Le Théorème

de la

Progression Arithmétique

de

Dirichlet

Delphine Longuet

Encadrant : Abdelmejid Bayad

Mémoire de Maîtrise

Université d'Evry-Val d'Essonne

Année 2002-2003

Table des matières

Introduction

Il y a près de vingt-trois siècles, Euclide démontrait l'infinitude de l'ensemble des nombres premiers. Sa preuve, qui tient en quelques lignes, est la suivante. On considère l'ensemble des nombres premiers comme étant fini et on note $p_1, p_2, \ldots, p_n$ ses éléments. On considère ensuite le nombre suivant :

$$P = p_1 p_2 \ldots p_n + 1$$

Ce nombre n'est divisible par aucun des p_i, donc il existe un nombre premier strictement supérieur à tous les p_i qui divise P. Il en résulte que l'ensemble des nombres premiers est infini.

Le même type d'argument sert à montrer qu'il existe une infnité de nombres premiers de certaines sortes. Comme tous les nombres premiers après 2 sont impairs, chacun se trouve dans une des deux progressions suivantes :

(a) 1, 5, 9, 13, 17, 21, 25, ...

(b) 3, 7, 11, 15, 19, 23, 27, ...

La progression (a) est formée des nombres s'écrivant sous la forme $4x + 1$ pour $x \geq 0$, la progression (b) de ceux s'écrivant sous la forme $4x - 1$ pour $x \geq 1$ (ou $4x + 3$ pour $x \geq 0$, ce qui revient au même). Nous allons tout d'abord démontrer qu'il y a une infinité de nombres premiers dans la progression (b).

En raisonnant par l'absurde, on considère qu'il n'y a que n nombres premiers notés $q_1, q_2, \ldots, q_n$ s'écrivant $4x - 1$, avec $q_1 = 3$. On considère alors le nombre N défini comme suit :

$$N = 4(q_1 q_2 \ldots q_n) - 1$$

C'est aussi un nombre de la forme $4x - 1$. Tous les facteurs premiers de N ne peuvent pas être de la forme $4x + 1$, car le produit de deux nombres de la forme $4x + 1$ est aussi un nombre de cette forme :

$$(4x + 1)(4y + 1) = 4(4xy + x + y) + 1$$

Etant donné que tous les nombres premiers sont répartis entre (a) et (b), N a forcément au moins un facteur premier de la forme $4x - 1$. Ce facteur ne peut être aucun des q_i car $N \equiv -1 (\text{mod } q_i)$, pour tout $i = 1, \ldots, n$. Donc il existe un nombre premier de la forme $4x - 1$ supérieur à tous les q_i et ainsi la progression (b) contient une infinité de nombres premiers.

On ne peut pas utilisé le même argument pour montrer qu'il y a une infinité de nombres premiers dans la progression (a), car si on construit un nombre de la forme $4x + 1$, il n'en découle pas nécessairement que ce nombre a un facteur premier de cette forme. On procède donc comme suit. On note les nombres premiers de la suite (a) par $r_1, r_2, \ldots, r_n$, et on considère le nombre M défini par :

$$M = (r_1 r_2 \ldots r_n)^2 + 1$$

Tout nombre de la forme a^2+1 se décompose en un produit de facteurs premiers de la forme $4x+1$, multiplié ou non par 2 (on admettra ce résultat dont la démonstration fait appel à des notions qui nous éloigneraient du sujet). Puisque M n'est divisible par aucun des r_i, il existe un nombre premier de la forme $4x+1$ supérieur à tous les r_i. Il y a donc une infinité de nombres premiers dans la progression (a).

On retrouve la même situation avec les progressions $6x+1$ et $6x-1$. Ces progressions excluent tous les nombres divisibles par 2 ou 3, par conséquent chaque nombre premier se trouve dans l'une ou l'autre de ces progressions. On prouve en appliquant des méthodes similaires à celles employées précédemment que chacune de ces progressions contient une infinité de nombres premiers.

On considère maintenant une progression arithmétique quelconque $mx+a$ avec $x \geq 0$. Si les entiers m et a ont un diviseur commun, alors chacun des nombres de la suite a ce diviseur et n'est donc pas premier (à part peut-être a). On doit donc supposer que m et a sont premiers entre eux. Il semble alors possible que la suite obtenue contienne une infinité de nombres premiers. On énonce le théorème suivant :

Théorème de progression arithmétique *Soient $m, a \in \mathbb{N}^*$, premiers entre eux. Il existe une infinité de nombres premiers dans la progression arithmétique $mx+a$, $x \in \mathbb{N}$.*

En 1785, Adrien-Marie Legendre, au cours de sa démonstration de la loi de réciprocité quadratique, introduit ce résultat sans le démontrer. Il essaiera plus tard d'en établir une preuve mais n'y parviendra pas. La première démonstration fut donnée par Peter-Gustav Lejeune-Dirichlet dans un mémoire présenté devant l'Académie des Sciences de Berlin en 1837. La méthode de Dirichlet, sortant du cadre de la théorie algébrique des nombres pour exploiter des résultats d'analyse, est la première de ce type. Elle repose sur l'étude des fonctions L de Dirichlet, définies au moyen de fonctions arithmétiques particulières, appelées caractères, bien adaptées aux progressions arithmétiques dont il est question. On va donc commencer par introduire les différentes notions citées ainsi que les propriétés dont on aura besoin dans la démonstration finale.

1 Caractères d'un groupe abélien fini

Les progressions arithmétiques que l'on considère sont du type $mx+a$ où a est premier avec m, c'est-à-dire appartient au groupe multiplicatif formé des éléments inversibles de l'anneau $\mathbb{Z}/m\mathbb{Z}$. C'est pourquoi un rôle important sera joué par le groupe abélien fini $\left(\mathbb{Z}/m\mathbb{Z}\right)^*$, ainsi que ses caractères, notion que l'on va introduire d'une façon générale.

Dans cette partie, on désignera par G le groupe abélien fini (G, .).

1.1 Dual d'un groupe abélien fini

Définition 1.1 *On appelle l'homomorphisme* $\chi : (\mathrm{G}, .) \to (\mathbb{C}^*, \times)$ *un caractère de* G. *Les caractères de* G *forment le groupe* $(\mathrm{Hom}(\mathrm{G}, \mathbb{C}^*), \times)$ *qu'on note* $\widehat{\mathrm{G}}$ *et qu'on appelle dual de* G.

Il est aisé de voir que $\widehat{\mathrm{G}}$ est un groupe. On définit tout d'abord l'unité χ_0 de $\widehat{\mathrm{G}}$ par $\chi_0(a) = 1$ pour tout $a \in \mathrm{G}$. Ensuite, si $\chi, \psi \in \widehat{\mathrm{G}}$, on a $\chi\psi$ défini par $\chi\psi(a) = \chi(a)\psi(a)$ pour tout $a \in \mathrm{G}$, et $\chi\psi$ est un caractère. Enfin, on définit l'inverse de $\chi \in \widehat{\mathrm{G}}$ par $\chi^{-1}(a) = \chi(a)^{-1} = \overline{\chi(a)}$ car $\chi(a) \in \mathbb{U}_n$. On voit que $\chi^{-1} \in \widehat{\mathrm{G}}$ et que $\chi\chi^{-1} = \chi\overline{\chi} = \chi_0$.

On va maintenant énoncer quelques propositions qui vont permettre de démontrer ce qu'on appelle les "relations d'orthogonalité", dont on aura besoin par la suite.

Proposition 1.1 *Soit* H *un sous-groupe de* G. *Tout caractère de* H *peut être prolongé en un caractère de* G.

Démonstration

Si H = G, il n'y a rien à démontrer.

