PUBLICATIONS MATHEMATIQUES D'ORSAY

81.01

JOURNÉES DE THÉORIE ANALYTIQUE ET ÉLÉMENTAIRE DES NOMBRES

ORSAY, 2 ET 3 JUIN 1980

Université de Paris-Sud
Département de Mathématique
Bât. 425
91405 ORSAY France

Code-matière AMS : (Bẽjian) 10 K 30, (Deshouillers) 10 L 05, (Durand) 30 C 10, (Elliott) 10 02 - 10 H 25 (Erdös, Nicolas) 10 A 20, (Fouvry) 10 H 20, (Greaves) 10 H 30, (Meyer) 10 A 20 (Odoni) 10 H 15, (Tenenbaum) 10 H 15.

Mots-Clefs : (Bẽjian) Discrẽpance, (Deshouillers) Addition de suites, (Durand) Polynômes, (Elliott) Fonctions arithmẽtiques, (Erdös, Nicolas) Grandes valeurs de fonctions arithmẽtiques, (Fouvry) Grand crible, (Greaves) crible, (Meyer) Fonctions additives - Fonctions multiplicatives, (Odoni) Extensions galoisiennes, (Tenenbaum) Diviseurs.

PUBLICATIONS MATHEMATIQUES D'ORSAY

81.01

JOURNÉES DE THÉORIE ANALYTIQUE ET ÉLÉMENTAIRE DES NOMBRES

ORSAY, 2 ET 3 JUIN 1980

Université de Paris-Sud

Département de Mathématique

Bât. 425

91405 ORSAY France

JOURNÉES DE THÉORIE ANALYTIQUE ET ÉLÉMENTAIRE DES NOMBRES

ORSAY, 2 ET 3 JUIN 1980

INTRODUCTION.

Des journées de Théorie Analytique et Elémentaire des Nombres ont été organisées à Orsay les 2 et 3 juin 1980, avec l'aide financière de la Société Mathématique de France.

Ces journées ont réuni une cinquantaine de participants, dont 5 étrangers : P.D.T.A. Elliott (Boulder), G. Greaves (Cardiff), H. Iwaniec (Varsovie), R.W.K. Odoni (Exeter), W. Schmidt (Boulder).

Nous avons rassemblé dans ce fascicule les textes des différentes conférences sauf celle de W. Schmidt, qui sera publiée ailleurs.

TABLE DES MATIÈRES

SUR UNE CONSTANTE LIEE A LA DISCREPANCE DES SUITES.

R. BÉJIAN

Soient $x > 0$, k un intervalle du tore $\mathbb{T}$ et $u = (u_n)_n$ une suite sur $\mathbb{T}$; notons $A(k,x,u)$ le nombre des entiers $n \leq x$ pour lesquels u_n appartient à k. L'écart correspondant est la quantité définie par

$$E(k,x,u) = A(k,x,u) - x\ell(k)$$

où $\ell(k)$ désigne la longueur de l'intervalle k.

Les discrépances $D(x,u)$ et $D^*(x,u)$ à l'origine sont définies par

$$D(x,u) = \sup_k |E(k,x,u)|$$

$$D^*(x,u) = \sup_{0<a<1} |E([0,a[,x,u)|.$$

Nous définissons de même la discrépance en x relativement à un intervalle I du tore en posant

$$D_I(x,u) = \sup_{k \subset I} |E(k,x,u)| \ .$$

W. Schmidt (1) a montré l'existence d'une constante $C^* \geq \frac{1}{100}$ telle que pour toute suite u on ait $\overline{\lim_N} \frac{D^*(N,u)}{\log N} \geq C$. Par ailleurs pour la suite de Van der Corput nous avons $\overline{\lim_N} \frac{D^*(N)}{\log N} \leq \frac{1}{3 \log 2} = 0,48...$. Ceci prouve que la minoration précédente est la meilleure possible en ce qui concerne le logarithme, et que nous avons l'encadrement $0,01 \leq C^* \leq 0,48$. Nous pouvons donc chercher une meilleure estimation de C^* ;

comme $D^* \leq D \leq 2D^*$, il existe une constante C telle que pour toute suite u, $\overline{\lim_N} \frac{D(N,u)}{\log N} \geq C$ et le même problème se pose pour C.

Nous avons les encadrements

$$0,06... \leq C^* \leq 0,22...$$

$$0,12... \leq C \leq 0,38... .$$

Les majorations sont dues à H. Faure (2) et les minorations résultant du théorème suivant :

THEOREME.- *Pour tout intervalle I et toute suite u du tore, on a*

$$\overline{\lim_N} \frac{D_I(N,u)}{\log N} \geq \sup_{a>2} \frac{a-2}{4(a-1)\log a} = 0,1203... .$$

La démonstration du théorème repose sur deux grands lemmes. Le premier est analogue au lemme principal de W. Schmidt. Soit u une suite donnée ; notons K, L, L' trois intervalles du tore avec L et L' contenus dans K ; soit N un entier positif fixé et considérons la restriction à $[0,N[$ de la fonction $x \longrightarrow D_K(x)$; notons $\mathbb{T}_N$ le tore modulo N et soient x et y deux éléments de $\mathbb{T}_N$. Nous introduisons la quantité $h(L,L',x,y)$ définie comme étant le maximum des quatre quantités suivantes :

$$\inf_{a\in L} E([0,a[,]x,y]) - \sup_{a\in L'} E([0,a[,]x,y])$$

$$\inf_{a\in L'} E([0,a[,]x,y]) - \sup_{a\in L} E([0,a[,]x,y])$$

$$\inf_{a\in L} E([0,a[,]y,x]) - \sup_{a\in L'} E([0,a[,]y,x])$$

$$\inf_{a\in L'} E([0,a[,]y,x]) - \sup_{a\in L} E([0,a[,]y,x]).$$

LEMME 1. $D_K(x) + D_K(y) \geq \frac{1}{2}\{D_L(x)+D_L(y)+D_{L'}(x)+D_{L'}(y)\} + h(L,L',x,y)$.

Posons $h^+(L,L',x,y) = \sup\{0, h(L,L',x,y)\}$;

comme $L \subset K$, nous avons $D_L(x) \leq D_K(x)$ et par suite le lemme 1 est encore vrai avec $h^+(L,L',x,y)$.

LEMME 2. *Soient* $a > 2$, $\varepsilon \in]0, \frac{a-2}{4(a-1)}[$, $\frac{p}{q}$ *un rationnel de* $]0,1[$, *sous sa forme irréductible et* t *un entier positif.*

Posons $N_t = [a^{qt}]$ *la partie entière de* a^{qt} *et soit* $K = [\alpha,\beta[$ *un intervalle contenu dans* I, *de longueur* $\frac{\ell(I)}{a^i}$ *avec* $0 \le i \le pt-1$.

Posons $L = [\alpha, \alpha + \frac{\ell(K)}{a}[$ *et* $L' = [\beta - \frac{\ell(K)}{a}, \beta[$.

Alors il existe t_0 *tel que pour tout* $t \ge t_0$ *on ait :*

$$\text{(i)} \qquad M(K,N_t) \ge \frac{1}{2}\{M(L,N_t) + M(L',N_t)\} + \frac{a-2}{4(a-1)} - \varepsilon$$

$$\text{(ii)} \qquad M(I,N_t) \ge \frac{p}{q}\left(\frac{a-2}{4(a-1)} - \varepsilon\right)\frac{\log N_t}{\log A} \ ;$$

Dans ces minorations $M(K,N)$ *est la moyenne définie par* $\frac{1}{N}\int_0^N D_K(x)dx$.

Par itération la première minoration implique la seconde, et de la seconde résulte le théorème d'une manière assez classique. Le travail le plus long et le plus technique consiste à établir la minoration (i) ;

soient I_α un intervalle contenu dans $\mathbb{T}_N$, m_α son milieu, x un point de I_α et $y = 2m_\alpha - x$; il résulte du lemme 1 que

$$\int_{I_\alpha} D_K(x)dx > \frac{1}{2}\{\int_{I_\alpha} D_L(x)dx + \int_{I_\alpha} D_{L'}(x)dx\} + \frac{1}{2}\int_{I_\alpha} h^+(L,L',x,2m_\alpha - x)dx \ .$$

Envisageons une partition de $\mathbb{T}_N$ par une famille finie d'intervalles I_α ; en sommant sur α et en divisant par N la minoration précédente, nous obtenons

$$M(K,N) \ge \frac{1}{2}\{M(L,N) + M(L',N)\} + \frac{1}{2N}\sum_\alpha \int_{I_\alpha} h^+(L,L',x,2m_\alpha - x)dx \ .$$

Le problème consiste à trouver une partition de $\mathbb{T}_N$ pour laquelle la minoration correspondante fournisse un terme complémentaire $\frac{1}{2N}\sum_\alpha \int_{I_\alpha} h^+(L,L',x,2m_\alpha - x)dx$ qui soit le plus grand possible.

Les critères nécessaires pour obtenir une bonne partition de $\mathbb{T}_N$ résultent du lemme 1.

(1) *SCHMIDT W. Irregularities of distribution VII. Acta Arith. t. 21 p. 45-60 (1972).*

(2) *FAURE H. Discrépance des suites associées à un système de numération (à paraître)*

R. BEJIAN
Université de Provence
13331 MARSEILLE Cedex 3

THEORIE ADDITIVE ET POINTS ENTIERS SUR LES COURBES

J.M. DESHOUILLERS ET F. DRESS

Soit $\mathcal{A} = \{0 < a_1 < \ldots < a_L\}$ une suite finie strictement croissante de L entiers positifs et $r_2^{\mathcal{A}}(N)$ le nombre de manières d'écrire l'entier N comme somme de deux éléments de $\mathcal{A}$; le lecteur se convaincra sans peine de la validité de la majoration

$$r_2^{\mathcal{A}}(N) \leqslant L = \text{Card } \mathcal{A}$$

et de ce que cette majoration est meilleure possible (en choisissant $\mathcal{A} = \{1,2,3,\ldots,L\}$ et $N = L+1$).

Nous nous proposons ici d'indiquer comment ce résultat peut être amélioré lorsque l'on suppose la suite $\Delta^1\mathcal{A} = \{a_2-a_1, \ldots, a_L-a_{L-1}\}$ des différences premières de la suite $\mathcal{A}$ strictement croissante, ce que l'on peut également visualiser ainsi :

il existe une fonction $f : [1,L] \to \mathbb{R}$ croissante et strictement concave telle que pour tout entier $n \in [1,L]$, on ait $f(n) = a_n$, interprétation qui sera utile par la suite.

THEOREME 1.- *Pour toute suite finie $\mathcal{A}$ dont la suite $\Delta^1\mathcal{A}$ des différences premières est strictement croissante, on a $\forall N$:*

$$r_2(N) \leqslant 4(\text{Card } \mathcal{A})^{2/3}.$$

Ce résultat est le meilleur possible en cela qu'il existe une constante absolue positive c *telle que pour tout entier* L *on peut trouver une suite finie* $\mathcal{A}$ *à* L *éléments, telle que* $\Delta^1\mathcal{A}$ *soit strictement croissante et telle qu'on ait :*

$$\exists N \qquad r_2^{\mathcal{A}}(N) \geqslant c(\mathrm{Card}\,\mathcal{A})^{2/3} .$$

Le résultat suivant montre que l'exposant $2/3$ de la majoration du théorème 1 ne peut pas être arbitrairement réduit, même si l'on suppose que la suite $\Delta^n\mathcal{A}$ (où n est en entier "grand") des différences n-ièmes (i.e. $\Delta^n\mathcal{A} = \Delta^1(\Delta^{n-1}\mathcal{A})$) est strictement croissante.

THEOREME 2.- *Pour tout entier* L *suffisamment grand et tout entier positif* n *, il existe une suite finie* $\mathcal{A}$ *de cardinal* L *telle que*

(i) $\Delta^h\mathcal{A}$ *est strictement croissante*

(ii) $\exists N \qquad r_2^{\mathcal{A}}(N) \geqslant \frac{1}{2} L^{1/2}$.

Il résulte du théorème 1 que l'exposant $1/2$ de la minoration (ii) ne peut pas être remplacé par un nombre strictement supérieur à $2/3$ et nous sommes prêts a parier qu'en fait $1/2$ est le meilleur exposant possible... .

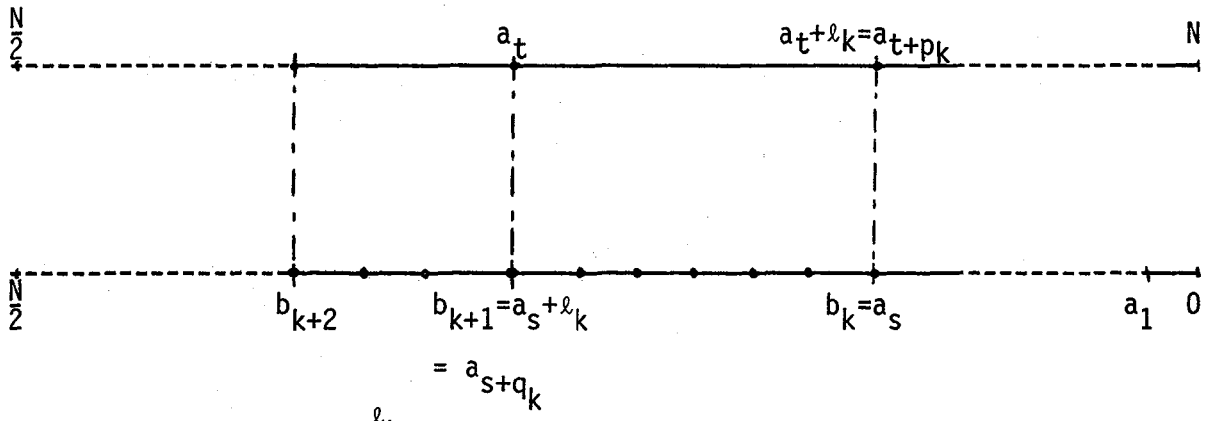
Nous démontrerons successivement la première partie du théorème 1, puis le théorème 2, puis la seconde partie du théorème 1 où nous réutiliserons, dans un contexte un peu plus sophistiqué le rapport qui apparaît entre la géométrie des nombres et la théorie additive.

§ 1. THEOREME 1 : démonstration de la majoration.

Soient $\mathcal{A}$ une suite finie de L entiers positifs telle que la suite $\Delta^1\mathcal{A}$ soit strictement croissante et N un entier positif. On notera $b_1 < b_2 < \ldots < b_K$ la sous-suite des éléments de $\mathcal{A}$ au plus égaux à $\frac{N}{2}$ et tels que $N - b_k$ soit également élément de $\mathcal{A}$; on a bien sûr $r_2^{\mathcal{A}}(N) \leqslant 2K$ et il suffit donc d'établir la majoration

$$K \leqslant 2L^{2/3} .$$

Soit k un entier de l'intervalle $[1,K-1[$; le nombre d'éléments de la suite $\mathcal{A}$ dans l'intervalle $]b_k, b_{k+1}]$ sera noté q_k ; on notera de même p_k le nombre d'éléments de la suite $\mathcal{A}$ dans l'intervalle $[N-b_{k+1}, N-b_k[$; enfin, la longueur de l'intervalle $]b_k, b_{k+1}]$ sera notée ℓ_k ; c'est également la longueur de l'intervalle $[N-b_{k+1}, N-b_k[$. Ces différentes notations sont résumées dans la figure ci-dessous



Le quotient $\frac{\ell_k}{q_k}$ qui représente l'écart moyen entre deux éléments de $\mathcal{A}$ de l'intervalle $]b_k,b_{k+1}]$ est strictement inférieur à $\frac{\ell_{k+1}}{q_{k+1}}$ puisque la suite $\Delta^1\mathcal{A}$ est strictement croissante, et de même le quotient $\frac{\ell_k}{p_k}$ est strictement supérieur à $\frac{\ell_{k+1}}{p_{k+1}}$; on a donc

$$\frac{\ell_k}{q_k} < \frac{\ell_{k+1}}{q_{k+1}} \qquad \text{et} \qquad \frac{\ell_k}{p_k} > \frac{\ell_{k+1}}{p_{k+1}}$$

d'où l'on déduit

$$\frac{q_{k+1}}{q_k} < \frac{\ell_{k+1}}{\ell_k} < \frac{p_{k+1}}{p_k}$$

et donc

$$\frac{p_k}{q_k} < \frac{p_{k+1}}{q_{k+1}} .$$

Par le même argument, le quotient $\frac{\ell_{K-1}}{q_{K-1}}$ est strictement inférieur à $\frac{\ell_{K-1}}{p_{K-1}}$ et donc $\frac{p_{K-1}}{q_{K-1}} < 1$.

On a la minoration

$$L \geqslant q_1 + \ldots\ldots + q_{K-1} + p_1 + \ldots\ldots + p_{K-1} + 1 \tag{1}$$

et en outre la relation

$$0 < \frac{p_1}{q_1} < \ldots\ldots < \frac{p_{K-1}}{q_{K-1}} < 1$$

qu'on utilisera sous la forme

$$\frac{1}{2} < \frac{q_{K-1}}{p_{K-1}+q_{K-1}} < \ldots\ldots < \frac{q_1}{p_1+q_1} < 1.$$

Définissons l'entier M par la relation

(2) $\qquad 2(1+2+\ldots+M) \leqslant K-1 < 2(1+2+\ldots+(M+1)).$

Parmi les nombres $p_1+q_1,\ldots, p_{K-1}+q_{K-1}$, dénominateurs de rationnels distincts de l'intervalle $]\frac{1}{2},1[$, au plus 1 est égal à 3 et 1 à 4, au plus 2 sont égaux à 5 et 2 à 6, etc... . Puisqu'il y en a au moins $2(1+2+\ldots+M)$, on a :

$$p_1+q_1+\ldots+p_{K-1}+q_{K-1} \geqslant 1.3+1.4+2.5+\ldots+M.(2M+1)+M.(2M+2)$$

d'où l'on déduit, grâce à (1) :

$$L \geqslant \frac{M(M+1)(8M+13)}{6} + 1.$$

Il résulte de (2) que l'on a $K \leqslant (M+1)(M+2)+2$ ce qui entraîne en particulier $K \leqslant 2.L^{2/3}$.

On notera que l'on peut bien sûr raffiner et améliorer la constante. De toute façon il faut commencer par introduire l'indicateur d'Euler pour obtenir une valeur optimale.

§ 2. DEMONSTRATION DU THEOREME 2.

Soit L un entier positif suffisamment grand ; on pose $M = [\sqrt{L}] + 3$ et on considère la fonction $f : [1,L] \to \mathbb{R}$ définie par $f(x) = M - \sqrt{M^2-x}$.

La fonction f est de classe $\mathcal{C}^\infty$ sur $[1,L]$, toutes ses dérivées y sont strictement positives, et en outre $f(M^2-\ell^2)$ (qui vaut $M-\ell$) est entier pour tout entier ℓ de l'intervalle $[\frac{M}{4}, \frac{3M}{4}]$.

L'entier n étant donné, on peut, en perturbant légèrement la fonction f, obtenir une fonction g de classe $\mathcal{C}^{(n+1)}$ sur $[1,L]$ telle que :

(3) $\forall\ m \leqslant n+1, \quad \forall\ x \in [1,L] \ : \ g^{(m)}(x) > 0$

(4) $\forall\ \ell \in [\frac{M}{4}, \frac{3M}{4}] \cap \mathbb{N}\ , \qquad g(M^2 - \ell^2) = M - \ell$

(5) $\forall\ \ell \in [1,L] \cap \mathbb{N}\ , \qquad g(\ell) \in \mathbb{Q}\ .$

Il nous reste à démontrer que la suite $\mathcal{A} = \{D\ g(\ell),\ \ell \in [1,L] \cap \mathbb{N}\}$, où D désigne un multiple commun aux dénominateurs des nombres rationnels $g(\ell)$ $(\ell = 1,\ldots,L)$ satisfait les conditions du Théorème 2. La première condition étant une conséquence facile de (3), nous nous attacherons à la deuxième. On pose $N := DM$. Pour tout entier $\ell \in [\frac{M}{4}, \frac{3M}{4}]$, il en est de même pour $M-\ell$ et on a

$$\begin{aligned} DM &= D(M-\ell) + D(M-(M-\ell)) \\ &= Dg(M^2-\ell^2) + Dg(M^2-(M-\ell)^2) \end{aligned}$$

et donc $r_2^{\mathcal{A}}(N) \geqslant \frac{M}{2} - 1 \geqslant \frac{1}{2} L^{1/2}$.

§ 3. THEOREME 1 (suite) : démonstration de la minoration.

Cette démonstration est basée sur le résultat suivant :

PROPOSITION (Jarník, 1925).- *Il existe deux constantes strictement positives* c_1 *et* c_2 *telles que pour tout entier positif* M, *on peut trouver une fonction* $f : [0,M] \to \mathbb{R}$ *telle que l'on ait :*

(6) $f(0) = 0, \quad f'(0) > 0, \quad f''(t) > 0$ *pour* $t \in [0,M]$

(7) $f(M) \leqslant c_2.M$

(8) $\exists\ 1 < u_1 < \ldots < u_K < M : \ u_k \in \mathbb{N},\ f(u_k) \in \mathbb{N},\ K > c_1 M^{2/3}.$

Nous allons démontrer que pour tout entier L de la forme $[2M + c_2M + 1]$ on peut trouver une suite $\mathcal{A}$ satisfaisant les conditions requises (avec en outre $c = c_1(2+c_2)^{-2/3}$).

