Autour du théorème de Brun-Titchmarsh

Joseph Basquin

Septembre 2005

Remerciements et historique du stage

Mes remerciements vont à Olivier Ramaré qui, déjà bien avant mon stage à Lille, m'a guidé dans la découverte de la théorie analytique des nombres — notamment par ses courriels toujours très éclairants.
Je tiens à le remercier ensuite pour avoir immédiatement accepté ma demande en vue d'effectuer mon stage de magistère sous sa direction. Les nombreuses discussions que nous avons pu échanger, et plus généralement la grande qualité de son encadrement, tout au long de mon séjour à Lille m'ont été des plus profitables. Enfin son aide pour la rédaction du présent mémoire m'a été très précieuse.

* * *

Le sujet proposé pour ce stage m'a séduit d'emblée, car il présentait l'avantage d'aborder différentes facettes de la théorie analytique des nombres, à savoir méthodes d'analyse complexe d'une part et méthodes élémentaires d'autre part.

Dans un premier temps, il m'a fallu asseoir un certain nombre de connaissances considérées comme classiques dans le domaine, que j'avais entrevues de nombreuses fois depuis plusieurs années dans mes lectures — mais jamais réellement couchées sur le papier, c'est désormais chose faite !

À ce titre, j'ai tenté par exemple de présenter les classiques *théorème des nombres premiers* et *théorème de la progression arithmétique* sous une forme un peu moins académique que celle que l'on trouve dans les ouvrages traditionnels, dans un but avant tout didactique, ce qui j'espère pourra aider le débutant.

J'ai pu ensuite approcher des techniques plus modernes comme les méthodes de crible et entrevoir où se situaient les problèmes actuels.

Ce travail aura été passionnant par son contenu mathématique bien sûr, mais aussi par le contact avec le monde de la recherche qu'il m'a offert.

Notations et préliminaires

Le pgcd (resp. le ppcm) de deux entiers a et b est noté (a,b) (resp. $[a,b]$). La lettre p, en tant qu'entier, désigne toujours un nombre premier. Étant donné un ensemble $\mathcal{A}$, $|\mathcal{A}|$ désigne son cardinal, et $\mathbf{1}_{\mathcal{A}}$ sa fonction caractéristique.

On désigne conformément à l'usage par $\pi(x)$ le nombre de nombres premiers inférieurs à x. Le logarithme népérien est noté log. Les itérés $\log\log$, $\log\log\log$, etc. sont notés $\log_2$, $\log_3$, etc. La partie entière d'un nombre réel x est notée $[x]$, sa partie fractionnaire $\{x\}$. Étant données des fonctions f, g, nous utilisons les notations usuelles $f \sim g$, $f = o(g)$, et indifféremment la notation de Landau $f = \mathcal{O}(g)$ et celle de Vinogradov $f \ll g$.
Les nombres complexes seront usuellement notés $s = \sigma + i\tau$.

On suppose connues les notions élémentaires sur les fonctions arithmétiques (fonctions $f : \mathbb{N} \to \mathbb{C}$), leur convolution, notée $*$.
On utilise les notations classiques pour les fonctions arithmétiques usuelles : μ désigne la fonction de Möbius, ϕ l'indicatrice d'Euler, $\mathbf{1}$ la fonction constante égale à 1, etc.
Lors de l'étude, en théorie analytique des nombres, des fonctions arithmétiques, apparaissent fréquemment les séries de Dirichlet qui leur sont associées (à f on associe $F(s) = \sum_{n\geq 1} \frac{f(n)}{n^s}$). Cela s'explique notamment par le lien étroit entre le produit de convolution et le produit des séries de Dirichlet :

$$\left(\sum_{n\geq 1} \frac{f(n)}{n^s}\right)\left(\sum_{n\geq 1} \frac{g(n)}{n^s}\right) = \sum_{n\geq 1} \frac{h(n)}{n^s},$$
$$\text{avec } h(n) = (f*g)(n) = \sum_{n_1 n_2 \leq n} f(n_1)g(n_2) \quad (1)$$

(pour s dans le domaine de convergence des trois séries).

On remarquera l'analogie avec le lien entre le produit de Cauchy de deux

suites et le produit des séries entières qui leurs sont associées :

$$\left(\sum_{n\geq 0} a_n z^n\right)\left(\sum_{n\geq 0} b_n z^n\right) = \sum_{n\geq 0} c_n z^n,$$
$$\text{avec } c_n = \sum_{n_1+n_2\leq n} f(n_1)g(n_2). \quad (2)$$

Pour les notions de bases relatives aux séries de Dirichlet, on pourra se référer à [Ten95]. On fera également usage de lemmes classiques d'analyse, tels que la sommation d'Abel, la formule de sommation d'Euler-Maclaurin, etc.

Introduction

Démontrés depuis plus d'un siècle, deux grands théorèmes de théorie analytique des nombres concernant les nombres premiers nous renseignent sur leur distribution : il s'agit du *théorème des nombres premiers*, dû indépendamment à de la Vallée Poussin et Hadamard en 1896, et plus de soixante ans auparavant du *théorème de la progression arithmétique* de Dirichlet, donnant l'existence d'une infinité de nombres premiers congrus à a modulo q (avec a premier à q).

Ce deuxième théorème s'est précisé en un "théorème des nombres premiers en progressions arithmétiques" qui donne une évaluation asymptotique du nombre de nombres premiers inférieurs à x dans les différentes classes modulo q, pour q fixé, et $x \to \infty$.
Si l'on souhaite faire tendre q vers l'infini en même temps que x, les problèmes actuels se situent au niveau de la dépendance entre q et x, et de l'*effectivité* de tels résultats : certains théorèmes font apparaître des constantes dans les termes d'erreurs, dont on ne sait qu'établir l'existence, sans pouvoir les calculer numériquement ! Cela limite grandement notre connaissance pratique sur la distribution des nombres premiers, et nécessite donc un traitement particulier.

D'autre part, se sont développées tout au long du XXème siècle, des méthodes dites de *crible* qui fournissent d'autres types de résultats, et notamment sur la répartition de nombres premiers dans les petits intervalles. A ce titre, on peut citer le théorème de Brun-Titchmarsh, dont nous démontrerons une version légèrement plus faible :

$$\sum_{\substack{M+1\leq p\leq M+N \\ p=a \pmod q}} 1 \leq 2\frac{N}{\phi(q)\log(N/q)} \tag{3}$$

La question de savoir si la constante 2 apparaissant ici est optimale n'est pas tranchée, toujours est-il qu'une amélioration — ne serait-ce que de remplacer 2 par $2-\xi$ pour $\xi > 0$ — aurait des répercutions importantes dans toute la théorie, répercutions auxquelles nous allons nous intéresser ici.

Plus précisément, on montrera qu'une telle amélioration entraîne une meilleure connaissance de la distribution des nombres premiers en progressions arithmétiques, au sens de l'effectivité du résultat mentionné ci-dessus.

Avant d'attaquer la preuve du résultat en question, nous détaillons quelque peu le paysage arithmétique classique.

Chapitre 1

Définitions et résultats élémentaires

Quand on s'intéresse à la distribution des nombres premiers, la lecture de tables numériques nous amène à conjecturer (ce qu'ont fait Gauss et Legendre notamment) qu'il y a un nombre premier tous les $[\log n]$ entiers (autour d'un entier de taille n), i.e. un entier de taille n est premier avec une "probabilité" $1/\log n$. Ainsi, entre 1 et x, on peut conjecturer qu'il y a environ $\sum_{n\geq 2} 1/\log n \sim \int_2^x \frac{dt}{\log t} \sim \frac{x}{\log x}$ nombres premiers.

Soit alors $\pi(x)$ le nombre de nombres premiers entre 1 et x.
La conjecture annoncée plus haut est en fait le

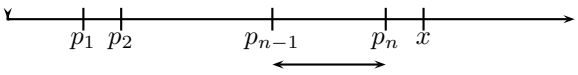
Théorème 1 (des nombres premiers) $\pi(x) \sim \frac{x}{\log x}$

Remarque. Sans aller jusqu'à avoir un tel équivalent, on peut avoir plus facilement que ledit théorème un encadrement $ax/\log x \leq \pi(x) \leq bx/\log x$, a et b constantes (voir les théorèmes dus à Tchebychev).

Si la fonction π est simple à définir, ce n'est pas nécessairement la *meilleure* fonction à étudier. En effet, travailler avec une fonction de croissance en $x/\log x$ n'est pas des plus maniables ! On introduira alors par la suite une fonction ψ qui contiendra la même information que π mais qui aura une croissance que l'on espère plus facile à repérer : on fera tout en définissant ψ pour avoir même une croissance linéaire $\psi(x) \sim x$.

En fait, on peut écrire $\pi(x) = \sum_{p\leq x} 1$, ce qui indique que l'on fait une somme sur tous les nombres premiers, et chaque fois que l'on en rencontre un, on lui associe un *poids* de 1 dans la somme. En mettant un autre poids, on peut arriver à une fonction plus adaptée à ce que l'on souhaite. Nous avions

conjecturé initialement que l'on rencontrait un nombre premier tous les $[\log n]$ entiers. Associons donc le poids $\log p$ à chaque nombre premier p.
Ce poids symbolise moralement la distance de p par rapport au nombre premier précédent. Ainsi, si l'on note (p_n) la suite croissante des nombres premiers, $\log p_n$ doit valoir environ $p_n - p_{n-1}$. Si nos prédictions probabilistes sont exactes, on peut espérer $\sum_{p_n \leq x} \log p_n \approx \sum_{p_n \leq x} p_n - p_{n-1} \approx x$.



Pour une simple raison technique, on regardera non seulement les nombres premiers mais aussi les puissances de nombres premiers (cela ne change en réalité pas grand chose !) et l'on introduit la fonction de von Mangoldt :

$$\Lambda(n) \;=\; \begin{cases} \log p \text{ si } n = p^\nu \\ 0 \text{ sinon} \end{cases}$$

On définit alors la fonction $\psi(x) = \sum_{n \leq x} \Lambda(n)$. Il est équivalent et plus simple ici de travailler avec ψ qu'avec π, voir par exemple [TMF00] : le théorème des nombres premiers est équivalent à l'assertion $\psi(x) \sim x$.

