0,1]\!]^r} \mu\left(\prod_{i=1}^{r} p_i^{k_i}\right)\log\left(\prod_{i=1}^{r} p_i^{\alpha_i - k_i}\right)$$

Ainsi

$$\sum_{d/m} \mu(d)\log\left(\frac{m}{d}\right) = \sum_{(k_1,\ldots,k_r) \in [\![0,1]\!]^r} (-1)^{\sum_{i=1}^{r} k_i} \sum_{j=1}^{r} (\alpha_j - k_j)\log(p_j)$$

Par suite

$$\sum_{d/m}\mu(d)\log\Big(\frac{m}{d}\Big)=\log\Big(\prod_{i=1}^{r}p_i^{\alpha_i}\Big)(1+(-1))^r-\sum_{(k_1,\dots,k_r)\in[\![0,1]\!]^r}(-1)^{\sum_{i=1}^{r}k_i}\sum_{j=1}^{r}k_j\log(p_j)$$

Ainsi

$$\sum_{d/m}\mu(d)\log\Big(\frac{m}{d}\Big)=\sum_{j=1}^{r}\log(p_j)\sum_{(k_1,\dots,k_r)\in[\![0,1]\!]^r}(-1)^{\sum_{\substack{i=1\\ i\neq j}}^{r}k_i}\ k_j$$

Ainsi

$$\sum_{d/m}\mu(d)\log\Big(\frac{m}{d}\Big)=\sum_{j=1}^{r}\log(p_j)\Big[\prod_{\substack{i=1\\ i\neq j}}^{r}(1-1)\Big](0+1)=0^{r-1}\sum_{j=1}^{r}\log(p_j)$$

Si $r=1$, on a $\sum_{d/m}\mu(d)\log\big(\frac{m}{d}\big)=\log(p_1)=\Lambda(m)$

si $r\geqslant 2$, on a $\sum_{d/m}\mu(d)\log\big(\frac{m}{d}\big)=0=\Lambda(m)$

d'où

$$\boxed{\forall m\in\mathbb{N}^\star\ \Lambda(m)=\sum_{d/m}\mu(d)\log\Big(\frac{m}{d}\Big)}$$

✠✠✠✠✠✠✠✠✠✠✠

Par caractère, on entendra toujours caractère de $G(N)$. On dira qu'un caractère $\chi\neq 1$ est non trivial.

On notera encore χ la fonction de $\mathbb{N}$ dans $\mathbb{C}$ définie par $\chi(m)=\chi(m \bmod N)$ si m et N sont premiers entre eux et $\chi(m)=0$ sinon. On a la formule $\chi(\mathrm{ab})=\chi(a)\chi(b)$ pour tout a,b.

Définition 5.

Soit χ un caractère non trivial, On définie la fonction $f:\mathbb{N}\to\mathbb{C}$, par :

$$\forall n\in\mathbb{N}\, f(n)=\sum_{d|n}\chi(d)$$

On définit la fonction g par :

$$\forall x\geqslant 0,\, g(x)=\sum_{n\leqslant x}\frac{f(n)}{\sqrt{n}}$$

Proposition 3.

Soit χ un caractère non trivial, on a les séries $\sum_{n\geqslant 1}\frac{\chi(n)}{n}$ et $\sum_{n\geqslant 1}\frac{\chi(n)}{n}\log(n)$ convergent

On note dans la suite $L(\chi)=\sum_{n\geqslant 1}\frac{\chi(n)}{n}$ et $L_1(\chi)=\sum_{n\geqslant 1}\frac{\chi(n)}{n}\log(n)$

Démonstration. (Proposition 3) □

Soit χ un caractère non triviale, et $m\in\mathbb{N}^\star$,
Puisque pour tout entier $n\geqslant 3$, on a

$$\left|\chi(n)\frac{\log(n)}{n}\right|\geqslant\left|\frac{\chi(n)}{n}\right|$$

Il suffit de montrer que la série $\sum_{n\geqslant 1}\chi(n)\frac{\log(n)}{n}$ converge.

on a d'aprés le théorème 5

$$\sum_{n=1}^{N}\chi(n)=\sum_{\substack{n=1\\ n\wedge N=1}}^{N}\chi(n)=\sum_{g\in G(N)}\chi(g)=0\quad(\star)$$

On a d'après la formule de sommation d'ABEL (le théorème 8)

$$\sum_{n=1}^{m}\chi(n)\frac{\log(n)}{n}=\sum_{n=1}^{m}\chi(n)\frac{\log(m)}{m}+\sum_{n=1}^{m-1}\left(\frac{\log(n+1)}{n+1}-\frac{\log(n)}{n}\right)\sum_{i=1}^{n}\chi(i)$$

Or par la division euclidienne de m par N, on a l'existance de $(q,r)\in\mathbb{N}^2$ tel que $r<n$, et $m=N.q+r$

On a alors

$$\sum_{n=1}^{m}\chi(n)=\sum_{n=1}^{\mathrm{nq}+r}\chi(n)=\sum_{k=0}^{q-1}\left(\sum_{n=1+k.N}^{(k+1)N}\chi(n)\right)+\sum_{n=1+q.N}^{q.N+r}\chi(n)$$