3.1. Nous commencerons par indiquer sans démonstration un résultat concernant la stabilité d'une "fonction de Jarník" aux petites perturbations

LEMME.- *Soit* M *un entier positif donné et* f *une fonction de* $[0,M]$ *dans* $\mathbb{R}$ *satisfaisant (6), (7), (8).*

Il existe un nombre réel positif ε *tel que pour tout* M*-uplet* $(y_1,\dots,y_M)$ *de réels satisfaisant* $0 \leqslant y_m - f(m) \leqslant \varepsilon$ *, on peut trouver* $g : [0,M] \to \mathbb{R}$ *satisfaisant (6), (7) et :*

(9) *pour* $m \in [0,M] \cap \mathbb{N}$ *, on a* $g(m) = y_m$.

3.2. On pose $R := [M + c_2M + 1]$ et on choisit un rationnel positif tel que $(M+R)^2\delta < \min(1, \frac{\varepsilon}{2})$, où ε est associé à la fonction de Jarník par le lemme ci-dessus.

Pour $m \in [0,M]$, on choisit alors y_m rationnel dans l'intervalle $[f(m), f(m)+\varepsilon[$ avec les contraintes supplémentaires

- $y_0 = 0$
- $y_1 > (2R-1).\delta$ (loisible car $f(1) \geqslant 0$ et $(2R-1)\delta < \varepsilon$)
- $y_{u_k} = f(u_k) + 2(R+M)^2\delta - R^2\delta - (R - u_k - f(u_k))^2\,\delta$

(et alors on notera que y_{u_k} est bien rationnel).

3.3. On considère alors une fonction g satisfaisant (6), (7) et (9) et on pose

$$\begin{aligned}
\alpha_1 &= 1 + \delta - (R+M)^2\delta \\
&\vdots \\
\alpha_R &= R + R^2\delta - (R+M)^2\delta \\
&= R + 0 + g(0) + R^2\delta - (R+M)^2\delta \\
&\vdots \\
\alpha_{R+M} &= R + M + g(M) + R^2\delta - (R+M)^2\delta \ .
\end{aligned}$$

Tous ces termes étant rationnels, on en choisit un dénominateur commun D, et on pose

$$a_j = D.\alpha_j \quad (1 \leqslant j \leqslant L, \text{ avec } \quad L = R+M = [c_2M + 2M + 1]).$$

3.4. Pour montrer que la suite $\mathcal{A} = \{a_1 < \ldots < a_L\}$ est telle que $\Delta^1\mathcal{A}$ soit strictement croissante, on remarque

. que pour $1 \leqslant j \leqslant R-1$, la quantité $\alpha_{j+1} - \alpha_j = 1 + (2j+1)\delta$ est une fonction strictement croissante de j,

. que pour $1 \leqslant i \leqslant M$, il existe θ_1, θ_2, θ_3 positifs tels que

$$\alpha_{R+i+1} - \alpha_{R+i} = 1 + g(i+1) - g(i) = 1 + g'(i+\theta_1)$$

$$\alpha_{R+i} - \alpha_{R+i-1} = 1 + g(i) - g(i-1) = 1 + g'(i-\theta_2)$$

et donc

$$\alpha_{R+i+1} - 2\alpha_{R+i} + \alpha_{R+i-1} = g'(i+\theta_1) - g'(i-\theta_2)$$

$$= (\theta_1 - \theta_2)\, g''(\theta_3) > 0$$

. et qu'enfin

$$\alpha_{R+1} - 2\alpha_R + \alpha_{R-1} = 1 + g(1) - 1 - (2R-1)\delta > 0$$

par construction de $g(1)$.

3.5. Il suffit maintenant de démontrer que $2DR$ est somme d'au moins K façons de deux éléments de $\mathcal{A}$, ou que $2R$ est somme d'au moins K façons de deux éléments α_j. Pour tout entier k de l'intervalle $[1,K]$, on a en effet, d'après le choix y_{u_k} et de $g(u_k)$:

$$\alpha_{R+u_k} + \alpha_{R-u_k-f(u_k)} = R + u_k + g(u_k) + R^2\delta - (R+M)^2\delta + R - u_k - f(u_k) + (R-u_k-f(u_k))^2\delta$$

$$- (R+M)^2\delta = 2R\,.$$

J.M. DESHOUILLERS et F. DRESS
U.E.R. Mathématique et Informatique
Laboratoire associé au C.N.R.S. n° 226
Université de Bordeaux I

F 33405 TALENCE Cedex

RELATION DE SZEGÖ SUR LA DERIVEE D'UN POLYNOME

ALAIN DURAND

1. Si P est un polynôme à coefficients complexes de degré n, un célèbre théorème dû à Bernstein établit que

$$(*) \qquad \max_{|z|\leq 1} |P'(z)| \leq n \max_{|z|\leq 1} |P(z)| .$$

Ce résultat est à l'origine d'une masse importante de travaux, tant sur les polynômes algébriques $P(z) = \sum_{k=0}^{n} a_k z^k$, que sur les polynômes trigonométriques $f(\theta) = \sum_{k=0}^{n} (a_k \cos k\theta + b_k \sin k\theta)$. Un grand nombre de ces travaux ont visé à obtenir des inégalités plus précises que $(*)$ en faisant, par exemple, des hypothèses sur la localisation des racines du polynôme P. Il se trouve que ces derniers résultats peuvent être déduits, pour certains d'entre eux, d'une relation fondamentale, bien qu'hélas assez peu connue, et due à Szegö [9] (voir aussi de Bruijn [3]). Pour la formuler, convenons d'appeler <u>région circulaire</u> l'image du disque unité (ouvert ou fermé) par une transformation homographique non dégénérée $z \mapsto \gamma(z) = \frac{az+b}{cz+d}$. (Suivant la position du pôle éventuel de γ, une région circulaire est donc un disque ou son complémentaire, ou encore un demi-plan). La relation de Szegö s'énonce ainsi

<u>THEOREME</u>.- *Soit* $\mathcal{C}$ *une région circulaire. Soient* P *un polynôme de degré* $n \geq 1$ *et*

$$S = \{P(z) / z \in \mathcal{C}\} .$$

Alors pour tout couple $(\alpha,z) \in \mathcal{C} \times \mathcal{C}$, *on a*

$$(\alpha - z) \frac{P'(z)}{n} + P(z) \in S .$$

Notre but ici est de démontrer ce théorème et en donner quelques applications.

2. INEGALITE DE BASE.

La preuve donnée ici de la relation de Szegö s'appuie sur le résultat suivant

LEMME.- *Soient* $\omega_1,\dots,\omega_n$ *des nombres complexes tels que* $\lambda = \sup_{1\le j\le n} |\omega_j| \le 1$ *et* $\omega_j \neq -1$ $(j=1,\dots,n)$. *Alors*

$$\left| \sum_{1\le j\le n} \frac{\omega_j}{1+\omega_j} \right| \le \lambda \left| \sum_{1\le j\le n} \frac{1}{1+\omega_j} \right| .$$

Preuve. En écrivant $\omega_j = \lambda\ \alpha_j$ $(j=1,\dots,n)$, on doit donc montrer que

$$\left| \sum_{1\le j\le n} \frac{\alpha_j}{1+z\alpha_j} \right| \le \left| \sum_{1\le j\le n} \frac{1}{1+z\alpha_j} \right|$$

pour tout $(\alpha_1,\dots,\alpha_n,z) \in \mathbb{C}^{n+1}$ tel que $\max_{1\le j\le n} |\alpha_j| \le 1$ et $|z| < 1$ (cette relation sera alors aussi vérifiée, par continuité, si $|z| = 1$ avec $z\alpha_j \neq -1$ pour $j=1,\dots,n$). On raisonne par récurrence sur $n \ge 1$, le cas $n = 1$ étant évident. A l'ordre $n+1$ $(n \ge 1)$, par hypothèse de récurrence on peut alors écrire

$$\sum_{2\le j\le n+1} \frac{\alpha_j}{1+z\alpha_j} = n\,\frac{\gamma}{1+z\gamma}$$

avec γ tel que $|\gamma| \le 1$. On doit donc montrer que

$$\left|\frac{\alpha_1}{1+z\alpha_1} + \frac{n\gamma}{1+\gamma z}\right| \le \left|\frac{1}{1+\alpha_1 z} + \frac{n}{1+\gamma z}\right|$$

pour $|\alpha_1| \le 1$, $|\gamma| \le 1$ et $|z| < 1$, c'est-à-dire, sous les mêmes hypothèses,

$$|f(z,\alpha_1,\gamma)| \le 1$$

où f est définie par

$$f(z,\alpha_1,\gamma) = \frac{az + b}{cz + 1}$$

avec $a = \alpha_1\gamma$, $b = \dfrac{n\gamma+\alpha_1}{n+1}$ et $c = \dfrac{\gamma+n\alpha_1}{n+1}$.

Pour z fixé, $|z| < 1$, la fonction $(\alpha_1,\gamma) \to f(z,\alpha_1,\gamma)$ est analytique dans le polydisque $|\alpha_1| \le 1$, $|\gamma| \le 1$. Donc

$$\sup_{|\alpha_1|\le 1,\,|\gamma|\le 1} |f(z,\alpha_1,\gamma)| = \sup_{|\alpha_1|=|\gamma|=1} |f(z,\alpha_1,\gamma)|.$$

Or pour $|\alpha_1| = |\gamma| = 1$, on a $b = a\bar{c}$ et $|a| = 1$, d'où

$$|f(z,\alpha_1,\gamma)| = \left|\frac{z+\bar{c}}{cz+1}\right| \le 1$$

puisque $|z| < 1$ et $|c| \le 1$.

3. PREUVE DU THEOREME.

Soit $(\alpha,z) \in \mathfrak{C} \times \mathfrak{C}$ et posons $\omega = (\alpha - z)\frac{P'(z)}{n} + P(z)$. Si $\omega \notin S$, alors le polynôme $Q(u) = P(u) - \omega$ vérifie $Q(u) \neq 0$ pour tout $u \in \mathfrak{C}$. Pour obtenir une contradiction, il suffit donc de montrer que pour un tel polynôme

$$(\beta - u)\frac{Q'(u)}{n} + Q(u) \neq 0$$

pour tout $(\beta,u) \in \mathfrak{C} \times \mathfrak{C}$. (Cela revient à traduire le cas $0 \notin S$). Comme ceci est trivial si $\beta = u$, on peut supposer $\beta \neq u$ et en introduisant le polynôme

$$T(y) = Q(u + y(\beta - u))$$

pour $(\beta,u) \in \mathfrak{C} \times \mathfrak{C}$ fixé, il suffit par conséquent de montrer que si $\mathfrak{C}_1$ est une région circulaire contenant 0 et 1 ($\mathfrak{C}_1$ est ici l'image de $\mathfrak{C}$ par la similitude $\omega \mapsto \frac{\omega - u}{\beta - u}$) et si T est un polynôme de degré n ne s'annulant pas dans $\mathfrak{C}_1$, alors

$$(*) \qquad \frac{T'(0)}{n} + T(0) \neq 0.$$

Remarquons que si $\alpha_1, \ldots, \alpha_n$ sont les racines de T, on a

$$\frac{T'(y)}{T(y)} = \sum_{1\le j\le n} \frac{1}{y - \alpha_j}.$$

Ecrire que α_j n'appartient pas à $\mathfrak{C}_1$ revient à écrire (en tenant compte du fait que $0 \in \mathfrak{C}_1$ et $1 \in \mathfrak{C}_1$) :

$\frac{1}{\alpha_j} = 1 + (1-c)\left(\frac{\alpha z_j - 1}{bz_j + 1}\right)$ pour $j = 1, \ldots, n$ où $c \neq 1$, $|\alpha| \le 1$, $|b| \le 1$, $|z_j| \le 1$ et $\max\{|z_j|, |bz_j|\} < 1$. (La transformation homographique associée à $\mathfrak{C}_1$ est ici $z \mapsto \frac{z+b}{cz+d}$ avec $d = b + \alpha(1-c)$).

Sous ces hypothèses, la relation $(*)$ devient

$$\alpha \cdot \sum_{1\le j\le n} \frac{z_j}{1+bz_j} \neq \sum_{1\le j\le n} \frac{1}{1+bz_j},$$

ce qui est une conséquence directe du lemme précédent.

4. QUELQUES RESULTATS SUR LES POLYNOMES ALGEBRIQUES.

Si $P \in \mathbb{C}[x]$ est de degré n, on note

$P^*(z) = z^n \bar{P}(\frac{1}{z})$ $(\bar{P}(z) = \overline{P(\bar{z})}$ pour $|z| = 1)$ et $\|P\| = \sup_{|z|\leq 1} |P(z)|$.

Pour $|z| = 1$, il est facile de vérifier que

$$|P^{*\prime}(z)| = |n\, P(z) - z\, P'(z)|.$$

4.1. D'après la relation de Szegö, pour tout z, $|z| = 1$, le disque fermé de centre $P(z) - z\,\frac{P'(z)}{n}$ et de rayon $\frac{|P'(z)|}{n}$ est contenu dans l'ensemble $S = \{P(z) \,/\, |z| \leq 1\}$. En écrivant que S est contenu dans le disque fermé de centre 0 et de rayon $\|P\|$, ou encore que S est contenu dans la bande $\{\omega \in \mathbb{C} \,/\, |\mathrm{Re}\ \omega| \leq \sup_{|z|\leq 1} |\mathrm{Re}(P(z))|\}$, on obtient ainsi

LEMME 1.- *Soit $P \in \mathbb{C}[x]$ un polynôme de degré n. Alors pour $|z| = 1$*

$$n\,|P(z)| \leq |P'(z)| + |P^{*\prime}(z)| \leq n\|P\|$$

et

$$n\,|\mathrm{Re}(P(z))| \leq |P'(z)| + |\mathrm{Re}(n\,P(z) - z\,P'(z))| \leq n \cdot \sup_{|z|\leq 1} |\mathrm{Re}(P(z))|.$$

En particulier

$$\|P'\| \leq n \cdot \sup_{|z|\leq 1} |\mathrm{Re}(P(z))| \leq n\,\|P\|.$$

Remarquons au passage que si $P^* = \lambda P$, $\lambda \in \mathbb{C}$ (ce qui implique $|\lambda| = 1$), donc en particulier si P a toutes ses racines sur le cercle $|z| = 1$, alors $\|P'\| = \frac{n}{2}\|P\|$.

4.2. Supposons à présent que P n'ait pas de racines dans le disque $|z| < k$ $(k \geq 1)$. D'après la relation de Szegö, on a donc pour z fixé, $|z| < k$,

$$(\alpha - z)\,\frac{P'(z)}{n} + P(z) \neq 0$$

pour tout α tel que $|\alpha| < k$. On en déduit que la fonction continue $r \to r|P'(z)| - |n\,P(z) - z\,P'(z)|$ ne s'annule pas sur $[0,k[$, donc garde un signe constant et par suite $r|P'(z)| \leq |n\,P(z) - z\,P'(z)|$ pour $r \in [0,k[$, d'où $k|P'(z)| \leq |n\,P(z) - z\,P'(z)|$. Cette inégalité étant vérifiée pour $|z| < k$, elle est aussi vérifiée à la limite pour $|z| = 1$ (puisque $k \geq 1$). On a donc obtenu

LEMME 2.- *Soit $P \in \mathbb{C}[x]$ un polynôme non nul n'ayant pas de racines dans le disque $|z| < k$ $(k \geq 1)$. Alors pour $|z| = 1$*

$$k|P'(z)| \leq |P^{*\prime}(z)|.$$

Compte-tenu du lemme 1, on en déduit

LEMME 3.- *Soit* $P \in \mathbb{C}[X]$ *un polynôme de degré* $n \geq 1$ *n'ayant pas de racines dans le disque* $|z| < k$ $(k \geq 1)$. *Alors*

$$\|P'\| \leq \frac{n}{1+k} \|P\| .$$

En considérant le polynôme P^*, le lemme 3 permet de minorer $\|P'\|$ si on suppose que P a toutes ses racines dans le disque $|z| \leq k$ $(k < 1)$. On obtient en effet

$$\|P'\| \geq \frac{n+kj}{k+1} \|P\|$$

si $P(z) = z^j P_1(z)$ avec $P_1(0) \neq 0$.

En fait, une meilleure minoration peut être facilement obtenue.

LEMME 4.- *Soit* $P \in \mathbb{C}[X]$ *un polynôme non nul ayant toutes ses racines dans le disque* $|z| \leq 1$. *Alors pour* $|z| = 1$

$$|P'(z)| \geq \left(\sum_{\alpha, P(\alpha)=0} \frac{1}{1+|\alpha|} \right) |P(z)|.$$

Preuve : La relation est immédiate si z est racine de P. Sinon on écrit :

$$\left|\frac{P'(z)}{P(z)}\right| = \left|\frac{z\,P'(z)}{P(z)}\right| \geq \left|\mathrm{Re}\left(\frac{z\,P'(z)}{P(z)}\right)\right| = \sum_{\alpha, P(\alpha)=0} \frac{1-\mathrm{Re}(\alpha\bar{z})}{|z-\alpha|^2} .$$

Il suffit alors de remarquer que

$$\frac{1 - \mathrm{Re}(\beta)}{|1-\beta|^2} \geq \frac{1}{1+|\beta|}$$

si $|\beta| \leq 1$, $\beta \neq 1$.

Note : L'inégalité $\|P'\| \leq n\|P\|$ est connue sous le nom de théorème de Bernstein. On pourra se reporter par exemple aux livres de Bernstein [1] (Chap. I. § 10) et de Lorentz [7] (p. 40), ou encore à un article de Boas [2] (pour une forme généralisée de ce théorème).

L'inégalité meilleure $\|P'\| \leq n \sup_{|z|\leq 1} |\mathrm{Re}(P(z))|$ a quant à elle été obtenue par Szegö [10].

Les lemmes 2 et 3 sont dûs à Malik [8] (ainsi que le principe de

démonstration de ces lemmes). Par le résultat énoncé dans le lemme 3, Malik généralisait un théorème de Lax [6] (dont l'énoncé correspond au cas $k = 1$).

Le lemme 4 se trouve énoncé dans Giroux et al. [4], alors que la relation déduite du lemme 3 (avec $k = 1$) est due à Turan [11].

Parmi les très nombreux travaux concernant le théorème de Bernstein, citons, par exemple, ceux de Giroux, Rahman et Schmeisser ([4] et [5]).

5. DEUX INEGALITES SUR LES POLYNOMES TRIGONOMETRIQUES.

Si $$f(t) = a_0 + \sum_{k=1}^{n} (a_k \cos k t + b_k \sin k t)$$

est un polynôme trigonométrique de degré n, on note

$$\tilde{f}(t) = \sum_{k=1}^{n} (a_k \sin k t - b_k \cos k t)$$

et

$$\|f\| = \sup_{t \in \mathbb{R}} |f(t)|.$$

Remarquons que pour $z = e^{it}$, on a

$$z^n f(t) = z^n P(z) + P^*(z)$$

avec $P(z) = \frac{a_0}{2} + \sum_{k=1}^{n} \frac{(a_k - ib_k)}{2} z^k$.

5.1. Inégalité de Schaake. Van der Corput.

Soit f *un polynôme trigonométrique à ceofficients réels de degré* n. *Alors pour tout* $t \in \mathbb{R}$

$$(f'(t))^2 + n^2 (f(t))^2 \leq n^2 \|f\|^2 .$$

Preuve : Si $f(t) = a_0 + \sum_{k=1}^{n} (a_k \cos k t + b_k \sin k t)$, on a pour $z = e^{it}$

$$z^n f(t) = z^n P(z) + P^*(z) = Q(z)$$

avec $P(z) = \frac{a_0}{2} + \sum_{k=1}^{n} \frac{(a_k - ib_k)}{2} z^k$.

Donc Q est de degré $2n$ vérifiant $Q^* = Q$ et $\|Q\| = \|f\|$. Il vient

$$Q(e^{it}) = e^{int} f(t),$$

d'où

$$i\, e^{it} Q'(e^{it}) = e^{int}(f'(t) + i n f(t)),$$

et par conséquent, compte-tenu du lemme 1

$$(f'(t))^2 + n^2(f(t))^2 = |Q'(e^{it})|^2 \leq \left(\frac{2n}{2}\right)^2 \|Q\|^2 = n^2 \|f\|^2 .$$

5.2. Inégalité de Szegö.

Soit f *un polynôme trigonométrique à coefficients réels de degré* n. *Alors pour tout* $t \in \mathbb{R}$

$$|n\, f(t) - \tilde{f}'(t)| + \sqrt{(f'(t))^2 + (\tilde{f}'(t))^2} \leq n \|f\| .$$

Preuve : Là encore, on écrit pour $z = e^{it}$

$$z^n f(t) = z^n P(z) + P^*(z) = 2z^n \operatorname{Re}(P(z)). \tag{1}$$

Donc P est de degré n vérifiant $\sup_{|z|=1} |\operatorname{Re}(P(z)| = \frac{1}{2}\|f\|$. On obtient alors

$$f'(t) = 2 \operatorname{Re}(i\, e^{it} P'(e^{it})). \tag{2}$$

D'autre part, d'après la définition de $\tilde{f}'$, on a pour $z = e^{it}$

$$z^n \tilde{f}'(t) = z^n P_1(z) + P_1^*(z)$$

avec $P_1(z) = z\, P'(z)$, d'où

$$\tilde{f}'(t) = 2 \operatorname{Re}(e^{it} P'(e^{it})). \tag{3}$$

Des relations (2) et (3), on tire donc

$$\sqrt{(f'(t))^2 + (\tilde{f}'(t))^2} = 2|P'(e^{it})|.$$

D'autre part, des relations (1) et (3), on déduit

$$|n\, f(t) - \tilde{f}'(t)| = 2|\operatorname{Re}(n\, P(e^{it}) - e^{it} P'(e^{it}))|.$$

L'inégalité de l'énoncé se déduit du lemme 1 en notant que

$$\sup_{|z|=1} |\operatorname{Re}(P(z))| = \frac{1}{2}\|f\| .$$

REFERENCES

[1] S. BERNSTEIN. Leçons sur les propriétés extrêmales et la meilleure approximation des fonctions analytiques d'une variable réelle. Gauthier-Villars, Paris (1926).