Les démonstrations habituelles du théorème des nombres premiers passe par l'analyse complexe (il existe des démonstrations élémentaires, mais elles ne sont nullement aisées : le terme *élémentaire* indique seulement qu'elles n'utilisent pas l'analyse complexe !), introduisons donc la fonction ζ de Riemann. Soit :

$$\zeta(s) = \sum_n \frac{1}{n^s},$$

pour $\Re e\, s > 1$. La définition donnée ici n'a clairement aucun sens pour $\Re e\, s \leq 1$. Par contre, on utilisera son *prolongement analytique* au plan complexe en une fonction méromorphe (ayant comme seul pôle $s = 1$). On pourra se référer à nouveau à [Ten95] pour une méthode classique (il y a plusieurs façons d'y parvenir, toutes menant fort heureusement à la même fonction !) de prolongement de ζ.

On a l'importante formule suivante, appelée identité d'Euler, qui fait le lien entre ζ (somme sur tous les nombres entiers) et un produit sur les nombres premiers[1] :

$$\zeta(s) = \prod_p \left(1 - \frac{1}{p^s}\right)^{-1} \tag{1.1}$$

[1] On peut voir cette identité comme une version analytique du théorème d'existence et d'unicité de la décomposition d'un entier en facteurs premiers, c'est ce qui est d'ailleurs utilisé dans la démonstration de l'identité en question.

pour $\Re e\, s > 1$.

Signalons que l'on a un *développement en produit eulérien* similaire pour toute fonction arithmétique f complètement multiplicative [2] ; ainsi pour $\Re es > 1$, on a : $\sum_n f(n)/n^s = \prod_p (1 - f(p)/p^s)^{-1}$.

Une connaissance précise de la répartition des nombres premiers repose sur une bonne connaissance de la fonction ζ et en particulier de ses zéros (parmi ceux-ci, on distingue les zéros de partie réelle négative, que l'on connaît parfaitement, et ceux compris dans la bande $0 \leq \Re e\, s \leq 1$, que l'on nomme zéros "non triviaux"). A titre d'illustration, on a la formule suivante due à von Mangoldt, qui exprime ψ au moyen d'une somme sur les zéros non triviaux de ζ :

$$\psi(x) = x - \sum_{\rho} \frac{x^\rho}{\rho} - \log(2\pi) - \frac{1}{2}\log(1 - x^{-2}),$$

pour $x \neq p^\nu$, la somme convergente en "valeur principale". La démonstration n'est pas éloignée de celle du théorème des nombres premiers que nous donnerons ici (voir [EMF75]).

On peut montrer le théorème des nombres premiers sous la forme la plus simple $\psi(x) = x + o(x)$ grâce au simple fait que ζ n'a pas de zéros dans le demi-plan $\Re e\,(s) \geq 1$ (on sait qu'il n'y en a pas pour $\Re e\,(s) > 1$ grâce à la formule (1.1), il suffit donc de montrer qu'il y en a pas sur la droite verticale $\Re e\,(s) = 1$). Pour une telle démonstration, voir [TMF00] p.50, [Ten95] p.171.

Si l'on veut un terme d'erreur plus fin qu'un simple $o(x)$, on a besoin d'une meilleure localisation des zéros que celle annoncée au paragraphe précédent. C'est à une telle preuve que nous allons nous intéresser ici.

[2] On appelle ainsi une fonction arithmétique f qui vérfie $f(mn) = f(m)f(n)$ pour tous (m, n).

Chapitre 2

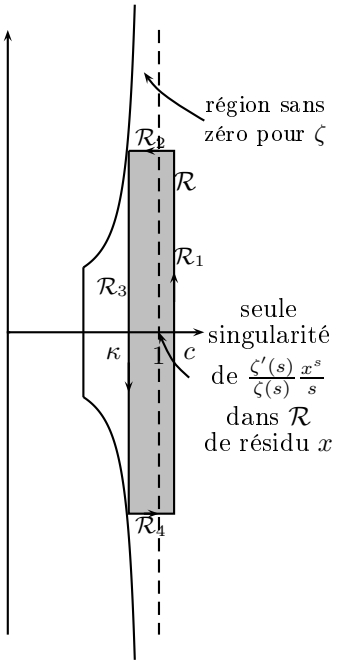
Théorème des nombres premiers

Nous donnons d'abord un schéma de la preuve du théorème, avant d'entrer dans les détails de la démonstration.

$$-\frac{\zeta'(s)}{\zeta(s)} = \sum_0^\infty \frac{\Lambda(n)}{n^s}$$ par dérivation logarithmique de ζ (terme à terme) et par l'identité d'Euler $\zeta(s) = \prod_p (1-1/p^s)^{-1}$

$\Downarrow(1)$ formule de Perron tronquée

$$\psi(x) = -\frac{1}{2i\pi}\int_{c-iT}^{c+iT} \frac{\zeta'(s)}{\zeta(s)}\frac{x^s}{s}ds + \mathcal{O}(\log x(1+x\frac{\log T}{T}))$$



$\Downarrow(2)$ théorème des résidus appliqué à l'intérieur du rectangle $\mathcal{R}$; l'absence de zéros pour ζ entraîne l'absence de singularités autres que 1 pour l'intégrande

$$\psi(x) = x - \frac{1}{2i\pi}\int_{\mathcal{R}_2+\mathcal{R}_3+\mathcal{R}_4} \frac{\zeta'(s)}{\zeta(s)}\frac{x^s}{s}ds + \mathcal{O}(\log x(1+x\frac{\log T}{T}))$$

$\Downarrow(3)$ majorations de $|\int_{\mathcal{R}_2+\mathcal{R}_4}\dots|$, $|\int_{\mathcal{R}_3}\dots|$, et choix optimal de T

$$\psi(x) = x + \mathcal{O}(xe^{-c_0\sqrt{\log x}})$$

(1) Pour ceux qui veulent aller vite, on peut appliquer le lemme 2 car $|\Lambda(n)| \leq \log n$ d'une part et $|\zeta'(\sigma)/\zeta(\sigma)| \ll 1/(\sigma-1)$ (pour $\sigma > 1$) (en effet la même propriété pour ζ, obtenue par comparaison série/intégrale, implique celle-ci) d'autre part.

Les formules de Perron permettent d'obtenir à partir d'une série de Dirichlet $F(s) = \sum_{n\geq 1} a_n/n^s$ la fonction sommatoire de ses coefficients[1] $A(x) = \sum_{n\leq x} a_n$.

Lemme 1 *Pour $x \in \mathbb{R}\backslash\mathbb{N}$ et $c > 0$ supérieur à l'abscisse de convergence absolue de F, on a :*

$$\sum_{n\leq x} a_n = \frac{1}{2i\pi}\int_{c-i\infty}^{c+i\infty} F(s)\frac{x^s}{s}ds, \tag{2.1}$$

[1] on remarquera l'analogie avec les théorèmes de Cauchy, qui permettent d'obtenir les coefficients a_n d'une série entière $\sum_{n\geq 1} a_n z^n$ par intégration complexe.

où l'intégrale est semi-convergente.

Remarque. Pour un énoncé plus général, voir [Ten95].

Idée de la démonstration. Tout repose sur le cas $F(s) = n^{-s}$ et l'on obtient le résultat pour $F(s) = \sum_{n\geq 1} a_n/n^s$ par sommation (avec quand même un soin particulier au niveau des passages à la limite). Il s'agit de montrer que :

$$\frac{1}{2i\pi}\int_{c-i\infty}^{c+i\infty}\left(\frac{x}{n}\right)^s\frac{ds}{s} = \begin{cases} 1 \text{ si } x > n \\ 0 \text{ si } x < n \end{cases}$$

(avec semi-convergence de l'intégrale).

Pour cela, on montre (en utilisant l'intégration complexe et le théorème des résidus) que :

$$\left|\frac{1}{2i\pi}\int_{c-iT}^{c+iT}\left(\frac{x}{n}\right)^s\frac{ds}{s} - \mathbf{1}_{[n,\infty[}\right| \ll \frac{(x/n)^c}{T|\log x/n|} \tag{2.2}$$

pour $x \neq n$, $c > 0$.

Nous aurons besoin ici d'une formule de Perron modifiée : on ne connaît pas forcément bien la fonction que l'on intègre $F(s)$ sur toute une bande verticale $s \in c + i\mathbb{R}$, surtout pour des grandes valeurs[2] de $|\Im m\, s|$.

C'est pourquoi l'on modifie la formule de Perron, de telle sorte à pouvoir contrôler la contribution de $|\Im m\, s| > T$ (où T est un paramètre) à l'intégrale (2.1) :

Lemme 2 (Formule de Perron tronquée) *Soit $F(s) = \sum_{n\geq 1} a_n/n^s$ une série de Dirichlet d'abscisse de convergence absolue finie σ_a, dont on suppose que :*

$$\sum_{n\geq 1} |a_n|/n^\sigma \ll (\sigma - \sigma_a)^{-a}$$

pour un certain $a > 0$ et pour tout $\sigma > \sigma_a$. On suppose de plus que $(|a_n|)$ est majorée par une fonction croissante B. Alors :

$$\sum_{n\leq x} a_n = \frac{1}{2i\pi}\int_{c-iT}^{c+iT} F(s)\frac{x^s}{s}ds + \mathcal{O}\left(x^{\sigma_a}\frac{(\log x)^a}{T} + B(2x)(1 + x\frac{\log T}{T})\right)$$

pour $x \geq 2$, $T \geq 2$, $c = \sigma_a + \frac{1}{\log x}$.

[2] Voir la remarque (2).

Démonstration.