Ainsi

$$\sum_{n=1}^{m}\chi(n)=\sum_{k=0}^{q-1}\left(\sum_{n=1}^{N}\chi(n+k.N)\right)+\sum_{n=1}^{r}\chi(n+q.N)$$

Par suite

$$\sum_{n=1}^{m}\chi(n)=\sum_{k=0}^{q-1}\left(\sum_{n=1}^{N}\chi(n)\right)+\sum_{n=1}^{r}\chi(n)=q\sum_{n=1}^{N}\chi(n)+\sum_{n=1}^{r}\chi(n)$$

D'après $(\star)$ $\sum_{n=1}^{N}\chi(n)=0$, alors :

$$\sum_{n=1}^{m}\chi(n)=\sum_{n=1}^{r}\chi(n)$$

Ainsi par l'inégalité triangulaire

$$\left|\sum_{n=1}^{m}\chi(n)\right|\leqslant\sum_{n=1}^{r}|\chi(n)|$$

Donc :

$$\sum_{n=1}^{m}\chi(n)\frac{\log(m)}{m}=O\left(\frac{\log(m)}{m}\right)=o(1)$$

Et on a de plus :

$$\left(\frac{\log(n+1)}{n+1}-\frac{\log(n)}{n}\right)\sum_{i=1}^{n}\chi(i)=O\left(\frac{\log(n+1)}{n+1}-\frac{\log(n)}{n}\right)$$

Avec $\frac{\log(n)}{n}\underset{n\longrightarrow+\infty}{\longrightarrow}0$,alors la serie telescopique $\sum_{n\geqslant1}\left(\frac{\log(n+1)}{n+1}-\frac{\log(n)}{n}\right)$ converge

Ainsi la série $\sum_{n\geqslant1}\left[\left(\frac{\log(n+1)}{n+1}-\frac{\log(n)}{n}\right)\sum_{i=1}^{n}\chi(i)\right]$ converge aussi.

On en déduit que la série $\boxed{\sum_{n\geqslant1}\chi(n)\frac{\log(n)}{n}\text{ converge.}}$

par suite $\boxed{\sum_{n\geqslant1}\frac{\chi(n)}{n}\text{ converge}}$

Proposition 4.
La fonction f est arithmétique, et pour tout entier $n \in \mathbb{N}$, on a $f(n) \geqslant 0$,
De plus :

$$f(n) \geqslant 1 \text{ si } n \text{ est un carré}$$

Démonstration. (Proposition 4) □

Soit $(n, m) \in \mathbb{N}^\star \times \mathbb{N}^\star$, tel que $n \wedge m = 1$,

On a pour tout d diviseur de n et d' diviseur de m $d.d'$ est un diviseur de $n.m$

Soit D un diviseur de $n.m$, montrons l'existance et l'unicité d'un couple $(d, d') \in \mathbb{N}^\star \times \mathbb{N}^\star$, tel que d diviseur de n et d' diviseur de m et $D = d.d'$

On pose $a = D \wedge n$, on a alors a / D et a / n

Soient $p_1, \ldots, p_r, p_{r+1}, \ldots, p_l$ des nombres premiers deux à deux distincts et $\alpha_1, \ldots, \alpha_l \in \mathbb{N}^\star$ tel que $n = \prod_{i=1}^{r} p_i^{\alpha_i}$ et $n = \prod_{i=r+1}^{l} p_i^{\alpha_i}$

On a alors $n.m = n = \prod_{i=1}^{l} p_i^{\alpha_i}$, puisque D est un diviseur de $n.m$ alors

$\exists \lambda_1, \ldots, \lambda_l \in \mathbb{N}$ tel que $\forall i \in [\![1, l]\!]$ $\lambda_i \leqslant \alpha_i$ et $D = \prod_{i=1}^{l} p_i^{\lambda_i}$

On a $a = D \wedge n$, alors $a = \prod_{i=1}^{r} p_i^{\min(\lambda_i, \alpha_i)} = \prod_{i=1}^{r} p_i^{\lambda_i}$

Alors

$$\frac{D}{a} = \prod_{i=r+1}^{l} p_i^{\lambda_i}$$

Donc $\frac{D}{a} \wedge n = 1$, et $\frac{D}{a}$ divise D donc divise aussi $n.m$, via le lemme de GAUSS on en deduit que $\frac{D}{a}$ divise m

Donc tout diviseur $m.n$ est le produit d'un diviseur de n et d'un diviseur de m, Montrons maintenant que cette décomposition est unique.

Soient $d, d', D, D' \in \mathbb{N}^\star$ tel que $d.d' = D.D'$ avec d, D (resp d', D') sont des diviseurs de n (resp. de m)

On a alors d divise $D.D'$ avec d est premier a D' (puisque n et m sont premiers entre eux), d'après le lemme de GAUSS d divise D

De même on trouve D divise d ,donc $D = d$, d'où $D = d$ et $D = d'$.

