PUBLICATIONS MATHÉMATIQUES D'ORSAY

Groupe de travail en théorie analytique et élémentaire des nombres

1989 - 1990

92 - 01

Université de PARIS-SUD

Département de Mathématiques
Bâtiment 425
91405 ORSAY France

PUBLICATIONS

MATHÉMATIQUES

D'ORSAY

Groupe de travail
en théorie analytique et élémentaire
des nombres

1989 - 1990

92 - 01

Université de PARIS-SUD

Département de Mathématiques
Bâtiment 425
91405 ORSAY France

TABLE DES MATIÈRES

DES NOUVELLES DES AUTOMATES

Jean-Paul ALLOUCHE

Cet article résume deux exposés indépendants donnés fin 1989 et début 1990. le premier, intitulé "Suites k-régulières" relatait un travail en commun avec J. Shallit ([4]), le second avait pour titre "Sur la transcendance de la série formelle Π" et annonçait un article accepté pour publication dans la nouvelle série du Séminaire de Théorie des Nombres de Bordeaux ([2]).

I.– Suites q-régulières

Une suite U à valeurs dans un alphabet (ensemble fini) est q-automatique si son q-noyau (c'est-à-dire l'ensemble de sous-suites $\{n \longrightarrow U(q^k n + r); k \geq 0; 0 \leq r \leq q^k - 1\}$) est fini. Par exemple la somme des chiffres de n en base q, réduite modulo q, est une suite q-automatique. Comment généraliser cette notion au cas d'une suite à valeurs dans un ensemble infini ? La somme des chiffres de n en base q (non réduite) peut-elle entrer dans un tel cadre plus général ? Nous proposons dans un article avec Shallit ([4]) la notion de suite q-régulière :

DÉFINITION. — *Une suite à valeurs dans un anneau commutatif et nœthérien R est dite q-régulière si son q-noyau engendre un R-module de type fini.*

Notons que si l'anneau R est fini, on retrouve la notion de suite q-automatique (c'est d'ailleurs aussi le cas pour un anneau infini si on se limite aux suites qui ne prennent qu'un nombre fini de valeurs). Notons aussi que la somme des chiffres en base q, ainsi que la suite du nombre d'occurrences d'un certain bloc de chiffres dans l'écriture de l'entier n en base q, sont q-régulières.

Remarquons que cette définition "fixe" l'ensemble dans lequel les suites prennent leurs valeurs, alors qu'une suite q-automatique le reste si on renomme l'alphabet. Un certain nombre de propriétés des suites q-automatiques "passent" aux suites q-régulières (voir [4]), mais ce que nous

voudrions souligner ici, c'est qu'un très grand nombre de suites qui apparaissent dans la littérature sont q-régulières, ainsi, en vrac, en plus des deux exemples ci-dessus : les polynômes, la valuation q-adique, la suite de Moser-de Bruijn (suite croissante des entiers qui s'écrivent comme sommes de puissances distinctes de 4), la suite "horrible" de Loxton et van der Poorten, la suite associée au code de Gray binaire, la suite de van der Corput, le nombre de partitions de l'entier n en au plus j parties, le nombre d'entiers inférieurs à n qui sont somme de trois carrés... des précisions sur ces exemples, et d'autres exemples sont donnés dans [4].

Remarque :

Une autre généralisation de la notion de suite q-automatique a été donnée par Sharif et Woodcock dans [6] et par Harase dans [5] : une suite U à valeurs dans un corps K de caractéristique p (fini ou pas) est dite p-automatique si, en notant $\overline{K}$ un surcorps parfait du corps K, (par exemple la clôture algébrique, ou la clôture radicielle de K), le $\overline{K}$-espace vectoriel engendré par l'ensemble de sous-suites $\{n \longrightarrow U^{1/p^k}(p^k n + r); k \geq 0; 0 \leq r \leq p^k - 1\}$ est de dimension finie sur $\overline{K}$. L'inconvénient de cette notion est que le p de la p-automaticité est nécessairement égal à la caractéristique du corps K (ou, à la rigueur, à une puissance de cette caractéristique), l'avantage est que le théorème de Christol, Kamae, Mendès France et Rauzy reste vrai dans ce cas : une suite U à valeurs dans le corps K de caractéristique p est p-automatique si et seulement si la série formelle $\sum_0^\infty U(n)X^n$ est algébrique sur $K(X)$, voir [6] et [5], voir aussi le survol [1].

II.– Sur la transcendance de la série formelle Π

Soit $\mathbb{F}_q$ un corps fini de caractéristique p et de cardinal $q = p^r$. Carlitz a introduit en 1935 une fonction, qui est appelée aujourd'hui fonction zéta de Carlitz, définie par :

$$\forall n \in \mathbb{N}^* \quad \zeta(n) = \sum{}' \frac{1}{P^n}$$

où P décrit les polynômes unitaires dans $\mathbb{F}_q[X]$. Notons que $\zeta(n)$ est un élément de $\mathbb{F}_q((X^{-1}))$.

Carlitz prouve, entre autres, que :

$$(q-1)|m \Longrightarrow \zeta(m) = \xi^m r_m$$

où r_m est une fraction rationnelle (c'est-à-dire un élément de $\mathbb{F}_q(X)$), et ξ la série formelle de Laurent définie par :

$$\xi = (X^q - X)^{1/(q-1)} \cdot \prod_{k=1}^{+\infty} \Big(1 - \frac{X^{q^k} - X}{X^{q^{k+1}} - X}\Big).$$

Dans les années 40, Wade a montré la transcendance de la série formelle ξ sur $\mathbb{F}_q(X)$, (ce qui implique la transcendance des valeurs de ζ pour les arguments divisibles par $q-1$). En 1988, Damamme et Hellegouarch ont obtenu d'autres valeurs de m pour lesquelles $\zeta(m)$ est transcendante; puis Yu a montré que toutes les valeurs de ζ sont transcendantes en utilisant les modules de Drinfeld. Enfin, tout récemment, Damamme a obtenu une preuve "élémentaire" des résultats de Yu.

Nous avons prouvé dans [2] (où on trouvera aussi toute la bibliographie évoquée ci-dessus) que la transcendance de la série formelle $\prod$ donnée par

$$\prod = \prod_{k=1}^{+\infty} \Big(1 - \frac{X^{q^k} - X}{X^{q^{k+1}} - X}\Big),$$

donc celle de ξ et celle de $\zeta(m)$ pour $(q-1)|m$, s'obtiennent très simplement en utilisant le théorème de Christol, Kamae, Mendès France et Rauzy. Voici le schéma de la preuve :

on pose $\alpha = \prod_{k=0}^{+\infty} \Big(\frac{1-X^{q^k}}{X^{q^{k+1}}}\Big)$, on prouve sans peine que α est algébrique ($\alpha^q = \alpha(1 - X^{1-q})^{-1}$), puis on remarque que :

$$\frac{\alpha}{\prod} = \prod_{j=0}^{\infty} \Big(1 - \frac{1}{X^{q^{j+1}} - 1}\Big) = \sum_{n=0}^{+\infty} a(n) X^{-n},$$

où $|a(n)|$ est la fonction caractéristique de l'ensemble des entiers qui s'écrivent $\sum \varepsilon_k (q^k - 1)$ (où ε_k vaut 0 ou 1). Pour montrer la transcendance de la série formelle Π, il suffit alors de prouver que la suite $(|a(n)|)$ n'est pas q-automatique, ce qui est détaillé dans [2]. Notons pour finir que, dans le cas $q = 2$, la suite $|a(n)|$ est le point fixe infini commençant par 1 de la substitution $1 \longrightarrow 110$, $0 \longrightarrow 0$, et que le lien de cette suite avec la définition de von Neumann des entiers naturels est expliqué dans [3].

BIBLIOGRAPHIE

Les travaux cités dans le texte qui ne sont pas référencés ci-dessous se trouvent dans les bibliographies de [2] et de [4].

[1] J.-P. ALLOUCHE. — Note sur un article de Sharif et Woodcock, *Séminaire de Théorie des Nombres de Bordeaux, 2ème série*, **1**, (1989), 163-187.

[2] J.-P. ALLOUCHE. — Sur la transcendance de la série formelle Π, *Séminaire de Théorie des Nombres de Bordeaux, 2ème série*, 2(1), (1990), 103-117.

[3] J.-P. ALLOUCHE, J. BÉTRÉMA, J. SHALLIT. — Sur des points fixes de morphismes d'un monoïde libre, *R.A.I.R.O., Informatique théorique et applications*, 23, **3**, (1989), 235-249.

[4] J.-P. ALLOUCHE, J. SHALLIT. — *The ring of k-regular sequences*, Preprint, 1990, à paraître dans Theoretical Computer Science.

[5] T. HARASE. — Algebraic elements in formal power series rings, *Isr. J. Math.*, 63, **3**, (1988), 281-288.

[6] H. SHARIF, C.F. WOODCOCK. — Algebraic functions over a field of positive characteristic and Hadamard products, *J. London Math. Soc.* (2), **37**, (1988), 395-403.

Jean-Paul ALLOUCHE
C.N.R.S. U.R.A. 0226
Mathématiques et Informatique
351, Cours de la libération
F-33405 TALENCE CEDEX

Travaux de Pomerance sur la fonction φ d'Euler

Michel BALAZARD et Abdelhakim SMATI

L'étude de l'interaction entre l'addition et la multiplication (ou entre l'ordre naturel et l'ordre de la divisibilité) est l'un des grands thèmes de la théorie analytique des nombres. Opérant un subtil décalage sur les facteurs premiers d'un entier, la fonction d'Euler est une source inépuisable de problèmes arithmétiques difficiles. Leurs solutions nécessitent souvent le recours aux théorèmes les plus profonds de la théorie, ainsi qu'une grande ingéniosité combinatoire. Nous nous proposons de présenter ici quelques uns de ces problèmes et d'introduire le lecteur aux nombreux travaux de Carl Pomerance sur le sujet. Nous aborderons les questions suivantes, $N(m)$ désignant le nombre de solutions en n de $\varphi(n) = m$.

1°) L'étude de la congruence

$$n \equiv a \mod \varphi(n), \quad a \in \mathbb{Z}.$$

2°) La conjecture de Carmichael ($N(m) \neq 1$ pour tout m).

3°) L'ordre maximal de $N(m)$.

4°) La loi de Gauss pour le nombre de facteurs premiers de $\varphi(n)$.

5°) L'évaluation du nombre de valeurs distinctes de la fonction d'Euler inférieures à une limite donnée.

Notre étude n'est pas exhaustive (cf. [9] par exemple, pour d'autres questions sur $\varphi(n)$ abordées par Pomerance). Nous tenons à remercier Carl Pomerance pour les commentaires et suggestions qu'il nous a communiqués à la lecture d'une première version de cet article.

1°) Sur la congruence $n \equiv a \pmod{\varphi(n)}$, $a \in \mathbb{Z}$.

On sait que si p est un nombre premier, alors

$$\varphi(p) = p - 1.$$

En 1932, Lehmer [20] posa la question de savoir s'il existe des entiers composés n tels que

$$\varphi(n) \mid n - 1.$$

C'est un problème encore ouvert. En fait il est vraisemblable que de tels entiers n'existent pas; cela fournirait une caractérisation (peu pratique) des nombres premiers. Dans son article de 1932, Lehmer montra que si un tel entier composé n existe, alors n est impair, sans facteur carré, et le nombre de ses diviseurs premiers est $\omega(n) \geq 7$. D'autres travaux suivirent, notamment ceux de Schuh [34] (1944) donnant $\omega(n) \geq 11$, de Lieuwens [21] (1970) montrant que si un tel entier n existe alors :

$$\begin{aligned} &\text{si} \quad 3|n, \quad \omega(n) \geq 213 \quad \text{et} \quad n > 5,5.10^{570} \\ \text{et} \quad &\text{si} \quad 30\nmid n, \quad \omega(n) \geq 13. \end{aligned}$$

Pour ce dernier cas, Wall [39] a montré en 1980 que $\omega(n) \geq 26$.

Dans une série d'articles [26], [27], [28], parus en 1975, 1976 et 1977, Pomerance étudia plus généralement la congruence

$$n \equiv a \ (\mathrm{mod}\, \varphi(n)), \ a \in \mathbb{Z}.$$

Considérant les ensembles :

$$F(a) = \{n : n \equiv a \ (\mathrm{mod}\, \varphi(n))\}, \ a \in \mathbb{Z},$$

on peut se poser les questions suivantes :

(a) Possèdent-ils un nombre fini ou infini d'éléments ?

(b) Peut-on décrire leurs éléments ?

(c) Quelle est la densité de $F(a)$?

En 1932, Lehmer identifia huit éléments de $F(-1)$. Sierpiński [35] en 1964, décrivit complètement l'ensemble $F(0)$ en montrant :

$$F(0) = \{1\} \cup \{2^\alpha 3^\beta : \alpha > 0 \ \text{ et } \ \beta \geq 0\}.$$

Pomerance (1975) montra que pour tout $a \in \mathbb{Z}$, l'ensemble $F(a)$ possède au moins quatre éléments. La preuve est simple; en effet, on vérifie que

$$\begin{aligned} &1 \text{ et } 2 \in F(a) \quad \text{pour tout} \quad a \in \mathbb{Z}, \\ &4 \text{ et } 6 \in F(a) \quad \text{pour tout} \quad a \in \mathbb{Z}, \quad a \text{ pair}. \end{aligned}$$

Enfin, si a est impair, on a $3 \in F(a)$ et

$$\begin{aligned} 5 \in F(a) \quad &\text{si} \quad a \equiv 1 \pmod 4 \\ 15 \in F(a) \quad &\text{si} \quad a \equiv 7 \pmod 8 \\ 9 \in F(a) \quad &\text{si} \quad a \equiv 3 \pmod{24} \\ 35 \in F(a) \quad &\text{si} \quad a \equiv 11 \pmod{24} \\ 7 \in F(a) \quad &\text{si} \quad a \equiv 19 \pmod{24}. \end{aligned}$$

Passons à l'étude de la fonction de comptage $N(F(a), x)$, l'objet principal de l'étude de Pomerance, où l'on note :

$$N(E, x) := \operatorname{card}\{n : 1 \le n \le x \ \text{ et } \ n \in E\},$$

pour tout sous-ensemble E de l'ensemble des entiers positifs.

La description de Sierpiński de l'ensemble $F(0)$ implique immédiatement que

$$N(F(0), x) \ll \log^2 x,$$

$\ll$ étant la notation de Vinogradov ; en particulier, la densité de $F(0)$ est nulle.

L'ensemble $F(1)$ contient tous les nombres premiers. Plus généralement, si $a \in F(0)$, alors $F(a)$ contient l'ensemble

$$F^o(a) := \{pa;\ p \text{ premier},\ p \nmid a\}.$$

En effet, $pa = a + \frac{a}{\varphi(a)}\varphi(pa)$, si p est premier et $p \nmid a$. Notons alors :

$$\begin{aligned} F'(a) &= F(a) \setminus F^o(a), \quad \text{si } a \in F(0); \\ F'(a) &= F(a), \qquad\qquad\ \ \text{si } a \notin F(0). \end{aligned}$$

Ainsi, $F'(1) = \{1\} \cup L$, où L est l'ensemble des entiers composés n tels que

$$\varphi(n) | n - 1.$$

Pomerance a donné trois majorations de $N(F'(a), x)$, de plus en plus fines.

THÉORÈME 1 (Pomerance [26]). — *On a, pour tout entier a et tout nombre réel $\beta < \frac{1}{\sqrt{2}}$,*

$$N(F'(a), x) = O(xe^{-\beta\sqrt{\log x \cdot \log_2 x}}).$$

Ici et dans toute la suite, $\log_k$ désigne la k-ième itérée de la fonction logarithme.

Une conséquence de ce théorème est que, quel que soit l'entier a,

$$N(F(a), x) = O\Big(\frac{x}{\log x}\Big);$$

en particulier, la densité de $F(a)$ est nulle.

La démonstration du théorème 1 est fondée sur les deux lemmes suivants, où α désigne une constante positive absolue telle que

$$(x \geq 1) \text{ et } (\varphi(n) \leq x) \Longrightarrow n \leq \alpha x \log_2(3x)$$

(cf. [16], theorem 328).

LEMME 1. — *Soient a, c des entiers, $c \geq 1$, et p_1, p_2 des nombres premiers tels que :*

(*i*) $p_i \nmid c$, $i = 1, 2$;

(*ii*) $p_i > 1 + 2\alpha \log\log(3c)$, $i = 1, 2$;

(*iii*) $p_i c > 64a^2$, $i = 1, 2$;

(*iv*) $p_i c \in F'(a)$, $i = 1, 2$.

Alors $p_1 = p_2$.

LEMME 2 (Erdös [6]). — *Soit x un nombre réel ≥ 3 et $y = (\log x \cdot \log_2 x)^{1/2}$. Le nombre d'entiers positifs $m \leq x$ qui ne vérifient pas les deux conditions*

(*i*) *le plus grand premier facteur de m est supérieur à $e^{y/\sqrt{2}}$;*

(*ii*) *le carré du plus grand facteur premier de m ne divise pas m, est $O(xe^{-\beta y})$ pour tout nombre réel $\beta < \frac{1}{\sqrt{2}}$ fixé à l'avance.*

Démonstration du théorème 1 : Reprenons les notations des lemmes 1 et 2, et supposons x assez grand de sorte que

$$e^{y/\sqrt{2}} > 1 + 2\alpha \log_2(3x).$$

Au vu du lemme 2, on peut se restreindre à considérer les entiers m de $F'(a)$, $m \leq x$, vérifiant les conditions (i) et (ii) de ce lemme. Supposons que les entiers $m \in F'(a)$, $64a^2 \leq m \leq x$, vérifiant (i) et (ii) du lemme 2, sont $m_1, m_2, \ldots, m_t$. Ecrivons $m_i = p_i c_i$, où p_i est le plus grand facteur premier de m_i, et $p_i \nmid c_i$. On a

$$c_i \leq x/e^{y/\sqrt{2}} \quad \text{pour } i = 1, 2, \ldots, t.$$

Pour conclure, il suffit d'observer que les c_i sont deux à deux distincts, d'après le lemme 1.

Comme $F'(1) = \{1\} \cup L$ avec $L = \{n \text{ composé} : \varphi(n) | n-1\}$, on obtient, en posant $a = 1$ dans le théorème 1 :

$$N(L, x) \ll x e^{-\beta\sqrt{\log x \cdot \log_2 x}}. \tag{1}$$

Si $n \in L$, alors $a^{n-1} \equiv 1 \pmod{n}$ pour tout a tel que $(a, n) = 1$ donc n est un nombre de Carmichael (on dit aussi pseudo-premier absolu). Un résultat de Knödel [19] sur les nombres de Carmichael implique (1), et un résultat d'Erdös [8] sur ces mêmes nombres donne le résultat suivant, meilleur que (1) :

$$N(L, x) \ll x \exp(-c \log x \cdot \log_3 x / \log_2 x), \tag{2}$$

pour une certaine constante absolue positive c.

S'inspirant des arguments de Knödel et Erdös, Pomerance améliora le théorème 1 en montrant :

THÉORÈME 2 (Pomerance [27]). — *On a, pour tout* $a \in \mathbb{Z}$:

$$N(F'(a), x) = O(x^{2/3} (\log_2 x)^{1/3})$$

En particulier, on a :

$$N(L, x) \ll x^{2/3} (\log_2 x)^{1/3},$$

ce qui améliore (2).