Nous voyons que le terme en $|\log x/n|$ au dénominateur dans (2.2) amènera des complications si x est proche de n. D'où la nécessité de la disjonction de cas suivante :

$\left|1/2i\pi \int_{c-iT}^{c+iT} (x/n)^s \, ds/s - \mathbf{1}_{[n,\infty[}\right|$ est soit :

- $$\ll \frac{x^c}{n^c T}$$
  si $n \notin [1/2x, 2x]$, i.e. $|\log x/n| > \log 2$, grâce à (2.2).
- $$\ll \frac{x^c}{n^c(1+T|\log x/n|)}$$
  si $n \in [1/2x, 2x]$. Cela toujours en appliquant (2.2) si $T|\log x/n| > 1$; et si $T|\log x/n| < 1$, cette estimation résulte de : $|1/2i\pi \int_{c-iT}^{c+iT} (x/n)^s \, ds/s| \ll (x/n)^c \int_{c-iT}^{c+iT} ds/s + (x/n)^c \int_{c-iT}^{c+iT} ((x/n)^{i\tau} - 1) ds/s \ll (x/n)^c$

(ces inégalités étant valables uniformément en T et en x).

En sommant sur n et en multipliant par a_n, le terme d'erreur de

$$\sum_{n \le x} a_n - \frac{1}{2i\pi} \int_{c-iT}^{c+iT} F(s) \frac{x^s}{s} ds$$

émanant du premier cas ci-dessus est :

$$\ll x^c \sum_{n \notin [\frac{1}{2}x, 2x]} \frac{|a_n|}{n^c T} \ll \frac{x^c}{T} \sum_{n \ge 1} \frac{|a_n|}{n^c} \ll \frac{x^{\sigma_a}}{T} (\log x)^a$$

La contribution dans le terme d'erreur provenant du deuxième cas est :

$$\ll \sum_{x/2 \le n \le 2x} \frac{|a_n|}{n^c(1+T|\log x/n|)} \ll B(2x) \sum_{0 \le j \le x+1} \frac{1}{1+Tj/x}$$

où j est la distance de n à l'entier le plus proche de x (ce qui nous donne $|\log x/n| \gg |j|/x$). Ainsi ceci nous donne (en séparant la dernière somme suivant que $j \le$ ou $> x/T$) un terme d'erreur lié au deuxième cas :

$$\ll B(2x)(1 + x/T + x\frac{\log T}{T}) = B(2x)(1 + x\frac{\log T}{T}).$$

On peut obtenir d'autres formules de sommation similaires, en remplaçant par exemple la fonction x^s/s apparaissant dans (2.1) par la fonction $\Gamma(s)x^s$:

Lemme 3

$$\frac{1}{2i\pi}\int_{c-i\infty}^{c+i\infty} F(s)\Gamma(s)x^s ds = \sum_{n\geq 1} a_n e^{-n/x}$$

Remarque. Voir plus généralement la transformation de Mellin, la transformée de $\begin{cases} 0 & \text{si} \quad x<1 \\ 1/2 & \text{si} \quad x=1 \\ 1 & \text{si} \quad x>1 \end{cases}$ étant $1/s$, celle de e^{-x} étant $\Gamma(s)$.

Région sans zéros pour ζ. Trouver une région sans zéros pour ζ ne repose que sur un nombre restreint d'arguments ; la démonstration qui suit n'utilise d'ailleurs que peu d'information sur la fonction ζ elle-même, et peut s'adapter au cas d'autres fonctions.

Pour cela, rappelons-nous d'abord l'exercice classique suivant : pour un polynôme P, si $x_1, \ldots, x_n$ sont ses zéros, on a :

$$\frac{P'}{P} = \sum_{i=1}^{n} \frac{1}{X - x_i}$$

Dans le cas d'une fonction holomorphe F on peut avoir une formule d'origine similaire, mais en fonction seulement de zéros concentrés dans un domaine borné ; plus précisément une expression de la forme :

$$\frac{F'(s)}{F(s)} = \sum_{\rho \text{ zéro de } F \text{ dans } \mathcal{D}} \frac{1}{s-\rho} + (\text{terme d'erreur lié à } F \text{ dans un domaine plus grand que } \mathcal{D}) \quad (2.3)$$

On démontre aisément une telle formule avec des outils d'analyse complexe, valable dans un disque $|s - s_0| \leq \frac{R}{4}$, avec $\mathcal{D}$ le disque $|s - s_0| \leq \frac{R}{2}$, et un terme d'erreur $\mathcal{O}(\frac{\log M/m}{R})$, où M est une borne supérieure de F sur $|s - s_0| \leq R$, et m une borne inférieure de $F(s_0)$.

Remarque. De façon générale, pour une fonction holomorphe F, une expression en F'/F permet de faire apparaître des pôles simples $m/(s-\rho)$, où ρ est un zéro de multiplicité m. C'est ce qui permet notamment d'obtenir le théorème de Rouché, etc.

Nous montrons ici :

Théorème 2 *Il existe une constante positive c_1 telle que la fonction ζ ne s'annule pas dans la région $\sigma \geq 1 - \frac{c_1}{\log(2+|\tau|)}$.*

Démonstration.

Soit $\rho = \beta + i\gamma$ un zéro de ζ, et $s = \sigma + i\tau$ tel que $\sigma > 1$ (on fixera s ultérieurement). On a, par le lemme d'analyse complexe annoncé[3] :

[3]Pour cela, il faut une majoration et une minoration de ζ. Pour la majoration, utilisons la formule donnant le prolongement de ζ à $\sigma > 0$: $\zeta(s) = \frac{s}{s-1} - s\int_1^\infty \{t\}\, t^{-s-1} dt$. En majorant dans l'intégrale $\{t\}$ par 1, on a $\zeta(s) \ll |\tau|$ pour $\sigma \geq \sigma_0$ où $\sigma_0 > 0$ est fixé.

Pour la minoration, $|\frac{1}{\zeta(s)}| = |\sum_n \frac{\mu(n)}{n^s}| \ll \zeta(\sigma)$ (la première identité étant obtenue en utilisant (1) avec la formule $\mathbf{1} * \mu = \delta$, qui n'est autre que la formule d'inversion de Möbius !) En prenant $\sigma = 1 + \frac{1}{\log|\tau|}$, et avec $\zeta(\sigma) \ll \frac{1}{\sigma - 1}$ on obtient bien $\zeta(s) \gg \frac{1}{\log|\tau|}$.

$$-\frac{\zeta'(s)}{\zeta(s)} = -\sum_{|\rho-s|\leq\frac{1}{2}} \frac{1}{s-\rho} + \mathcal{O}(\log|\tau|).$$

En prenant la partie réelle :

$$-\Re e\,\frac{\zeta'(s)}{\zeta(s)} \leq \sum_{|\rho-s|\leq\frac{1}{2}} \Re e\,-\frac{1}{s-\rho} + \mathcal{O}(\log|\tau|) \tag{2.4}$$

On remarque que :

$$\Re e\,-\frac{1}{s-\rho} = \frac{-(\sigma-\beta)}{|s-\rho|^2} \leq 0$$

(en effet $\sigma > 1$, et $\beta \leq 1$ car ζ ne s'annule pas dans le demi-plan $\beta > 1$, par le produit eulérien).

Ce qui nous donne le droit d'enlever dans la majoration (2.4) autant de termes de la somme que l'on veut !

L'inégalité $3 + 4\cos\theta + \cos 2\theta = 2(1+\cos\theta)^2 \geq 0$ donne, puisque $\Lambda(n) \geq 0$:

$$\Re e \sum_{n\geq 1} \frac{\Lambda(n)}{n^\sigma}(3 + 4e^{-i\tau\log n} + e^{-2i\tau\log n}) \geq 0$$

$$3\Re e\,-\frac{\zeta'(\sigma)}{\zeta(\sigma)} + 4\Re e\,-\frac{\zeta'(\sigma+i\tau)}{\zeta(\sigma+i\tau)} + \Re e\,-\frac{\zeta'(\sigma+2i\tau)}{\zeta(\sigma+2i\tau)} \geq 0$$

Le premier terme est $\frac{3}{\sigma-1} + \mathcal{O}(1)$; dans le second on ne garde dans la somme de (2.4) que le terme correspondant au zéro $\rho = \beta + i\gamma$; dans le troisième on ne garde rien de la somme !

Cela nous donne :

$$\frac{3}{\sigma-1} + \Re e\,-\frac{4}{s-\rho} + \mathcal{O}(\log|\tau|) \geq 0$$

En choisissant s tel que $\tau = \gamma$, et et précisant la constante du $\mathcal{O}$:

$$\frac{3}{\sigma-1} - \frac{4}{\sigma-\gamma} \geq c_2 \log|\gamma|$$

En choisissant une bonne valeur de σ, par exemple $\sigma = 1 + \frac{1}{2c_2\log|\tau|}$, on arrive enfin à :

$$1 - \beta \geq \frac{c_3}{\log|\gamma|}$$

Tout ce que nous avons utilisé ici est vrai pour $|\tau|$ "suffisamment grand", i.e. supérieur à une borne bien fixée τ_0. Cela est également vrai, quitte à modifier la constante c_3, pour les valeurs de τ plus petites que τ_0 (par compacité, car ζ ne s'annule pas[4] sur $\Re e\, s = 1$). On a finalement le résultat, écrit avec une autre constante c_1 et $\log(2+|\tau|)$ à la place de $\log|\tau|$ pour que l'expression garde un sens même pour $|\tau|$ petit.

(2) Avec cette région sans zéros pour ζ, on peut obtenir une région *rectangulaire* $[\kappa, c] \times [-T, T]$ (délimitée par $\mathcal{R}$) sans zéros pour ζ, avec $\kappa = 1 - c_4/\log T$ et $c = 1 + 1/\log x$.

Dès lors, dans cette région, $(\zeta'(s)/\zeta(s))(x^s/s)$ n'a pas de singularités autres que 1 (elles proviendraient d'éventuels zéros du dénominateur, mais il n'y en a pas, on a tout fait pour !), et cette singularité est un pôle simple de résidu x.

