Astérisque

ENRICO BOMBIERI

Le grand crible dans la théorie analytique des nombres

Astérisque, tome 18 (1974)

<http://www.numdam.org/item?id=AST_1987__18__1_0>

TABLE DES MATIÈRES

INTRODUCTION

Les notes qui suivent développent un cours donné en Mai 1973 au Collège de France sur "le grand crible".

La méthode du grand crible est, à l'heure actuelle, l'un des outils les plus puissants en théorie multiplicative des nombres. Grosso modo, on peut la définir comme l'analyse harmonique des progressions arithmétiques, aussi bien du point de vue additif que multiplicatif. Un rôle fondamental y est joué par deux inégalités (cf. th. 4, cor. 2 et th. 7, 8, 7A) que l'on peut interpréter comme des variantes de l'inégalité de Bessel pour des systèmes "presque" orthogonaux de fonctions.

Les applications à la théorie des nombres prennent deux formes :

La première, et la plus élémentaire, est la forme additive, étudiée aux §§ 2,3, qui conduit directement aux résultats arithmétiques typiques du crible de Selberg. On trouvera au §§ 0, 1 la définition d'un crible, et le théoreme de Linnik sur le plus petit non-reste quadratique mod. p ; nous avons donné aussi la formulation de Rényi du grand crible.

La seconde forme du grand crible est multiplicative ; elle concerne l'analyse harmonique relativement aux caractères $\chi(n)$ de Dirichlet ; c'est l'objet des §§ 4, 5.

La suite de ces notes est consacrée aux applications de la forme multiplicative du grand crible. Au § 6, nous démontrons un théorème de densité pour les zéros des fonctions L , et nous en déduisons le théorème de Linnik sur le plus petit nombre premier appartenant à une progression arithmétique. Une variante du théorème de densité, utilisable dans l'étude des nombres premiers appartenant à de petits intervalles, est discutée au § 10.

Le § 7 contient une démonstration simplifiée du théorème de Bombieri-Vinogradov sur la distribution des nombres premiers dans les progressions arithmétiques. Les §§ 8, 9 appliquent ce résultat au théorème de Rényi sur l'équation $p+2 = p_1 \cdots p_r$, avec $p, p_1, \ldots, p_r$ premiers ; nous donnons une démonstration simple du fait que cette équation est résoluble avec $r \leqq 4$.

Le § 11 contient des remarques bibliographiques relatives aux différentes sections.

En résumé, ces notes contiennent quelques-unes des applications les plus importantes de la méthode du grand crible : théorèmes de densité, distribution des nombres premiers dans les progressions arithmétiques, lien avec le petit crible de Brun-Selberg, etc. Toutefois, l'exposé n'a rien de systématique : je me suis borné à donner des échantillons des diverses façons dont on peut appliquer la méthode ; bien souvent aussi, pour simplifier les démonstrations, je n'ai pas donné les énoncés les plus forts possibles.

§ 0. Préliminaires.

Soient :

(a) un ensemble $\mathcal{N}$ d'entiers,
(b) un ensemble $\mathcal{P}$ de nombres premiers,
(c) pour tout $p \in \mathcal{P}$, un ensemble Ω_p de classes mod p.

Un <u>crible</u> est par définition la donnée de $(\mathcal{N}, \mathcal{P}, \Omega_p)$ et l'on s'intéresse à l'<u>ensemble criblé</u>

$$\mathcal{N}_0 = \{n \in \mathcal{N} \mid n \pmod p \notin \Omega_p \text{ pour tout } p \in \mathcal{P}\}.$$

On remarque que, dans la pratique, on prend

$$\mathcal{N} = \{M < n \leqq M+N\}$$

un intervalle de longueur N, ou

$$\mathcal{N} = \{p \leqq N\}$$

l'ensemble des nombres premiers $\leqq N$, ou

$$\mathcal{N} = \{f(n),\ n \leqq N\}$$

où f est un polynôme.

Plaçons-nous dans le premier cas, et posons

$$\omega(p) = |\Omega_p|, \quad \text{nombre d'éléments de } \Omega_p.$$

Le problème fondamental est d'obtenir des majorations et des minorations pour $|\mathcal{N}_0|$ en fonction de N, $\mathcal{P}$ et des $\omega(p)$. L'ensemble criblé $\mathcal{N}_0$ est très sensible au choix des éléments de Ω_p, comme on le voit dans les exemples suivants :

$$\text{I} \qquad \begin{cases} \mathcal{N} = (1,N) \\ \mathcal{P} = (p \leqq N) \\ \Omega_p = \{0\} \end{cases}$$

$$\text{II} \qquad \begin{cases} \mathcal{N} = (1,N) \\ \mathcal{P} = (p \leqq N) \\ \Omega_p = \begin{cases} \{0\} & \text{si } p \leqq N/2 \\ \{1\} & \text{si } N/2 < p \leqq N \end{cases} \end{cases}$$

Dans (I), $\mathcal{N}_0$ est l'ensemble des entiers $\leqq N$ qui ne sont divisibles par aucun

nombre premier $\leqq N$, et l'on a donc

$$|\eta_o| = 1 .$$

Dans (II) η_o contient tous les nombres premiers p tels que $N/2 < p \leqq N$, donc

$$|\eta_o| \sim \frac{N}{2 \log N} .$$

On a $\omega(p) = 1$ dans les deux cas ; ceci montre que l'on ne doit pas s'attendre à des résultats asymptotiques sur $|\eta_o|$ dans le cas le plus général.

Toutefois, pour des choix particuliers des Ω_p , conduisant à des ensembles criblés η_o de signification arithmétique simple, on conjecture qu'il existe une formule asymptotique pour $|\eta_o|$. Un exemple est le crible

$$\eta = (1,N)$$

$$\mathcal{P} = (p \leqq \sqrt{N})$$

$$\Omega_p = \mathcal{E} \bmod p$$

où $\mathcal{E}$ est un ensemble d'entiers fini fixé. La suite criblée η_o correspondante est essentiellement l'ensemble des entiers n tels que $\sqrt{N} < n \leqq N$ et que $n - e$ soit premier pour tout $e \in \mathcal{E}$.

Démontrer une formule asymptotique pour $|\eta_o|$ est d'habitude un problème très difficile, souvent même inabordable. L'importance de la méthode du crible est que, même si elle n'arrive presque jamais à résoudre complètement le problème en question, elle fournit le plus souvent des inégalités non triviales pour $|\eta_o|$.

§ 1. Quelques exemples. Le crible de Linnik et Renyi.

On va considérer trois exemples

Exemple 1. Le crible d'Eratosthène :

$$\begin{cases} \mathcal{A} = (1,N) \\ \mathcal{P} = (p \leqq \sqrt{N}) \\ \Omega_p = \{0\} \quad . \end{cases}$$

Il est évident que

$$\mathcal{A}_0 = 1 \cup \{\text{nombres premiers } p \text{ tels que } \sqrt{N} < p \leqq N\} \quad .$$

Exemple 2.

$$\begin{cases} \mathcal{A} = (1,N) \\ \mathcal{P} = (p \leqq \sqrt{N}) \\ \Omega_p = \{0,2\} \quad . \end{cases}$$

On voit aisément que $\mathcal{A}_0$ décrit l'ensemble des nombres premiers jumeaux dans $(\sqrt{N}, N)$.

Exemple 3.

$$\begin{cases} \mathcal{A} = (1,N) \\ \mathcal{P} = (p \leqq \sqrt{N}) \\ \Omega_p = \{a \mid a \text{ n'est pas résidu quadratique mod } p\}. \end{cases}$$

Il est clair que

$$\mathcal{A}_0 \supseteq \{\text{carrés } \leqq N\}$$

(est-il vrai qu'on a égalité si N est assez grand ?)

Les estimations du crible donnent, dans les trois cas[1]

$$|\mathcal{A}_0| \ll \frac{N}{\log N}$$

$$|\mathcal{A}_0| \ll \frac{N}{(\log N)^2}$$

$$|\mathcal{A}_0| \ll \sqrt{N} \ .$$

---

(1) On fait usage de la notation $\ll_{a,b\ldots}$ de Vinogradov pour indiquer une inégalité avec un facteur constant non specifié, qui dépend seulement des paramètres $a,b,\ldots$.

Les exemples 1 et 2 sont typiques du petit crible :

$$\omega(p) \text{ est borné,}$$

et l'exemple 3 est typique du grand crible :

$$\omega(p) \text{ croît comme } p$$

(on a $\omega(p) = \frac{p-1}{2}$ si $p > 2$).

La méthode de Viggo Brun ou de Selberg s'applique bien au petit crible. Le premier résultat sur le grand crible est dû à Linnik (1941) :

THÉORÈME 1. *Soit* $\mathcal{N} = (1,N)$, $\mathcal{P} = (p \leqq \sqrt{N})$. *Alors pour tout* τ , $0 < \tau < 1$, *on a*

$$|\mathcal{N}_o| \leqq \frac{c_o N}{\tau^2 \# \{p \in \mathcal{P} \mid \omega(p) > \tau p\}} .$$

On ne démontrera pas ici ce théorème, car on obtiendra plus loin des résultats beaucoup plus forts.

On conjecture que le plus petit non-résidu quadratique mod p est $\ll_\varepsilon p^\varepsilon$ pour tout p , et il est même $\ll (\log p)^2$ si l'hypothèse de Riemann pour les fonctions $L(s,\chi)$, χ mod p , est vraie. On sait aussi qu'il est $\ll_\varepsilon p^{1/4\sqrt{e} + \varepsilon}$, pour tout p ; la démonstration (due à Burgess) utilise l'hypothèse de Riemann pour les courbes hyperelliptiques sur $\mathbb{F}_p$.

On a l'application suivante (due aussi à Linnik) du Théorème 1 :

THÉORÈME 2. *Le nombre des nombres premiers* $p \leqq N$ *tels que le plus petit non-résidu quadratique* mod p *soit* $> N^\varepsilon$, *est borné par une constante* $c(\varepsilon)$.

COROLLAIRE. *Pour tout* $\varepsilon > 0$, *le nombre des* $p \leqq x$ *tels que le plus petit non-résidu quadratique* mod p *soit* $> p^\varepsilon$, *est majoré par*

$$\ll_\varepsilon \text{loglog } x .$$

Le corollaire montre que les exceptions à la conjecture sont très rares.

Preuve. Considérons le crible

$$\mathcal{N} = (1,N)$$
$$\mathcal{P} = \{p \leqq \sqrt{N} \mid \text{tout } b \leqq N^\varepsilon \text{ est résidu quadratique mod } p\}$$
$$\Omega_p = \{\text{non-résidus quadratiques mod } p\} .$$

On a $$\omega(p) = \frac{p-1}{2} \quad (p > 2) .$$

Soit maintenant $n \leqq N$, tel que tout facteur premier q de n satisfasse à $q \leqq N^{\varepsilon}$. Il est clair que, si $p \in \mathcal{P}$, alors n est résidu quadratique mod p, car tout diviseur premier q de n l'est. On a donc $n \in \eta_0$, autrement dit

$$\eta_0 \supseteq \eta_1$$

où

$$\eta_1 = \{n \leqq N \mid \text{tout diviseur premier } q \text{ de } n \text{ satisfait à } q \leqq N^{\varepsilon}\} .$$

Lemme. Il existe une fonction $\delta(\varepsilon) > 0$ telle que

$$|\eta_1| \sim \delta(\varepsilon) N .$$

Le Théorème 2 est conséquence immédiate du lemme, car le Théorème 1 (avec $\tau = 1/3$) donne

$$\delta(\varepsilon) N \sim |\eta_1| \leqq |\eta_0| \ll \frac{N}{|\mathcal{P}|}$$

c'est-à-dire $$|\mathcal{P}| \ll \delta(\varepsilon)^{-1} ,$$

Q.E.D.

Preuve du Lemme. Soit $R(N,z)$ le nombre des entiers $n \leqq N$ dont tous les facteurs premiers soient $\leqq z$. Si $p' < p$ sont deux nombres premiers consécutifs, on a

$$R(N,p) = \sum_{r=0}^{\infty} R\left(\frac{N}{p^r} , p'\right)$$

car tout nombre $n \leqq N$ n'ayant que des facteurs premiers $\leqq p$ s'écrit de façon unique comme $n = p^r n'$, où $n' \leqq \frac{N}{p^r}$ n'a que des facteurs premiers $\leqq p'$. Par récurrence, on voit que, si $y \leqq z$, on a

$$R(N,y) = R(N,z) - \sum_{y < p \leqq z} R\left(\frac{N}{p} , p'\right)$$

$$- \sum_{y < p \leqq z} \sum_{r=2}^{\infty} R\left(\frac{N}{p^r} , p'\right)$$

où p' est le nombre premier qui précède p.

Il est clair que la somme double est $o(N)$, car $R(N,z) \leqq N$ et

$$\sum_{p} \sum_{r=2}^{\infty} \frac{1}{p^r} < +\infty ,$$

donc

$$R(N,y) \sim R(N,z) - \sum_{y< p \leqq z} R(\frac{N}{p} ,p') .$$

Supposons trouvés un entier $k \geqq 1$ et une fonction $\delta(u)$, définie pour $u > 1/k$ et de classe C^1 , telle que la formule asymptotique

$$R(N,z) \sim \delta(\frac{\log z}{\log N})N$$

soit valable pour $\frac{\log z}{\log N} > 1/k$, avec $N \to \infty$. Nous démontrerons plus loin que la même formule asymptotique vaut encore pour $\frac{\log z}{\log N} > 1/(k+1)$, à condition de définir $\delta(u)$ dans l'intervalle $\frac{1}{k+1} < u \leqq \frac{1}{k}$ par l'équation

$$\delta(u) = 1 - \int_u^1 \delta(\frac{v}{1-v}) \frac{dv}{v} .$$

Comme, pour $k = 1$, on peut prendre $\delta(u) = 1$ pour $u > 1$, une simple récurrence sur k montrera alors que

$$R(N,z) \sim \delta(\frac{\log z}{\log N}) N$$

où la fonction $\delta(u)$ est définie par

$$\delta(u) = 1 \quad \text{si} \quad u \geqq 1$$

$$\delta(u) = 1 - \int_u^1 \delta(\frac{v}{1-v}) \frac{dv}{v} \quad \text{si} \quad 0 < u < 1 .$$

Comme $\delta(u) \geqq 0$ et $\delta'(u) = \frac{1}{u} \delta(\frac{u}{1-u})$, il est clair que $\delta(u) > 0$ pour $u > 0$ (noter que, si $\delta(u_o) = 0$, on a $\delta'(u) = 0$ pour $0 < u < u_o$), et cela complètera la démonstration du lemme.

Pour passer de k à $k+1$, nous procèderons de la manière suivante :

Soit $N^{\frac{1}{k+1} + \varepsilon} < z \leqq N^{\frac{1}{k}}$, où $\varepsilon > 0$ est fixé.

On a : $$R(N,z) \sim N - \sum_{z<p\leq N} R(\frac{N}{p},p') \ .$$

Comme $\log p' \sim \log p$ et $p > N^{\frac{1}{k+1}+\varepsilon}$, on a

$$\frac{\log p'}{\log (N/p)} > \frac{1}{k} + \frac{\varepsilon}{k} \ ,$$

et l'hypothèse de récurrence montre que

$$R(\frac{N}{p},p') = \delta(\frac{\log p'}{\log (N/p)})\frac{N}{p} + o(\frac{N}{p})$$

pour $z < p \leqq N$.
On a également

$$\sum_{z<p\leq N} \frac{1}{p} \ll \log(\frac{\log N}{\log z}) + 1 \ll 1 \ ,$$

d'où

$$R(N,z) \sim N - \sum_{z<p\leq N} \delta(\frac{\log p'}{\log (N/p)})\frac{N}{p} \ .$$

Comme $\delta(u)$ est de classe C^1 pour $u > \frac{1}{k}$, on peut remplacer $\frac{\log p'}{\log (N/p)}$ par $\frac{\log p}{\log (N/p)}$ dans la formule ci-dessus. Soit maintenant

$$A(t) = \sum_{t<p\leq N} \frac{1}{p} \ .$$

On a

$$- \sum_{z<p\leq N} \delta(\frac{\log p}{\log (N/p)})\frac{1}{p} = \int_z^N \delta(\frac{\log t}{\log (N/t)})dA(t) \ ;$$

utilisant l'estimation élémentaire

$$A(t) = \log(\frac{\log N}{\log t}) + O(\frac{1}{\log t}) \ ,$$

on trouve, après changement de variables et intégration par parties

$$\int_z^N \delta(\frac{\log t}{\log (N/t)})dA(t) \sim - \int_{\log z/\log N}^1 \delta(\frac{v}{1-v}) \frac{dv}{v} \ .$$

Ceci achève le passage de k à $k+1$, et en même temps la démonstration du lemme.

L'étape suivante est due à Rényi. On considère une suite arbitraire d'entiers

$$1 \leqq n_1 < n_2 < \ldots < n_Z \leqq N$$

et l'on pose

$$Z(p,a) = \#\{n_i \mid n_i \equiv a \pmod p\} .$$

Il est clair que

$$\sum_{a=1}^{p} Z(p,a) = Z$$

donc "en moyenne" on a

$$Z(p,a) \sim \frac{Z}{p} .$$

Si p,p' sont deux nombres premiers distincts, les congruences $n \equiv a \pmod p$ et $n \equiv a' \pmod{p'}$ sont indépendantes. Utilisant des idées tirées de la théorie des probabilités, Rényi considère la <u>variance</u>

$$V = \sum_{p \leqq X} p \sum_{a=1}^{p} \left(Z(p,a) - \frac{Z}{p}\right)^2$$

et démontre le résultat suivant :

<u>THÉORÈME 3</u>. (Rényi). <u>Si</u> $X \leqq (N/12)^{1/3}$ <u>alors</u>

$$V \leqq 2NZ .$$

Ce résultat est tantôt plus fort, tantôt plus faible, que le Théorème de Linnik. En effet, si $\{n_i\} = \eta_o$, la définition de η_o entraîne que

$$Z(p,a) = 0 \quad \text{si } a \in \Omega_p ,$$

donc on a

$$p \sum_{a=1}^{p} \left(Z(p,a) - \frac{Z}{p}\right)^2 \geqq \frac{\omega(p)}{p} Z^2$$

et

$$|\eta_o| = Z \leqq \frac{2N}{\left(\sum_{\substack{p \in \mathcal{P} \\ p \leqq (N/12)^{1/3}}} \omega(p)/p\right)} .$$

Ce résultat est visiblement plus fort que l'inégalité de Linnik, mais il a le défaut de ne s'appliquer qu'aux nombres premiers $\leqq (N/12)^{1/3}$, alors que Linnik pouvait aller jusqu'à $N^{1/2}$. Par contre, un avantage de l'inégalité de Rényi est qu'elle donne un résultat pour n'importe quelle suite, et pas seulement pour les suites criblées. A l'heure actuelle, on sait que

(i) on a pour tout X

$$V \leqq (N + X^2)Z \qquad \text{(cf. fin du § 2)} ;$$

(ii) il n'y a pas de raison de se borner à considérer une variance liée seulement aux nombres premiers. Il est plus commode d'oublier la formulation arithmétique et d'utiliser directement un résultat analytique.

§ 2. La forme analytique additive du grand crible.

On note $\|x\|$ la distance de x à $\mathbb{Z}$, autrement dit

$$\|x\| = \min_{n\in\mathbb{Z}} |x-n| .$$

Soient $x_1,\dots,x_R$ R nombres réels distincts avec

$$\min_{i\neq j} \|x_i-x_j\| \geq \delta > 0 ;$$

on dit alors que les x_i sont δ- bien espacés.

Dans la pratique, les x_i sont des nombres réels mod 1 (i.e. des éléments de $\mathbb{R}/\mathbb{Z}$), représentants de $\frac{1}{n}\mathbb{Z}/\mathbb{Z}$ ou de $\mathbb{Q}/\mathbb{Z}$.

Exemple 1. Les $x_j = j/n$, $j = 1,2,\dots,n$ forment un système de nombres $\frac{1}{n}$- bien espacés.

Exemple 2. Les nombres a/q, $(a,q) = 1$, $1 \leq a \leq q$, $q = 1,2,\dots,Q$ forment un système Q^{-2}- bien espacé.

On considère maintenant un polynôme trigonométrique

$$S(x) = \sum_{M+1}^{M+N} a_n e^{2\pi i n x}$$

de longueur N, à coefficients complexes quelconques.

THÉORÈME 4. Si les x_j sont δ-bien espacés, on a

$$\sum_{j=1}^{R} |S(x_j)|^2 \leq (N+\delta^{-1}) \sum_{M+1}^{M+N} |a_n|^2 .$$

COROLLAIRE 1. On a

$$\sum_{j=1}^{q} |S(j/q)|^2 \leq (N+q) \sum_{M+1}^{M+N} |a_n|^2 .$$

COROLLAIRE 2. On a

$$\sum_{q\leq Q} \sum_{\substack{a=1 \\ (a,q)=1}}^{q} |S(a/q)|^2 \leq (N+Q^2) \sum_{M+1}^{M+N} |a_n|^2 .$$

Remarques. Dans les applications à la théorie des nombres, on s'intéresse au cas où

$$N\delta \to \infty$$

donc $\delta^{-1} = o(N)$.

Si $N\delta \to 0$, on peut remplacer $N + \delta^{-1}$ par $\delta^{-1} + O(\delta^2 N^3)$, qui est essentiellement une estimation exacte (on démontre que la constante dans $O(...)$ est plus grande que $\frac{1}{12}$ et plus petite que 270). Dans ce dernier cas, comme

$$\lim_{\delta \to 0} \delta \sum_{j=1}^{[1/\delta]} |S(j\delta)|^2 = \int_0^1 |S(x)|^2 dx = \sum_{M+1}^{M+N} |a_n|^2 ,$$

le Théorème 4 mesure la déviation d'une somme de Riemann pour $\int_0^1 |S(x)|^2 dx$, par rapport à la valeur limite $\int_0^1 |S(x)|^2 dx$.

En fait, on démontrera ici une forme plus faible du Théorème 4, avec $N+2\delta^{-1}$ au lieu de $N+\delta^{-1}$; cela suffit d'ailleurs très bien pour les applications arithmétiques.

On commence par le

Lemme de Selberg. Soit H un espace complexe avec produit scalaire $(,)$. Soient $\varphi_1, \varphi_2, \ldots, \varphi_R$, $f \in H$. On a

$$\sum_{i=1}^{R} \frac{|(f,\varphi_i)|^2}{\sum_{j=1}^{R} |(\varphi_i,\varphi_j)|} \leq \|f\|^2 .$$

Preuve. On a, pour tout $(\xi_i) \in \mathbb{C}^R$:

$$\|f - \sum_i \xi_i \varphi_i\|^2 \geq 0 .$$

Donc

$$\|f\|^2 - 2\mathrm{Re}\Big(\sum_i \bar{\xi}_i (f,\varphi_i)\Big) + \sum_{i,j} \xi_i \bar{\xi}_j (\varphi_i,\varphi_j) \geq 0$$

et comme on a

$$|\xi_i \bar{\xi}_j| \leq \frac{1}{2} (|\xi_i|^2 + |\xi_j|^2)$$

on obtient

$$\sum_{i,j} \xi_i \bar{\xi}_j \, (\varphi_i, \varphi_j) \leqq \frac{1}{2} \sum_{i,j} (|\xi_i|^2 + |\xi_j|^2) |(\varphi_i, \varphi_j)|$$

$$= \sum_{i,j} |\xi_i|^2 \, |(\varphi_i, \varphi_j)|$$

et

$$\|f\|^2 - 2 \operatorname{Re} \sum_i \bar{\xi}_i \, (f, \varphi_i) + \sum_i |\xi_i|^2 \Big(\sum_j |(\varphi_i, \varphi_j)| \Big) \geqq 0 \, .$$

En choisissant

$$\xi_i = \frac{(f, \varphi_i)}{\sum_{j=1}^{R} |(\varphi_i, \varphi_j)|}$$

on obtient l'inégalité de Selberg,

Q.E.D.