Donnons la démonstration du théorème 2 ; elle est assez simple, utilisant le lemme 1 et le théorème chinois des restes.

Si $a = 0$, le résultat est conséquence de la description de Sierpiński de $F(0)$.

Supposons $a \neq 0$. Soit x assez grand, et $n \leq x$, $n \in F'(a)$. On peut supposer $n > x^{2/3}(\log_2 x)^{1/3}$. Deux cas se présentent :

(i) il existe un diviseur premier p de n tel que $p > x^{1/3}(\log_2 x)^{-1/3}$;

(ii) tout diviseur premier p de n est $\leq x^{1/3}(\log_2 x)^{-1/3}$.

Dans le premier cas, p^2 ne peut diviser n car sinon $p|\varphi(n)$ et donc $p|a$, ce qui est impossible si x est assez grand puisque $a \neq 0$. Ecrivons $n = pc$ avec $p\nmid c$, d'où $c \leq x^{2/3}(\log_2 x)^{1/3}$. Le lemme 1 permet de dire qu'à chaque choix de n correspond un seul choix de c. Par conséquent, le nombre d'entiers n tels que (i) est vérifié est $\ll x^{2/3}(\log_2 x)^{1/3}$.

Dans le deuxième cas, n possède certainement un diviseur m vérifiant

$$x^{1/3}(\log_2 x)^{2/3} < m \leq x^{2/3}(\log_2 x)^{1/3} \tag{3}$$

On a donc :

$$n \equiv 0 \pmod m \quad \text{et} \quad n \equiv a \pmod{\varphi(m)}. \tag{4}$$

Le théorème chinois des restes prouve donc que pour chaque m vérifiant (3), il existe au plus

$$1 + \frac{x(m, \varphi(m))}{m\varphi(m)} \tag{5}$$

entiers n multiples de m et vérifiant (ii). Comme $m|n$ et $\varphi(m)|\varphi(n)$, on a $(m, \varphi(m))|(n, \varphi(n))|a$ donc (5) est

$$\leq 1 + |a|\frac{x}{m\varphi(m)} \leq 1 + \frac{|a|\alpha x \log_2(3x)}{m^2}$$

Il s'ensuit que le nombre des entiers n pour lesquels (ii) est vérifié est inférieur à

$$\sum{}'\left(1 + \frac{|a|\alpha x \log_2(3x)}{m^2}\right) \ll x^{2/3}(\log_2 x)^{1/3},$$

où $\sum'$ signifie une sommation portant sur les entiers m vérifiant (3). Cela termine la démonstration du théorème 2.

Enfin, en utilisant un argument plus élaboré, Pomerance montra en 1977 le théorème suivant :

THÉORÈME 3 (Pomerance [28]). — *On a pour tout* $a \in \mathbb{Z}$,

$$N(F'(a), x) = O(\sqrt{x}(\log x)^{3/4}).$$

Nous allons esquisser la démonstration de ce théorème. Dans un premier temps, on ramène l'étude de $F'(a)$ à celle de l'ensemble $F''(a)$ de ses éléments sans facteur carré, à l'aide du lemme suivant :

LEMME 3. — *On a, pour tout* $a \in \mathbb{Z}$,

$$N(F'(a), x) \leq 4a^2 + \sum_{d|a} N\Big(F''\Big(\frac{a}{d}\Big), x\Big)$$

L'argument essentiel est le lemme combinatoire suivant, qui montre que tout sous-intervalle raisonnable de $[0, \log n]$, où $n \in F''(a)$, contient $\log m$ où m est un diviseur de n.

LEMME 4. — *Soient* $\delta \geq 0$, $a_1 \geq a_2 \geq \cdots \geq a_t > 0$, $B_i = \sum_{j=i}^{t} a_j$, $1 \leq i \leq t$. *Supposons que*

$$a_i \leq \delta + B_{i+1} \quad \text{pour} \quad 1 \leq i \leq t-1.$$

Alors, pour tout y *compris entre* 0 *et* B_1, *il existe un sous-ensemble* S *de* $\{1, 2, \ldots, t\}$ *tel que*

$$y - \delta - a_t < \sum_{i \in S} a_i \leq y.$$

LEMME 5. — *Soit* $n \in F''(a)$, $n = p_1 p_2 \cdots p_k$, *avec* $p_1 > p_2 > \cdots > p_k$, $k = \omega(n)$. *Supposons que* $n > 16a^2$. *Alors on a*

$$p_i < (i+1)(1 + \prod_{j=i+1}^{k} p_j) \quad \textit{pour} \quad i = 1, \ldots, k-1.$$

LEMME 6. — *Il existe une constante positive absolue β telle que*

$$p(n) < \beta\sqrt{k \log k},$$

pour $n \in F''(a)$, $n \geq 16a^2$, où $p(n)$ est le plus petit facteur premier de n et $k = \omega(n)$. De plus, si $k > 4$, alors $p(n) \leq k + 1$.

Voici comment on déduit le théorème 3 de ces lemmes :

Soit $n \in F''(a)$ avec $16a^2 \leq n \leq x$, $n = p_1 p_2 \cdots p_k$, $k = \omega(n)$, $p_1 > p_2 > \cdots > p_k$. On peut supposer

$$n > g(x) := x^{1/2}(\log x)^{3/4}.$$

On pose $a_i = \log p_i$, $\delta = \log(2k)$, $t = k$ et $y = \log g(x)$. Le lemme 5 montre que l'hypothèse du lemme 4 est vérifié, à savoir :

$$\log p_i \leq \log(2k) + \sum_{j=i+1}^{k} \log p_j \quad \text{pour} \quad 1 \leq i \leq k-1.$$

Le lemme 4 montre alors qu'il existe un diviseur m de n tel que

$$\frac{g(x)}{2kp_k} < m \leq g(x).$$

Le lemme 6 et la relation $\omega(n) \ll \log n / \log_2(3n)$ donnent :

$$x^{1/2}(\log x)^{-\frac{3}{4}} \log_2 x \ll m \leq g(x).$$

Le même raisonnement que pour le théorème 2 montre alors que

$$N(F''(a), x) = O(\sqrt{x}(\log x)^{3/4})$$

et le théorème 3 découle immédiatement de cette relation et du lemme 3.

Terminons ce paragraphe par quelques remarques.

1°) Il y a un fossé entre le résultat :

$$N(L, x) \ll \sqrt{x}(\log x)^{3/4}$$

et le fait qu'on ne connaisse aucun élément de L. Dans ce contexte, Pomerance émet la

CONJECTURE A. — $N(L,x) \ll_\varepsilon x^\varepsilon$, *pour tout* $\varepsilon > 0$.

2°) Pomerance s'est intéressé également à l'étude de la congruence

$$\sigma(n) \equiv a \pmod{n},$$

où a est entier, σ désignant la fonction somme des diviseurs. Si l'on pose

$$\begin{aligned} S(a) &= \{n : \sigma(n) \equiv a \pmod{n}\}, \\ S^o(a) &= \{pn : p \text{ premier}, \ p \nmid n, \ n \in S(0) \text{ et } \sigma(n) = a\} \\ \text{et } S'(a) &= S(a) \setminus S^o(a), \end{aligned}$$

on peut faire une étude analogue. Par exemple, le théorème 1 reste vrai si l'on remplace $F'(a)$ par $S'(a)$; il serait intéressant d'établir les analogues des théorèmes 2 et 3.

Les paragraphes 2°), 3°), 5°) abordent l'étude de $N(m)$, le nombre des entiers naturels n vérifiant

$$\varphi(n) = m. \tag{6}$$

Pour tout m, $N(m)$ est fini, ce qui équivaut à dire que $\varphi(n)$ tend vers l'infini avec n. Il est clair que $N(m) = 0$ pour m impair > 1, mais il existe également une infinité d'entiers m pairs tels que $N(m) = 0$, par exemple $m = 2 \cdot 7^k$, $k = 1, 2 \cdots$ En fait, nous verrons au 5°) que presque tous les entiers m vérifient $N(m) = 0$, et nous étudierons le nombre d'exceptions $\leq x$.

D'autre part, (6) peut posséder beaucoup de solutions pour m fixé; par exemple $N(1920) = 63$, c'est-à-dire que 1920 est 63 fois valeur de φ : 1920 est une valeur "populaire" de la fonction d'Euler, suivant l'expression de Pomerance. Nous aborderons cet aspect des choses au 3°).

2°) La conjecture de Carmichael

En 1922, Carmichael [3] conjectura que $N(m) \neq 1$ pour tout entier m, c'est-à-dire que pour tout entier $n \geq 1$, il existe un entier $n' \geq 1$, $n' \neq n$, tel que $\varphi(n') = \varphi(n)$. Ce problème est toujours ouvert.

En 1947, Klee [18] montra que $N(m) \neq 1$ pour $m < 10^{400}$. En 1982, Masai et Valette [23] ont amélioré le résultat de Klee en montrant que $N(m) \neq 1$ pour $m < 10^{10\ 000}$.

En 1974, dans son premier article publié, Pomerance [29] s'intéressa à cette question. Il donna une condition suffisante pour que la conjecture de Carmichael soit fausse :

THÉORÈME 4. — *Soit n un entier naturel tel que pour tout nombre premier p, $p-1|\varphi(n)$ implique $p^2|n$. On a alors $N(\varphi(n)) = 1$.*

Si n' est un entier ≥ 1 tel que $\varphi(n') = \varphi(n)$, il s'agit de montrer que $n' = n$ pour démontrer le théorème. Cela se fait facilement en montrant que n et n' ont les mêmes facteurs premiers et que ceux-ci apparaissent avec les mêmes exposants dans la factorisation de n et n'. Nous omettons les détails.

Il est probable qu'il n'existe aucun entier n vérifiant la condition du théorème 4. Pour justifier cette remarque, Pomerance donne l'argument heuristique suivant. Sous la

CONJECTURE B. — *Pour tout $k \geq 2$, $(p_k - 1) \mid \prod_{i=1}^{k-1} p_i(p_i - 1)$, où p_i est le i-ième nombre premier,*

il n'existe aucun entier n vérifiant la condition du théorème 4. En effet, si n est un tel entier, alors $2^2|n$. Mais la conjecture B implique que $p_k^2|n$ si $p_1^2, p_2^2, \ldots, p_{k-1}^2$ divisent tous n. Il est alors clair que n serait divisible par tous les nombres premiers.

3°) L'ordre maximal de $N(m)$

Dans un article fondamental de 1935, Erdös [7] démontra l'existence d'une constante positive absolue c telle que

$$N(m) > m^c \tag{7}$$

soit vraie pour une infinité d'entiers m. Soit θ la borne supérieure des nombres c admissibles; Erdös conjectura que $\theta = 1$ et ce problème est toujours ouvert. De cet article, Pomerance tira un critère permettant de déduire des minorations de θ d'estimations concernant les nombres

premiers p tels que $p-1$ n'ait pas de grand facteur premier. Introduisons quelques notations.

$P(n)$ est le plus grand diviseur premier de n (par convention, $P(1)=1$);

$$\psi(x,y) := \mathrm{card}\{n : 1 \le n \le x \text{ et } P(n) \le y\};$$

$$\Pi(x,y) := \mathrm{card}\{p : 2 \le p \le x \text{ et } P(p-1) \le y\};$$

$$\pi(x) := \sum_{p \le x} 1, \text{ où } p \text{ désigne un nombre premier générique.}$$

Compte tenu du postulat général affirmant que la décomposition de $p-1$ en facteurs premiers est "normale", il est naturel de conjecturer que

$$\Pi(x,y)/\pi(x) \sim \psi(x,y)/x,$$

ou au moins

$$\Pi(x,y)/\pi(x) \gg \psi(x,y)/x,$$

pour x et y tendant vers l'infini, peut-être pas indépendamment mais en tout cas dans une large zone du secteur $2 \le y \le x$.

Soit $f(x)$ une fonction tendant vers l'infini avec x. Nous noterons $\mathcal{H}(f(x))$ l'hypothèse suivante :

on a $\Pi(x,y) \gg \psi(x,y)/\log x$,

pour $x \ge x_0$ *et* $x \ge y \ge f(x)$,

(x_0 et la constante cachée dans $\gg$ pouvant dépendre de f).

Nous pouvons maintenant énoncer le critère d'Erdös-Pomerance :

LEMME 7 (Pomerance [30], [32]). — *Soit u un réel, $0 < u < 1$, tel que $\mathcal{H}(x^u)$ soit vraie. On a $\theta \ge 1-u$. De plus, pour tout $c < 1-u$, la suite $m_1 < m_2 < \cdots$ des solutions de (7) vérifie*

$$\frac{\log m_{i+1}}{\log m_i} \longrightarrow 1 \quad \textit{quand} \quad i \longrightarrow +\infty.$$

Il est bien connu (voir par exemple [38], théorème III.5.6) que

$$\psi(x,x^u) \gg_u x,$$

pour tout u fixé, $0 < u < 1$, donc $\mathcal{H}(x^u)$ s'écrit

$$\Pi(x, x^u) \gg_u \pi(x).$$

Il est probable que $\mathcal{H}(x^u)$ soit vraie pour tout u, $0 < u < 1$, mais il s'agit d'un problème ouvert extrèmement difficile. Comme on a de toutes façons $N(m) \leq \alpha m \log_2(3m)$, la conjecture d'Erdös ($\theta = 1$) semble très plausible.

Démontrons le lemme 7. Soit donc u tel que $0 < u < 1$ et que $\mathcal{H}(x^u)$ soit vraie, et c tel que $0 < c < 1 - u$. Posons $y = (\log x)^{1/u}$; soit $\varepsilon = \varepsilon(u)$ assez petit et $x_0 = x_0(u)$ assez grand, de sorte que, pour $x \geq x_0$:

$$M := \operatorname{card}\{p : \varepsilon y \leq p \leq y \quad \text{et} \quad P(p-1) \leq y^u\} \geq \varepsilon \frac{y}{\log y},$$

enfin posons $k = \left[\frac{\log x}{\log y}\right] = u\frac{\log x}{\log y} + O(1)$.

Considérons maintenant les entiers n sans facteur carré, ayant k facteurs premiers p, vérifiant tous :

$$\varepsilon y \leq p \leq y \quad \text{et} \quad P(p-1) \leq y^u.$$

Ces entiers n satisfont à $(\varepsilon y)^k \leq n \leq y^k$, donc à

$$x^{1-\eta(x)} \leq n \leq x, \tag{8}$$

où $\eta(x)$ tend vers zéro quand x tend vers l'infini.

Leur nombre total est le coefficient binomial

$$\binom{M}{k} \geq \left(\frac{M}{k}\right)^k = x^{1-u+o(1)},$$

après un petit calcul.

D'autre part, ces entiers n vérifient $P(\varphi(n)) \leq y^u = \log x$ donc le nombre des $\varphi(n)$ est au plus $\psi(x, \log x)$.

Erdös montra en 1963 la relation :

$$\psi(x, \log x) = 4^{(1+o(1))\log x/\log_2 x}$$

(voir [38], théorème III.5.2, pour un résultat plus général dû à de Bruijn). En utilisant simplement l'estimation $\psi(x, \log x) = x^{o(1)}$, le principe des

tiroirs montre qu'il existe un entier m qui s'écrit au moins $x^{1-u+o(1)}$ fois $\varphi(n)$ avec n vérifiant (8). Comme $\varphi(n) = n^{1+o(1)}$, on en déduit l'existence d'une fonction positive $\alpha(x)$ tendant vers zéro quand x tend vers l'infini telle que, pour tout x assez grand, l'intervalle

$$x^{1-\alpha(x)} \leq m \leq x,$$

contienne au moins une solution de (7). Cette dernière assertion n'est qu'une autre formulation du lemme 7.

On a donc ramené la recherche de minorants de θ à celle de nombres réels u aussi petits que possible tels que $\mathcal{H}(x^u)$ soit vraie. Sans entrer trop dans les détails, donnons quelques indications sur cette question.

Tout d'abord, on a $\Pi(x,y) = \Pi(x-1,y,1)$ où

$$\Pi(x,y,a) := \text{card}\{n; 1 \leq n \leq x,\ P(n) \leq y \quad \text{et} \quad an+1 \text{ premier}\},\ a \geq 1.$$

La fonction $\Pi(x,y,a)$ vérifie l'identité de Buchstab suivante :

$$\Pi(x,y,a) - \Pi(x,z,a) = \sum_{z<q\leq y} \Pi\Big(\frac{x}{q}, q, qa\Big),\ \ y < z,$$

où q désigne un nombre premier générique.

Voici maintenant comment Erdös prouve l'existence d'un réel u, $0 < u < 1$, tel que $\mathcal{H}(x^u)$ soit vraie. On a

$$\begin{aligned} \pi(x) - \Pi(x,x^u) &= \sum_{x^u<q\leq x-1} \Pi\Big(\frac{x-1}{q}, q, q\Big) \\ &\leq \sum_{m<x^{1-u}} \sum_{\substack{p\leq x/m \\ mp+1 \text{ premier}}} 1\ . \end{aligned}$$

Le crible de Brun ou de Selberg assure l'existence d'une constante c telle que

$$\sum_{\substack{p\leq y \\ mp+1 \text{ premier}}} 1 \leq (c+o(1))\frac{y}{\log^2 y}\frac{m}{\varphi(m)}$$

où le $o(1)$ est uniforme par rapport à m quand y tend vers l'infini (cf. [15], theorem 3.12, par exemple).

On a donc pour u fixé, $0 < u < 1$,

$$\pi(x) - \Pi(x, x^u) \leq (c + o(1)) \frac{x}{\log^2(x^u)} \sum_{m < x^{1-u}} \frac{1}{\varphi(m)}$$

$$= \left(cc' \frac{1-u}{u^2} + o(1) \right) \frac{x}{\log x},$$

où c' est la constante telle que

$$\sum_{m \leq t} \frac{1}{\varphi(m)} \sim c' \log t \quad \text{quand} \quad t \quad \text{tend vers l'infini.}$$

Il suffit alors de choisir u tel que $cc' \frac{1-u}{u^2} < 1$ pour que $\mathcal{H}(x^u)$ soit vraie. Une légère modification de cet argument a permis à Wooldridge [40] de donner en 1979 la minoration $\theta \geq 3 - 2\sqrt{2} = 0,17157\cdots$.

Dans [30], Pomerance observe d'abord que $\Pi\left(\frac{x-1}{q}, q, q\right) = \pi(x, q, 1)$ si $q > \sqrt{x}$, où

$$\pi(x, k, \ell) := \sum_{\substack{p \leq x \\ p \equiv \ell \bmod k}} 1,$$

donc

$$\pi(x) - \Pi(x, \sqrt{x}) = \sum_{\sqrt{x} < q \leq x} \pi(x, q, 1).$$

Il majore ensuite cette somme à l'aide d'un résultat de Goldfeld [14] (conséquence du théorème de Bombieri-Vinogradov) et d'un résultat de Hooley [17] (amélioration en moyenne du théorème de Brun-Titchmarsh). Il obtient ainsi

$$\Pi(x, \sqrt{x}) \geq (1 - 4\log(5/4) + o(1)) x / \log x.$$

En particulier, $\mathcal{H}(\sqrt{x})$ est vraie et $\theta \geq \frac{1}{2}$, mais on peut aller plus loin. Comme on a dans tous les cas,

$$\Pi\left(\frac{x-1}{q}, q, q\right) \leq \pi(x, q, 1),$$

il vient pour $u < \frac{1}{2}$:

$$\Pi(x, \sqrt{x}) - \Pi(x, x^u) \leq \sum_{x^u < q \leq \sqrt{x}} \pi(x, q, 1).$$

On peut de nouveau utiliser le théorème de Bombieri-Vinogradov (pour $x^u < q \leq \sqrt{x}(\log x)^{-B}$) et le théorème de Brun-Titchmarsh (pour $\sqrt{x}(\log x)^{-B} < q \leq \sqrt{x}$) pour trouver une valeur de $u < \frac{1}{2}$ telle que $\mathcal{H}(x^u)$ soit vraie :

THÉORÈME 5 (Pomerance [30]). — *Si* $c < 1 - 625/512e = 0,55092\cdots$, *on a* $N(m) > m^c$ *pour une infinité de valeurs entières de* m.