(3) Quitte à rétrécir la région rectangulaire obtenue en modifiant la constante c_4, on peut montrer une majoration[5] $|\zeta'(s)/\zeta(s)| \ll \log T$ dans la région sans zéros annoncée, d'où :

- sur les segments horizontaux $\mathcal{R}_2$ et $\mathcal{R}_4$, $|s| \geq T$, d'où

$$|\frac{\zeta'(s)}{\zeta(s)}\frac{x^s}{s}| \ll x^{1+1/\log x}\frac{\log T}{T}$$

  La longueur des segments étant ≤ 2, on a :

$$|\int_{\mathcal{R}_2+\mathcal{R}_2} \ldots| \ll x\frac{\log T}{T}$$

- sur le segment vertical $\mathcal{R}_3$:

$$|\frac{\zeta'(s)}{\zeta(s)}\frac{x^s}{s}| \ll \frac{x^{1-\frac{c_4}{\log T}}}{|s|}(\log T)$$

$$|\int_{\mathcal{R}_3} \ldots| \ll x^{1-\frac{c_4}{\log T}}(\log T)\int_{\mathcal{R}_3}\frac{ds}{|s|} \ll x^{1-\frac{c_4}{\log T}}(\log T)^2$$

  En choisissant $T = e^{\sqrt{c_4 \log x}}$, on trouve le terme d'erreur souhaité.

Remarque. On avait bien besoin d'utiliser une formule de Perron "tronquée en hauteur" car on ne connaît que des domaines $\mathcal{D}$ sans zéros de ζ, de largeur donnée $\delta > 0$, **bornés en hauteur**. (Notons que c'est $\inf\{\Re e\, s, s \in \mathcal{D}\}$ qui intervient ici, donc le fait d'utiliser un domaine non rectangulaire n'apporterait rien !)

[4] Cela se montre aisément grâce à l'inégalité trigonométrique vue plus haut, d'où nous tirons $|\zeta(\sigma)|^3|\zeta(\sigma+i\tau)|^4|\zeta(\sigma+2i\tau)| \geq 1$; on constate ensuite qu'un zéro en $1+i\tau$ amènerait une divergence de ζ en $1+2i\tau$!

[5] Voir [Ten95].

Signalons que l'obtention d'une région sans zéros $\Re e\, s \geq 1-\delta$ constituerait une nouvelle fantastique en théorie analytique des nombres !

Un raisonnement similaire à la démonstration précédente montre que l'hypothèse de Riemann (l'absence de zéros de ζ dans $\Re e\, s > 1/2$) implique (il y a en fait équivalence)

$$\psi(x) = x + \mathcal{O}(x^{1/2+\varepsilon}) \qquad (\forall \varepsilon > 0).$$

Chapitre 3

Crible

On attribue généralement l'idée du crible à Eratosthène, qui donnait un algorithme pour trouver les nombres premiers. Legendre fut un des premiers à en déduire une formule ayant pour application un moyen (théorique) pour calculer $\pi(x)$:
On sait qu'un entier n est premier s'il n'a pas de diviseur inférieur à $\sqrt{n}$, donc un entier $\sqrt{x} \leq n \leq x$ est premier s'il n'a pas de diviseur inférieur à $\sqrt{x}$, ce qui est équivalent à dire que n est premier à $P = \prod_{p \leq \sqrt{x}} p$, ou encore $\delta((n, P)) = 1$, avec :

$$\delta(n) = \begin{cases} 1 & \text{si} \quad n = 1 \\ 0 & \text{si} \quad n > 1 \end{cases}$$

Ainsi $\pi(x) - \pi(\sqrt{x}) + 1 = \sum_{n \leq x} \delta((n, P))$.

On utilise alors la formule $\delta = \mathbf{1} * \mu$ $\left(\sum_{d|n} \mu(d) = \begin{cases} 1 & \text{si} \quad n = 1 \\ 0 & \text{si} \quad n > 1 \end{cases} \right)$ pour écrire[1] :

$$\sum_{n \leq x} \sum_{d|(n,P)} \mu(d) = \sum_{d \leq x} \mu(d) \sum_{\substack{n \leq x \\ d|n}} 1 = \sum_{d|P} \mu(d) \left[\frac{x}{d} \right]$$

On peut ensuite utiliser l'esimation $[x] = x + \mathcal{O}(1)$, mais on ne peut en déduire directement quelque chose de non trivial pour $\pi(x)$, en raison du terme

[1] Cette formule donne un éclairage sur la fonction de Möbius — dont la définition peut paraître bien mystérieuse pour le débutant : la dernière identité traduit le fait que pour obtenir le nombre de nombre premiers entre $\sqrt{x}$ et x, il faut **décompter** le nombre de multiples des nombres premiers $\leq \sqrt{x}$ (2, 3, 5, etc.). Cependant les multiples de $2 \cdot 3$, $2 \cdot 5$, $3 \cdot 5$, etc. auront été décomptés deux fois, il faut donc corriger cela en **ajoutant** une fois le nombre des multiples des entiers ayant exactement deux facteurs premiers. Mais alors les multiples de $2 \cdot 3 \cdot 5$, etc. (les multiples des nombres ayant exactement trois facteurs premiers) auront été rajoutés deux fois, il faut donc les **décompter** une fois, etc. D'où une alternance de ± 1 en fonction du nombre de facteurs premiers : c'est bien ce qui apparaît dans la définition de la fonction de Möbius !

d'erreur bien trop important résultant du $\mathcal{O}(1)$. Cependant, c'est tout l'enjeu de la théorie du crible, véritablement initiée par Brun dans les années 1920, que de réussir à obtenir de tels résultats, en raffinant cette méthode.

Le néophyte pourra se référer à [Odl71], ou aux exposés introductifs [Gre] ; cependant la référence incontournable est [HR74].

Nous utilisons ici la méthode de crible de Selberg pour majorer le nombre de nombres premiers $p = a \pmod q$ (avec $(a,q) = 1$) dans l'intervalle $[M+1, M+N]$. On démontre une version légèrement plus faible du

Théorème 3 (Brun-Titchmarsh)

$$\sum_{\substack{M+1\leq p\leq M+N\\ p=a \pmod q}} 1 \leq 2\frac{N}{\phi(q)}\frac{1}{\log N/q}.$$

où la constante 2 est remplacée par $(2 + o(1))$.

Démonstration.

Soit (λ_d) une suite de nombres réels soumise à la condition $\lambda_1 = 1$. L'idée du crible de Selberg repose sur les faits simples suivants :

- un carré est toujours positif,
- pour p premier dans $[M+1, M+N]$ et $p > z$, $\sum_{d|p} \lambda_d \geq 1$, si l'on a mis comme condition supplémentaire $\lambda_d = 0$ pour $d > z$, où z est un paramètre que l'on choisira ultérieurement.

On a ainsi :

$$S = \sum_{\substack{M+1\leq p\leq M+N\\ p=a \pmod q}} 1 \leq \underbrace{\sum_{\substack{M+1\leq n\leq M+N\\ n=a \pmod q}} \left(\sum_{d|n} \lambda_d\right)^2}_{Z} + z$$

Le problème revient donc à minimiser Z. Nous développons le carré :

$$Z = \sum_{d_1,d_2\leq z} \lambda_{d_1}\lambda_{d_2} \sum_{\substack{M+1\leq n\leq M+N\\ [d_1,d_2]|n\\ n=a \pmod q}} 1$$

La condition $(a,q) = 1$ implique que seuls les d tels que $(d,q) = 1$ interviennent dans la dernière somme. Dans ce cas on a :

$$\sum_{\substack{M+1\leq n\leq M+N\\ [d_1,d_2]|n\\ n=a \pmod q}} 1 = \frac{N}{[d_1,d_2]q} + \mathcal{O}(1)$$

On pose $\lambda_d = 0$ si $(d,q) \neq 1$, ainsi :

$$Z = \frac{N}{q} \underbrace{\sum_{d_1,d_2 \leq z} \frac{\lambda_{d_1}\lambda_{d_2}}{[d_1,d_2]}}_{Z_0} + \mathcal{O}(\sum_{d_1,d_2 \leq z} |\lambda_{d_1}||\lambda_{d_2}|) \tag{3.1}$$

Nous suivons la méthode développée par Selberg pour déterminer les λ_d optimaux pour minimiser le terme principal de (3.1) :

$$Z_0 = \sum_{d_1,d_2 \leq z} (d_1,d_2) \frac{\lambda_{d_1}}{d_1}\frac{\lambda_{d_2}}{d_2} = \sum_{\ell \leq z} \phi(\ell) (\underbrace{\sum_{\substack{d \leq z \\ \ell | d}} \frac{\lambda_d}{d}}_{y_\ell})^2$$

(on a utilisé pour la dernière égalité l'identité arithmétique $id = \mathbf{1} * \phi$)[2]

On peut exprimer les λ_d en fonction des y_ℓ : $\lambda_d/d = \sum_{\substack{\ell \leq z \\ d|\ell}} \mu(\ell/d) y_l$, et la condition $\lambda_1 = 1$ devient donc $\sum_{\ell \leq z} \mu(\ell) y_\ell$.

Il s'agit donc à présent de minimiser la forme quadratique $Z_0 = \sum_{\ell \leq z} \phi(\ell) y_\ell^2$ sous la condition précédente. Notons que l'on a également $y_\ell = 0$ si $(\ell, q) \neq 1$.

Par la méthode des multiplicateurs de Lagrange, en notant θ un tel multiplicateur, on a pour $(\ell, q) = 1$,

$$y_\ell = \frac{\theta \mu(\ell)}{2\phi(\ell)}$$

et

$$\underbrace{\frac{\theta}{2} \sum_{\substack{\ell \leq z \\ (\ell,q)=1}} \frac{\mu^2(\ell)}{\phi(\ell)}}_{G_q(z)} = 1.$$

Donc

$$y_\ell = \frac{\mu(\ell)}{\phi(\ell) G_q(z)}, \text{ si } (\ell, q) = 1,$$

et en reportant dans Z_0, on obtient

$$Z_0 = \frac{1}{G_q(z)}.$$

[2]Cette identité nous a permis de faire passer (d_1, d_2) au niveau de la sommation, et ainsi de découpler d_1 et d_2 ; en effet $\ell | (d_1, d_2) \Leftrightarrow \ell | d_1$ et $\ell | d_2$.