Soit maintenant $H = \ell^2$ l'espace des suites (α_n), $n \in \mathbb{Z}$, de carré sommable, avec produit scalaire

$$(\alpha, \beta) = \sum_n \alpha_n \bar{\beta}_n \, .$$

On prend

$$f = \begin{cases} a_n & \text{si} \quad |n| \leqq N \\ 0 & \text{si} \quad |n| > N \end{cases}$$

$$\varphi_j = \begin{cases} e^{-2\pi i n x_j} & \text{si} \quad |n| \leqq N \\ \left(\frac{N+L-|n|}{L}\right)^{\frac{1}{2}} e^{-2\pi i n x_j} & \text{si} \quad N < |n| \leqq N + L \\ 0 \quad \text{si} & \text{si} \quad N + L < |n| \end{cases}$$

Il est clair que

$$\|f\|^2 = \sum_{-N}^{N} |a_n|^2 \, , \qquad (f, \varphi_j) = \sum_{-N}^{N} a_n \, e^{2\pi i n x_j} \, ;$$

on a aussi

$$(\varphi_i,\varphi_j) = \sum_{-N}^{N} e^{-2\pi i n(x_i-x_j)} + \sum_{N<|n|\leq N+L} \frac{N+L-|n|}{L} e^{-2\pi i n(x_i-x_j)}$$

$$= \frac{1}{L}\left\{\left(\frac{\sin \pi(N+L)(x_i-x_j)}{\sin \pi(x_i-x_j)}\right)^2 - \left(\frac{\sin \pi N(x_i-x_j)}{\sin \pi(x_i-x_j)}\right)^2\right\},$$

donc

$$(\varphi_i,\varphi_i) = 2N + L$$

$$|(\varphi_i,\varphi_j)| \leq \frac{1}{L \sin^2 \pi(x_i-x_j)} \quad \text{si} \quad i \neq j .$$

En utilisant l'inégalité

$$|\sin \pi x| \geq 2|x| \quad \text{pour} \quad |x| \leq \frac{1}{2}$$

on obtient

$$\sin^2 \pi(x_i-x_j) = \sin^2 \pi\|x_i-x_j\| \geq (2\|x_i-x_j\|)^2 .$$

On a $\|x_i-x_j\| \geq \delta$ si $i \neq j$, donc par le principe des tiroirs, pour tout i fixé, on a au plus deux indices j tels que $\|x_i-x_j\| \in I_\delta$ où I_δ est un intervalle donné de longueur δ. D'après les inégalités précédentes on a

$$\sum_{j=1}^{R} |(\varphi_i,\varphi_j)| = 2N + L + \sum_{j\neq i} |(\varphi_i,\varphi_j)|$$

$$\leq 2N + L + \frac{1}{4L} \sum_{\substack{j=1 \\ j\neq i}}^{R} \frac{1}{\|x_i-x_j\|^2}$$

$$\leq 2N + L + \frac{1}{4L} \sum_{k\geq 1} \frac{1}{(k\delta)^2} \#\{x_j \mid k\delta \leq \|x_i-x_j\| < (k+1)\delta\}$$

$$\leq 2N + L + \frac{1}{4L} \sum_{k=1}^{\infty} \frac{2}{(k\delta)^2} = 2N + L + \frac{\pi^2}{12} \frac{1}{L\delta^2} .$$

Jusqu'à présent, le paramètre L était un entier arbitraire. On choisit maintenant $L = [\frac{1}{\delta}] + 1$, et l'on a

$$\sum_{j=1}^{R} |(\varphi_i,\varphi_j)| \leqq 2N + 2\delta^{-1} .$$

Le Lemme de Selberg donne

$$\sum_{j=1}^{R} \Big| \sum_{-N}^{N} a_n e^{2\pi i n x_j} \Big|^2 \leqq (2N + 2\delta^{-1}) \sum_{-N}^{N} |a_n|^2$$

et l'on obtient le Théorème 4 (avec $N + 2\delta^{-1}$ au lieu de $N + \delta^{-1}$) en faisant une translation par $e^{2\pi i(N+M+1)x}$ et en remplaçant $2N + 1$ par N .

Q.E.D.

Soit $M < n_1 < n_2 < \ldots < n_Z \leqq M+N$ une suite de Z entiers dans un intervalle de longueur N . Soit

$$a_n = \begin{cases} 1 & \text{si } n = n_j \\ 0 & \text{si } n \neq n_j \end{cases}$$

la fonction caractéristique de la suite n_j . On prend

$$S(x) = \sum_{j=1}^{Z} e^{2\pi i n_j x} .$$

Si p est un nombre premier, on a

$$\sum_{a=1}^{p-1} |S(a/p)|^2 = \sum_{a=1}^{p-1} \sum_{j,h=1}^{Z} e^{2\pi i (n_j - n_h)a/p}$$

$$= p\Big(\sum_{\substack{j,h=1 \\ n_j \equiv n_h \pmod p}}^{Z} 1 \Big) - Z^2$$

$$= p \sum_{a=1}^{p} Z(p,a)^2 - Z^2$$

$$= p \sum_{a=1}^{p} \Big(Z(p,a) - \frac{Z}{p}\Big)^2 .$$

Appliquant le Corollaire 2, on trouve

$$V = \sum_{p \le X} p \sum_{a=1}^{p} (Z(p,a) - \frac{Z}{p})^2 \le (N + X^2)Z ,$$

ce qui améliore l'inégalité de Rényi.

THÉORÈME 5. On a l'inégalité

$$\sum_{q \le X} q \sum_{a=1}^{q} \left[\sum_{d|q} \frac{\mu(d)}{d} Z(\frac{q}{d},a) \right]^2 \le (N + X^2)Z .$$

Preuve.

Il suffit de démontrer que

$$\sum_{\substack{a=1 \\ (a,q)=1}}^{q} |S(\frac{a}{q})|^2 = q \sum_{h=1}^{q} \left[\sum_{d|q} \frac{\mu(d)}{d} Z(\frac{q}{d},h) \right]^2$$

où $S(x) = \sum_j e^{2\pi i n_j x}$ est le polynôme trigonométrique associé à la suite $\{n_j\}$.

On a :

$$S(\frac{a}{q}) = \sum_{h=1}^{q} Z(q,h)\, e^{2\pi i \frac{ah}{q}} ,$$

d'où

$$q\, Z(q,h) = \sum_{a=1}^{q} S(\frac{a}{q})\, e^{-2\pi i \frac{ah}{q}} .$$

Si l'on pose

$$T(q,h) = \sum_{\substack{a=1 \\ (a,q)=1}}^{q} S(\frac{a}{q})\, e^{-2\pi i \frac{ah}{q}} ,$$

il est clair que

$$q\, Z(q,h) = \sum_{d|q} T(\frac{q}{d},h) ,$$

et la formule d'inversion de Möbius donne

$$T(q,h) = q \sum_{d|q} \frac{\mu(d)}{d} Z(\tfrac{q}{d},h) \ .$$

Vu la définition de $T(q,h)$, on a donc

$$\sum_{h=1}^{q} |T(q,h)|^2 = q \sum_{\substack{a=1 \\ (a,q)=1}}^{q} |S(\tfrac{a}{q})|^2 \ ,$$

Q.E.D.

§ 3. Applications arithmétiques. Le crible de Selberg (I).

THÉORÈME 6. Soit $(\mathcal{N}, \mathcal{P}, \Omega_p)$ un crible, avec

$$\mathcal{N} = (M + 1, M + N)$$

et soit $\mathcal{Q}$ l'ensemble des $q \leqq Q$ qui sont produits de nombres premiers appartenant à $\mathcal{P}$. On a l'inégalité

$$|\mathcal{N}_o| \leqq \frac{N + Q^2}{L} ,$$

où

$$L = \sum_{q \in \mathcal{Q}} \mu^2(q) \prod_{p|q} \frac{\omega(p)}{p-\omega(p)} .$$

Remarque. La méthode de Selberg donne

$$|\mathcal{N}_o| \leqq \frac{|\mathcal{N}|}{L} + R$$

où R est un reste assez compliqué. Dans le cas $\mathcal{N} = (M + 1, M + N)$ l'estimation de R est du type $R \ll Q^2/L$, ce qui est équivalent à l'inégalité du Théorème 6. Toutefois la méthode de Selberg a l'avantage de s'appliquer à des suites $\mathcal{N}$ très générales.

Preuve. On démontrera l'inégalité

$$\Big|\sum_{\mathcal{N}_o} a_n\Big|^2 \mu^2(q) \prod_{p|q} \frac{\omega(p)}{p-\omega(p)} \leqq \sum_{\substack{a=1 \\ (a,q)=1}}^{q} |S(a/q)|^2$$

et le Théorème 6 sera une conséquence immédiate du Corollaire 2 au Théorème 4.

Soit

$$J(q) = \prod_{p|q} \frac{\omega(p)}{p-\omega(p)} ;$$

il s'agit de démontrer

$$\sum_{\substack{a=1 \\ (a,q)=1}}^{q} |S(a/q)|^2 \geqq |S(0)|^2 J(q) .$$

Si cette inégalité est valable pour tout a_n, en remplaçant a_n par

$a_n\, e^{2\pi i n\beta}$, on obtient

$$\sum_{\substack{a=1\\(a,q)=1}}^{q} |S(a/q+\beta)|^2 \geq |S(\beta)|^2\, J(q) \ .$$

Supposons avoir démontré cela pour q et q' , avec $(q,q') = 1$. Par le théorème chinois, on a

$$\sum_{\substack{c=1\\(c,qq')=1}}^{qq'} |S(c/qq')|^2 = \sum_{\substack{a=1\\(a,q)=1}}^{q} \sum_{\substack{b=1\\(b,q')=1}}^{q'} |S(\frac{a}{q} + \frac{b}{q'})|^2$$

$$\geq \sum_{\substack{b=1\\(b,q')=1}}^{q'} |S(b/q')|^2\, J(q)$$

$$\geq |S(0)|^2\, J(q)\, J(q') \ ,$$

ce qui démontre l'inégalité pour qq' . Il suffit donc de vérifier le résultat dans le cas où $q = p$, nombre premier.

Soit

$$S(p,a) = \sum_{\substack{n\in\eta_o\\ n\equiv a (\mathrm{mod}\ p)}} a_n \ ;$$

on a

$$\sum_{a=1}^{p-1} |S(a/p)|^2 = p \sum_{a=1}^{p} |S(p,a)|^2 - |S(0)|^2$$

(on a déjà vérifié cette identité dans le cas où a_n est la fonction caractéristique de η_o) et d'autre part, il est évident que $S(p,a) = 0$ si $a \in \Omega_p$. L'inégalité de Cauchy donne

$$|S(0)|^2 = |\sum_{a=1}^{p} S(p,a)|^2 \leq [p-\omega(p)] \sum_{a=1}^{p} |S(p,a)|^2 \ ,$$

donc

$$p \sum_{a=1}^{p} |S(p,a)|^2 - |S(0)|^2 \geq J(p) \; |S(0)|^2 \; .$$

Q.E.D.

COROLLAIRE. (Théorème de Brun-Titchmarsh) - Soit $\pi(x;k,\ell)$ le nombre des premiers $p \leq x$ tels que $p \equiv \ell \pmod k$, où $(k,\ell) = 1$. On a

$$\pi(M+N \; ; \; k,\ell) - \pi(M \; ; \; k,\ell) \leq \frac{2N}{\varphi(k)\log(N/k)} \left(1 + O\left(\frac{\log\log(N/k)}{\log(N/k)}\right)\right)$$

pour $M \geq 1$, $N \geq 3k$.

La constante dans $O(...)$ est absolue.

Remarques. Le résultat, avec la constante 2, est dû à Selberg. Il est important que l'inégalité ne dépende pas de M , et soit aussi valable pour k assez grand. Montgomery et Vaughan ont démontré l'inégalité plus explicite

$$\pi(M+N \; ; \; k,\ell) - \pi(M \; ; \; k,\ell) \leq \frac{2N}{\varphi(k) \; \log(N/k)} \; ,$$

valable pour $M \geq 1$, $N \geq 3k$.

Preuve du Corollaire. On prend le crible suivant

$$\mathcal{N} = \left(\frac{M+1-\ell}{k} \; , \; \frac{M+N-\ell}{k}\right)$$

qui est un intervalle de longueur $\leq \frac{N}{k} + 1$,

$$\mathcal{P} = (p \leq Q \; , \; p \nmid k)$$

(et donc $\underline{Q} = (q \leq Q \; , \; (q,k) = 1)$) ,

$$\Omega_p = \{-\ell \; k^{-1}\}$$

ce qui a un sens, car k est inversible dans $\mathbb{Z}/(p)$, $p \in \mathcal{P}$.

Si $r = kn + \ell$ est un nombre premier, $r > Q$, alors $kn + \ell \not\equiv 0 \pmod p$, c'est-à-dire

$$n \notin \Omega_p$$

et donc $n \in \mathcal{N}_o$. D'où

$$\pi(M+N \; ; \; k,\ell) - \pi(M \; ; \; k,\ell) \leq |\mathcal{N}_o| + Q \; .$$

On a par le Théorème 6

$$|\eta_o| \leqq \frac{N/k + 1 + Q^2}{L}$$

où

$$L = \sum_{q \in \underline{Q}} \mu^2(q) \prod_{p|q} \frac{\omega(p)}{p-\omega(p)}$$

$$= \sum_{\substack{q \leqq Q \\ (q,k)=1}} \frac{\mu^2(q)}{\varphi(q)} .$$

On a

$$\frac{k}{\varphi(k)} \sum_{\substack{q \leqq Q \\ (q,k)=1}} \frac{\mu^2(q)}{\varphi(q)}$$

$$= \sum_{\substack{q \leqq Q \\ (q,k)=1 \\ q \text{ sans facteur carré}}} \frac{1}{q} \prod_{p|q} \left(1 + \frac{1}{p} + \frac{1}{p^2} + \ldots\right) \prod_{p'|k} \left(1 + \frac{1}{p'} + \frac{1}{p'^2} + \ldots\right)$$

$$\geqq \sum_{n \leqq Q} \frac{1}{n} > \log Q ,$$

donc on obtient

$$L > \log Q .$$

On en conclut l'inégalité

$$\pi(M+N ; k,\ell) - \pi(M ; k,\ell) \leqq \frac{N+k+kQ^2}{\varphi(k) \log Q} + Q$$

d'où le résultat cherché, en prenant

$$Q = (N/k)^{1/2} \left(\log \frac{N}{k}\right)^{-1} .$$

§ 4. La forme multiplicative du grand crible.

Soient χ un caractère de Dirichlet, q son conducteur. On utilisera les notations suivantes :

$\sum_{\chi}^{*}$, $\sum_{\chi \bmod q}^{*}$: sommation sur les caractères primitifs de conducteur q ;

$$\tau(\chi) = \sum_{\substack{a=1 \\ (a,q)=1}}^{q} \chi(a)\, e^{2\pi i a/q} \quad : \text{somme de Gauss associée à } \chi ;$$

χ_0 : caractère principal ;

$\sum_{a}'$: sommation sur $1 \leqq a \leqq q$, $(a,q) = 1$.

THÉORÈME 7. On a l'inégalité

$$\sum_{q \leqq Q} \sum_{\chi \bmod q}^{*} \Big| \sum_{M+1}^{M+N} a_n \chi(n) \Big|^2 \leqq (N+Q^2) \sum_{M+1}^{M+N} |a_n|^2 .$$

THÉORÈME 8. Supposons que $a_n = 0$ si n a un facteur premier $\leqq Q$. On a alors

$$\sum_{q \leqq Q} (\log \tfrac{Q}{q}) \sum_{\chi \bmod q}^{*} \Big| \sum_{M+1}^{M+N} a_n \chi(n) \Big|^2 \leqq (N+Q^2) \sum_{M+1}^{M+N} |a_n|^2 .$$

Preuve. Si $(n,q) = 1$, on a pour tout $\chi \bmod q$

$$\tau(\bar{\chi})\, \chi(n) = \sum_{a}' \bar{\chi}(a)\, e^{2\pi i \frac{an}{q}} \qquad (n,q) = 1$$

et on a aussi, pour tout n et tout χ primitif $\bmod q$,

$$\tau(\bar{\chi})\, \chi(n) = \sum_{a}' \bar{\chi}(a)\, e^{2\pi i \frac{an}{q}} \qquad \chi \text{ primitif} .$$

On sait que

$$|\tau(\chi)|^2 = \begin{cases} \mu^2(q/q^*)q^* & \text{si } (q/q^*, q^*) = 1 \\ 0 & \text{si } (q/q^*, q^*) > 1 \end{cases}$$

où q^* est le conducteur du caractère primitif $\chi^* \bmod q^*$ qui induit $\chi \bmod q$. En particulier,

$$|\tau(\chi)|^2 = q \quad \text{si} \quad \chi \quad \text{est primitif} \quad \bmod q .$$

Donc on a

$$\begin{aligned}
& q \sum_{\chi \bmod q}^{*} \Big| \sum_{M+1}^{M+N} a_n \chi(n) \Big|^2 \\
&= \sum_{\chi \bmod q}^{*} \Big| \sum_{M+1}^{M+N} a_n \tau(\bar{\chi}) \chi(n) \Big|^2 \\
&= \sum_{\chi \bmod q}^{*} \Big| \sum_{M+1}^{M+N} a_n \sum_{a}^{'} \bar{\chi}(a) e^{2\pi i \frac{an}{q}} \Big|^2 \\
&\leqq \sum_{\chi \bmod q} \Big| \sum_{M+1}^{M+N} a_n \sum_{a}^{'} \bar{\chi}(a) e^{2\pi i \frac{an}{q}} \Big|^2 \\
&= \varphi(q) \sum_{a}^{'} \Big| \sum_{M+1}^{M+N} a_n e^{2\pi i \frac{an}{q}} \Big|^2 ,
\end{aligned}$$

la dernière égalité résultant de l'orthogonalité des caractères. Le Théorème 7 découle aussitôt du Corollaire 2 au Théorème 4 et de l'inégalité

$$\frac{q}{\varphi(q)} \sum_{\chi \bmod q}^{*} \Big| \sum_{M+1}^{M+N} a_n \chi(n) \Big|^2 \leqq \sum_{a}^{'} |S(a/q)|^2$$

avec $S(x) = \sum_{M+1}^{M+N} a_n e^{2\pi i n x}$, démontrée ci-dessus.

La preuve du Théorème 8 est similaire. On utilise ici l'identité pour les sommes de Gauss valable pour tout caractère χ, si $(n,q) = 1$. La condition que n n'ait pas de facteurs premiers $\leqq Q$ implique que $(n,q) = 1$ pour tout $q \leqq Q$. On obtient donc

$$\frac{1}{\varphi(q)} \sum_{\chi \bmod q} |\tau(\bar{\chi})|^2 \Big| \sum_{M+1}^{M+N} a_n \chi(n) \Big|^2 = \sum_{a}^{'} |S(a/q)|^2$$

pour tout $q \leqq Q$.

Tout caractère de Dirichlet $\chi \bmod q$ est induit par un caractère primitif

$\chi^* \bmod q^*$ et

$$\chi(n) = \chi^*(n) \quad \text{si} \quad (n,q) = 1 \ .$$

Donc

$$\sum_{q \leqq Q} \frac{1}{\varphi(q)} \sum_{\chi \bmod q} |\tau(\bar{\chi})|^2 \Big| \sum_{M+1}^{M+N} a_n \chi(n)\Big|^2$$

$$= \sum_{q \leqq Q} \frac{1}{\varphi(q)} \sum_{q^* | q} \sum_{\chi^* \bmod q^*} |\tau(\bar{\chi})|^2 \Big| \sum_{M+1}^{M+N} a_n \chi^*(n)\Big|^2$$

$$= \sum_{q \leqq Q} \frac{1}{\varphi(q)} \sum_{\substack{q^* | q \\ (q/q^*, q^*)=1}} \mu^2(q/q^*) q^* \sum_{\chi^* \bmod q^*} \Big| \sum_{M+1}^{M+N} a_n \chi^*(n)\Big|^2 \ .$$

On a $\varphi(q) = \varphi(q/q^*)\, \varphi(q^*)$ si $(q/q^*, q^*) = 1$, donc en écrivant

χ , q au lieu de χ^* , q^*

d au lieu de q/q^*

on obtient

$$\sum_{q \leqq Q} \left\{ \frac{q}{\varphi(q)} \sum_{\substack{d \leqq Q/q \\ (d,q)=1}} \frac{\mu^2(d)}{\varphi(d)} \right\} \sum_{\chi \bmod q}^{*} \Big| \sum_{M+1}^{M+N} a_n \chi(n)\Big|^2$$

$$= \sum_{q \leqq Q} \sum_{a}{}' |S(a/q)|^2 \leqq (N+Q^2) \sum_{M+1}^{M+N} |a_n|^2 \ .$$

On a déjà vérifié que

$$\frac{q}{\varphi(q)} \sum_{\substack{d \leqq X \\ (d,q)=1}} \frac{\mu^2(d)}{\varphi(d)} > \log X$$

(voir la démonstration du Corollaire au Théorème 6) ; cela complète la démonstration du Théorème 8.

Remarque. Le Corollaire au Théorème 6 se déduit aisément du Théorème 8. Si on prend $M > Q$, $a_n = 1$ si $n = p$ nombre premier, $a_n = 0$ dans les autres cas, le terme avec $q = 1$ est

$$(\log Q)\, [\pi(M+N) - \pi(M)]^2 \ ,$$

d'où

$$(\log Q)[\pi(M+N)-\pi(M)]^2 \leqq (N+Q^2)[\pi(M+N)-\pi(M)]$$

et l'inégalité du Corollaire donne

$$\pi(M+N)-\pi(M) \leqq \frac{N+Q^2}{\log Q} \ .$$

Le résultat suivant, dû à Selberg, est une généralisation des Théorèmes 7 et 8.

THÉORÈME 7A. Soit $c_r(n)$ la somme de Ramanujan $\sum_{\substack{u=1\\(u,r)=1}}^{r} e^{2\pi i n \frac{u}{r}}$. On a

$$\sum_{\substack{qr\leqq Q\\(q,r)=1}} \frac{q}{\varphi(qr)} \sum_{\chi \bmod q}^{*} \Big| \sum_{M+1}^{M+N} a_n \chi(n)\, c_r(n)\Big|^2$$

$$\leqq \sum_{q\leqq Q} \sum_{\substack{a=1\\(a,q)=1}} |S(\tfrac{a}{q})|^2 \leqq (N+Q^2) \sum_{M+1}^{M+N} |a_n|^2 \ .$$

Preuve. Soit χ un caractère primitif mod q et soit r avec $(q,r) = 1$. On a

$$\sum_{\substack{b=1\\(b,qr)=1}}^{qr} \bar{\chi}(b)\, e^{2\pi i n \frac{b}{qr}}$$

$$= \sum_{\substack{a=1\\(a,q)=1}}^{q} \sum_{\substack{u=1\\(u,r)=1}}^{r} \bar{\chi}(ra+qu)\, e^{2\pi i n \left(\frac{a}{q}+\frac{u}{r}\right)}$$

$$= \bar{\chi}(r) \left(\sum_{\substack{a=1\\(a,q)=1}}^{q} \bar{\chi}(a)\, e^{2\pi i n \frac{a}{q}} \right) \left(\sum_{\substack{u=1\\(u,r)=1}}^{r} e^{2\pi i n \frac{u}{r}} \right)$$

$$= \bar{\chi}(r)\, \chi(n)\, \tau(\bar{\chi})\, c_r(n) \ .$$

On a $|\tau(\bar{\chi})|^2 = q$, car χ est primitif mod q, et $|\bar{\chi}(r)| = 1$ car $(r,q) = 1$. On multiplie alors par a_n et on somme par rapport à n. Cela donne, après sommation sur q et r :

$$\sum_{\substack{qr\le Q\\(q,r)=1}} \frac{q}{\varphi(qr)} \sum_{\chi \bmod q}^{*} \Big| \sum_{M+1}^{M+N} a_n \chi(n)\, c_r(n)\Big|^2$$

$$= \sum_{\substack{qr\le Q\\(q,r)=1}} \frac{1}{\varphi(qr)} \sum_{\chi \bmod q}^{*} \Big| \sum_{\substack{b=1\\(b,qr)=1}}^{qr} \bar\chi(b)\, S(\tfrac{b}{qr})\Big|^2 .$$

Si χ_1 est le caractère mod qr induit par le caractère primitif χ mod q, on a

$$\chi_1(b) = \chi(b) \quad \text{pour} \quad (b,qr) = 1 .$$

La dernière somme est donc

$$\le \sum_{qr\le Q} \frac{1}{\varphi(qr)} \sum_{\chi \bmod q}^{*} \Big| \sum_{\substack{b=1\\(b,qr)=1}}^{qr} \bar\chi(b)\, S(\tfrac{b}{qr})\Big|^2$$

$$= \sum_{q\le Q} \frac{1}{\varphi(q)} \sum_{\chi \bmod q} \Big| \sum_{\substack{b=1\\(b,q)=1}}^{q} \bar\chi(b)\, S(\tfrac{b}{q})\Big|^2$$

$$= \sum_{q\le Q} \sum_{\substack{b=1\\(b,q)=1}}^{q} |S(\tfrac{b}{q})|^2 ,$$

Q.E.D.

§ 5. La forme analytique multiplicative du grand crible.

Soit $\sum_1^\infty a_n n^{it}$ une série de Dirichlet absolument convergente :

$$\sum_n |a_n| < +\infty .$$

THÉORÈME 9. Si $\tau = e^{1/T}$ on a

$$\int_{-T}^{T} |\sum_n a_n n^{it}|^2 \, dt \ll T^2 \int_0^\infty |\sum_y^{\tau y} a_n|^2 \frac{dy}{y} .$$

Ce théorème est dû à Gallagher.

Preuve. Soit, plus généralement,

$$S(t) = \sum_\nu c(\nu) e^{2\pi\nu i t} ,$$

où les exposants ν forment une suite arbitraire de nombres réels, et $\sum_\nu |c(\nu)| < +\infty$.