Remarquons que le même raisonnement montre que l'ensemble des réels u, $0 < u < 1$, tels que $\mathcal{H}(x^u)$ soit vraie, est un intervalle ouvert $]u_0, 1[$. En particulier, on peut prendre $c \leq 1 - u$ dans le lemme 7.

Le meilleur résultat actuellement connu est dû à Friedlander [13]. En modifiant une méthode de Balog et en utilisant des travaux récents de lui-même, Bombieri et Iwaniec, il a démontré que $\theta \geq 1 - (2\sqrt{e})^{-1} = 0,69673\cdots$.

Pomerance a d'autre part démontré le

THÉORÈME 6 (Pomerance [30]). — *On a*

$$N(m) \leq m \ \exp(-(1+o(1))\log m \cdot \log_3 m/\log_2 m). \tag{9}$$

De plus, si $\mathcal{H}(\exp\sqrt{\log x})$ *est vraie, on a l'égalité pour une infinité d'entiers* m.

On ramène en fait la majoration de $N(m)$ à un problème de crible : si $\varphi(n) = m$, on a :

$$n \leq \alpha m \ \log_2(3m) =: x \quad \text{et} \quad (p|n) \Longrightarrow (p-1|m). \tag{10}$$

On majore donc $N(m)$ par le nombre X des entiers positifs n vérifiant (10). En supposant n sans facteur carré (restriction de peu d'importance), Erdös a obtenu un tel résultat dans [8]. Pomerance [32] montra comment utiliser la méthode de Rankin pour majorer X : pour $\sigma \geq \frac{1}{2} + \varepsilon$, $\varepsilon > 0$, on a

$$\begin{aligned} X \leq x^\sigma \sum_{(p|n)\Longrightarrow(p-1|m)} n^{-\sigma} &= x^\sigma \prod_{p-1|m} (1-p^{-\sigma})^{-1} \\ &\ll_\varepsilon x^\sigma \ \exp \sum_{p-1|m} p^{-\sigma} \\ &\leq x^\sigma \ \exp \sum_{d|m} d^{-\sigma} \\ &< x^\sigma \ \exp \prod_{p|m} (1-p^{-\sigma})^{-1} \\ &< x^\sigma \ \exp \ \exp\Big(\sum_{p|m} p^{-\sigma} + O_\varepsilon(1)\Big). \end{aligned}$$

Or $\sum_{p|m} p^{-\sigma} \leq \sum_{k=1}^{\omega(m)} p_k^{-\sigma}$, où p_k désigne le k-ième nombre premier et $p_{\omega(m)} \leq \frac{3}{2}\omega(m)\log\omega(m) \leq 2\log m \leq 2\log x =: y$ pour m assez grand, donc

$$\sum_{p|m} p^{-\sigma} \leq \sum_{p\leq y} p^{-\sigma}.$$

Cette dernière somme est évaluée facilement à l'aide du théorème des nombres premiers et d'une sommation partielle :

$$\sum_{p\leq y} p^{-\sigma} = \ell i(y^{1-\sigma})\Big(1 + O\Big(\frac{1}{\log y}\Big)\Big) + O(|\log(1-\sigma)|),$$

pour $y^{1-\sigma} \geq 2$.

En prenant $\sigma = 1 - \log_3 x/\log_2 x$, on vérifie que cela est

$$\ll \log_2 x/\log_3 x,$$

d'où

$$X \leq x\exp\Big(-\frac{\log x\cdot\log_2 x}{\log_3 x} + (\log x)^{o(1)}\Big),$$

ce qui entraîne (9).

Quant à la deuxième assertion du théorème 6, nous laissons sa démonstration au lecteur. Il suffit de suivre le schéma de démonstration du lemme 7. On prend cette fois $y = \exp((\log_2 x)^2)$,

$$M := \mathrm{card}\{p : p \leq y \quad \text{et} \quad P(p-1) \leq \exp\sqrt{\log y} = \log x\},$$

et on utilise les estimations suivantes :

$$\psi(x, \exp\sqrt{\log x}) = x\ \exp\Big(-\Big(\frac{1}{2} + o(1)\Big)\sqrt{\log x}\cdot\log_2 x\Big)$$

([32], theorem 2.1), et

$$\psi(x, \log x) = \exp(O(\log x/\log_2 x)), \quad ([38], \text{théorème III.5.2}).$$

CONJECTURE C. — *On a*

$$\max_{m\le x} N(m) = x \ \exp(-(1+o(1))\log x\cdot \log_3 x/\log_2 x).$$

Ce problème a évidemment un lien avec l'étude de la moyenne de $N(m)$. Ce dernier problème, dit d'Erdös-Bateman, a suscité de nombreuses recherches, récapitulées dans [36] et [37]. Donnons le meilleur résultat connu, dû à Bateman [2] (1972, voir aussi [1]) :

$$R(x) := \sum_{m\le x} N(m) - \frac{\zeta(2)\zeta(3)}{\zeta(6)}x = O_\varepsilon\Big(x\exp -\sqrt{\Big(\frac{1}{2}-\varepsilon\Big)\log x\cdot\log_2 x}\Big)$$

pour tout $\varepsilon > 0$.

Observons que $\max(|R(m)|, |R(m-0)|) \ge \frac{1}{2}N(m)$. On a donc $R(x) = \Omega(x^c)$ pour tout $c < \theta$ et la conjecture C entraînerait que $R(x) = \Omega(x\ \exp(-(1+o(1))\log x\cdot\log_3 x/\log_2 x)$.

4°) **La loi de Gauss pour le nombre de facteurs premiers de $\varphi(n)$.**

Soit donc $\omega(n) := \sum_{p|n} 1$ et $\Omega(n) := \sum_{p^\alpha \| n} \alpha$ respectivement le nombre de diviseurs premiers et le nombre total de facteurs premiers de l'entier positif n. En 1985, Erdös et Pomerance [12] mirent en évidence une loi de Gauss pour $\omega(\varphi(n))$ et $\Omega(\varphi(n))$.

THÉORÈME 7. — *Pour tout nombre réel u, on a*

$$\lim_{x\to+\infty}\frac{1}{x}\operatorname{card}\{n : 1\le n\le x,$$

$$\Omega(\varphi(n)) - \frac{1}{2}(\log_2 x)^2 \le \frac{u}{\sqrt{3}}(\log_2 x)^{3/2}\} = G(u),$$

où $G(u) = \frac{1}{\sqrt{2\pi}}\int_{-\infty}^{u} e^{-t^2/2}dt$. Le même résultat est vrai si l'on remplace Ω par ω.

Voici les principales étapes de la démonstration. On approche la fonction additive $\Omega(\varphi(n))$ par $f(n) = \sum_{p|n}\Omega(p-1)$, fonction fortement additive à laquelle on peut appliquer le

THEOREME de KUBILIUS et SHAPIRO ([5], theorem 12.2). — *Soit $f(n)$ une fonction fortement additive à valeurs réelles. Pour $x > 0$, posons :*

$$A(x) = \sum_{p \leq x} f(p)p^{-1},$$

$$B(x) = \Big(\sum_{p \leq x} f(p)^2 p^{-1}\Big)^{1/2}.$$

Supposons que la condition de Feller-Lindeberg soit vérifiée :

$$\text{pour tout } \varepsilon > 0,\ B(x)^{-2} \sum_{\substack{p \leq x \\ |f(p)| \geq \varepsilon B(x)}} f(p)^2 p^{-1} \longrightarrow 0, \quad (x \longrightarrow +\infty).$$

Alors on a pour tout nombre réel u :

$$\frac{1}{x}\,\mathrm{card}\{n : 1 \leq n \leq x,\ f(n) - A(x) \leq uB(x)\} \longrightarrow G(u), \quad (x \longrightarrow +\infty).$$

On est donc conduit à estimer les quantités

$$A(x) = \sum_{p \leq x} \Omega(p-1)/p$$

$$\text{et} \quad B(x)^2 = \sum_{p \leq x} \Omega(p-1)^2/p$$

Erdös et Pomerance donnent alors un résultat plus général :

LEMME 8. — *Posons $\Omega_y(n) = \sum_{\substack{p^\alpha \| n \\ p \leq y}} \alpha$. On a uniformément pour $3 \leq y \leq x$*

$$\sum_{p \leq x} \Omega_y(p-1) = \frac{x \log_2 y}{\log x} + O\Big(\frac{x}{\log x}\Big),$$

$$\sum_{p \leq x} \Omega_y(p-1)^2 = \frac{x(\log_2 y)^2}{\log x} + O\Big(\frac{x \log_2 y}{\log x}\Big).$$

Ces sommes s'évaluent par inversion de sommations et font donc intervenir la répartition des nombres premiers dans certaines progressions arithmétiques : on utilise notamment les théorèmes de Bombieri-Vinogradov et Brun-Titchmarsh. La deuxième somme est la plus difficile à estimer; une erreur observée par Smati se trouve d'ailleurs dans la

démonstration de [12] (voir [9] pour une démonstration correcte). Bien entendu, on obtient par sommation partielle :

$$\begin{aligned} A(x) &= \tfrac{1}{2}(\log_2 x)^2 + O(\log_2 x) \\ \text{et} \quad B(x)^2 &= \tfrac{1}{3}(\log_2 x)^3 + O((\log_2 x)^2). \end{aligned}$$

Pour vérifier la condition de Feller-Lindeberg, Erdös et Pomerance majorent $\sum_{\substack{p\le x\\ \Omega(p-1)>T}} \Omega(p-1)^2 p^{-1}$ par $\sum_{\substack{n\le x\\ \Omega(n)>T}} \Omega(n)^2 n^{-1}$ et utilisent un résultat d'Erdös et Sárközy sur la loi locale de $\Omega(n)$. Cela donne :

$$\sum_{\substack{p\le x\\ \Omega(p-1)>T}} \Omega(p-1)^2 p^{-1} \ll 2^{-T} T^4 (\log x)^4. \tag{11}$$

On peut en fait supprimer le facteur T^4 en utilisant un théorème de Nicolas [24] ; il est probable que l'on puisse également remplacer $(\log x)^4$ par $(\log x)^3$.

Pour passer de $f(n)$ à $\Omega(\varphi(n))$, on remarque que

$$\Omega(\varphi(n)) = f(n) + \Omega(n) - \omega(n),$$

et que le nombre des entiers $n \le x$ tels que $\Omega(n) - \omega(n) \ge k$ est $o(x)$ dès que k tend vers l'infini, d'après l'inégalité de Turan-Kubilius (par exemple).

Il est plus délicat de passer de $\Omega(\varphi(n))$ à $\omega(\varphi(n))$. Cette dernière fonction de n n'est plus additive mais on a, d'une part :

$$\Omega(\varphi(n)) - \Omega_y(\varphi(n)) = \omega(\varphi(n)) - \omega_y(\varphi(n))$$

pour $x(1 + o(1))$ nombres entiers $n \le x$, où

$$y = (\log_2 x)^2 \quad \text{et} \quad \omega_y(m) = \sum_{\substack{p\mid m\\ p\le y}} 1$$

(il suffit de compter les entiers $n \le x$ tels que $p^2 | \varphi(n)$ avec $p > y$). D'autre part,

$$0 \le \Omega_y(\varphi(n)) - \omega_y(\varphi(n)) \le \Omega_y(\varphi(n)) \le 2 \log_2 x \log_4 x$$

pour $x(1 + o(1))$ nombres entiers $n \le x$, d'après l'inégalité de Turan-Kubilius et le lemme 8.

Erdös et Pomerance observent aussi que la loi de Gauss est vérifiée par $\Omega(\lambda(n))$ et $\omega(\lambda(n))$, où λ est la fonction de Carmichael, et conjecturent la même répartition Gaussienne pour $\Omega(\ell_a(n))$ et $\omega(\ell_a(n))$, n décrivant l'ensemble des nombres entiers premiers à a, et $\ell_a(n)$ désignant le plus petit entier positif k tel que $a^k \equiv 1 \mod n$ (on a $\ell_a(n)|\lambda(n)|\varphi(n)$).

Pour estimer la vitesse de convergence vers la loi de Gauss dans le théorème 7, on peut utiliser le résultat général suivant, dû à Elliott ([5], theorem 20.5) :

LEMME 9. — *Soit $f(n)$ une fonction arithmétique additive à valeurs réelles, $\beta(x)$ une fonction positive pour $x \geq 3$ et*

$$\alpha(x) = \sum_{\substack{p^k \leq x \\ |f(p^k)| \leq \beta(x)}} \frac{f(p^k)}{p^k}\Big(1 - \frac{1}{p}\Big).$$

Alors on a uniformément pour z réel et $x \geq 3$:

$$x^{-1}\,\mathrm{card}\{n : 1 \leq n \leq x \quad et \quad f(n) - \alpha(x) \leq z\beta(x)\} = G(z) + O(\inf_{\varepsilon > 0} \Delta(\varepsilon)),$$

où

$$\Delta(\varepsilon) = \varepsilon + \sum_{\substack{p \leq x \\ |f(p)| > \varepsilon\beta(x)}} \frac{1}{p} + \left| 1 - \frac{1}{\beta(x)^2} \sum_{\substack{p \leq x \\ |f(p)| \leq \varepsilon\beta(x)}} f(p)^2 p^{-1} \right| +$$

$$+ \frac{1}{\beta(x)^2} \sum_{\substack{p^k \leq x, k \geq 2 \\ \varepsilon\beta(x) < |f(p^k)| \leq \beta(x)}} f(p^k)^2 p^{-k} + \sum_{\substack{p^k \leq x \\ |f(p^k)| > \beta(x)}} p^{-k}.$$

Ici nous prenons $f(n) = \Omega(\varphi(n))$, $\beta(x) = \frac{1}{\sqrt{3}}(\log_2 x)^{3/2}$. Une application répétée d'analogues de (11) montre que

$$\Delta(\varepsilon) \ll \varepsilon + 2^{-T}\frac{(\log x)^4}{(\log_2 x)^3} + \frac{1}{\log_2 x}, \quad \text{où } T = \varepsilon\beta(x).$$

En prenant $\varepsilon = 10(\log_2 x)^{-\frac{1}{2}}$ on obtient la

PROPOSITION. — *On a uniformément pour x et u réels, $x \geq 3$:*

$$x^{-1}\,\mathrm{card}\{n : 1 \leq n \leq x \quad et \quad \Omega(\varphi(n)) \leq \tfrac{1}{2}(\log_2 x)^2 + \tfrac{u}{\sqrt{3}}(\log_2 x)^{3/2}\} =$$
$$= G(u) + O((\log_2 x)^{-1/2}).$$

Pour $\omega(\varphi(n))$ on peut suivre le raisonnement d'Erdös et Pomerance comparant cette fonction à $\Omega(\varphi(n))$ et obtenir un terme reste en $O(\log_4 x \cdot (\log_2 x)^{-1/2})$.

Dans un premier temps, nous avions pensé que ce dernier résultat pourrait être amélioré en $O((\log_2 x)^{-\frac{1}{2}})$, comme pour $\Omega(\varphi(n))$. Carl Pomerance nous a convaincu qu'il était plus raisonnable de formuler la

CONJECTURE D. — *On a uniformément pour x et u réels, $x \geq 3$:*

$$x^{-1}\,\mathrm{card}\{n : 1 \leq n \leq x \text{ et } \omega(\varphi(n)) \leq \frac{1}{2}(\log_2 x)^2 + \frac{u}{\sqrt{3}}(\log_2 x)^{3/2}\} =$$
$$= G(u) + \sqrt{\frac{3}{2\pi}}\, e^{-\frac{u^2}{2}} \frac{\log_4 x}{(\log_2 x)^{1/2}} + O((\log_2 x)^{-1/2}).$$

Pour démontrer la conjecture D, il s'agit de montrer que l'ordre normal de $\Omega(\varphi(n)) - \omega(\varphi(n))$ est $\log_2 n \cdot \log_4 n$, avec une convergence suffisamment rapide. Cela résulterait par exemple des formules conjecturales suivantes pour les moments d'ordre 1 et 2 :

$$\sum_{n \leq x} \{\Omega(\varphi(n)) - \omega(\varphi(n))\} = x\ \log_2 x \cdot \log_4 x + O(x(\log_2 x)^{1/2}/\log_4 x)$$

$$\text{et} \quad \sum_{n \leq x} \{\Omega(\varphi(n)) - \omega(\varphi(n))\}^2 = x(\log_2 x \cdot \log_4 x)^2 + O(x(\log_2 x)^{3/2}).$$

Le comportement statistique global de $\Omega(\varphi(n))$ et $\omega(\varphi(n))$ étant élucidé, on peut naturellement s'interroger sur le comportement local. Les conjectures suivantes semblent raisonnables, mais peuvent être difficiles :

CONJECTURE E. — *Soit B un nombre réel positif fixé. On a uniformément pour x tendant vers l'infini et $|k - \frac{1}{2}(\log_2 x)^2| \leq B(\log_2 x)^{3/2}$:*

$$x^{-1}\,\mathrm{card}\{n : 1 \leq n \leq x \quad et \quad \Omega(\varphi(n)) = k\} \quad \sim$$
$$\sim \quad x^{-1}\,\mathrm{card}\{n : 1 \leq n \leq x \quad et \quad \omega(\varphi(n)) = k\} \quad \sim \sqrt{\tfrac{3}{2\pi}} \tfrac{e^{-t^2/2}}{(\log_2 x)^{3/2}},$$

où $t = \frac{k - \frac{1}{2}(\log_2 x)^2}{(\log_2 x)^{3/2}/\sqrt{3}}$.

CONJECTURE F. — *On a uniformément pour $x \geq 3$ et k entier positif :*

$$\mathrm{card}\{n : 1 \leq n \leq x \quad et \quad \Omega(\varphi(n)) = k\} \ll x(\log_2 x)^{-3/2},$$

et la même chose pour $\omega(\varphi(n))$.

5°) L'évaluation du nombre de valeurs distinctes de la fonction d'Euler inférieures à une limite donnée.

Il s'agit ici d'étudier

$$V(x) := \mathrm{card}\{m : 1 \leq m \leq x \quad et \quad N(m) > 0\}.$$

$V(x)$ est donc le nombre de nombres entiers positifs inférieurs ou égaux à x qui sont des valeurs de la fonction d'Euler.

Jusqu'à présent, la recherche s'est concentrée sur la détermination du comportement asymptotique de $\log V(x)$ (cf. [25], [7], [10], [11], [31], [22]).