[2] R.P. BOAS. The derivative of a trigonometric integral. J. London Math. Soc. 12 (1937), 164-165.

[3] N.G. de BRUIJN. Inequalities concerning polynomials in the complex domain. Nederl. Akad. Wetensch. Pro. 50 (1947), 1265-1272 = Indag. Math. 9 (1947), 591-598.

[4] A. GIROUX, Q.I. RAHMAN, G. SCHMEISSER. On Bernstein's inequality. Can. J. Math. 31 n° 2 (1979), 347-353.

[5] A. GIROUX, Q.I. RAHMAN. Inequalities for a polynomial with a prescribed zero. Trans. Amer. Math. Soc. 193 (1974), 67-98.

[6] P.D. LAX. Proof of a conjecture of P. Erdös on the derivative of a polynomial. Bull. Amer. Math. Soc. 50 (1944), 509-513.

[7] G.G. LORENTZ. Approximation of functions. Athena Series. Selected Topics in Math. Holt, Rinehart and Winston. USA (1966).

[8] M.A. MALIK. On the derivative of a polynomial. J. London Math. Soc. (2) 1 (1969), 57-60.

[9] G. SZEGŐ. Bermerkungen zu einem Satz von J.H. Grace über die Wurzeln algebraischer Gleichungen. Math. Z. 13 (1922), 28-55.

[10] G. SZEGŐ. Uber einen Satz des Herrn Serge Bernstein. Schriften der Königsberger Gelehrten Gesellschaft. 5 (1928), 59-70.

[11] P. TURAN. Uber die Ableitung von Polynomen. Compositio Math. 7 (1939), 89-95.

A. DURAND
Département de Mathématiques
Université de Limoges
123, Rue Albert Thomas

87060 LIMOGES Cedex

RECENT RESULTS IN THE THEORY OF ARITHMETIC FUNCTIONS.

P.D.T.A. ELLIOTT*

An arithmetic function $f(n)$ is said to be additive if it satisfies the relation $f(ab) = f(a) + f(b)$ for every pair of integers a,b with $(a,b) = 1$. An arithmetic function $g(n)$ is said to be multiplicative if in the same circumstances it satisfies $g(ab) = g(a)g(b)$. For our purposes nothing is lost if we restrict additive functions to having real values. Multiplicative functions may assume complex values.

This survey is based upon an invited address given at the two day meeting held in Orsay, Paris, on June the second and third, 1980. It is in two parts.

ADDITIVE FUNCTIONS.

The classical problems involving such functions are mainly concerned with value distribution, of the type considered in the theory of probability. An important early account of this study may be found in Kubilius [19]. More recently there is a short book of Babu [2], written in the spirit of Novoselov, and an extensive historical account by the author, Elliott [7], in two volumes. Taken together with the paper of Philipp [22] on the arithmetic simulation of Brownian motion, these cover the area quite well. Accordingly I shall move on to

* *Supported by a John Simon Guggenheim Foundation Fellowship.*

discuss the newer and not-fully-developed study of the differences of additive functions.

Here (as oft-times before) there is a pioneering result of Erdös [12], who proved that if $f(n+1) - f(n) \to 0$ as $n \to \infty$ then $f(n)$ must have the form $A \log n$ for some constant A, for all positive integers n. He could obtain the same result if, instead, $f(n)$ was assumed to be non-decreasing with n. In his paper Erdös raised a number of questions, two of which interest us here.

(1) Does the assumption

$$x^{-1} \sum_{n \le x} |f(n+1) - f(n)| \to 0, \quad x \to \infty,$$

force $f(n) = A \log n$?

(2) If $|f(n+1) - f(n)| \le c_1$ for some constant c_1 and all $n \ge 1$, must there be constants A and c_2 so that $|f(n) - A \log n| \le c_2$ for all $n \ge 1$?

The solution of these questions required new ideas. Question (1) was independently settled in the affirmative by Kátai [16] and Wirsing [24]. In fact Wirsing proved slightly more in the same paper.

Question (2) proved to be more difficult, and was settled by Wirsing [25], using a characteristically ingenious approach. Interestingly enough, a simple statistical model played an important role in his proof.

Two developments were pursued. The first is exemplified by the following two questions of Katai [17].

(3) Characterize those additive functions $f_i(n)$, $i = 1,\ldots,k$, $(k \ge 2)$ for which

$$f_1(n+1) + \ldots + f_k(n+k) \to 0,$$

as $n \to \infty$.

(4) If $a > 0$, b, $A > 0$, B are integers, $\begin{vmatrix} a & A \\ b & B \end{vmatrix} \neq 0$, characterize those additive functions $f(n)$ for which

$$f(an+b) - f(An+B) \to C$$

as $n \to \infty$, C a constant.

Progress in this area was mainly confined to $k = 2$, and small values of a,b, with $A = 1$, $B = 0$. See, for example, Kátai [17], Mauclaire [20].

The second line of development was due to Wirsing and Suck. Improving the work of Suck, Wirsing showed, in particular, that if $f(n)$ is completely additive ($f(ab) = f(a) + f(b)$ for every pair of integers a,b) and satisfies $f(n+1) - f(n) = o(\log n)$ as $n \to \infty$, then $f(n) = A \log n + o(\log n)$. This result is in a sense best-possible. Surprisingly a simple conclusion of this type cannot be drawn if we assume only that $f(n)$ is additive. Broadly speaking, Wirsing's method, which applies the theory of Markov chains, is successful if $f(n+1) - f(n) = O(\beta(n))$ where $\beta(n)$ does not exceed a not-too-large fixed power of $\log n$. An account of it is to appear in the printed proceedings of the conference in Number Theory held in Durham, England in the summer of 1979.

Independently, the present author developed a mean-square method which, besides giving similar results, allows questions of type (4) to be settled. For convenience of exposition we state two (typical) results for strongly-additive functions, those additive functions $f(n)$ which satisfy $f(p^m) = f(p)$, p, $m \geq 2$.

THEOREM 1 (Elliott).- *Let* $\beta(x) > 0$ *be an unbounded non-decrasing function of* x (≥ 1) *which satisfies*

$$\limsup_{x \to \infty} \beta(x^y)/\beta(x) < \infty$$

for each fixed $y > 0$. *Let* $a > 0$, $A > 0$, B *be integers,* $\begin{vmatrix} a & A \\ b & B \end{vmatrix} \neq 0$, *and let*

$$(5) \qquad \frac{1}{x\beta(x)^2} \sum_{n \leq x} |f(an+b) - f(An+B)|^2 \to 0, \quad x \to \infty.$$

Then there is a decomposition

$$(6) \qquad \sum_{p \leq x} \frac{f(p)}{p} = \alpha_1(x) + \alpha_2(x)$$

where for each fixed $y > 0$,

$$\alpha_1(x^y) = y\alpha_1(x) + o(\beta(x)) \quad , \quad \alpha_2(x^y) = \alpha_2(x) + o(\beta(x))$$

as $x \to \infty$. *Moreover,*

$$(7) \qquad \frac{1}{\beta(x)^2} \sum_{p \le x} \frac{1}{p}\Big(f(p) - \frac{\alpha_1(x)}{\log x} \log p\Big)^2 \to 0, \quad x \to \infty.$$

Conversely, (6) *with* (7) *imply the validity of* (5).

From this result, by means of the Selberg sieve method, one may readily deduce

THEOREM 2 (Elliott).- *In the notation of theorem 1 let*

$$f(an+b) - f(An+B) = o(\beta(n))$$

hold as $n \to \infty$.

Then there is a decomposition of the type at (6) *, and*

$$f(n) = \alpha_1(n) + o(\beta(n))$$

as $n \to \infty$.

It follows that if for some $y > 1$ we have

$$\limsup_{x \to \infty} \beta(x^y)/\beta(x) < y \ ,$$

then $\alpha_1(n)$ must have the form $D \log n + o(\beta(n))$. (See, for example, Elliott [7], volume II, lemma (11.8), pp. 8-11). Hence if $f(n+1) - f(n) = o((\log n)^\alpha)$ for $\alpha < 1$ then $f(n) = D \log n + o((\log n)^\alpha)$. If $\alpha > 1$ then a similar hypothesis leads to the (best-possible) conclusion $f(n) = o((\log n)^\alpha)$. However, from $f(n+1) - f(n) = o(\log n)$ we may conclude that $f(n) = \alpha_1(n) + o(\log n)$, where $\alpha_1(x^y) = y\alpha_1(x) + o(\beta(x))$. Thus $\alpha_1(x)$ behaves like a logarithm, but need not be one. This is consistent with (and gives another proof for) the result of Wirsing.

The same methods give

THEOREM 3 (Elliott).- *Let* $f(an+b) - f(An+B) = O(1)$ *for all* $n \ge n_0$ *for an additive function* $f(n)$. *Then there is a constant* D *so that* $f(n) = D \log n + O(1)$ *for all* n $(\ge n_1)$ *which are prime to* (a,A).

This result enables one to settle question (4) of Kátai. The condition that n is prime to (a,A) is necessary. For example if $a = A = 3$, $b = 1$, $B = 2$, then the hypothesis of theorem 3 tells us nothing about the behaviour of $f(n)$ on the powers 3^m.

The proof method of these three theorems works equally well if we consider two additive functions $f(an+b) - f'(An+B)$.

Most of these results are not yet published, although part of the proof of theorem 3 may be found in Elliott [11] (see also Elliott [10]).

More generally, one should now investigate functions of the form

$$L(n) = f_1(a_1n+b_1) + \ldots + f_k(a_kn+b_k), \quad k \geq 2 ,$$

where $\begin{vmatrix} a_i & b_i \\ a_j & b_j \end{vmatrix} \neq 0$ if $1 \leq i < j \leq k$. Furthermore a weaker hypothesis than that of (5) should be studied ; for example "$L(n)$ is small in frequency."

One may view our results so far in terms of a larger program. Consider the class of completely additive arithmetic functions $f(n)$. We extend the definition of $f(\ )$ to positive rational numbers by $f(a/b) = f(a) - f(b)$. It then satisfies $f(rs) = f(r) + f(s)$ for every pair of positive rational numbers r and s. Let $h(x)$ be a rational function of x with rational coefficients.

The program now consists of characterizing in terms of their behaviour on the prime numbers, those additive functions for which $f(h(n))$ increases slowly in some sense, e.g.

$$\sum_{n \leq x} f(h(n))^2 = O(x),$$

or $f(h(n)) = O(1)$.

The early results of this century considered the case $h(x) = x$. Our more recent studies of the differences of additive functions enable us to now consider $h(x) = (ax+b)/(Ax+B)$. Many questions naturally suggest themselves ; here are four.

(8) If $\frac{1}{x} \sum_{n \leq x} |f(an+b) - f(An+B)| \longrightarrow 0, \quad (x \to \infty)$,

must $f(n) = D \log n$ for $(n,a,A) = 1$? This question is still open as far as I know. For a survey of results in this direction see Mauclaire [20].

(9) If $\frac{1}{x} \sum_{n \le x} |f(n^2+1)| \to 0, \quad x \to \infty$,

must $f(p) = 0$ for every prime $p \equiv 1 \pmod 4$?

(10) If $f(n^3+1) = O(1)$ is $f(p) = O(1)$ for each prime p ?

(11) If $f(n^3+2) = O(1)$ is $f(p) = O(1)$ for those primes p which divide some integer of the form n^3+2 ?

I conclude this part of the survey by noting that there is an intimate connection between this larger study, and the representation of positive rational numbers r in the form

$$r = \prod_{i=1}^{k} h(s_i)^{\varepsilon_i}$$

where the s_i are positive rational integers, and each ε_i is $+1$ or -1. This connection was indicated by Wolke [27], Dress and Wolkmann [6]. Here an important rôle is played by Kátai's notion [18] of "sets of uniqueness."

Moreover, such representations are very helpful in the study of Dirichlet characters. Suppose, for example, that when r is an integer we can find suitable s_i in the range $1 \le s_i \le cr^{\theta}$, s_i an integer. Let χ be a character defined to the prime modulus p. If $\chi(h(m)) = 1$ for all positive integers $m \le cH^{\theta}$ then $\chi(r) = 1$ for all positive integers $r \le H$. According to a result of Burgess [3] one must have $H = O_{\varepsilon}(p^{1/4+\varepsilon})$ for each fixed $\varepsilon > 0$. Hence there exists an m exceeding $O_{\varepsilon}(p^{\theta/4+\varepsilon})$ for which $\chi(h(m)) \neq 1$.

MULTIPLICATIVE FUNCTIONS.

The classical and still unsolved problem is to give necessary and sufficient conditions in order that a multiplicative function $g(n)$ has a finite mean value

(12) $$A = \lim_{x \to \infty} x^{-1} \sum_{n \le x} g(n) .$$

There is an interesting application of these ideas to Ramanujan's τ-function. This function is defined by the identity

$$\sum_{n=1}^{\infty} \tau(n)x^n = x \prod_{j=1}^{\infty} (1 - x^j)^{24} .$$

It was conjectured by Ramanujan and proved by Mordell [21] that $\tau(n)$ is multiplicative. Hardy [14] proved that

$$d_1 x^{12} \leq \sum_{n \leq x} \tau(n)^2 \leq d_2 x^{12} , \qquad x \geq 1 ,$$

for positive constant d_1, d_2, and Rankin |23| sharpened this to an asymptotic estimate

$$\sum_{n \leq x} \tau(n)^2 = Fx^{12} + O(x^{12 - \mu})$$

for a certain $\mu > 0$.

Accordingly the function $g(n) = |\tau(n)|n^{-11/2}$ is multiplicative and belongs to the class L^2. In fact an integration by parts shows that $g^2( )$ has a non-zero mean value.

The general theory of multiplicative arithmetic functions now allows us to assert that <u>either</u>

$$\frac{1}{x} \sum_{n \leq x} |\tau(n)|n^{-11/2} \to 0 , \quad x \to \infty ,$$

<u>or</u> the series

$$\sum p^{-1} \left(\frac{|\tau(p)|}{p^{11/2}} - 1\right)^2$$

taken over the prime numbers, converges, and not both.

Without the use of Deligne's result that $|\tau(p)| < 2p^{11/2}$ we obtain

<u>THEOREM 4</u> (Elliott).- *Let* $0 < \delta < 2$ *hold. Then*

$$A_\delta = \lim_{x \to \infty} x^{-1} \sum_{n \leq x} \left(\frac{|\tau(n)|}{n^{11/2}}\right)^\delta$$

exists and is finite. Moreover, either every $A_\delta = 0$ *or the series*

$$\sum p^{-1} \left(\frac{|\tau(p)|}{p^{11/2}} - 1\right)^2$$

converges.

We do not even know what the conditions should look like. For general references see Hardy and Wright [15], Chapters 16, 17, 18, and Atkinson and Cherwell [1].

Assuming that $|g(n)| \leq 1$ for every positive n, Delange [5] gave necessary and sufficient conditions in order that $g(\ )$ should possess a non-zero mean-value.

Under the same condition on $g(\ )$ the case $A = 0$ was dealt with by Wirsing [26], when $g(\ )$ is essentially real, and Halász [13], in general. Their proofs were quite novel and changed our view of things considerably.

A detailed account of the relevant works of these three authors may be found in Volume one of the author's book, Elliott [7].

More recently the class L^{α} of arithmetic functions for which

$$\limsup_{x \to \infty} x^{-1} \sum_{n \leq x} |g(n)|^{\alpha}$$

is finite have been studied.

The author, Elliott [8] (see also Elliott [7], Volume 1, Chapter 10) gave necessary and sufficient conditions in order that a multiplicative function $g(n)$ belongs to the class L^2 and has a non-zero mean-value. Alternative proofs of the necessity part of the argument were given by Daboussi and Delange [4], and of the sufficiency part by W. Schwarz (Frankfurt).

More generally, the corresponding problem (with $A \neq 0$) has been settled for $\alpha > 1$ by the author (Elliott [9]) and by H. Daboussi (Orsay).

For the case $A = 0$ I have a slightly weaker result. Assume at the outset that $g(\ )$ belongs to the class L^{α}, for some $\alpha > 1$. Then necessary and sufficient conditions can be given in order for it to have the mean-value zero, (Elliott [9]).

In these results the methods of Wirsing and Halász play an important rôle, along with various ideas and results from the probabilistic theory of numbers.

We do not know a necessary and sufficient condition that a given multiplicative function belongs to the class L^{α}, $\alpha > 0$.

It follows from a conjecture of Sato and Tate that

$$\sum_{p<x} p^{-1}(|\tau(p)|p^{-11/2} - 1)^2 \sim 2 \operatorname{loglog} x , \quad x \to \infty .$$

One would therefore lay ones money on the possibility that the A_δ , $0 < \delta < 2$, are all zero.

REFERENCES

[1] F.V. ATKINSON, Lord CHERWELL. The mean values of arithmetical functions. Quart. J. Math. Oxford ser. 20 (1949), 65-79.

[2] G.J. BABU. Probabilistic Methods in the Theory of Arithmetic Functions. Macmillan, Delhi, 1978.

[3] D.A. BURGESS. On character sums and primitive roots. Proc. London Math. Soc. (3) 12 (1962), 179-192.

[4] H. DABOUSSI, H. DELANGE. On a theorem of P.D.T.A. Elliott on multiplicative functions. J. London Math. Soc. 14 (1976), 345-356.

[5] H. DELANGE. Sur les fonctions arithmétiques multiplicatives. Ann. Scient. Ec. Norm. Sup. 3e série t. 78 (1961), 273-304.

[6] F. DRESS and B. WOLKMANN. Ensembles d'unicité pour les fonctions arithmétiques additives ou multiplicatives. Comptes Rendus Acad. Sci. Paris, 287 A (1978), 43-46.

[7] P.D.T.A. ELLIOTT. Probabilistic Number Theory. Grundlehren series, vols. 239, 240. Springer, New York 1979, 1980.

[8] P.D.T.A. ELLIOTT. A mean-value theorem for multiplicative functions. Proc. London Math. Soc. (3) 31 (1975) 418-438.

[9] P.D.T.A. ELLIOTT. Mean value theorems for multiplicative functions bounded in mean α-power, $\alpha > 1$. J. Austral. Math. Soc. (Series A) 29 (1980), 177-205.

[10] P.D.T.A. ELLIOTT. On the differences of additive arithmetic functions. Mathematika 24 (1977), 153-165.

[11] P.D.T.A. ELLIOTT. Sums and differences of additive arithmetic functions in mean square. Journal für die reine und angewandte Mathematik 309 (1979) 21-54.

[12] P. ERDÖS. On the distribution function of additive functions. Annals Annals of Math. 47 (1946), 1-20.

[13] G. HÁLASZ. Über die Mittelwerte multiplikativer zahlentheorelischer Funktionen. Acta Math. Acad. Sci. Hungar. 19 (1968), 365-403.

[14] G.H. HARDY. Note on Ramanujan's arithmetic function $\tau(n)$. Math. Proc. Cambridge Philos. Soc. 23 (1927), 675-680.

[15] G.H. HARDY, E.M. WRIGHT. An introduction to the Theory of Numbers. Oxford (Fourth edition) 1960.

[16] I. KÁTAI. On a problem of P. Erdös. J. Number Theory 2 (1970), 1-6.

[17] I. KÁTAI. Some results and problems in the theory of additive functions. Acta Sc. Math. Szeged. 30 (1969), 305-311.

[18] I. KÁTAI. On sets characterizing number-theoretical functions. Acta Arithmetica XIII (1968), 315-320.

[19] J. KUBILIUS. Probabilistic Methods in the Theory of Numbers. Amer. Math. Soc. Translations of Math. Monographs, n° 11. Providence 1964.

[20] J.L. MAUCLAIRE. Sur la régularité des fonctions additives. Séminaire Delange-Pisot-Poitou, Théorie des Nombres 15, Paris, 1973/74, n° 23.

[21] L.J. MORDELL. On Mr. Ramanujan's empirical expansions of modular functions. Math. Proc. Cambridge Philos. Soc. 19 (1917), 117-124.

[22] W. PHILIPP. Arithmetic Functions and Brownian Motion. Amer. Math. Soc. Proceedings of Symposia in Pure Math., XXIV (1973), 233-246.

[23] R.A. RANKIN. Contributions to the theory of Ramanujan's function $\tau(n)$ and similar arithmetical functions. Math. Proc. Cambridge Philos. Soc. 35 (1934), 357-372.