Posons

$$F_\delta(x) = \begin{cases} \delta^{-1} & \text{si } |x| \leq \frac{1}{2}\delta \\ 0 & \text{si } |x| > \frac{1}{2}\delta \end{cases} .$$

Il est clair que

$$C_\delta(x) \overset{\text{déf}}{=\!=} \delta^{-1} \sum_{|\nu - x| \leq \frac{1}{2}\delta} c(\nu) = \sum_\nu c(\nu) F_\delta(x-\nu) .$$

Par transformation de Fourier, cela donne :

$$\hat{C}_\delta = S \, \hat{F}_\delta ,$$

et la formule de Plancherel montre que :

$$\int_{-\infty}^{\infty} |C_\delta|^2 \, dx = \int_{-\infty}^{\infty} |S(t)\hat{F}_\delta(t)|^2 \, dt .$$

Mais

$$\hat{F}_\delta(t) = \frac{\sin \pi\delta t}{\pi\delta t} \gg 1$$

pour $|t| < \frac{1}{2\delta}$. Donc

$$\int_{-T}^{T} |S(t)|^2 \, dt \ll \int_{-\infty}^{\infty} |\delta^{-1} \sum_{x}^{x+\delta} c(\nu)|^2 \, dx$$

avec par exemple $\delta = \frac{1}{2\pi T}$. En prenant $\nu = \log n$, $n = 1,2,\ldots$ et en faisant le changement de variable $2\pi x = \log y$, on obtient le Théorème 9.

THÉORÈME 10. *Si* $\sum_n |a_n| < +\infty$ *et* $T \geqq 1$ *on a*

$$\sum_{q \leqq Q} \sum_{\chi}^{*} \int_{-T}^{T} |\sum_{1}^{\infty} a_n \chi(n) n^{it}|^2 \, dt \ll \sum_{1}^{\infty} |a_n|^2 (n+Q^2T) .$$

Preuve. Soit $\tau = e^{1/T}$. D'après le Théorème 9 on a

$$\sum_{q \leqq Q} \sum_{\chi}^{*} \int_{-T}^{T} |\sum_{1}^{\infty} a_n \chi(n) n^{it}|^2 \, dt$$

$$\ll T^2 \int_0^{\infty} \sum_{q \leqq Q} \sum_{\chi}^{*} |\sum_{y}^{\tau y} a_n \chi(n)|^2 \frac{dy}{y}$$

$$\ll T^2 \int_0^{\infty} \sum_{y}^{\tau y} |a_n|^2 [y(\tau-1)+Q^2] \frac{dy}{y} \quad \text{(Théorème 7)}$$

$$= T^2 \sum_{n} |a_n|^2 \int_{n/\tau}^{n} [y(\tau-1)+Q^2] \frac{dy}{y}$$

$$\ll \sum_{1}^{\infty} |a_n|^2 (n+Q^2T) .$$

Q.E.D.

En utilisant le Théorème 8, on obtient :

THÉORÈME 11. Soient a_n , T comme dans le Théorème 10. Supposons de plus que $a_n = 0$ si n a un facteur premier $\leqq Q$. On a alors

$$\sum_{q\leqq Q} (\text{Log}\,\frac{Q}{q}) \sum_{\chi \bmod q}^{*} \int_{-T}^{T} \Big| \sum_{1}^{\infty} a_n \chi(n) n^{it} \Big|^2 \, dt$$

$$\ll \sum_{1}^{\infty} |a_n|^2 (n+Q^2T) \ .$$

Soit Ω un ensemble fini de caractères de Dirichlet généralisés

$$\omega(n) = \chi(n) n^{it} \ .$$

On pose

$$\|\omega\| = q(|t|+1)$$

si χ est défini mod q , et

$$D = \max_{\omega,\omega' \in \Omega} \|\bar{\omega}\, \omega'\| \ .$$

Définition. On dit que Ω est δ- bien espacé si pour

$$\omega = \chi(n) n^{it} \quad , \quad \omega' = \chi'(n) n^{it'} \quad , \quad \omega,\omega' \in \Omega \text{ et } \omega \neq \omega'$$

on a

(i) ou bien $\bar{\chi}\chi'$ est non-principal

(ii) ou bien $\bar{\chi}\chi' = \chi_o$ et $|t-t'| \geqq \delta$.

Soit $\mathcal{N}$ un ensemble d'entiers,

$$\mathcal{N} \subseteq (N/2, N) \ .$$

On cherche des inégalités du type du "grand crible"

$$\sum_{\Omega} \Big| \sum_{\mathcal{N}} a_n \omega(n) \Big|^2 \leqq K \sum_{\mathcal{N}} |a_n|^2$$

avec $K = K(\mathcal{N},\Omega)$. On peut interpréter K de la façon suivante. Soient

$L^2(\mathcal{N})$: espace des suites $\{a_n\}_{n\in\mathcal{N}}$

$L^2(\Omega)$: espace des suites $\{\alpha_\omega\}_{\omega\in\Omega}$

munis du produit scalaire usuel. Définissons l'opérateur "Série de Dirichlet"

$$\mathcal{B} : L^2(\mathcal{N}) \to L^2(\Omega)$$

par la formule

$$\mathcal{B}(\{a_n\}_{n\in\mathcal{N}}) = \{\sum_{\mathcal{N}} a_n \omega(n)\}_{\omega\in\Omega} .$$

Il est clair que

$$K = \|\mathcal{B}\|^2 .$$

Plus généralement, on a

$$(\sum_{\Omega} |\sum_{\mathcal{N}} a_n \omega(n)|^q)^{1/q} \leqq \|\mathcal{B}\|_{p,q} (\sum_{\mathcal{N}} |a_n|^p)^{1/p}$$

où $\|\mathcal{B}\|_{p,q}$ est la norme de l'opérateur

$$\mathcal{B} : L^p(\mathcal{N}) \to L^q(\Omega) .$$

Il est bien connu que

$$\|\mathcal{B}\|_{p,q} = \|\mathcal{B}^*\|_{q',p'}$$

où $\mathcal{B}^*$ est l'opérateur adjoint de $\mathcal{B}$ et

$$\frac{1}{p} + \frac{1}{p'} = 1 , \quad \frac{1}{q} + \frac{1}{q'} = 1 .$$

L'opérateur adjoint $\mathcal{B}^*$ est donné par la formule

$$\mathcal{B}^*(\{\alpha_\omega\}_{\omega\in\Omega}) = \{\sum_{\Omega} \alpha_\omega \bar{\omega}(n)\}_{n\in\mathcal{N}} .$$

On peut aussi remarquer que $\log \|\mathcal{B}\|_{p,q}$ est une fonction convexe de $(\frac{1}{p}, \frac{1}{q})$ pour $p,q \geqq 1$ (Théorème de Riesz-Thorin) ; ce fait peut être utilisé pour obtenir par interpolation des majorations non triviales de $\|\mathcal{B}\|_{p,q}$. Bien que nous ne donnions ici que le cas de $\|\mathcal{B}\| = \|\mathcal{B}\|_{2,2}$, le cas général $\|\mathcal{B}\|_{p,q}$, $p,q \geqq 2$, est également important pour les applications en théorie des nombres.

Lemme. Soit $f(n)$ une fonction telle que

$$f(n) \geqq \begin{cases} 1 & \text{si } n \in \mathcal{N} \\ 0 & \text{si } n \notin \mathcal{N} \end{cases}$$

et soit

$$L(\omega) = \sum_{1}^{\infty} f(n)\omega(n) \ .$$

Alors

$$\|\mathcal{B}\|^2 \leqq \max_{\omega\in\Omega} \sum_{\omega'\in\Omega} |L(\bar{\omega}\ \omega')| \ .$$

Preuve. On a $\|\mathcal{B}\| = \|\mathcal{B}^*\|$ $(p = q = 2)$ et $\|\mathcal{B}^*\|$ est défini par l'inégalité

$$\sum_{\mathcal{H}} |\sum_{\Omega} \alpha_\omega \bar{\omega}(n)|^2 \leqq \|\mathcal{B}^*\|^2 \sum_{\Omega} |\alpha_\omega|^2 \ ;$$

il suffit donc de majorer

$$\sum_{1}^{\infty} f(n) |\sum_{\Omega} \alpha_\omega \bar{\omega}(n)|^2 \ .$$

On a

$$\sum_{1}^{\infty} f(n) |\sum_{\Omega} \alpha_\omega \bar{\omega}(n)|^2$$

$$= \sum_{\Omega\times\Omega} \alpha_\omega \bar{\alpha}_{\omega'} L(\bar{\omega}\ \omega')$$

$$\leqq \sum_{\Omega\times\Omega} \frac{1}{2} (|\alpha_\omega|^2 + |\alpha_{\omega'}|^2) |L(\bar{\omega}\ \omega')|$$

$$\leqq \max_{\omega\in\Omega} \sum_{\omega'\in\Omega} |L(\bar{\omega}\ \omega')| \sum_{\Omega} |\alpha_\omega|^2 \ ,$$

Q.E.D.

Lemme. Soit Ω un ensemble de caractères généralisés, $(4 \log D)^2$-bien espacé.

Soit $$f(n) = 3[e^{-(n/N)^k} - e^{-(2n/N)^k}]$$

avec $k = 4 \log D$. On a alors

$$|L(\bar{\omega}\omega')| \ll N \quad \text{si} \quad \omega = \omega' ;$$

$$|L(\bar{\omega}\omega')| \ll ND^{-4} \quad \text{si} \quad \omega \neq \omega' , \quad N \geq 4D(\log D)^4 ;$$

$$|L(\bar{\omega}\omega')| \ll D^{1/2}(\log D)^3 + ND^{-4} \quad \text{si} \quad \omega \neq \omega' .$$

Preuve. On a

$$L(\bar{\omega}\omega') = \frac{1}{2\pi i} \int_{(c)} L(w+i(t-t'),\bar{\chi}\chi') \, \Gamma(\tfrac{w}{k}+1) \, \frac{N^w-(N/2)^w}{w} \, dw ,$$

où

$$\int_{(c)} = \int_{c-i\infty}^{c+i\infty} , \quad \text{avec} \quad c > 1 .$$

La première inégalité du Lemme est claire, car

$$\sum_1^\infty f(n) \ll \int_0^\infty e^{-(t/N)^k} \, dt \ll N .$$

Pour la deuxième inégalité, on déforme le contour d'intégration en un nouveau contour, réunion des intervalles

$$L_{1,2} = \{w \mid u = c , \ |v| \geq (\log D)^3\}$$

$$L_{3,4} = \{w \mid \delta \leq u \leq c , \ |v| = (\log D)^3\}$$

$$L_5 = \{w \mid u = \delta , \ |v| \leq (\log D)^3\}$$

où $\delta = -k/2 = -2 \log D$. Si $\bar{\chi}\chi' = \chi_0$, il intervient un résidu égal à

$$\frac{\varphi(q)}{q} \, \Gamma(\frac{1+i(t'-t)}{k}+1) \, \frac{N^{1+i(t'-t)}-(N/2)^{1+i(t'-t)}}{1+i(t'-t)}$$

où q est le module de $\bar{\chi}\chi'$ et, vu l'hypothèse que Ω est bien espacé, on a alors

$$|t'-t| \geq (4 \log D)^2 .$$

On a aussi

$$|\Gamma(\tfrac{w}{k}+1)| \ll e^{-|v|}$$

pour $-k/2 \leqq u \leqq c$, donc la contribution du résidu est majorée par ND^{-4} . Si q est le module de $\bar{\chi}\chi'$, on a aussi

$$|L(s,\bar{\chi}\chi')| \ll \left(\frac{q(|s|+2)}{2\pi}\right)^{\frac{1}{2}-\sigma} \log[q(|s|+2)]$$

pour $\sigma \leqq 0$, avec une constante absolue dans $\ll$. Les intégrales sur $L_{1,2}$ et $L_{3,4}$ sont majorées par

$$N^c \, e^{-\frac{1}{4}(\log D)^2} (\log D)^2$$

et

$$N^c \, e^{-\frac{1}{4}(\log D)^2} (\log D)^2 + N^{\delta}\left(\frac{q(|t-t'|+2(\log D)^3}{2\pi}\right)^{\frac{1}{2}-\delta} e^{-\frac{1}{4}(\log D)^2} (\log D)^2$$

respectivement. On a

$$q(|t-t'|+2(\log D)^3) \leqq 2D(\log D)^3$$

donc

$$\left|\int_{L_{3,4}}\right| \ll D^{\frac{1}{2}}(\log D)^{\frac{3}{2}}\left(\frac{2D(\log D)^3}{2\pi N}\right)^{-\delta} e^{-\frac{1}{4}(\log D)^2} (\log D) \ll D^{-2}$$

car

$$\left(\frac{2D(\log D)^3}{2\pi N}\right)^{-\delta} \leqq \left(\frac{1}{4\pi \log D}\right)^{-\delta} = (4\pi \log D)^{-2 \log D}$$

si $N \geqq 4D (\log D)^4$. La majoration de $\left|\int_{L_5}\right|$ est similaire, et on obtient la deuxième inégalité du Lemme, en prenant $c = 1 + \frac{1}{\text{Log } N}$.

La troisième majoration est tout à fait analogue, en prenant $\delta = 0$ au lieu de $\delta = -k/2$.

Q.E.D.

THÉORÈME 12. Soit Ω un ensemble de caractères généralisés, $(4 \log D)^2$ bien espacé. On a alors

$$\|\mathcal{B}\|^2 \ll N + D (\log D)^8$$

et

$$\|\mathcal{B}\|^2 \ll N + |\Omega| D^{1/2} (\log D)^3 .$$

Preuve. On a $|\Omega| \ll D^3$, car les caractères χ sont de module $\leqq D$, et on a au plus $\leqq D$ valeurs de t pour $\omega = \chi(n) n^{it}$, d'après l'hypothèse que Ω est bien espacé. Des deux lemmes ci-dessus on déduit aisément

$$\|\mathcal{B}\|^2 \ll N + |\Omega| N D^{-4} \ll N$$

si $N \geqq 4D (\log D)^4$, et

$$\|\mathcal{B}\|^2 \ll N + |\Omega| D^{1/2} (\log D)^3$$

dans tous les cas.

Soit alors $N < 4D (\log D)^4$. On considère des nombres premiers

$$p_1 < p_2 < \ldots < p_R$$

tels que

$$4D(\log D)^4 \leqq N p_i \leqq 4D(\log D)^7$$

et

$$\prod_{i=1}^{R} p_i > D , \quad R \ll \log D ;$$

c'est toujours possible, car il y a $\gg (\log D)^2$ nombres premiers dans l'intervalle

$$\left(\frac{4D(\log D)^4}{N} , \frac{4D(\log D)^7}{N}\right) .$$

Pour tout $\omega = \chi(n) n^{it} \in \Omega$, il existe p_i tel que

$$|\omega(p_i)| = 1 ,$$

sinon on aurait $p_i | q$, où q est le module de χ, et $D < \prod_{i=1}^{R} p_i \leqq q$, ce

qui est absurde. Donc

$$\sum_{\Omega} |\sum_{\mathcal{N}} a_n \omega(n)|^2 \leqq \sum_{i=1}^{R} \sum_{\Omega} |\sum_{\mathcal{N}} a_n \omega(p_i n)|^2$$

$$= \sum_{i=1}^{R} \sum_{\Omega} |\sum_{p_i \mathcal{N}} a_n^{(i)} \omega(n)|^2$$

où $a_n^{(i)} = a_{n/p_i}$. On a $Np_i \geqq 4D(\log D)^4$, donc

$$\sum_{\Omega} |\sum_{p_i \mathcal{N}} a_n^{(i)} \omega(n)|^2 \ll Np_i \sum_{p_i \mathcal{N}} |a_n^{(i)}|^2$$

$$= Np_i \sum_{\mathcal{N}} |a_n|^2$$

$$\ll D(\log D)^7 \sum_{\mathcal{N}} |a_n|^2 ,$$

vu ce qui a déjà été démontré. On a aussi $R \ll \log D$, donc

$$\sum_{\Omega} |\sum_{\mathcal{N}} a_n \omega(n)|^2 \ll D(\log D)^8 \sum_{\mathcal{N}} |a_n|^2$$

si $N \geqq 4D(\log D)^4$,

Q.E.D.

Remarques. On a des estimations plus précises que celles fournies par la Théorème 12. La conjecture de Montgomery est

Conjecture 1. Si Ω est $(4 \log D)^2$ -bien espacé, on a

$$\|\mathcal{B}\|^2 \ll N + D^{\varepsilon}|\Omega| .$$

On conjecture aussi :

Conjecture 2. Si Ω est $(4 \log D)^2$ -bien espacé, on a

$$\|\mathcal{B}\|_{p,p} \ll (N^{1/2} + D^{1/p}) N^{1/2-1/p} (ND)^{\varepsilon} ,$$

pour tout $p \geqq 2$.

La Conjecture 2 est vraie si $p = 2k$, k entier. Ces conjectures ont beaucoup d'importance en théorie des nombres premiers.

Enfin, on remarquera que, par sommation partielle, on a encore l'inégalité

$$\sum_{\Omega} |\sum_{\eta} a_n \omega(n) n^{-\sigma_\omega}|^2 \ll \|\mathcal{B}\|_{2,2}^2 \sum_{\eta} |a_n|^2$$

pour tout $\sigma_\omega \geq 0$; cette généralisation est utilisée dans la démonstration des théorèmes de densité pour les zéros des fonctions L .

§ 6. Applications. Le théorème de Linnik.

Soit $P_{k,\ell}$ le plus petit nombre premier p dans la progression $p \equiv \ell \pmod{k}$, où $(k,\ell) = 1$. On a le résultat suivant, dû à Linnik :

THÉORÈME 13. Il existe une constante $c_o > 0$ effectivement calculable telle que

$$P_{k,\ell} \leqq k^{c_o}$$

pour tout $k \geqq 2$ et tout ℓ, $(k,\ell) = 1$.

On va déduire le Théorème de Linnik d'un théorème de densité pour les zéros des fonctions L de Dirichlet.

On commence par le

Lemme de Landau-Page. Il existe une constante $c_1 > 0$ telle que

$$L(s,\chi) \neq 0$$

pour

$$\sigma \geqq 1 - \frac{c_1}{\log T}, \quad |t| \leqq T \qquad (T \geqq 2)$$

et tout caractère primitif χ de module $q \leqq T$, avec au plus une exception

$$L(\beta_1,\chi_1) = 0.$$

Le zéro exceptionnel β_1 est réel, simple, unique et

$$\chi_1^2 = \chi_o .$$

On a aussi, pour une constante $c_2 > 0$, l'inégalité

$$1-\beta_1 \geqq \frac{c_2}{T^{1/2} \log T} .$$

(Les constantes c_1, c_2 sont effectivement calculables.)
Pour la démonstration, voir les notes bibliographiques du § 11.

On écrira

$$\delta_1 = 1-\beta_1$$

et on appellera β_1, χ_1 le zéro et le caractère exceptionnels (relatifs à T et c_1).

Soit $N(\alpha,T;\chi)$ le nombre des zéros de $L(s,\chi)$ dans

$$\alpha \leqq \sigma \leqq 1 , \quad |t| \leqq T ,$$

zéro exceptionnel exclu.

THÉORÈME 14. On a

$$\sum_{q\leqq T} \sideset{}{^*}\sum_{\chi \bmod q} N(\alpha,T;\chi) \ll T^{c_3(1-\alpha)} .$$

Si en outre il y a un zéro exceptionnel β_1 , on a

$$\sum_{q\leqq T} \sideset{}{^*}\sum_{\chi \bmod q} N(\alpha,T;\chi) \ll (\delta_1 \log T)\, T^{c_3(1-\alpha)} .$$

Les constantes implicites dans $\ll$ et c_3 sont absolues et effectivement calculables.

Remarque. Selberg a démontré que, pour $T \geqq 2$, on a

$$\sum_{q\leqq Q} \sideset{}{^*}\sum_{\chi \bmod q} N(\alpha,T;\chi) \leqq c(\varepsilon)\, (T^{3+\varepsilon}Q^{5+\varepsilon})^{1-\alpha} .$$

En particulier, la première partie du Théorème 14 est valable avec

$$c_3 = 8+\varepsilon .$$

Voici deux applications immédiates du Théorème 14 :

THÉORÈME 15. (Théorème de Siegel).
Pour tout $\varepsilon > 0$, il existe une constante $c(\varepsilon) > 0$ telle que

$$1-\beta_1 \geqq c(\varepsilon)\, T^{-\varepsilon} .$$

(La constante $c(\varepsilon)$ n'est pas effectivement calculable.)

Preuve. Soit θ la borne supérieure de la partie réelle des zéros des fonctions L de Dirichlet. Si $\theta < 1$, le Théorème 15 est évident. Supposons donc $\theta = 1$. Alors, pour tout $\varepsilon > 0$, il existe un caractère $\tilde{\chi}$ et un zéro $\tilde{\rho} = \tilde{\beta}+i\tilde{\gamma}$ de $L(x,\tilde{\chi})$ tels que

$$1-\varepsilon < \tilde{\beta} < 1 .$$

Soit $\tilde{q}$ le module de $\tilde{\chi}$, et soit

$$T \geqq \max\left(\tilde{q}, |\tilde{\gamma}|, \exp\left(\frac{c_1}{1-\tilde{\beta}}\right)\right) .$$

La condition

$$T \geqq \exp\left(\frac{c_1}{1-\tilde{\beta}}\right)$$

implique que $\tilde{\beta}$ n'est pas un zéro exceptionnel relatif à T, c_1 . On a donc

$$N(1-\varepsilon, T; \tilde{\chi}) \geqq 1$$

et l'inégalité du Théorème 14 donne

$$1 \ll (\delta_1 \log T)\, T^{c_3 \varepsilon} ,$$

c'est-à-dire

$$\delta_1 \gg (\log T)^{-1}\, T^{-c_3 \varepsilon} .$$

Q.E.D.

THÉORÈME 16. *Soit β_1 un zéro exceptionnel relatif à T, c_1 . Il existe des constantes $c_4, c_5 > 0$ telles que, si $\delta_1 \log T \leqq c_5/e$, alors*

$$L(s,\chi) \neq 0$$

pour

$$\sigma \geqq 1 - c_4 \frac{\log \frac{c_5}{\delta_1 \log T}}{\log T} , \quad |t| \leqq T \qquad (T \geqq 2)$$

et tout caractère primitif χ de module $q \leqq T$, sauf le cas où

$$L(\beta_1, \chi_1) = 0 .$$

Preuve. Si $\beta+i\gamma$ est un zéro non-exceptionnel de $L(s,\chi)$, alors

$$1 \leqq \sum_{q \leqq T} \sum_{\chi \bmod q}^{*} N(\beta, T; \chi) \ll (\delta_1 \log T)\, T^{c_3(1-\beta)} ,$$

Q.E.D.

Remarque. La démonstration usuelle du Théorème de Linnik utilise le Théorème 16 et la première partie du Théorème 14. La deuxième inégalité du Théorème 14 semble être nouvelle.

La démonstration du Théorème 14 utilise plusieurs lemmes :

Lemme de Turán. Soient $z_1,\dots,z_N \in \mathbb{C}$ et soit $K \geq N$. Il existe k, tel que $K \leq k \leq 2K$, et que

$$|z_1^k+\dots+z_N^k| \geq \left(\frac{|z_1|}{50}\right)^k .$$

Nous ne donnerons pas la preuve de ce lemme ; c'est un cas particulier du « Second Main Theorem of Turán », de démonstration fort compliquée.

Lemme de Densité. Soit $L(s,\chi)$ une fonction L où χ est un caractère de module $q \leq T$, et soit $w = 1+iv$, $|v| \leq T$ et $|v| \geq 2$ si $\chi = \chi_0$.

Alors $L(s,\chi)$ a $\ll r \log T$ zéros dans le cercle

$$|s-w| \leq r ,$$

uniformément pour

$$\frac{1}{\log T} \leq r \leq \frac{1}{4} .$$

Preuve. On a dans $|s-w| \leq \frac{1}{2}$

$$\frac{L'}{L}(s,\chi) = \sum_{|\rho-w|\leq 1} \frac{1}{s-\rho} + O(\log T) ,$$

donc

$$\sum_{|\rho-w|\leq 1} \frac{1}{w+r-\rho} = O(\log T) - \sum_n \frac{\Lambda(n)}{n^{1+r+iv}}\ \chi(n)$$

$$= O(\log T) + O(1/r) .$$

On a

$$\mathrm{Re}\ \frac{1}{w+r-\rho} \geq 0 ,$$

$$\mathrm{Re}\ \frac{1}{w+r-\rho} \geq \frac{1}{2r} \quad \text{si} \quad |\rho-w| \leq r ,$$

donc

$$\frac{1}{2r} \#\{\text{zéros dans } |s-w| \leq r\} \ll \log T + \frac{1}{r} ,$$

Q.E.D.

Posons maintenant, pour tout χ de module $q \leqq T$,

$$F(s,\chi) = \frac{L'}{L}(s,\chi)$$

s'il n'y a pas de zéro exceptionnel (relatif à T,c_1) et, dans le cas où $\beta_1 = 1-\delta_1$ est un zéro exceptionnel de $L(s,\chi_1)$, posons

$$F(s,\chi) = \frac{L'}{L}(s,\chi) + \frac{L'}{L}(s+\delta_1,\chi\chi_1) .$$

Dans la suite, on va considérer seulement le deuxième cas, qui est le plus difficile.