Le meilleur résultat connu est le

THÉORÈME 8 (Maier-Pomerance 1988 [22]). — *Soit c_0 l'unique nombre réel vérifiant $0 < c_0 < 1$ et $\sum_{n=1}^{+\infty}((n+1)\log(n+1) - n\ \log n - 1)c_0^n = 1$; soit $c = \frac{1}{2|\log c_0|} = 0,8178\cdots$. On a :*

$$V(x) = \frac{x}{\log x} \exp\{(c + o(1))(\log_3 x)^2\}.$$

Observons que l'équation définissant c_0 s'écrit aussi

$$\int_0^{+\infty} c_0^{[t]} \log t \ dt = 1.$$

La démonstration du théorème 8 est d'une grande sophistication et constitue à notre avis l'un des chefs-d'œuvre de la théorie combinatoire des nombres. Avant d'en donner un aperçu plus que sommaire, nous allons introduire quelques idées et considérations simples permettant au lecteur de se familiariser avec le problème.

Tout d'abord, l'équivalence $\log V(x) \sim \log x$ est triviale puisque

$$\pi(x) \leq V(x) \leq x.$$

Pour montrer que $\log V(x) = \log x - \log_2 x + o(\log_2 x)$, il s'agit donc de voir que

$$V(x) \ll_c \frac{x}{(\log x)^c} \tag{12}$$

pour tout $c < 1$.

Un argument simple de Pillai ([25]) permet de montrer (12) pour tout $c < \lambda_0 \log 2$, où λ_0 est la solution de

$$\lambda_0 \log 2 = \lambda_0 \log \lambda_0 - \lambda_0 + 1, \quad 0 < \lambda_0 < 1 :$$

si $m = \varphi(n)$ est compté dans $V(x)$ et $2^k \nmid m$, alors forcément $\omega(n) \leq k$. Par conséquent,

$$V(x) \leq \frac{x}{2^k} + \sum_{\substack{n \leq \alpha x \log_2(3x) \\ \omega(n) \leq k}} 1.$$

Si l'on suppose $k \leq (1-\varepsilon)\log_2 x$, l'inégalité de Hardy-Ramanujan et la formule de Stirling prouvent que

$$\sum_{\substack{n \leq \alpha x \log_2 x \\ \omega(n) \leq k}} 1 \ll_\varepsilon \frac{x \log_2 x}{(\log x)^{Q(\lambda)}},$$

où $Q(\lambda) = \lambda \log \lambda - \lambda + 1$ et $\lambda = \frac{k}{\log_2 x}$. Le choix $k = \lfloor \lambda_0 \log_2 x \rfloor$ donne la majoration de Pillai.

L'idée fondamentale, essentielle pour tous les développements ultérieurs, est dûe à Erdös [7]. Condensons-là par un aphorisme :

si la décomposition de n en produit de facteurs premiers est normale, celle de $\varphi(n)$ est anormale.

Citons d'emblée un détail technique important : on va découper $V(x)$ en morceaux du type $\operatorname{card}\{m; m \in A \text{ et } m = \varphi(n) \text{ où } n \in B\}$ et on majorera ce cardinal par $\operatorname{card} A$ ou $\operatorname{card} B$ suivant les cas.

On a :

$$V(x) = \operatorname{card}\{m : 1 \leq m \leq x \quad et \quad m = \varphi(n), \quad \text{où} \quad n \leq \alpha x \log_2(3x)\}$$

L'idée d'Erdös est d'écrire :

$V(x) \leq V_1(x) + V_2(x) + V_3(x)$, avec

$$V_1(x) = \mathrm{card}\{m : 1 \leq m \leq x \text{ et } m = \varphi(n) \text{ où } \omega(n) \leq \lambda \log_2 x\},$$
$$V_2(x) = \mathrm{card}\{m : 1 \leq m \leq x \text{ et } m = \varphi(n) \text{ où } \omega(n, E_1) \geq \tfrac{1}{2}\lambda \log_2 x\},$$
$$V_3(x) = \mathrm{card}\{m : 1 \leq m \leq x \text{ et } m = \varphi(n) \text{ où } \omega(n, E_2) \geq \tfrac{1}{2}\lambda \log_2 x\},$$

où $\omega(n, E) = \sum_{\substack{p \mid n \\ p \in E}} 1$ si E est un ensemble de nombres premiers, $E_1 = \{p; \omega(p-1) \leq \frac{40}{\lambda} + 1\}$ et $E_2 = \{p; \omega(p-1) > \frac{40}{\lambda} + 1\}$; λ est ici un paramètre positif fixé ultérieurement.

On utilise alors des renseignements sur la distribution des valeurs des fonctions "nombres de facteurs premiers", obtenus par la méthode inductive de Hardy et Ramanujan et une majoration de crible, par exemple :

$$\mathrm{card}\{n : 1 \leq n \leq x \text{ et } \omega(n, E) = k\} \ll x e^{-E(x)} \left(\frac{(E(x) + O(1))^k}{k!} \right)$$

où $E(x) := \sum_{\substack{p \leq x \\ p \in E}} 1/p$, et

$$\mathrm{card}\{p : 2 \leq p \leq x \quad \text{et} \quad \omega(p-1) = k\} \ll \frac{\pi(x)}{\log x} \frac{(\log_2 x + O(1))^{k-1}}{(k-1)!}.$$

En utilisant ce type de majoration, on voit que

$$V_1(x) \ll \tfrac{x}{(\log x)^{1-\varepsilon}} \quad \text{si } \lambda = \lambda(\varepsilon) \text{ est assez petit ;}$$
$$V_2(x) = o\left(\tfrac{x}{\log x}\right) \quad \text{car } E_1 \text{ est petit } \left(\sum_{p \in E_1} \frac{1}{p} < +\infty \right).$$

Enfin, si m est compté dans $V_3(x)$, on a

$$\Omega(m) = \Omega(\varphi(n)) > \frac{40}{\lambda} \cdot \frac{1}{2} \lambda \log_2 x = 20 \log_2 x$$

et le résultat de Nicolas [24], ou même celui de Hardy-Ramanujan :

$$\mathrm{card}\{m : 1 \leq m \leq x \quad \text{et} \quad \Omega(m) \geq k\} \ll (10/9)^{-k} x \log x,$$

permet de voir que $V_3(x) = o(x/\log x)$.

Retenons d'ores et déjà que l'essentiel de $V(x)$ vient de $V_1(x)$, donc d'entiers n ayant peu de facteurs premiers. En fait il s'avèrera que les entiers n fournissant le plus gros contingent de valeurs de $\varphi(n)$ ont un nombre de facteurs premiers de l'ordre de $\log_3 x$.

En 1973, Erdös et Hall [10] reprennent une variante de ce découpage et prouvent que

$$V(x) \ll \frac{x}{\log x} \exp(B\sqrt{\log_2 x}) \quad \text{pour tout } B > 2\sqrt{2/\log 2}.$$

En 1976, ces mêmes auteurs démontrent la minoration suivante [11] :

$$V(x) \gg \frac{x}{\log x} \exp(C(\log_3 x)^2) \quad \text{pour tout } C < 1/\log 16.$$

En 1986, Pomerance [31] obtient une majoration du même aspect :

$$V(x) \ll \frac{x}{\log x} \exp(C'(\log_3 x)^2) \quad \text{pour tout } C' > (2 - 2\log(e-1))^{-1}.$$

Observons qu'on peut se contenter ici d'étudier les entiers sans facteur carré. Soit en effet $V^*(x)$ le nombre de valeurs distinctes de $\varphi(n)$ pour n sans facteur carré. De l'encadrement :

$$V^*(x) \le V(x) \le \sum_t V^*(x/\varphi(t^2)),$$

il résulte que toute majoration ou minoration de $V^*(x)$ par une quantité du type $\frac{x}{\log x} \exp(A(x) + O(B(x)))$ où $A(x)$ et $B(x)$ sont positives et croissantes se transmet aussitôt à $V(x)$. Compte tenu des connaissances actuelles on peut donc étudier $V^*(x)$ au lieu de $V(x)$. Bien entendu, cela empêche d'aborder des questions plus fines comme celle d'Erdös et Hall : a-t-on $\lim\limits_{x\to+\infty} \frac{V(2x)}{V(x)} = 2$?

Dans [31], Pomerance introduit une importante idée nouvelle. Il s'intéresse aux k plus grands facteurs premiers de n :

$$P_1 > P_2 > \cdots > P_k,$$

et compare la décroissance de leur logarithme itéré (qui est normalement proche du nombre de facteurs premiers de leur image par φ) à une suite géométrique translatée $\beta^{i-1}\log_2 x - \log_3 x$, $i = 1, \ldots, k$. Si on a

$$\log_2 P_i > \beta^{i-1}\log_2 x - \log_3 x \quad \text{pour } i = 1, \ldots, k, \tag{13}$$

et si β et k sont assez grands, alors $\varphi(n)$ aura beaucoup de facteurs premiers et se trouvera donc dans un ensemble de petit cardinal.

Tout revient donc à majorer le nombre de $\varphi(n)$ distincts, inférieurs à x, avec n sans facteur carré vérifiant

$$\log_2 P_i \leq \beta^{i-1} \log_2 x - \log_3 x$$

pour au moins un i, $1 \leq i \leq k$, et ce problème se prête à une méthode itérative assez simple. Dans l'article [22] de Maier et Pomerance, on retrouve cette idée mais on observe cette fois que, sous la condition (13), $\varphi(n)$ aura aussi un nombre anormal de facteurs premiers appartenant à certains sous-intervalles de $[1, x]$ et cela permet de baisser la valeur de β.

En ce qui concerne la minoration, nous allons apercevoir quelques idées importantes en essayant de minorer

$$A(x) := \text{card}\{m : 1 \leq m \leq x \quad \text{et } m = (p-1)(q-1) \quad \text{où } 2 < p < q\}.$$

C'est le cardinal de la réunion des $\mathcal{A}(x,p)$, $2 < p \leq \sqrt{x} + 1$, où

$$\mathcal{A}(x,p) = \{m : 1 \leq m \leq x \quad \text{et } m = (p-1)(q-1),\ q > p\},$$

p étant ici fixé.

Notons $A(x,p) = \text{card}\,\mathcal{A}(x,p)$ et

$$B(x,p_1,p_2) = \text{card}\{m : 1 \leq m \leq x$$

$$\text{et } m = (p_1-1)(q-1) = (p_2-1)(q'-1), \quad \text{où } p_1 < q \text{ et } p_2 < q'\}.$$

On a évidemment

$$A(x) \geq \sum_{2<p\leq y} A(x,p) - \sum_{2<p_1<p_2\leq y} B(x,p_1,p_2), \quad \text{pour } 3 \leq y \leq x^{1/3}$$

(inégalité de Bonferroni).

Pour majorer $B(x,p_1,p_2)$ on fait appel à un lemme de crible, déductible par exemple du théorème 4.2 de [33].

LEMME 10. — *Soit $a \neq b$ deux nombres entiers positifs et $u = pgcd(a,b)$. Si $x > abu^{-2}$, le nombre de couples (q,q') de nombres premiers tels que $a(q-1) = b(q'-1) \leq x$ est*

$$\ll \frac{x/u}{\varphi(a/u)\varphi(b/u)\log^2(xu^2/ab)} \prod_{p \mid \frac{a-b}{u}} \left(1-\frac{1}{p}\right)^{-1}$$

Le lemme s'applique immédiatement et donne

$$B(x,p_1,p_2) \ll \frac{(p_1-1,p_2-1)}{(p_1-1)(p_2-1)} \frac{x}{\log^2 x} (\log_2 x)^3$$

uniformément pour $2 < p_1 < p_2 \leq x^{1/3}$.

Comme $A(x,p) \gg \frac{x}{p \log x}$ pour $p \leq x^{1/3}$, on en déduit :

$$A(x) \geq C_1 \frac{x}{\log x} \log_2 y -$$

$$C_2 \frac{x}{\log^2 x} (\log_2 x)^3 \sum_{2<p_1<p_2\leq y} (p_1-1,p_2-1)/(p_1-1)(p_2-1).$$

Cette dernière somme est majorée par :

$$\sum_{d \leq y} d\Big(\sum_{\substack{p \equiv 1 \bmod d \\ p \leq y}} (p-1)^{-1} \Big)^2 \ll \log^3 y.$$

Si l'on choisit $\log y = (\log x)^{1/4}$ par exemple, on obtient :

$$A(x) \gg \frac{x}{\log x} \log_2 x.$$

Tout le travail consiste ensuite à généraliser cet argument à $V_k(x) = \text{card}\{m : 1 \leq m \leq x \text{ et } m = (p_1-1)\cdots(p_k-1) \text{ où } p_1 < \cdots < p_k\}$, par induction sur k, puis à choisir k optimalement. Erdös et Hall montrent très simplement (en utilisant l'inégalité de Cauchy-Schwarz au lieu de celle de Bonferroni) que

$$V_k(x) \gg \frac{x}{\log x} \frac{(c \log_2 x)^{k-1}}{(k-1)!} 2^{-k^2}$$

et en déduisent facilement leur minoration.

Pour le théorème 8, Maier et Pomerance ramènent le problème à majorer par récurrence sur k le nombre de solutions en $2k+2$ nombres premiers $p_0, \dots, p_k$, $q_0, \dots, q_k$ d'un problème du type

$$\begin{cases} \frac{x}{2} \leq (p_0 - 1) \cdots (p_k - 1) = (q_0 - 1) \cdots (q_k - 1) \leq x \\ p_j \neq q_j, \quad j = 1, \dots, k \\ p_j, q_j \in \mathcal{P}_j, \quad j = 1, \dots, k \end{cases}$$

où $\mathcal{P}_j$ est un ensemble de nombres premiers p tels que $p-1$ ait une décomposition en facteurs premiers "normale" en un certain sens.

BIBLIOGRAPHIE

[1] M. BALAZARD et A. SMATI. — Elementary proof of a theorem of Bateman, *Analytic Number Theory (B.C. Berndt, H.G. Diamond, H. Halberstam, A. Hildebrand ed.), Birkhäuser* , (1990), 41-46.

[2] P.C. BATEMAN. — The distribution of values of the Euler function, *Acta Arith.* **21**, (1972), 329-345.

[3] R.D. CARMICHAEL. — Note on Euler's φ-function, *Bull. A.M.S.* **28**, (1922), 109-110.

[4] G.L. COHEN et P. HAGIS. — On the number of prime factors of n if $\varphi(n)|n-1$, *Nieuw Arch. Wisk., (3)* **28**, (1980), 177-185.

[5] P.D.T.A. ELLIOTT. — *Probabilistic number theory I, II*, Springer-Verlag, New York, 1980.

[6] P. ERDÖS. — On primitive abundant numbers, *J. London Math. Soc.* **10**, (1935), 49-58.

[7] P. ERDÖS. — On the normal number of prime factors of $p-1$ and some other related problems concerning Euler's φ-function, *Quart. J. Math. (Oxford Ser.)* **6**, (1935), 205-213.

[8] P. ERDÖS. — On pseudoprimes and Carmichael numbers, *Pub. Math. Debrecen* **4**, (1956), 201-206.

[9] P. ERDÖS, A. GRANVILLE, C. POMERANCE et C. SPIRO. — On the normal behavior of the iterates of some arithmetic functions, *Analytic Number Theory (B.C. Berndt, H.G. Diamond, H. Halberstam, A. Hildebrand ed.), Birkhäuser* , (1990), 165-204.

[10] P. ERDÖS et R.R. HALL. — On the values of Euler's φ-function, *Acta Arith.* **22**, (1973), 201-206.

[11] P. ERDÖS et R.R. HALL. — Distinct values of Euler's φ-function, *Mathematika* **23**, (1976), 1-3.

[12] P. ERDÖS et C. POMERANCE. — On the normal number of prime factors of $\varphi(n)$, *Rocky Mountain J. of Math.* **15**, (1985), 343-352.

[13] J.B. FRIEDLANDER. — Shifted primes without large prime factors, *NATO Number Theory Conf., (R. Mollin, ed.)* , (Banff 1988), 393-401.

[14] M. GOLDFELD. — On the number of primes p for which $p + a$ has a large prime factor, *Mathematika* **16**, (1969), 23-27.

[15] H. HALBERSTAM et H.E. RICHERT. — *Sieve Methods*, Academic Press., London, 1974.

[16] G.H. HARDY et E.M. WRIGHT. — *Introduction to the theory of numbers, 5^{th} ed.*, The Clarendon Press., Oxford University Press., New York, 1979.

[17] C. HOOLEY. — On the greatest prime factor of $p + a$, *Mathematika* **20**, (1973), 135-143.

[18] V.L. KLEE, Jr. — On a conjecture of Carmichael, *Bull. A.M.S.* **53**, (1947), 1183-1186.

[19] W. KNÖDEL. — Eine obere Schranke für die Anzahl der Carmichaelschen Zahlen kleiner als x, *Arch. Math.* **4**, (1953), 282-284.

[20] D.H. LEHMER. — On Euler's totient function, *Bull. A.M.S.* **38**, (1932), 745-757.

[21] E. LIEUWENS. — Do there exist composite numbers M for which $k\varphi(M) = M - 1$ holds?, *Nieuw Arch. Wisk. (3)* **18**, (1970), 165-169.

[22] H. MAIER et C. POMERANCE. — On the number of distinct values of Euler's φ-function, *Acta Arith.* **49**, (1988), 263-275.

[23] P. MASAI et A. VALETTE. — A lower bound for a counterexample in Carmichael's conjecture, *Boll. Un. Mat. Ital. (6)* **1-A**, (1982), 313-316.

[24] J.-L. NICOLAS. — Sur la distribution des nombres entiers ayant une quantité fixée de facteurs premiers, *Acta Arith.* **44**, (1984), 191-200.

[25] S.S. PILLAI. — On some functions connected with $\varphi(n)$, *Bull. A.M.S.* **35**, (1929), 832-836.

[26] C. POMERANCE. — On the congruences $\sigma(n) \equiv a(\mathrm{mod}\, n)$ and $n \equiv a(\mathrm{mod}\, \varphi(n))$, *Acta Arith.* **26**, (1975), 265-272.

[27] C. POMERANCE. — On composite n for which $\varphi(n)|n-1$, *Acta Arith.* **28**, (1976), 387-389.

[28] C. POMERANCE. — On composite n for which $\varphi(n)|n-1$, II, *Pacif. J. Math.* **69**, (1977), 177-186.

[29] C. POMERANCE. — On Carmichael's conjecture, *Proc. A.M.S.* **43**, (1974), 297-298.

[30] C. POMERANCE. — Popular values of Euler's function, *Mathematika* **27**, (1980), 84-89.

[31] C. POMERANCE. — On the distribution of the values of Euler's function, *Acta Arith.* **47**, (1986), 63-70.

[32] C. POMERANCE. — Two methods in elementary analytic number theory, *NATO Number Theory Conf., (R. Mollin, ed.) Banff*, (1988), 135-161.

[33] K. PRACHAR. — *Primzahlverteilung*, Springer, 1957.

[34] F. SCHUH. — $n-1$ peut-il être divisible par $\varphi(n)$ lorsque n est composé (en néerlandais), *Mathematica, Zutphen, B* **12**, (1944), 102-107.

[35] W. SIERPINSKI. — *Elementary Theory of Numbers*, Warsawa, 1964.

[36] A. SMATI. — *Répartition des valeurs de la fonction d'Euler et de certaines fonctions multiplicatives, Thèse*, Université de Limoges, 1990.

[37] A. SMATI. — Le problème d'Erdös et Bateman sur la fonction d'Euler, à paraître au *Séminaire de Théorie des Nombres de Bordeaux.*

[38] G. TENENBAUM. — *Introduction à la théorie analytique et probabiliste des nombres*, Institut E. Cartan, Nancy, 1990.