Soit H un sous-groupe strict de G et $x \in$ G - H. Il existe des entiers $k \geq 1$ tels que $x^k \in$ H, au moins $k = n$ l'ordre de G car $x^n = 1$. Soit k_0 le plus petit de ces entiers, alors $k_0 \geq 2$ car $x \notin$ H. On peut alors écrire tout entier $k' \in \mathbb{Z}$ sous la forme $k' = k_0 a + b$, où $a \in \mathbb{Z}$ et $0 \leq b < k_0$. Ainsi, pour avoir $x^{k'} \in$ H, comme $x^{k_0 a} \in$ H, il faut que $x^b \in$ H. Mais k_0 est le plus petit entier k tel que $x^k \in$ H, et $b < k_0$ donc pour que x^b appartienne à H, il faut que $b = 0$, c'est-à-dire $k' = k_0 a$.

Soit χ un caractère de G. On va maintenant construire un prolongement χ' de χ au sous-groupe de G noté H' engendré par H et x. H' contient strictement H car $x \notin$ H. D'une part, on prend $z \in \mathbb{C}$ tel que $z^{k_0} = \chi(x^{k_0})$. D'autre part, tout élément h' de H' s'écrit sous la forme $h' = hx^r$, où $h \in$ H et $r \in \mathbb{Z}$. A priori, on n'a pas unicité de l'écriture de h'. Si h' s'exprime aussi sous la forme $h' = gx^s$, avec $g \in$ H et $s \in \mathbb{Z}$, alors $x^{s-r} = hg^{-1} \in$ H, d'où $s - r = k_0 a$, avec $a \in \mathbb{Z}$, et on a

$$\begin{aligned}\chi(h)z^r\chi(g)^{-1}z^{-s} &= \chi(hg^{-1})z^{-k_0a} \\ &= \chi(hg^{-1})\chi(x^{k_0})^{-a} \\ &= \chi(hg^{-1})\chi(x^{-k_0a}) \\ &= \chi(1) \qquad\qquad \text{car } hg^{-1} = x^{k_0a} \\ &= 1\end{aligned}$$

Ainsi le produit $\chi(h)z^r$ ne dépend pas de la décomposition de h'. On pose alors

$$\chi'(h') = \chi(h)z^r$$

χ' est bien un morphisme car $\chi'(h'_1h'_2) = \chi'(h'_1)\chi'(h'_2)$, pour tous $h'_1, h'_2 \in$ H', et χ' prolonge χ sur H' car pour $r = 0$, on a bien $\chi'(h) = \chi(h)$, pour tout $h \in$ H.

On a donc construit un prolongement de χ sur H'. Comme H' contient strictement H et que G est fini, on obtient un prolongement de χ sur G entier en un nombre fini d'itérations.

□

Proposition 1.2 $\widehat{\mathrm{G}}$ *est isomorphe à* G.

Démonstration

On sait que tout groupe abélien fini est produit direct de groupes cycliques. Il suffit donc de montrer la proposition pour G groupe cyclique, puis de montrer que le produit direct des duals est isomorphe au dual du produit, ce qui est évident si on considère l'isomorphisme

$$\begin{aligned}\psi : \widehat{\mathrm{G}} &\to \widehat{\mathrm{H}}_1 \times \widehat{\mathrm{H}}_n \\ \chi &\mapsto \left(\chi_{|\mathrm{H}_1}, \ldots, \chi_{|\mathrm{H}_n}\right)\end{aligned}$$

On considère G groupe cyclique. On note n son ordre, et a l'élément qui l'engendre. Soit $\chi \in \widehat{\mathrm{G}}$ et $\chi(a) = b$. Alors

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

Donc $b \in \mathbb{U}_n$, le groupe cyclique des racines n-ièmes de l'unité de $\mathbb{C}$. D'où $\mathrm{Im}(\chi) \subset \mathbb{U}_n$. On considère alors le morphisme

$$\begin{aligned}\varphi : \widehat{\mathrm{G}} &\to \mathbb{U}_n \\ \chi &\mapsto \chi(a)\end{aligned}$$

On veut montrer que φ est un isomorphisme. φ est injectif car si $\chi(a) = 1$, alors χ est identiquement égal à 1, puisque a est un générateur de G.

Pour montrer que φ est surjectif, on introduit les morphismes suivants :

$$\begin{aligned} f : \mathbb{Z} &\to \mathrm{G} & \qquad g : \mathbb{Z} &\to \mathbb{U}_n \\ 1 &\mapsto a & 1 &\mapsto \eta \end{aligned}$$

f est surjectif; en effet, pour tout $k \in \mathbb{Z}$ $f(k) = a^k$ et tout élément de G s'écrit a^k avec $k \in \mathbb{Z}$, et a donc un antécédent par f. De plus, $n\mathbb{Z} = \mathrm{Ker}(f) \subset \mathrm{Ker}(g)$. On peut donc factoriser g par f, c'est-à-dire qu'il existe $\chi : \mathrm{G} \to \mathbb{U}_n$ tel que $\chi \circ f = g$. On a alors

$$\eta = g(1) = \chi \circ f(1) = \chi(a)$$

Donc pour tout $\eta \in \mathbb{U}_n$, il existe $\chi \in \widehat{\mathrm{G}}$ tel que $\varphi(\chi) = \eta$. D'où φ est surjectif.
Ainsi $\widehat{\mathrm{G}}$ est isomorphe à $\mathbb{U}_n$, donc cyclique d'ordre n.

□

Proposition 1.3 $\widehat{\widehat{\mathrm{G}}}$ *est isomorphe à* G.

Démonstration

Si $x \in \mathrm{G}$, l'applcation $\chi \mapsto \chi(x)$ est un caractère de $\widehat{\mathrm{G}}$. On obtient alors le morphisme

$$\begin{aligned} \varepsilon \quad : \quad & \mathrm{G} \to \widehat{\widehat{\mathrm{G}}} \\ & x \mapsto \chi(x) \end{aligned}$$

On va montrer que ε est un isomorphisme.

Puisqu'un groupe et son dual sont de même ordre, $\widehat{\widehat{\mathrm{G}}}$ est du même ordre que $\widehat{\mathrm{G}}$, qui est du même ordre que G. Il suffit donc de montrer que ε est injectif, c'est-à-dire que si a est un élément de G, $a \neq 1$, il existe un caractère χ de G tel que $\chi(a) \neq 1$. Soit H le sous-groupe cyclique de G engendré par a. En reprenant les notations de la démonstration précédente, on a vu que pour tout $\eta \in \mathbb{U}_n$, il existe χ caractère de H tel que $\chi(a) = \eta$, donc si on prend $\eta \neq 1$, $\chi(a) \neq 1$. De plus, d'après la proposition 1.1, on peut prolonger χ en un caractère de G. D'où ε est bien injectif, donc surjectif, et $\widehat{\widehat{\mathrm{G}}}$ est isomorphe à G.

□

1.2 Relations d'orthogonalité

Proposition 1.4 (Relations d'orthogonalité) *Soient* $\chi, \psi \in \widehat{\mathrm{G}}$, $a, b \in \mathrm{G}$ *et* n *l'ordre de* G.

$$\sum_{a \in \mathrm{G}} \chi(a)\overline{\psi(a)} = n\delta_{\chi,\psi} \tag{1.1}$$

$$\sum_{\chi \in \widehat{\mathrm{G}}} \chi(a)\overline{\chi(b)} = n\delta_{a,b} \tag{1.2}$$

Démonstration

(1.1) Comme $\chi(a)\overline{\psi(a)} = \chi\psi^{-1}(a)$, il suffit de montrer que

$$\sum_{a \in \mathrm{G}} \chi(a) = n\delta_{\chi,\chi_0}$$

Par définition de χ_0, on a

$$\sum_{a\in \mathrm{G}} \chi_0(a) = \sum_{a\in \mathrm{G}} 1 = \mathrm{Card}(\mathrm{G}) = n$$

Soit $\chi \in \widehat{\mathrm{G}}$, $\chi \neq \chi_0$. Alors il existe $b \in \mathrm{G}$ tel que $\chi(b) \neq 1$. On a

$$\chi(b) \sum_{a\in \mathrm{G}} \chi(a) = \sum_{a\in \mathrm{G}} \chi(ab) = \sum_{a\in \mathrm{G}} \chi(a)$$

Donc $(\chi(b) - 1) \sum_{a\in \mathrm{G}} \chi(a) = 0$ et comme $\chi(b) \neq 1$, $\sum_{a\in \mathrm{G}} \chi(a) = 0$.