[24] E. WIRSING. Characterization of the logarithm as an additive function. Amer. Math. Soc. Proc. of Symp. in Pure Math. XX (1971), 375-381.

[25] E. WIRSING. A characterization of $\log n$ as an additive function. Symposia Mathematica IV (1970), 45-57. Academic Press, London, New-York.

[26] E. WIRSING. Das asymptotische Verhalten von Summen über multiplikative Funktionen II, Acta. Math. Acad. Sci. Hungar. 18 (1967), 411-467.

[27] D. WOLKE. Bemerkungen über Eindeutigkeitsmengen additiver Funktionen. Elemente Math. 33 (1978), 14-16.

P.D.T.A. ELLIOTT
Department of Mathematics,
University of Colorado
BOULDER, COLORADO 80309,
U.S.A.

GRANDES VALEURS D'UNE FONCTION LIEE AU PRODUIT D'ENTIERS CONSECUTIFS

P. ERDÖS & J.L. NICOLAS

1. INTRODUCTION.

Soit $m \geq 1$, $k \geq 1$. On pose $\pi = \pi(m,k) = (m+1)\ldots(m+k)$ et pour $1 \leq i \leq k$, $\pi_i^* = \pi_i^*(m,k) = \frac{\pi(m,k)}{m+i}$.

On appelle $P(m,k)$ l'ensemble des n tels que $n|\pi$ et $\forall\, i$, $1 \leq i \leq k$, $n \nmid \pi_i^*$. Si $n \in P(m,k)$, on a $\forall\, i$, $1 \leq i \leq k$, $(m+i,n) > 1$. Si $n \in P(m,k)$, $\forall\, i$, $1 \leq i \leq k$, $\exists q$ premier, $q|n$ tel que $v_q(n) > v_q(\pi_i^*)$, en désignant par v_q la valuation q-adique.

Pour n fixé, on appelle $f(n)$ le plus grand k pour lequel il existe m tel que $n \in P(m,k)$. On a $f(n) \leq n$ et comme $m \equiv m' \bmod n$ entraîne $P(m,k) = P(m',k)$, on a :

$$f(n) = \max\{k\,;\, n \in P(m,k)\,;\, 1 \leq m \leq n\,;\, 1 \leq k \leq n\}\,.$$

Exemple : Soit $n = t!$. On a de façon évidente $t! \in P(1,t-1)$, ce qui entraîne $f(t!) \geq t-1$. D'autre part, pour tout $m \geq 1$, $t! | \pi(m,t)$, ce qui entraîne que $\forall\, m \geq 1$, $t! \notin P(m,t+1)$ et donc $f(t!) \leq t$. P. Erdös avait conjecturé que pour $n \geq 2k$, $\binom{n}{k}$ avait un diviseur de la forme $n-i$, $0 \leq i \leq k-1$. Dans l'article [Sch], A. Schinzel donnait le contre-exemple $n = 99215$, $k = 15$, et A. Schinzel et P. Erdös démontraient que la conjecture était fausse pour une infinité de n. Peut être existe-t-il une constante $c > 0$ telle que $\binom{n}{k}$ a un diviseur d vérifiant $cn \leq d \leq n$. Il en résulte pour la fonction f : pour $1 \leq t \leq 14$, $f(t!) = t-1$, $f(15!) = 15$, car $15! \in P(99200, 15)$ et pour une infinité de t, on a $f(t!) = t$.

L'étude de la fonction f est une généralisation du problème de Jacobstahl (cf. [Erd]), qui propose d'étudier $C(n)$ la longueur de la plus longue suite d'entiers tous non premiers avec n. On a : $f(n) \leq C(n)$. Le théorème 1 nous donnera une estimation asymptotique pour l'ordre maximum de $f(n)$. On connait beaucoup moins sur $C(n)$. (cf. [Iwa]). On trouvera d'autres résultats sur des sujets voisins dans [Sel] et [Gri].

Nous obtenons les résultats suivants :

THEOREME 1.- *Soit* $\omega(n) = \sum_{p|n} 1$; $\Omega(n) = \sum_{p|n} v_p(n)$; $\omega^*(n) = \sum_{p|n, p>\omega(n)} 1$.

Alors on a : $\omega^*(n) \leq f(n) \leq \Omega(n)$ *pour tout* n, *et* $\sum_{n\leq x} f(n) = (1+o(1)) x \log\log x$.

Il est faux que $\omega(n) \leq f(n)$: $f(120) = 3$.

THEOREME 2.- *L'ordre maximum de la fonction* $f(n)$ *est :*

$$\frac{e^{\gamma/2}}{2} \frac{\log n}{\sqrt{\log\log n}} + \frac{\gamma e^{\gamma}}{4} \frac{\log n}{\log\log n} (1+o(1))$$

où γ *est la constante d'Euler, ce qui veut dire que* $f(n)$ *est toujours inférieur ou égal à cette quantité, et qu'il y a égalité pour une infinité de* n.

THEOREME 3.- *On dit que* n *est* f*-hautement abondant si* $n' < n \Rightarrow f(n') < f(n)$

Il existe des constantes c_1 *et* $c_2 > 0$ *telles que, pour un nombre* n f*-h.a. assez grand, on ait, en posant* $k = f(n)$:

i) Si p *premier vérifie*

$$\log p \leq e^{-\gamma/2} \sqrt{\log k} \left(1 - \frac{c_1}{\sqrt[4]{\log k}}\right)$$

alors p *divise* n.

ii) Si p *premier vérifie*

$$e^{-\gamma/2} \sqrt{\log k} \left(1 + \frac{c_2}{\sqrt[4]{\log k}}\right) \leq \log p \quad \text{et} \quad p \leq k/2$$

alors p *ne divise pas* n.

iii) Si $p|n$ *et si* $p > k$, *alors tous les nombres premiers* q *tels que* $k < q < p$ *divisent* n *et le plus grand facteur premier* P *de* n *vérifie :*

$$P \sim e^{-\frac{1}{2}\log n}.$$

Pour étudier les grandes valeurs de la fonction f, nous avons défini, après Ramanujan (cf. [Ram]), les nombres f- h.a.. Les premières valeurs sont 2, 6, 24, 120, 560. On a $560 = 2^4.5.7 \in P(73,5)$, et c'est la forme de ce nombre, non multiple de 3 qui a fait deviner la forme générale des nombres f- h.a. donnée par le théorème 3.

La précision des résultats des théorèmes 2 et 3 est surprenante, si l'on compare avec ceux obtenus sur le problème de Jacobstahl par exemple (cf. [Erd]). De même si l'on considère la restriction f_Q de f à l'ensemble $Q = \{n ; p < q \Rightarrow v_p(n) \geq v_q(n)\}$ il est impossible de donner un équivalent pour l'ordre maximum de f_Q. On peut démontrer : $f_Q(n) \leq \frac{2 \log n}{\log \log n}(1+o(1))$ pour tout n. Mais on ne peut pas affirmer pour le moment l'existence de k entiers consécutifs tous multiples d'un nombre premier $p \leq k^{1-\varepsilon}$. La meilleure minoration est donc $f_Q(n) \geq \frac{\log n}{\log \log n}(1+o(1))$ pour une infinité de n (comprenant les valeurs $n = t!$).

L'outil fondamental dans les démonstrations des théorèmes 2 et 3 est le lemme suivant qui est un lemme de crible linéaire, et nous remercions H. Iwaniec pour ses remarques sur ce sujet.

LEMME de crible.- *Soit $\mathcal{A}$ un ensemble de X nombres entiers consécutifs. Soit $\mathcal{P}$ un ensemble de nombres premiers tels que :*

$$\sum_{\substack{p \leq X \\ p \in \mathcal{P}}} \frac{\log p}{p} \leq \lambda \sqrt{\log X}$$

où λ est un nombre positif fixé. On pose $W(z) = \prod_{\substack{p<z \\ p\in\mathcal{P}}} (1 - \frac{1}{p})$.

Soit $\mathcal{S}(\mathcal{A},\mathcal{P},z)$ l'ensemble des éléments de $\mathcal{A}$ divisibles par aucun nombre premier $p \in \mathcal{P}$, $p < z$, et $S(\mathcal{A},\mathcal{P},z) = \operatorname{Card} \mathcal{S}(\mathcal{A},\mathcal{P},z)$; alors on a : pour $1 \leq z \leq X$ $\exp(-\sqrt{\log X})$:

$$S(\mathcal{A},\mathcal{P},z) = X\, W(z)\left(1 + O\left(\frac{1}{\sqrt{\log X}}\right)\right)$$

et pour $1 \leq z \leq X$:

$$S(\mathcal{A},\mathcal{P},z) = X\, W(z)\left(1 + O\left(\frac{\log \log X}{\sqrt{\log X}}\right)\right)$$

où les O dépendent de λ, mais sont uniformes par rapport à $\mathcal{A},\mathcal{P},z$.

Malheureusement nous ne donnons pas de valeurs numériques aux constantes qui figurent dans les O, car elles sont difficilement calculables ; cela nous empêche d'expliciter c_1 et c_2 dans le théorème 3. On ne peut donc pas utiliser i et ii de ce théorème pour construire un algorithme de calcul des nombres f - h.a.

Le lemme suivant nous est également utile :

LEMME.- *Soit* $\mathcal{P}$ *une famille finie de nombres premiers. On pose :*

$$W(\mathcal{P}) = \prod_{p\in\mathcal{P}} (1-\frac{1}{p}) \; ; \quad S(\mathcal{P}) = \sum_{p\in\mathcal{P}} \frac{\log p}{p} \; ; \quad F(\mathcal{P}) = W(\mathcal{P})\, S(\mathcal{P}).$$

Il existe une constance $C > 0$ *telle que l'on ait :*

$$F(\mathcal{P}) \geq e^{-\gamma} - \frac{C}{S(\mathcal{P})}$$

où γ *est la constante d'Euler.*

Avec les résultats de Rosser et Schoenfeld, la fonction F *est croissante sur les ensembles* Q_ξ *des nombres premiers* $\leq \xi$.

On peut noter que la structure des nombres f - h.a. est très différente de celle des nombres hautement composés de Ramanujan, avec essentiellement deux blocs de facteurs premiers : les petits nombres premiers d'une part, et ceux plus grands que k/2 d'autre part. Notons aussi qu'au prix de calculs plus longs il est possible d'améliorer le développement asymptotique donné par le théorème 2.

Quelques problèmes non résolus : Désignant par $n_1, n_2, \ldots, n_j, \ldots$ la suite des nombres f - h.a. il ne nous a pas été possible de répondre aux questions suivantes : A-t-on toujours $f(n_{j+1}) - f(n_j) = 1$? ou même seulement $f(n_{j+1}) - f(n_j)$ est-elle bornée ? Existe-t-il $c > 0$ tel que $n_{j+1}/n_j = O(\log n_j)^c$?

REFERENCES

[Erd] P. ERDŐS. On the integers relatively prime to n and on a number theoretic function considered by Jacobstahl. Math. Scand., t. 10, 1962, p. 163-170.

[Gri] C.A. GRIMM. A conjecture on consecutive composite numbers. Amer. Math. Monthly t. 76, 1969, p. 1126-1128.

[Iwa] H. IWANIEC. On the error term in the linear sieve. Acta Arithmetica, t. 19, 1971, p. 1-30.

[Ram] S. RAMANUJAN. Highly composite numbers. Proc. London Math. Soc., Series 2, t. 14, 1915, p.347-400 ; and collected papers. Cambridge, at the University Press, 1927, p. 78-128.

[Ros] J.B. ROSSER and L. SCHOENFELD. Approximate formulas for some functions of prime numbers, Illinois J. of Math., t. 6, 1962, p. 64-94.

[Sch] A. SCHINZEL. Sur un problème de P. Erdös, Colloq. Math., t. 5, 1958, p. 198-204.

[Sel] P. ERDŐS and J.L. SELFRIDGE. Some problems on the prime factors of consecutive integers II. Proc. Washington State Univ. Conf. on number theory, 1971, p. 13-21. Math. Rew. t. 47, n° 5, 1974, # 6625.

P. ERDŐS et J.L. NICOLAS
Département de Mathématiques
U.E.R. des Sciences de Limoges
123, Avenue Albert Thomas

87060 LIMOGES Cédex.

UN RESULTAT VOISIN DU THEOREME DE BOMBIERI-VINOGRADOV

E. FOUVRY

1. NOTATIONS ET RESULTATS.

Si $\mathcal{E}$ est une suite d'entiers, on désigne par $\mathcal{E}(x)$, $\mathcal{E}_q$ et $\mathcal{E}(x\,;q,a)$ la suite des termes de $\mathcal{E}$ respectivement

inférieurs ou égaux à x,

divisibles par q,

inférieurs ou égaux à x et congrus à a modulo q.

La lettre p désignant toujours un nombre premier, on définit les fonctions

$$\pi(x,z) = \sum_{\substack{n\le x \\ p\mid n \Rightarrow p\ge z}} 1$$

et

$$\pi(x,z\,;q,a) = \sum_{\substack{n\le x \\ n\equiv a(\mathrm{mod}\ q) \\ p\mid n \Rightarrow p\ge z}} 1 \ .$$

Pour a entier, on considère l'inégalité :

$$(1) \qquad \forall\, A \quad \sum_{\substack{q\le Q \\ (q,a)=1}} \left|\pi(x,z\,;q,a) - \frac{1}{\varphi(q)}\,\pi(x,z)\right| \ll_A x\,(\log x)^{-A} \ .$$

(Q s'appelle le niveau de distribution, paramètre important dans les applications de méthodes de crible).

Le théorème de Bombieri-Vinogradov ([1],[7]) affirme que (1) est vraie pour $Q = x^{1/2-\varepsilon}$ et $z = x^{1/2}$ (en fait, ils traitaient la fonction $\pi(x\,;q,a)$ et

Bombieri trouva un résultat un peu plus fort). La valeur de Q n'a pas été améliorée et on conjecture que (1) est vraie pour $Q = x^{1-\varepsilon}$ et $z = x^{1/2}$ (conjecture d'Halberstam et Richert [5]).

Iwaniec et l'auteur ont montré qu'on peut dépasser la valeur $\frac{1}{2} - \varepsilon$ de l'exposant de Q, mais pour des valeurs de l'exposant de z très petites.

THEOREME 1.- *Si* $1 \leq |a| \leq x$, $Q = x^{\frac{11}{21}}$ *et* $z \leq x^{\frac{1}{883}}$ *l'inégalité* (1) *est vraie.*

La méthode employée s'applique à d'autres suites. Ainsi, soient $\mathcal{M} \subset \mathbb{N}$ vérifiant

(i) $\exists\, c \quad |\mathcal{M}(2x)| - |\mathcal{M}(x)| \gg x\,(\log x)^{-c}$

(ii) $\forall\, q \geq 2 \quad \forall\, A \quad |\mathcal{M}_q(x)| \ll_A x(\log x)^{-A}$

et $\mathcal{N} \subset \mathbb{N}$ vérifiant la condition (i) et

(iii) $\forall\, A \quad \forall\, (a,q) = 1 \quad |\mathcal{N}(x\,;q,a)| = \frac{|\mathcal{N}(x)|}{\varphi(q)} + O_A(x(\log x)^{-A})$.

A l'aide de $\mathcal{M}$ et $\mathcal{N}$ on construit la suite finie $\mathcal{A} = \mathcal{A}(\mathcal{M},\mathcal{N},M,N)$ des entiers $mn+a$ où $m \in \mathcal{M} \cap]M,2M]$ et $n \in \mathcal{N} \cap]N,2N]$ $(M,N \geq 2)$.

Rappelons la majoration des sommes de Kloosterman obtenue grâce aux travaux de A. Weil :

LEMME.- *Pour* $0 < \xi_2 - \xi_1 \leq b$, *on a*

$$\sum_{\substack{\xi_1 < k \leq \xi_2 \\ (k,b)=1}} e\left(d\,\frac{\bar{k}}{b}\right) \ll (b,d)^{1/2}\, b^{1/2}\tau(b)\log 2b.$$

Hooley a émis l'hypothèse, que dans le lemme précédent on peut tenir compte de l'intervalle de sommation. Plus précisément

HYPOTHESE R^* ([4]).- *Pour* $0 < \xi_2 - \xi_1 \leq b$, *on a*

$$\sum_{\substack{\xi_1 < k \leq \xi_2 \\ (k,b)=1}} e\left(d\,\frac{\bar{k}}{b}\right) \ll (\xi_2 - \xi_1 + 1)^{1/2}\,(d,b)^{1/2}\, b^{\varepsilon}.$$

Sous cette hypothèse, on démontre :

THEOREME 2.- *Avec l'hypothèse* R^*, *et en supposant*

$$1 \leq |a| \leq MN \quad \text{et} \quad M \leq N \leq M^{\frac{4}{3}-\delta_0} \quad (\delta_0 > 0) \quad \text{on a}$$

$$\forall A \ \forall \varepsilon > 0 \quad \sum_{\substack{q \leq N^{1-\varepsilon} \\ (q,a)=1}} \left| |\mathcal{A}_q| - \frac{|\mathcal{A}|}{\varphi(q)} \right| \ll_{A,\varepsilon} MN(\log MN)^{-A}.$$

Ainsi, en prenant $N = M^{\frac{4}{3}-\varepsilon}$, on voit que la suite $\mathcal{A}$, dont le cardinal et les termes sont de l'ordre de MN, a pour niveau de distribution $(MN)^{\frac{4}{7}-2\varepsilon}$.

Enfin le dernier théorème n'utilise pas la conjecture R^*, mais donne un résultat lorsque $\mathcal{N} = \mathcal{P}$ suite des nombres premiers.

THEOREME 3.- *Avec les notations précédentes, en prenant* $\mathcal{N} = \mathcal{P}$ *et en supposant*

$$1 \leq |a| \leq MN$$

et

$$M \leq N \leq M^{\frac{10}{9}-\delta_0} \quad (\delta_0 > 0)$$

on a

$$\forall A \ \forall \varepsilon > 0 \quad \sum_{\substack{q \leq N^{1-\varepsilon} \\ (q,a)=1}} \left| |\mathcal{A}_q| - \frac{|\mathcal{A}|}{\varphi(q)} \right| \ll_{A,\varepsilon} MN(\log MN)^{-A}.$$

De même pour $N = M^{\frac{10}{9}-\varepsilon}$, $\mathcal{A}$ a pour niveau de distribution $(MN)^{\frac{10}{19}-2\varepsilon}$.

On va donner quelques indications sur la démonstration de ces théorèmes ([2],[3]).

2. DEMONSTRATION.

Il faut d'abord remarquer que le théorème 1 se traite de la même façon que les deux autres. En appliquant un lemme combinatoire ([2] lemme 1) obtenu par itération de l'identité de Buchstab, on exprime $\pi(x,z\,;q,a)$ et $\pi(x,z)$ comme des formes bilinéaires. Puis en découpant chacune des sommes, on doit majorer

$$R(K,L,Q) = \sum_{\substack{Q<q\leq 2Q \\ (q,a)=1}} \sum_{\substack{K<k\leq 2K \\ (k,q)=1}} \left| \sum_{\substack{L<\ell\leq 2L \\ \ell k \equiv (\mathrm{mod}\, q)}} \alpha_\ell - \frac{1}{\varphi(q)} \sum_{\substack{L<\ell\leq 2L \\ (\ell,q)=1}} \alpha_\ell \right|$$

où $|\alpha_\ell| \leq 1$. (Pour le théorème 1, $\alpha_\ell = 1$ ou 0 suivant que tous les diviseurs premiers de ℓ sont supérieurs à un certain z_1 ou non. Pour les théorèmes 2 et 3, α_ℓ est la fonction caractéristique de $\mathcal{N}$).

Par l'inégalité de Cauchy-Schwarz, on obtient

$$R^2(K,L,Q) \le QK \sum_{\substack{Q<q\le 2Q\\(q,a)=1}} \sum_{\substack{K<k\le 2K\\(k,q)=1}} \Big| \sum_{\substack{L<\ell\le 2L\\ \ell k\equiv -a \,(\mathrm{mod}\, q)}} \alpha_\ell - \frac{1}{\varphi(q)} \sum_{\substack{L<\ell\le 2L\\(\ell,q)=1}} \alpha_\ell \Big|^2$$

$$= QK\,\{W(Q) - 2V(Q) + U(Q)\}$$

en développant le carré.

Chacun des termes $W(Q)$, $V(Q)$ et $U(Q)$ est évalué sous forme d'un terme principal et d'un terme d'erreur. $W(Q)$ est le plus délicat à traiter. Par définition

$$W(Q) = \sum_{\substack{Q<q\le 2Q\\(q,a)=1}} \sum_{\substack{K<k\le 2K\\(k,q)=1}} \sum_{\substack{L<\ell_1,\ell_2\le 2L\\ \ell_1 k\equiv \ell_2 k\equiv -a \,(\mathrm{mod}\, q)}} \alpha_{\ell_1}\alpha_{\ell_2}$$

$$= \sum_{\substack{Q<q\le 2Q\\(q,a)=1}} \sum_{\substack{L<\ell_1,\ell_2\le 2L\\ \ell_1\equiv \ell_2 \,(\mathrm{mod}\, q)\\ (\ell_1\ell_2,q)=1}} \alpha_{\ell_1}\alpha_{\ell_2} \sum_{\substack{K<k\le 2K\\ k\equiv -a\overline{\ell_1} \,(\mathrm{mod}\, q)}} 1 \,.$$

Mais

$$\sum_{\substack{K<k\le 2K\\ k\equiv -a\overline{\ell_1} \,(\mathrm{mod}\, q)}} 1 = \Big[\frac{2K + a\overline{\ell_1}}{q}\Big] - \Big[\frac{K + a\overline{\ell_1}}{q}\Big] = \frac{K}{q} - \Big\{\frac{2K + a\overline{\ell_1}}{q}\Big\} + \Big\{\frac{K + a\overline{\ell_1}}{q}\Big\} \,.$$

Le terme $\frac{K}{q}$ est la partie principale, les deux autres termes sont des termes d'erreur pour lesquels on ne peut se contenter de la majoration $O(1)$.