Il vient alors

$$f(n)f(m) = \left(\sum_{d/n} \chi(d)\right)\left(\sum_{d'/m} \chi(d')\right) = \sum_{d/n}\sum_{d'/m} \chi(d)\chi(d') = \sum_{\substack{d/n \\ d'/m}} \chi(d.d')$$

On utilise ce qu'on a montrer ,on a alors

$$f(n)f(m) = \sum_{d/n.m} \chi(d) = f(n.m)$$

Si n n'est pas premier à N, on a $\chi(n) = 0$ (par définition)

Sinon, on a $n \in G(N)$ qui est fini, notons a l'ordre de n dans $G(N)$
On a

$$1 = \chi(1) = \chi(n^a) = \chi(n)^a$$

Et donc $\chi(n)$ est une racine a-eme de l'unité, puisqu'on suppose que χ à valeurs réelles, on a $\chi(n)$ est donc égal à -1 ou 1, En conclusion χ est à valeurs dans $\{-1, 0, 1\}$
Soit p un nombre premier, on a pour tout $n \in \mathbb{N}$

$$f(p^n) = \sum_{k=0}^{n} \chi(p)^k = \begin{cases} 1 \quad \text{si } \chi(p) = 0 \\ n+1 \quad \text{si } \chi(p) = 1 \\ \frac{1+(-1)^n}{2} \quad \text{si } \chi(p) = -1 \end{cases}$$

en décomposant n en facteurs premiers $f(n) = \prod_{p|n} f(p^{v_p(n)})$

chacun des termes est positif, d'apès ce qui précède et même supérieur ou egal à 1 si $v_p(n)$ est pair, on en déduit

$$\boxed{f(n)\geqslant 0 \text{ et } f(n)\geqslant 1 \text{ si } n \text{ est un carré}}$$

Proposition 5.
On a

$$\lim_{x\to+\infty} g(x)=+\infty$$

Démonstration. (Proposition 5) □

d'après ce qui précéde, pour tout $m\in\mathbb{N}^\star$ et $x\geqslant m^2$, on a

$$g(x)\geqslant\sum_{k=1}^{m^2}\frac{f(k)}{\sqrt{k}}\geqslant\sum_{k=1}^{m}\frac{f(k^2)}{k}\geqslant\sum_{k=1}^{m}\frac{1}{k}$$

Par divergence de $\sum_{k\geqslant 1}\frac{1}{k}$, on a $\boxed{\lim_{x\to+\infty} g(x)=+\infty}$

Proposition 6.
On a pour tout $x\geqslant 0$

$$g(x)=\sum_{d'\leqslant\sqrt{x}}\frac{1}{\sqrt{d'}}\sum_{\sqrt{x}<d\leqslant\frac{x}{d'}}\frac{\chi(d)}{\sqrt{d}}+\sum_{d\leqslant\sqrt{x}}\frac{\chi(d)}{\sqrt{d}}\sum_{d\leqslant\frac{x}{d}}\frac{1}{\sqrt{d'}}$$

Démonstration. (Proposition 6) □

3)
l'application $(d,d')\longmapsto(d.d',d)$ de l'ensemble des couples $(d,d')\in\mathbb{N}^\star\times\mathbb{N}^\star$ vérifiant $n\leqslant x$ et d/n est bien définie et bijective de réciproque $(n,d)\longmapsto\left(d,\frac{n}{d}\right)$,on en déduit :

$$g(x)=\sum_{n\leqslant x}\sum_{d/n}\frac{\chi(d)}{\sqrt{n}}=\sum_{d.d'\leqslant x}\frac{\chi(d)}{\sqrt{d.d'}}$$

où la seconde somme est prise qur l'ensemble des couples (d,d') des entiers $\geqslant$1, tel que $d.d'\leqslant x$, pour de tels entiers, on a $d\leqslant\frac{x}{d'}\leqslant x$, et $d'\leqslant\frac{x}{d}\leqslant x$
et $d'\leqslant\sqrt{x}\Leftrightarrow d>\sqrt{x}$

En coupant en deux somme selon que $d<\sqrt{x}$ ou pas, il vient

$$g(x)=\sum_{\substack{d.d'\leqslant x\\ d>\sqrt{x}}}\frac{\chi(d)}{\sqrt{d.d'}}+\sum_{\substack{d.d'\leqslant x\\ d\leqslant\sqrt{x}}}\frac{\chi(d)}{\sqrt{d.d'}}$$

D'où

$$\boxed{g(x)=\sum_{d'\leqslant\sqrt{x}}\frac{1}{\sqrt{d'}}\sum_{\sqrt{x}<d\leqslant\frac{x}{d'}}\frac{\chi(d)}{\sqrt{d}}+\sum_{d\leqslant\sqrt{x}}\frac{\chi(d)}{\sqrt{d}}\sum_{d\leqslant\frac{x}{d}}\frac{1}{\sqrt{d'}}}$$

Proposition 7.

On a pour tout $x\geqslant 0$

$$g(x)-\sqrt{x}L(\chi)\text{ est bornée}$$

Et $L(\chi)$ est non nul.