(1.2) Comme $\chi(a)\overline{\chi(b)} = \chi(ab^{-1})$, il suffit de montrer que

$$\sum_{\chi\in \widehat{\mathrm{G}}} \chi(a) = n\delta_{a,1}$$

Il est clair qu'on a

$$\sum_{\chi\in \widehat{\mathrm{G}}} \chi(1) = \sum_{\chi\in \widehat{\mathrm{G}}} 1 = \mathrm{Card}(\widehat{\mathrm{G}}) = n$$

Soit $a \in \mathrm{G}$, $a \neq 1$. Comme on l'a vu dans la preuve de la proposition 1.3, il existe $\psi \in \widehat{\mathrm{G}}$ tel que $\psi(a) \neq 1$. On a

$$\psi(a) \sum_{\chi\in \widehat{\mathrm{G}}} \chi(a) = \sum_{\chi\in \widehat{\mathrm{G}}} \psi\chi(a) = \sum_{\chi\in \widehat{\mathrm{G}}} \chi(a)$$

Donc $(\psi(a) - 1) \sum_{\chi\in \widehat{\mathrm{G}}} \chi(a) = 0$ et comme $\psi(a) \neq 1$, $\sum_{\chi\in \widehat{\mathrm{G}}} \chi(a) = 0$.

□

1.3 Caractères modulaires

Soit $m \in \mathbb{N}^*$. On considère maintenant le groupe multiplicatif $\left(\mathbb{Z}/m\mathbb{Z}\right)^*$ des éléments inversibles de l'anneau $\mathbb{Z}/m\mathbb{Z}$. C'est un groupe abélien fini d'ordre $\varphi(m)$, où φ est la fonction d'Euler, qui à $m \in \mathbb{N}^*$ associe le nombre d'entiers k premiers avec m tels que $1 \leq k \leq m$. Ce groupe admet donc $\varphi(m)$ caractères.

Définition 1.2 *Etant donné un caractère $\tilde{\chi}$ de $\left(\mathbb{Z}/m\mathbb{Z}\right)^*$, on appelle caractère modulo m associé à $\tilde{\chi}$ l'application χ de $\mathbb{Z}$ dans $\mathbb{C}$ définie par $\chi(a) = \tilde{\chi}(\bar{a})$ si* $\mathrm{pgcd}(a, m) = 1$ *($\bar{a}$ désigne la classe de a dans $\left(\mathbb{Z}/m\mathbb{Z}\right)^*$), et $\chi(a) = 0$ si* $\mathrm{pgcd}(a, m) \neq 1$.

On remarque que si χ est un caractère modulo m, $\chi(ab) = \chi(a)\chi(b)$ quels que soient les entiers a et b. On note aussi que les caractères modulo m sont des fonctions $\varphi(m)$-périodiques. On définit le caractère principal modulo m comme étant la fonction égale à 1 pour $\text{pgcd}(a, m) = 1$ et 0 sinon, c'est-à-dire la fonction indicatrice des entiers premiers à m.

On va maintenant interpréter les relations d'orthogonalité pour les caractères modulo m. De la définition 1.2 et de la proposition 1.4, on déduit

Proposition 1.5 *Soient χ et ψ deux caractères modulo m, et $a, b \in \mathbb{Z}$.*

$$\sum_{a=0}^{m-1} \chi(a)\overline{\psi(a)} = \varphi(m)\delta_{\chi,\psi}$$

$$\sum_{\chi} \chi(a)\overline{\chi(b)} = \varphi(m)\delta_{\bar{a},\bar{b}}$$

où la somme s'étend sur tous les caractères modulo m et $\bar{a}$ désigne la classe de a dans $\left(\mathbb{Z}/m\mathbb{Z}\right)^*$.

2 Séries de Dirichlet

Dans cette partie, $s \in \mathbb{C}$.

Définition 2.1 *Si f est une fonction arithmétique, i.e. $f : \mathbb{N} \to \mathbb{C}$, alors sa série de Dirichlet est*

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

Tout comme générer une fonction de la forme $A(x) = \sum_{n=1}^{\infty} a_n x^n$ sert à étudier la suite des a_n définis par récurrence, la série de Dirichlet $F(s)$ sert à étudier la fonction arithmétique f.

On énonce maintenant une propriété de certaines fonctions arithmétiques qui nous sera utile par la suite.

Définition 2.2 *Une fonction arithmétique f est dite multiplicative si $f(nn') = f(n)f(n')$ pour tous n et n' premiers entre eux. Elle est dite complètement multiplicative si elle vérifie cette propriété pour tous entiers n et n'.*

Donc si f est multiplicative, elle est entièrement déterminée par ses valeurs pour les puissances de nombres premiers. Si elle est complètement multiplicative, il suffit de connaître ses valeurs pour les nombres premiers.

2.1 Produits eulériens

Proposition 2.1 *Soit une fonction arithmétique f multiplicative et bornée. Sa série de Dirichlet converge absolument pour $\Re(s) > 1$, et sa somme dans ce domaine est égale au produit infini convergent*

$$\prod_p \left(1 + f(p)p^{-s} + f(p^2)p^{-2s} + \ldots\right) \tag{2.1}$$

Si f est complètement multiplicative, alors sa série de Dirichlet est égale à

$$\prod_p \frac{1}{1 - f(p)p^{-s}} \tag{2.2}$$

Dans le cas complètement multiplicatif, le produit $\prod_p (1 - f(p)p^{-s})^{-1}$ s'appelle produit eulérien associé à f.

Démonstration

Comme f est bornée, la convergence absolue de la série pour $\Re(s) > 1$ est évidente.

(2.1) La méthode consiste à considérer le produit $P_k(s)$ des k premiers facteurs puis à montrer que $P_k(s)$ tend vers la série de Dirichlet de f lorsque k tend vers l'infini. Soient $p_1, \ldots, p_k$ les k premiers nombres premiers. On définit $P_k(s)$ comme suit

$$P_k(s) = \prod_{i=1}^{k} \left(1 + f(p_i)p^{-s} + f(p_i^2)p_i^{-2s} + \ldots\right)$$

Le terme général du développement de $P_k(s)$ est $\dfrac{f(p_1^{e_1}) \ldots f(p_k^{e_k})}{(p_1^{e_1} \ldots p_k^{e_k})^s} = \dfrac{f(p_1^{e_1} \ldots p_k^{e_k})}{(p_1^{e_1} \ldots p_k^{e_k})^s}$, car f est multiplicative. D'après le théorème fondamental de l'arithmétique, chaque k-uplet $(e_1, \ldots, e_k)$ détermine un unique n, donc

$$P_k(s) = \sum_{n \in A_k} f(n)n^{-s}$$

où $A_k = \{n \in \mathbb{N},\ n = p_1^{e_1} \ldots p_k^{e_k},\ e_i \geq 0\}$ est l'ensemble des entiers dont les facteurs premiers sont parmi les p_i. Si $n \notin A_k$, alors il est divisible par un nombre premier $p > p_k$, et donc $n > p_k$. On a donc

$$\left| P_k(s) - \sum_{n=1}^{\infty} f(n)n^{-s} \right| = \left| \sum_{n \notin A_k} f(n)n^{-s} \right| \leq \sum_{n \notin A_k} |f(n)n^{-s}| \leq \sum_{n > p_k} |f(n)n^{-s}|$$

Comme $\displaystyle\sum_{n=1}^{\infty} |f(n)n^{-s}|$ converge, on a $\displaystyle\lim_{k\to\infty} \sum_{n>p_k} |f(n)n^{-s}| = 0$. Donc

$$\lim_{k\to\infty} \left| P_k(s) - \sum_{n=1}^{\infty} f(n)n^{-s} \right| = 0$$

d'où le résultat.