Il reste alors à estimer $G_q(z)$. On peut montrer pour $(e,f)=1$ que

$$\frac{e}{\phi(e)}G_{ef}(z/e) \leq G_f(z) \leq \frac{e}{\phi(e)}G_{ef}(z)$$

Ceci nous permet d'une part d'obtenir $|\lambda_d| \leq 1$, ce qui nous donne un terme d'erreur pour (3.1) majoré par z^2. En effet, si $(d,q)=1$,

$$\lambda_d = \frac{d}{G_q(z)} \sum_{\substack{\ell \leq z \\ d|\ell \\ (\ell,q)=1}} \mu(\ell/d)\frac{\mu(\ell)}{\phi(\ell)} = \frac{\mu(d)d}{G_q(z)} \sum_{\substack{md \leq z \\ (m,dq)=1}} \frac{\mu^2(m)}{\phi(m)\phi(d)} = \mu(d)\frac{d}{\phi(d)}\frac{G_{dq}(z/d)}{G_q(z)}$$

et on peut appliquer l'inégalité précédente.

D'autre part $G_q(z) \geq (\phi(q)/q)G_1(z)$ et le problème concernant $G_q(z)$ revient simplement à évaluer $G_1(z)$.

On a

$$G_1(z) = \sum_{\ell \leq z} \frac{\mu^2(\ell)}{\phi(\ell)} = \sum_{\ell \leq z} \frac{\mu^2(\ell)}{\ell} \prod_{p|\ell} \frac{1}{1-1/p}$$

Or :

$$\prod_{p|\ell} \frac{1}{1-1/p} = \prod_{p|\ell} \sum_{k=0}^{\infty} \frac{1}{p^k} = \sum_{p \,|\, d \Rightarrow p \,|\, \ell} \frac{1}{d}$$

(la dernière somme porte sur tous les entiers d qui ont comme facteurs premiers seulement ceux de ℓ).
D'autre part, chaque entier $m \geq 1$ se décompose de manière unique sous la forme $m = \ell\, d$ avec $\mu^2(\ell) = 1$ (ℓ sans facteur carré) et $p \,|\, d \Rightarrow p \,|\, \ell$, on a donc finalement :

$$\log z \leq \sum_{1 \leq m \leq z} \frac{1}{m} \leq \sum_{1 \leq \ell \leq z} \frac{\mu^2(\ell)}{\ell} \sum_{p \,|\, d \Rightarrow p \,|\, \ell} \frac{1}{d} = G_1(z)$$

Rassemblons toutes les inégalités obtenues, ce qui nous donne :

$$S \leq \frac{N}{\phi(q)}\frac{1}{\log z} + z^2 + z$$

En prenant $z = (y/q)^{1/2}(\log y/q)^{-1}$, on a, comme annoncé,

$$S \leq (2+o(1))\frac{N}{\phi(q)}\frac{1}{\log N/q}.$$

Chapitre 4

Des nombres premiers en progressions arithmétiques

4.1 Introduction

En vue d'étudier la distribution des nombres premiers dans les progressions arithmétiques, nous allons utiliser la méthode initiée par Dirichlet pour démontrer le

Théorème 4 (de la progression arithmétique) *Soit a et q des entiers ≥ 1, premiers entre eux. Il existe une infinité de nombres premiers p congrus à a modulo q.*

Remarque. Comme souvent en théorie analytique des nombres, on conjecture que "ce qui n'est pas trivialement interdit se réalise".
Ici, il n'est pas possible qu'un nombre premier p soit congru à a modulo q si a et q ne sont pas premiers entre eux (p serait alors trivialement divisible par (a, q) et donc non premier !), c'est pourquoi l'on doit rajouter une condition supplémentaire dans l'énoncé du théorème.
Hormis cette restriction évidente, rien ne semble s'opposer à ce qu'un nombre premier soit congru à a modulo q, avec a premier à q. Bien plus est vrai en fait : non seulement il y a une infinité de nombres premiers dans chacune de ces classes $a \pmod q$ (avec a premier à q), mais ceux-ci se répartissent même de façon équitable dans les différentes classes. Comme il y a $|(\mathbb{Z}/q\mathbb{Z})^*| = \phi(q)$ classes, on peut penser que : $\pi(a, q, x) \sim \pi(x)/\phi(q)$, ce qui bien le cas comme on le verra par la suite.

Mais n'anticipons pas et voyons d'abord comment arriver au théorème 4. Pour cela nous allons introduire la notion de *caractères* sur les groupes abé-

liens finis (le cadre plus général étant celui des groupes topologiques n'est pas développé ici). Avant tout quelques définitions :

Soit G un groupe abélien fini. Un *caractère* de G est un homomorphisme de G dans le groupe multiplicatif $\mathbb{C}^*$ des nombres complexes.
On note $\hat{G}$ l'ensemble des caractères de G, qu'on munit de la structure naturelle de groupe multiplicatif (c'est à dire pour χ_1 et χ_2 deux caractères de G, $\chi_1\chi_2$ est l'homomorphisme $x \mapsto \chi_1(x)\chi_2(x)$)
L'élément neutre de $\hat{G}$ (l'identité sur G), appelé caractère *principal* de G, sera noté χ_0 ou $\mathbf{1}$.

Idée de la démonstration. Pour montrer l'existence d'une infinité de nombres premiers $p = a \pmod q$, Dirichlet propose de montrer que $\sum_{p=a \pmod q} 1/p$ diverge, d'où on veut étudier la limite de $\sum_{p=a \pmod q} 1/p^s$ quand s tend vers 1.

1) Rappelons-nous le cas standard des nombres premiers, non en progression arithmétique. On a (le tout reposant sur l'identité d'Euler : $\sum_n 1/n^s = \prod_p (1 - 1/p^s)^{-1}$) :

$$\sum_p \frac{1}{p^s} = \log \zeta(s) + \mathcal{O}(1) \qquad (s \to 1, \Re e\, s > 1) \tag{4.1}$$

Étudier $\sum_p 1/p^s$ revient ainsi à connaître $\zeta(s) = \sum_n 1/n^s$.

2) Si on voulait faire de même dans le cas des nombres premiers en progression arithmétique, il faudrait pouvoir relier $\sum_{p=a \pmod q} 1/p^s = \sum_p \mathbf{1}_{a,q}(p)/p^s$ à $\sum_n \mathbf{1}_{a,q}(n)/n^s$, où $\mathbf{1}_{a,q}(n) = \begin{cases} 1 & \text{si } n = a \pmod q \\ 0 & \text{sinon} \end{cases}$ est la fonction caractéristique des entiers congrus à a modulo q.

Malheureusement, $\mathbf{1}_{a,q}$ n'est pas complètement multiplicative, donc on n'a pas le produit eulérien désiré qui aurait permis d'avoir un analogue de (4.1).

Toute l'astuce repose dans le fait de décomposer $\mathbf{1}_{a,q}$ comme somme de fonctions qui elles, sont complètement multiplicatives : les caractères. On verra par la suite qu'on a ainsi la "décomposition de Fourier" suivante :

$$\mathbf{1}_{a,q}(n) = \frac{1}{\phi(q)} \sum_{\chi \bmod q} \overline{\chi(a)}\chi(n)$$

Cela nous donne alors :

$$\sum_p \frac{\mathbf{1}_{a,q}(p)}{p^s} = \frac{1}{\phi(q)} \sum_{\chi \bmod q} \overline{\chi(a)} \sum_p \frac{\chi(p)}{p^s} \tag{4.2}$$

Une fois cette décomposition effectuée, on peut espérer avoir un analogue de (4.1), et réussir à exprimer $\sum_p \chi(p)/p^s$ en fonction d'analogues de fonctions ζ : les fonctions L.

Soit $L(s,\chi) = \sum_n \chi(n)/n^s$. Comme les caractères χ sont complètement multiplicatifs, on a le produit eulérien[1] suivant :

$$L(s,\chi) = \prod_p \left(1 - \frac{\chi(p)}{p^s}\right)^{-1}, \tag{4.3}$$

donc en prenant le logarithme,

$$\sum_p \frac{\chi(p)}{p^s} = \log L(s,\chi) + \mathcal{O}(1) \qquad (s \to 1, \Re e\, s > 1)$$

En remplaçant dans (4.2), on a :

$$\sum_{p=a \pmod q} \frac{1}{p^s} = \frac{1}{\phi(q)} \sum_{\chi \bmod q} \overline{\chi(a)} \log L(s,\chi) + \mathcal{O}(1) \qquad (s \to 1, \Re e\, s > 1)$$

En montrant que ces fonctions L sont toutes $\neq 0$ quand $s = 1$, sauf l'une d'entre elles, on arrive bien à une divergence de la somme en question, d'où l'infinité de nombres premiers congrus à a modulo q.

4.2 Notions sur les caractères

4.2.1 Caractères additifs sur $\mathbb{Z}/n\mathbb{Z}$

On va déterminer les caractères de $(\mathbb{Z}/n\mathbb{Z}, +)$, pour n entier quelconque.

On considère pour $a \in \mathbb{Z}/n\mathbb{Z}$:

$$\begin{array}{rccc} f_a : & \mathbb{Z}/n\mathbb{Z} & \longrightarrow & \mathbb{C} \\ & x & \longmapsto & e^{2i\pi ax/n} \end{array}$$

C'est un caractère de $(\mathbb{Z}/n\mathbb{Z}, +)$, et tout caractère de $(\mathbb{Z}/n\mathbb{Z}, +)$ est de ce type. En effet soit χ un tel caractère. On a : $\chi(1)^n = 1$ donc $\chi(1) = \omega$ est une racine n-ième de l'unité, et χ est alors tout simplement l'application $x \mapsto \omega^x$.

L'application

$$\begin{array}{ccc} \mathbb{Z}/n\mathbb{Z} & \longrightarrow & \widehat{\mathbb{Z}/n\mathbb{Z}} \\ a & \longmapsto & f_a \end{array}$$

est donc clairement un isomorphisme : le groupe des caractères de $\mathbb{Z}/n\mathbb{Z}$ est isomorphe à $\mathbb{Z}/n\mathbb{Z}$.

[1] Voir chapitre 1.