Il est bien connu que

$$\frac{L'}{L}(s,\chi) = \sum_{|\rho-w|<1} \frac{1}{s-\rho} - \frac{\varepsilon_\chi}{s-1} + O(\log T)$$

dans $|s-w| \leqq \frac{1}{2}$, $w = 1+iv$, $|v| \leqq T$, avec $\varepsilon_\chi = 1$ si $\chi = \chi_o$, $\varepsilon_\chi = 0$ si $\chi \neq \chi_o$. On a donc

$$F(s,\chi) = \sum \frac{1}{s-\rho} + \sum \frac{1}{s+\delta_1-\rho'} + O(\log T)$$

avec

$$|s-w| \leqq \frac{1}{2} ,$$

$$w = 1+iv , \quad |v| \leqq T , \quad \text{et} \quad |v| \geqq 2 \quad \text{si} \quad \chi = \chi_o ,$$

où la première somme est étendue aux zéros ρ de $L(s,\chi)$ avec $|\rho-w| \leqq 1$, et la deuxième somme aux zéros ρ' de $L(s,\chi\chi_1)$ avec $|\rho'-\delta_1-w| \leqq 1$. En effet, si $\chi = \chi_o$ le terme $-\frac{1}{s-1}$ correspondant au pôle de $L(s,\chi_o)$ est absorbé par le reste car $|v| \geqq 2$, et, si $\chi = \chi_1$, le pôle de $L(s+\delta_1,\chi\chi_1)$ pour $s = 1-\delta_1$ est compensé par le zéro $1-\delta_1$ de $L(s,\chi_1)$.

Lemme A. Soit $\frac{1}{\log T} \leqq r \leqq 10^{-4}$, soit $K \geqq c_6 r \log T$, $w = 1+iv$, $|v| \leqq T$, $|v| \geqq 2$ si $\chi = \chi_o$. Soit χ de module $q \leqq T$.

Si la fonction $L(s,\chi)$ a un zéro non-exceptionnel dans $|s-w| \leqq r$, il existe un entier k ,

$$K \leqq k \leqq 2K ,$$

tel que

$$\left| \frac{1}{k!} \left(\frac{d}{ds}\right)^k F(w+r,\chi) \right| \geq (200r)^{-k-1} .$$

Preuve. On a

$$F(s,\chi) = \sum_\rho \frac{1}{s-\rho} + \sum_{\rho'} \frac{1}{s+\delta_1-\rho'} + O(\log T)$$

dans $|s-w| \leq \frac{1}{2}$, donc l'inégalité de Cauchy pour les dérivées des fonctions holomorphes donne

$$(-1)^k \frac{1}{k!} \left(\frac{d}{ds}\right)^k F(s,\chi)$$

$$= \sum_\rho \frac{1}{(s-\rho)^{k+1}} + \sum_{\rho'} \frac{1}{(s+\delta_1-\rho')^{k+1}} + O(4^k \log T) .$$

Soit $s_o = w+r = 1+r+iv$ et soit $\lambda = Ar$, où $A \geq 1$ est une constante, et considérons la contribution dans $\sum_\rho \frac{1}{(s_o-\rho)^{k+1}}$ des termes avec $|w-\rho| > \lambda$. Par le Lemme de Densité, le nombre des termes avec

$$2^j\lambda < |\rho-w| \leq 2^{j+1}\lambda ,$$

est borné par $O(2^j\lambda \log T)$. On a $|s_o-\rho| \geq |w-\rho|$, donc on obtient

$$\left| \sum_{|w-\rho|>\lambda} \frac{1}{(s_o-\rho)^{k+1}} \right| \ll \sum_{j=0}^{\infty} (2^j\lambda \log T) \frac{1}{(2^j\lambda)^{k+1}}$$

$$\ll \lambda^{-k} \log T$$

pour $k \geq 1$. On a démontré que

$$(-1)^k \frac{1}{k!} \left(\frac{d}{ds}\right)^k F(s_o,\chi)$$

$$= \sum\nolimits' \frac{1}{(s_o-\rho)^{k+1}} + \sum\nolimits' \frac{1}{(s_o+\delta_1-\rho')^{k+1}} + O(\lambda^{-k} \log T)$$

si $\lambda \leq \frac{1}{4}$, les sommes étant étendues aux zéros avec

$$|\rho-w| \leq \lambda , \quad |\rho'-\delta_1-w| \leq \lambda .$$

Encore une fois par le Lemme de Densité, le nombre N de termes dans les deux sommes est

$$N \ll \lambda \log T .$$

En appliquant le Lemme de Turán, on en déduit que, si $K \geqq N$, il existe k, avec $K \leqq k \leqq 2K$, tel que

$$\left| \frac{1}{k!} \left(\frac{d}{ds}\right)^k F(s_o) \right| \geqq \left(\frac{1}{50|s_o-\rho_o|}\right)^{k+1} - O(\lambda^{-k} \log T)$$

pour n'importe quel zéro non-exceptionnel ρ_o de $L(s,\chi)$ dans $|s-w| \leqq \lambda$. S'il existe ρ_o avec $|\rho_o-w| \leqq r$, on a $|s_o-\rho_o| \leqq 2r$, donc

$$\left(\frac{1}{50|s_o-\rho_o|}\right)^{k+1} - O(\lambda^{-k} \log T) \geqq \frac{1}{(100\ r)^{k+1}} - O(\lambda^{-k} \log T) .$$

On a

$$\lambda^{-k} \log T = (Ar)^{-k} \log T = (200\ r)^{-k-1} \frac{(200)^{k+1}}{A^k}\ r \log T$$

$$\ll (200\ r)^{-k-1} \left(\frac{200}{A}\right)^k (r \log T) ,$$

et si $A > 200$

$$\left(\frac{200}{A}\right)^k \leqq \left(\frac{200}{A}\right)^K \leqq \left(\frac{200}{A}\right)^{c_6\ r \log T} ;$$

donc, avec $A \geqq 400$, on a

$$\begin{aligned} &(100\ r)^{-k-1} - O(\lambda^{-k} \log T) \\ &\geqq (100\ r)^{-k-1} - O\left((200\ r)^{-k-1} \frac{r \log T}{(2^{c_6})^{r \log T}}\right) \\ &\geqq (200\ r)^{-k-1} , \end{aligned}$$

si la constante c_6 est assez grande (car $r \log T \geqq 1$).

On avait la condition

$$\lambda = Ar \leqq \frac{1}{4} ,$$

donc $r \leqq 10^{-4}$, $A = 400$ suffit.

Q.E.D.

Lemme B. Soit $\frac{1}{\log T} \leqq r \leqq 10^{-4}$, soit $w = 1+iv$, $|v| \leqq T$, $|v| \geqq 2$ si $\chi = \chi_0$. Soit χ de module $q \leqq T$. Il existe des constantes $A \geqq 1$, $B > 0$, $C > 0$, $c_7 > 0$ avec la propriété suivante :

Si la fonction $L(s,\chi)$ a un zéro non-exceptionnel dans $|s-w| \leqq r$, alors, pour tout $x > T^B$, on a

$$\int_x^{x^A} \Big| \sum_x^y \frac{a_p}{p^w} \chi(p) \Big|^2 \frac{dy}{y} \geqq c_7 (\log x)^3 x^{-Cr},$$

où :

$a_p = \log p$ s'il n'y a pas de caractère exceptionnel,

$a_p = (\log p)[1 + \frac{\chi_1(p)}{p^{\delta_1}}]$ si χ_1 est exceptionnel et $\beta_1 = 1-\delta_1$ est le zéro exceptionnel.

Preuve. On a, pour $\sigma > 1$:

$$\frac{1}{k!} \left(\frac{d}{ds}\right)^k F(s,\chi) = \frac{(-1)^{k+1}}{k!} \sum_n \frac{\Lambda(n)}{n^s} (\log n)^k \chi(n)\, b_n$$

où $b_n = 1$ s'il n'y a pas de caractère exceptionnel, et $b_n = 1 + \frac{\chi_1(n)}{n^{\delta_1}}$ si χ_1 est exceptionnel. On pose

$$p_k(u) = \frac{1}{k!} e^{-u} u^k,$$

et par le Lemme A précédent on obtient l'inégalité

$$\Big| \sum_n \frac{\Lambda(n)}{n^w} \chi(n)\, b_n\, p_k(r \log n) \Big| \geqq r^{-1} (200)^{-k-1}$$

pour un entier k avec $K \leqq k \leqq 2K$, et tout $K \geqq c_6 r \log T$:

Il est facile de voir que

$$\begin{cases} p_k(u) \leqq (360)^{-k} & \text{si } u < 10^{-3}k \\ p_k(u) \leqq (360)^{-k} e^{-u/2} & \text{si } u > 20\,k. \end{cases}$$

On prend

$$K = r \log x ,$$

ce qui est possible si $x > T^{c_6}$, donc

$$r \log x \leqq k \leqq 2r \log x$$

et

$$r \log n < 10^{-3} k \quad \text{pour} \quad n < x^{10^{-3}}$$

$$r \log n > 20\, k \quad \text{pour} \quad n > x^{40} .$$

Par les inégalités vérifiées par la fonction $p_k(u)$, la contribution des termes avec $n < x^{10^{-3}}$, $n > x^{40}$ à la somme $\sum \frac{\Lambda(n)}{n^w} \chi(n)\, b_n\, p_k(r \log n)$, est négligeable. Donc, pour $T \geqq T_o$ et $x > T^{c_6}$, on obtient

$$\Big| \sum_{x^{10^{-3}}}^{x^{40}} \frac{\Lambda(n)}{n^w} \chi(n)\, b_n\, p_k(r \log n) \Big| \geqq \frac{1}{2}\, r^{-1}\, (200)^{-k-1} .$$

On a $p_k(u) \leqq 1$, car $\sum_{k=0}^{\infty} p_k(u) = 1$, et il est facile de voir que la contribution des $n = p^a$, $a \geqq 2$ est négligeable, donc

$$\Big| \sum_{x^{10^{-3}}}^{x^{40}} \frac{a_p}{p^w} \chi(p)\ \ p_k(r \log p) \Big| \gg r^{-1} (200)^{-k} .$$

Posons, pour simplifier l'écriture,

$$S(y) = \sum_{X}^{y} \frac{a_p}{p^w} \chi(p) ,$$

$$X = x^{10^{-3}} , \quad Y = x^{40} .$$

On a

$$\sum_{x^{10^{-3}}}^{x^{40}} \frac{a_p}{p^w} \chi(p)\, p_k(r \log p) = \int_X^Y p_k(r \log y)\, d\, S(y)$$

$$= S(Y)\, p_k(r \log Y) - \int_X^Y S(y)\, \frac{r}{y}\, p_k'(r \log y)\, dy \ .$$

On a aussi

$$p_k'(u) = p_{k-1}(u) - p_k(u) \ ,$$

donc

$$|p_k'(u)| \leqq 1$$

et comme $S(Y)$ est négligeable, on en conclut que

$$\int_X^Y |S(y)|\, \frac{dy}{y} \gg r^{-2}(200)^{-k}$$

$$\gg r^{-2}(200)^{-2r \log x}$$

$$\gg (\log x)^2\, x^{-C'r} \ ,$$

la dernière inégalité résultant de ce que $r \log x \geqq 1$, donc

$$x^{2r} = e^{2r \log x} \geqq (1+r \log x)^2 > (r \log x)^2 \ .$$

En appliquant l'inégalité de Cauchy, on voit bien que

$$\int_X^Y |S(y)|^2\, \frac{dy}{y} \gg (\log x)^3\, x^{-C'r} \ ,$$

d'où le résultat, car

$$Y = X^{40000} \ , \quad x = X^{1000} \ ,$$

Q.E.D.

Preuve du Théorème 14. Par le Lemme de Landau-Page, on peut supposer

$$\alpha \leqq 1 - \frac{c_1}{\log T} \ ,$$

car sinon on a

$$N(\alpha, T; \chi) = 0 \ .$$

Soit $\rho = \beta + i\gamma$ un zéro non-exceptionnel de $L(s,\chi)$, avec $\beta \geqq \alpha$. On prend

$$r = c_8(1-\alpha) \ , \quad c_8 \geqq 2 \ ,$$

avec $c_8 > 1/c_1$; on a $\frac{1}{\log T} \leqq r \leqq 10^{-4}$ si $\alpha > 1 - c_8^{-1}\, 10^{-4}$, ce qu'on supposera dans la suite. Alors on a

$$|\rho - (1+iv)| \leqq 1 - \beta + |\gamma - v| \leqq \frac{1}{2} r + |\gamma - v| \leqq r$$

pour $|\gamma - v| \leqq \frac{1}{2} r$. En appliquant le lemme B ci-dessus, on obtient

$$\int_x^{x^A} \int_{\gamma - \frac{1}{2}r}^{\gamma + \frac{1}{2}r} \Big| \sum_x^y \frac{a_p}{p^{1+iv}} \chi(p) \Big|^2 \, dv \, \frac{dy}{y}$$

$$\gg r \, (\log x)^3 \, x^{-Cr} \ ,$$

donc, en sommant sur les zéros ρ :

$$r \, (\log x)^3 \, x^{-Cr} \, N(\alpha, T; \chi)$$

$$\ll \int_x^{x^A} \sum_\rho \int_{\gamma - \frac{1}{2}r}^{\gamma + \frac{1}{2}r} \Big| \sum_x^y \frac{a_p}{p^{1+iv}} \chi(p) \Big|^2 \, dv \, \frac{dy}{y}$$

$$\ll (r \log T) \int_x^{x^A} \int_{-T-r}^{T+r} \Big| \sum_x^y \frac{a_p}{p^{1+iv}} \chi(p) \Big|^2 \, dv \, \frac{dy}{y} \ ,$$

la dernière inégalité provenant du fait qu'un point de l'intervalle $(-T-r, T+r)$ appartient à $\ll r \log T$ intervalles $(\gamma - \frac{1}{2}r \ , \ \gamma + \frac{1}{2}r)$, par le lemme de Densité. On en conclut aisément que

$$\sum_{q \leqq T} \sideset{}{^*}\sum_{\chi} N(\alpha, T; \chi)$$

$$\ll \frac{\log T}{(\log x)^3} \, x^{Cr} \int_x^{x^A} \sum_{q \leqq T} \sideset{}{^*}\sum_{\chi \bmod q} \int_{-T-r}^{T+r} \Big| \sum_x^y \frac{a_p}{p^{1+iv}} \chi(p) \Big|^2 \, dv \, \frac{dy}{y}$$

$$\ll \frac{x^{Cr}}{(\log x)^3} \int_x^{x^A} \sum_{q \leqq T^2} (\log \frac{T^2}{q}) \sum_\chi^* \int_{-T-r}^{T+r} \Big| \sum_x^y \frac{a_p}{p^{1+iv}} \chi(p) \Big|^2 \, dv \, \frac{dy}{y}$$

$$\ll \frac{x^{Cr}}{(\log x)^3} \int_x^{x^A} \sum_x^y \frac{|a_p|^2}{p^2} (p + T^5) \frac{dy}{y} ,$$

la dernière inégalité résultant du Théorème 11, qui est applicable si $x > T^2$, ce que l'on suppose dans la suite.

Il est clair que la contribution du terme

$$\int_x^{x^A} \sum_x^y \frac{|a_p|^2}{p^2} T^5 \frac{dy}{y}$$

est majorée par

$$\frac{T^5 \log x}{x} \sum_x^{x^A} \frac{|a_p|^2}{p} ,$$

d'où

$$\sum_{q \leqq T} \sum_\chi^* N(\alpha, T; \chi) \ll \frac{x^{Cr}}{(\log x)^2} \sum_x^{x^A} \frac{|a_p|^2}{p} ,$$

si $x > T^5$, ce que l'on suppose dans la suite.
On a vérifié que, si

$$1 - c_8^{-1} 10^{-4} \leqq \alpha \leqq 1 - \frac{c_1}{\log T} ,$$

$$x \geqq T^{\max(5,B)} ,$$

on a

$$\sum_{q \leqq T} \sum_\chi^* N(\alpha, T; \chi) \ll \frac{x^{c_9(1-\alpha)}}{(\log x)^2} \sum_x^{x^A} \frac{|a_p|^2}{p} ,$$

où

$a_p = \log p$ s'il n'y a pas de zéro exceptionnel,

$a_p = (\log p)[1 + \frac{\chi_1(p)}{p^{\delta_1}}]$ si χ_1 est le caractère exceptionnel et $\beta_1 = 1 - \delta_1$ le zéro exceptionnel. Pour compléter la démonstration du Théorème 14, on remarquera que la condition sur α n'est pas restrictive, car le Théorème 14 est trivial si $\alpha \leqq 1 - \varepsilon_o$, $\varepsilon_o > 0$ arbitraire, si l'exposant c_3 est assez grand ; il suffit donc de démontrer

Lemme C. Si $x \geq T^{c_{10}}$, on a

$$\sum_x^{x^A} \frac{|a_p|^2}{p} \ll (\log x)^2$$ s'il n'y a pas de zéro exceptionnel,

$$\sum_x^{x^A} \frac{|a_p|^2}{p} \ll \delta_1 (\log x)^3$$ si χ_1 est le caractère exceptionnel et $\beta_1 = 1 - \delta_1$ le zéro exceptionnel.

Preuve. La première partie du lemme est triviale car $|a_p|^2 \ll (\log p)^2$. Soit donc

$$a_p = (\log p)[1 + \frac{\chi_1(p)}{p^{\delta_1}}] ;$$

alors

$$a_p^2 \leqq 2(\log p)^2 (1 + \chi_1(p)) + O(\delta_1 (\log p)^3)$$

et il suffit de vérifier l'inégalité

$$\sum_{\substack{x \\ \chi_1(p)=1}}^{x^A} \frac{1}{p} \ll \delta_1 \log x .$$

Posons

$$\zeta(s) L(s,\chi_1) = \sum_n \frac{c_n}{n^s} ,$$

d'où

$$c_n = \sum_{d|n} \chi_1(d) = \prod_{p^\nu \| n} (1+\chi_1(p)+\ldots+\chi_1(p^\nu)) \ .$$

La fonction c_n est multiplicative et $c_n \geqq 0$ pour tout n, $c_p = 2$ si $\chi_1(p) = 1$.

On a

$$\Big(\sum_{n<x} \frac{c_n}{n}\Big) \Big(\sum_{\substack{x \\ \chi_1(p)=1}}^{x^A} \frac{1}{p} \Big)$$

$$\leqq \Big(\sum_{n<x} \frac{c_n}{n}\Big) \Big(\sum_{x}^{x^A} \frac{c_p}{p}\Big)$$

$$\leqq \sum_{x}^{x^{A+1}} \frac{c_m}{m} \ ,$$

car $c_n c_p = c_{np}$ si $(n,p) = 1$.

On a aussi

$$\sum_{x}^{x^{A+1}} \frac{c_m}{m} \ll L(1,\chi_1) \log x \ .$$

En effet,

$$\sum_{n\leq z} \frac{c_n}{n} = \sum_{dm\leq z} \frac{\chi_1(d)}{dm}$$

$$= \sum_{d\leq z^{1/2}} \frac{\chi_1(d)}{d} \sum_{m\leq z/d} \frac{1}{m} + \sum_{m< z^{1/2}} \frac{1}{m} \sum_{z^{1/2}<d\leq z/m} \frac{\chi_1(d)}{d}$$

$$= \sum_{d\leq z^{1/2}} \frac{\chi_1(d)}{d} \{\log \frac{z}{d} + \gamma + O(\frac{d}{z})\} + \sum_{m< z^{1/2}} \frac{1}{m} O(\frac{T}{z^{1/2}} + \frac{Tm}{z}) \ ,$$

car $\displaystyle\sum_{d> D} \frac{\chi_1(d)}{d} = \sum_{d> D} \frac{1}{d(d+1)} \sum_{u\leq d} \chi_1(u) = O(\frac{T}{D})$.

On en conclut facilement que

$$\sum_{n\leq z} \frac{c_n}{n} = L(1,\chi_1)(\log z+\gamma) + L'(1,\chi_1) + O(\frac{T \log z}{z^{1/2}})$$

et

$$\sum_{x}^{x^{A+1}} \frac{c_n}{n} = L(1,\chi_1)\, A \log x + O(\frac{T \log x}{x^{1/2}}) \ .$$

Par le Lemme de Landau-Page, on a $L(1,\chi_1) \gg T^{-\frac{1}{2}}(\log T)^{-3}$ donc le reste est négligeable si $x > T^4$, ce que l'on suppose dans la suite. On a démontré

$$\Big(\sum_{n<x} \frac{c_n}{n} \Big) \Big(\sum_{\substack{x \\ \chi_1(p)=1}}^{x^A} \frac{1}{p} \Big) \ll L(1,\chi_1) \log x \ .$$

On a, pour $k \geq 1$, l'inégalité

$$\sum_{n<x} \frac{c_n}{n} \geq x^{-\delta_1} \sum_{n<x} \frac{c_n}{n^{\beta_1}}$$

$$\geq x^{-\delta_1} \sum_{n<x} \frac{c_n}{n^{\beta_1}} (1 - \frac{n}{x})^k$$

$$= x^{-\delta_1} \frac{k!}{2\pi i} \int_{(2)} \zeta(\beta_1+w)\, L(\beta_1+w,\chi_1) \frac{x^w}{w(w+1)\ldots(w+k)}\, dw$$

$$= \frac{k!}{(1+\delta_1)\ldots(k+\delta_1)} \ \frac{1}{\delta_1} L(1,\chi_1)$$

$$+ x^{-\delta_1} \frac{k!}{2\pi i} \int_{(-\frac{1}{2})} \zeta(\beta_1+w)\, L(\beta_1+w,\chi_1) \frac{x^w}{w(w+1)\ldots(w+k)}\, dw \ ;$$

on remarquera que $L(\beta_1+w,\chi_1)\frac{1}{w}$ est régulière pour $w = 0$, et que le seul pôle de la fonction intégrée dans $\mathrm{Re}\, w \geq -\frac{1}{2}$ est $w = \delta_1$. Si $k \geq 2$ l'intégrale est absolument convergente, et elle est majorée par $\ll T x^{-1/2}$, qui est négligeable par rapport à $L(1,\chi_1)$. On a donc vérifié que

$$\sum_{n<x} \frac{c_n}{n} \gg \frac{1}{\delta_1} L(1,\chi_1)$$

et l'on a aussi

$$\Big(\sum_{n<x} \frac{c_n}{n}\Big) \Big(\sum_{\substack{x \\ \chi_1(p)=1}}^{x^A} \frac{1}{p}\Big) \ll L(1,\chi_1) \log x ,$$

d'où l'inégalité

$$\sum_{\substack{x \\ \chi_1(p)=1}}^{x^A} \frac{1}{p} \ll \delta_1 \log x ,$$

Q.E.D.

Preuve du Théorème de Linnik (Th. 13). Soit $q \leq T$. Par les formules explicites de la théorie des nombres premiers, on a

$$\sum_{\substack{p\leq x \\ p\equiv a \pmod q}} \log p = \frac{x}{\varphi(q)} - \frac{1}{\varphi(q)} \sum_{\chi \bmod q} \bar{\chi}(a) \sum_{\substack{\beta_\chi \geq 1/2 \\ |\gamma_\chi|\leq T}} \frac{x^{\rho_\chi}}{\rho_\chi}$$

$$+ O(x^{\frac{1}{2}}) + O\Big(\frac{x \log x}{T}\Big) ,$$

où ρ_χ indique les zéros de $L(s,\chi)$.