Démonstration. (Proposition 7) □

La fonction g est en escalier par définition, et donc continue par morceaux sur son domaine de définition, la fonction $x\longmapsto g(x)-2\sqrt{x}L(\chi)$ est également continue par morceaux sur son domaine de définition, donc pour montrer qu'elle est bornée, il suffit de montrer qu'elle est bornée au voisinage de $+\infty$

Pour $m=[x]$, on a $g(x)=g(m)$ (par définition de g) , donc

$$g(x)-2\sqrt{x}L(\chi)=g(m)-2\sqrt{m}L(\chi)-2L(\chi)-2L(\chi)\frac{x-m}{\sqrt{x}+\sqrt{m}}$$

Puisque $\lim\limits_{x\longmapsto+\infty}\frac{x-[x]}{\sqrt{x}+\sqrt{[x]}}=0$, donc

$$g(x)-2\sqrt{x}L(\chi)=g(m)-2\sqrt{m}L(\chi)+o(1)$$

On se ramène à démontrer que $g(x)-2\sqrt{x}L(\chi)=o(1)$ dans le cas où x est un entier, par ailleurs, par définition , on a:

$$2\sqrt{m}L(\chi)=2\sqrt{m}\sum_{k=1}^{+\infty}\frac{\chi(k)}{k}=2\sum_{k=1}^{+\infty}\frac{\chi(k)}{k}\sqrt{\frac{m}{k}}$$

Donc : $g(m)-2\sqrt{m}L(\chi)$ est égal à:

$$\sum_{d'\leqslant\sqrt{m}}\frac{1}{\sqrt{d'}}\sum_{\sqrt{m}<d\leqslant\frac{m}{d'}}\frac{\chi(d)}{\sqrt{d}}+\sum_{d\leqslant\sqrt{m}}\frac{\chi(d)}{\sqrt{d}}\left(\sum_{d\leqslant\frac{m}{d}}\frac{1}{\sqrt{d'}}-2\sqrt{\frac{m}{d}}\right)-2\sqrt{m}\sum_{d>\sqrt{m}}\frac{\chi(d)}{d}$$

On va démontrer que chacun des termes du membre de droite de cette égalité est bornée avec m, ce qui permet de conclure

On applique le raisenement de la question 1 avec $u_m=\chi(m)$

On note $U_m=\sum_{d=1}^{m}\chi(d)$, on a vu que la suite $(U_m)_{m\geqslant1}$ est bornée, et on dispose donc d'un réel positif A tel que $|U_m|\leqslant A$, Supposons que la suite $(v_m)_{m\geqslant1}$ soit de signe constant de décroissante en valeur absolue, alors pour tout $n\leqslant m$, on a

$$\sum_{n<d\leqslant m}v_du_d=\sum_{d\leqslant m}v_du_d-\sum_{d\leqslant n}v_du_d$$

Donc

$$\sum_{n<d\leqslant m}v_du_d=U_mv_m-U_nv_n+\sum_{d=n}^{m-1}U_d(v_d-v_{d+1})$$

Et par hypothèse de monotonie et de signe sur $(v_m)_{m\geqslant1}$,on a :

$$\left|\sum_{n<d\leqslant m}u_dv_d\right|\leqslant A\left(|v_m|+|v_n|+\sum_{d=n}^{m-1}(|v_d|-|v_{d+1}|)\right)=2A|v_n|$$

Donc

$$\sum_{n<d\leqslant m}u_dv_d=O(v_n)$$

Si de plus, la série $\sum u_dv_d$ converge, alors on peut passer à la limite dans l'inégalité précédente, il vient

$$\sum_{n<d}u_dv_d=O(v_n)$$

On prend d'abord $v_m=\frac{1}{m}$, qui constitue le terme général d'une suite décroissante, positive, avec ce qui précéde, et puisque la série définissant $L(\chi)$ converge, il vient

$$\left|-2\sqrt{m}\sum_{d>\sqrt{m}}\frac{\chi(d)}{d}\right|=\sqrt{m}O\left(\frac{1}{[\sqrt{m}]}\right)=O(1)$$

On prend ensuite $v_m = \frac{1}{\sqrt{m}}$ qui est également le terme général d'une suite positive décroissante, il vient alors:

$$\sum_{\sqrt{m}<d\leqslant\frac{m}{d'}} \frac{\chi(d)}{\sqrt{d}} = O\left(\frac{1}{\sqrt{[\sqrt{m}]}}\right)$$

Or, par comparaison entre une série (De RIEMANN) divergente et une intégrale dans le cas d'une fonction continue positive, on a

$$\sum_{d'<\sqrt{m}} \frac{1}{\sqrt{d'}} \underset{m\to+\infty}{\sim} 2\sqrt{[\sqrt{m}]}$$

Et donc

$$\sum_{d'<\sqrt{m}} \frac{1}{\sqrt{d'}} \sum_{\sqrt{m}<d\leqslant\frac{m}{d'}} \frac{\chi(d)}{\sqrt{d}} = O(1)$$

Pour étudier le dernier termen on constate :

$$\sum_{d'\leqslant\frac{m}{d}} \frac{1}{\sqrt{d'}} - 2\sqrt{\frac{m}{d}} = \sum_{d'\leqslant\frac{m}{d}} \left(\frac{1}{\sqrt{d'}} - \int_{d'-1}^{d'} \frac{\mathrm{dt}}{\sqrt{t}}\right) + 2\sqrt{\left[\frac{m}{d}\right]} - 2\sqrt{\frac{m}{d}}$$

Or

$$\sqrt{\left[\frac{m}{d}\right]} - \sqrt{\frac{m}{d}} = \frac{\left[\frac{m}{d}\right] - \frac{m}{d}}{\sqrt{\left[\frac{m}{d}\right]} + \sqrt{\frac{m}{d}}} = O\left(\sqrt{\frac{d}{m}}\right)$$