4.2.2 Caractères de groupes abéliens finis

De façon générale pour G groupe abélien fini, le groupe des caractères de G est isomorphe à G.

Pour cela on remarque que :

$$\begin{array}{ccc} \hat{G_1} \times \hat{G_1} & \longrightarrow & \widehat{G_1 \times G_2} \\ (\chi_1, \chi_2) & \longmapsto & \chi_1 \times \chi_2 : \begin{array}{ccc} G_1 \times G_2 & \longrightarrow & \mathbb{C}^* \\ (x_1, x_2) & \longmapsto & \chi_1(x_1)\chi_2(x_2) \end{array} \end{array}$$

est une bijection.

Démonstration. L'injectivité est triviale :

$$\chi_1\chi_2 = \mathbf{1} \Rightarrow (\chi_1\chi_2)(x_1, 0) = 1 = \chi_1(x_1),$$

et cela pour tout $x_1 \in G_1$, donc $\chi_1 = \mathbf{1}$. De même $\chi_2 = \mathbf{1}$.

Pour la surjectivité, on voit que si χ est un caractère de $\widehat{G_1 \times G_2}$, $\chi_1 : x_1 \mapsto \chi(x_1, 0)$ est un caractère de G_1, de même on définit x_2 ; on a bien $\chi_1(x_1)\chi_2(x_2) = \chi(x_1, x_2)$.

Pour montrer comme annoncé que $\hat{G} \cong G$, on écrit G comme produit de groupes abéliens cycliques :

$$G \cong \prod_{i=1}^{r} \mathbb{Z}/n_i\mathbb{Z}$$

En appliquant le lemme ci-dessus par récurrence, on obtient

$$\hat{G} \cong \prod_{i=1}^{r} (\widehat{\mathbb{Z}/n_i\mathbb{Z}}, +) \cong \prod_{i=1}^{r} (\mathbb{Z}/n_i\mathbb{Z}, +) \cong G$$

On a les relations suivantes, dites d'orthogonalité :

Lemme 4

$$\sum_{x \in G} \chi(x) = \begin{cases} |G| & si\ \chi = \chi_0 \\ 0 & si\ \chi \neq \chi_0 \end{cases}$$

$$\sum_{\chi \in \hat{G}} \chi(x) = \begin{cases} |G| & si\ x = 0 \\ 0 & si\ x \neq 0 \end{cases}$$

$$\sum_{x \in G} \chi_1(x)\overline{\chi_2(x)} = \begin{cases} |G| & si\ \chi_1 = \chi_2 \\ 0 & si\ \chi_1 \neq \chi_2 \end{cases}$$

$$\sum_{\chi\in\hat{G}} \chi(x_1)\overline{\chi(x_2)} = \begin{cases} |G| & si\ x_1 = x_2 \\ 0 & si\ x_1 \neq x_2 \end{cases}$$

Démonstration.

$$\sum_{x\in G} \chi(x) = \sum_{x\in G} \chi(yx) = \underbrace{\chi(y)}_{\neq 1} \sum_{x\in G} \chi(x)$$

Donc $\sum_{x\in G} \chi(x) = 0$. On laisse les autres vérifications au lecteur ; notons que l'on utilise pour la deuxième relation le fait que pour tout $x \in G$, il existe $\psi \in \hat{G}$ tel que $\psi(x) \neq 1$.

Lemme 5 (décomposition de Fourier) *Pour une fonction $f : G \longrightarrow \mathbb{C}$, on a :*

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

où $\hat{f}(\chi) = \frac{1}{|G|}\sum_{y\in G} f(y)\overline{\chi(y)}$.

Exemple : Pour $G = (\mathbb{Z}/n\mathbb{Z}, +)$, cette décomposition est tout simplement :

$$f(x) = \sum_{a \mod n} \hat{f}(a)e^{2i\pi a/n}$$

où $\hat{f}(a) = \frac{1}{n}\sum_{y\in G} f(y)e^{-2i\pi y/n}$.

Remarque. L'ensemble des fonctions $G \longrightarrow \mathbb{C}$ est en fait muni d'un produit hermitien

$$\langle f_1, f_2\rangle = \sum_{x\in G} f_1(x)\overline{f_2(x)}$$

et les caractères forment une base orthogonale. On a ainsi l'égalité de Parseval, etc.

4.2.3 Caractères multiplicatifs

On applique le cas précédent à $G = ((\mathbb{Z}/q\mathbb{Z})^*, \times)$.
Si χ est un caractère de $(\mathbb{Z}/q\mathbb{Z})^*$, on l'étend à $\mathbb{Z}/q\mathbb{Z}$ en posant $\chi(x) = 0$ si $(x, q) \neq 1$. On étend ensuite χ à $\mathbb{Z}$, en composant avec la projection canonique $\mathbb{Z} \to \mathbb{Z}/q\mathbb{Z}$; on remarquera que l'on obtient alors une fonction arithmétique complètement multiplicative. Ce sont ces fonctions sur $\mathbb{Z}$ que l'on appelle *caractères de Dirichlet*.

Dans la suite, on prendra toujours q premier.

Exemples :

1) Un caractère général.
Soit g un générateur de $(\mathbb{Z}/q\mathbb{Z})^*$.

$$\begin{array}{rccl} \chi : & (\mathbb{Z}/q\mathbb{Z}) & \longrightarrow & \mathbb{C} \\ & x = g^t & \longmapsto & \exp(2i\pi t/(q-1)) \\ & 0 & \longmapsto & 0 \end{array}$$

2) Caractère quadratique.
Soit H le sous-groupe des carrés de $(\mathbb{Z}/q\mathbb{Z})^*$, on a $|H| = \frac{q-1}{2}$.

$$\begin{array}{rccl} \chi : & (\mathbb{Z}/q\mathbb{Z}) & \longrightarrow & \mathbb{C} \\ & x & \longmapsto & x^{(q-1)/2} \\ & 0 & \longmapsto & 0 \end{array}$$

Il s'agit tout simplement du symbole de Legendre $\left(\frac{x}{q}\right)$, c'est un caractère quadratique ($\chi^2 = \mathbf{1}$).

Remarque. En utilisant (5), on peut décomposer en caractères multiplicatifs de $((\mathbb{Z}/q\mathbb{Z})^*, \times)$, comme annoncé en introduction, la fonction caractéristique des entiers congrus à a modulo q :

$$\mathbf{1}_{a,q}(n) = \frac{1}{\phi(q)} \sum_{\chi \bmod q} \overline{\chi(a)}\chi(n) \tag{4.4}$$

4.2.4 Inégalité de Polyà-Vinogradov

Théorème 5 (Polyà-Vinogradov) *Soit χ un caractère de Dirichlet non principal modulo q, avec q premier. On a :*

$$\forall N \geq 1, \left| \sum_{n \leq N} \chi(n) \right| \leq \sqrt{q} \log q$$

Remarque. La majoration donnée par le théorème pour $N < \sqrt{q}\log q$ est moins bonne que la majoration triviale $\left|\sum_{n\leq N} \chi(n)\right| \leq N$ (car $|\chi(n)| \leq 1$).

Par contre, pour $N \geq \sqrt{q}\log q$, la majoration implique que les $\chi(n)$ ne peuvent pas être tous égaux à $+1$: des compensations doivent se produire pour

avoir une telle majoration. On trouve ainsi, pour χ caractère réel non principal, que le plus petit n tel que $\chi(n) = -1$ est $\ll \sqrt{q}\log q$ (cela donne notamment une majoration du plus petit non-résidu quadratique modulo q, avec χ le symbole de Legendre).

Démonstration. On développe χ en caractères additifs :

$$\chi(n) = \sum_{a \mod q} \widehat{\chi}(a) e(na/q)$$

avec

$$\widehat{\chi}(a) = \frac{1}{q} \sum_{b \mod {}^* q} \chi(b) e(-ab/q)$$

Par changement de variable $c = ab$ dans la somme pour $a \neq 0$, on obtient :

$$\widehat{\chi}(a) = \frac{1}{q} \sum_{c \mod {}^* q} \chi(ca^{-1}) e(-c/q) = \overline{\chi(a)}\widehat{\chi}(1)$$

donc :

$$|\widehat{\chi}(a)| = |\widehat{\chi}(1)|$$

Par l'identité de Parseval, on a :

$$\sum_{n \mod q} |\chi(n)|^2 = q \sum_{a \mod q} |\widehat{\chi}(a)|^2$$

Cela nous donne $q - 1 = q\sum_{a \mod q} |\widehat{\chi}(1)|^2$, donc $|\widehat{\chi}(a)| = |\widehat{\chi}(1)| = 1/\sqrt{q}$ pour $a \neq 0$; d'autre part comme χ est non principal, $\widehat{\chi}(0) = 0$. Ainsi[2] :

$$\underbrace{\sum_{n \leq N} \chi(n)}_{\text{somme incomplète pour la taille}} = \underbrace{\sum_{a \mod {}^* q}}_{\text{somme complète pour la place finie } q} \widehat{\chi}(a) \underbrace{\sum_{n \leq N} e(na/q)}_{e(a/q)\frac{e(Na/q)-1}{e(a/q)-1}}$$

Or

$$\left| \frac{e(Na/q) - 1}{e(a/q) - 1} \right| \leq \frac{1}{|\sin(\pi a/q)|} \leq \frac{q}{2|a|}$$

pour $|a|/q \leq 1/2$. Donc la somme ci-dessus est majorée par :

$$\sum_{\substack{-q/2 < a \leq q/2 \\ a \neq 0}} \frac{1}{\sqrt{q}} \frac{q}{2|a|} \leq \sqrt{q}\log q$$

[2] Un exemple de *complétion* d'une somme.

4.2.5 Conducteur et caractères primitifs

Soit $\chi : \mathbb{Z} \to \mathbb{C}$ un caractère de Dirichlet. Nous cherchons à définir le plus petit module q pour lequel χ est un caractère modulo q.