(2.2) Si f est complètement multiplicative, alors $f(p^e) = f(p)^e$ pour chaque puissance de nombre premier. L'équation (2.1) donne alors

$$\begin{aligned} \sum_{n=1}^{\infty} f(n)n^{-s} &= \prod_{p} \left(1 + f(p)p^{-s} + f(p^2)p^{-2s} + \ldots\right) \\ &= \prod_{p} \left(1 + f(p)p^{-s} + f(p)^2p^{-2s} + \ldots\right) \\ &= \prod_{p} \left(\frac{1}{1 - f(p)p^{-s}}\right) \end{aligned}$$

□

On va maintenant montrer une condition suffisante pour que la série converge pour $\Re(s) > 0$. On commence par montrer un lemme préliminaire.

Lemme 2.1 (Abel) *Soient $(a_n)_{n\in\mathbb{N}}$ et $(b_n)_{n\in\mathbb{N}}$ deux suites. On pose*

$$A_{m,p} = \sum_{n=m}^{p} a_n \qquad\qquad S_{m,m'} = \sum_{n=m}^{m'} a_n b_n$$

On a alors

$$S_{m,m'} = \sum_{n=m}^{m'-1} A_{m,n}(b_n - b_{n+1}) + A_{m,m'}b_{m'}$$

Démonstration

On remarque tout d'abord que

$$a_n = \sum_{i=m}^{n} a_i - \sum_{i=m}^{n-1} a_i = A_{m,n} - A_{m,n-1}$$

On a alors

$$\begin{aligned} S_{m,m'} &= \sum_{n=m}^{m'} (A_{m,n} - A_{m,n-1})b_n \\ &= \sum_{n=m}^{m'} A_{m,n}b_n - \sum_{n=m+1}^{m'} A_{m,n-1}b_n \\ &= \sum_{n=m}^{m'} A_{m,n}b_n - \sum_{n=m}^{m'-1} A_{m,n}b_{n+1} \\ &= \sum_{n=m}^{m'-1} A_{m,n}(b_n - b_{n+1}) + A_{m,m'}b_{m'} \end{aligned}$$

□

Proposition 2.2 *Si les sommes partielles* $A_{m,p} = \sum_{n=m}^{p} f(n)$ *sont bornées, la série de Dirichlet de* f *converge pour* $\Re(s) > 0$.

Démonstration

On suppose que les sommes $A_{m,p}$ sont majorées par une constante K. L'application du lemme d'Abel donne

$$|S_{m,m'}| \leq K \left(\sum_{n=m}^{m'-1} \left| \frac{1}{n^s} - \frac{1}{(n+1)^s} \right| + \left| \frac{1}{m'^s} \right| \right)$$

□

2.2 Séries de Dirichlet à coefficients positifs

Proposition 2.3 *Soit* $f(s) = \sum a_n n^{-s}$ *une série de Dirichlet dont les coefficients* a_n *sont réels positifs. Si* f *converge pour* $\Re(s) > r$, $r \in \mathbb{R}$, *et si* f *peut être prolongée analytiquement en une fonction holomorphe au voisinage de* $s = r$, *alors il existe* $\varepsilon \in \mathbb{R}^*$ *tel que* f *converge pour* $\Re(s) > r - \varepsilon$.

Démonstration

On peut supposer que $r = 0$, le résultat général s'en déduisant par une translation.

Comme f est holomorphe pour $\Re(s) > 0$ et dans un voisinage de 0, elle est holomorphe, par exemple, sur le disque de centre 1 et de rayon $1 + \varepsilon$, c'est-à-dire pour tous les s tels que $|s - 1| \leq 1 + \varepsilon$. f est donc égale à la somme de sa série de Taylor dans ce disque. La dérivée p-ième de f est donnée par la formule

$$f^{(p)}(s) = \sum_{n=0}^{\infty} a_n (-\ln n)^p n^{-s}$$

D'où

$$f^{(p)}(1) = (-1)^p \sum_{n=0}^{\infty} a_n (\ln n)^p n^{-1}$$

La série de Taylor de f au voisinage de 1 est donc, pour tout s tel que $|s - 1| \leq 1 + \varepsilon$,

$$f(s) = \sum_{p=0}^{\infty} \frac{1}{p\,!} (z - 1)^p f^{(p)}(1)$$

En particulier pour $s = -\varepsilon$, on a

$$f(-\varepsilon) = \sum_{p=0}^{\infty} \frac{1}{p\,!} (1 + \varepsilon)^p (-1)^p f^{(p)}(1)$$

La série $(-1)^p f^{(p)}(1) = \sum a_n (\ln n)^p n^{-1}$ est convergente et ses termes sont positifs. La série suivante à termes positifs est donc convergente

$$f(-\varepsilon) = \sum_{p=0}^{\infty} \sum_{n=0}^{\infty} a_n \frac{1}{p\,!} (1 + \varepsilon)^p (\ln n)^p n^{-1}$$

En regroupant les termes différemment, on obtient

$$\begin{aligned} f(-\varepsilon) &= \sum_{n=0}^{\infty} a_n n^{-1} \sum_{p=0}^{\infty} \frac{1}{p\,!} (1 + \varepsilon)^p (\ln n)^p \\ &= \sum_{n=0}^{\infty} a_n n^{-1} e^{(1+\varepsilon) \ln n} \\ &= \sum_{n=0}^{\infty} a_n n^{-1} n^{(1+\varepsilon)} \\ &= \sum_{n=0}^{\infty} a_n n^{\varepsilon} \end{aligned}$$

La série de Dirichlet donnée converge donc pour $s = -\varepsilon$, donc aussi pour tout s tel que $\Re(s) > -\varepsilon$.

□

3 Fonction ζ et densité de Dirichlet

Dans cette partie, s est un réel strictement supérieur à 1.

La fonction ζ est définie par

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

Au XVIII$^{\text{ème}}$ siècle, Euler découvre la formule fondamentale suivante qui relie cette somme étendue à tous les entiers à un produit infini portant sur tous les nombres premiers.

Proposition 3.1

$$\zeta(s) = \prod_{p} \frac{1}{1 - p^{-s}}$$

Démonstration C'est en fait une application de la proposition 2.1 à la fonction constante 1, évidemment bornée et complètement multiplicative. □

3.1 Etude de ζ lorsque s tend vers 1

Proposition 3.2

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

Démonstration

Pour un s fixé, t^{-s} est une fonction décroissante de t. On a donc

$$(n+1)^{-s} < \int_n^{n+1} t^{-s}\, dt < n^{-s}$$

Si on somme sur n de 1 à l'infini, on obtient

$$\zeta(s) - 1 < \int_1^{\infty} t^{-s}\, dt < \zeta(s)$$

Or

$$\int_1^{\infty} t^{-s}\, dt = \frac{1}{s-1}$$

On a donc d'une part

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

et d'autre part

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

d'où l'on déduit

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

Il suffit maintenant de prendre la limite de chaque terme lorsque s tend vers 1, et on obtient

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

□

Corollaire

$$\lim_{s\to 1} \frac{\ln \zeta(s)}{\ln(s-1)^{-1}} = 1$$

Démonstration

On pose $(s-1)\zeta(s) = \rho(s)$. En passant au logarithme, on obtient $\ln(s-1) + \ln \zeta(s) = \ln \rho(s)$. Si on divise les deux membres de cette égalité par $\ln(s-1)^{-1}$, on a alors

$$\frac{\ln \zeta(s)}{\ln(s-1)^{-1}} = 1 + \frac{\ln \rho(s)}{\ln(s-1)^{-1}}$$

D'après la proposition 3.2, $\rho(s) \to 1$ lorsque s tend vers 1, donc $\ln \rho(s) \to 0$, et on obtient le résultat.