La deuxième somme est

$$- \chi_1(a) \frac{x^{\beta_1}}{\beta_1} + O\Big(\frac{1}{\varphi(q)} \sum_{q\leq T} {\sum_{\chi \bmod q}}^{*} {\sum_{|\gamma_\chi|\leq T}}' x^{\beta_\chi}\Big)$$

(on a le terme $- \chi_1(a) \frac{x^{\beta_\chi}}{\beta_1}$ seulement s'il existe un zéro exceptionnel relatif à T, c_1) où $\sum'$ ne compte pas le zéro exceptionnel. Le terme dans $O(\ldots)$ est

$$\sum_{q\leqq T} \sum_{\chi \bmod q}^{*} \sum_{|\gamma_\chi|\leqq T}{}' x^{\beta_\chi}$$

$$= -\int_{1/2-}^{1} x^{\alpha}\, d_\alpha \Sigma\Sigma N(\alpha,T;\chi)$$

$$= x^{\frac{1}{2}} \Sigma\Sigma N(\tfrac{1}{2},T;\chi) + \log x \int_{1/2}^{1} (\Sigma\Sigma N(\alpha,T;\chi))\, x^{\alpha} d\alpha$$

$$\ll x^{\frac{1}{2}} T^{5} + \log x \int_{1/2}^{1-c_1/\log T} (\Sigma\Sigma N(\alpha,T;\chi))\, x^{\alpha} d\alpha ,$$

par le lemme de Landau-Page. Par le Théorème 14 l'intégrale est majorée par

$$\ll (\delta_1 \log T)\, x^{1-c_1/\log T} \int_{1/2}^{1} \left(\frac{T^{c_3}}{x}\right)^{1-\alpha} d\alpha$$

$$\ll \frac{\delta_1 \log T}{\log (x/T^{c_3})}\, x^{1-c_1/\log T} \qquad \text{si} \quad x > T^{c_3} .$$

(on remplace $\delta_1 \log T$ par 1 s'il n'y a pas de zéro exceptionnel). Soit $x = T^{A}$, où $A \geqq c_3 + 1$. On obtient

$$\sum_{\substack{p\leqq x \\ p\equiv a \pmod q}} \log p = \frac{1}{\varphi(q)} \left(x - \chi_1(a) \frac{x^{\beta_1}}{\beta_1}\right)$$

$$+ O\left(\frac{x}{\varphi(q)} (\delta_1 \log T) \exp(-c_1 A)\right)$$

$$+ O\left(\frac{x \log x}{T}\right) + O\left(\frac{1}{\varphi(q)} x^{\frac{1}{2}} T^{5}\right) .$$

Il est facile de voir que

$$x - \chi_1(a) \frac{x^{\beta_1}}{\beta_1} \gg (\delta_1 \log T)\, x$$

et d'autre part, on a

$$\delta_1 \log T \gg T^{-1/2}$$

par le lemme de Landau-Page. Si A est assez grand, le deuxième terme est négligeable par rapport au premier. Si T est plus grand que $\varphi(q)\, T^{1/2}$, par exemple $T = q^4$, le troisième terme est aussi négligeable. Le quatrième terme est négligeable si $A \geq 12$. Donc, si $x = q^{c_o}$ et si c_o est assez grand, on voit bien que

$$\sum_{\substack{p \leq x \\ p \equiv a \pmod q}} \log p \gg \frac{x}{\varphi(q)} (\delta_1 \log T) \gg \frac{x}{\varphi(q)}\, q^{-2} ,$$

et le Théorème de Linnik est démontré.

§ 7. Applications. Le théorème des nombres premiers dans les progressions arithmétiques.

Soit

$$\psi(x;q,a) = \sum_{\substack{n\leq x \\ n\equiv a(\mathrm{mod}\ q)}} \Lambda(n) .$$

Le Théorème des Nombres Premiers donne la relation asymptotique

$$\psi(x;q,a) \sim \frac{x}{\varphi(q)} ,$$

pour q fixé et $x \to \infty$. Il serait fort utile d'avoir des résultats aussi pour $q \to \infty$. Le meilleur résultat connu valable sans exception est le

Théorème de Siegel-Walfisz. On a

$$\psi(x;q,a) = \frac{x}{\varphi(q)} + O\left(\frac{x}{(\log x)^N}\right)$$

uniformément pour $q \leq (\log x)^N$, et tout $N > 0$. La constante dans $O(\ldots)$ est effectivement calculable seulement si $N < 2$.

On a déjà obtenu une borne supérieure pour $\psi(x;q,a)$ (Théorème de Brun-Titchmarsh) valable pour $q < x$. Le résultant suivant montre que la formule asymptotique $\psi(x;q,a) \sim \frac{x}{\varphi(q)}$ est valable pour presque tous les $q \leq \frac{x^{1/2}}{(\log x)^N}$:

THÉORÈME 17. Soit $\ell = \log x$. Pour tout $A > 0$ il existe $B = B(A) > 0$ tel que

$$\sum_{q\leq x^{1/2}\ell^{-B}} \max_{y\leq x} \max_{(a,q)=1} \left|\psi(y;q,a) - \frac{y}{\varphi(q)}\right| \ll x\,\ell^{-A} .$$

La constante B est explicite (par exemple $B = 24A + 46$) mais la constante dans $\ll$ n'est pas effectivement calculable.

Remarque. Le Théorème 17 est dû à Bombieri et A.I. Vinogradov. On va donner ici une modification d'une démonstration de Gallagher, qui utilise directement le grand crible, sans passer par l'intermédiaire des théorèmes de densité.

On démontre le théorème en plusieurs étapes :

1. Réduction à $\psi_k(x;\chi)$.

Soient

$$\psi_k(x;q,a) = \frac{1}{k!} \sum_{n\le x} \Lambda(n)\,\chi(n)\,(\log\frac{x}{n})^k$$

$$\psi_k(x,\chi) = \frac{1}{k!} \sum_{\substack{n\le x\\ n\equiv a(\mathrm{mod}\ q)}} \Lambda(n)\,(\log\frac{x}{n})^k .$$

Il est clair que

$$\psi_k(x;q,a) = \frac{1}{\varphi(q)} \sum_{\chi \bmod q} \bar\chi(a)\ \psi_k(y,\chi) ,$$

donc

$$\sum_{q\le x^{1/2}\ell^{-B}} \max_{y\le x} \max_{(a,q)=1} |\psi_k(y;q,a) - \frac{\psi_k(y,\chi_o)}{\varphi(q)}|$$

$$\le \sum_{q\le x^{1/2}\ell^{-B}} \frac{1}{\varphi(q)} \max_{y\le x} \sum_{\chi\ne\chi_o} |\psi_k(y,\chi)| .$$

Si $\chi^* \bmod q^*$ est le caractère primitif qui induit $\chi \bmod q$ (et donc $q^*|q$), on a

$$|\psi_k(y,\chi)| = |\psi_k(y,\chi^*)| + O(\ell^{k+2}) .$$

On a aussi

$$\sum_{\substack{q\le z\\ q^*|q}} \frac{1}{\varphi(q)} \ll \frac{1}{\varphi(q^*)} \log z ,$$

donc il suffit de majorer

$$\sum_{q\le x^{1/2}\ell^{-B}} \frac{1}{\varphi(q)} \sum_{\chi \bmod q}^{*} \max_{y\le x} |\psi_k(y,\chi)| .$$

En utilisant l'inégalité $\frac{1}{\varphi(q)} \ll \frac{\ell}{q}$ et en décomposant l'intervalle $q \leqq x^{1/2\ell - B}$ en $\ll \ell$ intervalles du type $(M,2M)$, on voit que l'expression ci-dessus est majorée par

$$\ell^3 \max_{Q \leqq x^{1/2\ell - B}} Q^{-1} \sum_{1 < q \leqq Q} \sum_{\chi \bmod q}^{*} \max_{y \leqq x} |\psi_k(y,\chi)| .$$

2. Application du Grand Crible.

On a la formule

$$\psi_k(y,\chi) = \frac{1}{2\pi i} \int_{(c)} -\frac{L'}{L}(s,\chi) \frac{y^s}{s^{k+1}} \, ds$$

pour $c > 1$, $k \geqq 1$. On pose maintenant

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

$$F_z = F_z(s,\chi) = \sum_{n \leqq z} \Lambda(n) \frac{\chi(n)}{n^s}$$

$$G_z = G_z(s,\chi) = \sum_{n > z} \Lambda(n) \frac{\chi(n)}{n^s}$$

$$M_z = M_z(s,\chi) = \sum_{n \leqq z} \mu(n) \frac{\chi(n)}{n^s} ,$$

et on utilise l'identité

$$-\frac{L'}{L} = G_z(1-LM_z) + F_z(1-LM_z) - L'M_z .$$

Comme $F_z(1-LM_z)$ et $L'M_z$ sont des fonctions entières à croissance polynomiale dans toute bande verticale, il est facile de voir que, si $k \geqq 1$, on a

$$\psi_k(y,\chi) = \frac{1}{2\pi i}\int_{(c)} G_z(1-LM_z)\frac{y^s}{s^{k+1}}\,ds$$

$$+\frac{1}{2\pi i}\int_{(\frac12)} F_z(1-LM_z)\frac{y^s}{s^{k+1}}\,ds$$

$$+\frac{1}{2\pi i}\int_{(\frac12)} -L'M_z\frac{y^s}{s^{k+1}}\,ds\ ,$$

pour tout $c > 1$.

Soit $c = 1 + \ell^{-1}$. En utilisant plusieurs fois l'inégalité

$$2|ab| \leq |a|^2 + |b|^2\ ,$$

on obtient

$$\sum_{1<q\leq Q}\ \sideset{}{^*}\sum_{\chi \bmod q}\ \max_{y\leq x}|\psi_k(y,\chi)|$$

$$\ll x\sum_{q\leq Q}\ \sideset{}{^*}\sum_{\chi \bmod q}\int_{(c)}|G_z|^2+|1-LM_z|^2\frac{|ds|}{|s|^{k+1}}$$

$$+x^{\frac12}\sum_{q\leq Q}\ \sideset{}{^*}\sum_{\chi \bmod q}\int_{(\frac12)}(1+|F_z|^2+|M_z|^2+|F_zM_z|^2+|L|^2+|L'|^2)\frac{|ds|}{|s|^{k+1}}\ .$$

Par le Théorème 10, on a

$$\sum_{q\leq Q}\ \sideset{}{^*}\sum_{\chi \bmod q}\int_{(c)}|G_z|^2\frac{|ds|}{|s|^{k+1}} \ll \sum_{n>z}\frac{\Lambda^2(n)}{n^{2c}}(n+Q^2)$$

$$\ll \sum_{n>z}\frac{(\log n)^2}{n^{2c}}(n+Q^2) \ll \ell^3+\ell^3\frac{Q^2}{z}\ .$$

On a aussi $$1 - LM_z = - \sum_{n>z} \Big(\sum_{\substack{d|n \\ d\leqq z}} \mu(d) \Big) \frac{\chi(n)}{n^s} ,$$

donc

$$\sum_{q\leqq Q} \sum_{\chi \bmod q}^{*} \int_{(c)} |1-LM_z|^2 \frac{|ds|}{|s|^{k+1}} \ll \sum_{n>z} \frac{\big(\sum_{d|n} 1 \big)^2}{n^{2c}} (n+Q^2)$$

$$\ll \ell^4 + \ell^4 \frac{Q^2}{z} .$$

Par une application immédiate du Théorème 10, on a encore

$$\sum_{q\leqq Q} \sum_{\chi \bmod q}^{*} \int_{(\frac{1}{2})} (1+|F_z|^2+|M_z|^2+|F_z M_z|^2) \frac{|ds|}{|s|^{k+1}}$$

$$\ll (z^2+Q^2)\, \ell^6 .$$

Il reste à examiner

$$\sum_{q\leqq Q} \sum_{\chi \bmod q}^{*} \int_{(\frac{1}{2})} (|L|^2+|L'|^2) \frac{|ds|}{|s|^{k+1}} ,$$

ce que l'on fait facilement en approchant L et L' par des polynômes de Dirichlet et en utilisant encore une fois le Théorème 10. Soit

$$A(x) = A(x,\chi) = \sum_{n\leqq x} \chi(n) ,$$

χ de module q , $\chi \neq \chi_o$. Il est évident que

$$|A(x)| \leqq q .$$

On a

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

$$= \sum_{1}^{U} \frac{\chi(n)}{n^s} + \int_{U+}^{\infty} x^{-s}\, d[A(x)-A(U)]$$

$$= \sum_1^U \frac{\chi(n)}{n^s} + s\int_U^\infty \frac{A(x)-A(U)}{x^{s+1}}\,dx ,$$

d'où le prolongement analytique de $L(s,\chi)$ pour $\sigma > 0$. Il est clair maintenant que

$$L(s,\chi) = \sum_1^U \frac{\chi(n)}{n^s} + O(|s|\frac{q}{U^\sigma})$$

pour $\varepsilon_o \leqq \sigma$. Si $\sigma = \frac{1}{2}$, $U = z^2$, le reste est $\ll |s|\frac{Q}{z}$, donc

$$|L(\tfrac{1}{2}+it,\chi)|^2 \ll |\sum_1^{z^2} \frac{\chi(n)}{n^{\frac{1}{2}+it}}|^2 + |s|^2\frac{Q^2}{z^2} .$$

En appliquant l'inégalité de Cauchy (pour les dérivées des fonctions holomorphes) au cercle de centre $\frac{1}{2} + it = s$ et de rayon $\frac{1}{\log U}$, on obtient

$$L'(s,\chi) = -\sum_1^U \frac{\chi(n)\log n}{n^s} + O(|s|\frac{q\log U}{U^\sigma}) ,$$

d'où

$$|L'(\tfrac{1}{2}+it,\chi)|^2 \ll |\sum_1^{z^2} \frac{\chi(n)\log n}{n^{\frac{1}{2}+it}}|^2 + |s|^2\frac{Q^2}{z^2}(\log z)^2 .$$

Par le Théorème 10, il est facile de voir que, si $k \geqq 3$, on a

$$\sum_{1<q\leqq Q} \sum_{\chi \bmod q}^{*} \int_{(\frac{1}{2})} (|L|^2+|L'|^2)\frac{|ds|}{|s|^{k+1}}$$

$$\ll (z^2+Q^2)\ell^3 + \frac{Q^4}{z^2}\ell^2 .$$

On a donc prouvé que

$$Q^{-1} \sum_{1<q\leqq Q} \sum_{\chi \bmod q}^{*} \max_{y\leqq x} |\psi_k(y,\chi)|$$

$$\ll x\ell^4Q^{-1} + x\ell^4Qz^{-1} + x^{\frac{1}{2}}\ell^6z^2Q^{-1} + x^{\frac{1}{2}}\ell^6Q + x^{\frac{1}{2}}\ell^2Q^3z^{-2} .$$

L'expression ci-dessus est $\ll x\ell^{-3-A}$ si on prend $z = Q\ell^{8+A}$ et si on limite Q à l'intervalle

$$\ell^{8+A} \leqq Q \leqq x^{\frac{1}{2}}\ell^{-25-3A} ,$$

donc, si Q satisfait à cette limitation, on (pour $k \geqq 3$)

$$\ell^3Q^{-1} \sum_{1<q\leqq Q} \sum_{\chi \bmod q}^{*} \max_{y\leqq x} |\psi_k(y,\chi)| \ll x\ell^{-A} .$$

3. Application du Théorème de Siegel.

Par le Théorème de Siegel-Walfisz on a

$$\max_{y\leqq x} |\psi_k(y,\chi)| \ll x\,\ell^{-N}$$

pour tout caractère non-principal χ , de module $q \leqq \ell^{8+A}$, et tout N . Il est évident que cela prouve encore la dernière inégalité de la section précédente pour l'intervalle

$$Q \leqq \ell^{8+A} .$$

On conclut que, avec

$$B = 3A + 25 ,$$

on a

$$\sum_{q\leqq x^{1/2}\ell^{-B}} \max_{y\leqq x} \max_{(a,q)=1} |\psi_k(y;q,a) - \frac{\psi_k(y;\chi_o)}{\varphi(q)}|$$

$$\ll x\,\ell^{-A}$$

pour $k \geqq 3$. On remarquera aussi que l'on peut remplacer $\psi_k(y;\chi_o)$ par y , par le Théorème des Nombres Premiers.

4. Conclusion.

La fonction $\psi_k(x) = \psi_k(x;q,a)$ est positive et croissante, donc pour tout $\lambda > 0$ on a

$$\frac{1}{\lambda}\int_{e^{-\lambda}x}^{x} \psi_k(t)\,\frac{dt}{t} \leqq \psi_k(x) \leqq \frac{1}{\lambda}\int_{x}^{e^{\lambda}x} \psi_k(t)\,\frac{dt}{t}\,.$$

On a aussi l'identité

$$\psi_{k+1}(x) = \int_{1}^{x} \psi_k(t)\,\frac{dt}{t}\,,$$

d'où l'on tire facilement

$$\max_{y\leq x}\ \max_{(a,q)=1} \left|\psi_k(y;q,a) - \frac{y}{\varphi(q)}\right|$$

$$\ll \lambda\,\frac{x}{\varphi(q)} + \frac{1}{\lambda}\ \max_{y\leq e^{\lambda}x}\ \max_{(a,q)=1} \left|\psi_{k+1}(y;q,a) - \frac{y}{\varphi(q)}\right|\,.$$

Si $\lambda = \ell^{-\frac{1}{2}(A+1)}$, on voit que, si $x\,\ell^{-A}$ est une borne supérieure pour les sommes des ψ_k, alors $x\,\ell^{-\frac{1}{2}(A-1)}$ est une borne supérieure pour les sommes avec les ψ_{k-1}. En commençant avec $k = 3$, et $8A + 7$ au lieu de A (donc $B = 24A + 46$), on obtient bien le Théorème 17.

[Noter que l'argument du n° 2, à la différence de celui de Gallagher, n'utilise pas la borne de Pólya - Vinogradov $\left|\sum_{n\leq x} \chi(n)\right| \ll \sqrt{q}\,\log q$; la borne triviale $\left|\sum_{n\leq x} \chi(n)\right| \leq q$ suffit.]

§ 8. Le crible de Selberg (II).

Soient $\mathcal{N}$ un ensemble d'entiers et $\mathcal{N}_d$ le sous-ensemble

$$\mathcal{N}_d = \{n \in \mathcal{N} \mid n \equiv 0 \pmod{d}\} .$$

On supposera que

$$|\mathcal{N}_d| = \frac{1}{f(d)} |\mathcal{N}| + R_d$$

où $f(n)$ est une fonction multiplicative, et R_d un reste. On pose

$$f_1 = f * \mu ,$$

c'est-à-dire $f_1(n) = \sum_{d|n} f(d)\mu(\frac{n}{d})$. Soit $\{\lambda_\nu\}$ une suite de nombres réels avec $\lambda_\nu = 0$ si ν est assez grand, $\lambda_\nu = 0$ si ν a un facteur carré, et soit

$$\zeta_r = \mu(r)\, f_1(r) \sum_\nu \frac{\lambda_{\nu r}}{f(\nu r)} ,$$

d'où, par la formule d'inversion de Möbius,

$$\lambda_\nu = \mu(\nu)\, f(\nu) \sum_r \frac{\mu^2(r\nu)}{f_1(r\nu)} \zeta_{r\nu} .$$

On considère la somme

$$S = \sum_{n \in \mathcal{N}} \Big(\sum_{d|n} a_d\Big)\Big(\sum_{\nu|n} \lambda_\nu\Big)^2 ,$$

et le problème de l'estimation asymptotique de S . On a le résultat suivant :

THÉORÈME 18. On a

$$S = |\mathcal{N}|\, \mathfrak{S} + O\Big(\sum_m \Big(\sum_{d|m} |a_d|\Big)\Big(\sum_{\nu|m} |\lambda_\nu|\Big)^2 |R_m|\Big)$$

où $\mathfrak{S}$ est donné par la formule

$$\mathfrak{S} = \sum_{\substack{m \\ (m,d)=1}} \sum_d \frac{\mu^2(m)}{f_1(m)} \frac{a_d}{f(d)} \Big(\sum_{r|d} \mu(r)\, \zeta_{rm}\Big)^2 .$$

Preuve. On a

$$\sum_{\eta} \Big(\sum_{d|n} a_d\Big)\Big(\sum_{\nu|n} \lambda_\nu\Big)^2$$

$$= \sum_{d} \sum_{\nu_1} \sum_{\nu_2} a_d \lambda_{\nu_1} \lambda_{\nu_2} |\eta_{[d,\nu_1,\nu_2]}|$$

où $[a,b,\dots,r]$ est le plus petit commun multiple de $a,b,\dots,r$. D'après la définition de R_d, on a donc

$$\sum_{d} \sum_{\nu_1} \sum_{\nu_2} a_d \lambda_{\nu_1} \lambda_{\nu_2} |\eta_{[d,\nu_1,\nu_2]}|$$

$$= |\eta| \sum_{d} \sum_{\nu_1} \sum_{\nu_2} \frac{a_d \lambda_{\nu_1} \lambda_{\nu_2}}{f([d,\nu_1,\nu_2])} + \sum_{d} \sum_{\nu_1} \sum_{\nu_2} a_d \lambda_{\nu_1} \lambda_{\nu_2} R_{[d,\nu_1,\nu_2]} .$$

Il est clair que

$$\Big|\sum_{d} \sum_{\nu_1} \sum_{\nu_2} a_d \lambda_{\nu_1} \lambda_{\nu_2} R_{[d,\nu_1,\nu_2]}\Big| \leqq \sum_{m} \Big(\sum_{d|m} |a_d|\Big)\Big(\sum_{\nu|m} |\lambda_\nu|\Big)^2 |R_m| ,$$

et il reste donc à prouver que

$$\mathfrak{S} = \sum_{d} \sum_{\nu_1} \sum_{\nu_2} \frac{a_d \lambda_{\nu_1} \lambda_{\nu_2}}{f([d,\nu_1,\nu_2])}$$

$$= \sum_{\substack{m \\ (m,d)=1}} \sum_{d} \frac{\mu^2(m)}{f_1(m)} \frac{a_d}{f(d)} \Big(\sum_{r|d} \mu(r)\, \zeta_{rm}\Big)^2 .$$

On a l'identité

$$\max(a,b,c) = a+b+c-\min(a,b)-\min(a,c)-\min(b,c)+\min(a,b,c)$$

d'où

$$\frac{1}{f([d,\nu_1,\nu_2])} = \frac{1}{f(d)} \frac{1}{f(\nu_1)} \frac{1}{f(\nu_2)} \frac{f((d,\nu_1))f((d,\nu_2))f((\nu_1,\nu_2))}{f((d,\nu_1,\nu_2))}$$

car f est multiplicative (on note $(a,b,\dots,r)$ le plus grand commun diviseur de $a,b,\dots,r$).

Soient maintenant

$$f_1 = f * \mu \ , \quad f_{-1} = \frac{1}{f} * \mu \ ,$$

ce qui implique

$$f((\nu_1,\nu_2)) = \sum_{\substack{r \mid \nu_1 \\ r \mid \nu_2}} f_1(r) \ ,$$

$$\frac{1}{f((d,\nu_1,\nu_2))} = \sum_{\substack{s \mid d \\ s \mid \nu_1 \\ s \mid \nu_2}} f_{-1}(s) \ .$$

On a alors

$$\sum_d \sum_{\nu_1} \sum_{\nu_2} \frac{a_d \lambda_{\nu_1} \lambda_{\nu_2}}{f([d,\nu_1,\nu_2])}$$

$$= \sum_d \sum_{\nu_1} \sum_{\nu_2} \frac{\lambda_{\nu_1} f((d,\nu_1))}{f(\nu_1)} \frac{\lambda_{\nu_2} f((d,\nu_2))}{f(\nu_2)} \frac{a_d}{f(d)} \sum_{\substack{r \mid \nu_1 \\ r \mid \nu_2}} f_1(r) \sum_{\substack{s \mid d \\ s \mid \nu_1 \\ s \mid \nu_2}} f_{-1}(s)$$

$$= \sum_r \sum_d \sum_s f_1(r) \, f_{-1}(s) \frac{a_d}{f(d)} \left(\sum_{\nu \equiv 0 (\mathrm{mod}\, [r,s])} \frac{\lambda_\nu}{f(\nu)} f((d,\nu)) \right)^2$$

car les conditions $r \mid \nu$, $s \mid \nu$ équivalent à $[r,s] \mid \nu$. Regroupant les termes avec $[r,s] = m$ donné, et posant pour simplifier l'écriture

$$y_{d,m} = \sum_{\nu \equiv 0 (\mathrm{mod}\ m)} \frac{\lambda_\nu}{f(\nu)} f((d,\nu)) \ ,$$

on obtient

$$\mathfrak{S} = \sum_m \sum_d \frac{a_d}{f(d)} \left\{ \sum_{\substack{[r,s]=m \\ s \mid d}} f_1(r) \, f_{-1}(s) \right\} y_{d,m}^2 \ .$$

Vu l'hypothèse $\lambda_\nu = 0$ si ν a un facteur carré, on a $y_{d,m} = 0$ si m a un facteur carré. On supposera donc dans la suite que m est sans facteur carré.

Lemme. Soit m sans facteur carré. On a alors

$$\sum_{\substack{[r,s]=m \\ s|d}} f_1(r)\, f_{-1}(s) = \begin{cases} f_1(m) & \text{si } (m,d) = 1 \\ 0 & \text{si } (m,d) > 1 \end{cases}$$

Preuve. Si m est sans facteur carré, la condition $[r,s] = m$ équivaut à

$$r = \frac{m}{s} \cdot t\,, \quad t|s\,, \quad s|m$$

et l'on a

$$f_1(r) = \frac{f_1(m)}{f_1(s)}\, f_1(t)\,,$$

d'où

$$\sum_{\substack{[r,s]=m \\ s|d}} f_1(r)\, f_{-1}(s)$$

$$= \sum_{\substack{s|m \\ s|d}} \frac{f_1(m)}{f_1(s)}\, f_{-1}(s) \sum_{t|s} f_1(t)$$

$$= f_1(m) \sum_{s|(m,d)} \frac{f_{-1}(s)}{f_1(s)}\, f(s)\,.$$

Si p est un nombre premier, on a

$$f_1(p) = f(p)-1\,, \quad f_{-1}(p) = \frac{1}{f(p)} - 1$$

et

$$\frac{f_{-1}(p)}{f_1(p)}\, f(p) = -1 = \mu(p)\,;$$

comme $\frac{f_{-1}}{f_1}\, f$ est multiplicative, on en déduit que $\frac{f_{-1}(s)}{f_1(s)}\, f(s) = \mu(s)$

si s est sans facteur carré. Mais on a

$$\sum_{s|n} \mu(s) = \begin{cases} 1 & \text{si } n = 1 \\ 0 & \text{si } n > 1 \end{cases},$$

ce qui complète la preuve du Lemme.