[39] D.W. WALL. — Conditions for $\varphi(N)$ to properly divide $N-1$ *in a collection of manuscripts related to the Fibonacci sequence (ed. V.-F. Hagatt et M. Bichnell-Johnson)* 205-208.

[40] K.R. WOOLDRIDGE. — Values taken many times by Euler's phi-function, *Proc. A.M.S.* **76**, (1979), 229-234.

Michel Balazard
CeReMaB
351, Cours de la Libération
33405 TALENCE CEDEX

Abdelhakim Smati
Mathématiques
Faculté des Sciences
123, rue A. Thomas
87060 LIMOGES CEDEX

MÉTHODE DES MOMENTS ET FONCTIONS ADDITIVES

Hubert DELANGE

Il est entendu une fois pour toutes que, dans tout ce qui suit, la lettre p est utilisée pour désigner les nombres premiers, et la lettre n pour désigner les entiers > 0.

1. Le théorème suivant, dû à Erdös et Kac [7], est bien connu :

THÉORÈME. — *Soit f une fonction arithmétique réelle fortement additive. On suppose que*

$$|f(p)| \leq M \text{ pour tout } p \text{ et } \sum \frac{f(p)^2}{p} < \infty.$$

On pose

$$A(x) = \sum_{p \leq x} \frac{f(p)}{p} \text{ et } B(x) = \Big(\sum_{p \leq x} \frac{f(p)^2}{p}\Big)^{\frac{1}{2}}$$

(de sorte que $B(x)$ tend vers $+\infty$ quand x tend vers $+\infty$). Alors, pour tout t réel, quand x tend vers $+\infty$

$$\frac{1}{x}\#\Big\{n \leq x : \frac{f(n) - A(x)}{B(x)} \leq t\Big\} = G(t) + o(1),$$

où $G(t) = (1/\sqrt{2\pi}) \int_{-\infty}^{t} e^{-u^2/2} du$.

Autrement dit, la distribution des nombres $\frac{f(n)-A(x)}{B(x)}$ où $n \leq x$ converge vers la distribution normale de Gauss.

La démonstration originale était basée sur le théorème central limite du calcul des probabilités et un lemme arithmétique obtenu à l'aide du crible de Brun.

Ultérieurement Kac suggéra d'essayer d'établir le théorème en montrant que les moments convergent vers ceux de la distribution normale de Gauss, c'est-à-dire que, pour chaque $q \in \mathbb{N}^*$,

$$\frac{1}{x} \sum_{n \leq x} \Big(\frac{f(n) - A(x)}{B(x)}\Big)^q \text{ tend vers } \mu_q = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{+\infty} u^q e^{-u^2/2} du,$$

ce qui équivaut à

$$(1) \qquad \sum_{n\le x}(f(n)-A(x))^q = \mu_q x B(x)^q + o(xB(x)^q).$$

Ceci a été réalisé en 1955 par H. Halberstam [8]. Sa démonstration comportait des calculs compliqués. Je l'ai simplifiée d'abord dans [1] et [2], puis dans des cours à Orsay et à Urbana. Sous sa forme définitive, la démonstration est basée sur le lemme suivant, démontré dans [4] :

LEMME 1. — *Soit E un ensemble fini non vide de nombres premiers, et soit f une fonction fortement additive satisfaisant à*

$$f(p) = 0 \text{ pour } p \notin E.$$

On pose $A = \sum_{p\in E} \frac{f(p)}{p}$ *et*

$$\Phi(z) = \prod_{p\in E}\Big(1+\frac{e^{zf(p)}-1}{p}\Big)\exp\Big(-\frac{zf(p)}{p}\Big) = \sum_{q=0}^{\infty} a_q z^q.$$

On a pour tout $q \in \mathbb{N}^*$

$$\left|\sum_{n\le x}(f(n)-A)^q - q!a_q x\right| \le \Big(\frac{3}{2}\Big)^q\Big(\sum_{p\in E}|f(p)|\Big)^q.$$

Pour démontrer (1) on applique ce lemme à la fonction "tronquée" $f_y(n) = \sum_{\substack{p\mid n\\ p\le y}} f(p)$, où $y \ge 2$, l'ensemble E étant l'ensemble des nombres premiers $\le y$.

N étant un entier > 0 arbitraire, en prenant $y = x^{1/2N}$ on montre que, pour $q \le 2N$,

$$\sum_{n\le x}(f_y(n)-A(y))^q = \mu_q x B(y)^q + o(xB(y)^q).$$

On en déduit que (1) a lieu pour $q \le N$.

2. Le théorème d'Erdös et Kac a été généralisé par Shapiro (voir [6], chapitre 12, th. 12.2).

Au lieu de $|f(p)| \leq M$, Shapiro suppose que, pour tout $\varepsilon > 0$,

$$\sum_{\substack{p \leq x \\ |f(p)| > \varepsilon B(x)}} \frac{f(p)^2}{p} = o(B(x)^2). \quad (x \longrightarrow \infty).$$

Ici les moments de la distribution considérée ne convergent pas forcément quand x tend vers l'infini. Un exemple en est donné dans [5].

On peut cependant encore démontrer le théorème de Shapiro par la méthode des moments. On utilise pour cela un nouveau lemme (démontré encore dans [4]).

LEMME 2. — *Soit f une fonction fortement additive et soit, pour $y \geq 2$,*

$$f_y(n) = \sum_{\substack{p|n \\ p \leq y}} f(p).$$

On a pour $q \in \mathbb{N}^*$ et $x > y$

$$\sum_{n \leq x} |f(n) - f_y(n)|^q \leq x \Big(\frac{\log x}{\log y}\Big)^{q-1} \sum_{y < p \leq x} \frac{|f(p)|^q}{p}.$$

La fonction f satisfaisant aux hypothèses du théorème de Shapiro, soit g_x la fonction définie par

$$g_x(n) = \sum_{\substack{p|n \\ |f(p)| \leq B(x)}} f(p).$$

En utilisant les lemmes 1 et 2 on prouve que, pour chaque q,

$$\sum_{n \leq x} (g_x(n) - A(x))^q = \mu_q x B(x)^q + o(xB(x)^q),$$

d'où il résulte que, quand x tend vers l'infini, la distribution des nombres $\frac{g_x(n) - A(x)}{B(x)}$ où $n \leq x$ converge vers la distribution normale de Gauss.

Par suite sa fonction caractéristique, égale à

$$\frac{1}{[x]} \sum_{n \leq x} \exp\Big(it \frac{g_x(n) - A(x)}{B(x)}\Big),$$

tend vers celle de la distribution de Gauss, c'est-à-dire $e^{-t^2/2}$.

Mais on voit facilement que la différence entre cette fonction caractéristique et celle de la distribution des nombres $\frac{f(n)-A(x)}{B(x)}$ où $n \leq x$ tend vers zéro.

3. Notons qu'on a utilisé ici le fait que, si les moments d'une distribution convergent vers ceux de la distribution de Gauss, cette distribution converge vers celle de Gauss, fait établi par Chebichev à une époque où on n'avait pas encore introduit les fonctions caractéristiques.

La méthode peut s'appliquer à d'autres distributions que celle de Gauss, en utilisant le lemme suivant qui permet de passer des moments à la fonction caractéristique.

LEMME 3. — *Soit G une fonction réelle définie sur*

$$\{(n,x) : x \geq x_0 \quad et \quad n \leq x\} \ (x_0 \geq 1).$$

On suppose que

(*a*) *Pour chaque $q \in \mathbb{N}$, quand x tend vers l'infini*

$$\frac{1}{x} \sum_{n \leq x} G(x,n)^q = \alpha_q(x) + o(1) \quad (avec \ \alpha_0(x) = 1);$$

(*b*) *Pour tout $q \in \mathbb{N}$ et tout $x \geq x_0$, $|\alpha_q(x)| \leq c_q$, la série entière $\sum_{q=0}^{\infty} \frac{c_q}{q!} z^q$ ayant un rayon de convergence infini.*

Soit, pour $x \geq x_0$ et z complexe quelconque,

$$\Psi_x(z) = \sum_{q=0}^{\infty} \frac{\alpha_q(x)}{q!} z^q$$

(de sorte que Ψ_x est une fonction entière).

Alors, pour tout t réel, quand x tend vers l'infini,

$$\frac{1}{x} \sum_{n \leq x} \exp(it \ G(n,x)) = \Psi_x(it) + o(1).$$

Ce lemme est démontré dans [4].

La méthode générale pour établir un résultat concernant une fonction additive donnée consistera à introduire une fonction auxiliaire donnant lieu à une distribution dont les moments convergent.

Ou bien cette fonction auxiliaire, dépendant d'un paramètre, donnera lieu à une distribution approchant celle qu'on veut étudier. Ou bien elle donnera lieu à une distribution qui détermine celle qu'on veut étudier.

C'est le premier cas qui a lieu dans la démonstration donnée dans [4] du théorème bien connu de Kubilius sur les fonctions "de classe (H)".

On va voir que, dans le second cas, on peut obtenir des résultats concernant des fonctions additives qui ne sont pas forcément fortement additives.

4. A titre d'exemple, on va démontrer ici le théorème suivant, dû à Erdös (voir [6], chapitre 5, th. 5.2).

THÉORÈME 1. — *Soit f une fonction additive réelle satisfaisant à*

$$\sum_{|f(p)|>1} \frac{1}{p} < \infty \quad et \quad \sum_{|f(p)|\leq 1} \frac{f(p)^2}{p} < \infty.$$

Soit $A(x) = \sum_{\substack{p\leq x \\ |f(p)|\leq 1}} \frac{f(p)}{p}$.

Quand x tend vers l'infini, la distribution des nombres $f(n) - A(x)$ où $n \leq x$ converge vers une distribution limite dont la fonction caractéristique est

$$P(t) = \prod_p (1 + u_p(t)) \exp(-v_p(t)),$$

où

$$u_p(t) = -\frac{1}{p} + \left(1 - \frac{1}{p}\right) \sum_{r=1}^{\infty} \frac{e^{itf(p^r)}}{p^r}$$

et

$$v_p(t) = \begin{cases} it\frac{f(p)}{p} & si \quad |f(p)| \leq 1, \\ 0 & si \quad |f(p)| > 1. \end{cases}$$

4.1. On doit démontrer que l'on a, quand x tend vers l'infini,

$$\frac{1}{x} \sum_{n\leq x} \exp(it(f(n) - A(x))) = P(t) + o(1), \tag{2}$$

et que la fonction P est continue.

On voit qu'il suffit d'établir le résultat suivant :

Soit f^* la fonction fortement additive déterminée par

$$f^*(p) = \begin{cases} f(p) & si \quad p > 2 \quad et \quad |f(p)| \leq 1, \\ 0 & si \quad p = 2 \quad ou \quad |f(p)| > 1. \end{cases}$$

Soit $A^*(x) = \sum_{p \leq x} \frac{f^*(p)}{p}$.

Quand x tend vers l'infini, on a

$$\frac{1}{x} \sum_{n \leq x} \exp(it(f^*(n) - A^*(x))) = P^*(t) + o(1), \tag{3}$$

où

$$P^*(t) = \prod \Big(1 + \frac{e^{itf^*(p)} - 1}{p}\Big) \exp\Big(-it \frac{f^*(p)}{p}\Big),$$

le produit étant uniformément convergent sur tout ensemble compact.

On utilise d'abord le lemme suivant, dont nous donnerons la démonstration en appendice :

LEMME 4. — *Soient g et g^* des fonctions multiplicatives satisfaisant à*

$$|f(n)| \leq 1 \quad et \quad |f^*(n)| \leq 1 \quad pour\ tout\ n.$$

(Précisons ici que, dans la définition de "fonction multiplicative", nous supposons que la fonction est égale à 1 pour $n = 1$).

Soit $G(x) = \frac{1}{x} \sum_{n \leq x} g(n)$ *et* $G^*(x) = \frac{1}{x} \sum_{n \leq x} g^*(n)$.

On suppose que

(a) $\sum \frac{|g(p) - g^*(p)|}{p} < \infty$;

(b) $\sum_{r=0}^{\infty} g(2^r) z^r \neq 0$ *pour* $|z| = \frac{1}{2}$;

(c) *Pour tout* $\lambda > 1$, $G^*(\lambda x) - G^*(x) = o(1)$ *quand x tend vers l'infini.*

Alors, quand x tend vers l'infini,

$$G(x) = G^*(x) \prod \Big(1 + \sum_{r=1}^{\infty} \frac{g(p^r)}{p^r}\Big) \Big(1 + \sum_{r=1}^{\infty} \frac{g^*(p^r)}{p^r}\Big)^{-1} + o(1),$$

le produit étant absolument convergent.

(2) se déduit de (3) de la façon suivante :

t réel étant fixé, soit

$$g(n) = \exp(itf(n)) \quad \text{et} \quad g^*(n) = \exp(itf^*(n)).$$

Ces fonctions satisfont aux hypothèses du lemme 4.

Elles sont multiplicatives et on a $|g(n)| = |g^*(n)| = 1$ pour tout n. On a $\sum \frac{|g(p)-g^*(p)|}{p} < \infty$ car

$$g(p) - g^*(p) = \begin{cases} 0 & \text{si} \quad p > 2 \quad \text{et} \quad |f(p)| \leq 1, \\ \exp(itf(p)) - 1 & \text{si} \quad p = 2 \quad \text{ou} \quad |f(p)| > 1. \end{cases}$$

On a pour $|z| < 1$: $\sum_{r=0}^{\infty} g^*(2^r) z^r = \frac{1}{1-z} \neq 0$.

De plus, pour tout $\lambda > 1$,

$$G^*(\lambda x) - G^*(x) = o(1) \text{ quand } x \text{ tend vers l'infini}$$

car (3) équivaut à

$$G^*(x) = P^*(t) \exp(it\ A^*(x)) + o(1) \tag{4}$$

et on a

$$|A^*(\lambda x) - A^*(x)| \leq \sum_{x < p \leq \lambda x} \frac{|f^*(p)|}{p} \leq \sum_{x < p \leq \lambda x} \frac{1}{p} = o(1).$$

Le lemme 4 donne

$$G(x) = G^*(x) \prod \Big(1 + \sum_{r=1}^{\infty} \frac{g(p^r)}{p^r}\Big)\Big(1 + \sum_{r=1}^{\infty} \frac{g^*(p^r)}{p^r}\Big)^{-1} + o(1),$$

ce qui, d'après (4), est équivalent à

$$G(x) = \Big(P^*(t) \prod \Big(1 + \sum_{r=1}^{\infty} \frac{g(p^r)}{p^r}\Big)\Big(1 + \sum_{r=1}^{\infty} \frac{g^*(p^r)}{p^r}\Big)^{-1}\Big) \exp(it\ A^*(x)) + o(1).$$

Comme g^* est fortement multiplicative,

$$1 + \sum_{r=1}^{\infty} \frac{g^*(p^r)}{p^r} = 1 + \frac{g^*(p)}{p-1} = \frac{p}{p-1}\Big(1 + \frac{g^*(p)-1}{p}\Big) = \frac{p}{p-1}\Big(1 + \frac{e^{itf^*(p)} - 1}{p}\Big).$$

On voit ainsi que

$$P^*(t)\prod\Big(1+\sum_{r=1}^{\infty}\frac{g(p^r)}{p^r}\Big)\Big(1+\sum_{r=1}^{\infty}\frac{g^*(p^r)}{p^r}\Big)^{-1}=\prod\Big(1-\frac{1}{p}\Big)\Big(1+\sum_{r=1}^{\infty}\frac{g(p^r)}{p^r}\Big)\exp\Big(-it\frac{f^*(p)}{p}\Big)$$

$$=\Big(\prod_{p\le x}\Big(1-\frac{1}{p}\Big)\Big(1+\sum_{r=1}^{\infty}\frac{g(p^r)}{p^r}\Big)\Big)\exp(-itA^*(x))+o(1).$$

Ainsi (5) donne

$$G(x)=\prod_{p\le x}\Big(1-\frac{1}{p}\Big)\Big(1+\sum_{r=1}^{\infty}\frac{g(p^r)}{p^r}\Big)+o(1).$$

Maintenant

$$\frac{1}{x}\sum_{n\le x}\exp(it(f(n)-A(x)))=G(x)\exp(-itA(x))$$

$$=\Big(\prod_{p\le x}\Big(1-\frac{1}{p}\Big)\Big(1+\sum_{r=1}^{\infty}\frac{g(p^r)}{p^r}\Big)\Big)\exp(-itA(x))+o(1)$$

$$=\prod_{p\le x}\Big(1-\frac{1}{p}\Big)\Big(1+\sum_{r=1}^{\infty}\frac{g(p^r)}{p^r}\Big)\exp(-v_p(t)+o(1)$$

puisque $\sum_{p\le x} v_p(t)=itA(x)$, et ceci est équivalent à (2).

Reste à établir que la fonction P est continue.

Pour celà nous utilisons encore un autre lemme :

LEMME 5. — *Soient $u_1,u_2,\dots,u_n,\dots$ et $v_1,v_2,\dots,v_n,\dots$ des fonctions réelles ou complexes définies sur un ensemble A.*

Soit B un sous-ensemble de A.

On suppose que, pour tout n et tout $t\in B$,

$$|u_n(t)|\le U_n \quad et \quad |u_n(t)-v_n(t)|\le V_n,$$

où U_n et V_n sont des constantes telles que

$$\sum_1^{\infty}U_n^2<\infty \quad et \quad \sum_1^{\infty}V_n<\infty.$$

Alors le produit infini $\prod_{n=1}^{\infty}(1+u_n(t))\exp(-v_n(t))$ *est uniformément convergent sur* B *et sa valeur est bornée sur cet ensemble.*

Ceci est le lemme de la page 108 de [3].

Ce lemme montre que, quel que soit $T>0$, le produit

$$\prod(1+u_p(t))\exp(-v_p(t))$$

est uniformément convergent pour $|t|\leq T$.

Tout d'abord on voit immédiatement que $|u_p(t)|\leq \frac{2}{p}$, et par suite $|u_p(t)-v_p(t)|\leq \frac{2}{p}$ si $|f(p)|>1$.

D'autre part, si $|f(p)|\leq 1$,

$$u_p(t)-v_p(t)=\frac{e^{itf(p)}-itf(p)-1}{p}-\frac{e^{itf(p)}}{p^2}+\left(1-\frac{1}{p}\right)\sum_{r=2}^{\infty}\frac{e^{itf(p^r)}}{p^r},$$

d'où il résulte que

$$|u_p(t)-v_p(t)|\leq\frac{|t|^2}{2}\cdot\frac{f(p)^2}{p}+\frac{2}{p^2}.$$

On a donc pour $|t|\leq T$

$$|u_p(t)|\leq U_p \quad \text{et} \quad |u_p(t)-v_p(t)|\leq V_p,$$

où

$$U_p = \frac{2}{p}$$

et

$$V_p = \begin{cases} \frac{2}{p} & \text{si} \quad |f(p)|>1, \\ \frac{T^2}{2}\cdot\frac{f(p)^2}{p}+\frac{2}{p^2} & \text{si} \quad |f(p)|\leq 1, \end{cases}$$

de sorte que $\sum U_p^2<\infty$ et $\sum V_p<\infty$.