□

Proposition 3.3 $\ln \zeta(s) = \sum_p p^{-s} + R(s)$ *avec* $R(s)$ *bornée.*

Démonstration

On utilise le développement limité suivant au voisinage de 1

$$-\ln(1-x) = \sum_{k=1}^{\infty} \frac{x^k}{k}$$

On a alors

$$\begin{aligned} \ln \zeta(s) &= \sum_p \ln(1-p^{-s})^{-1} \\ &= \sum_p \sum_{k=1}^{\infty} \frac{p^{-ks}}{k} \\ &= \sum_p p^{-s} + \sum_p \sum_{k=2}^{\infty} \frac{p^{-ks}}{k} \end{aligned}$$

On majore la seconde somme comme suit :

$$\begin{aligned} \sum_p \sum_{k=2}^{\infty} \frac{p^{-ks}}{k} &\leq \frac{1}{2} \sum_p \sum_{k=2}^{\infty} p^{-ks} \qquad (*) \\ &= \frac{1}{2} \sum_p \frac{p^{-2s}}{1-p^{-s}} \\ &\leq \frac{1}{2(1-2^{-s})} \sum_p p^{-2s} \qquad (*) \\ &\leq \frac{1}{2(1-2^{-1})} \sum_p p^{-2} \qquad (**) \\ &\leq \zeta(2) \end{aligned}$$

Les majorations $(*)$ proviennent de l'inégalité suivante, où la série des a_n est convergente et celle des b_n strictement croissante, avec $\forall n \in \mathbb{N}$, $a_n \geq 0$ et $b_n > 0$.

$$\sum_{n=0}^{\infty} \frac{a_n}{b_n} \leq \frac{1}{b_0} \sum_{n=0}^{\infty} a_n$$

La majoration $(**)$ provient du fait que $s > 1$, car $\forall x > 0$, $x^{-s} \leq x^{-1}$.

□

Corollaire

$$\lim_{s \to 1} \frac{\sum_p p^{-s}}{\ln(s-1)^{-1}} = 1$$

Démonstration

Cela découle directement de la proposition 3.3 et du corollaire à la proposition 3.2.

□

3.2 Densité de Dirichlet

Définition 3.1 *On dit qu'une partie $\mathcal{P}$ de l'ensemble des nombres premiers a la densité de Dirichlet δ si*

$$\lim_{s \to 1} \frac{\sum_{p \in \mathcal{P}} p^{-s}}{\ln(s-1)^{-1}} = \delta$$

On voit que $\delta \in [0, 1]$. Si $\mathcal{P}$ est de cardinalité finie, sa densité est nulle. D'autre part, la corollaire à la proposition 3.3 nous montre que la densité de Dirichlet de l'ensemble des nombres premiers est égale à 1. A l'aide de cette notion, on peut énoncer le théorème de progression arithmétique de manière plus précise.

Théorème 3.1 *Soient $a, m \in \mathbb{N}^*$, premiers entre eux. Soit $\mathcal{P}_a$ l'ensemble des nombres premiers p tels que $p \equiv a \pmod{m}$. L'ensemble $\mathcal{P}_a$ a une densité de Dirichlet égale à $1/\varphi(m)$.*

4 Fonctions L de Dirichlet

Dans cette partie, $s \in \mathbb{C}$.

Soient $m \in \mathbb{N}^*$ et un caractère χ modulo m. On définit la fonction L de Dirichlet associée à χ par :

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

Comme $|\chi(n)n^{-s}| \leq n^{-\Re(s)}$, on voit que les termes de $L(s,\chi)$ sont dominés en valeur absolue par les termes correspondants de $\zeta(\Re(s))$. Donc $L(s,\chi)$ converge pour $\Re(s) > 1$.

4.1 Produit eulérien de L

Proposition 4.1 *Pour $\chi = \chi_0$, on a*

$$L(s,\chi_0) = \prod_{p|m}(1-p^{-s})\zeta(s)$$

En particulier, $L(s,\chi_0)$ est prolongeable analytiquement pour $\Re(s) > 0$ et admet $s = 1$ comme pôle simple.

Démonstration

$$\begin{aligned} L(s,\chi_0) &= \prod_{p\nmid m}(1-p^{-s})^{-1} \\ &= \prod_{p|m}(1-p^{-s})\prod_{p}(1-p^{-s})^{-1} \\ &= \prod_{p|m}(1-p^{-s})\zeta(s) \end{aligned}$$

□

Proposition 4.2 *Pour $\chi \neq \chi_0$, $L(s,\chi)$ converge dans le domaine $\Re(s) > 0$ et on a*

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

Démonstration

Pour prouver la convergence pour $\Re(s) > 0$, d'après la proposition 2.2, il suffit de vérifier que les sommes

$$A_{u,v} = \sum_{n=u}^{v} \chi(n) \qquad\qquad u \leq v$$

sont bornées. D'après les relations d'orthogonalité des caractères modulaires (proposition 1.5), on a

$$\sum_{n=u}^{u+m-1} \chi(n) = 0$$

car $\chi \neq \chi_0$. Il suffit donc de majorer les sommes $A_{u,v}$ lorsqu'elles comportent moins de m termes, c'est-à-dire $v-u < m-1$. Or dans ce cas, $A_{u,v}$ contient au plus $\varphi(m)$ termes non nuls, par définition du caractère modulaire χ, et chacun de ces termes est majoré par 1 en valeur absolue, on a donc

$$|A_{u,v}| \leq \varphi(m)$$

et la convergence est montrée.

Pour montrer la décomposition en produit, on applique la proposition 2.1. Il suffit de vérifier que tout caractère χ est borné et complètement multiplicatif.

$|\chi(a)| \leq 1 \ \forall a \in \mathbb{N}^*$, donc χ est borné. D'autre part, si on note $\tilde{\chi}$ le caractère de $\left(\mathbb{Z}/m\mathbb{Z}\right)^*$ auquel est associé χ, pour tous $a, b \in \mathbb{N}^*$ premiers avec m on a

$$\chi(ab) = \tilde{\chi}(\overline{ab}) = \tilde{\chi}(\bar{a}\bar{b}) = \tilde{\chi}(\bar{a})\tilde{\chi}(\bar{b}) = \chi(a)\chi(b)$$

Si, par contre, a n'est pas premier avec m, le produit ab n'est pas non plus premier avec m, on a donc

$$\chi(ab) = 0 = \chi(a)\chi(b)$$

Donc χ est complètement multiplicatif.

□

4.2 $L(1,\chi) \neq 0$

La propriété des fonctions L qui joue un rôle décisif dans la preuve du théorème de progression arithmétique est la non-nullité de $L(1,\chi)$. C'est ce point que l'on va étudier maintenant, en énonçant tout d'abord un lemme préliminaire.

Soient $m \in \mathbb{N}^*$, p premier. Si $\bar{p} \in \left(\mathbb{Z}/m\mathbb{Z}\right)^*$, c'est-à-dire si p ne divise pas m, on pose $g(p) = \varphi(m)/n$ où n désigne l'ordre de p dans $\left(\mathbb{Z}/m\mathbb{Z}\right)^*$.

Lemme 4.1 *On a l'identité*

$$(1-T^n)^{g(p)} = \prod_{\chi}(1-\chi(p)T)$$

le produit étant étendu à tous les caractères χ de $\left(\mathbb{Z}/m\mathbb{Z}\right)^*$.