Et donc

$$\sum_{d\leqslant\sqrt{m}} \frac{\chi(d)}{d}\left(\sum_{d'\leqslant\frac{m}{d}} \frac{1}{\sqrt{d'}} - 2\sqrt{\frac{m}{d}}\right) = \sum_{d\leqslant\sqrt{m}} \left[\int_{d'-1}^{d'} \left(\frac{1}{\sqrt{d'}} - \frac{1}{\sqrt{t}}\right)\mathrm{dt} + \frac{\chi(d)}{d} O\left(\sqrt{\frac{d}{m}}\right)\right]$$

On remarque qu'on a :

$$\sum_{d\leqslant\sqrt{m}} \frac{\chi(d)}{d} O\left(\sqrt{\frac{d}{m}}\right) = \sum_{d\leqslant\sqrt{m}} O\left(\sqrt{\frac{1}{m}}\right) = O(1)$$

Et que $\int_{d'-1}^{d'} \left(\frac{1}{\sqrt{d'}} - \frac{1}{\sqrt{t}}\right)\mathrm{d}t < 0$

On en déduit que $d \longmapsto \sum_{d' \leqslant \frac{m}{d}} \int_{d'-1}^{d'} \left(\frac{1}{\sqrt{d'}} - \frac{1}{\sqrt{t}}\right)\mathrm{d}t$ est négative et croissante (ie décroissante en valeur absolue) par décroissance de $d \longmapsto \frac{m}{d}$, on pose donc, enfin

$$v_d = \frac{1}{\sqrt{d}} \sum_{d' \leqslant \frac{m}{d}} \int_{d'-1}^{d'} \left(\frac{1}{\sqrt{d'}} - \frac{1}{\sqrt{t}}\right)\mathrm{d}t$$

de sorte que la suite $(v_d)_{d \geqslant 1}$ est négative et décroissante en valeur absolue en tant que produit de deux termes tous deux décroissantes en valeur absolue l'un positif et l'autre négatif, on obtient donc

$$\sum_{d \leqslant \sqrt{m}} \frac{\chi(d)}{d} \sum_{d' \leqslant \frac{m}{d}} \int_{d'-1}^{d'} \left(\frac{1}{\sqrt{d'}} - \frac{1}{\sqrt{t}}\right)\mathrm{d}t = O\left(\int_0^m \frac{\mathrm{d}t}{\sqrt{t}} - \sum_{d'=1}^{m} \frac{1}{\sqrt{d'}}\right)$$

L'intégrale s'entendant comme une limite, or par comparaison entre série et intégrale, on a :

$$\int_1^{m+1} \frac{\mathrm{d}t}{\sqrt{t}} \leqslant \sum_{d'=1}^{m} \frac{1}{\sqrt{d'}} \leqslant \int_0^m \frac{\mathrm{d}t}{\sqrt{t}}$$

Et donc, puisque $\sqrt{m} - \sqrt{m+1} = \frac{-1}{\sqrt{m}+\sqrt{m+1}} = o(1)$

On en déduit

$$\sum_{d \leqslant \sqrt{m}} \frac{\chi(d)}{d} \sum_{d' \leqslant \frac{m}{d}} \int_{d'-1}^{d'} \left(\frac{1}{\sqrt{d'}} - \frac{1}{\sqrt{t}}\right)\mathrm{d}t = O(1)$$

Et ainsi

$$\boxed{g(x) - 2\sqrt{x}L(\chi) \text{ est bornée}}$$

On en déduit que la fonction $x \longmapsto 2\sqrt{x}L(\chi)$ tend vers l'infini en $-\infty$ et donc que $L(\chi)$ est strictement positif, en particulier :

$$\boxed{L(\chi) \text{ est non nul}}$$

Théorème 10.

Soit χ un caractère non trivial

Si $L(\chi)\neq 0$, alors la fonction $x\to \sum_{n\leqslant x}\frac{\mu(n)\chi(n)}{n}$ est bornée

Si $L(\chi)\neq 0$, alors la fonction $x\to L_1(\chi)\sum_{n\leqslant x}\frac{\mu(n)\chi(n)}{n}+\log(x)$ est bornée

Démonstration. (Théorème 10) □

Soit χ un caractère non trivial
Si $L(\chi)\neq 0$
Posons pour tout $x\geqslant 0$, $G(x)=\sum_{1\leqslant n\leqslant x}\frac{x}{n}\chi(n)$

La fonction G est le produit de l'identité et une fonction en escalier, elle est donc continue par morceaux sur son domaine de définition, et il suffit de montrer qu'elle est bornée au voisinage de l'infini, D'après la proposition 3, la série $\sum_{n\geqslant 1}\frac{\chi(n)}{n}$ converge, il vient par positivité et décroissance de $\left(\frac{1}{n}\right)_{n\geqslant 1}$

$$G(x)-x.L(\chi)=x\sum_{n>x}\frac{\chi(n)}{n}=O\left(\frac{x}{[x]}\right)=O(1)$$

i.e $G(x)-x.L(\chi)$ est bornée.

le caractère χ étant multiplicatif, on applique le théorème 9
avec $F=\mathrm{id}$, $H=\chi$ et donc les applications notées G sont identiques.
On en déduit

$$x=\sum_{1\leqslant k\leqslant x}\mu(k)G\left(\frac{x}{k}\right)\chi(k)$$

Donc

$$x-L(\chi)\sum_{1\leqslant k\leqslant x}\mu(k)\frac{\chi(k)}{k}=\sum_{1\leqslant k\leqslant x}\mu(k)\chi(k)\left(G\left(\frac{x}{k}\right)-\frac{x}{k}L(\chi)\right)$$