On dit que deux caractères χ_1 modulo q_1 et χ_2 modulo q_2 sont équivalents si pour $(n, q_1 q_2) = 1$, on a $\chi_1(n) = \chi_2(n)$. Il s'agit bien d'une relation d'équivalence. Pour un caractère χ donné, le plus petit entier q tel que χ est équivalent à un caractère modulo q est appelé le *conducteur* de χ. Un caractère modulo q est dit *primitif* si son conducteur est q.

4.3 Fonctions L de Dirichlet

Les fonctions L introduites plus haut sont convergentes pour $\sigma > 0$ par critère d'Abel (reposant sur la sommation d'Abel). Elles se prolongent, tout comme la fonction ζ, au plan complexe tout entier en une fonction méromorphe, et même holomorphe si χ n'est pas le caractère principal χ_0. Elles ne s'annulent pas pour $\Re e\, s > 1$, par le produit eulérien (4.3).

On peut avoir une première estimation de la valeur de $L(1, \chi) = \sum_n \chi(n)/n$ ainsi :

$$\left|\sum_n \frac{\chi(n)}{n}\right| = \left|\sum_n \chi(n) \int_n^\infty \frac{dt}{t^2}\right| = \left|\int_1^\infty (\sum_{n=1}^t \chi(n)) \frac{dt}{t^2}\right| \leq \int_1^q \underbrace{\left|\sum_{n=1}^t \chi(n)\right|}_{\leq t} \frac{dt}{t^2} + \int_q^\infty \underbrace{\left|\sum_{n=1}^t \chi(n)\right|}_{\leq q} \frac{dt}{t^2} \leq \log q + 1 \quad (4.5)$$

En utilisant l'inégalité de Polyà-Vinogradov, on peut améliorer ce résultat :

$$\left|\int_1^\infty (\sum_{n=1}^t \chi(n)) \frac{dt}{t^2}\right| \leq \int_1^{\sqrt{q}\log q} \underbrace{\left|\sum_{n=1}^t \chi(n)\right|}_{\leq t} \frac{dt}{t^2} + \int_{\sqrt{q}\log q}^\infty \underbrace{\left|\sum_{n=1}^t \chi(n)\right|}_{\leq \sqrt{q}\log q} \frac{dt}{t^2} \leq \frac{1}{2}\log q + \log_2 q + 1 \quad (4.6)$$

Remarque. La valeur de $L(1, \chi)$ pour χ caractère réel primitif modulo q est liée à l'extension $\mathbb{Q}(\sqrt{\pm q})$ et en particulier au nombre de classes d'idéaux

de ce corps quadratique. On se tournera vers un cours de théorie algébrique des nombres pour aborder ce sujet.

4.4 Théorème des nombres premiers en progressions arithmétiques

Tout comme l'on a défini et utilisé la fonction ψ à la place de π, on fera usage ici de : $\psi(x,q,a) = \sum_{\substack{n\leq x \\ n=a \pmod q}} \Lambda(n)$.

On a, à q fixé et $x \to \infty$, $\psi(x,q,a) \sim x/\phi(q)$. Un des problèmes majeurs de la théorie analytique des nombres réside dans l'obtention d'un tel résultat quand q tend vers l'infini.

Lors de l'étude du théorème des nombres premiers, l'obtention d'une région sans zéros pour la fonction ζ s'est avérée capitale. Ce sont les fonctions L qui jouent ce rôle dans le théorème des nombres premiers en progressions arithmétiques.

Lemme 6 *Soit* $\mathcal{L}_q(s) = \prod_{\chi \bmod q} L(s,\chi)$.
Il existe une constante positive c_1 *telle que* $\mathcal{L}_q(s)$ *n'ait aucun zéro dans la région* $\sigma \geq 1 - \frac{c_1}{\log q(|\tau|+2)}$, *sauf au plus un zéro* β *qui serait réel et associé à un caractère réel* χ^* *; De plus il existe une constante* $c_2 > 0$ *telle que* $|L(s,\chi)|$, $|\frac{L'}{L}(s,\chi)|$, $|\frac{1}{L}(s,\chi)|$ *soient* $\leq c_2 \log q(|\tau|+2)$ *dans cette région sauf pour* $\chi = \chi^*$.
Pour $\chi = \chi^*$, *s'il existe, on a la même majoration pour* $|L(s,\chi^*)|$, $|\frac{L'}{L}(s,\chi^*) - \frac{1}{s-\beta}|$, $|\frac{1}{L(s,\chi^*)(x-\beta)}|$.

On appelle couramment l'éventuel zéro (lié à la région "sans zéros" précisée) le zéro exceptionnel ou zéro de Siegel, que l'on notera systématiquement β (attention au fait qu'il y a éventuellement un zéro pour chaque q !) ; on notera également $\delta = 1 - \beta$.

Théorème 6 (des nombres premiers de Gallagher (1970)) *1) Soit* $q \geq 1$ *tel qu'il n'existe pas de zéro exceptionnel. Il existe une constante effective* c_1 *telle que :*

$$\psi(x,q,a) = \frac{x}{\phi(q)} + \mathcal{O}(\frac{x}{\phi(q)} e^{-c_1\sqrt{\log x}})$$

pour $q \leq e^{\sqrt{\log x}}$.

2) Soit $q \geq 1$ *tel qu'il existe un zéro exceptionnel* β. *Il existe une constante*

effective c_1 telle que

$$\psi(x,q,a) = \frac{x}{\phi(q)}(1 - \frac{\chi^*(a)}{\beta}x^{-\delta}) + \mathcal{O}(\frac{x}{\phi(q)}\delta e^{-c_1\sqrt{\log x}})$$

pour $q \leq e^{\sqrt{\log x}}$.

Corollaire 1 *Il existe une constante $c_3 > 0$ telle que pour tout $q \geq 1$ pour lequel il n'existe pas de zéro exceptionnel, on ait : pour tout a premier à q, il existe un nombre premier $p = a \pmod q$ et $p \leq q^{c_3}$.*

Ce dernier résultat a en fait été démontré inconditionnellement par Linnik en 1944.

Remarque. Attardons-nous ici sur le caractère effectif de telles estimations. Par *effectif*, on entend un résultat dont on *peut* numériquement calculer la constante qui apparaît dans le terme d'erreur — calcul numérique dont on se dispense parfois, l'on fait alors usage de la traditionnelle notation $\mathcal{O}$ ou bien "il existe une constante..." ! Il est important de noter que de tels résultats sont bel et bien utilisables en pratique : si l'on fixe par exemple $q = 10000$, on saura trouver une borne en delà de laquelle on peut trouver un $p = a \pmod q$.
A l'inverse, des résultats *non effectifs* (i.e. dont on ne peut calculer les constantes qui interviennent mais seulement en établir l'existence) ne sont d'aucun usage pratique et ne fournissent ainsi que des renseignements qualitatifs.

A titre d'exemple, une seconde de réflexion montre que l'assertion suivante est vraie :
Il existe une constante C telle que l'existence de p, $p+2$ paire de nombres premiers jumeaux avec $p > C$ implique que l'ensemble des nombres premiers jumeaux est infini.
Démontrer l'infinité de nombres premiers jumeaux revient ... à calculer effectivement cette constante C ! Ce genre d'énoncé, vide de tout contenu, montre qu'un résultat avec une constante ineffective n'est parfois d'aucune utilité.

Idée de la démonstration. On a par la formule de décomposition (4.4) :

$$\psi(x,q,a) = \sum_{n\leq x}\Lambda(n)\mathbf{1}_{a,q}(n) = \sum_{n\leq x}\Lambda(n)\frac{1}{\phi(q)}\sum_{\chi \bmod q}\overline{\chi(a)}\chi(n)$$

$$= \frac{1}{\phi(q)}\sum_{\chi \bmod q}\overline{\chi(a)}\underbrace{\sum_{n\leq x}\Lambda(n)\chi(n)}_{\psi(x,\chi)} \quad (4.7)$$

La série de Dirichlet associée à $n \mapsto \Lambda(n)\chi(n)$ est $\sum_n \Lambda(n)\chi(n)/n^s = -L'/L(s,\chi)$ (cette identité se montre de même que pour ζ, c'est-à-dire par dérivation logarithmique et par la formule du produit eulérien pour L).

On obtient la formule sommatoire de ses coefficients $\psi(x,\chi)$ au moyen des formules de Perron :

$$\psi(x,\chi) = -\frac{1}{2i\pi}\int_{c-iT}^{c+iT} \frac{L'}{L}(s,\chi)\frac{x^s}{s}ds + \mathcal{O}(\ldots)$$

On fait alors la somme sur les différents caractères pour obtenir $\psi(x,q,a)$. L'étape suivante consiste bien sûr à déplacer la droite d'intégration de l'autre côté de la droite $\Re e\, s = 1$.

Le domaine sans zéros des fonctions L nous assure que $L'/L(s,\chi)$ est holomorphe, sauf pour $\chi = \chi_0$: dans ce cas l'égalité $L(s,\chi_0) = \zeta(s)\prod_{p|q}(1-1/p^s)$ amène un résidu de x pour $\frac{L'}{L}(s,\chi_0)\frac{x^s}{s}$.

Remarque. A propos du zéro/caractère exceptionnel lié à la région sans zéros précisée plus haut, on sait montrer que (voir [Pin76] pour les références respectives) :

- $$\beta \leq 1 - \frac{1}{\sqrt{q}}$$
  (Haneke, 1973/76),
- $$L(1,\chi) \gg \frac{1}{q^\varepsilon},$$
  où la constante impliquée est ineffective (Siegel, 1935),
- $$L(1,\chi) \geq \frac{\varepsilon}{10q^\varepsilon}$$
  pour tout χ primitif, sauf au plus un (Tatuzawa, 1951).

Chapitre 5

Théorème principal

Nous sommes à présent en mesure de préciser le lien entre une amélioration du théorème de Brun-Titchmarsh et une amélioration du théorème de nombres premiers en progressions arithmétiques.

Une version améliorée de l'inégalité de Brun-Titchmarsh serait d'obtenir pour un certain $\xi > 0$:

$$\sum_{\substack{x \leq p \leq x+y \\ p=\ell \pmod q}} 1 \leq (2-\xi)\frac{y}{\phi(q)\log(y/q)}$$

pour $q \geq 2$ et ℓ des entiers premiers entre eux, avec des conditions sur q et x.