Démonstration

(i) Soit $\mathbb{U}_n$ l'ensemble des racines n-ièmes de l'unité de $\mathbb{C}$. On a $|\mathbb{U}_n| = n$, où $|\,.\,|$ note le cardinal. On commence par démontrer que

$$1 - T^n = \prod_{z \in \mathbb{U}_n} (1 - zT)$$

Pour tout $z \in \mathbb{U}_n$, $\left(\frac{1}{z}\right)^n = \frac{1}{z^n} = 1$, donc $\frac{1}{z}$ est racine de $1 - T^n$. On a alors

$$\begin{aligned} 1 - T^n &= -\prod_{z \in \mathbb{U}_n} \left(T - \frac{1}{z}\right) \\ &= -\prod_{z} \left(\frac{zT - 1}{z}\right) \\ &= -\frac{\prod_z (zT - 1)}{\prod_z z} \\ &= -(-1)^n \frac{\prod_z (1 - zT)}{\prod_z z} \\ &= \frac{(-1)^{n+1}}{\prod_z z} \prod_z (1 - zT) \end{aligned}$$

Le produit des éléments de $\mathbb{U}_n$ dépend de la parité de n. On sait que pour tout $z \in \mathbb{U}_n$, il existe $0 \leq k < n$ tel que $z = e^{2ik\pi/n}$. D'où

$$\begin{aligned} \prod_{z \in \mathbb{U}_n} z &= \prod_{k=0}^{n-1} e^{2ik\pi/n} \\ &= \exp\left(\frac{2i\pi}{n} \sum_{k=0}^{n-1} k\right) \\ &= \exp\left(\frac{2i\pi}{n} \frac{(n-1)n}{2}\right) \\ &= e^{(n-1)i\pi} \end{aligned}$$

Donc si n est pair, $\prod_z z = -1$, et si n est impair, $\prod_z z = 1$, d'où $\frac{(-1)^{n+1}}{\prod z} = 1$.

On obtient donc

$$1 - T^n = \prod_{z \in \mathbb{U}_n} (1 - zT)$$

(ii) D'autre part, on montre que pour tout $z \in \mathbb{U}_n$, il existe $g(p)$ caractères χ de $\left(\mathbb{Z}/m\mathbb{Z}\right)^* = \mathrm{G}_m$ tels que $\chi(p) = z$.

On considère le morphisme suivant

$$\begin{aligned} \psi \quad : \quad & \widehat{\mathrm{G}}_m \to \mathbb{U}_n \\ & \chi \ \mapsto \chi(p) \end{aligned}$$

On a $\mathrm{Ker}(\psi) = \{\chi \in \widehat{\mathrm{G}}_m, \chi(p) = 1\}$. De plus, on sait que

$$|\mathrm{Ker}(\psi)||\mathrm{Im}(\psi)| = |\widehat{\mathrm{G}}_m| = \varphi(m)$$

Or ψ est surjectif par construction, donc $|\mathrm{Im}(\psi)| = |\mathbb{U}_n| = n$, d'où

$$|\mathrm{Ker}(\psi)| = \frac{\varphi(m)}{n} = g(p)$$

Donc pour tout $z \in \mathbb{U}_n$, il existe $g(p)$ caractères χ de G_m tels que $\chi(p) = z$.

On déduit donc des deux points que l'on vient de démontrer

$$\begin{aligned}
(1 - T^n)^{g(p)} &= \left(\prod_{z \in \mathbb{U}_n} (1 - zT) \right)^{g(p)} && \text{d'après (i)} \\
&= \prod_{z \in \mathbb{U}_n} (1 - zT)^{g(p)} \\
&= \prod_{z \in \mathbb{U}_n} \prod_{\substack{\chi \text{ tq} \\ \chi(p) = z}} (1 - \chi(p)T) && \text{d'après (ii)} \\
&= \prod_{\chi} (1 - \chi(p)T)
\end{aligned}$$

□

On définit maintenant la fonction ζ_m comme suit : pour $s > 1$

$$\zeta_m(s) = \prod_{\chi} L(s, \chi)$$

où le produit est étendu à tous les caractères χ de $\left(\mathbb{Z}/m\mathbb{Z}\right)^*$.

Proposition 4.3

$$\zeta_m(s) = \prod_{p \nmid m} \frac{1}{(1 - p^{-ns})^{g(p)}}$$

C'est une série de Dirichlet à coefficients entiers positifs et convergente pour $\Re(s) > 1$.

Démonstration

On utilise le produit eulérien de L et le lemme 4.1 où $T = p^{-s}$.

$$\begin{aligned}
\zeta_m(s) &= \prod_{\chi} L(s, \chi) \\
&= \prod_{\chi} \prod_{p \nmid m} \frac{1}{1 - \chi(p)p^{-s}} \\
&= \prod_{p \nmid m} \prod_{\chi} \frac{1}{1 - \chi(p)p^{-s}} \\
&= \prod_{p \nmid m} (1 - p^{-ns})^{-g(p)}
\end{aligned}$$

La convergence se déduit des propositions 4.1 et 4.2.

□

Théorème 4.1 *$L(1,\chi) \neq 0$ pour tout $\chi \neq \chi_0$.*

Démonstration

Par l'absurde, on suppose qu'il existe un caractère $\chi \neq \chi_0$ tel que $L(1,\chi) = 0$. Alors $\zeta_m(1) = 0$ et ζ_m est holomorphe en $s = 1$. D'après les propositions 4.1 et 4.2, ζ_m est alors holomorphe pour tout s tel que $\Re(s) > 0$. Puis d'après la proposition 2.3, comme ζ_m est une série de Dirichlet à coefficients positifs, elle converge pour tout s tel que $\Re(s) > 0$.

Or chaque terme du produit peut être minoré de la façon suivante

$$\begin{aligned} \frac{1}{(1-p^{-ns})^{g(p)}} &= \left(1 + p^{-ns} + p^{-2ns} + \ldots\right)^{g(p)} \\ &\geq \left(1 + p^{-\varphi(m)s} + p^{-2\varphi(m)s} + \ldots\right) \\ &\geq p^{-\varphi(m)s} \end{aligned}$$

□

5 Démonstration du théorème 3.1

Pour démontrer le théorème 3.1, on a besoin d'étudier le comportement de la fonction

$$g_a(s) = \sum_{p \in \mathcal{P}_a} p^{-s}$$

lorsque s tend vers 1, $s \in \mathbb{R}$.

Soit χ un caractère de $\left(\mathbb{Z}/m\mathbb{Z}\right)^*$, on pose

$$f_\chi(s) = \sum_{p \nmid m} \chi(p) p^{-s}$$

Lemme 5.1 *On a*

$$g_a(s) = \frac{1}{\varphi(m)} \sum_{\chi} \overline{\chi(a)} f_\chi(s)$$

où la somme est étendue à tous les caractères χ de $\left(\mathbb{Z}/m\mathbb{Z}\right)^*$.

Démonstration

On a

$$\sum_{\chi} \overline{\chi(a)} f_\chi(s) = \sum_{p \nmid m} \sum_{\chi} \overline{\chi(a)} \chi(p) p^{-s}$$

D'après la proposition 1.5, on a

$$\begin{aligned} \sum_{\chi} \overline{\chi(a)} \chi(p) &= \varphi(m) && \text{si } a \equiv p \pmod{m} \Leftrightarrow p \in \mathcal{P}_a \\ &= 0 && \text{sinon} \end{aligned}$$

Donc

$$\begin{aligned} \sum_{p \nmid m} \sum_{\chi} \overline{\chi(a)} \chi(p) p^{-s} &= \sum_{p \in \mathcal{P}_a} \varphi(m) p^{-s} \\ &= \varphi(m) g_a(s) \end{aligned}$$

d'où le résultat.

□

On étudie maintenant le comportement de la fonction f_χ lorsque s tend vers 1.

Lemme 5.2

$$\lim_{s \to 1} \frac{f_{\chi_0}(s)}{\ln(s-1)^{-1}} = 1$$

Démonstration

D'après le corollaire à la proposition 3.3

$$\lim_{s\to 1} \frac{\sum_p p^{-s}}{\ln(s-1)^{-1}} = 1$$

Or $f_{\chi_0}(s)$ ne diffère de $\sum_p p^{-s}$ que par les diviseurs premiers de m, qui sont en nombre fini. Les deux fonctions ont donc le même comportement à la limite, d'où

$$\lim_{s\to 1} \frac{f_{\chi_0}(s)}{\ln(s-1)^{-1}} = 1$$

□

Lemme 5.3 *Si $\chi \neq \chi_0$, f_χ reste bornée lorsque s tend vers 1.*

Démonstration

On va avoir besoin d'utiliser le logarithme de la fonction $L(s,\chi)$. Même en considérant s réel, $L(s,\chi)$ est complexe, on doit donc définir ce qu'est le logarithme d'une fonction complexe.