On a donc

$$\mathfrak{S} = \sum_{\substack{m \\ (m,d)=1}} \sum_{d} \frac{a_d}{f(d)} f_1(m)\, y_{d,m}^2 .$$

Pour compléter la démonstration du Théorème 18, on va exprimer les $y_{d,m}$ au moyen des $y_{1,m}$. On a en effet

$$y_{d,m} = \sum_{t} \frac{\lambda_{mt}}{f(mt)} f((d,mt))$$

et la formule d'inversion de Möbius donne donc

$$\frac{\lambda_m}{f(m)} f((d,m)) = \sum_{t} \mu(t)\, y_{d,mt}$$

$$\frac{\lambda_m}{f(m)} = \sum_{t} \mu(t)\, y_{1,mt} ,$$

d'où

$$y_{d,m} = \sum_{s,t} f((d,mt))\, \mu(s)\, y_{1,mst}$$

$$= \sum_{r} \left\{ \sum_{t|r} f((d,mt))\, \mu\left(\frac{r}{t}\right) \right\} y_{1,mr} .$$

Lemme. Si $(d,m) = 1$ et si r est sans facteur carré, on a

$$\sum_{t|r} f((d,mt))\, \mu\left(\frac{r}{t}\right) = \begin{cases} f_1(r) & \text{si } r|d \\ 0 & \text{si } r \nmid d \end{cases}$$

Preuve. On a $(d,mt) = (d,t)$ car $(d,m) = 1$. Soit alors

$$\rho = (d,r) , \quad \tau = (d,t)$$

$$r = \rho r' , \quad t = \tau t' .$$

Comme r est sans facteur carré, tout diviseur t de r s'écrit de façon unique sous la forme $t = \tau t'$, où $\tau | \rho$, $t' | r'$. On a

$$\mu(\frac{r}{t}) = \mu(\frac{\rho}{\tau}) \mu(\frac{r'}{t'}) ,$$

donc

$$\sum_{t|r} f((d,mt)) \mu(\frac{r}{t}) = \sum_{\tau|\rho} \sum_{t'|r'} f(\tau) \mu(\frac{\rho}{\tau}) \mu(\frac{r'}{t'})$$

$$= f_1(\rho) \sum_{t'|r'} \mu(\frac{r'}{t'}) = \begin{cases} f_1(\rho) & \text{si } r' = 1 \\ 0 & \text{si } r' > 1 , \end{cases}$$

et le Lemme est démontré.

On déduit de là

$$y_{d,m} = \sum_{r|d} f_1(r) y_{1,mr}$$

pour $(d,m) = 1$, et donc

$$\mathfrak{S} = \sum_{\substack{m \\ (m,d)=1}} \sum_{d} \frac{a_d}{f(d)} f_1(m) \Big(\sum_{r|d} f_1(r) y_{1,mr}\Big)^2 .$$

Utilisant la formule

$$\zeta_t = \mu(t) f_1(t) y_{1,t} ,$$

on obtient le Théorème 18.

Remarque. Le Théorème 18 généralise le résultat classique de Selberg

$$\mathfrak{S} = \sum_{m} \frac{\mu^2(m)}{f_1(m)} \zeta_m^2$$

dans le cas où $a_d = 0$ si $d > 1$, $a_1 = 1$.

§ 9. Application du crible de Selberg.

On va considérer maintenant le problème de déterminer des nombres premiers p tels que $p + 2$ ait au plus r_o facteurs premiers, avec r_o constante absolue. Le premier résultat dans cette direction est dû à Viggo Brun, qui a démontré l'existence d'une infinité d'entiers n tels que $n(n+2)$ ait au plus r_o facteurs premiers, avec r_o constante absolue. Selberg a démontré qu'il existe une infinité d'entiers n tels que n ait au plus 2, et $n+2$ au plus 3 facteurs premiers.

En combinant les méthodes du petit et du grand crible, Rényi a démontré pour la première fois l'existence d'une infinité de nombres premiers p tels que $p+2$ ait au plus r_o facteurs premiers, avec r_o constante absolue. Le meilleur résultat connu est avec $r_o = 2$, démontré par J.-R. Chen (Sci. Sinica, 1973). On va donner ci-dessous une démonstration relativement simple du résultat avec $r_o = 4$:

THÉORÈME 19. *Il existe une infinité de nombres premiers* p *tels que* $p+2$ *ait au plus* 4 *facteurs premiers.*

Remarque. On démontrera, comme d'habitude dans ce type de problème, un résultat plus fort : le nombre des $p \leqq x$, tels que

$$p+2 = p_1 \cdots p_r ,$$

$r \leqq 4$, $p_i > p^a$ où $a > 0$ est une constante suffisamment petite, est $\gg \dfrac{x}{(\log x)^2}$.

Preuve. Considérons la somme

$$S = \sum_{p \leqq x} \Big(\sum_{\substack{d \mid p+2 \\ d < y}} a_d \Big) \Big(\sum_{\substack{\nu \mid p+2 \\ \nu < z}} \lambda_\nu \Big)^2$$

où $a_d = 0(1)$, $|\lambda_d| \leqq 1$, $\lambda_d = 0$ si d a un facteur carré. En appliquant le Théorème 18, on obtient facilement

$$S = \mathrm{Li}(x)\, \mathfrak{S} + 0 \Big(\sum_{\substack{m < yz^2 \\ (m,2)=1}} d^3(m) |R_m| \Big)$$

avec

$$R_m = \max_{u \leq x} \left| \pi(u;m,-2) - \frac{\mathrm{Li}(u)}{\varphi(m)} \right| ,$$

et

$$\mathfrak{S} = \sum_{\substack{m<z \\ (m,d)=1}}{}' \sum_{d<y}{}' \frac{\mu^2(m)}{\varphi_1(m)} \frac{a_d}{\varphi(d)} \Big(\sum_{\substack{r \mid d \\ r \leq z/m}} \mu(r)\, \zeta_{rm} \Big)^2 ,$$

où $\sum'$ signifie que m et d sont impairs.

Si $yz^2 < x^{\frac{1}{2}} \ell^{-B}$, B assez grand, le reste $O(\ldots)$ est majoré par $x\, \ell^{-A}$. En effet,

$$\begin{aligned} \sum d^3(m) |R_m| &\leq \Big(\sum \frac{d^6(m)}{m} \Big)^{\frac{1}{2}} \Big(\sum m |R_m|^2 \Big)^{\frac{1}{2}} \\ &\ll \ell^{\frac{65}{2}} \Big(\sum m |R_m|^2 \Big)^{\frac{1}{2}} \\ &\ll \ell^{\frac{65}{2}}\, x^{\frac{1}{2}} \Big(\sum |R_m| \Big)^{\frac{1}{2}} \\ &\ll \ell^{\frac{65}{2}}\, x^{\frac{1}{2}}\, x^{\frac{1}{2}}\, \ell^{-A/2} = x\, \ell^{(65-A)/2} , \end{aligned}$$

par le Théorème 17 sur la distribution des nombres premiers dans les progressions arithmétiques.

Soit

$$\zeta_r = \zeta_1 \quad \text{si} \quad r < z \quad \text{est sans facteur carré}$$

$$\zeta_r = 0 \quad \text{dans les autres cas.}$$

Soit encore

$$a_1 = 1 , \quad a_d = 0 \quad \text{si} \quad d > 1 .$$

Il est immédiat que

$$\mathfrak{S} = \Big\{ \sum_{m<z}{}' \frac{\mu^2(m)}{\varphi_1(m)} \Big\} \zeta_1^2 ,$$

d'où

$$\sum_{p\leqq x}\Big(\sum_{\substack{\nu\mid p+2\\ \nu<z}}\lambda_\nu\Big)^2 \sim \Big\{\sum_{m<z}{}'\frac{\mu^2(m)}{\varphi_1(m)}\Big\}\zeta_1^2\,\mathrm{Li}(x)$$

$$=\Big\{\sum_{m<z}{}'\frac{\mu^2(m)}{\varphi_1(m)}\Big\}^{-1}\lambda_1^2\,\mathrm{Li}(x)\ .$$

Avec la même choix des ζ_r , soit maintenant

$$a_d = 1 \quad \text{si} \quad d \quad \text{est premier , } d = p < y$$

$$a_d = 0 \quad \text{sinon.}$$

On a alors

$$\mathfrak{S} = \sum_{m<z}{}'\sum_{\substack{2<p<y\\ (m,p)=1}}\frac{\mu^2(m)}{\varphi_1(m)}\,\frac{1}{p-1}\,\Big(\sum_{\substack{r\mid p\\ r<z/m}}\mu(r)\,\zeta_{mr}\Big)^2$$

et il est clair que

$$\sum_{r\mid p}\mu(r)\,\zeta_{mr} = \begin{cases}\zeta_1 & \text{si} \quad \frac{z}{m}\leqq p\\ \\ 0 & \text{si} \quad p<\frac{z}{m}\end{cases},$$

d'où

$$\mathfrak{S} = \sum_{m<z}{}'\frac{\mu^2(m)}{\varphi_1(m)}\Big\{\sum_{\substack{\frac{z}{m}\leqq p<y\\ p\nmid 2m}}\frac{1}{p-1}\Big\}\zeta_1^2\ .$$

On a la formule élémentaire

$$\sum_{p\leqq t}\frac{1}{p-1} = \log(1+\log t) + A_o + O\Big(\frac{1}{1+\log t}\Big)$$

avec une constante A_o . Il est facile de voir que

$$\sum_{m<z}{}'\frac{\mu^2(m)}{\varphi_1(m)}\,\frac{1}{1+\log\frac{z}{m}} \ll \frac{\log\log z}{\log z}\sum_{m<z}{}'\frac{\mu^2(m)}{\varphi_1(m)}$$

et que

$$\sum_{m\leq z}{}' \frac{\mu^2(m)}{\varphi_1(m)} \sum_{\substack{p\mid 2m \\ \frac{z}{m}\leqq p<y}} \frac{1}{p-1} \ll \frac{1}{\log\log z} \sum_{m\leq z}{}' \frac{\mu^2(m)}{\varphi_1(m)} ,$$

donc on a (si $z \leqq y$) :

$$\zeta_1^{-2}\, \mathfrak{S} = \log\left(\frac{\log y}{\log z}\right) \sum_{m\leq z}{}' \frac{\mu^2(m)}{\varphi_1(m)}$$

$$+ \sum_{m\leq z}{}' \frac{\mu^2(m)}{\varphi_1(m)} \log\left(\frac{\log z}{1+\log \frac{z}{m}}\right)$$

$$+ o\left(\sum_{m\leq z}{}' \frac{\mu^2(m)}{\varphi_1(m)}\right).$$

Un calcul élémentaire par sommation partielle montre que

$$\sum_{m\leq z}{}' \frac{\mu^2(m)}{\varphi_1(m)} \log\left(\frac{\log z}{1+\log \frac{z}{m}}\right) \sim \sum_{m\leq z}{}' \frac{\mu^2(m)}{\varphi_1(m)}$$

(ceci vient essentiellement du fait que

$$\sum_{m\leq z}{}' \frac{\mu^2(m)}{\varphi_1(m)} = A_1 \log z + A_2 + O(z^{-\frac{1}{4}}) \quad \text{et}$$

que $\displaystyle\int_0^1 \log \frac{1}{1-u}\, du = 1$) . On en conclut que

$$\sum_{p\leqq x} \Big(\sum_{\substack{d\mid p+2 \\ d<y}} a_d\Big)\Big(\sum_{\substack{\nu\mid p+2 \\ \nu<z}} \lambda_\nu\Big)^2$$

$$\sim \left\{1 + \log\left(\frac{\log y}{\log z}\right)\right\} \left\{\sum_{m\leq z}{}' \frac{\mu^2(m)}{\varphi_1(m)}\right\} \zeta_1^2\, \mathrm{Li}(x)$$

$$= \left[1 + \log\left(\frac{\log y}{\log z}\right)\right] \left\{\sum_{m\leq z}{}' \frac{\mu^2(m)}{\varphi_1(m)}\right\}^{-1} \lambda_1^2\, \mathrm{Li}(x) ,$$

si $yz^2 < x^{\frac{1}{2}}\, \ell^{-B}$.

Soient alors

$$y = x^{\frac{1}{4}+\varepsilon_o} , \quad z = x^{\frac{1}{8}-\varepsilon_o} ,$$

avec $\varepsilon_o > 0$ assez petit. Par les formules asymptotiques obtenues, on a

$$\sum_{p\leqq x}\left[2 - \Big(\sum_{\substack{d\mid p+2\\ d<y}} a_d\Big)\right]\Big(\sum_{\substack{\nu\mid p+2\\ \nu<z}} \lambda_\nu\Big)^2$$

$$\sim \Big(1 - \log\frac{2+8\varepsilon_o}{1-8\varepsilon_o}\Big)\Big\{\sum_{m<z}{}' \frac{\mu^2(m)}{\varphi_1(m)}\Big\}^{-1} \lambda_1^2 \,\mathrm{Li}(x) .$$

Comme $\log 2 < 1$, si ε_o est assez petit, le membre de droite tend vers $+\infty$ pour $x \to +\infty$. Mais alors on a

$$2 - \sum_{\substack{d\mid p+2\\ d<y}} a_d > 0$$

pour beaucoup de nombres premiers $p \leqq x$. Comme $\sum_d a_d$ est le nombre de facteurs premiers de $p+2$ plus petits que y , il y a au plus un tel facteur premier plus petit que y . Mais il y a au plus trois facteurs premiers plus grands que y , car $y \geqq p^{\frac{1}{4}+\varepsilon_o}$. Donc $p+2$ a au plus 4 facteurs premiers,

Q.E.D.

On remarquera que dans cette démonstration on n'a pas essayé d'optimiser le choix des a_d et ζ_r (ou des λ_ν) ; il semble probable que, si on le faisait, on pourrait alors obtenir $r_o = 3$ mais les calculs deviennent compliqués.

D'autre part, le résultat énoncé dans la remarque au Théorème 19 provient du choix

$$a_p = 2 \quad \text{si} \quad p < x^a$$

$$a_p = 1 \quad \text{si} \quad x^a < p < y ;$$

on laisse les détails au lecteur.

§ 10. Théorèmes de densité.

On considère ici le problème de la majoration des sommes

$$\sum_{q \leqq Q} \sum_{\chi \bmod q}^{*} N(\alpha, T; \chi)$$

où $N(\alpha,T;\chi)$ est le nombre des zéros de $L(s,\chi)$ dans le rectangle $\alpha \leq \sigma \leq 1$. $|t| \leqq T$, $T \geqq 2$. Les majorations obtenues sont du type

$$\sum_{q \leqq Q} \sum_{\chi \bmod q}^{*} N(\alpha, T; \chi) \ll (TQ^2)^{c(\alpha)(1-\alpha)} (\log TQ)^A$$

et le problème principal est d'obtenir de bonnes estimations pour $c(\alpha)$.

Les premiers résultats de ce type sont dus à Carlson (1920), avec

$$c(\alpha) = 4\alpha \quad \text{si} \quad Q = 1 .$$

Plus tard, Ingham a amélioré le résultat de Carlson, avec

$$c(\alpha) = \frac{3}{2-\alpha} \quad \text{si} \quad Q = 1$$

et cette valeur est encore la meilleure obtenue si $\frac{1}{2} \leqq \alpha \leqq \frac{3}{4}$.

Le premier résultat pour T fixe et Q variable est dû à Bombieri, avec

$$c(\alpha) = \frac{4}{3-2\alpha} ;$$

la démonstration utilise de façon essentielle la méthode du grand crible. Enfin, le premier résultat valable uniformément en T et Q est dû à Montgomery, avec

$$c(\alpha) = \min\left(\frac{3}{2-\alpha} , \frac{2}{\alpha}\right) .$$

Le point essentiel de ces estimations est que l'on peut les utiliser en arithmétique. Par exemple, Hardy et Littlewood ont démontré la résolubilité de l'équation

$$n = p_1+p_2+p_3$$

(n impair assez grand, p_i nombres premiers) en partant de l'hypothèse que $L(s,\chi) \neq 0$ pour $\sigma > \frac{3}{4}$. Plus tard, après la solution de I.M. Vinogradov, Linnik a montré que la méthode initiale de Hardy et Littlewood marchait encore si on utilisait des théorèmes de densité. Pour beaucoup d'applications l'Hypothèse de Densité : $c(\alpha) \leqq 2$,

donne les mêmes résultats que l'hypothèse de Riemann généralisée. On sait maintenant que l'hypothèse de densité est vraie pour $\frac{5}{6} \leqq \alpha \leqq 1$ et que $c(\alpha) \leqq \frac{12}{5}$.

THÉORÈME 20. On a la majoration

$$\sum_{q \leqq Q} \sum_{\chi \bmod q}^{*} N(\alpha,T;\chi) \ll (TQ^2)^{\frac{3}{2-\alpha}(1-\alpha)} (\log TQ)^A .$$

Preuve. Soit

$$M_\chi(s,\chi) = \sum_{n \leqq X} \mu(n) \frac{\chi(n)}{n^s} ,$$

$$b_n = \sum_{\substack{d \mid n \\ d \leqq X}} \mu(d) ,$$

donc

$$L(s,\chi)\, M_\chi(s,\chi) = 1 + \sum_{n > X} b_n \frac{\chi(n)}{n^s}$$

pour $\sigma > 1$, car $b_1 = 1$, $b_n = 0$, si $1 < n \leqq X$.

On pose

$$D = TQ^2 , \quad Y = X^{3/2}$$

et l'on prend

$$X = D^{\frac{1}{2-\alpha}} .$$

On a la formule

$$1 + \sum_{n > X} b_n \frac{\chi(n)}{n^s} e^{-n/Y} = L(s,\chi)\, M_\chi(s,\chi)$$

$$+ \frac{1}{2\pi i} \int_{(-\sigma+\frac{1}{2})} L(s+w,\chi)\, M_\chi(s+w,\chi)\, \Gamma(w+1) \frac{Y^w}{w}\, dw$$

pour $\frac{1}{2} \leqq \sigma \leqq 1$, avec un terme supplémentaire $M_\chi(1,\chi_o)\, \Gamma(2-s) \frac{Y^{1-s}}{1-s}$ si $\chi = \chi_o$

est le caractère principal ; vu la décroissance rapide de $\Gamma(2-s)$ pour $t \to \infty$, ce terme n'a pas d'importance dans les estimations qu'on va faire ci-dessous.

Soit $s = \rho = \beta+i\gamma$ un zéro de $L(s,\chi)$ avec $\beta \geqq \alpha$. Vu la décroissance exponentielle de la fonction Γ sur les droites verticales, l'équation précédente donne l'estimation

$$1 \ll \Big| \sum_{n>X} b_n \frac{\chi(n)}{n^\rho} e^{-n/Y} \Big| + Y^{\frac{1}{2}-\alpha} \int_{\gamma-(\log D)^2}^{\gamma+(\log D)^2} |L(\tfrac{1}{2}+it,\chi)| \, |M_\chi(\tfrac{1}{2}+it,\chi)| \, dt .$$

On partage alors les zéros en trois classes :

(I) $$1 \ll \Big| \sum_{n>X} b_n \frac{\chi(n)}{n^\rho} e^{-n/Y} \Big| ;$$

(II) il existe t_ρ avec $|t_\rho - \gamma| < (\log D)^2$

tel que

$$|M_\chi(\tfrac{1}{2}+it_\rho,\chi)| > X^{\alpha-\frac{1}{2}} ;$$

(III) $$\int_{\gamma-(\log D)^2}^{\gamma+(\log D)^2} |L(\tfrac{1}{2}+it,\chi)| \, dt \gg (\frac{Y}{X})^{\alpha-\frac{1}{2}} = X^{\frac{1}{2}\alpha-\frac{1}{4}} ;$$

il est clair que tout zéro appartient à au moins une classe. Soit $N_\ell, \ell = 1,2,3$ le nombre des zéros de toutes les fonctions $L(s,\chi)$, χ primitif de module au plus Q, dans la ℓ-ième classe, avec $\beta \geqq \alpha$, $|\gamma| \leqq T$. Toute fonction L a au plus $\ll \log D$ zéros dans $|t-t_o| \leqq 1$, pour tout $|t_o| \leqq T$, donc dans la ℓ-ième classe il y a un sous-ensemble $\mathcal{R}_\ell$ de zéros $(5 \log D)^2$-bien espacés, et

$$|\mathcal{R}_\ell| \gg N_\ell (\log D)^{-3} .$$

Estimation de $|\mathcal{R}_1|$. Soit Ω l'ensemble des caractères généralisés $\omega(n) = \frac{\chi(n)}{n^{i\gamma}}$, avec $\beta+i\gamma \in \mathcal{R}_1$. Par le Théorème 12 et la remarque suivant sa démonstration, on a, en partageant l'intervalle (X,Y) en $\ll \log D$ sous-intervalles I_ν du type $(N_\nu, 2N_\nu)$ et un intervalle final (N_{ν_o}, Y) avec

$N_{\nu_o} \cong \frac{1}{2} Y$:

$$|R_1| \ll \sum_{\Omega} |\sum_{X}^{Y} b_n n^{-\beta}\, \omega(n)|^2$$

$$\ll (\log D) \sum_{\nu} \sum_{\Omega} |\sum_{I_\nu} b_n n^{-\beta}\, \omega(n)|^2$$

$$\ll (\log D) \sum_{\nu} [|I_\nu| + D(\log D)^8] \sum_{I_\nu} \frac{|b_n|^2}{n^{2\alpha}}$$

$$\ll (\log D) \sum_{\nu} [|I_\nu| + D(\log D)^8] |I_\nu|^{1-2\alpha} (\log D)^5$$

$$\ll Y^{2-2\alpha} (\log D)^7 + DX^{1-2\alpha} (\log D)^{15}$$

$$\ll D^{\frac{3}{2-\alpha}(1-\alpha)} (\log D)^{15}.$$

Estimation de $|R_2|$. Elle est tout à fait analogue, en prenant pour Ω l'ensemble des $\omega(n) = \frac{\chi(n)}{n^{it_\rho}}$, $\rho \in R_2$. On obtient aisément par le Théorème 12 l'inégalité

$$|R_2| \ll D^{\frac{3}{2-\alpha}(1-\alpha)} (\log D)^3 .$$

Estimation de $|R_3|$. On a maintenant, si I_ρ indique l'intervalle $|t-\gamma| < (\log D)^2$:

$$|R_3|\, X^{2\alpha-1} \ll \sum_{R_3} \Big(\int_{I_\rho} |L(\tfrac{1}{2}+it,\chi)|\,dt \Big)^4$$

$$\ll (\log D)^6 \sum_{R_3} \int_{I_\rho} |L(\tfrac{1}{2}+it,\chi)|^4 dt$$

$$\ll (\log D)^6 \sum_{q \le Q} \sideset{}{^*}\sum_{\chi \bmod q} \int_{-2T}^{2T} |L(\tfrac{1}{2}+it,\chi)|^4 dt ,$$

car l'ensemble $\mathfrak{R}_3$ est $(4 \log D)^2$ -bien espacé.

On a

$$\sum_{q \leqq Q} \sum_{\chi \bmod q}^{*} \int_{-2T}^{2T} |L(\tfrac{1}{2}+it,\chi)|^4 \, dt \ll D(\log D)^{10} ,$$

d'où

$$|\mathfrak{R}_3| \ll DX^{1-2\alpha}(\log D)^{16} = D^{\frac{3}{2-\alpha}(1-\alpha)}(\log D)^{16} ,$$

et la conclusion du Théorème 20 (avec $A = 19$) résulte de $N_1+N_2+N_3 \ll (|\mathfrak{R}_1|+|\mathfrak{R}_2|+|\mathfrak{R}_3|)(\log D)^3$.

Pour compléter la démonstration du Théorème, on va vérifier :

Lemme. On a la majoration

$$\sum_{q \leqq Q} \sum_{\chi \bmod q}^{*} \int_{-T}^{T} |L(\tfrac{1}{2}+it,\chi)|^4 dt \ll D(\log D)^{10} .$$

Preuve du Lemme. On utilise ici une idée de Ramachandra.

On a pour $\sigma > 1$:

$$L^2(s,\chi) = \sum_{1}^{\infty} d(n) \frac{\chi(n)}{n^s}$$

et donc

$$L^2(s,\chi) = \sum_{1}^{\infty} d(n) \frac{\chi(n)}{n^s} e^{-n/Z}$$

$$- \frac{1}{2\pi i} \int_{(c)} L^2(s+w,\chi) \, \Gamma(w+1) \frac{Z^w}{w} \, dw$$

pour $-1 < c < 0$ (il y a un terme additionnel sans importance dans le cas où $\chi = \chi_0$, provenant du résidu du pôle de $\zeta^2(s+w) \, \Gamma(w+1) \frac{Z^w}{w}$ pour $w = 1-s$) .