On développe donc les parties fractionnaires en série de Fourier. Après diverses transformations, on est ramené à majorer la forme bilinéaire

$$S = S(h,L) = \sum_{\substack{L<\ell_1,\ell_2\le 2L\\ (\ell_1,\ell_2)=1}} \alpha_{\ell_1}\,\alpha_{\ell_2}\, e\Big(ah\,\frac{\overline{\ell_1}}{\ell_2}\Big) \quad (h \in \mathbb{Z}^*)$$

pour laquelle une majoration triviale est $S \ll L^2$, et on remarque qu'il suffit de montrer :

$$S \ll L^{\gamma}\,\tau(h) \quad (\gamma < 2) \tag{2}$$

pour dépasser la valeur critique $\frac{1}{2}$ de l'exposant du niveau de distribution. Par l'inégalité de Cauchy Schwarz :

$$S \ll L^{1/2}\Big\{ \sum_{L<\ell_2,\ell_2'\le 2L} \Big| \sum_{\substack{L<\ell_1\le 2L\\ (\ell_1,\ell_2\ell_2')=1}} e\Big(a\,h\,\Big(\frac{\overline{\ell_1}}{\ell_2} - \frac{\overline{\ell_1}}{\ell_2'}\Big)\Big)\Big|\Big\}^{1/2} \,.$$

Pour simplifier l'exposé, on ne considère que la contribution S' des (ℓ_2,ℓ_2') avec $(\ell_2,\ell_2') = 1$,

$$S' = \sum_{\substack{L<\ell_2,\ell_2'\le 2L \\ (\ell_2,\ell_2')=1}} \Big| \sum_{\substack{L<\ell_1\le 2L \\ (\ell_1,\ell_2\ell_2')=1}} e\Big(ah\Big(\frac{\overline{\ell_1}}{\ell_2} - \frac{\overline{\ell_1}}{\ell_2'}\Big)\Big)\Big| = \sum_{\substack{L<\ell_2,\ell_2'\le 2L \\ (\ell_2,\ell_2')=1}} \Big| \sum_{\substack{L<\ell_1\le 2L \\ (\ell_1,\ell_2\ell_2')=1}} e\Big(ah(\ell_2'-\ell_2)\frac{\overline{\ell_1}}{\ell_2\ell_2'}\Big)\Big|$$

$$\ll L^{3+\varepsilon}\tau(h) \quad \text{(d'après le lemme).}$$

On obtient pour S une majoration pire que la majoration triviale.

Par contre avec l'hypothèse R^*, on a

$$S' \ll L^{\frac{5}{2}+\varepsilon}\tau(h)$$

et la relation (2) est vérifie avec $\gamma = \frac{7}{4} + \varepsilon$.

Dans le cas du théorème 3, on peut prendre

$$\alpha_{\ell_2} = \Lambda(\ell_2)$$

et appliquer l'identité de Vaughan à la somme

$$\sum_{\substack{L<\ell_2\le 2L \\ (\ell_2,\ell_1)=1}} \Lambda(\ell_2)\, e\Big(ah\,\frac{\overline{\ell_1}}{\ell_2}\Big).$$

Quant au théorème 1, on applique de nouveau le lemme combinatoire déjà mentionné, pour arriver à la majoration de

$$S_1 = \sum_{g>G} \sum_{L<\ell_1\le 2L} \Big| \sum_{\substack{L<\ell_2\le 2L \\ (\ell_2,\ell_1)=1 \\ \ell_2\equiv 0 (\mathrm{mod}\ g)}} \beta_{\ell_2}\, e\Big(ah\,\frac{\overline{\ell_1}}{\ell_2}\Big)\Big|$$

où $|\beta_{\ell_2}| \le 1$ et $G = L^{\delta}$ $(\delta > 0)$.

Par l'inégalité de Cauchy-Schwarz, on a

$$S_1 \ll L^{1/2}\Big\{ \sum_{\substack{L<\ell_2,\ell_2'\le 2L \\ \ell_2\equiv\ell_2'\equiv 0(\mathrm{mod}\ g)}} \Big| \sum_{\substack{L<\ell_1\le 2L \\ (\ell_1,\ell_2\ell_2')=1}} e\Big(ah\Big(\frac{\overline{\ell_1}}{\ell_2} - \frac{\overline{\ell_1}}{\ell_2'}\Big)\Big)\Big| \Big\}^{1/2}.$$

On se contente d'étudier la contribution des couples (ℓ_2,ℓ_2') avec $(\ell_2,\ell_2') = g$. Dans ce cas le dénominateur commun est $\ell_2\ell_2'\, g^{-1}$,

$$\sum_{\substack{L<\ell_1\le 2L\\(\ell_1,\ell_2\ell_2')=1}} e\left(ah\left(\frac{\overline{\ell_1}}{\ell_2}-\frac{\overline{\ell_1}}{\ell_2'}\right)\right)=\sum_{\substack{L<\ell_1\le 2L\\(\ell_1,\ell_2\ell_2')=1}} e\left(ah(\ell_2' g^{-1}-\ell_1' g^{-1})\frac{\overline{\ell_1}}{\ell_2\ell_2' g^{-1}}\right)$$

$$\ll (L^2 g^{-1})^{\frac{1}{2}+\varepsilon}(h,\ell_2\ell_2' g^{-1})^{\frac{1}{2}} \quad \text{par le lemme.}$$

On a donc la majoration (2) avec $\gamma = 2-\frac{\delta}{4}+\varepsilon$.

Le terme principal de $W(Q)-2V(Q)+U(Q)$ s'écrit

$$M\sum_{\substack{Q<q\le 2Q\\(q,a)=1}}\frac{1}{\varphi^2(q)}\sum_{\substack{\lambda(\mathrm{mod}\ q)\\(\lambda,q)=1}}\Big|\sum_{\substack{L<\ell\le 2L\\\ell\equiv\lambda(\mathrm{mod}\ q)}}\alpha_\ell-\frac{1}{\varphi(q)}\sum_{\substack{L<\ell\le 2L\\(\ell,q)=1}}\alpha_\ell\Big|^2$$

et se majore avec l'inégalité de grand crible, le théorème de Siegel-Walfisz ou la condition (iii), d'une façon analogue à la démonstration du théorème de Barban-Davenport-Halberstam.

REFERENCES

[1] E. BOMBIERI. On the large sieve, Mathematika 12 (1965), 201-225.

[2] E. FOUVRY et H. IWANIEC. On a theorem of Bombieri-Vinogradov's type. (à paraître).

[3] E. FOUVRY. (à paraître).

[4] C. HOOLEY. On the greatest prime factor of a cubic polynomial. J. Reine angew. Math. 303/304 (1978), 21-50.

[5] H.L. MONTGOMERY. Topics in Multiplicative Number Theory. Lectures Notes in Math. 227 (1971), Berlin and New-York.

[6] R.C. VAUGHAN. On the estimation of trigonometric sums over primes and related questions. Institut Mittag-Leffler Report N° 9 (1977).

[7] A.I. VINOGRADOV. The density hypothesis for Dirichlet L-series (Russe), Izv. Akad. Nauk SSSR, Ser. Mat. 29 (1965), 903-934 ; Corrigendum : ibid. 30 (1966), 719-720.

Etienne FOUVRY
U.E.R. de Mathématiques et d'Informatique
Université de Bordeaux I
351, Cours de la Libération

33405 TALENCE CEDEX

WEIGHTED SIEVES

G. GREAVES

1. INTRODUCTION.

In the sieve method we may study sets $\mathcal{A} = \mathcal{A}_X$ of integers $(X \to \infty)$ such that

$$\text{(A1)} \qquad \sum_{a \in \mathcal{A},\, a \equiv 0 \bmod d} 1 = \frac{X}{d}\rho(d) + E(X,d)$$

$$\text{(A2)} \qquad \sum_{w \leqslant p < z} \frac{\rho(p)\log p}{p-\rho(p)} - K \log \frac{z}{w} = O(1)$$

$$\text{(A3)} \qquad \sum_{d \leqslant D} \mu^2(d)\,|E(X,d)| = O\left(\frac{X}{\log^{K+1} x}\right);$$

cf. Halberstam & Richert [3], where many examples of such $\mathcal{A}$ are presented.

The important constant K is the dimension of the sieve, and I will discuss only the case $K = 1$.

Having decided this, further properties of ρ are unimportant, and I will gain brevity with no real loss of generality by fixing $\rho(p) = 1$. This is not sufficient for many important applications, but it does provide a sufficient framework in which to study the one-dimensional sieve method.

The condition (A3) estimates the error terms $E(X,d)$ "trivially" i.e. via their absolute values. Especially since the publication of [3], much work has been done on "non trivial" estimations of the error terms in the sieve : see eg [4]. In the sieve with weights, we will see that there is much work to be done on the main term : accordingly I am happy not to worry too much as yet about the error terms.

For informal discussion, we may abbreviate the conditions (A1)-(A3) to

$$\sum_{\substack{a\in\mathcal{A}\\ a\equiv 0 \bmod d}} 1 \sim \frac{X}{d} \quad \text{when} \quad d \leqslant D = D_X .$$

In this situation we may take any $\lambda(d)$ and form

$$m(a) = \sum_{d\leqslant D} \lambda(d).$$

Then

$$\sum_{a\in\mathcal{A}} m(a) \sim X \sum_{d\leqslant D} \frac{\lambda(d)}{d} .$$

Thus if

$$\sum_{d\leqslant D} \frac{\lambda(d)}{d} > 0 ,$$

with sufficient uniformity in X to cover our neglect of E-terms, then some a in $\mathcal{A}$ has $m(a) > 0$. We should construct $\lambda(d)$ so that this property $m(a) > 0$ is "interesting".

In the unweighted sieve, "interesting" means that a has no prime factors $< z$ (to be chosen) and the main term is completely known in the 1-dimensional case. That is to say there is the theorem that subject to (A1)-(A3)

$$\sum_{\substack{a\in\mathcal{A}\\ p\mid a \Rightarrow p > D^{1/s}=z}} 1 \geqslant X \prod_{p<z} \left(1-\frac{\varrho(p)}{p}\right) \{f(s)+O\left(\frac{se^{-s}}{\log^{1/5} z}\right)\} + O\left(\frac{X}{\log^2 X}\right), \qquad (1)$$

and a similar upper bound with f replaced by F. The function $f(s)$ satisfies a certain integral equation, and has the property

$$f(s) > 0 \iff s > 2.$$

An example due to Selberg shows that this number 2, and indeed the functions F, f, are best possible.

2. WEIGHTED SIEVES : SUMMARY OF RESULTS.

We now impose the extra condition

(A4) $$a \in \mathcal{A} \Rightarrow a < D^g.$$

The number g is the degree of the weighted sieve problem. Trivially, $g \geqslant 1$ always.

The notation P_R will denote a number having at most R prime factors, where for present purposes we agree to count each repeated prime factor once only.

The unweighted sieve shows that if $g < R/2$ then some a is a P_R, if X is large enough. In view of the failure of this method in the most interesting case $R = 1$, we alter our requirements and ask that for specified R some a should be a P_R without demanding that it should be free of small prime factors.

The available results in this subject are that if

$$g < R - \delta_R = \Lambda_R$$

then some a is a P_R. The standard conjecture is that these results are true if $\Lambda_R = R$, and an example of Selberg shows that this would be best possible. However the available theorems only lead to results as summarised in this table :

	δ_R (all R)	δ_2
Richert [6]	0,262...	0,167...
(by Richert's method)	0,178...	0,136...
Laborde [5]	0,144...	0,108...
Greaves [1]	0,124...	0,0636...

3. WEIGHTED SIEVES : OUTLINE OF METHODS.

We sketch the weighting device of Richert, which also plays a rôle in all subsequent work. Consider

$$m(a) = W(1) - \sum_{\substack{p \mid a \\ p<D}} \{W(1) - W(\tfrac{\log p}{\log D})\} .$$

The simplest example is $W(x) = x$. Then (where we denote the number of prime factors of a by $v(a)$)

$$m(a) \leqslant 1 - \sum_{p \mid a} (1 - \frac{\log P}{\log D}) \leqslant 1 - v(a) + g.$$

So $m(a) > 0 \Longrightarrow v(a) < g+1$. In particular when $g = R$ we have

$$m(a) > 0 \Longrightarrow v(a) \leqslant R.$$

Thus this function W is appropriate if we were hoping to prove $\Lambda_R = R$ in (2).

If however we proceed as in § 1 we obtain

$$\sum_a m(a) \sim X \{1 - \sum_{p<D} \frac{1-\log P/\log D}{P}\} \sim - X \log\log D,$$

so that the method fails in a divergent way because of the factor $\log\log D$. This factor arises from the small primes P ($< D^s$, say) so in Richert's paper this device is applied to those a from $\mathcal{A}$, forming a set $\mathcal{A}^*$ say, that have no prime factor smaller than a suitably chosen $z = D^s$. The unweighted sieve is used to perform the estimation.

This (and similar) methods suffer from the important defect that they reject a certain proportion of those P_R that we seek, namely those having a small prime factor $p < z$. It is not surprising that we do not obtain $\Lambda_R = R$ by this approach, and that we have to use a function $W(x)$ differing from x. Richert takes

$$W(1) = U - V$$
$$W(x) \leqslant \begin{cases} x - V & (0 < x\ ;\ V < x < U) \\ W(1) & (U < x < 1 \end{cases} \Bigg\} \begin{pmatrix} V < U < 1,\ \frac{1}{2} < U, \\ V + RU \leqslant g \end{pmatrix} ,$$

using a combinatorial argument of the type described above, and thus shows that we may take $\Lambda_R = RU + V$ with $U < 1$ and $V\ (< 0)$ suitably specified.

I cannot say much here about the proof of the unweighted sieve theorem (1) save that it is based upon the ideas of Viggo Brun. Brun modified Legendre's identity (where we imply $z > p_1 > p_2 \ldots$)

$$\sum_{p \mid a \Rightarrow p \geqslant z} 1 = \sum_{a} 1 - \sum_{p_1 \mid a} 1 + \sum_{p_1 p_2 \mid a} 1 - \sum_{p_1 p_2 p_3 \mid a} 1 + \sum_{p_1 p_2 p_3 p_4 \mid a} 1 - \ldots$$
$$= \sum_{d \mid a} \mu(d)$$

to

$$\sum_{p \mid a \Rightarrow p \geqslant z} 1 > \sum_{a} 1 - \sum_{p_1 \mid a} 1 + \sum_{\substack{p_1 B \mid a \\ p_2 < B_2}} 1 - \sum_{\substack{p_1 p_2 p_3 \mid a \\ p_2 < B_2}} 1 + \sum_{\substack{p_1 p_2 p_3 p_4 \\ p_2 < B_2 \\ p_4 < B_4}} 1 - \ldots$$
$$= \sum_{d \mid a} \mu_B(d), \quad \text{say.}$$

My approach to this problem incorporates the weight function at the outset, and begins with an expression

$$\lambda(d) = \mu_B(d) \{W(1) - \sum_{p \mid d} W(\frac{\log P}{\log D})\} \qquad (3)$$

We shall see that this represents an only partially successful attempt to avoid the defect noted above resulting from the earlier methods reliance on the unweighted sieve. I had to work with a function

$$W(1) = U - V$$
$$W(p) = \begin{cases} x - V & (\frac{1}{4} < x < U) \\ x - (1-U)/3 & (T < x < \frac{1}{4}) \\ 0 & (0 < x < T) \end{cases}$$

where $V < U < 1$, $\frac{1}{2} < U$, $V + RU \leqslant g$ (again, and for the same reasons) and also $3V + U \leqslant 1$. This is because once again a positive estimate did not result when $W(x) = x$.

One can prove that with this W and $\lambda(d)$ as in (3) that $m(a) = \sum_{d|a} \lambda(d)$ is positive only if a is a P_R. The main term gives (Q_1 being the least prime factor of a)

$$\sum_{\substack{a \in \mathcal{A} \\ a = P_R}} m(Q_1) \geqslant \frac{2X}{\log D} \mathfrak{m}(W),$$

where

$$\mathfrak{m}(W) = -\int_{\frac{1}{2}}^{1} \frac{W(1)-W(x)}{1-x} \frac{dx}{x} + \int_0^{\frac{1}{2}} \frac{W(x)}{1-x} \frac{dx}{x} - \int_0^{\frac{1}{4}} \frac{W(x)}{x} h(x,1)\, dx.$$

Here, a function $h(x,s)$ satisfies a certain integral equation. When $W(x) = x$, this reduces to the (negative) quantity

$$-\int_0^{\frac{1}{4}} h(x,1)\, dx.$$

One can prove $h(x,1) \sim \log(x^{-1})$ as $x \to 0$, and this integral is convergent. Thus, if applied when $W(x) = x$, the method does not fail in the divergent manner of earlier methods. On the other hand $h(x,1) > 1/(1-x)$ for smaller x, so it is better to take $W(x) = 0$ for these x. The method then shares the undesirable property, of refusing to count some of the P_R that we seek.

The fact that $h(x,1) \to \infty$ as $x \to 0$ can be appreciated by considering the coefficient of say $W(\log 2/\log D)$ in the expression for $\sum \lambda(d)/d$ arising from (3). This may be related to the fact that $f(s)$ in the unweighted sieve theorem (1) is already zero for s as large as 2. One may therefore speculate that the failure of our method to establish the conjecture $\Lambda_R = R$ stems from the fact that it still rests too heavily on the notions of the established sieve method, and that some completely new approach may be required.

REFERENCES

[1] G. GREAVES. A weighted sieve of Brun's type.
To appear in Acta Arith.

[2] G. GREAVES. Rosser's sieve with weights.
To appear in the Proceedings of the Symposium in Analytic Number Theory held in Durham in 1979.

[3] H. HALBERSTAM & H.E. RICHERT. Sieve methods.
London, 1974.

[4] H. IWANIEC. A new form on the error term in the linear sieve.
To appear in Acta Arith.

[5] M. LABORDE. Buchstab's sifting weights.
To appear in Mathematika.

[6] H.E. RICHERT. Selberg's sieve with weights.
Mathematika 16 (1969), 1-22.

G. GREAVES
Department of Pure Mathematics
Univ. Coll.

CARDIFF CF1 1XL Wales U.K.

SUITES DE RUDIN-SHAPIRO ET PAPIERS PLIES

M. MENDÈS-FRANCE

L'essentiel de mon exposé est tiré de deux articles à paraître. Le premier "Principe de la symétrie perturbée" doit être publié dans le Séminaire de Théorie des Nombres (Delange, Pisot, Poitou), 1979-1980. Le second doit paraître au Bulletin de la Société Mathématique de France (en commun avec G. Tenenbaum : Dimension des courbes planes, papiers pliés et suites de Rudin-Shapiro).

Itérer une infinité de fois l'opération de plier une feuille de papier sur elle-même engendre, par dépliage une suite infinie à deux éléments "plis rentrant", "plis sortant". Codées de façon convenable, ces suites donnent lieu à des courbes polygonales infinies dont on peut calculer la "dimension". Elles ont un comportement à la Peano, ce qui se traduit par le fait qu'elles ont pour dimension 2. Ce calcul est en rapport étroit avec les suites de Rudin-Shapiro.

ENSEMBLES D'UNICITE POUR LES FONCTIONS ADDITIVES. ETUDE ANALOGUE DANS LE CAS DES FONCTIONS MULTIPLICATIVES.

JACQUES MEYER

NOTATIONS.

$\mathcal{P}$ désigne l'ensemble des nombres premiers et $\mathcal{P}'$ l'ensemble des puissances de nombres premiers :

$$\mathcal{P}' = \{p^r \; ; \; p \in \mathcal{P}, \; r \in \mathbb{N}^*\} \; .$$

Soit n un entier $\geqslant 1$ et p un élément de $\mathcal{P}$. On désigne par $\nu_p(n)$ l'exposant de p dans la décomposition de n en facteurs premiers.

Soit p^r un élément de $\mathcal{P}'$. On dit que p^r divise exactement un entier $n \geqslant 1$ (et l'on note $p^r \| n$) si et seulement si $r = \nu_p(n)$.

1. INTRODUCTION.

1.1. La notion d'ensemble d'unicité pour les fonctions complètement additives a été introduite par Katai [1] : Une fonction arithmétique complètement additive est déterminée par sa restriction à l'ensemble $\mathcal{P}$ des nombres premiers. D'autres parties de $\mathbb{N}^*$ vérifient cette propriété, et Katai les nomme "ensembles d'unicité".