4.2. Remarquons maintenant que le résultat à établir est une conséquence immédiate du théorème général suivant :

THÉORÈME 2. — *Soit* f *une fonction fortement additive réelle satisfaisant à*

$$|f(p)|\leq M \quad \textit{pour tout} \quad p \quad \textit{et} \quad \sum\frac{f(p)^2}{p}<\infty,$$

et soit $A(x) = \sum_{p \leq x} \frac{f(p)}{p}$.

Quand x *tend vers l'infini on a pour tout* t *réel*

$$\frac{1}{x} \sum_{n \leq x} \exp(it(f(n) - A(x))) = \prod \Big(1 + \frac{e^{itf(p)} - 1}{p}\Big) \exp\Big(-it \frac{f(p)}{p}\Big) + o(1),$$

où le produit converge uniformément par rapport à t *sur tout ensemble compact, et par suite les nombres* $f(n) - A(x)$ *où* $n \leq x$ *ont une distribution limite dont la fonction caractéristique est ce produit.*

Démonstration : Choisissons un entier $N > 0$ arbitraire et considérons pour $y \geq 2$ la fonction tronquée f_y définie par

$$f_y(n) = \sum_{\substack{p/n \\ p \leq y}} f(p).$$

Elle satisfait les hypothèses du lemme 1, avec E égal à l'ensemble des nombres premiers $\leq y$.

On est conduit à introduire la fonction entière

$$\Phi_y(z) = \prod_{p \leq y} \Big(1 + \frac{e^{zf(p)} - 1}{p}\Big) \exp\Big(-\frac{zf(p)}{p}\Big) = \sum_{q=0}^{\infty} a_q(y) z^q.$$

Le lemme montre que pour tout $q \in \mathbb{N}^*$ et tout $x \geq 1$

$$\Big| \sum_{n \leq x} (f_y(n) - A(y))^q - q! a_q(y) x \Big| \leq \Big(\frac{3}{2}\Big)^q M^q \pi(y)^q.$$

Nous prenons (pour $x \geq 2^{2N}$) $y = x^{1/2N}$.

On voit que, quand x tend vers l'infini, on a pour $1 \leq q \leq 2N$

$$\sum_{n \leq x} (f_y(n) - A(y))^q = q! a_q(y) x + o(x). \tag{6}$$

Nous remarquons maintenant que, étant donné $R > 0$ quelconque, le produit

$$\prod \Big(1 + \frac{e^{zf(p)} - 1}{p}\Big) \exp\Big(-\frac{zf(p)}{p}\Big)$$

est uniforément convergent pour $|z| \leq R$. Cela résulte du lemme 5 car, pour $|z| \leq R$,

$$\Big|\frac{e^{zf(p)}-1}{p}\Big| \leq \frac{e^{MR}-1}{p} \text{ et } \Big|\frac{e^{zf(p)}-1-zf(p)}{p}\Big| \leq \frac{e^{MR}-MR-1}{M^2}\cdot\frac{f(p)^2}{p}.$$

Par suite, quand y tend vers l'infini, $\Phi_y(z)$ converge uniformément sur tout ensemble compact vers la fonction entière

$$\Phi(z) = \prod\Big(1+\frac{e^{zf(p)}-1}{p}\Big)\exp\Big(-z\frac{f(p)}{p}\Big).$$

Si $\Phi(z) = \sum_{q=0}^{\infty} \beta_q z^q$, pour chaque q, $a_q(y)$ tend vers β_q.

Ainsi (6) donne pour $1 \leq q \leq 2N$

$$\sum_{n\leq x}(f_y(n)-A(y))^q = q!\beta_q x + o(x). \quad (x \longrightarrow \infty) \tag{7}$$

Ceci est vrai aussi pour $q = 0$ puisque $\beta_0 = \Phi(o) = 1$.

Maintenant, en partant de

$$f_y(n) - A(x) = (f_y(n) - A(y)) - (A(x) - A(y))$$

et utilisant la formule du binôme, on voit que l'on a pour $q \geq 1$

$$\sum_{n\leq x}(f_y(n)-A(x))^q = \sum_{n\leq x}(f_y(n)-A(y))^q + \sum_{k=1}^{q}(-1)^k\binom{q}{k}(A(x)-A(y))^k\Big(\sum_{n\leq x}(f_y(n)-A(y))^{q-k}\Big).$$

Mais

$$|A(x)-A(y)| \leq \sum_{y<p\leq x}\frac{|f(p)|}{p} \leq \Big(\sum_{y<p\leq x}\frac{1}{p}\Big)^{1/2}\Big(\sum_{y<p\leq x}\frac{f(p)^2}{p}\Big)^{\frac{1}{2}},$$

quantité qui est $o(1)$ car $\sum_{y<p\leq x}\frac{1}{p} = O(1)$ et $\sum\frac{f(p)^2}{p} < \infty$.

Il résulte donc de (7) que l'on a pour $1 \leq q \leq 2N$

$$\sum_{n\leq x}(f_y(n)-A(x))^q = q!\beta_q x + o(x). \tag{8}$$

Encore une fois, ceci a lieu aussi pour $q = 0$.

Utilisant à nouveau la formule du binôme on voit que, pour $q \geq 1$,

$$\sum_{n\leq x}(f_y(n) - A(x))^q = \sum_{n\leq x}(f_y(n) - A(x))^q + \sum_{k=1}^{q}\binom{q}{k}\Big(\sum_{n\leq x}(f(n) - f_y(n))^k(f_y(n) - A(x))^{q-k}\Big).$$

D'après (8), pour $q \leq 2N$ la première somme au second membre est égale à $q!\beta_q x + o(x)$.

On voit que, pour $1 \leq q \leq N$, la partie restante du second membre est $o(x)$.

En effet, pour $1 \leq k \leq q$, l'inégalité de Cauchy montre que la somme

$$\sum_{n\leq x}(f(n) - f_y(n))^k(f_y(n) - A(x))^{q-k}$$

est de module au plus égal à

$$\Big(\sum_{n\leq x}(f(n) - f_y(n))^{2k}\Big)^{\frac{1}{2}}\Big(\sum_{n\leq x}(f_y(n) - A(x))^{2q-2k}\Big)^{\frac{1}{2}}.$$

D'après (8), on a $\sum_{n\leq x}(f_y(n) - A(x))^{2q-2k} = O(x)$.

D'autre part, le lemme 2 donne

$$\sum_{n\leq x}(f(n) - f_y(n))^{2k} \leq x(2N)^{2k-1}\sum_{y<p\leq x}\frac{|f(p)|^{2k}}{p} \leq x(2N)^{2k-1}M^{2k-2}\sum_{y<p\leq x}\frac{f(p)^2}{p},$$

quantité qui est $o(x)$ du fait que $\sum \frac{f(p)^2}{p} < \infty$.

Ainsi, il est démontré que pour $1 \leq q \leq N$

$$\sum_{n\leq x}(f(n) - A(x))^q = q!\beta_q x + o(x).$$

Ceci vaut aussi pour $q = 0$ puisque $\beta_0 = 1$ et, puisque N est arbitraire, c'est vrai pour tout $q \geq 0$.

Finalement le lemme 3, avec $G(x,n) = f(n) - A(x)$, $\alpha_q(x) = q!\beta_q$ et $c_q = q!|\beta_q|$, donne le résultat voulu.

5. Appendice : Démonstration du lemme 4

Pour chaque p, les séries $\sum_{r=0}^{\infty} g(p^r)z^r = 1 + \sum_{r=1}^{\infty} g(p^r)z^r$ et $\sum_{r=0}^{\infty} g^*(p^r)z^r = 1 + \sum_{r=1}^{\infty} g^*(p^r)z^r$ sont absolument convergentes pour $|z| < 1$.

Désignons par $\mathcal{G}_p(z)$ et $\mathcal{G}_p^*(z)$ leurs sommes.

$\mathcal{G}_p(z)$ et $\mathcal{G}_p^*(z)$ sont $\neq 0$ pour $|z| < \frac{1}{2}$ car $\left|\sum_{r=1}^{\infty} g(p^r)z^r\right| < 1$ et $\left|\sum_{r=1}^{\infty} g^*(p^r)z^r\right| < 1$. La fonction $\mathcal{G}_p(z)/\mathcal{G}_p^*(z)$ est donc holomorphe dans le disque $|z| < \frac{1}{2}$.

Soit h la fonction multiplicative déterminée par le fait que, pour chaque p, on a pour $|z| < \frac{1}{2}$

$$\frac{\mathcal{G}_p(z)}{\mathcal{G}_p^*(z)} = 1 + \sum_{r=1}^{\infty} h(p^r)z^r.$$

Comme $h(1) = 1$, ceci est équivalent à

$$\sum_{k=0}^{r} g^*(p^k)h(p^{r-k}) = g(p^r), \quad r = 0,1,2,\dots . \tag{9}$$

Ceci montre que $g = g^* * h$, puisque $g^* * h$ est multiplicative et, pour chaque p et chaque $r \in \mathbb{N}^*$, $(g^* * h)(p^r) = g(p^r)$.

Les égalités (9) montrent, par récurrence sur r, que $|h(p^r)| \leq 2^r$.

Il en résulte que, pour chaque $p > 2$,

$$\sum_{r=2}^{\infty} \frac{|h(p^r)|}{p^r} \leq \frac{1}{p(p-2)}$$

et, comme $h(p) = g(p) - g^*(p)$, $\sum_{r=1}^{\infty} \frac{|h(p^r)|}{p^r} \leq \frac{|g(p)-g^*(p)|}{p} + \frac{1}{p(p-2)}$.

Par suite $\sum_{p>2} \left(\sum_{r=1}^{\infty} \frac{|h(p^r)|}{p^r} \right) < \infty$.

Maintenant, d'après l'hypothèse (b), il existe $\rho \in]\frac{1}{2}, 1[$ tel que la fonction $\mathcal{G}_2(z)/\mathcal{G}_2^*(z)$ est holomorphe dans le disque $|z| < \rho$, et on a

$$\sum_{r=0}^{\infty} h(2^r)z^r = \frac{\mathcal{G}_2(z)}{\mathcal{G}_2^*(z)} \quad \text{pour} \quad |z| < \rho.$$

En particulier on a $\sum_{r=0}^{\infty} \frac{h(2^r)}{2^r} = \frac{\mathcal{G}_2(1/2)}{\mathcal{G}_2^*(1/2)}$ et la série est absoluement convergente.

On voit ainsi que $\sum_p \Big(\sum_{r=1}^{\infty} \frac{|h(p^r)|}{p^r} \Big) < \infty$.

Il en résulte que la série $\sum_1^{\infty} \frac{h(n)}{n}$ est absolument convergente et sa somme est la valeur du produit absolument convergent

$$\prod \Big(\sum_{r=0}^{\infty} \frac{h(p^r)}{p^r} \Big) = \prod \frac{\mathcal{G}_p(1/p)}{\mathcal{G}_p^*(1/p)} = \prod \Big(1 + \sum_{r=1}^{\infty} \frac{g(p^r)}{p^r} \Big) \Big(1 + \sum_{r=1}^{\infty} \frac{g^*(p^r)}{p^r} \Big)^{-1}$$

Maintenant, de ce que $g = g^* * h$ il résulte que

$$\begin{aligned} G(x) &= \sum_{n \le x} \frac{h(n)}{n} G^*\Big(\frac{x}{n}\Big) \\ &= \sum_{n=1}^{\infty} \frac{h(n)}{n} G^*\Big(\frac{x}{n}\Big) \quad \text{puisque } G^*\Big(\tfrac{x}{n}\Big) = 0 \text{ pour } n > x. \end{aligned}$$

On a ainsi

$$G(x) - G^*(x) \sum_{n=1}^{\infty} \frac{h(n)}{n} = - \sum_{n=1}^{\infty} \frac{h(n)}{n} \Big(G^*(x) - G^*\Big(\frac{x}{n}\Big) \Big).$$

La série au second membre est uniformément convergente pour $x \ge 1$ car son terme général est de module $\le 2\frac{|h(n)|}{n}$. D'après l'hypothèse (c) chaque terme tend vers zéro quand x tend vers l'infini.

BIBLIOGRAPHIE

[1] H. DELANGE. — Sur un théorème d'Erdös et Kac, *Acad. Roy. Belg., Cl. Sci.* **5**, (1956), 130-144.

[2] H. DELANGE. — Sur certaines fonctions arithmétiques additives, *Séminaire Delange-Pisot, 2ème année*, (1960-61), n° 6.

[3] H. DELANGE. — Sur des formules de Atle Selberg, *Acta Arith.* **19**, (1971), 105-146.

[4] H. DELANGE. — On the use of the method of moments for the study of additive functions, *à paraître dans J. Number Theory.*

[5] H. DELANGE and H. HALBERSTAM. — A note on additive functions, *Pacific J. Math.* **7**, (1957), 1551-1556.

[6] P.D.T.A. ELLIOTT. — *Probabilistic Number Theory*, Springer Verlag, 1979.

[7] P. ERDÖS and M. KAC. — The Gaussian law of errors in the theory of additive number-theoretic functions, *Amer. J. Math.* **62**, (1940), 738-742.

[8] H. HALBERSTAM. — On the distribution of additive number-theoretic functions II, *J. London Math. Soc.* **31**, (1956), 1-14.

H. DELANGE
Mathématique, Bât. 425
Université de Paris-Sud
91405 ORSAY CEDEX

Polynôme de petite mesure

Mohamed KERADA

1. Introduction

On note S (resp. T) l'ensemble des nombres de Pisot (resp. l'ensemble des nombres de Salem). Dans [8] Salem a montré que chaque point de S est un point limite de T. Dans [6] D.W. Boyd a établi le résultat suivant :

Pour tout polynôme Q unitaire à coefficients entiers de degré s vérifiant $Q* = \varepsilon Q$; avec $\varepsilon = \pm 1$ et possédant $s-2$ racines distincts sur $|z| = 1$ et une racine $\sigma > 1$ dans $|z| > 1$ et pour tout entier k $1 \leq k \leq n$, il existe des polynômes P unitaires à coefficients entiers de degré n tels que $Q(z) = zP(z)+\varepsilon P*(z)$ et possèdant le zéros dans $|z| > 1$ et $n-k$ zéros dans $|z| < 1$. Ce résultat a permis à M.-J. Bertin et D.W. Boyd de caractériser les petits nombres de Salem en deux classes [2]. Nous proposons ici de généraliser cette caractéristation à des polynômes de petite mesure et possédant j racines dans $|z| > 1$, donnés par D.W. Boyd [7].

2. Rappels et définitions

On rappelle [3] que si P est un polynôme à coefficients réels de degré d et $j \in \mathbb{N} - \{0\}$; on définit le polynôme Q par :

$$Q(z) = z^j P(z) + \varepsilon P^*(z), \tag{1}$$

avec $\varepsilon = \pm 1$ et P^* le polynôme réciproque de P.

Lemme 1. — *Soit P un polynôme de $\mathbb{R}[z]$ tel que P et $P*$ soient premiers entre eux et Q le polynôme défini comme dans (1). Alors l'équation $Q(z,t) = z^j P(z) + \varepsilon t P*(z) = 0$ définit une courbe algébrique $z = Z(t)$ possédant $j+d$ branches (où $d = \deg P$), notées $z_k(t)$ ayant les propriétés suivantes :*

1) $z_k(D(0,1)) \subset D(0,1)$ *ou* $z_k(D(0,1)) \subset \mathbb{C} - \overline{D(0,1)}$,

2) $z_k(1)$ *est égal à une racine de Q de module 1;*

3) *si α est racine de Q de module 1, il existe au moins une branche z_k telle que $z_k(1) = \alpha$.*

DÉFINITION 1. — *Avec les notations du Lemme* 1, *soit* α *une racine de* Q *de module* 1

S'il existe une seule branche z_k *telle que* $z_k(1) = \alpha$ *et* $|z_k(0)| < 1$ (resp. $|z_k(0) > 1$). *On dit que* α *est une "sortie"* (resp. *"entrée"*).

Si la branche z_k *est telle que* $z_k(1) = \alpha$ *et* $|z_k| < 1$ resp. $|z_k(0)| > 1$). *On dit que la branche* z_k *"sort"* (resp. *"entre"*) *en* α.

LEMME 2 (Boyd [6]). — *Avec les notations du Lemme 1, soit* α *une racine de* Q *de module 1, alors si* α *est une racine simple de module 1 de* Q, α *est une "entrée" (resp. "sortie") si et seulement si* $\varepsilon\ \alpha^{1-d}P(\alpha)Q'(\alpha) > 0$ (resp. < 0). *Si* α *est une racine multiple d'ordre* k *de module 1 de* Q ($k \geq 2$), *alors il existe* k_1 *branches entrant en* α *et* k, *branches sortant en* α, *avec* $k_1 + k_2 = k$ *et* $k_1 \geq [\frac{k}{2}]$, $k_2 \geq [\frac{k}{2}]$.

DÉFINITION 2. — *Soit* P *un polynôme à coefficients entiers irréductible* $P(z) = c_0 z^n + \cdots + c_{n-1}z + c_n$ *et* $\theta_1, \ldots, \theta_n$ *les zéros de* P. *On appelle mesure de Mahler de* P *la quantité*

$$M(P) = |c_0| \prod_{i=1}^{n} \max(|\theta_i|, 1).$$

3. DÉFINITIONS ET RÉSULTATS DE BASE

DÉFINITION 3. — *Soit* τ *un entier algébrique* ($|\tau| > 1$). *On dit que* τ *est un i-Salem si son polynôme minimal possède* $i - 1$ *racines différentes de* τ *dans* $|z| > 1$ *et au moins une racine sur* $|z| = 1$.

DEFINITION 4. — *Soit* τ *un entier algébrique* ($|\tau| > 1$). *On dit que* τ *est un i-Pisot si son polynôme minimal possède* $i - 1$ *racines différentes de* τ *dans* $|z| > 1$ *et les autres racines dans* $|z| > 1$.

4. Généralisation de la construction de Boyd

Théorème 1. — *Soit P un polynôme à coefficient, réels de degré s, soit Q le polynôme défini par $Q(z) = z^j P + \varepsilon P*(z)$, $\varepsilon = \pm 1$.*

On suppose que le polynôme Q vérifie les propriétés suivantes :

a) les zéros de Q sont tous simples,

b) Q a j racines dans $|z| < 1$,

c) $\varepsilon\ \alpha^{1-s} P(\alpha) Q'(\alpha) < 0$ quelque soit α zéro de module 1 de Q.

Alors P a j zéros dans $|z| > 1$ et $s - j$ zéros dans $|z| < 1$.

Preuve :

Soit k le nombre de zéros de P dans $|z| < 1$; d'après (b), (c) et le Lemme de Boyd, il y a $s - j$ *"sorties"* qui proviennent donc d'autant de zéros de $z^j P(z)$ dans $|z| < 1$; de plus les j zéros de Q de module inférieur à 1 sont des fins de branches commençant dans $|z| < 1$ donc en des zéros de $z^j P(z)$. D'où $s - j + j = j + k$ et $k = s - j$.

Théorème 2. — *Soit P un polynôme à coefficients réels de degré s, soit Q le polynôme défini par $Q(z) = z^j P(z) + \varepsilon P*(z)$, $\varepsilon = \pm 1$. On suppose que le polynôme Q vérifie les propriétés suivantes :*

a) les zéros de Q sont tous simples;

b) Q a j zéros dans $|z| > 1$;

c) $\varepsilon \alpha^{1-s} P Q'(\alpha) > 0$ quel que soit α zéro de Q de module 1.

Alors P a tous ses zéros dans $|z| > 1$.

Preuve :

On raisonne de la même façon que dans le théorème 1.