Ainsi

$$x-L(\chi)\sum_{1\leqslant k\leqslant x}\mu(k)\frac{\chi(k)}{k}=O\left(\sum_{1\leqslant k\leqslant x}|\mu(k)\chi(k)|\right)$$

Or μ et χ sont bornés par 1 (on a déjà remarqué que χ prend ses valeurs non nulles dans les racines de l'unité) donc

$$x.L(\chi)\sum_{1\leqslant k\leqslant x}\mu(k)\frac{\chi(k)}{k}=O(x)$$

And

$$L(\chi)\sum_{1\leqslant k\leqslant x}\mu(k)\frac{\chi(k)}{k}=O(1)$$

Par conséquent, si $L(\chi)$ est non nul, et puisqu'on a affaire à une fonction en escalier, donc continue par morceaux sur son domaine de définition.

$$\boxed{\sum_{n\leqslant x}\frac{\mu(n)\chi(n)}{n}\text{ est bornée}}$$

Si $L(\chi)=0$, posons pour tout $x>1$, $G_1(x)=\sum_{1\leqslant n\leqslant x}\left(\frac{x}{n}\log\left(\frac{x}{n}\right)\right)\chi(n)$

Par définition et par convergence des séries définissant $L(\chi)$ et $L_1(\chi)$

On a , en tenant compte de $L(\chi)=0$

$$G_1(x)+x.L_1(\chi)=G_1(x)+x.L(\chi)+x.L_1(x)$$

Ainsi

$$G_1(x)+x.L_1(\chi)=-x.\log(x)\sum_{n>x}\frac{\chi(n)}{n}+x\sum_{n>x}\frac{\chi(n)\log(n)}{n}$$

Or, pour tout $n\geqslant 3$, on a $\log(n)\geqslant 1$ et donc

$$\log(n+1)=\log(n)+\log\left(1+\frac{1}{n}\right)\leqslant\log(n)+\frac{1}{n}\leqslant\log\left(1+\frac{1}{n}\right)+\log(n)\frac{n}{n+1}$$

Les suites $\left(\frac{1}{n}\right)_{n\geqslant 1}$ et $\left(\frac{\log(n)}{n}\right)_{n\geqslant 3}$ sont donc positives et decroissantes, il résulte alors des relations obtenues en proposition 7

Pour $x>2$;

$$\sum_{n>x}\frac{\chi(n)}{n}=O\left(\frac{1}{x}\right)\text{ et }\sum_{n>x}\frac{\chi(n)\log(n)}{n}=O\left(\frac{\log(x)}{x}\right)$$

D'où

$$G_1(x) = -x.L_1(x) + O(\log(x))$$

On applique le théorème 9 , avec $F = \mathrm{id} \times \log$ et $H = \chi$, les applications notées G_1 et G dans la théorème 9 coincident alors et on en déduit

$$x.\log(x) = \sum_{1 \leqslant k \leqslant x} \mu(k) G_1\Big(\frac{x}{k}\Big)\chi(k)$$

et donc,

$$x.\log(x) + x.L_1(\chi) \sum_{1 \leqslant k \leqslant x} \mu(k)\frac{\chi(k)}{k} = \sum_{1 \leqslant k \leqslant x} \mu(k)\chi(k)\Big(G_1\Big(\frac{x}{k}\Big) + \frac{x}{k}L_1(x)\Big)$$

Ainsi

$$x.\log(x) + x.L_1(\chi) \sum_{1 \leqslant k \leqslant x} \mu(k)\frac{\chi(k)}{k} = O\left(\sum_{1 \leqslant k \leqslant x} \log\Big(\frac{x}{k}\Big)\right)$$

Avec

$$O\left(\sum_{1 \leqslant k \leqslant x} \log\Big(\frac{x}{k}\Big)\right) = O(x.\log(x) - \log([x]!))$$

Ainsi en utilisant la formule de stirling:

$$O\left(\sum_{1 \leqslant k \leqslant x} \log\Big(\frac{x}{k}\Big)\right) = O(x.\log(x) - [x]\log([x]) + O(x))$$

Ainsi

$$O\left(\sum_{1 \leqslant k \leqslant x} \log\Big(\frac{x}{k}\Big)\right) = O\left((x - [x]).\log(x) - [x]\log\left(\frac{x}{[x]}\right) + O(x)\right)$$

Avec

$$O\left((x - [x]).\log(x) - [x]\log\left(\frac{x}{[x]}\right) + O(x)\right) = O(1).\log(x) + O(x).O(1) + O(x)$$

Et

$$O(1).\log(x)+O(x).O(1)+O(x)=O(x)$$

Et donc

$$\log(x)+L_1(\chi)\sum_{1\leqslant k\leqslant x}\mu(k)\frac{\chi(k)}{k}=O(1)$$

Et ainsi, puisqu'on a affaire à des fonctions continues par morceaux sur leur domaine de définition

$$\boxed{\log(x)+L_1(\chi)\sum_{1\leqslant k\leqslant x}\mu(k)\frac{\chi(k)}{k}\text{ est bornée}}$$

Théorème 11.