Autrement dit une partie A de $\mathbb{N}^*$ est un ensemble d'unicité (pour les fonctions complètement additives) si la seule fonction complètement additive qui soit nulle sur A est la fonction identiquement nulle. Cette définition se généralise aux fonctions additives : une partie A de $\mathbb{N}^*$ est un ensemble d'unicité (pour les fonctions additives) si la seule fonction additive qui soit nulle sur A est la fonction identiquement nulle. Les premiers travaux sur les ensembles d'unicité ont consisté à démontrer qu'un ensemble donné était ensemble d'unicité [1,2,3]. Par une approche différente, F. Dress et B. Wolkmann [4] et, indépendamment, D. Wolke [5] ont établi une condition nécessaire et suffisante pour qu'une partie de $\mathbb{N}^*$ soit ensemble d'unicité (pour les fonctions complètement additives).

Utilisant la même approche, on établit ici des conditions nécessaires et suffisantes pour qu'une partie de $\mathbb{N}^*$ soit ensemble d'unicité pour les fonctions additives. De plus on résoud le problème analogue pour les fonctions multiplicatives.

1.2. Rappelons le résultat de Dress-Wolkmann-Wolke.

PROPOSITION 1.- *Une partie* $A = \{a_i\}_{i\in I}$ *de* $\mathbb{N}^*$ *est un ensemble d'unicité pour les fonctions complètement additives si et seulement si tout entier naturel* $n \geqslant 1$ *peut se mettre sous la forme*

$$n = a_{i_1}^{\alpha_{i_1}} a_{i_2}^{\alpha_{i_2}} \dots a_{i_k}^{\alpha_{i_k}},$$

où les a_{ij} $(1 \leqslant j \leqslant k)$ *sont des éléments de* A, *les* α_{ij} $(1 \leqslant j \leqslant k)$ *sont*

des nombres rationnels et k *un entier dépendant de* n.

Cette proposition peut également s'énoncer ainsi :

Une partie $A = \{a_i\}_{i\in I}$ *est un ensemble d'unicité si et seulement si, pour tout entier naturel* $n \geqslant 1$, *il existe une suite* $(\alpha_i(n))_{i\in I}$ *d'éléments de* $\mathbb{Q}$, *presque tous nuls, telle que :*

$$\forall\ p\in\mathcal{P} \qquad \nu_p(n) = \sum_{\substack{i\in I \\ p\mid a_i}} \alpha_i(n)\ \nu_p(a_i).$$

La démonstration de cette proposition repose sur le fait suivant : A est ensemble d'unicité si et seulement si la famille $\{\mathrm{Log}\ a\}_{a\in A}$ est génératrice du $\mathbb{Q}$-espace vectoriel engendré par $\{\mathrm{Log}\ p\}_{p\in\mathcal{P}}$.

1.3. A ce sujet une remarque.

Dans l'article déjà cité [1], Katai remarque que si l'on se donne un sous-ensemble $\mathcal{P}_1$ de $\mathcal{P}$ et une suite quelconque de nombres complexes $\{x_p\}_{p\in\mathcal{P}_1}$, il existe (au moins) une fonction complètement additive f telle que

$$\forall\ p\in\mathcal{P}_1 \qquad f(p) = x_p\ .$$

Et il ajoute : "It is easy to prove that a set of natural numbers $A = \{a_1, a_2, \ldots\}$ has the last property if and only if a_i, a_j are relatively prime for all $i \neq j$. Thus the structural survey of these sets is not difficult".

Cette affirmation est cependant inexacte, comme le montre l'exemple suivant :

Prenons $A = \{2,6\}$. Deux nombres complexes quelconques x_2 et x_6 étant donnés, il existe une infinité de fonctions complètement additives telles que $f(2) = x_2$ et $f(6) = x_6$: ce sont les fonctions complètement additives vérifiant

$$f(2) = x_2,\ f(3) = x_6 - x_2,\ f(p) \text{ quelconque pour } p \geqslant 5.$$

Appelons "ensemble compatible"† toute partie $A = \{a_i\}_{i\in I}$ de $\mathbb{N}^*$ telle que,

---

† pour les fonctions complètement additives.

pour toute suite quelconque de nombres complexes $(x_i)_{i\in I}$, il existe (au moins) une fonction complètement additive vérifiant

$$\forall\ i\in I \qquad f(a_i) = x_i\ .$$

Il ressort de la démonstration de la proposition 1 [ainsi qu'on l'expliquera plus clairement dans la démonstration analogue dans le cas des fonctions additives] que l'on a le résultat suivant :

A est un ensemble compatible si et seulement si $\{\mathrm{Log}\ a\}_{a\in A}$ *est une partie du* $\mathbb{Q}$*-espace vectoriel engendré par* $\{\mathrm{Log}\ p\}_{p\in\mathcal{P}}$.

2. LE CAS DES FONCTIONS ADDITIVES (à valeurs dans $\mathbb{R}$).

2.1. Nous allons démontrer la proposition suivante :

PROPOSITION 2.- *Soit* $A = \{a_i\}_{i\in I}$ *une partie de* $\mathbb{N}^*$. *Il est équivalent de dire :*

i) A *est un ensemble d'unicité (pour les fonctions additives).*

ii) Pour tout entier naturel $n \geqslant 1$, *il existe une suite* $(\alpha_i(n))_{i\in I}$ *d'éléments de* $\mathbb{Q}$, *presque tous nuls, telle que*

$$\forall\ p\in\mathcal{P},\ \forall\ r\in\mathbb{N}^* \qquad \sum_{\substack{i\in I\\ p^r\| a_i}} \alpha_i(n) = \begin{cases} 1 & \text{si } p^r\| n \\ 0 & \text{si } p^r\nmid n \end{cases}.$$

iii) Toute fonction additive, dont la restriction sur A *est à valeurs dans* $\mathbb{Q}$, *est à valeurs dans* $\mathbb{Q}$.

2.2. Démonstration de ii) $\Rightarrow$ iii).

Soit f une fonction additive. Pour tout entier $n \geqslant 1$, on a les égalités :

$$f(n) = \sum_{p^r \| n} f(p^r)$$

$$= \sum_{p \in \mathcal{P}} \sum_{r \geqslant 1} \Big(\sum_{\substack{i \in I \\ p^r \| a_i}} \alpha_i(n) \Big) f(p^r)$$

$$= \sum_{i \in I} \alpha_i(n) \sum_{p \in \mathcal{P}} \sum_{\substack{r \geqslant 1 \\ p^r \| a_i}} f(p^r)$$

$$f(n) = \sum_{i \in I} \alpha_i(n) \, f(a_i).$$

De cette dernière égalité, il ressort clairement que si $f(A) \subset \mathbb{Q}$, alors $f(n) \in \mathbb{Q}$ pour tout entier $n \geqslant 1$.

2.3. Démonstration de iii) $\Rightarrow$ i).

Soit f une fonction additive telle que $f(A) = \{0\}$. Ceci implique, d'après iii) que $f(n) \in \mathbb{Q}$ pour tout entier $n \geqslant 1$. Considérons la fonction additive $g = \frac{f}{\sqrt{2}}$; g est nulle sur A et, par conséquent, $g(n) \in \mathbb{Q}$ pour tout entier $n \geqslant 1$.

Pour que $g(n)$ et $f(n)$ appartiennent simultanément à $\mathbb{Q}$, il faut que

$$f(n) = g(n) = 0.$$

On a montré ainsi que f est identiquement nulle.

2.4. Démonstration de i) $\Rightarrow$ ii).

Soit $(\xi_k)_{k \geqslant 1}$ une suite de nombres réels $\mathbb{Q}$-linéairement indépendants et $\mathcal{P}' = \{p'_1, p'_2, \ldots, p'_h, \ldots\}$ l'ensemble des puissances de nombres premiers rangés dans l'ordre naturel :

$$\mathcal{P}' = \{2, 3, 2^2, 5, 7, \ldots\} .$$

On définit une fonction additive L par

$$L(p'_k) = \xi_k \qquad \forall\, k \geqslant 1,$$

et on appelle V_L le $\mathbb{Q}$-espace vectoriel engendré par $\{L(p'_k)\}_{k \geqslant 1}$.

Cet espace vectoriel présente les propriétés suivantes.

a. $\{L(p'_k)\}_{k\geqslant 1}$ est une base de V_L .

b. Pour toute application linéaire ϕ de V_L dans $\mathbb{R}$, la fonction arithmétique $g_\phi = \phi \circ L$ est additive.

Pour démontrer la propriété b, il suffit de voir que, pour tous les nombres entiers m et $n \geqslant 1$ tels que $(m,n) = 1$, on a :

$$g_\phi(mn) = \phi \circ L(mn) = \phi(L(m) + L(n)) = \phi \circ L(m) + \phi \circ L(n)$$
$$= g_\phi(m) + g_\phi(n).$$

c. Pour toute fonction additive g, il existe une application linéaire ϕ_g de V_L dans $\mathbb{R}$ telle que :

$$g = \phi_g \circ L.$$

Pour démontrer la propriété c, il suffit de voir que l'application linéaire ϕ, définie par ses valeurs sur la base $\{L(p'_k)\}_{k\geqslant 1}$ par $\phi(L(p'_k)) = g(p'_k)$ $\forall\, k \geqslant 1$, vérifie

$$\forall\, n \geqslant 1 \qquad \phi(L(n)) = \sum_{p^r \| n} \phi(L(p^r)) = \sum_{p^r \| n} g(p^r) = g(n).$$

Considérons maintenant U_L le $\mathbb{Q}$-sous-espace vectoriel de V_L engendré par $\{L(a_i)\}_{i\in I}$ et montrons que i) implique

$$U_L = V_L.$$

Pour cela supposons que $U_L \subsetneq V_L$. Il existe alors un élément p'_0 de $\mathcal{P}'$ tel que $L(p'_0) \notin U_L$. Soit B_0 une base de U_L, $B_0 \cup \{L(p'_0)\}$ peut être complété en une base B de V_L.

Soit g_ϕ la fonction additive associée à l'application linéaire ϕ de V_L dans $\mathbb{R}$ définie par :

$$\begin{cases} \phi(b) = 0 & \forall\ b \in B - \{L(p'_0)\} \\ \phi(L(p'_0)) = 1. \end{cases}$$

Pour tout entier $n \geqslant 1$, il existe des coefficients rationnels $(\beta_b(n))_{b\in B}$

presque tous nuls tels que

$$L(n) = \sum_{b\in B} \beta_n(n)b,$$

de telle sorte que

$$g_\phi(n) = \phi\Big(\sum_{b\in B} \beta_b(n)b\Big) = \sum_{b\in B} \beta_b(n)\phi(b).$$

Ainsi on a construit une fonction additive nulle sur A [car si $a\in A$, $L(a)\in U_L$ et $g_\phi(a) = 0$] sans être identiquement nulle [car $g_\phi(p'_0) = 1$] . Donc A ne peut être ensemble d'unicité.

On a donc montré que i) $\Rightarrow$ $U_L = V_L$.

D'après cette dernière égalité, il existe, pour tout entier $n \geqslant 1$, des coefficients rationnels $(\alpha_i(n))_{i\in I}$ presque tous nuls tels que :

$$L(n) = \sum_{i\in I} \alpha_i(n)\, L(a_i).$$

D'après la propriété c, la fonction additive δ_{p^r} (où p^r est un élément quelconque de $\mathfrak{P}'$) définie par

$$\delta_{p^r}(n) = \begin{cases} 1 & \text{si } p^r \| n \\ 0 & \text{si } p^r \nmid n, \end{cases}$$

vérifie $$\delta_{p^r}(n) = \sum_{i\in I} \alpha_i(n)\, \delta_{p^r}(a_i).$$

Ceci prouve l'affirmation ii) et achève la démonstration de la proposition 2.

2.5. Appelons "ensemble compatible" (pour les fonctions additives) toute partie $A = \{a_i\}_{i\in I}$ de $\mathbf{N}^*$ telle que, pour toute suite quelconque de nombres réels $(x_i)_{i\in I}$, il existe (au moins) une fonction additive vérifiant

$$\forall\, i\in I \qquad f(a_i) = x_i.$$

Les propriétés b et c du paragraphe précédent montrent que la donnée d'une fonction additive (à valeurs dans $\mathbf{R}$) est équivalente à la donnée d'une application linéaire de V_L dans $\mathbf{R}$, autrement dit est équivalente à la donnée de la valeur de cette application linéaire sur une base de V_L. Ainsi nous avons la proposition

PROPOSITION 3.- *Une partie* $A = \{a_i\}_{i\in I}$ *de* $\mathbb{N}^*$ *est un ensemble compatible si et seulement si* $\{L(a_i)\}_{i\in I}$ *est une partie libre de* V_L .

Remarque. Pour une partie A donnée de $\mathbb{N}^*$, le fait que $\{L(a_i)\}_{i\in I}$ soit une famille libre ou liée est indépendant de la fonction L choisie. En effet, soit $A = \{a_i\}_{i\in I}$ une partie de $\mathbb{N}^*$. Il est aisé de démontrer que A est une famille liée si et seulement si il existe un indice $i_0 \in I$ et des coefficients rationnels $(\alpha_i)_{i\in I-\{i_0\}}$ presque tous nuls tels que :

$$\forall\, p\in\mathcal{P},\ \forall\, r\in\mathbb{N}^* \qquad \sum_{\substack{i\in I-\{i_0\}\\ p^r \| a_i}} \alpha_i = \begin{cases} 1 & \text{si } p^r \| a_{i_0} \\ 0 & \text{si } p^r \nmid a_{i_0} \end{cases} .$$

3. LE CAS DES FONCTIONS MULTIPLICATIVES (à valeurs dans $\mathbb{C}$).

3.1. L'analogue, pour les fonctions multiplicatives, de la notion d'ensemble d'unicité (pour les fonctions additives) est la notion d'ensemble unitaire.

Nous dirons qu'une partie A de $\mathbb{N}^*$ est un ensemble unitaire (pour les fonctions multiplicatives) si la seule fonction multiplicative qui prenne la valeur 1 en tout point de A est la fonction identiquement égale à 1.

PROPOSITION 4.- *Soit* $A = \{a_i\}_{i\in I}$ *une partie de* $\mathbb{N}^*$. *Il est équivalent de dire :*

i) A *est un ensemble unitaire (pour les fonctions multiplicatives).*

ii) Toute fonction additive, dont la restriction à A *est à valeurs dans* $\mathbb{Z}$ *, est à valeurs dans* $\mathbb{Z}$.

iii) Pour tout entier naturel $n \geqslant 1$, *il existe une suite* $(\alpha_i(n))_{i\in I}$ *d'éléments de* $\mathbb{Z}$ *, presque tous nuls, telle que :*

$$\forall\, p\in\mathcal{P},\ \forall\, r\in\mathbb{N}^* \qquad \sum_{\substack{i\in I\\ p^r \| a_i}} \alpha_i(n) = \begin{cases} 1 & \text{si } p^r \| n \\ 0 & \text{si } p^r \nmid n \end{cases} .$$

3.2. Démonstration de i) ⇒ ii).

Soit f une fonction additive telle que

$\forall\, a \in A, \qquad f(a) \in \mathbb{Z}$.

La fonction multiplicative $g = e^{2i\pi f}$ vérifie

$\forall\, a \in A, \qquad g(a) = 1$;

et comme A est un ensemble unitaire,

$\forall\, n \in \mathbb{N}^*, \qquad g(n) = 1$.

On en déduit :

$\forall\, n \in \mathbb{N}^*, \qquad f(n) \in \mathbb{Z}$.

3.3. Démonstration de ii) ⇒ iii).

Remarquons tout d'abord que la condition ii) implique que A est un ensemble d'unicité pour les fonctions additives. En effet, soit f une fonction additive telle que $f(A) = \{0\}$. Ceci implique, d'après ii) que $f(n) \in \mathbb{Z}$ pour tout entier $n \geqslant 1$. Considérons la fonction additive $g = \frac{f}{\sqrt{2}}$; g est nulle sur A et, par conséquent, $g(n) \in \mathbb{Z}$ pour tout entier $n \geqslant 1$.

Pour que $f(n)$ et $g(n)$ appartiennent simultanément à $\mathbb{Z}$, il faut que $f(n) = g(n) = 0$.

On a ainsi montré que f est identiquement nulle.

Désignons par M_L le $\mathbb{Z}$-module engendré par $\{L(p'_k)\}_{k\geqslant 1}$.

Ce module présente les propriétés suivantes :

a - $\{L(p'_k)\}_{k\geqslant 1}$ est une base de M_L, car, rappelons-le, cette famille est par définition $\mathbb{Q}$-libre.

b - Pour toute application linéaire ϕ de M_L dans $\mathbb{R}$, la fonction arithmétique $g_\phi = \phi \circ L$ est additive.

La démonstration de cette propriété est identique à celle de la propriété b du paragraphe 2.4.

c - Pour toute fonction additive g, il existe une application linéaire ϕ_g

de M_L dans $\mathbb{R}$ telle que

$$g = \phi \circ L.$$

La démonstration de cette propriété est identique à celle de la propriété c du paragraphe 2.4.

Considérons maintenant N_L le sous-module de M_L engendré par $\{L(a_i)\}_{i\in I}$ et montrons que ii) implique

$$N_L = M_L.$$

Pour cela supposons que $N_L \subsetneq M_L$. Il existe un élément p'_0 de $\mathcal{P}'$ tel que $L(p'_0) \notin N_L$.

Soit $\{u_k\}_{k\in\mathbb{N}}$ une base de N_L (qui est libre comme sous-module d'un module libre sur un anneau principal) $\{u_k\}_{k\in\mathbb{N}}$ est aussi une base du $\mathbb{Q}$-sous-espace vectoriel U_L (engendré,rappelons-le, par $\{L(a_i)\}_{i\in I}$) qui est identique au $\mathbb{Q}$-espace V_L (engendré par $\{L(p'_k)\}_{k\geq 1}$) car, d'après la remarque faite au début du paragraphe, A est un ensemble d'unicité. Par suite, il existe des coefficients rationnels $(\alpha_k(p'_0))_{k\in\mathbb{N}}$ presque tous nuls tels que $L(p'_0) = \sum_{k\in\mathbb{N}} \alpha_k(p'_0)u_k$, et il en existe au moins un, appelons-le α_{k_0} , qui n'appartient pas à $\mathbb{Z}$.

Soit g_ϕ la fonction additive associée à l'application linéaire ϕ de V_L dans $\mathbb{R}$ vérifiant

$$\begin{cases} \phi(u_{k_0}) = 1 \\ \phi(u_k) = 0 \quad \forall\, k\in\mathbb{N}-\{k_0\} . \end{cases}$$

Pour tout élément a de A, il existe une suite $(\alpha_k(a))_{k\in\mathbb{N}}$ d'éléments de $\mathbb{Z}$, presque tous nuls, telle que

$$L(a) = \sum_{k\in\mathbb{N}} \alpha_k(a)u_k .$$

Ainsi : $$g_\phi(a) = \alpha_{k_0}(a) \in \mathbb{Z} .$$

On a donc construit une fonction additive g_ϕ dont la restriction à A est à valeurs dans $\mathbb{Z}$ sans être toujours à valeurs dans $\mathbb{Z}$ (car $g_\phi(p'_0) = \alpha_{k_0} \notin \mathbb{Z}$).

Par conséquent on a montré que ii) $\Rightarrow$ $N_L = M_L$.

D'après cette dernière égalité, il existe, pour tout entier $n \geqslant 1$, des coefficients entiers relatifs $(\alpha_i(n))_{i\in I}$, presque tous nuls, tel que

$$L(n) = \sum_{i\in I} \alpha_i(n) L(a_i).$$

Il suffit maintenant de remarquer que la fonction additive δ_{p^r} (où p^r est un élément quelconque de $\mathcal{P}'$) vérifie

$$\delta_{p^r}(n) = \sum_{i\in I} \alpha_i(n)\ \delta_{p^r}(a_i)$$

pour prouver la condition iii).

3.4. Démonstration de iii) $\Rightarrow$ i).

Elle commence par un lemme.

LEMME.- *Soit* $A \subset \mathbb{N}^*$ *un ensemble d'unicité. Toute fonction multiplicative vérifiant* $f_{|A} = 1$ *est de module égal à* 1.

Il convient de commencer la démonstration du lemme par la remarque suivante :

Soit p^r un élément quelconque de $\mathcal{P}'$; il existe alors (au moins) un élément a de A tel que

$$p^r \| a.$$

En effet, la condition ii) de la proposition 2 implique que

$$\sum_{\substack{i\in I \\ p^r \| a_i}} \alpha_i(p^r) = 1,$$

ce qui prouve qu'il existe (au moins) un élément de A divisible exactement par p^r

Soit maintenant une fonction multiplicative f dont la restriction à A, $f_{|A}$, vaut 1. Ceci implique, d'après la remarque précédente, que $f(n) \neq 0$ $\forall\, n \geqslant 1$.

La fonction additive $\mathrm{Log}|f|$ est alors partout définie et sa restriction à A est nulle. D'après l'hypothèse (A ensemble d'unicité) elle est identiquement nulle et, par conséquent,

$$|f(n)| = 1 \quad \forall\, n \in \mathbb{N}^*.$$

Une dernière remarque avant de démontrer que iii) $\Rightarrow$ i) : la condition iii) entraîne trivialement la condition ii) de la proposition 2. Ainsi la condition iii) implique que A est un ensemble d'unicité.

Soit maintenant une fonction multiplicative f dont la restriction à A est égale à 1. D'après la remarque précédente, on peut appliquer le lemme et dire que f est de module égal à 1.