On utilise maintenant l'équation fonctionnelle

$$L(s,\chi) = \Psi(s,\chi) \, L(1-s,\bar{\chi})$$

et l'intégrale devient, pour $-1 < c < -\sigma$:

$$\frac{1}{2\pi i}\int_{(c)} \psi^2(s+w,\chi) \sum_1^\infty d(n) \frac{\bar\chi(n)}{n^{1-s-w}} \Gamma(w+1) \frac{Z^w}{w}\, dw$$

$$= \frac{1}{2\pi i}\int_{(c)} \psi^2(s+w,\chi) \sum_{n>Z} d(n) \frac{\bar\chi(n)}{n^{1-s-w}} \Gamma(w+1) \frac{Z^w}{w}\, dw$$

$$+ \frac{1}{2\pi i}\int_{(c')} \psi^2(s+w,\chi) \sum_1^Z d(n) \frac{\bar\chi(n)}{n^{1-s-w}} \Gamma(w+1) \frac{Z^w}{w}\, dw$$

avec $-1 < c' < 0$. On remarque que, dans la dernière intégrale, on a changé l'abscisse d'intégration de c à c' .

On prend alors

$$s = \frac{1}{2} + it\ ,\quad c = -\frac{1}{2} - \frac{1}{\log D}\ ,\quad c' = -\frac{1}{\log D}\ ,\quad Z = D\ ;$$

sur $\mathrm{Re}\ w = c$ on a $|\psi^2(s+w,\chi)\ Z^w| \ll D^{\frac{1}{2}}$, et sur $\mathrm{Re}\ w = c'$ on a $|\psi^2(s+w,\chi)\ Z^w| \ll 1$, donc on obtient

$$|L(\tfrac{1}{2}+it,\chi)|^2 \ll \Big|\sum_1^\infty d(n) \frac{\chi(n)}{n^{\frac{1}{2}+it}} e^{-n/D}\Big|$$

$$+ D^{\frac{1}{2}} \int_{-\infty}^{\infty} \Big| \sum_{n>D} d(n) \frac{\bar\chi(n)}{n^{1+\frac{1}{\log D}+iv}} \Big|\, e^{-|v-t|}\, dv$$

$$+ \log D \int_{-\infty}^{\infty} \Big|\sum_1^D d(n) \frac{\bar\chi(n)}{n^{\frac{1}{2}+\frac{1}{\log D}+iv}} \Big|\, e^{-|v-t|}\, dv\ ,$$

et finalement

$$\sum_{q\leq Q} \sum_{\chi \bmod q}^{*} \int_{-T}^{T} |L(\tfrac{1}{2}+it,\chi)|^4 \, dt$$

$$\ll \sum_{q\leq Q} \sum_{\chi \bmod q}^{*} \int_{-T}^{T} \Big|\sum_{1}^{\infty} d(n) \frac{\chi(n)}{n^{\frac{1}{2}+it}} e^{-n/D}\Big|^2 dt$$

$$+ D \sum_{q\leq Q} \sum_{\chi \bmod q}^{*} \int_{-T}^{T} dt \int_{-\infty}^{\infty} \Big|\sum_{n>D} d(n) \frac{\bar{\chi}(n)}{n^{1+\frac{1}{\log D}+iv}}\Big|^2 e^{-|v-t|} dv$$

$$+ (\log D)^2 \sum_{q\leq Q} \sum_{\chi \bmod q}^{*} \int_{-T}^{T} \int_{-\infty}^{\infty} \Big|\sum_{1}^{D} d(n) \frac{\bar{\chi}(n)}{n^{\frac{1}{2}+\frac{1}{\log D}+iv}}\Big|^2 e^{-|v-t|} dv \; ;$$

le lemme résulte alors d'une application facile du Théorème 10 ,

Q.E.D.

On ne donnera pas ici les estimations plus fines de $c(\alpha)$, comme $c(\alpha) \leq \frac{12}{5}$, qui utilisent les estimations plus délicates de $\|\mathcal{A}\|_{2,2}^2$ dans le Théorème 12. Les idées sont les mêmes, mais il y a beaucoup de complications de détail pour optimiser le choix des paramètres. On renvoie pour cela à la bibliographie relative à cette section.

§ 11. Notes Bibliographiques.

§ 0,1. Le grand crible se trouve pour la première fois dans l'article de Linnik [L] de 1941. Les recherches de Rényi datent de 1948 à 1959, en particulier [Re 1] sur l'équation $2n = p+p_1 \ldots p_{r_o}$, [Re 2] et [Re 3].

§ 2,3. Le premier résultat comparable au Théorème 4 est dans Roth [Ro] en 1964. La méthode de [B 1], 1965 est assez différente. La démonstration simple donnée ici est dans [B 2] ; pour plus de renseignements, voir Montgomery [M 1] et [M 2], et l'intéressant article de Selberg [S 2]. Les Théorèmes 5 et 6 sont dans Montgomery [M 3] et la démonstration donnée ici est due à Gallagher [G 1].

§ 4. Le Théorème 7 est de Gallagher [G 2] ; une forme plus faible est dans [B 1]. Le Théorème 8 est de Bombieri et Davenport. Le Théorème 7A est de Selberg, avec une démonstration différente [S 2].

§ 5. La première partie de ce paragraphe est entièrement due à Gallagher [G 3]. La deuxième partie est dans Forti et Viola [F - V 1].

§ 6. La démonstration du Théorème de Linnik est emprunté à Gallagher [G 3], mais la deuxième partie du Théorème 14 est nouvelle. Pour les propriétés des fonctions L et le Lemme de Landau-Page, voir Davenport [D] ou Prachar [P]. Pour le Lemme de Turán, il existe une belle version de Tijdeman [T]. La preuve du dernier lemme est une simplification des arguments donnés dans [P], Ch. X.

La démonstration du Théorème 14 a été très simplifiée par Selberg (non publié) en utilisant le Théorème 7A au lieu du Théorème 8 ; en particulier, il n'utilise pas la méthode de Turán et il peut obtenir des majorations très explicites.

§ 7. Le Théorème 17 est dans [B 1] ; une forme plus faible est due à A.I. Vinogradov [V]. La démonstration donnée ici est une variante de [G 4]. On peut consulter aussi [M 1] et la monographie de Huxley [H 1].

§ 8,9. Le contenu de ces paragraphes semble nouveau. Le lecteur intéressé par les techniques du petit crible est renvoyé à Selberg[S 1], [S 2] et à l'excellent article de Richert [Ri].

§ 10. Le Théorème 20 est dû à Montgomery [M 4] et la démonstration simplifiée du Lemme est due à Ramachandra [Ra]. Le lecteur pourra consulter [M 1], [H 1], [H 2], [F-V 2] au sujet des théorèmes de densité.

BIBLIOGRAPHIE

[B1] Bombieri, E. On the Large Sieve. Mathematika 12(1965), 201-225.

[B2] " A note on the Large Sieve. Acta Arith. 18(1971), 401-404.

[D] Davenport, H. Multiplicative Number Theory. Markham, Chicago 1967 (Sans les théorèmes 4, 4A du § 23).

[F-V1] Forti, M. et Viola, C. On large sieve type estimates for the Dirichlet series operator. Proc. Symposia Pure Math. XXIV 1973, 31-49.

[F-V2] " Density estimates for the zeros of L-functions. Acta Arith. 23 (1973), 379-391.

[G1] Gallagher, P.X. Sieving by prime powers. Proc. 1972 Number Theory Conference in Boulder, (1972), 95-99.

[G2] " The Large Sieve. Mathematika 14 (1967), 14-20.

[G3] " A Large Sieve Estimate Near $\sigma = 1$. Inv. Math. 11 (1970), 329-339.

[G4] " Bombieri's mean value theorem. Mathematika 15 (1968), 1-6.

[H1] Huxley, M.N. The Distribution of Prime Numbers. Oxford Math. Monographs 1972.

[H2] " On the difference between consecutive primes. Inventiones Math. 16 (1972), 191-201.

[L] Linnik, Yu. V. Le grand crible. Dokl. Akad. Nauk SSSR 30 (1941), 292-294 (en russe).

[M1] Montgomery, H.L. Topics in Multiplicative Number Theory. Springer Lecture Notes 227 (1971).

[M2] " Hilbert's inequality and the large sieve. Proc. 1972 Number Theory Conference in Boulder, (1972), 156-161.

[M3] " A note on the large sieve. J. London Math. Soc. 43 (1968), 93-98.

[M4] " Zeros of L-functions. Inventiones Math. 8 (1969), 334-345.

[P] Prachar, K. Primzahlverteilung, Springer, Berlin 1957.

[Ra] Ramachandra, K. A simple proof of the mean fourth power estimate for $\zeta(\frac{1}{2}+it)$ and $L(\frac{1}{2}+it,\chi)$. A paraître dans Ann. Scuola Normale Sup. Pisa.

[Re1] Rényi, A. On the representation of an even number as the sum of a prime and of an almost prime. Izv. Akad. Nauk SSSR Ser. Mat. 12 (1948), 57-78, et Amer. Math. Soc. Translations (2) 19, (1962), 229-321.

[Re2] " On the large sieve of U.V. Linnik. Compositio Math. 8 (1950), 68-75.

[Re3] " New version of the probabilistic generalization of the large sieve. Acta Math. Acad. Sci. Hungar. 10 (1959), 217-226.

[Ri] Richert, H.-E. Selberg's sieve with weights. Proc. Symposia Pure Math. XX (1971), 287-310.

[S1] Selberg, A. Sieve Methods. Proc Symposia Pure Math. XX (1971), 311-351.

[S2] " Remarks on Sieves. Proc. 1972 Number Theory Conference in Boulder, (1972), 205-216.

[T] Tijdeman, R. On the distribution of the values of certain functions. Academic Service, Amsterdam 1969.

[V] Vinogradov, A.I. Sur l'hypothèse de densité pour les fonctions L de Dirichlet. Izv. Akad. Nauk SSSR Ser. Mat. 29 (1965), 903-934 et Correction,Izv. Akad. Nauk SSSR Ser. Mat. 30 (1966), 719-720 (en russe).

Enrico BOMBIERI
Scuola Normale Superiore
Piazza dei Cavalieri
56100 Pisa (Italia)

SUMMARY

These notes on Analytic Number Theory are an expanded version of a series of lectures given at Collège de France in May 1973, on the subject of the Large Sieve.

The method of the Large Sieve today is one of the most powerful tools in Multiplicative Number Theory. Roughly speaking, it may be considered as Fourier analysis of arithmetic progressions, both from the additive and multiplicative point of view. The key tools are two basic estimates (see Theorem 4, Corollary 2 and Theorems 7, 8, 7A) which may be regarded as Bessel's inequality for a system of almost orthogonal functions.

The applications to Number Theory come from two sources. The first, and also more elementary, is the additive form dealt with in § 2, 3, which leads directly to arithmetical results typical of Selberg's sieve. For this reason in § 0, 1 we start with a simple definition of a sieve and the theorem of Linnik on the least quadratic non-residue mod p ; we also give Rényi's formulation of the Large Sieve.

The second, and deeper, formulation of the Large Sieve is multiplicative and deals with a Fourier analysis with respect to Dirichlet's characters $\chi(n)$. This is dealt with in § 4 and generalized in § 5.

The rest of these notes is devoted to applications of the multiplicative form of the Large Sieve. In § 6, we prove a density theorem for zeros of L-functions, from which we deduce the deep theorem of Linnik on the least prime in an arithmetic progression. Another type of density theorem, which can be used for studying the distribution of primes in short intervals, is discussed in § 10.

In § 7, we give a simplified proof of the Bombieri-Vinogradov theorem on distribution of primes in arithmetic progressions, and § 8 and 9 deal with a typical application of the result obtained in § 7, namely Rényi's theorem on the equation $p+2 = p_1 \ldots p_r$, with p, p_i primes. The simple proof we give of the solubility of this equation with $r \leqq 4$ introduces some new ideas in the Selberg sieve method.

In these notes I have tried to present some of the most important applications of the method of the Large Sieve, in particular the Density Theorems, the distribution of primes in arithmetic progressions and the connection with the small sieve (Brun-Selberg). I should stress here that the results obtained are only samples of the various ways in which one can apply this method ; also, in

order not to complicate the proofs, I have not always given the strongest result available.

The final § 11 contains bibliographical notes relevant to the various sections.

§ 12. Some recent developments

(added for the second edition, 1987)

I. One of the most important applications of the large sieve consists in obtaining a result of the distribution of primes in large arithmetic progressions (§ 7, Théorème 17). It was conjectured by Elliott and Halberstam that such a result may hold for $q \le Q$ with $Q = x^{\vartheta}$ with some $\vartheta > \frac{1}{2}$ and possibly $\vartheta = 1 - \varepsilon$, for any $\varepsilon > 0$. At the present moment, even the result with $Q = x^{1/2}$ remains open. On the other hand, important progress has been made by injecting new ideas into the large sieve methods. These ideas may be described as :

(a) the systematic use of bilinear forms ;

(b) combinatorial techniques ;

(c) the introduction of Kloosterman sums into the analysis of remainder terms.

This has led to the proof of the analogue of Théorème 17 for quite general arithmetical functions, which we are going to describe, following Bombieri, Friedlander and Iwaniec (Acta Mathematica, 156 (1986), 203-251).

Roughly speaking, the basic principle is that if the analogue of Théorème 17 holds for two arithmetical functions f and g, then it holds for the Dirichlet convolution $f * g$. We state it in precise form as follows.

Let $f(n)$ be an arithmetical function. If $(a,q) = 1$, then the progressions $qm + a$ are independent of each other and, since there are $\varphi(q)$ such progressions for fixed q, the mean value of $\sum_{\substack{n\le x\\ n\equiv a \,(\mathrm{mod}\ q)}} f(n)$ is simply $\frac{1}{\varphi(q)} \sum_{\substack{n\le x\\ (n,q)=1}} f(n)$.
This leads us to introduce the remainder

$$\Delta_f(x;q,a) = \sum_{\substack{n\le x\\ n\equiv a \,(\mathrm{mod}\ q)}} f(n) - \frac{1}{\varphi(q)} \sum_{\substack{n\le x\\ (n,q)=1}} f(n)$$

and ask for estimates for Δ_f. For most applications, it suffices to obtain results of type

$$\Delta_f(x;q,a) \ll \frac{1}{\varphi(q)} \|f\| \, x^{1/2} \, \ell^{-A}$$

with $\ell = \log x$ and

$$\|f\| = \Big(\sum_{n\le x} |f(n)|^2 \Big)^{1/2},$$

for any $A > 0$, with the implied constant in $\ll$ dependent only on A, and we

want this result to be valid uniformly in q in a large range.
There are different formulations according as the sought for uniformity is for all or almost all q or a. There are four levels of difficulty :

(M 1) almost all q and almost all a.

Here we seek to estimate Δ_f on average with respect both q and a ; the main quantity we deal with is

$$\sum_{q<Q} \sum_{\substack{a=1 \\ (a,q)=1}}^{q} |\Delta_f(x;q,a)|^2 .$$

Results of this type are called of Barban - Davenport - Halberstam type.

(M 2) almost all q and all a.

Here we seek to estimate

$$\sum_{q<Q} \max_{(a,q)=1} |\Delta_f(x;q,a)| .$$

Results of this type are the proper analogue of Théorème 17.

(M 3) almost all q and fixed a.

Here we seek to estimate

$$\sum_{q<Q}{}' |\Delta_f(x;q,a)| ,$$

where Σ' means that q is restricted to q and a being coprime.

(M 4) all q and all a.

Here we seek to estimate $\Delta_f(x;q,a)$ directly.

We leave aside (M 4), and begin with (M 1) and (M 2).

We use the notation $n \sim N$ to indicate an interval $\frac{1}{2} N < n < 2N$.

DEFINITION.- *The sequence* β_n, $n \le x$ *is said to satisfy a Siegel - Walfisz condition if for any* $d \ge 1$, $k \ge 1$ *and* a *with* $(k,a) = 1$ *we have*

$$\Big| \sum_{\substack{n\le x \\ n\equiv a \pmod k \\ (n,d)=1}} \beta_n - \frac{1}{\varphi(k)} \sum_{\substack{n\le x \\ (n,dk)=1}} \beta_n \Big| \ll \tau(d)^{B_1} \, \|\beta\| \, x^{1/2} \, \ell^{-A}$$

with some $B_1 > 0$ *and any* $A > 0$, *the constant implied in* $\ll$ *depending only on* A.

Here we have written $\tau(d)$ for the number of divisors of d and

$$\|\beta\| = \left(\sum_{n \le x} |\beta_n|^2 \right)^{1/2} .$$

THEOREM 21.- *Let* β_n , $n \le x$, *be complex numbers satisfying the Siegel - Walfisz condition. For any* $A > 0$ *there exists* $B = B(A) > 0$ *such that*

$$\sum_{q < x\ell^{-B}} \sum_{(a,q)=1} \Big| \sum_{n \equiv a \pmod q} \beta_n - \frac{1}{\varphi(q)} \sum_{(n,q)=1} \beta_n \Big|^2 \ll \|\beta\|^2 \times \ell^{-A} .$$

If $\beta_n = \Lambda(n)$, this is a form of the Barban - Davenport - Halberstam theorem.

Proof.- It is immediate that

$$\sum_{q \le Q} \sum_{(a,q)=1} \Big| \sum_{n \equiv a \pmod q} \beta_n - \frac{1}{\varphi(q)} \sum_{(n,q)=1} \beta_n \Big|^2$$

$$= \sum_{q \le Q} \frac{1}{\varphi(q)} \sum_{\chi \ne \chi_o} \Big| \sum_n \beta_n \chi(n) \Big|^2 .$$

Let χ be induced by $\psi \bmod f$, $f > 1$. Then

$$\sum_n \beta_n \chi(n) = \sum_{(n,q/f)=1} \beta_n \psi(n)$$

and since $\varphi(q) \ge \varphi(f)\varphi(q/f)$, we get

$$\sum_{q \le Q} \frac{1}{\varphi(q)} \sum_{\chi \ne \chi_o} \Big| \sum_n \beta_n \chi(n) \Big|^2$$

$$\le \sum_{r \le Q} \frac{1}{\varphi(r)} \sum_{2 \le f \le Q/r} \frac{1}{\varphi(f)} \sum_{\psi \bmod f}^{*} \Big| \sum_{(n,r)=1} \beta_n \psi(n) \Big|^2 .$$

We split the inner sum in f into two parts :

$$S_1(r) = \sum_{2 \le f \le F} \frac{1}{\varphi(f)} \sum_{\psi \bmod f}^{*} \Big| \sum_{(n,r)=1} \beta_n \psi(n) \Big|^2$$

and

$$S_2(r) = \sum_{F < f \le Q/r} \frac{1}{\varphi(f)} \sum_{\psi \bmod f}^{*} \Big| \sum_{(n,r)=1} \beta_n \psi(n) \Big|^2 .$$

We estimate $S_1(r)$ by splitting $\sum_{(n,r)=1}$ into progressions mod f and applying the Siegel - Walfisz property of β_n , getting first

$$\sum_{(n,r)=1} \beta_n \psi(n) \ll \|\beta\| \tau^{B_1}(r)\ f\ x^{1/2}\ \ell^{-A}$$

and then

$$S_1(r) \ll \tau^{2B_1}(r)\ F^3\ \|\beta\|^2\, x\ \ell^{-2A}\ .$$

Now we estimate $S_2(r)$ by splitting the sum into $\ll \log Q$ intervals of type $(U,2U)$ and applying the large sieve inequality

$$S_2(r) \ll \log Q \sup_{F<U\le Q} \frac{\log Q}{U} \sum_{f\le U} \sum_{\psi \bmod f}{}^{*} \Big| \sum_{(n,r)=1} \beta_n \psi(n)\Big|^2$$

$$\ll (\log Q)^2 \sum_{F<U\le Q} \frac{1}{U}(U^2+x)\ \|\beta\|^2$$

$$\ll \left(Q+\frac{x}{F}\right)\ \|\beta\|^2 (\log Q)^2\ .$$

We conclude that, for some $B_2 = B_2(B_1)$:

$$\sum_{r\le Q} \frac{1}{\varphi(r)}\ (S_1(r)+S_2(r)) \ll \|\beta\|^2 (\log Q)^{B_2}\ \{x\ F^3\ \ell^{-2A} + x\ F^{-1} + Q\}$$

and Theorem 21 follows by choice of F,Q , starting with sufficiently large A .

Our next result is the analogue of Théorème 17 for a class of arithmetical functions ; the first results of this type are due to Motohashi (1976).

THEOREM 22.- *Let* $f(n)$, $n \le x$, *be the Dirichlet convolution of two sequences* $\alpha = (\alpha_m)$, $\beta = (\beta_n)$ *and suppose that there is* ϑ , $0 < \varepsilon \le \vartheta \le 1-\varepsilon$, *such that*

(i) α *is supported in* $m \sim M = x^{1-\vartheta}$

(ii) β *is supported in* $n \sim N = x^{\vartheta}$ *and satisfies the Siegel - Walfisz condition.*

For any $A > 0$ *there exists* $B = B(A) > 0$ *such that*

$$\sum_{q\le x^{1/2}\ell^{-B}} \max_{(a,q)=1} |\Delta_f(x;q,a)| \ll \|\alpha\|\ \|\beta\|\ x^{1/2}\ \ell^{-A}\ ,$$

where the constant implied in $\ll$ *depends only on* A *and* ε .

Remark.- As it will be clear from the proof, the condition on M,N can be replaced by $MN = x$ and $M \gg \ell^C$ for every $C > 0$ and $\log N \gg \ell^{\delta}$ for some $\delta > 0$. This more general form is useful in extending Theorem 22 to fairly general arithmetical functions $f(n)$.

Proof.- We have

$$\Delta_{\alpha*\beta}(x;q,a) = \frac{1}{\varphi(q)} \sum_{\chi \neq \chi_o} \bar{\chi}(a) \left(\sum_m \alpha_m \chi(m) \right) \left(\sum_n \beta_n \chi(n) \right) .$$

We proceed as in the proof of Theorem 21, reducing to primitive characters, so that we need to bound

$$\sum_{r \leq Q} \frac{1}{\varphi(r)} (S_1(r) + S_2(r))$$

where

$$S_1(r) = \sum_{2 \leq f \leq F} \frac{1}{\varphi(f)} \sum_{\psi \bmod f}^{*} \Big| \sum_{(m,r)=1} \alpha_m \psi(m) \Big| \Big| \sum_{(n,r)=1} \beta_n \psi(n) \Big|$$

and

$$S_2(r) = \sum_{F < f \leq Q} \frac{1}{\varphi(f)} \sum_{\psi \bmod f}^{*} \Big| \sum_{(m,r)=1} \alpha_m \psi(m) \Big| \Big| \sum_{(n,r)=1} \beta_n \psi(n) \Big| .$$

For $S_1(r)$, we use Cauchy's inequality :

$$S_1(r) \leq \left\{ \sum_{2 \leq f \leq F} \frac{1}{\varphi(f)} \sum_{\psi \bmod f}^{*} \Big| \sum_{(m,r)=1} \alpha_m \psi(m) \Big|^2 \right\}^{1/2}$$

$$\left\{ \sum_{2 \leq f \leq F} \frac{1}{\varphi(f)} \sum_{\psi \bmod f}^{*} \Big| \sum_{(n,r)=1} \beta_n \psi(n) \Big|^2 \right\}^{1/2}$$

To the first sum involving α we apply the large sieve inequality, while the second sum involving β is estimated, exactly as in the proof of Theorem 21, by applying the Siegel - Walfisz condition. This yields

$$S_1(r) \ll \|\alpha\| \, \|\beta\| \, x^{1/2} \, \tau^{B_1}(r) \, F^{3/2} (\log N)^{-A} ,$$

provided $F < M^{1/2}$.

The estimation of $S_2(r)$ proceeds as in the proof of Theorem 21, by dividing the interval for f into $\ll \log Q$ subintervals of the type $(U,2U)$, applying Cauchy's inequality to separate α and β and finally applying the large sieve inequality twice. One gets

$$S_2(r) \ll (\log Q)^2 \, \|\alpha\| \cdot \|\beta\| \sup_{F < U < Q} U^{-1} (U^2 + M)^{1/2} (U^2 + N)^{1/2}$$

$$\ll (\log Q)^2 \, \|\alpha\| \cdot \|\beta\| \, (Q + M^{1/2} + N^{1/2} + (MN)^{1/2} F^{-1}) .$$

It is now easy to estimate $\sum_{r \leq Q} \frac{1}{\varphi(r)} (S_1(r) + S_2(r))$ to complete the proof

of Theorem 22.

In order to extend the result of Theorem 22 to more general functions f, one uses two main techniques :

(A) taking linear combinations of convolutions,

(B) using a sieve in order to eliminate from the support of f the values of n with "small" prime factors.

In this way, one can show that the conclusion of Theorem 22 applies to very large classes of arithmetical functions, such as divisor functions $\tau_k(n)$ and their powers, the Euler function, the Möbius function, and so on. Rather than describing this in more detail, we move now to the combinatorial analysis involved in (A) and (B).