On a :

$$L_1(\chi)\sum_{d\leqslant x}\frac{\mu(d)\chi(d)}{d}=\sum_{m\leqslant x}\Lambda(m)\frac{\chi(m)}{m}+O(1)$$

Démonstration. (Théorème 11) □

Puisque la suite $\left(\frac{\log(n)}{n}\right)_{n\geqslant 3}$ est positive et décroissante

En utilisant les relations de la proposition 7 on obtient

$$\sum_{n>m}\frac{\chi(n)\log(x)}{n}=O\left(\frac{\log(m)}{m}\right)$$

Par definition et par associativité, on a puisque la seconde somme est finie et par multiplicativiité de χ

$$L_1(\chi)\sum_{d\leqslant x}\frac{\mu(d)\chi(d)}{d}=\sum_{d\leqslant x}\left(\sum_{n=1}^{+\infty}\frac{\chi(n)\log(n)}{n}\frac{\mu(d)\chi(d)}{d}\right)$$

Ainsi

$$L_1(\chi)\sum_{d\leqslant x}\frac{\mu(d)\chi(d)}{d}=\sum_{d\leqslant x}\sum_{n\leqslant\frac{x}{d}}\frac{\chi(n)\log(n)}{n}\frac{\mu(d)\chi(d)}{d}+\sum_{d\leqslant x}\sum_{n>\frac{x}{d}}\frac{\chi(n)\log(n)}{n}\frac{\mu(d)\chi(d)}{d}$$

Par suite

$$L_1(\chi)\sum_{d\leqslant x}\frac{\mu(d)\chi(d)}{d}=\sum_{m\leqslant x}\sum_{d/m}\mu(d).\log\Big(\frac{m}{d}\Big)\frac{\chi(m)}{m}+\sum_{d\leqslant x}O\left(\frac{d.\log\big(\frac{x}{d}\big)}{x}\right)\frac{\mu(d)\chi(d)}{d}$$

En utilisant la bijective $(d,n)\longmapsto(n.d,d)$, et la proposition 2, il vient

$$L_1(\chi)\sum_{d\leqslant x}\frac{\mu(d)\chi(d)}{d}=\sum_{m\leqslant x}\Lambda(m)\frac{\chi(m)}{m}+\frac{1}{x}\sum_{d\leqslant x}O\Big(\log\Big(\frac{x}{d}\Big)\Big)$$

Or, on a vu que : $\sum\limits_{d\leqslant x}\log\big(\frac{x}{d}\big)=O(x)$ et donc

$$L_1(\chi)\sum_{d\leqslant x}\frac{\mu(d)\chi(d)}{d}=\sum_{m\leqslant x}\Lambda(m)\frac{\chi(m)}{m}+O(1)$$

Enfin on a :

$$\sum_{m\leqslant x}\Lambda(m)\frac{\chi(m)}{m}=\sum_{p\leqslant x}\log(p)\sum_{n\leqslant\frac{\log(x)}{\log(p)}}\frac{\chi(p)^n}{p^n}$$

$$\sum_{m\leqslant x}\Lambda(m)\frac{\chi(m)}{m}=\sum_{p\leqslant x}\log(p)\frac{\chi(p)}{p}+\sum_{p\leqslant x}\log(p)\sum_{2\leqslant n\leqslant\frac{\log(x)}{\log(p)}}\frac{\chi(p)^n}{p^n}$$

Avec

$$\sum_{p\leqslant x}\log(p)\sum_{2\leqslant n\leqslant\frac{\log(x)}{\log(p)}}\frac{\chi(p)^n}{p^n}=\sum_{p\leqslant x}\log(p)\sum_{2\leqslant n\leqslant\frac{\log(x)}{\log(p)}}O\left(\frac{1}{p^n}\right)$$

Par suite:

$$\sum_{p\leqslant x}\log(p)\sum_{2\leqslant n\leqslant\frac{\log(x)}{\log(p)}}\frac{\chi(p)^n}{p^n}=\sum_{p\leqslant x}O\left(\frac{1}{p^2}\frac{1}{1-\frac{1}{p}}\right)\log(p)=O(1)$$

Ainsi:

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

Puisque $\log(p)\frac{1}{p^2}\frac{1}{1-\frac{1}{p}} \underset{p\to+\infty}{\sim} \frac{\log(p)}{p^2} = O\left(\frac{1}{p^{\frac{3}{2}}}\right)$ et donc par comparaison avec une série de RIEMANN convergente, on a $\sum \log(p)\frac{1}{p^2}\frac{1}{1-\frac{1}{p}}$ est absolument convergente, il en résulte

$$\boxed{L_1(\chi)\sum_{n\leqslant x}\frac{\mu(n)\chi(n)}{n} = \sum_{p\leqslant x}\frac{\chi(p)\log(p)}{p} + O(1)}$$

Proposition 6.