Définissons une fonction additive g par :

$$\forall\, p^r \in \mathcal{P}', \quad f(p^r) = e^{2\pi i g(p^r)}, \quad 0 \leqslant g(p^r) < 1.$$

Alors, $\forall\ n \geqslant 1, \quad f(n) = e^{2i\pi g(n)}$.

On a les égalités suivantes :

$$\forall\, n \geqslant 1 \qquad f(n) = \prod_{p^r \| n} e^{2i\pi g(p^r)} = e^{2i\pi \sum_{p^r \| n} g(p^r)}$$

$$= e^{2i\pi \sum_{p\in\mathcal{P}} \sum_{r\geqslant 1} \left(\sum_{\substack{i\in I \\ p^r \| a_i}} \alpha_i(n) \right) g(p^r)}$$

$$= e^{2i\pi \sum_{i\in I} \alpha_i(n) \sum_{p\in\mathcal{P}} \sum_{\substack{r>1 \\ p^r \| a_i}} g(p^r)}$$

$$= e^{2i\pi \sum_{i\in I} \alpha_i(n)\, g(a_i)}$$

$$= \prod_{i\in I} \left[e^{2i\pi g(a_i)} \right]^{\alpha_i(n)}$$

$$= \prod_{i\in I} f(a_i)^{\alpha_i(n)}$$

$$= 1.$$

Ce qui prouve que A est un ensemble unitaire et achève la démonstration de la proposition 4.

3.5. On aurait pu restreindre l'étude au cas des fonctions complètement multiplicatives et obtenir la proposition :

PROPOSITION 5.- *Une partie* $A = \{a_i\}_{i\in I}$ *de* $\mathbb{N}^*$ *est un ensemble unitaire (pour les fonctions complètement multiplicatives) si et seulement si tout entier* $n \geq 1$ *peut se mettre sous la forme*

$$n = a_{i_1}^{\alpha_{i_1}} a_{i_2}^{\alpha_{i_2}} \dots a_{i_k}^{\alpha_{i_k}},$$

où les a_{ij} $(1 \leq j \leq k)$ *sont des éléments de* A, *les* α_{ij} $(1 \leq j \leq k)$ *sont des éléments de* $\mathbb{Z}$ *et* k *un entier dépendant de* n.

La démonstration de la proposition repose sur le fait suivant : A est un ensemble unitaire (pour les fonctions complètement multiplicatives) si et seulement si le $\mathbb{Z}$-module engendré par $\{\text{Log } a\}_{a\in A}$ est égal au $\mathbb{Z}$-module engendré par $\{\text{Log } p\}_{p\in\mathcal{P}}$.

4. REMARQUES.

4.1. Comme on l'a vu tout ensemble unitaire est un ensemble d'unicité. La réciproque est, bien entendu, fausse. Il existe même des ensembles très semblables dont l'un est ensemble unitaire et l'autre est (seulement) ensemble d'unicité.

Exemple : Soit $A_1 = \{3^\alpha, \alpha \geq 1\} \cup \{3k+1, k \geq 0\}$

$$A_2 = \{3^\alpha, \alpha \geq 1\} \cup \{3k+2, k \geq 0\}$$

A_2 est un ensemble unitaire mais A_1 est seulement un ensemble d'unicité.

Montrons que A_2 est un ensemble unitaire. Soit f une fonction multiplicative dont la restriction à A_2 est la fonction 1. Tout entier m se met sous la forme

$$m = 3^\alpha m' \quad \text{où} \quad m' \equiv 2\ (3) \quad \text{ou} \quad m' \equiv 1\ (3)\ ;$$

de telle sorte que $f(m) = f(m')$.

Si $m' \equiv 2\ (3)$, il est clair que $f(m) = f(m') = 1$.

Si $m' \equiv 1\ (3)$, on peut trouver un nombre m'' tel que

$$(m',m'') = 1 \quad \text{et} \quad m'' \equiv 2\ (3).$$

Ainsi $$f(m) = f(m') = f(m')f(m'') = f(m'm'') = 1,$$

car $m'm'' \in A_2$.

Montrons que A_1 est un ensemble d'unicité. Soit g une fonction additive dont la restriction à A_1 est la fonction nulle. Reprenant la décomposition précédente de tout entier $m \geqslant 1$, il est clair que le seul cas à étudier est celui des entiers $n \equiv 2\ (3)$. On peut alors trouver deux entiers n_1 et n_2 congrus à 2 modulo 3 tels que :

$$(n_1,n) = (n_2,n) = (n_1,n_2) = 1.$$

Ainsi :
$$2f(n) = f(n_1) + f(n) + f(n_2) + f(n) - |f(n_1)+f(n_2)|$$
$$f(n) = \frac{1}{2} f(n_1n) + \frac{1}{2}f(n_2n) - \frac{1}{2}f(n_1n_2)$$
$$= 0.$$

A_1 n'est pas un ensemble unitaire. En effet la fonction multiplicative h définie par

$$h(p^r) = \begin{cases} -1 & \text{si } p^r \equiv 2\ (3) \\ 1 & \text{si } p^r \equiv 1\ (3) \text{ ou si } p = 3, \end{cases}$$

est égale à 1 sur A_1.

4.2. Il semble très difficile de montrer que l'ensemble $B = \{p+1\ ;\ p \in \mathcal{P}\}$ est un ensemble unitaire. Le meilleur résultat "accessible" est, semble-t-il, le suivant :

PROPOSITION 6.- *Il existe un entier* $a \geqslant 1$ *tel que, quelle que soit la fonction multiplicative* f *dont la restriction à l'ensemble* $\{p+1\ ;\ p \in \mathcal{P}\}$ *vaut* 1

$$\forall\ n \geqslant 1 \qquad [f(n)]^a = 1.$$

La démonstration de cette proposition utilise le résultat suivant qui est une simple généralisation d'un résultat antérieur de Katai [2] :

PROPOSITION 7.- *Il existe un entier* N *et une partie* S *de* $\mathcal{P}'$ *vérifiant* $\sum_{p' \in S} \frac{1}{p'} < \infty$ *, tels que pour tout élément* p' *de* $\mathcal{P}'$-S *supérieur ou égal à* N *, il existe un nombre premier* p *tel que*

$$p+1 = d\,p'$$

où tout diviseur q' *de* d *appartenant à* $\mathcal{P}'$ *vérifie*

$$q' < p' \quad et \quad q' \notin S.$$

Soit maintenant une fonction multiplicative f dont la restriction à B vaut 1 et g la fonction additive définie par :

$$\forall\, p' \in \mathcal{P}', \qquad f(p') = e^{2i\pi g(p')}, \quad 0 \leqslant g(p') < 1.$$

Comme l'ensemble B est ensemble d'unicité (la démonstration, due à Elliott, figure dans [3]), on peut appliquer la proposition 2 et dire que, pour tout élément p' de $\mathcal{P}'$ inférieur à N, il existe une suite $(\alpha_p(p'))_{p \in \mathcal{P}}$ de nombres rationnels presque tous nuls tels que

$$f(p') = e^{2\pi i g(p')} = e^{2\pi i \sum_{p \in \mathcal{P}} \alpha_p(p')\, g(p+1)}.$$

Par suite il existe une suite d'entiers $(\beta_p(p'))_{p \in \mathcal{P}}$ presque tous nuls et un entier $a_{p'} \geqslant 1$ tels que :

$$f(p')^{a_{p'}} = e^{2\pi i \sum_{p \in \mathcal{P}} \beta_p(p') g(p+1)} = \prod_{p \in \mathcal{P}} [f(p+1)]^{\beta_p(p')} = 1.$$

Posons a = p.p.c.m. $(a_{p'}\ ;\ p' < N)$, de telle sorte que

$$\forall\, p' < N, \qquad f(p')^a = 1.$$

La proposition 7, permet alors, par récurrence, de dire que

$$\forall\, p' \in \mathcal{P}' - S, \qquad f(p')^a = 1.$$

Pour montrer enfin que les éléments p' de S vérifient la même relation, on peut utiliser un résultat obtenu dans [6] et dire que, pour chacun de ces

éléments, il existe une infinité de nombres premiers p tels que l'on ait :

$$p+1 = 2p'm$$

où m est sans facteur carré, est premier avec $2p'$ et n'a aucun facteur premier dans S.

Ainsi $f(m)^a = 1$, et par conséquent $f(2p')^a = 1$. Il suffit alors de remarquer que $f(2) = \frac{f(5+1)}{f(2+1)} = 1$ pour obtenir la proposition 6.

On peut également obtenir cette proposition à partir de résultats obtenus par Wirsing ([7]) mais cette dernière méthode, pas plus que celle exposée ici, ne permet de donner une estimation de la valeur de a.

REFERENCES

[1] I. KÁTAI. On sets characterizing number-theoretical functions. Acta Arith. 13, 1968, pp. 315-20.

[2] I. KÁTAI. On sets characterizing number-theoretical functions (II). (The set of "prime plus one"'s is a set of quasi-uniqueness). Acta Arith. 16, 1968, pp. 1-4.

[3] P.D.T.A. ELLIOTT. A conjecture of Katai. Acta Arith. 26, 1974, pp. 11-20.

[4] F. DRESS et B. WOLKAMNN. Ensembles d'unicité pour les fonctions arithmétiques additives ou multiplicatives. C.R. Acad. Sci. Paris t. 287 (10 juillet 78).

[5] D. WOLKE. Bemerkungen über Eindentigkeitsmengen additiver Funktionen. Elements of Math. 33/1, pp. 14-16 (1978).

[6] J. MEYER. Sur les fonctions additives bornées sur les nombres de la forme p+1, avec p premier. Bull. Soc. Math. France, 105, 1977, pp. 33-45.

[7] E. WIRSING. Additive functions with restricted growth on the numbers of the form p+1. Acta Arith., à paraître.

Jacques MEYER
Université de REIMS
Département de Mathématiques
Moulin de la Housse
B.P. 347
51062 REIMS Cedex

GENERALISATIONS DU THEOREME DE LANDAU SUR LES SOMMES DE DEUX CARRES : LA METHODE DE FONCTIONS FROBENIENNES

R.W.K. ODONI

0. INTRODUCTION.

Soit donnée une répartition des puissances des nombres premiers dans une famille finie $\{\mathcal{C}_j\}_{j\in\mathcal{J}} = \mathcal{C}$ de classes. On pose, pour tout $j\in\mathcal{J}$ et tout entier $n \geq 1$, $\nu_j(n)$ = nombre des $p^k \| n$ pour lesquels $p^k \in \mathcal{C}_j$. Alors on obtient un "vecteur des multiplicités" $\nu(n) = \{\nu_j(n)\}_{j\in\mathcal{J}}$, dont chaque coordonnée est un entier ≥ 0, ou, en d'autres termes, $\nu(n)$ appartient au secteur positif de $\mathbb{Z}^{\mathcal{J}}$. Soit maintenant $\mathcal{T}$ un sous-ensemble quelconque de $\mathbb{Z}^{\mathcal{J}}$; je considère le problème d'obtenir un développement asymptotique de

$$N(x\,;\mathcal{T}) \underset{\text{déf}}{=} \sum_{\substack{1\leq n\leq x \\ \nu(n)\in\mathcal{T}}} 1\,, \tag{0.1}$$

quand x tend vers l'infini ; on verra facilement que plusieurs questions concrètes et naturelles se ramènent au problème posé.

Introduisons la série génératrice de Dirichlet

$$F(s\,;\mathcal{T}) \underset{\text{déf}}{=} \sum_{\nu(n)\in\mathcal{T}} n^{-s}, \tag{0.2}$$

s étant une variable complexe dont la partie réelle $\sigma > 1$; sous cette restriction $F(s\,;\mathcal{T})$ est une fonction holomorphe de s, et on aura l'identité

$$\sum_{\substack{1\leq n\leq x \\ \nu(n)\in\mathcal{T}}} \log\frac{x}{n} = \frac{1}{2\pi i}\int_{\kappa-i\infty}^{\kappa+i\infty} \frac{x^s}{s^2}\, F(s\,;\mathcal{T})\, ds\,, \tag{0.3}$$

où $\kappa > 1$; (0.3) découle de la formule sommatoire de Mellin-Perron.

La formule (0.3) ne sera pas utile à moins que l'on connaisse le comportement de F (ou de son prolongement holomorphe (s'il en existe) à gauche de $\sigma = 1$) près de ses singularités, ainsi que sa croissance pour $|\text{Im } s| \to \infty$. La nécessité d'introduire les sommes et intégrales "à poids" dans (0.3) devient claire en considérant le cas particulier où $\mathcal{J} = \mathbb{Z}^{\mathcal{J}}$, pour lequel $f(s ; \mathcal{J}) = \zeta(s)$, la fonction zêta de Riemann. De toute façon, si l'on a un développement asymptotique convenable de la partie gauche de (0.3), on peut en déduire celui de (0.1) par une méthode bien connue (voir, par exemple, [1] pp. 6-7 ou 233-235).

Pour atteindre notre but, il nous faut maintenant étudier la fonction F de (0.2). On commence par introduire des variables complexes auxiliaires z_j $(j \in \mathcal{J})$, et on définit un produit eulérien

$$E(s ; z ; \mathcal{C}) \underset{\text{déf}}{=} \prod_p \{1 + \sum_{j \in \mathcal{J}} z_j \sum_{p^k \in \mathcal{C}_j} p^{-ks}\} , \tag{0.4}$$

qui converge absolument et uniformément pour $\sigma \geq 1 + \varepsilon$, $\varepsilon > 0$; ici p parcourt l'ensemble des nombres premiers. La fonction $E(s ; z ; \mathcal{C})$ est holomorphe pour $\sigma > 1$, et, comme fonction de $z = \{z_j\}_{j \in \mathcal{J}}$, elle est entière. On peut développer E comme série de Dirichlet

$$E(s ; z ; \mathcal{C}) = \sum_{n \geq 1} n^{-s} z^{\nu(n)} \qquad (\sigma > 1), \tag{0.5}$$

où $z^{\nu(n)}$ veut dire $\prod_j z_j^{\nu_j(n)}$.

Nous voudrions établir un rapport entre E et F. Pour cela on considère la série génératrice de $\mathcal{J}$, c'est-à-dire

$$S(z) = \sum_{\substack{m \in \mathcal{J} \\ m \geq 0}} z^m ; \tag{0.6}$$

on peut supposer dans (0.6) que tout $|z_j| < 1$, ce qui assure la convergence et l'holomorphie de S. On peut également écrire $S(z) = \sum_{m \geq 0} \varepsilon(m) z^m$, où $\varepsilon(m)$ est la fonction indicatrice de . Alors on a l'identité

$$F(s ; \mathcal{J}) = (2\pi i)^{-\# \mathcal{J}} \int_\Gamma \cdots \int E(s ; z^{-1} ; \mathcal{C}) S(z) \prod_j \frac{dz_j}{z_j} , \tag{0.7}$$

où $z^{-1} = \{z_j^{-1}\}_{j \in \mathcal{J}}$, et Γ est le cycle-produit dans $\mathbb{C}^{\mathcal{J}}$, dont le j-ième composant est le cercle $|z_j| = \rho < 1$, avec l'orientation habituelle. (0.7) repré-

sente un cas particulier de l'identité classique d'Hadamard (voir, par exemple, [2], pp. 157-159) ; elle relie les séries de puissances $\sum a_n z^n$, $\sum b_n z^n$ et $\sum a_n b_n z^n$ (ou, plutôt, sa généralisation simple aux séries multiples).

On voit maintenant, en vertu de (0.7), que l'étude de F se réduit aux études de E et de S. Comme posé ci-dessus, le problème de la détermination de (0.1) est trop général et difficile à résoudre, parce que les fonctions E et S qui interviennent dans (0.7) auront, en général, des singularités compliquées. Par exemple, il est possible que E n'ait aucun prolongement holomorphe (comme fonction de s), ce qui rendrait inutile la formule (0.3). Dans le § 1, nous imposerons quelques conditions assez naturelles qui nous aideront à exploiter (0.7).

1. LE CAS FROBENIEN.

Considérons maintenant un cas particulier du problème du § 0, qui se présente souvent dans plusieurs applications. Soit donnée une extension finie galoisienne $K/\mathbb{Q}$, non ramifiée au dehors de l'ensemble des diviseurs premiers de l'entier $D \geq 1$. Soit θ une application du monoide $\mathbb{N}^{(D)}$ (des entiers positifs premiers à D) dans un monoide commutatif fini M. On appelle θ <u>multiplicative</u> (resp. <u>totalement multiplicative</u>) si $\theta(ab) = \theta(a)\theta(b)$ pour tous les entiers $a, b \geq 1$ tels que $(a,D) = (b,D) = 1$ et $(a,b) = 1$ (resp. à l'exception de la dernière condition). On appelle θ <u>multiplicative frobénienne</u> si elle est multiplicative et satisfait à la condition

(F) : *Pour tout nombre premier* p, $p \nmid D$, *et tout* $n \geq 1$, *la valeur de* $\theta(p^n)$ *ne dépend que de* n *et de la classe* $[\frac{K/\mathbb{Q}}{p}]$ *de Frobenius de* p *dans* $G = \mathrm{Gal}\, K/\mathbb{Q}$.

(On se rappelle que $[\frac{K/\mathbb{Q}}{p}]$ est la classe de conjugaison dans G qui contient, pour chaque idéal premier $\mathfrak{p}$ de K qui divise p, l'automorphisme de Frobenius $\varphi = \varphi_{\mathfrak{p}}$ pour lequel $\varphi(x) \equiv x^p \pmod{\mathfrak{p}}$ pour tout entier x de K).

<u>Exemples</u>. (a) Soit $k \geq 1$ entier, M = groupe des racines $\varphi(k)$-ièmes de l'unité dans $\mathbb{C}$, $D = 2k$, $K = \mathbb{Q}(\zeta)$ (ζ = racine k-ième primitive de 1), $\theta(a) = \chi(a)$,

où χ est un caractère de Dirichlet (mod k). La multiplicativité totale de θ est triviale, tandis que la propriété frobénienne résulte du fait que la classe $[\frac{K/\mathbb{Q}}{p}]$ ne dépend que de la classe résiduelle de p (mod k).

(b) Soit F un corps de nombres algébriques, ayant pour groupe de classes d'idéaux le groupe (fini, abélien) I. On prend pour M l'ensemble 2^I des sous-ensembles de I, muni de l'opération binaire

$$A \circ B = \{ab \ ; \ a \in A, \ b \in B\} .$$

On convient de définir $A \circ \emptyset = \emptyset$ pour tout A M, si $\emptyset$ désigne l'ensemble vide. Alors M devient un monoide commutatif fini dont l'unité est I. Soit maintenant D le discriminant de $F/\mathbb{Q}$; si $(n,D) = 1$, on pose

(1.1) $\theta(n) = \{$classes qui contiennent des idéaux $\mathfrak{a}$ tels que $N\mathfrak{a} = n\}$,

où N = norme absolue. Alors on voit facilement que θ est multiplicative. La propriété frobénienne se déduit de la théorie des corps de classes ; on considère l'extension $K/\mathbb{Q}$ = enveloppe galoisienne du corps de classes hilbertien H de F ; les propriétés fonctorielles de l'automorphisme de Frobenius, et la loi de réciprocité d'Artin nous donnent que $\theta(p^t) = \theta(q^t)$ pour tout $t \geq 1$, si $[\frac{K/\mathbb{Q}}{p}] = [\frac{K/\mathbb{Q}}{q}]$, p et q étant nombres premiers qui ne divisent pas D.

Nous allons montrer que le problème général du § 0 est résoluble quand la répartition $\{\mathcal{C}_j\}_{j \in \mathcal{J}}$ est associée à une fonction frobénienne d'une façon naturelle. On remarque immédiatement que le formalisme du § 0 n'est changé que trivialement si l'on veut omettre un ensemble fini de nombres premiers, avant de faire la répartition. Omettons donc les nombres premiers qui divisent D ; on donne aux éléments de M les étiquettes j $(j \in \mathcal{J})$ et on pose

(1.2) $$\mathcal{C}_j = \{p^k \ ; \ p \nmid D, \ \theta(p^k) = m_j\} .$$

Considérons maintenant (0.7) (où E reçoit la modification triviale de l'omission des facteurs premiers de D). Le comportement de E devient clair en prenant le logarithme (principal) du produit eulérien (0.4) ; en supposant z borné, on utilise le développement de Taylor de $\log(1+w)$ (w petit), ce qui montre que les singularités de E sont dûes à la série

$$(1.3)\qquad \sum_{p/D}\ \sum_{j\in\mathcal{J}} z_j \sum_{\substack{k\\ p^k\in\mathcal{C}_j}} p^{-ks} = \sum_j z_j \sum_p \sum_{\substack{k\\ p^k\in\mathcal{C}_j}} p^{-ks}\ .$$

A ce point on se rappelle que θ est frobénienne ; alors on peut invoquer le théorème de Cebotarev - Hecke - Artin (voir [3], [4]). On a

$$(1.4)\qquad \sum_{[\frac{K/\mathbb{Q}}{p}]=<\tau>} p^{-s} - \frac{\#<\tau>}{\#G}\log\frac{1}{s-1} = R_\tau(s)$$

où $<\tau>$ désigne la classe de conjugaison engendrée par $\tau\in G$, et la fonction $R_\tau(s)$ possède un prolongement holomorphe dans une région

$$(1.5)\qquad \mathcal{R} : \sigma > 1 - \frac{c_1}{\log(4+t^2)}\ ,\ (c_1>0),$$

(où $s=\sigma+it$, t réel), tandis que dans $\mathcal{R}$ la croissance de $R_\tau(s)$ est dominée par $(\log\log(4+t^2))^{c_2}$ quand $t^2\to\infty$; ici, les constantes c_1 et c_2 ne dépendent que du corps K. Ce théorème nous donne la connaissance des singularités de E nécessaire pour l'utilisation de (0.7).