II. We owe to Linnik the basic idea that the study of the distribution of prime numbers can be reduced to the study of generalized divisor functions. The most flexible form of this principle is that introduced by Heath - Brown ; the identity for $-\frac{L'}{L}$ in section 2 of § 7 (Gallagher) is another instance of the application of Linnik's principle.

Let $A = A(s) = \Sigma \frac{a_n}{n^s}$ be a (formal) Dirichlet series and let $|_z$ denote the truncation $A|_z = \sum_{n \le z} \frac{a_n}{n^s}$. We illustrate Heath - Brown's idea with an example. Suppose we want to study the von Mangoldt function $\Lambda(n)$ for $n \le x$. The generating function for $\Lambda(n)$ is $-\frac{\zeta'}{\zeta}$ where ζ is the Riemann zeta function, and its singular points come from the zeros of ζ. Now let $M_z = \sum_{n \le z} \frac{\mu(n)}{n^s}$ be a truncation of $\frac{1}{\zeta}$; M_z may be considered an approximation for $\frac{1}{\zeta}$, where all singularities have disappeared.
It is clear that

$$\zeta M_z = 1 + \sum_{n>z} \frac{b_n}{n^s}$$

for suitable coefficients $b_n = b_n(z)$, hence

$$(1 - \zeta M_z)^k = \sum_{n>z^k} \frac{c_n(z,k)}{n^s}$$

for suitable coefficients $c_n(z,k)$. If $z^k > x$, it is clear that

$$(A(1-\zeta M_z)^k)|_x = 0$$

for any Dirichlet series A. We apply the last equation with $A = -\frac{\zeta'}{\zeta}$ and deduce

$$-\frac{\zeta'}{\zeta}\Big|_x = \sum_{j=1}^{k} (-1)^j \binom{k}{j} \left(\zeta' \zeta^{j-1} M_z^j\right)\Big|_x .$$

This proves

Heath-Brown's Identity. Let k be a positive integer such that $z^k > x$. Then for $n \le x$ we have

$$\Lambda(n) = \sum_{j=1}^{k} (-1)^{j-1} \binom{k}{j} \sum_{\substack{m_1 \dots m_j \, n_1 \dots n_j = n \\ n_1, \dots, n_j \le z}} (\log m_1)\, \mu(n_1) \dots \mu(n_j) .$$

In order to show how to use Heath-Brown's identity, we sketch an argument which shows how Theorem 22 can be used to give yet another proof of Theorem 17. Our exposition will be necessarily very sketchy, since the full details are rather cumbersome.

We start with Heath-Brown's identity for $z = (2x)^{1/3}$ and $k = 3$ and begin by splitting $n \le x$ into subintervals of the type $(U, 2U)$. This reduces us easily to assume that $n \sim x$. Next, we split the ranges for the m_i and n_i, for each value of $j = 1,2,3$, into $\ll \left(\frac{1}{\delta} \log x\right)^{2k}$ intervals, each of the type $(U, (1+\delta)U)$, where $\delta \gg \ell^{-A_1}$ for fixed A_1. This means that we write $\Lambda(n)$ as a linear combination (with $\ll \ell^{A_2}$ terms, with bounded coefficients) of convolutions of the type $\alpha_1 * \dots * \alpha_j * \beta_1 * \dots * \beta_j$, in which α_i is supported in $(M_i, (1+\delta)M_i)$, β_i is supported in $(N_i, (1+\delta)N_i)$, $M_1 \dots M_j N_1 \dots N_j \sim x$ and $N_i \ll x^{1/3}$.

Case I. $x^{\varepsilon} < N_j$ for some $\varepsilon > 0$.

In this case, Theorem 22 applies to $\alpha_1 * \dots * \alpha_j * \beta_1 * \dots * \beta_j$ simply by choosing $\alpha = \alpha_1 * \dots * \alpha_j * \beta_1 \dots * \beta_{j-1}$ and $\beta = \beta_j$, because the Möbius function satisfies the Siegel-Walfisz condition.

Case II. $x^{\varepsilon} < M_j < x^{1-\varepsilon}$ for some $\varepsilon > 0$.

In this case, Theorem 22 applies to $\alpha_1 * \dots * \alpha_j * \beta_1 * \dots * \beta_j$ by choosing $\alpha = \alpha_1 * \dots * \alpha_{j-1} * \beta_1 * \dots * \beta_j$ and $\beta = \alpha_j$.

Case III. $M_1 > x^{1-5\varepsilon}$

In this case, we consider $m_2, \dots, m_j$, $n_1, \dots, n_j$ fixed and deal with m_1 only. Since α_1 is $\log m_1$ (or 1, if we had $M_i > x^{1-5\varepsilon}$ for some $i \ge 2$), the function α_1 is well-distributed in arithmetic progressions and Theorem 22 can be checked in this case directly.

Since, up to a permutation of factors, one of the three above cases always occurs, one concludes that the analogue of Theorem 17 holds for each arithmetic function occurring in the decomposition for $\Lambda(n)$ and hence for $\Lambda(n)$ itself.

The advantage in decomposing $\Lambda(n)$ as a sum of functions of type $\alpha_1 * \dots * \alpha_j * \beta_1 * \dots * \beta_j$ is however more evident if we deal with the distribution of $\Lambda(n)$ in progressions $qm+a$ with fixed a. In this case, it is possible to go beyond $q < x^{1/2}\ell^{-B}$ if not for every $\alpha_1 * \dots * \beta_j$ at least for a large portion of such convolutions, leaving behind few special configurations $\alpha_1 * \dots * \beta_j$.

III. We describe here the ideas behind the work of Fouvry, Deshouillers - Iwaniec, Bombieri - Friedlander - Iwaniec which have led to the first non-trivial results on the distribution of $\psi(x;q,a)$ for fixed a and large q, beyond $x^{1/2}$ with some applications.
The arguments here are rather technical and we have chosen not to give too much detail, leaving that to a reading of the relevant literature.

We deal here with a bilinear form

$$\sum_{\substack{q\sim Q\\(q,a)=1}} \gamma_q \Delta_{\alpha*\beta}(x;q,a)$$

where we assume in addition that α has support in $m \sim M$, β has support in $n \sim N$, where $MN = x$ and $x^{\varepsilon} < M < x^{1-\varepsilon}$, $x^{\varepsilon} < N < x^{1-\varepsilon}$ for some fixed $\varepsilon > 0$. The "weights" γ_q are fairly arbitrary, subject to

$$|\gamma_q| \le \tau(q)^{B_1}$$

for some B_1. Ideally, one would choose $\gamma_q = \operatorname{sign} \Delta_{\alpha*\beta}(x;q,a)$ and obtain non-trivial bounds for $\sum_{\substack{q\sim Q\\(q,a)=1}} |\Delta_{\alpha*\beta}(x;q,a)|$. The most optimistic conjecture, similar to the Elliott-Halberstam conjecture, would be :

Conjecture.- With the above hypotheses on α, β then, if β also satisfies a Siegel - Walfisz condition, we have for any $A > 0$ and a suitable $B = B(A) > 0$:

$$\sum_{\substack{q<x\ell^{-B}\\(q,a)=1}} |\Delta_{\alpha*\beta}(x;q,a)| \ll \|\alpha\| \cdot \|\beta\| x^{1/2}\ell^{-A},$$

the implied constant depending only on A and ε.

This cannot yet be done, even replacing $x\ell^{-B}$ by Q with $Q = x^{\vartheta}$ for some $\vartheta > \frac{1}{2}$. At the present moment, the class of weights γ_q for which a useful result for $\sum_{\substack{q\sim Q \\ (q,a)=1}} \gamma_q \Delta_{\alpha*\beta}(x;q,a)$ can be proved depends on the relative size of the supports M, N for α, β.

In what follows, we shall write EMT (for Expected Main Term) as an abbreviation for the expected asymptotics. Thus, if we write an expression $\sum_{n\equiv a(\mathrm{mod}\ q)} f(n) - \mathrm{EMT}$, the EMT is $\frac{1}{\varphi(q)} \sum_{(n,q)=1} f(n)$, at least in the case $(q,a) = 1$. This simplifies very much the formulae and helps to follow the steps in the estimates. The general philosophy is that the handling of the EMT's, although not necessarily easy, can be done by standard techniques and therefore one must concentrate one's attention on the handling of remainder terms.

Let us consider the general sum

$$\mathcal{D} = \sum_{\substack{q\sim Q \\ (qr,a)=1}} \sum_{r\sim R} \gamma_q \delta_r \left(\sum_{\substack{m\sim M \\ mn\equiv a(\mathrm{mod}\ qr)}} \sum_{n\sim N} \alpha_m \beta_n - \mathrm{EMT} \right),$$

where the "weights" γ_q, δ_r satisfy

$$|\gamma_q| \leq \tau^{B_1}(q), \quad |\delta_r| \leq \tau^{B_1}(r).$$

We start with an application of Cauchy's inequality

$$\mathcal{D}^2 \leq \|\delta\|^2 \|\alpha\|^2 \mathcal{S}$$

where

$$\mathcal{S} = \sum_{\substack{r\sim R \\ (r,am)=1}} \sum_{m\sim M} \left\{ \sum_{\substack{q\sim Q \\ (q,am)=1}} \gamma_q \left(\sum_{\substack{n\sim N \\ mn\equiv a(\mathrm{mod}\ qr)}} \beta_n - \mathrm{EMT} \right) \right\}^2$$

and we want to show that

$$\mathcal{S} \ll \|\beta\|^2 xR^{-1}\ell^{-A}$$

for any $A > 0$.

We begin with a smoothing of the above sum, by replacing it with

$$\mathcal{S}^* = \sum_{\substack{r\sim R \\ (r,am)=1}} \sum_{m=-\infty}^{\infty} f\left(\frac{m}{M}\right) \left\{ \sum_{\substack{q\sim Q \\ (q,am)=1}} \gamma_q \left(\sum_{\substack{n\sim N \\ mn\equiv a(\mathrm{mod}\ qr)}} \beta_n - \mathrm{EMT} \right) \right\}^2$$

where $f(t)$ is a C^∞ function such that

$$f(t) = 1 \quad \text{if} \quad 1 \le t \le 2$$

$$f(t) \ge 0 \quad \text{everywhere}$$

$$f(t) = 0 \quad \text{if} \quad t < \frac{1}{2} \quad \text{or} \quad t > 3 .$$

By squaring $\{\dots\}^2$, we write

$$\mathcal{S}^* = S_1 - 2 S_2 + S_3$$

where

$$S_1 = \sum_{(am,r)=1} \sum f\left(\frac{m}{M}\right) \left(\sum_{(q,am)=1} \gamma_q \sum_{mn \equiv a \pmod{qr}} \beta_n \right)^2 ,$$

$$S_2 = \sum_{(am,r)=1} f\left(\frac{m}{M}\right) \sum_{(am,q_1q_2)=1} \frac{\gamma_{q_1}\gamma_{q_2}}{\varphi(q_2r)} \sum\sum_{\substack{mn_1 \equiv a \pmod{q_1r} \\ (n_2,q_2r)=1}} \beta_{n_1} \beta_{n_2} ,$$

$$S_3 = \sum_{(am,r)=1} f\left(\frac{m}{M}\right) (EMT)^2 .$$

For S_3 one uses Poisson's summation formula in the form

Lemma.- For $H \ge q^{1+\varepsilon} M^{-1}$, *we have*

$$\sum_{m \equiv a \pmod{q}} f\left(\frac{m}{M}\right) = \frac{M}{q} \sum_{|h|<H} \hat{f}\left(\frac{Mh}{q}\right) e\left(-\frac{ah}{q}\right) + O\left(\frac{1}{q}\right) .$$

The lemma easily implies

$$\sum_{(m,r)=1} f\left(\frac{m}{M}\right) = \frac{\varphi(r)}{r} M \hat{f}(0) + O(\tau(r))$$

and this in turn yields the estimate

$$S_3 = M \hat{f}(0) X + O(N \|\beta\|^2 R^{-1} \mathcal{L}^{B_1})$$

with

$$X = \sum_{(a,rq_1q_2)=1} \frac{\varphi(q_1q_2r)}{q_1q_2r\varphi(q_1r)\varphi(q_2r)} \gamma_{q_1} \gamma_{q_2} \sum\sum_{(n_i,q_ir)=1} \beta_{n_1} \beta_{n_2} .$$

For S_2, a similar estimate yields

$$S_2 = M \hat{f}(0) X + O(N \|\beta\|^2 Q \mathcal{L}^{B_1}) ,$$

which is still useful provided $NQR < x^{1-\varepsilon}$, for some $\varepsilon > 0$.

The estimate for S_1 is the most difficult and extracting from it the main term $M\hat{f}(0)X$ requires the Siegel - Walfisz hypothesis for β . We have

$$S_1 = \sum_{(am,r)=1} \sum f\left(\frac{m}{M}\right) \sum_{(am,q'q'')=1} \sum \gamma_{q'} \gamma_{q''} \sum_{\substack{mn_1 \equiv a \pmod{q'r} \\ mn_2 \equiv a \pmod{q''r}}} \sum \beta_{n_1} \beta_{n_2} .$$

Let $q_0 = (q',q'')$, $q_1 = q'/q_0$, $q_2 = q''/q_0$. The congruences $mn_1 \equiv a \pmod{q'r}$, $mn_2 \equiv a \pmod{q''r}$ can be replaced by a single congruence $m \equiv \mu \pmod{q_0q_1q_2r}$ where μ is determined by $\mu n_1 \equiv a \pmod{q_0q_1r}$, $\mu n_2 \equiv a \pmod{q_0q_2r}$. The part of the sum with large q_0 , specifically $q_0 > \ell^{A+B_2}$ for some B_2 , can be estimated directly and shown to be unimportant ; similarly, one estimates the sum where $(n_1, n_2) > \ell^{A+B_2}$. This means that we have to deal only with q_0 and (n_1, n_2) smaller than ℓ^{A+B_2} . The treatment of the sum is now greatly simplified if one assumes that $\beta_n = 0$ if n has a prime factor $< \ell^{A+B_2}$, since this allows us to assume $(n_1, n_2) = 1$ and also n_1 , n_2 squarefree. The removal of small prime factors (up to ℓ^{A+B_2}) can be obtained by an elementary sieve technique, which we assume we have done here already. This being said, summation over m yields

$$\sum_{m \equiv \mu \pmod{q_0q_1q_2r}} f\left(\frac{m}{M}\right) = \frac{M}{q_0q_1q_2r} \sum_{|h| \leq H} \hat{f}\left(\frac{Mh}{q_0q_1q_2r}\right) e\left(\frac{-\mu h}{q_0q_1q_2r}\right) + O\left(\frac{1}{q_0 Q^2 R}\right)$$

and, since $(n_1, n_2) = 1$, we have

$$\frac{\mu}{q_0q_1q_2r} \equiv a \frac{n_1 - n_2}{q_0 r} \frac{\overline{n_2q_1}}{n_1q_2} + \frac{a}{q_0q_1q_2rn_1} \pmod 1 ,$$

where $\overline{n_2q_1}$ denotes the inverse of $n_2q_1 \pmod{n_1q_2}$.

Since a is fixed, $\frac{a}{q_0q_1q_2rn_1} \ll \frac{1}{q_0 Q^2 RN}$ and since we can take

$$H = x^{\varepsilon_M - 1} Q^2 R ,$$

we see that

$$\sum_{m \equiv \mu \pmod{q_0q_1q_2r}} f\left(\frac{m}{M}\right) = \frac{1}{q_0q_1q_2r} \sum_{|h| < H} \hat{f}\left(\frac{Mh}{q_0q_1q_2r}\right) e\left(ah \frac{n_2 - n_1}{q_0 r} \frac{\overline{n_2q_1}}{n_1q_2}\right) + O(x^{2\varepsilon - 1}) .$$

On the assumption that $NQ^2R < x^{2-\varepsilon}$, one finds

$$S_1 = M\hat{f}(0) X_1 + R_1 + O(\|\beta\|^2 x R^{-1} \ell^{-A})$$

where

$$X_1 = \sum_{q_0 < \ell^{A+B_1}} \sum_{r \sim R} \sum\sum_{\substack{(q_1,q_2)=1 \\ (a,q_0q_1q_2r)=1}} \frac{\gamma_{q_0q_1}\,\gamma_{q_0q_2}}{q_0q_1q_2r} \sum\sum_{\substack{(n_1q_2,n_2q_1)=1 \\ n_1 \equiv n_2 \pmod{q_0 r}}} \mu^2(n_1n_2)\,\beta_{n_1}\,\beta_{n_2}\,,$$

and where

$$R_1 = \sum_{q_0 < \ell^{A+B_1}} \sum_{r \sim R} \sum\sum_{\substack{(q_1,q_2) \\ (a,q_0q_1q_2r)=1}} \frac{\gamma_{q_0q_1}\,\gamma_{q_0q_2}}{q_0q_1q_2r}$$

$$\sum\sum_{\substack{(n_1q_2,n_2q_1)=1 \\ n_1 \equiv n_2 (q_0 r)}} \mu^2(n_1n_2)\,\beta_{n_1}\,\beta_{n_2} \sum_{1 \le |h| \le H} M\,\hat{f}\left(\frac{hM}{q_0q_1q_2r}\right) e\left(ah\,\frac{n_2 - n_1}{q_0 r}\,\overline{\frac{n_2q_1}{n_1q_2}}\right).$$

The expression X_1 is different from X occurring in S_2 and S_3 and one needs to show that we can replace X_1 by X up to an admissible remainder term ; this is done by means of an application of Theorem 21. Now the terms involving X cancel out in $S_1 - 2\,S_2 + S_3$, leaving

$$\mathcal{S} \le R_1 + O(\|\beta\|^2 x R^{-1} \ell^{-A}) .$$

The hard part now consists in showing that R_1 is a relatively small remainder term.

The estimation of R_1 is now achieved in various ways, arranging the sum as $\sum \ldots \sum \mid \sum_{*\ldots*} \ldots \sum_{*\ldots*} \mid$ where $*\ldots*$ denote a well-chosen subset of variables.

Let us consider now the special case $R = 1$ and for simplicity the subcase $q_0 = 1$. We need to estimate

$$R_1 = \sum_{\substack{q_1,q_2 \\ (q_1q_2,a)=1}} \frac{\gamma_{q_1}\,\gamma_{q_2}}{q_1q_2} \sum_{(n_1q_2,n_2q_1)=1} \beta_{n_1}\,\beta_{n_2} \sum_{1 \le |h| \le H} M\,\hat{f}\left(\frac{Mh}{q_1q_2}\right) e\left(ah(n_2 - n_1)\,\overline{\frac{n_2q_1}{n_1q_2}}\right).$$

The function $\hat{f}$ is a smooth function and the fact that q_1 , q_2 appear in it is unimportant. In fact at this stage, one has

$$M\,\hat{f}\left(\frac{hM}{q_1q_2}\right) = q_1q_2 \int_{-\infty}^{\infty} f\left(\frac{\xi\,q_1q_2}{M}\right) e\,(h\xi)\,d\xi$$

which separates the variables h and q_1q_2 into an oscillating part $e(h\xi)$ and the non-oscillating part $q_1q_2\,f\left(\frac{\xi\,q_1q_2}{M}\right)$. By using Cauchy's inequality, we now remove the terms with the γ_{q_i} and f and replace R by a factor times the square root of

$$\max_{\xi} \sum_{\substack{q_1,q_2 \\ (q_1,q_2)=1}} g(q_1,q_2) \Big| \sum_h e(\xi h) \sum_{\substack{(n_1q_2,n_2q_1)=1 \\ n_1 \neq n_2}} \beta_{n_1} \beta_{n_2} e\Big(ah(n_2-n_1) \frac{\overline{n_2q_1}}{n_1q_2}\Big)\Big|^2$$

where $g(q_1,q_2)$ is a smooth function equal to 1 if $q_i \sim Q$ and supported in $\frac{1}{2} Q < q_i < 3 Q$. In order to obtain the required estimate for R we have to save somewhat more than H^2 with respect to the trivial estimate.

The simplest way of doing this consists in squaring the term $|\ldots|^2$ and making the summation over q_1, keeping everything else fixed. The sum over q_1 is now an exponential sum of the type

$$\sum_{q_1 \sim Q} e\left(\frac{b\,\bar{q}_1}{n_1n_3q_2}\right)$$

for some b, or in other words an incomplete Kloosterman sum to the modulus $n_1n_3q_2$. By Weyl's estimate for Kloosterman sums we obtain in general a bound $(N^2 Q)^{1/2+\varepsilon}$ for such a sum, which represents a gain of $(N^{-2} Q)^{1/2-\varepsilon}$ over the trivial bound. Thus the estimate is useful if

$$H^2 < x^{-\varepsilon} N^{-1} Q^{1/2},$$

that is

$$Q^{7/2} N^3 < x^{2-\varepsilon}.$$

This means that we can choose $Q = x^{\vartheta}$ with $\vartheta > \frac{1}{2}$ if N is small, say $N < x^{\frac{1}{12}-\varepsilon}$ for some $\varepsilon > 0$.

The more complicated estimates arise if one uses the Deshouillers - Iwaniec powerful result on bilinear forms with Kloosterman sum coefficients. This allows one to obtain useful results, say with $Q = x^{\vartheta}$ for some $\vartheta > \frac{1}{2}$, if $N < x^{1/6-\varepsilon}$.

Here are two results obtained by this method by Bombieri - Friedlander - Iwaniec.

THEOREM 23.- *Let* $a \neq 0$ *and let* $R < x^{1/10-\varepsilon}$. *For any* $A > 0$ *there exists* $B = B(A) > 0$ *such that provided* $Q R < x\, \ell^{-B}$ *we have*

$$\sum_{\substack{r \leq R \\ (r,a)=1}} \Big| \sum_{\substack{q \leq Q \\ (q,a)=1}} \Big(\psi(x;qr,a) - \frac{x}{\varphi(qr)}\Big)\Big| \ll x\, \ell^{-A},$$

with the constant implied in $\ll$ *dependent on* a, ε *and* A.

THEOREM 24.- *Let* $a \neq 0$, $x,y \geq 3$ *and* $Q \leq x^{1/2} y$. *Then*

$$\sum_{\substack{Q<q\le 2Q\\(q,a)=1}} \left| \pi(x;q,a) - \frac{li(x)}{\varphi(q)} \right| \ll \frac{x}{\log x} \left(\frac{\log y}{\log x}\right)^2 (\log\log x)^c$$

where c *is an absolute constant and the constant implied in* $\ll$ *depends on* a *alone.*

An application of Theorem 23, obtained independently by Bombieri - Friedlander - Iwaniec and Fouvry, is the full asymptotic for the *Titchmarsh Divisor Problem* : *Let* $a \neq 0$. *For any* $A > 0$ *we have*

$$\sum_{|a|<n\le x} \Lambda(n)\,\tau(n+a) = c_1(a)\, x \log x + c_2(a)\, x + O(x\ell^{-A}) ,$$

where

$$c_1(a) = \frac{\zeta(2)\,\zeta(3)}{\zeta(6)} \prod_{p\mid a} \left(1 - \frac{p}{p^2-p+1}\right)$$

and

$$c_2(a) = c_1(a) \left\{ 2 \sum_{p\mid a} \frac{p^2 \log p}{(p-1)(p^2-p+1)} - 2 \sum_{p} \frac{\log p}{p^2-p+1} + 2\gamma - 1 \right\} .$$

ADDITIONAL REFERENCES

[1] E. BOMBIERI, J.B. FRIEDLANDER and H. IWANIEC - *Primes in progression to large moduli*, *Acta Math.*, 156 (1986), 203-251.

[2] J.-M. DESHOUILLERS and H. IWANIEC - *Kloosterman sums and Fourier coefficients of cusp forms*, Invent. Math 70 (1982), 219-288.

[3] P.D.T.A. ELLIOTT and H. HALBERSTAM - *A conjecture in prime number theory*, Symp. Math. 4 (INDAM Rome, 1968-69), 59-72.

[4] E. FOUVRY - *Répartition des suites dans les progressions arithmétiques*, Acta Arith. 41 (1982), 359-382.

[5] E. FOUVRY - *Autour du théorème de Bombieri - Vinogradov*, Acta Math. 152 (1984), 219-244.

[6] E. FOUVRY and H. IWANIEC - *On a theorem of Bombieri - Vinogradov type*, Mathematika 27 (1980), 135 - 172.

[7] E. FOUVRY and H. IWANIEC - *Primes in arithmetic progressions*, Acta Arith. 42 (1983), 197-218.

[8] D.R. HEATH - BROWN - *Prime numbers in short intervals and a generalized Vaughan identity*, Can. J. Math. 34 (1982), 1365-1377.

[9] C. HOOLEY - *On the Barban - Davenport - Halberstam Theorem III*, J.L.M.S. (2), 10 (1975), 249-256.

[10] Y. MOTOHASHI - *An induction principle for the generalization of Bombieri's Prime Number Theorem*, Proc. Japan Acad. 52 (1976), 273-275.

[11] R.C. VAUGHAN - *An elementary method in prime number theory*, Acta Arith. 37 (1980), 111-115.