On a :

$$\sum_{p\leqslant x}\frac{\chi(p)\log(p)}{p} = \begin{cases} O(1) \text{ si } L(\chi)\neq 0 \\ -\log(x)+O(1) \text{ si } L(\chi)=0 \end{cases}$$

Démonstration. (Proposition 6) □

Il découle d'après les théorème 10 et 11, qu'on a

$$\sum_{p\leqslant x}\frac{\chi(p)\log(p)}{p} = L_1(\chi)\sum_{n\leqslant x}\frac{\mu(n)\chi(n)}{n} + O(1)$$

Et donc

$$\boxed{\sum_{p\leqslant x}\frac{\chi(p)\log(p)}{p} = \begin{cases} O(1) \text{ si } L(\chi)\neq 0 \\ -\log(x)+O(1) \text{ si } L(\chi)=0 \end{cases}}$$

Théorème 12.

$$\#G(N).\sum_{\substack{p\leqslant x \\ p\equiv 1[N]}}\frac{\chi(p)\log(p)}{p} = \log(x)+O(1)$$

Démonstration. (Théorème 12) □

Soit T le nombre de caractéres non triviaux tels que $L(\chi)=0$. Montrons d'abord que :

$$\#G(N).\sum_{\substack{p\leqslant x \\ p\equiv 1[N]}}\frac{\chi(p)\log(p)}{p} = (1-T)\log(x)+O(1)$$

Et puis que $T \leqslant 1$
D'apès la formule de Mernes si χ est trivial on a

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

Et donc en utilisant le résultat précédent

$$\sum_{\chi\in G(N)}\sum_{p\leqslant x}\frac{\chi(p)\log(p)}{p}=(1-T)\log(x)+O(1)$$

Puisqu'on affaire à des sommes finies, on peut les échanger, donc

$$\#G(N).\sum_{\substack{p\leqslant x\\ p\equiv 1[N]}}\frac{\chi(p)\log(p)}{p}=(1-T)\log(x)+O(1)$$

Comme le nombre de gauche est positif en tant qu'une somme de termes positifs, celui de droite l'est aussi et donc $T\leqslant 1$

Montrons maintenant $T=0$, pour conclure

Si χ est non trivial, et à valeurs réelles, alors $L(\chi)\neq 0$
D'après la propostion 7 ,n si χ n'est pas à valeurs réelles alors $\overline{\chi}$ est distinct de χ et $L(\overline{\chi})=\overline{L(\chi)}$, de sorte ue les deux sont simultanément nuls ou non, comme $T\leqslant 1$ aucun des deux n'est nul et finalement $T=0$.

Théorème 13.(Théorème de Dirichlet)
Soit l un entier premier à N alors

$$\{p\,\text{premier}\,/\,p\equiv l[N]\}\,\text{est infini.}$$

Démonstration. (Théorème 13) □

On déduit de ce qui précède que, pour χ non trivial, on a :

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

Donc,

$$\sum_{\chi\in G(N)}\sum_{p\leqslant x}\overline{\chi}(l)\frac{\chi(p)\log(p)}{p}=\sum_{p\leqslant x}\frac{\log(p)}{p}=\log(x)+O(1)$$

Puisque l est premier à N, on dispose d'une relation de BEZOUT, $a.l+b.N=1$, avec a et b deux entiers, et alors $\chi(a)\chi(l)=1$,

De plus si d est l'ordre de la classe modulo N dans $G(N)$ alors $l^d \equiv 1[N]$ et donc $\chi(l)^d=\chi(1)=1$ et $\chi(l)$ est une racine de l'unité et donc

$$\sum_{\chi\in G(N)} \bar{\chi}(l)\chi(p) = \sum_{\chi\in G(N)} \chi(a.p)$$

et cette derniere somme est nulle sauf si $a.p\equiv 1[N]$ auquel cas elle vaut $\#G(N)$.

D'après l'étude des groupes finis on a:

$a.p\equiv 1[N]$ si et seulement si $p\equiv l[N]$ et donc

$$\sum_{p\leqslant x}\sum_{\chi\in G(N)} \bar{\chi}(l)\frac{\chi(p)\log(p)}{p} = \#G(N)\sum_{\substack{p\leqslant x\\ p\equiv l[N]}}\frac{\log(p)}{p}$$

Si l'ensemble $\{p \text{ premier} / p\equiv l[N]\}$ est fini, alors la seconde somme est bornée (et même constante) au voisinage de l'infini, et saurait donc être équivalente à $\log(x)$

Par conséquent

$\{p \text{ premier} / p\equiv l[N]\}$ est infini.

Généralisations:

- La conjecture de Bunyakovsky généralise le théorème de Dirichlet aux polynômes de degré supérieur. Si même de simples polynômes quadratiques tels que x^2+1 (connu d'après le quatrième problème de Landau) atteindre une infinité de valeurs premières est un problème ouvert important.
- La conjecture de Dickson généralise le théorème de Dirichlet à plus d'un polynôme.
- L'hypothèse de Schinzel H généralise ces deux conjectures, c'est-à-dire se généralise à plus d'un polynôme avec un degré supérieur à un.
- Dans la théorie algébrique des nombres, le théorème de Dirichlet se généralise au théorème de densité de Chebotarev.
- Le théorème de Linnik (1944) concerne la taille du plus petit nombre premier dans une progression arithmétique donnée. Linnik a prouvé que la progression $a+n.d$ (comme n varie à travers les entiers positifs) contient un premier de magnitude au plus cd^L pour les constantes absolues c et L. Les chercheurs ultérieurs ont réduit L à 5.
- Un analogue du théorème de Dirichlet tient dans le cadre des systèmes dynamiques (T. Sunada et A. Katsuda, 1990).