Soit R le polynôme minimal d'un j-Salem de degré $2m$ et $\mathcal{U}$ un polynôme cyclotomique, alors $Q = \mathcal{U}R$ est réciproque ou antiréciproque ($Q* = \varepsilon Q$, $\varepsilon = \pm 1$), Q possède $s - 2j$ racines simples de module 1, avec deg $Q = s$. Le polynôme $\mathcal{U}$ sera en général un facteur de $z^j - 1$ sauf dans les théorèmes 5, 6 et 7 où $\mathcal{U}$ sera choisi de la façon suivante :

$\mathcal{U} = z^j - 1$ si $\varepsilon = -1$

$\mathcal{U} = z^{j-1} + \cdots + 1$ tel que $(z^{j-1} + \cdots + 1)(z - 1) = z^j - 1$ si $\varepsilon = 1$.

THÉORÈME 3. — *Soit le polynôme $Q = UMR$ à coefficients entiers de degré s, où U et R sont définis comme précédemment et M un polynôme cyclotomique à racines simples, M et U premiers entre eux. En outre si $\varepsilon = 1$ et s pair, le coefficient du milieu de Q est aussi pair. Alors il existe des polynômes P de degré n ayant n racines dans $|z| > 1$ tels que $Q(z) = z^j P(z) + \varepsilon P*(z)$, $\varepsilon = \pm 1$.*

Idée de la démonstration :

Puisque $Q* = \varepsilon Q$ et comme Q possède j racines dans $|z| > 1$ alors Q a $s - 2j$ racines sur $|z| = 1$ toutes simples donc les conditions (a) et (b) du théorème 2 sont vérifiées.

La démonstration utilise alros le lemme de Boyd.

THÉORÈME 4. — *Sous les hypothèses du théorème 3, il existe des polynômes P de degré n ayant j racines dans $|z| > 1$ et $n - j$ racines dans $|z| < 1$ tels que $Q(z) = z^d P(z) + \varepsilon P*(z)$.*

On raisonne de la même façon que dans le théorème 3, en remplaçant les inégalités d'*entrées* par les inégalités de *sorties*.

5. ENSEMBLES $A_q(j)$ ET $B_q(j)$

DÉFINITION 5. — *$A_q(j)$ est l'ensemble des j-Salem de polynôme minimal T produits par les polynômes P sans zéro dans $|z| \leq 1$ tels que $|P(0)| = q$.*

DÉFINITION 6. — *$B_q(j)$ est l'ensemble des j-Salem de polynôme minimal T produits par les polynômes P, sans zéro de module 1 possédant j zéros dans $|z| > 1$ et $n - j$ zéros dans $|z| < 1$, tels que $|P(0)| = q$.*

$T(j)$ est l'ensemble des j-Salem.

Remarques :

1) Le théorème 3 entraîne que,

$$T(j) \subset \bigcup_{q \geq 2} A_q(j) \quad \text{d'où} \quad T(j) = \cup_{q \geq 2} A_q(j).$$

2) Le théorème 4 entraîne que,

$$T(j) \subset \bigcup_{q \geq 0} B_q(j) \quad \text{d'où} \quad T(j) = \cup_{q \geq 0} B_q(j).$$

6. Caractérisation de certains sous-ensembles des $A_q(j)$ et $B_q(j)$

Définition 7. — *$A_q^*(j)$ est le sous-ensemble de $A_q(j)$ vérifiant en outre*

$$\begin{array}{ll} (z^j-1)MT & = z^jP(z)-P^*(z) \quad si\ \varepsilon=-1 \\ (z^{j-1}+\cdots+1)MT & = z^jP(z)+P^*(z) \quad si\ \varepsilon=1. \end{array}$$

Définition 8. — *$B_q^*(j)$ est le sous-ensemble de $B_q(j)$ vérifiant en outre :*

$$\begin{array}{ll} (z^j-1)MT & = z^jP(z)-P^*(z) \quad si\ \varepsilon=-1 \\ (z^{j-1}+\cdots+1)MT & = z^jP(z)+P^*(z) \quad si\ \varepsilon=1. \end{array}$$

Théorème 5. — *Soit τ un j-Salem de polynôme minimal T ayant un nombre impair de conjugués réels dans $]-\infty,-1]$ ou $[1,+\infty[$ (on peut donc toujours se ramener au cas $T(1)<0$ c'est-à-dire au cas du nombre impair de conjugués réels dans $[1,+\infty[$). Alors $\tau\in A_q^*(j)$ si et seulement si il existe un polynôme cyclotomique K à racines simples tel que $K(\zeta)\neq 0$, quel que soit ζ vérifiant $\zeta^j=1$ et un plynôme réciproque L tel que*

a) $L(0)=q-1$,

b) $\deg\ L=\deg\ KT-j$,

c) $L(1)\geq -K(1)T(1)$,

d) L possède toutes ses racines simples sur $|z|=1$. En outre si l'on a :

j **pair** *:* **ou bien** *$\varepsilon=-1$ soit $Q(z)=(z^j-1)KT$ alors $n=\deg\ KT$ est pair; on désigne par $i^{i\Psi_1},\ldots,e^{i\psi_{(n-j)/2}}$ les zéros de L situés sur $|z|=1$ et sur $z\geq 0$, tels que*

$$\psi_1<\psi_2<\cdots<\psi_{(n-j)/2}$$

et par $1,e^{i\varphi_1},\ldots,e^{i\varphi_{n-j)/2-1}}$, $e^{i\Pi}$ les zéros de $(z^j-1)KT$ situés sur $|z|=1$ et $Im\ z\geq 0$, tels que

$$0<\varphi_1<\varphi_2<\cdots<\varphi_{(n-j)/2}-1<\Pi,$$

alors on a les inégalités suivantes :

$$0<\psi_1<\varphi_1<\cdots<\psi_{(n-j)/2^{-1}}<\varphi_{(n-j)/2^{-1}}<\psi_{(n-j)/2}<\Pi$$

donc les zéros de L *et* $(z^j-1)KT$ *s'entrecroisent;*

ou bien $\varepsilon = 1$ *et* $Q(z) = (z^{z-1}+\cdots+1)KT$*; alors* $n+1 = \deg\ KT$ *est pair; on désigne par* $e^{i\psi_1},\ldots,e^{i\psi_{(n-j+1)/2}}$ *les zéros de* L *situés sur* $|z|=1$ *et* $Im\ z \geq 0$*, tels que*

$$\psi_1 < \psi_2 < \cdots < \psi_{(n-j+1)/2}$$

et par $e^{i\varphi_1},\ldots,e^{i\varphi_{(n-j-1)/2}}$, $e^{i\Pi}$ *les zéros de* $(z^{j-1}+\cdots+1)KT$ *situés sur* $|z|=1$ *et* $Im\ z \geq 0$*, tels que*

$$\varphi_1 < \varphi_2 < \cdots < \varphi_{(n-j+1)/2} < \Pi,$$

alors on a les inégalités suivantes :

$$\psi_1 < \varphi_1 < \cdots < \psi_{(n-j-1)/2} < \varphi_{(n-j-1)/2} < \psi_{(n-j+1)/2} < \Pi;$$

donc les zéros de L *et* $(z^{j-1}+\cdot+1)KT$ *s'entrecroisent.*

On a un énoncé analogue dans le cas j *impair.*

THÉORÈME 6. — *Soit* τ *un* j*-Salem de polynôme minimal* T *ayant un nombre pair de conjugués de module supérieur à 1 vérifiant* $T(1) > 0$ *et* $T(-1) > 0$*. Alors* $\tau \in A_q^*(j)$ *si et seulement si il existe un polynôme cyclotomique* K *à racines simples tel que* $K(\zeta) \neq 0$*, quel que soit* ζ *vérifiant* $\zeta^j = 1$*, et un polynôme* L *réciproque tel que :*

a) $L(0) = -q-1$,

b) $\deg\ KT - j = \deg\ L$,

c) $L(1) \leq -K(1)T(1)$,

c) L *possède toutes ses racines simples* $|z|=1$*. En outre si l'on a :* $\varepsilon = -1$ *soit* $Q(z) = (z^j-1)KT(z)T(z)$ *alors* $n = \deg\ KT$ *est pair; on désigne par* $e^{i\psi_1},\ldots,e^{i\psi_{(n-j)/2}}$ *les zéros de* L *situés sur* $|z|=1$ *et* $Im\ z \geq 0$ *tels que :*

$$\psi_1 < \psi_2 < \cdots < \psi_{(n-j)/2}$$

et par $1, e^{i\varphi_1},\ldots,e^{i\varphi_{(n-j)/2-1}}$, $e^{i\Pi}$ *les zéros de* $(z^j-1)K(z)T(z)$ *situés sur* $|z|=1$ *et* $Im\ z \geq 0$ *tels que*

$$0 < \varphi_1 < \cdots < \varphi_{(n-j)/2-1} < \Pi;$$

alors on a les inégalités suivantes :

$$0 < \psi_1 < \varphi_1 < \cdots < \psi_{(n-j)/2-1} < \phi_{(n-j)/2-1} < \psi_{(n-j)/2} < \Pi$$

donc les zéros de L *et* $(z^j - 1)K(z)T(z)$ *s'entrecroisent.*

$\varepsilon = 1$ *et* $Q(z) = (z^{j-1} + \cdots + 1)K(z)T(z)$ *alors* $n + 1 = \deg\ KT$*;* *on désigne par* $e^{i\psi_1}, \ldots, e^{i\psi_{(n-j+1)/2}}$ *les zéros de* L *situés sur* $|z| = 1$ *et* $Im\ z \geq 0$ *tels que*

$$\psi_1 < \cdots < \psi_{(n-j+1)/2}$$

et par $e^{i\varphi_1}, \ldots, e^{i\varphi_{(n-j-1d)/2}}$, $e^{i\Pi}$ *les zéros de* $(z^{j-1} + \cdot + 1)K(z)T(z)$ *situés sur* $|z| = 1$ *et* $Im\ z \geq 0$ *tels que*

$$\varphi_1 < \cdots < \varphi_{(n-j-1)/2} < \Pi;$$

alors on a les inégalités suivantes :

$$\psi_1 < \varphi_1 < \cdots < \psi_{(n-j-1)/2} < \varphi_{(n-j-1)/2} < \psi_{(n-j+1)/2} < \Pi$$

donc les zéros de L *et* $(z^{j-1} + \cdots + 1)K(z)T(z)$ *s'entrecroisent.*

THÉORÈME 7. — *Soit* τ *un* j*-Salem de polynôme minimal* T *vérifiant* $T(1) > 0$ *et* $T(-1) > 0$*. On a alors* j *pair. Alors* $\tau \in B_q^*(j)$ *pour* $\varepsilon = 1$ *si et seulement si il existe un polynôme cyclotomique* K *à racines simples tel que* $K(\zeta) \neq 0$ *quel que soit* ζ *vérifiant* $\zeta^j = 1$*; et un polynôme réciproque* L *tels que,*

a) $L(0) = 1 + P(0)$,

b) deg L : deg $KT - j$,

c) $L(1) = K(1)T(1)$,

d)

(i) ou bien L *est comme dans le théorème 6.*

(ii) ou bien L *possède un seule zéro dans* $|z| > 1$*. En outre si l'on écrit* $Q(z) = (z^{j-1} + \cdot + 1)(K(z)T(z)$*, avec* deg $KT - 1 =$ deg $P = n$ *impair, soient* $e^{i\psi_1}, \ldots, e^{i\psi_{\frac{n-j-1}{2}}}$ *les racines de* L *situés sur* $|z| = 1$ *et* $Im\ z \geq 0$ *tels que*

$$\psi_1 < \psi_2 < \cdots < \psi_{(n-j-1)/2}$$

et $e^{i\varphi_1}, \ldots, e^{i\varphi_{\frac{(n-j-1)}{2}}}$ *, et* $e^{i\Pi}$ *situés sur* $|z| = 1$ *et* $Im\ z \geq 0$ *tels que :*

$$\varphi_1 < \varphi_2 < \cdots < \varphi_{(n-j-1)/2} < \Pi;$$

alors on a les inégalités suivantes :

$$\psi_1 < \varphi_1 < \cdots < \psi_{\frac{(n-j-1)}{2}} < \varphi_{\frac{(n-j-1)}{2}} < \psi_{\frac{(n-j+1)}{2}} < \Pi$$

d'où les zéros de L *et* Q *s'entrecroisent.*

Remarque :
S'il existe un polynôme L réciproque cyclotomique tel que,

$$\deg\ L = \deg\ KT - j, \quad L(0) = 1 + P(0), \quad K(1)T(1) \geq L(1)$$

tel que les zéros de L et de $(z^{-1} - 1)KT$ s'entrecroisent alors

$$\tau \in B_q(j).$$

7. Exemples

On peut montrer que tout polynôme réciproque de petite mesure de degré inférieur ou égal à 12 appartient à l'un des enmsembles $B_q^*(j)$ ou $A_q^*(j)$, en exhibant un couple de polynômes cyclotomiques K et L vérifiant les conditions des théorème 5, 6 ou 7.

Pour les quelques exemples donnés ici, on indique la mesure, le nombre de racines extérieures au cercle unité et les coefficients de la première moitié du polynôme.

Mesure	Nombre de racines extérieures au disque unité	Première moitié du polynôme
1,7467934983	2	1 2 2 1

$K = 1$, $L = \Phi_8$, $K(1) = 1$, $L(1) = 2$, $T(1) = 11$, $\underline{\tau \in B_0^*(2)}$
Les arguments des racines de module 1 correspondants au polynôme T 54,89
Les arguments des racines de module 1 correspondants au polynôme KT 54,89
Les arguments des racines de module 1 correspondants au polynôme L 45 135

$$0 < \underline{45} < 54,89 < \underline{135} < 180$$

Mesure	Nombre de racines extérieures au disque unité	Première moitié du polynôme
1,8475219321	2	1 1 −1 −1 −1

$K = 1$, $L = \Phi_7$, $K(1) = 1$, $L(1) = 7$, $T(1) = -1$, $\underline{\tau \in A_2^*(2)}$
Les arguments des racines de module 1 correspondants au polynôme T 75,76 133,60
Les arguments des racines de module 1 correspondants au polynôme KT 75,76 133,60
Les arguments des racines de module 1 correspondants au polynôme L 51,4 102,9 154,2

$$0 < \underline{51,4} < 75,76 < \underline{102,9} < 133,60 < \underline{154,12} < 180$$

Mesure	Nombre de racines extérieures au disque unité	Première moitié du polynôme
1,6358170255	3	1 0 0 −1 −1 0

$K = 1$, $L = \Phi_2\Phi_9$, $K(1) = 1$, $L(1) = 2$, $T(1) = -1$, $\underline{\tau \in A_2^*(3)}$
Les arguments des racines de module 1 correspondants au polynôme T 56,08 163,39
Les arguments des racines de module 1 correspondants au polynôme KT 56,08 163,39
Les arguments des racines de module 1 correspondants au polynôme L 40 80 160 180

$$0 < \underline{40} < 56,08 < \underline{80} < 120 < \underline{160} < 163,39 < \underline{180}$$

Mesure	Nombre de racines extérieures au disque unité	Première moitié du polynôme
1,4907833576	3	1 0 0 −1 0 −1 1

$K = 1$, $L = \Phi_2\Phi_4\Phi_6\Phi_{10}$, $K(1) = 1$, $L(1) = 4$, $T(1) = -1$, $\underline{\tau \in A_2^*(3)}$
Les arguments des racines de module 1 correspondants au polynôme T 41,76 82,93 104,38
Les arguments des racines de module 1 correspondants au polynôme KT 41,76 82,93 104,38
Les arguments des racines de module 1 correspondants au polynôme L 36 60 90 108 180

$$0 < \underline{36} < 41,76 < \underline{60} < 82,93 < \underline{90} < 104,38 < \underline{108} < 120 < \underline{180}.$$

BIBLIOGRAPHIE

[1] M.-J. BERTIN. — Familles fermées de nombres algébriques, *Acta Arithmetica* **39**, (1981), 207-240.

[2] M.-J. BERTIN et D.W. BOYD. — *A characterisation of two related classes of Salem numbers*, J. Number Theory (to appear).

[3] M.-J. BERTIN et M. PATHIAUX DELEFOSSE. — *Conjecture de Lehmer et petits nombres de Salem*, Queen's papers in pure and applied mathematics, N° 81, 1989.

[4] D.W. BOYD. — Pisot and Salem numbers in intervals of the real line, *Math. Comp.* **32**, (1978), 1244-1260.

[5] D.W. BOYD. — Families of Pisot and Salem numbers, *Séminaire de Théorie des Nombres de Paris 1980-81, Birkhaüser* , (1982), 19-33.

[6] D.W. BOYD. — Small Salem Numbers, *Duke Math. J.* **44**, (1977), 315-327.

[7] D.W. BOYD. — Reciprocal polynomials having small measure, *Math. Comp.* **35**, (1980), 1361-1377.

[8] R. SALEM. — Power series with integral coefficients, *Duke Math. J.* **12**, (1945), 153-172.

[9] R. SALEM. — *Algebraic numbers and Fourier analysis* , D.C. Heath and CO Boston, 1963.

Mohamed KERADA
Université de Paris VI
Mathématique
4, place Jussieu
75005 PARIS

Propriétés algébriques des séries formelles liées au Shuffle

K. Hyra LAMÈCHE

Soit A un anneau commutatif unitaire de caractéristique zéro . Soient $X = (x_1 x_2 - x_n)$ un ensemble fini ou alphabet et X^* le monoïde libre engendré par X.

On notera $A << X >>$ (resp. $A_{rat} << X >>$) l'algèbre large des séries formelles sur X (resp. l'algèbre des séries rationnelles) à coefficients dans A.

Sur l'alphabet X on adopte un ordre qu'on prolonge à X^* en posant : $f \leq g$ si l'on a l'une des deux relations suivantes :

Soit $|f| < |g|$ où $|f|$ désigne le nombre de lettres de X figurant dans l'écriture du mot f si $f \in XX^*$ et 0 si $f = \varepsilon$ le mot neutre de X^*.

Soit $|f| = |g|$ et f précède g lexicographiquement. Si l'alphabet $X = (x)$ est réduit à une seule lettre alors nous sommes ramenés à l'étude des séries formelles à une variable. L'algèbre des séries formelles étant notée. $A[[X]]$, la sous-algèbre des polynômes étant elle notée $A[X]$.

Nous avons :

$$a \in A[[X]] \Longleftrightarrow a = \sum_{n \geq 0} a_n X^n \quad a_n \in A \ \forall n.$$

Dans une première partie, nous étudierons les propriétés liées au Shuffle lorsque $X = (x)$ puis nous étendrons ces propriétés au cas où l'alphabet X a au moins 2 lettres.

Au point de vue algébrique telle que l'étude des éléments nilpotents ou diviseurs de zéro, l'algèbre $A[[X]]$ (resp. sous-algèbre $A[X]$) munie du Shuffle se comporte comme l'algèbre $A[[X]]$ (resp. $A[X]$) munie du produit de Cauchy. Au point de vue inversion dans $A_{rat}[[X]]$, l'algèbre $A_{rat}[[X]]$ munie du Shuffle se comporte comme l'algèbre $A_{rat}[[X]]$ munie du produit de Hadamard.