On considère la définition de L sous forme de produit eulérien. Comme $|\chi(p)p^{-s}| < 1$, on a

$$\begin{aligned} \ln L(s,\chi) &= \sum_p \ln \frac{1}{1-\chi(p)p^{-s}} \\ &= \sum_p \sum_{n=1}^{\infty} \frac{\chi(p)^n}{np^{ns}} \end{aligned}$$

On peut décomposer $\ln L(s,\chi)$ de la façon suivante

$$\ln L(s,\chi) = \sum_p \frac{\chi(p)}{p^s} + \sum_p \sum_{n=2}^{\infty} \frac{\chi(p)}{np^{ns}}$$

D'une part, $\displaystyle\sum_p \frac{\chi(p)}{p^s} = f_\chi(s)$ car $\chi(p) = 0$ si p divise m. D'autre part, le deuxième terme de la somme est borné. En effet

$$\left| \sum_p \sum_{n=2}^{\infty} \frac{\chi(p)}{np^{ns}} \right| \leq \sum_p \sum_{n=2}^{\infty} \frac{1}{np^{ns}}$$

qui est borné d'après la proposition 3.3.

De plus, d'après le théorème 4.1, $\ln L(s,\chi)$ reste borné lorsque s tend vers 1. On a donc écrit $f_\chi(s)$ comme la différence de deux fonctions bornées, lorsque s tend vers 1, ce qui démontre le lemme.

□

On peut maintenant calculer la densité de l'ensemble $\mathcal{P}_a$. On a, d'après le lemme 5.1,

$$\begin{aligned}\lim_{s\to 1}\frac{g_a(s)}{\ln(s-1)^{-1}} &= \lim_{s\to 1}\frac{1}{\varphi(m)}\frac{\sum_\chi \overline{\chi(a)}f_\chi(s)}{\ln(s-1)^{-1}}\\ &= \frac{1}{\varphi(m)}\lim_{s\to 1}\left(\frac{f_{\chi_0}}{\ln(s-1)^{-1}}+\varepsilon(s)\right)\end{aligned}$$

D'après le lemme 5.2, le premier terme de la somme tend vers 1, et d'après le lemme 5.3, $\varepsilon(s)$ tend vers 0, car les $f_\chi(s)$ sont bornés si $\chi \neq \chi_0$. D'où

$$\lim_{s\to 1}\frac{g_a(s)}{\ln(s-1)^{-1}} = \frac{1}{\varphi(m)}$$

L'ensemble $\mathcal{P}_a$ est donc infini, le théorème est démontré.

6 Applications

Définition 6.1 *Soient $a, p \in \mathbb{Z}$ et soit l'équation*

$$x^2 \equiv a \pmod{p} \tag{6.1}$$

dont on cherche les solutions dans $\mathbb{Z}$. On appelle symbole de Legendre la notation $\left(\frac{a}{p}\right)$ dont on définit le sens de la manière suivante, si $\text{pgcd}(a,p) = 1$

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{si l'équation (6.1) admet une solution} \\ -1 & \text{sinon} \end{cases}$$

Si $\text{pgcd}(a,p) \neq 1$, *alors* $\left(\frac{a}{p}\right) = 0$.

On définit également la fonction $\varepsilon : \mathbb{Z} \to \{-1, 1\}$ par $\varepsilon(n) = \frac{n-1}{2} \pmod 2$.

6.1 Loi de réciprocité quadratique

Théorème 6.1 *Soient p et q deux nombres premiers distincts et différents de 2. On a*

$$\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right)(-1)^{\varepsilon(p)\varepsilon(q)}$$

C'est en 1785 que Legendre expose pour la première fois ce qui allait plus tard être appelé la loi de réciprocité quadratique. Pour justifier cette loi, il est amené à introduire au cours de son raisonnement des nombres premiers auxiliaires auxquels il impose la condition d'appartenir à certaines progressions arithmétiques nécessaires à sa démonstration. Il ne démontre pas l'existence de ces nombres premiers sur le moment, mais reconnaît qu'il serait nécessaire de s'y attarder. Plus tard, il tente une démonstration, qui se révèlera erronée quelques 50 ans plus tard.

En 1801, Gauss publie ses *Disquisitiones Arithmeticae*, dans lesquelles il expose les deux premières démonstrations de la loi de réciprocité quadratique, dont aucune n'utilise les nombres premiers qu'avait introduit Lengendre. Il n'est donc pas nécessaire d'utiliser le théorème de progression arithmétique pour prouver la loi de réciprocité quadratique, mais on peut penser qu'il est, historiquement parlant, intéressant de préciser que c'est au cours de cette démonstration que sont intervenus pour la première fois ces nombres premiers.

6.2 Solutions de $x^2 \equiv a \pmod{p}$, p premier

Proposition 6.1 *Soit a un entier non nul sans facteurs carrés et soit $m = 4|a|$. Il existe alors un unique caractère χ_a modulo m tel que $\chi_a(p) = \left(\frac{a}{p}\right)$ pour tout nombre premier p ne divisant pas m.*

Démonstration

On montre tout d'abord l'existence de χ_a. On suppose que $a = p_1 \dots p_k$ où les p_i sont des nombres premiers distincts et différents de 2. On définit χ_a de la manière suivante, pour tout $x \in \mathbb{Z}$

$$\chi_a(x) = (-1)^{\varepsilon(x)\varepsilon(a)} \left(\frac{x}{p_1}\right) \dots \left(\frac{x}{p_k}\right)$$

Si p est un nombre premier, premier avec m, c'est-à-dire un nombre premier distinct de 2 et des p_i, la loi de réciprocité quadratique donne

$$\begin{aligned}
\chi_a(p) &= (-1)^{\varepsilon(p)(\varepsilon(p_1)+\dots+\varepsilon(p_k))} \left(\frac{p}{p_1}\right) \dots \left(\frac{p}{p_k}\right) \\
&= (-1)^{\varepsilon(p)\varepsilon(p_1)} \left(\frac{p}{p_1}\right) \dots (-1)^{\varepsilon(p)\varepsilon(p_k)} \left(\frac{p}{p_k}\right) \\
&= \left(\frac{p_1}{p}\right) \dots \left(\frac{p_k}{p}\right) \\
&= \left(\frac{p_1 \dots p_k}{p}\right) \\
&= \left(\frac{a}{p}\right)
\end{aligned}$$

L'existence de χ_a est donc prouvée pour a impair.

Si a s'écrit $-b$, $2b$ ou $-2b$, avec b sans facteurs carrés et impair, alors on prend χ_a égal au produit de χ_b et de, respectivement, $(-1)^{\varepsilon(x)}$, $(-1)^{\omega(x)}$, ou $(-1)^{\varepsilon(x)+\omega(x)}$.

□

Proposition 6.2 *Soit $a \in \mathbb{Z}$ tel que a ne soit pas un carré. L'ensemble des nombres premiers p tels que $\left(\frac{a}{p}\right) = 1$ a pour densité $1/2$.*

Démonstration

On peut supposer a sans facteurs carrés. Soit $m = 4|a|$ et soit χ_a le caractère modulo m défini dans la proposition précédente. Soit H le noyau de χ_a dans $\left(\mathbb{Z}/m\mathbb{Z}\right)^*$. Soit p un nombre premier ne divisant pas m, et $\bar{p}$ son image dans $\left(\mathbb{Z}/m\mathbb{Z}\right)^*$. On a $\left(\frac{a}{p}\right) = 1$ si et seulement si $\bar{p} \in$ H.