Nous allons utiliser une version un peu plus faible de cette conjecture, n'utilisant pas l'aspect "petit intervalle" :

Hypothèse 1 *Il existe une constante $\xi > 0$ et une constante c, telles que pour $q \geq 2$ et ℓ des entiers premiers entre eux, et $q \leq (\log x)^c$, on ait :*

$$\sum_{\substack{x \leq p \leq 2x \\ p=\ell \pmod q}} 1 \leq \frac{2-\xi}{\phi(q)} \sum_{x \leq p \leq 2x} 1$$

Théorème 7 *Les problèmes suivants sont équivalents, pour c fixé :*
1) Démontrer l'hypothèse (1) pour $q \leq (\log x)^{c-\varepsilon}$ $(\forall \varepsilon > 0)$
2) Rendre effectif $L(1,\chi) \gg \frac{1}{q^{1/(c-\varepsilon)}}$ $(\forall \varepsilon > 0)$, pour tout caractère réel χ modulo q,
3) Rendre effectif $\psi(x,q,a) \sim \frac{x}{\phi(q)}$, pour $q \leq (\log x)^{c-\varepsilon}$ $(\forall \varepsilon > 0)$

Remarque.
- NB : seul 2) $\Rightarrow$ 3) nécessite réellement l'usage des $\varepsilon > 0$.

- Motohashi s'inspire d'idées semblables dans [Mot79].

Démonstration. 1) $\Rightarrow$ 2)

On reprend la démonstration donnée par [RSS96].

Sommons l'expression donnée par l'hypothèse pour les $\phi(q)/2$ classes ℓ modulo q telles que $\chi(\ell) = -1$. On a, pour x un paramètre qui sera fixé ultérieurement :

$$\sum_{\ell \text{ tel que } \chi(\ell)=-1} \sum_{x\leq p\leq 2x, p=\ell \pmod q} 1 \leq (1-\frac{\xi}{2}) \sum_{x\leq p\leq 2x} 1$$

Par conséquent le nombre de p dans $[x, 2x]$ tels que $\chi(p) = 1$ est

$$\geq \frac{\xi}{2} \sum_{x\leq p\leq 2x} 1 \gg \xi \frac{x}{\log x}$$

(où la dernière inégalité s'obtient par les estimations classiques de Tchebychev concernant $\pi(x)$).

Posons $G(s) = \zeta(s)L(s,\chi) = \sum_{n\geq 1} a_n/n^s$. On a :
- $a_n = (\mathbf{1} * \chi)(n) = \sum_{d|n} \chi(d) \geq 0$[1]
- $a_p = 1 + \chi(p) \geq 1$ pour p premier tel que $\chi(p) = 0$ ou 1.

Donc

$$\sum_{x\leq n\leq 2x} a_n \geq \sum_{x\leq p\leq 2x} a_p \gg \frac{\xi x}{\log x}.$$

Appliquons la formule de sommation donnée par le lemme (3) à la fonction $G(1+s)$, avec $c = 1$:

$$\frac{1}{2i\pi} \int_{c-i\infty}^{c+i\infty} G(s+1)\Gamma(s)((2x)^s - x^s)ds = \sum_n \frac{a_n}{n}(e^{-n/2x} - e^{-n/x})$$

$$\geq \sum_{x\leq n\leq 2x} \frac{a_n}{n}(e^{-n/2x} - e^{-n/x}) \gg \frac{1}{2x} \sum_{x\leq n\leq 2x} a_n \gg \frac{\xi}{\log x} \gg \frac{1}{q^{1/c-\varepsilon}}$$

pour $x = e^{q^{1/c-\varepsilon}}$ (car $e^{-n/2x} - e^{-n/x} \gg 1$ pour $x \leq n \leq 2x$).

En déplaçant l'intégrale jusqu'à $\Re e\, s = -\frac{1}{4}$, on obtient un résidu en 0 de $L(1,\chi)\log 2$ et donc :

$$\frac{1}{q^{1/c-\varepsilon}} \ll L(1,\chi) + x^{-1/4} \int_{1/4-i\infty}^{1/4+i\infty} |G(s+1)||\Gamma(s)|ds$$

[1] Rappelons que pour une fonction complètement multiplicative f, on a $\sum_{d|n} f(d) = \prod_{p^\nu||n}(1 + f(p) + f(p^2) + \ldots + f(p^\nu))$.

Comme $|\zeta(3/4+i\tau)| \ll |\tau|$, $|L(3/4+i\tau,\chi)| \ll q|\tau|$, et Γ se comporte comme $\ll \exp(-c|\tau|)$ $(c>0)$ sur les bandes verticales[2], on a un terme d'erreur :

$$\ll qx^{-1/4} = o\left(\frac{1}{q^{1/c-\varepsilon}}\right).$$

2) $\Rightarrow$ 3) Par le théorème des accroissements finis,

$$\frac{L(1,\chi)}{\delta} = L'(u,\chi),$$

avec $\beta \le u \le 1$. Or $L'(\sigma,\chi) = \mathcal{O}(\log^2 q)$ pour $1-1/\log q \le \sigma \le 1$ par sommation d'Abel, donc :

$$\delta \gg \frac{1}{q^{1/(c-2\varepsilon)}}$$

Donc le terme en $x^{-\delta}$ dans le théorème de Gallagher est $o(1)$ dès que $(\log x)^{c-3\varepsilon} \ge q$.

3) $\Rightarrow$ 1) est triviale, ce qui démontre le théorème. Nous donnons ici une autre preuve intéressante de l'implication

3) $\Rightarrow$ 2) L'équivalent donne $e^{-\delta \log x} = o(1)$ donc $\delta \log x \gg 1$ et finalement $\delta \ge 1/q^{1/c-\varepsilon}$ en prenant $\log x = q^{1/(c-\varepsilon)}$. D'où $L(1,\chi) \gg 1/q^{1/c-\varepsilon}$ par le résultat suivant (voir aussi [Pin76]) :

Lemme 7 (Hecke) *Si L est lié à un caractère χ modulo q ($q \ge 200$) non principal vérifiant $\delta \ge \alpha$, avec $0 < \alpha < 1/(20\log q)$, alors $L(1,\chi) \ge 0.23\alpha$.*

Démonstration. Nous utilisons le fait que l'on a, par la formule de sommation d'Euler-Maclaurin, pour $u \ge 1$ et $0 < \tau < 1$:

$$\sum_{m \le u} \frac{1}{m^{1-\tau}} = \frac{1}{\tau}(u^\tau - 1) + c_\tau + \frac{\theta}{u^{1-\tau}}$$

($|\theta| \le 1$ et $0 < c_\tau < 1$).

Soit toujours $g = \mathbf{1} * \chi \ge 0$ et remarquons que $g(m^2) \ge 1$ (voir la note 1). On a, pour $x = 100q/\alpha$:

[2] Voir la formule de Stirling complexe.

$$1,5 < \sum_{m^2 \leq x} \frac{1}{m^2} \leq \sum_{n \leq x} \frac{g(n)}{n} \leq \sum_{n \leq x} \frac{g(n)}{n^{1-\alpha}} = \sum_{d \leq x} \frac{\chi(d)}{d^{1-\alpha}} \sum_{m \leq x/d} \frac{1}{m^{1-\alpha}}$$
$$= \sum_{d \leq x} \frac{\chi(d)}{d^{1-\alpha}} \left(\frac{1}{\alpha} (\frac{x^\alpha}{d^\alpha} - 1) + c_\alpha + \frac{\theta_d d^{1-\alpha}}{x^{1-\alpha}} \right)$$
$$\leq \frac{x^\alpha}{\alpha} \sum_{d \leq x} \frac{\chi(d)}{d} + (c_\alpha - \frac{1}{\alpha}) \sum_{d \leq x} \frac{\chi(d)}{d^{1-\alpha}} + \sum_{d \leq x} \frac{1}{x^{1-\alpha}} \tag{5.1}$$

En complétant les sommes, en remarquant par sommation d'Abel que $|\sum_{d>x} \chi(d)/d^\tau| < q/x^\tau$, on a :

$$1,5 \leq \frac{x^\alpha}{\alpha} L(1,\chi) + 0,01x^\alpha + (c_\alpha - \frac{1}{\alpha}) L(1-\alpha,\chi) + 0,01x^\alpha + x^\alpha$$

Comme $c_\alpha - 1/\alpha < 0$ et $L(1-\alpha,\chi) > 0$ (car $L(1,\chi) > 0$, par continuité), on a :

$$1,5 \leq x^\alpha (\frac{L(1,\chi)}{\alpha} + 1,02)$$

Or $x^\alpha < 1,2$ d'après les conditions sur α ; on obtient alors aisément le résultat.

Bibliographie

[EMF75] W. J. Ellison and M. Mendès-France. *Les nombres premiers.* Hermann, 1975.

[Gre] B. J. Green. Notes on sieve theory. `http://www.maths.bris.ac.uk/~mabjg/expos.html`.

[HR74] H. Halberstam and H.-E. Richert. *Sieve methods.* Academic Press, 1974.

[Mot79] Y. Motohashi. A note on siegel's zeros. *Proc. Japan Acad., Ser. A*, 55 :190–192, 1979.

[Odl71] A. Odlyzko. Sieve methods, 1971. `http://www.dtc.umn.edu/~odlyzko/doc/complete.html`.

[Pin76] J. Pintz. Elementary methods in the theory of L-functions. I : Hecke's theorem. *Acta Arith.*, 31 :53–60, 1976.

[RSS96] K. Ramachandra, A. Sankaranarayanan, and K. Srinivas. Ramanujan's lattice point problem, prime number theory and other remarks. *Hardy-Ramanujan J.*, 19 :2–56, 1996.

[Ten95] G. Tenenbaum. *Introduction à la théorie analytique et probabiliste des nombres.* Cours spécialisés. SMF, 1995.

[TMF00] G. Tenenbaum and M. Mendès-France. *Les nombres premiers.* Que sais-je ? PUF, 2000.

Table des matières