Passons maintenant à la question du comportement de la fonction génératrice $S(z)$; pour la simplicité je me borne au cas où $\nu(n)\in\mathcal{J} \Leftrightarrow \theta(n)=\mu$, μ étant un élément fixe quelconque de M. Dans ce cas on peut donner une description assez précise de $S(z)$. Il s'agit de déterminer tous les vecteurs $\nu=\{\nu_j\}_{j\in\mathcal{J}}$ d'exposants non-négatifs pour lesquels

$$(1.6)\qquad \prod_{j\in\mathcal{J}} \mu_j^{\nu_j} = \mu\ ,$$

M étant un monoide fini, pour tout $j\in\mathcal{J}$ la suite $\{\mu_j^n\}$, $n=0,1,2,\ldots$, se répète (éventuellement). On peut donc associer à chaque relation (1.6) une relation "réduite", dans laquelle tous les exposants sont absolument bornés ; il ne faut que soustraire de chaque ν_j le multiple propre de la "période éventuelle" f_j de μ_j. (Ce multiple peut être 0 si ν_j appartient à la "queue antérieure", ou au "premier cycle", de la suite $\{\mu_j^n\}$). Alors l'ensemble des relations réduites de (1.6) est fini ; la somme $S(z)$ se décompose naturellement selon les relations réduites, tandis que toutes les sous-sommes correspondantes ont la forme d'une série géométrique, multipliée par un monôme en z. Il en résulte que $S(z)$ (pour z assez petit) est une fonction rationnelle de

la forme

$$\frac{P(z)}{\prod_{j\in\mathcal{J}} (1 - z_j^{f_j})} \tag{1.7}$$

où P est un polynôme. (Rappelons que f_j est la période éventuelle de μ_j).

La formule (1.7) nous donne le prolongement de $S(z)$ à une fonction méromorphe dans $\mathbb{C}^{\mathcal{J}}$ dont la variété polaire se décompose par rapport aux différentes variables. Ce prolongement nous permet de faire une déformation du cycle Γ qui intervient dans (0.7) ; on se rappelle que $E(s\,;w\,;\mathcal{C})$ est entière (comme fonction de w). Nous voudrions élargir Γ, en faisant tendre vers l'infini le rayon ρ des cercles composants. Grâce à la séparabilité des pôles de $S(z)$, le calcul des résidus peut être accompli une variable à la fois. Les pôles proviennent des vecteurs $\zeta = \{\zeta_j\}_{j\in\mathcal{J}}$, où ζ_j est ou bien une racine f_j-ième de 1, ou bien (peut être) ∞ (les derniers étant dûs au numérateur $P(z)$ de (1.7), si z_j y intervient). Si ζ_j est une racine de l'unité le z_j-pôle correspondant sera d'ordre ≤ 1, tandis que, si $\zeta_j = \infty$, l'ordre sera $\leq d_j - 1$, où $P(z)$ a le degré d_j relativement à z_j.

Un calcul élémentaire nous montre maintenant que (0.7), en faisant $\rho \to \infty$, rend une combinaison linéaire finie de termes du type

$$\partial E(s\,;z^{-1}\,;\mathcal{C})\big|_{z=\zeta}\,, \tag{1.8}$$

où ∂ est un opérateur différentiel à coefficients constants, et d'ordre fini, par rapport à z. En tenant compte de (1.3)-(1.5), on voit que les termes (1.8) ont, en général, la forme

$$Q(\log \tfrac{1}{s-1})\,(s-1)^{-\sum_j \delta_j \zeta_j^{-1}} \tag{1.9}$$

au voisinage de $s = 1$, où $Q(T)$ est un polynôme en T dont les coefficients sont des fonctions de s holomorphes dans la région $\mathcal{R}$ de (1.5), d'une croissance bornée par $|t|^{\varepsilon}$ $(\varepsilon > 0)$ quand $t^2 \to \infty$ dans $\mathcal{R}$, tandis que δ_j est la densité de Dirichlet des p pour lesquels $\theta(p) = \mu_j$. Bien entendu, les δ_j sont des nombres rationnels non négatifs, dont les dénominateurs divisent $[K:\mathbb{Q}]$. Si l'exposant $\sum_j \delta_j \zeta_j^{-1} = 0$, il est possible que (1.8) soit holomorphe

au voisinage de $s = 1$; par exemple, les δ_j peuvent être 0 pour tout j avec $\zeta_j = \infty$; alors le rôle de $s = 1$ sera joué par $s = 1/2$, ou $1/3$, ou $1/4$, etc., si $\deg Q = 0$.

En suivant la procédure de [5], on déforme le contour vertical de $\kappa - i\infty$ $\kappa + i\infty$, qui se présente dans (0.3), en un contour qui s'approche du bord gauche de $\mathcal{R}$, en évitant la coupure que l'on doit faire sur la ligne réelle, à la gauche de $s = 1$, pour que les logarithmes soient holomorphes et univalents sur le nouveau contour. On obtient alors le développement voulu de (0.3) dans le cas frobénien ; chaque pôle de $S(z)$ nous donne une combinaison linéaire finie de développements asymptotiques de l'espèce

$$(1.10) \qquad x(\log\log x)^{d-1}(\log x)^{\sum \delta_j\zeta_j^{-1}-1}\{c_0 + c_1(\log x)^{-1}+\ldots+c_n(\log x)^{-n}+\ldots\} ,$$

où $1 \le d \le \deg P(z)$ ($P(z)$ défini par (1.7)), pourvu que $s = 1$ soit une singularité de $\partial E(s ; \zeta^{-1} ; \mathcal{C})$; dans le cas dégénéré, où ∂E est holomorphe près de $s = 1$, l'exposant de x peut se changer en $1/2$, ou $1/3$, etc. Le terme d'erreur pour ces développements sera ou bien

$$(1.11) \qquad O(x \exp(-c(K)\sqrt{\log x}))$$

(dans le cas normal), ou bien

$$(1.12) \qquad O(x^{\frac{1}{m}} \exp(-c(K)\sqrt{\log x}))$$

($m \ge 2$) (dans les cas dégénérés).

2. QUELQUES APPLICATIONS.

(a) Généralisations du théorème de Landau sur les sommes de deux carrés.

Soient $F_1,\ldots,F_k$ des corps de nombres algébriques, soit donné dans F_i un $\mathbb{Z}$-module M_i de rang maximal, contenu dans l'anneau $\mathcal{O}_i$ des entiers de F_i , et soit $\alpha_i \in \mathcal{O}_i$. On considère les $n \ge 1$ dans $\mathbb{Z}$ pour lesquels

$$(2.1) \qquad n = N_{F_i/\mathbb{Q}}(\alpha_i + \mu_i) \qquad (\text{avec } \mu_i \in M_i)$$

est résoluble pour tout i, $1 \le i \le k$; on voudrait leur répartition.

Le cas où $k = 1$ et $F = \mathbb{Q}(\sqrt{-1})$ fut étudié par Landau [7] ; ses résultats furent

généralisés aux corps quadratiques quelconques par Bernays [8]. Pour tous ces cas la théorie classique des formes binaires quadratiques suffit pour la résolution. Cependant, pour les corps plus généraux, il nous faut introduire des idées plus profondes. Pour le cas général, on commence par se ramener au problème suivant : déterminer la répartition des n pour lesquels on peut satisfaire simultanément aux conditions

$$n = N\mathfrak{A}_i \ , \tag{2.2}$$

$\mathfrak{A}_i$ étant un idéal qui appartient à une classe $(\mathrm{mod}^* F_i)$ donnée dans F_i, où F_i est le plus grand idéal de $\mathfrak{O}_i$ contenu dans M_i. Ce problème est discuté en détail dans [9], [10], où j'ai démontré qu'il est réductible, grâce à la théorie des corps de classes, à un problème concernant une fonction multiplicative frobénienne du type du § 1 ; quelques problèmes encore plus généraux sont traités dans [10]. Dans tous les cas on obtient les développements asymptotiques du § 1.

(b) Problèmes qui concernent les coefficients des formes modulaires.

Dans [1] Serre a énoncé quelques résultats et problèmes associés aux formes modulaires "tordues" par les caractères impairs de Dirichlet. Dans certains cas on sait comment associer à une telle forme modulaire une famille de fonctions L d'Artin, en utilisant les opérateurs de Hecke et la transformation de Mellin. De cette manière on peut quelquefois étudier la répartition des coefficients de la forme modulaire qui satisfont à certaines conditions de congruence etc., par réduction à un problème concernant une fonction multiplicative frobénienne. J'ai discuté de telles questions dans [11] et [12], auxquels le lecteur intéressé pourra se référer.

3. REMARQUES EN CONCLUSION.

On peut songer à généraliser nos résultats ; par exemple, on voudrait peut-être admettre une famille infinie $\{\mathfrak{C}_j\}_{j\in\mathcal{J}}$ dans § 0 ; il est possible que l'on puisse attaquer de telles questions en utilisant quelques techniques de l'analyse fonctionnelle pour l'étude des fonctions génératrices d'une infinité de variables complexes ; sans doute, ce serait un problème assez difficile. Ou encore, dans le cas frobénien, on peut retenir la condition $\mathfrak{C}$ finie, tandis que l'on permet que le monoide M soit infini. On connaît quelques exemples où $S(z)$ est encore rationnelle, mais n'est plus séparable ; cette circonstance se présente si M est infini, mais engendré par un sous-ensemble fini. Pour ces exemples on doit utiliser la théorie générale des résidus (à plusieurs variables complexes), due à Leray [13], pour l'exploitation de (0.7).

En conclusion, je voudrais remercier le Professeur H. DELANGE, qui m'a signalé une certaine ressemblance entre certaines de mes méthodes et celles de ses oeuvres [5], [6].

REFERENCES

[1] J.P. SERRE. Divisibilité de certaines fonctions arithmétiques. Sém. Delange-Pisot-Poitou 197/75, # 20 (ou bien : L'Enseignement Math. XXII (1976), 227-260).

[2] E.C. TITCHMARSH. The Theory of Functions. (2e. ed. Clarendon Press, Oxford, 1939).

[3] H. HASSE. Zahlberitch. (3e Auflage, Physica Verlag, Würzburg-Wien, 1970) ; Tom 2, Kap. 5.

[4] J.C. LAGARIAS, A.M. ODLYZKO. Effective versions of the Cebotarev density theorem (Algebraic Number Fields, ed. Fröhlich, Academic Press, London, New-York, San Francisco, 1977), 409-464.

[5] H. DELANGE. Sur les formules de Atle Selberg. Acta Arithmetica XIX (1971), 105-146.

[6] H. DELANGE. Sur un théorème de Rényi-III. Acta Arithmetica XXIII (1973), 153-182.

[7] E. LANDAU. Handbuch der Lehre der Verteilung der Primzahlen. (Teubner, Leipzig, 1909) ; Tom 2, p. 643 et seq.

[8] P. BERNAYS. Uber die Darstellung..... durch primitiven binären qudratischen Formen (Dissertation, Göttingen 1912).

[9] R.W.K. ODONI. Global norm density theorems from an extended Cebotarev density theorem (Algebraic Number Fields, ed. Fröhlich - voir [4] - p. 485-495).

[10] R.W.K. ODONI. The distribution of integral and prime - integral values of systems of full - norm polynomials and affine - decomposable polynomials. Mathematika 26 (1979), 80-87.

[11] R.W.K. ODONI. Three problems of Serre on asymptotic properties of coefficients of modular forms on $\Gamma_0(N)$ (à paraître, Proc. London Math. Soc.).

[12] R.W.K. ODONI. Solution of some problems of Serre on modular forms ; the method of Frobenian functions (à paraître Proc. L.M.S. Symposium on Analytic Number Theory (Durham, July 1979)).

[13] J. LERAY. Le calcul différentiel et intégral sur une variété analytique complexe (Problème de Cauchy III). Bull. Soc. Math. France 87 (1959), 81-180.

R.W.K. ODONI
University of Exeter
Department of Mathematics
North Park Road
EXETER EX4 4QE England

SUR DES CONJECTURES D'ERDÖS ET MONTGOMERY CONCERNANT LES DIVISEURS D'UN ENTIER

G. TENENBAUM

Nous nous proposons ici de présenter certains résultats d'un travail en commun avec P. Erdös [6].

Le point de départ de notre étude réside en une conjecture d'Erdös datant de plus de quarante ans :

C1 : *Presque tout entier* n *possède au moins deux diviseurs* d *et* d' *satisfaisant à* $d < d' \leqslant 2d$.

En 1948, Erdös a montré que la suite des entiers possèdant cette propriété a effectivement une densité asymptotique, mais sa méthode ne permet pas d'établir que cette densité a pour valeur 1 [1].

Une justification heuristique de C1 peut être formulée ainsi : comme le nombre des valeurs distinctes des quantités $\log d'/d$, d et d' parcourant les diviseurs de n, est égal à

$$u(n) = \mathrm{card}\{d|n,\ d'|n : (d,d') = 1\} = \prod_{p^\nu \| n} (2\nu+1),$$

on a, pour tout entier n,

$$3^{\omega(n)} \leqslant u(n) \leqslant 3^{\Omega(n)},$$

où $\Omega(n)$ (resp. $\omega(n)$) désigne le nombre des facteurs premiers de n comptés avec (resp. sans) leur ordre de multiplicité ; de l'évaluation

$$\Omega(n) \sim \omega(n) \sim \log\log n$$

valable pour presque tout n, on tire donc

$$u(n) = (\log n)^{\log 3+o(1)}$$

pour presque tout n ; ainsi, on peut s'attendre à ce qu'un intervalle inclus dans $[-\log n, \log n]$ et de longueur λ contienne usuellement $\lambda(\log n)^{\log 3-1+o(1)}$ points $\log d'/d$ distincts ; la conjecture C1 exprime que dans le cas $I = [-\log 2, \log 2]$ le nombre de ces points est au moins égal à 2.

Cet argument a conduit Erdös à formuler la conjecture plus forte suivante, qu'il a annoncé pour pouvoir établir en 1964 [2].

C2 : *Pour tout réel positif* ε *et presque tout entier* n, *on a*

$$1+(\log n)^{1-\log 3-\varepsilon} < \min\{\frac{d'}{d} : d|n,\ d'|n,\ d < d'\} < 1+(\log n)^{1-\log 3+\varepsilon}.$$

Malheureusement, alors que l'inégalité de gauche a été récemment prouvée, sous une forme légèrement plus précise, par Erdös et Hall [5], celle de droite doit encore rester conjecturale.

Fondée sur le même argument heuristique, une autre conjecture est énoncée par Hall et l'auteur dans [7] :

C3 : *Pour tout réel* α *de* $[0,1]$ *et presque tout entier* n, *on a*

$$U(n,\alpha) := \mathrm{card}\{d|n, d'|n : (d,d') = 1,\ |\log\frac{d'}{d}| \leqslant (\log n)^{\alpha}\} = (\log n)^{\log 3-1+\alpha+o(1)}$$

Dans cet article, nous établissons que l'inégalité

$$U(n,\alpha) \leqslant (\log n)^{\log 3-1+\alpha+o(1)}$$

a effectivement lieu pour presque tout n, mais nous n'obtenons pas la borne inférieure souhaitée.

Désignons par $\tau(n)$ le nombre des diviseurs d'un entier n ; dans le but de prouver C1, Erdös a introduit la fonction arithmétique $\tau^+(n)$, égale au nombre des entiers k pour lesquels l'intervalle $[2^k, 2^{k+1}[$ contient au moins un diviseur de n. On a toujours $\tau^+(n) \leqslant \tau(n)$ et il suffirait, pour prouver C1, d'établir, pour presque tout n, l'inégalité stricte. Cela a conduit Erdös (voir par exemple [3]) à émettre la

conjecture suivante

C4 : *Quitte à négliger une suite d'entiers de densité nulle, le rapport* $\tau^+(n)/\tau(n)$ *tend vers* 0 *lorsque* n *tend vers l'infini.*

Dans [6], nous obtenons le résultat suivant qui, non seulement réfute C4, mais implique même que toute suite $\mathcal{A}$ telle que $\lim_{n\in\mathcal{A}} \frac{\tau^+(n)}{\tau(n)} = 0$ est de densité nulle

THEOREME 1. *Pour tout réel positif* ε *, il existe une constante* $c(\varepsilon)$ *telle que, pour tout réel* α *,* $0 \leqslant \alpha \leqslant 1$*, la densité supérieure de la suite des entiers* n *satisfaisant à* $\tau^+(n) \leqslant \alpha\, \tau(n)$ *ne dépasse pas* $c(\varepsilon)\alpha^{1-\varepsilon}$.

Notons $1 = d_1 < d_2 < \ldots < d_\tau = n$ la suite croissante des diviseurs d'un entier générique n ; et posons

$$\psi(n) := \max\{\log \frac{d_{i+1}}{d_i} : 1 \leqslant i \leqslant \tau-1\}$$

$$f(n) := \mathrm{card}\{i(1 \leqslant i \leqslant \tau-1) : (d_i, d_{i+1}) = 1\}$$

$$g(n) := \mathrm{card}\{i(1 \leqslant i \leqslant \tau-1) : d_i | d_{i+1}\}.$$

D'une manière générale les résultats impliquant les rapports entre d_i et d_{i+1} sont difficiles à obtenir. Dans [8], nous montrons que $\psi(n)/\log n$ possède une fonction de répartition continue sur $[0,1]$ et "voisine" de l'identité. Dans [4], Erdös et Hall, fournissent une minoration non triviale de l'ordre maximal de $f(n)$. Dans [6], nous établissons le résultat suivant

THEOREME 2. *Pour tout réel* α *de* $[0,1]$*, désignons par* $\Delta(\alpha)$ *la densité supérieure de la suite des entiers* n *satisfaisant à*

$$g(n) \leqslant \alpha\, \tau(n)$$

Alors on a $\lim_{\alpha \to 0} \Delta(\alpha) = 0$.

Ce résultat avait été conjecturé par Montgomery lors du Symposium de Théorie analytique des nombres de Durham en 1979. Son argument heuristique était le suivant : soit n un entier et p son plus petit facteur premier ; quitte à négliger une suite de n de densité nulle, on peut supposer $\log p \leqslant (\log n)^{o(1)}$; de plus, la moitié au

moins des diviseurs de n divisent n/p et, si $d_i \mid \frac{n}{p}$ mais $d_i \nmid d_{i+1}$ on a $d_{i+1} < p\, d_i$, or la mesure de $\bigcup_{d_i \mid (n/p)}]\log d_i, \log p\, d_i[$ ne dépasse pas $\tau(n) \log p$, elle est donc presque toujours $\leqslant (\log n)^{\log 2+o(1)}$ et l'on peut s'attendre à ce que la proportion des $\log d_{i+1}$ contenus dans cette réunion tende vers 0 comme $(\log n)^{\log 2-1+o(1)}$; le résultat conjecturé nécessite seulement qu'elle soit majorée par une constante $< \frac{1}{2}$.

Ainsi une même idée sous-tend les théorèmes 1 et 2 : les diviseurs d'un entier ne sont pas trop souvent trop proches. Le schéma de la démonstration du théorème 2 est le suivant : soit $n = pm$ un entier dont le plus petit facteur premier est p ; un argument voisin de celui qui est utilisé dans la preuve du théorème 1 permet d'établir, quitte à négliger une suite d'entiers n de densité supérieure tendant vers 0 avec ζ , qu'une proportion positive ζ des diviseurs δ de m sont tels que l'intervalle $]\frac{\delta}{p}, p\delta[$ ne contienne aucun diviseur de m autre que δ ; cela implique, en posant $\delta = d_i$, $d_i \mid n$, que $d_{i+1} = p\, d_i$, d'où

$$g(n) \geqslant \zeta\, \tau(m) \geqslant \frac{\zeta}{2}\, \tau(n).$$

BIBLIOGRAPHIE

[1] P. ERDÖS. *On the density of some sequences of integers*, Bull. Amer. Math. Soc. 54 (1948), 685-692.

[2] P. ERDÖS. *On some applications of probability to analysis and number theory*, J. London Math. Soc. 39 (1964), 692-696.

[3] P. ERDÖS. *Some unconventional problems in number theory*, Astérisque 61 (1979), 73-82.

[4] P. ERDÖS and R.R. HALL. *On some unconventional problems on the divisors of integers*, J. Austral. Math. Soc. (Series A) 25 (1978), 479-485.

[5] P. ERDÖS and R.R. HALL. *The propinquity of divisors*, Bull. London Math. Soc. 11 (1979), 304-307.

[6] P. ERDÖS et G. TENENBAUM. *Sur la structure de la suite des diviseurs d'un entier*, Ann. Inst. Fourier, à paraître.

[7] R.R. HALL et G. TENENBAUM. *Sur la proximité des diviseurs*, Proc. of the Symposium on progress in Analytic Number Theory (Durham 1979), à paraître.

[8] G. TENENBAUM. *Lois de répartition des diviseurs, 5*, J. London Math. Soc. (2) 20 (1979), 165-176.

G. TENENBAUM
U.E.R. de Mathématiques
Université de Bordeaux I

F 33405 TALENCE Cedex