□

Corollaire *Soit $a \in \mathbb{Z}$. Si l'équation* (6.1) *admet une solution pour presque tout p premier, elle admet une solution dans $\mathbb{Z}$.*

6.3 Existence de nombres rationnels de symboles de Hilbert donnés

Définition 6.2 *Soit $\mathbb{K}$ un corps, égal à $\mathbb{R}$ ou à un $\mathbb{Q}_p$, corps de nombres p-adiques, avec p premier. Soient $a, b \in \mathbb{K}^*$ et soit l'équation*

$$ax^2 + by^2 = z^2 \tag{6.2}$$

dont on cherche les solutions dans $\mathbb{K}^3$. On appelle symbole de Hilbert la notation (a, b) dont on définit le sens de la manière suivante

$$(a,b) = \begin{cases} 1 & \text{si l'équation (6.2) admet une solution} \\ -1 & \text{sinon} \end{cases}$$

Le corps $\mathbb{Q}$ se plonge comme sous-corps dense dans chacun des corps $\mathbb{Q}_p$ et $\mathbb{R}$. Si $a, b \in \mathbb{Q}^*$, on note $(a, b)_p$ (resp. $(a, b)_\infty$) le symbole de Hilbert de leurs images dans $\mathbb{Q}_p$ (resp. $\mathbb{R}$). On désigne par V la réunion de l'ensemble des nombres premiers et de l'infini, et on fait la convention $\mathbb{Q}_\infty = \mathbb{R}$.

Théorème 6.2 *Soit $(a_i)_{i\in I}$ une famille finie d'éléments de $\mathbb{Q}^*$. Soit $(\varepsilon_{i,v})_{i\in I, v\in V}$ une famille finie de nombres égaux à ± 1. Il existe $x \in \mathbb{Q}^*$ tel que $(a_i, x) = \varepsilon_{i,v}$ pour tout $i \in I$ et pour tout $v \in V$ si et seulement si*

(i) *presque tous les $\varepsilon_{i,v}$ sont égaux à 1*

(ii) *pour tout $i \in I$, $\prod_{v\in V} \varepsilon_{i,v} = 1$*

(iii) *pour tout $v \in V$, il existe $x_v \in \mathbb{Q}_v^*$ tel que $(a_i, x_v)_v = \varepsilon_{i,v}$, pour tout $i \in I$*

6.4 Théorème de Minkowski-Hasse

Définition 6.3 *On appelle forme quadratique de rang n sur un corps $\mathbb{K}$ toute application $f : \mathbb{K}^n \to \mathbb{K}$ telle que*

- *pour tout $\lambda \in \mathbb{K}$, pour tout $x \in \mathbb{K}^n$, $f(\lambda x) = \lambda^2 f(x)$*
- *$\phi : (x, y) \mapsto \frac{1}{2}(f(x + y) - f(x) - f(y))$ définie sur $\mathbb{K}^n \times \mathbb{K}^n$ est une forme bilinéaire sur $\mathbb{K}$.*

On dit que ϕ est la forme bilinéaire associée à f. De plus ϕ est symétrique et $\phi(x, x) = f(x)$. Inversement, toute forme bilinéaire symétrique ψ sur $\mathbb{K}^n \times \mathbb{K}^n$ définit une forme quadratique $x \mapsto \psi(x, x)$ sur $\mathbb{K}$ à laquelle elle est associée.

Définition 6.4 *On dit qu'une forme quadratique f définie sur $\mathbb{K}^n$ représente $a \in \mathbb{K}^*$ sur $\mathbb{K}$ s'il existe $x \in \mathbb{K}^n$ tel que $f(x) = a$. Comme par définition, $f(0) = 0$ quelque soit la forme quadratique f, on dit que f représente 0 sur $\mathbb{K}$ s'il existe au moins un $x \in \mathbb{K}$ non nul tel que $f(x) = 0$.*

Le théorème de la progression arithmétique permet de montrer le théorème suivant.

Théorème 6.3 *Une forme quadratique rationnelle représente* 0 *sur* $\mathbb{Q}$ *si et seulement si elle représente* 0 *sur tous les corps* $\mathbb{Q}_p$ *et sur* $\mathbb{R}$.

Corollaire *Une forme quadratique rationnelle représente* $a \in \mathbb{Q}^*$ *sur* $\mathbb{Q}$ *si et seulement si elle représente* a *sur tous les corps* $\mathbb{Q}_p$ *et sur* $\mathbb{R}$.

Ce résultat permet de décider si, lorsque la forme quadratique f sur $\mathbb{Q}$ de rang n et $a \in \mathbb{Q}^*$ sont donnés, l'équation $f(x) = a$ admet ou non des solutions dans $\mathbb{Q}^n$. Lorsque les coefficients de f sont dans $\mathbb{Z}$ ainsi que a, il est intéressant de savoir si cette équation admet ou non des solutions dans $\mathbb{Z}^n$. D'autres théorèmes, s'appuyant sur les deux résultats précédents, mais avec des hypothèses plus restreintes, permettent de décider de l'existence dans $\mathbb{Z}^n$ de solutions à l'équation $f(x) = a$.

7 Recherche de nombres premiers consécutifs en progression arithmétique

Voici des extraits de l'annonce officielle de la découverte de 10 nombres premiers consécutifs en progression arithmétique.

---

7 Mars 1998

Harvey Dubner, Tony Forbes, Nik Lygeros, Michel Mizony et Paul Zimmermann.

En Novembre 1997, alors que nous venions juste de découvrir 8 nombres premiers consécutifs en progression arithmétique, nous avons commencé à chercher une suite de 9 nombres, aidés par une centaine de personnes travaillant sur toutes sortes de PC et autres postes de travail. Le 15 Janvier 1998, un de nos assistants découvrit 9 nombres premiers consécutifs en progression arithmétique. Dans le même temps, nous initialisions la recherche d'une suite de 10 nombres. Comme pour 9, nous cherchions des nombres de la forme

$$Nm + x + 210b \qquad b = 0, 1, \ldots, 9$$

où $m = 2 \times 3 \times 5 \times 7 \times \ldots \times 193$ le produit des 44 premiers nombres premiers, $x = 54$ 53824 16838 87582 66818 97035 90110 65905 78659 34764 60487 38407 81923 51342 11034 95579 et $N = 0, 1, 2 \ldots$ Le nombre à 77 chiffres x a été choisi pour faire en sorte :

- que les 10 nombres $Nm + x + 210b$, $b = 0, 1, \ldots, 9$, ne soient pas divisibles par les nombres premiers 2,3,5,7,...,193
- autant que possible que les 9×209 nombres intermédiaires ne soient pas premiers.

Le 2 Mars 1998, nous découvrions une suite de 10 nombres premiers consécutifs en progression arithmétique. La valeur de N trouvée par ordinateur est 507 618 446 770 482, ce qui correspond aux 10 premiers consécutifs

$$P, P + 210, P + 420, P + 630, P + 840, P + 1050, P + 1260, P + 1470, P + 1680, P + 1890$$

où $P = 507618446770482m + x$, le premier terme de la suite étant le nombre à 93 chiffres 100 99697 24697 14247 63778 66555 87969 84032 95093 24689 19004 18036 03417 75890 43417 03348 88215 90672 29619.

Même si on nous a souvent fait remarquer que $10 + 1 = 11$, nous croyons que la recherche d'une progression arithmétique de 11 nombres premiers consécutifs est beaucoup trop difficile. L'écart minimum entre les entiers doit être 2310 au lieu de 210 et les nombres entrant en jeu pour une recherche optimale auraient des centaines de chiffres. Nous avons besoin d'une nouvelle idée, ou d'ordinateurs des milliards de fois plus puissants. Nous espérons donc que ce record durera longtemps.

Bibliographie

[1] J.P. Serre, *Cours d'Arithmétique*, PUF, 1970

[2] K. Ireland, M. Rosen, *A Classical Introduction to Modern Number Theory*, 2ème édition, Springer, 1990

[3] J.M. Arnaudiès, J. Bertin, *Groupes, Algèbres et Géométries*, tome 2, Ellipses, 1995

[4] R. Descombes, *Elements de Théorie des Nombres*, PUF, 1986

[5] M. Guinot, *Arithmétique pour amateurs*, Livre VI : *Un homme de caractère(s) : Dirichlet*, Aléas, 2000

[6] G.A. Jones, J.M. Jones, *Elementary Number Theory*, Springer, 1998