Éléments nilpotents et diviseurs de zéro

Soient $a = \sum_{n\geq 0} a_n X^n$ et $b = \sum_{n\geq 0} b_n X^n$ deux séries formelles. Le Shuffle de a par b noté : $a \sqcup\!\sqcup b$ est défini pour tout entier $n \geq 0$ par la relation

$$a \sqcup\!\sqcup b = \sum_{n\geq 0} (a \sqcup\!\sqcup b, X^n) X^n$$

où

$$(a \sqcup\!\sqcup b, X^n) = \sum_{0\leq p\leq n} C_n^p a_p b_{n-p}$$

soit $\ell(a)$ l'application linéaire de $A[[X]]$ dans elle-même définie pour toute série a par la formule :

$$\ell(a) = \ell\Big(\sum_{n\geq 0} a_n X^n\Big) = \sum_{n\geq 0} \frac{an}{n!} X^n$$

d'où

$$\ell(a \sqcup\!\sqcup b) = \ell \sum_{n\geq 0} \Big(\sum_{0\leq p\leq n} C_n^p a_p b_{n-p} \Big) X^n = \sum_{n.} \Big(\sum_{0\leq p\leq n} \frac{ap}{p!} \frac{b_{n-p}}{(n-p)!} \Big) X^{n.}$$

d'où

$$\ell(a \sqcup\!\sqcup b) = \ell(a) \times \ell(b)$$

l'application $\ell.$ est un isomorphisme de l'algèbre $A[[X]]$ munie du Shuffle dans l'algèbre $A[[X]]$ munie du produit de Cauchy.

PROPOSITION I. — *Soit* $a = \sum_{0\leq n\leq p} a_n X^n$ *un polynôme. Pour tout* $r \geq 2$ *soit :*

$$a^{(r)} = a \sqcup\!\sqcup a \sqcup\!\sqcup \cdots \sqcup\!\sqcup a \ (\textit{le Shuffle de a par lui même 2 fois})$$

un polygône est nilpotent si et seulement si chacun de des coefficients l'est.

La démonstration résulte immédiatement de la démonstration faite dans le cas où l'algèbre $A[X]$ est muni du produit de Cauchy.

Soit r l'ordre de nilpotence du polynôme a, d'où

$$\ell(a^{(r)}) = (\ell(a))^r = 0$$

par récurrence sur n où $0 \leq n \leq p$ on démontre que les coefficients du polynôme $\ell(a)$ sont nilpotents, d'où

$$\frac{a_n}{n!} \text{ est nilpotent } \forall n \ 0 \leq n \leq p.$$

L'anneau A étant de caractéristique zéro, a_n est nilpotent $\forall\ 0 \leq n \leq p$.

La réciproque est immédiate.

PROPOSITION II. — *Un polynôme* $a = \sum_{n\geq 0} a_n X^n$ *est un diviseur de zéro dans l'anneau* $A[X]$ *si et seulement si il existe* $r \in A - \{0\}$ *tel que*

$$r \sqcup\!\sqcup a = ra = 0.$$

Démonstration :

S'il existe $r \in A - \{0\}$ tel que $r \sqcup\!\sqcup a = ra = 0$ il est immédiat que le polynôme a est un diviseur de zéro.

Réciproquement

Soit $b = \sum_{0\leq n\leq q} b_n X^n$ un polynôme non nul tel que :

$$a \sqcup\!\sqcup b = 0$$

d'où $\ell(a \sqcup\!\sqcup b) = \ell(a) \times \ell(b) = 0$.

La relation $\ell(a) \times \ell(b) = 0$ fournit un système d'équations linéaires noté (I) dont les coefficients sont les coefficients du polynôme a et les inconnues les coefficients du polynôme b. Soit M la matrice du système (I). Ce système admettant une solution non triviale est de rang au plus égal à $q - 1$.

Il existe donc un élément non nul $k \in A - \{0\}$ qui annule tous les sous déterminants d'ordre q. Cet élément non nul permet par récurrence sur n de construire l'élément $r(G(1))$. Il existe $r \in A - \{0\}$ tel que :

$$\begin{aligned} r\ell(a) &= 0 \\ ou\ r\ell(a) &= \ell(r \sqcup\!\sqcup Q) = 0 \\ &\text{d'où } r \sqcup\!\sqcup a = 0. \end{aligned}$$

Si l'anneau A est de caractéristique $p \neq 0$. Les deux propositions I et II sont fausses. En effet pour $p = 2$ et $A = \mathbb{F}_2$ soit :

$$a = X^2 + X^4$$

nous avons $a \sqcup\!\sqcup a = 0$ bien qu'aucun élément non nul du corps $\mathbb{F}_2$ n'annule a. D'autre part aucun coefficient de a n'est nilpotent.

Ces deux propositions ne se prolongent pas à l'algèbre large $A[[X]]$ lorsque l'anneau A n'est pas nœthérien ou lorsque l'anneau A étant

quelconque les coefficients des séries a et b n'engendrent pas des idéaux de type fini. En effet :

$$\text{Soit} \quad A = \oplus_{i=0}^{\infty}\Big(\frac{K[X_i]}{(X_i^i)}\Big)$$

K étant un corps de caractéristique zéro d'où

$$\overline{X}_i \cdot \overline{X}_j = 0 \ \forall i \neq j$$

$$\text{et } \overline{X}_i^i = 0 \ \forall i$$

$$\text{si } a(T) = \sum_{i=0}^{\infty} \overline{X}_i T^i$$

chaque coefficient de la série a est nilpotent, mais la série a n'est pas nilpotente.

En effet s'il existait un entier $p \geq 1$ tel que :

$$(a(T))^p = 0 \Longrightarrow \frac{(X_i^i)^p}{i!} = 0 \ \forall i \geq 0$$

ce qui est impossible.

Inversion pour le Shuffle dans $A_{rat}[X]$

Soit $a = \sum\limits_{n\geq 0} a_n X^n$ une série rationnelle à coefficients dans A. Il existe un entier n_0 tel que $\forall\ n \geq n_0$ les coefficients a_n s'écrivent :

$$a_n = \sum_{1\leq i\leq r} P_i(n)\alpha_i^n$$

les P_i sont des polynômes et les α_i des nombres algébriques

$$\forall\ 1 \leq i \leq r.$$

Sans perte de généralité on peut supposer $n_0 = 0$, d'où

$$\ell(a) = \sum_{n\geq 0}\Big(\sum_{1\leq i\leq r} P_i(n)\frac{\alpha_i^n}{n!}\Big)X^n.$$

Pour tout i $1 \leq i \leq r$ soit r_i le degré du polynôme P_i. Par récurrence sur les r_i il est facile de voir que :

$$\ell(a) = \sum_{1 \leq i \leq r} A_i(X) e^{\alpha_i X}$$

où pour tout $i \leq i \leq r$, $A_i(X)$ est un polynôme de degré r_i. Il est immédiat que le Shuffle de deux séries rationnelles est une série rationnelle.

L'inverse d'une série rationnelle pour le Shuffle n'est pas nécessairement une série rationnelle comme le montre le contre-exemple suivant :

Soit $A = \mathbb{Z}$, $a = 1 + X$; $b = \sum_{n \geq 0} (-1)^n \cdot n! X^n$ d'où $a \sqcup\!\sqcup b = 1$ or la série b n'est pas rationnelle.

PROPOSITION III. — *Une série rationnelle est inversible pour le Shuffle si et seulement si elle est de la forme :*

$$a = \frac{a_0}{1 - \alpha X} \quad ou \quad a_0 \neq 0.$$

Démonstration :

Il est immédiat que si la série a est de la forme :

$$a = \frac{a_0}{1 - \alpha X} \quad \text{ou} \quad a_0 \neq 0$$

la série $b = \frac{a_0^{-1}}{1 + \alpha X}$ est telle que :

$$(a \sqcup\!\sqcup b, X^n) = \Big(\sum_{0 \leq p \leq n} C_n^p (-1)^p \Big) \alpha^n = 0 \quad \text{si} \quad n \geq 1$$

$$\text{et} \quad (a \sqcup\!\sqcup b, X^0) = 1.$$

Réciproque :

Soient $a = \sum_{n \geq 0} a_n X^n$ et $b = \sum_{n \geq 0} b_n X^n$ deux séries rationnelles telles que $a \sqcup\!\sqcup b = 1$ si

$$a_n = \sum_{1 \leq i \leq r} P_i(n) \alpha_i^n \quad \text{et} \quad b_n = \sum_{1 \leq j \leq t} Q_j(n) \beta_j^n$$

alors :

$$\ell(a) = \sum_{1\leq i\leq r} A_i(X)e^{\alpha_i X} \quad \text{et} \quad \ell(b) = \sum_{1\leq j\leq t} B_j(X)e^{B_j(X)}$$

d'où

$$\ell(a \sqcup\!\sqcup b) = \ell(a) \times \ell(b) = \sum_{1\leq i,j\leq \sup .r,t} A_i(X)B_j(X)e^{(\alpha_i+\beta_j)X} = 1.$$

Etant donnée l'unicité de l'écriture d'un polynôme nous avons nécessairement :

$$\alpha_i + \beta_j = 0 \quad \forall i,j$$

$$A_i(X)B_j(X) \text{ sont de degré } 0 \ \forall i,j$$

la série a se réduit donc à la forme :

$$a = \frac{a_0}{1-\alpha X}$$

et la série b se réduit aussi à la forme

$$b = \frac{a_0^{-1}}{1+\alpha X}$$

ce qui termine la démonstration.

PROPOSITION IV. — *Soit a une série rationnelle et b une série algébrique alors $a \sqcup\!\sqcup b$ est algébrique.*

Démonstration :

Il suffit de se ramener au cas où la série rationnelle a est de la forme :

$$a = \frac{X}{1-\alpha X}$$

or pour tout entier $p \geq 1$ nous avons la relation :

$$\frac{X^p}{(1-\alpha X)^{p+1}} = \sum_{n\geq p} \frac{n!}{p!(n-p)!}\alpha^{n-p}X^n$$

d'où

$$\frac{X}{1-\alpha X} \sqcup\!\sqcup b = \frac{1}{1-\frac{X}{\alpha}} b \cdot \left(\frac{X}{1-\frac{X}{\alpha}}\right) \odot \sum_{n\geq 1} \alpha^{n-1} X^n$$

où $\odot$ désigne le produit de Hadamard si a est une série rationnelle ayant des pôles d'ordre ≥ 2. Il suffit de remarquer que les pôles d'ordre ≥ 2 proviennent des pôles d'ordre 1 par dérivation successives. Or la dérivation d'une série algébrique d est le produit de Hadamard d'une série rationnelle par une série algébrique.

Par contre le Shuffle de deux séries algébriques n'est pas algébrique dans tous les cas.

Inversion pour le Shuffle dans $A_{rat} \ll X \gg$

Soit $X = (x_1, x_2, \cdots, x_p)$ où $p \geq 2$ un alphabet fini et $\mathbb{Z} \ll X \gg$ l'algèbre large du monoïde libre X^* sur $\mathbb{Z}$.

Soient $a = \sum_{f \in X^*} (a, f) f$ et $b = \sum_{f \in X^*} (b, f) f$ deux éléments de $A \ll X \gg$.

Si f est un mot de longueur n où $n \geq 1$.

$$f = x_{i_1} x_{i_2} \cdots x_{i_n} \quad \text{où} \quad x_{i_j} \in X \; \forall 1 \leq j \leq n$$

soit $K = (i_1 i_2 \cdots i_n)$ la suite ordonnée qui lui est associée.

Par définition le coefficient de f dans $a \sqcup\!\sqcup b$ s'écrit :

$$(a \sqcup\!\sqcup b, f) = \sum_{0 \leq s \leq n} (a, x_j, \cdots, x_{j_s})(b, x_{j_{s+1}} - x_{j_n})$$

pour toutes les décompositions ordonnées de la suite K.

THÉORÈME I. — *Si $a, b \in A_{rat} \ll X \gg$ alors la série $a \sqcup\!\sqcup b \in A_{rat} \ll X \gg$.*

Démonstration :

Soit x une lettre de l'alphabet X, le mot xf admet la décomposition en lettres de X :

$$xf = x x_{i_1} \cdots x_{i_n}$$

donc le coefficient du mot xf dans la série $a \sqcup\!\sqcup b$ s'écrit

$$(I) \qquad \begin{aligned}(a \sqcup\!\sqcup b, xf) = &\sum_{0\le s\le n}(a, xx_j, \cdots, x_{j_s})(b, x_{j_{s+1}} - x_{j_n}) \\ &+ \sum_{0\le s\le n}(a, x_j - x_{js})(b, xx_{j_{s+1}} \cdots x_{j_n}).\end{aligned}$$

La série a étant rationnelle soit μ une représentation du monoïde libre X^* dans l'anneau des matrices $M_N(A)$ qui lui est associée c'est-à-dire telle que l'on ait :

$$a(f) = (\mu f)_{1,N} \cdot \forall f \in XX^*.$$

De même la série b étant rationnelle, soit γ une représentation de X^* dans $M_R(A)$ qui lui est associée [S(1)].

Soit

$$(b, f) = (\gamma f)_{1,R} \quad \forall f \in XX^*.$$

La relation (I) s'écrit aussi :

$$\begin{aligned}(a \sqcup\!\sqcup b, xf) = &\sum_{\substack{0\le s\le n\\ 1\le j\le N}}(\mu x)_{1,j}(\mu x_j, \cdots, \mu x_{j_s})_{JN}(\gamma, x_{j_{s+1}} \cdots \gamma x_{jn})_{1,R} \\ &+ \sum_{\substack{0\le s\le n\\ 1\le j\le R}}(\mu x_{j_1} \cdots \mu x_{j_s})_{1N}(\gamma x)_{1,j}(\gamma x_{j_{s+1}} - \gamma_{jn})_{j,R}\end{aligned}$$

soit les séries

$$\begin{cases} a'_j &= a_j \sqcup\!\sqcup b \\ b'_j &= a \sqcup\!\sqcup b_j \\ a''_{j,j'} &= a_j \sqcup\!\sqcup b_{j'} \end{cases}$$

où

$$\begin{cases} a_j &= \sum_f (\mu f)_{jN} f \\ b_j &= \sum_f (\gamma f)_{j,R} f \end{cases}$$

la relation (I) s'écrit donc :

$$(a \sqcup\!\sqcup b, xf) = \sum_{1\le j\le N}(\mu x)_{1,j}(a'_j, f) + \sum_{1\le j\le R}(\gamma x)_{1,j}(b'_j, f).$$

Plus généralement nous avons le système suivant :

$$(II) \qquad \begin{cases} (a'_j, xf) &= \sum_{1\le j'\le N}(\mu x)_{j,j'}(a'_{j'}, f) &+ \sum_{1\le j'\le m}(\gamma x)_{1,j'}(a''_{j,j'}, f) \\ (b'_j, xf) &= \sum_{1\le j'\le N}(\mu x)_{1,j'}(a''_{j',j}, f) &+ \sum_{1\le j'\le R}(\gamma x)_{j,j'}(b'_j, f) \\ (a_{j,j'}, f) &= \sum_{1\le K\le N}(\mu x)_{j,K}(a''_{K,j'}, f) &+ \sum_{1\le \ell\le R}(\gamma x)_{j',\ell}(a''_{j,\ell}, f) \end{cases}$$

La relation (II) écrite pour toutes les lettres de l'alphabet X démontre que les séries $a''_{j,j'}$ sont solutions d'un système linéaire $\forall j, j'$, $1 \leq j \leq N$, $1 \leq j' \leq R$.

En particulier, la série $a \sqcup\!\sqcup b$ est rationnelle.

En prenant pour série rationnelle b la série caractéristique $\sum_{f \in X^*} f$ nous voyons que si la série a est rationnelle la série :

$$a \sqcup\!\sqcup b = \sum_f \Big(\sum_{\substack{\text{décompositions} \\ \text{de } f}} a, x_{i_1} - x_{i_s} \Big) f$$

est rationnelle.

Les deux propositions I et II s'étendent sans difficultés à l'algèbre des polynômes $A < X >$. Le raisonnement se fait par récurrence sur la longueur des mots appartenant au support des polynômes.

Soit $a = \sum_f (a, f) f$ une série rationnelle inversible pour le shuffle. Soit b son inverse.

Nous avons le théorème suivant qui est l'extension de la proposition III.

THÉORÈME II. — *Une série rationnelle est inversible pour le Shuffle si et seulement si la représentation qui lui est associée laisse stable un sous-espace de dimension* 1 *et si pour toute lettre* $x \in X$ *la série rationnelle* $a_x = \sum_{n \geq 0} (a, x^n) T^n$ *est inversible pour le Shuffle.*

Avant de démontrer le théorème II démontrons un lemme.

LEMME I. — *Soit* $a = \sum_f (a, f) f$ *une série rationnelle inversible pour le Shuffle alors la représentation* μ *qui lui est associée est réductible et l'espace laissé stable par* μ *est de dimension* 1.

En particulier dans le cas où la représentation est de degré 2, *elle est triangulisable.*

Démonstration :

Sans perte de généralité on peut se limiter au cas où l'alphabet X se réduit à 2 lettres x et y.

Pour toute lettre x (ou y) soit $a_x = \sum_{n \geq 0} (a, x^n) T^n$ la série rationnelle

à une variable et soit

$$b_x = \sum_{n\geq 0}(b, x^n)T^n \text{ son inverse pour le Shuffle}$$

le coefficient de x^n dans $a \sqcup\!\sqcup b$ est le même que celui de x^n dans $a_x \sqcup\!\sqcup b_x$ dans les 2 cas il est égal à :

$$\sum_{0\leq p\leq n} C_n^p(a, x^p)(b, x^{n-p}).$$

Donc pour toute lettre soit x (soit y) la série a_x (soit a_y) est inversible pour le Shuffle.

Donc si $\alpha_1, \alpha_2 \cdots \alpha_p$ sont les valeurs propres distinctes de la matrice μx nous avons pour tout entier $n \geq 0$

$$(a, x^n) = TrP\mu x^n = a_1\alpha_1^n + a_2\alpha_2^n + \cdots + a_p\alpha_p^n = a_1\alpha_1^n$$

Si la série a s'écrit

$$a = \sum_f (a, f)f = \sum_f (TrP\mu f)f$$

d'où la relations :

$$a_2\alpha_2^n + \cdots + a_p\alpha_p^n = 0 \quad \forall n \geq 0.$$

En écrivant les équations (I) et en considérant le système qui leur est associée les inconnues étant les a_i et les coefficients les α_i^n $2 \leq i \leq p$ nous voyons que le déterminant des coefficients est un Van Der Monde. Donc il n'est pas nul. La seule solution est donc la solution triviale :

$$a_2 = a_p = 0$$

d'où $TrP = a_1$.

De mêm si la série b s'écrit :

$$b = \sum_f (TrQ\gamma f)f$$

$$TrQ = a_1^{-1} \quad TrQ(\gamma x)^n = (-1)^n a_1^{-1}\alpha_1^n.$$

Par récurrence sur la longueur des mots $f \subset XX^*$ nous allons démontrer que $TrP\mu f$ ne dépend que du nombre d'occurences des lettres x et y.

Examinons tout d'abord le cas des mots les plus simples de longueur 2. Soient xy et yx

$$(II)\quad \begin{cases} (a \sqcup\!\sqcup b, xy) = b_0 TrP\mu x\mu y + a_0 TrQ\gamma x\gamma y + TrP\mu x \cdot TrQ\mu y + \\ \qquad\qquad TrP\mu y \cdot TrQ\mu x = 0 \\ (a \sqcup\!\sqcup b, yx) = b_0 TrP\mu y\mu x + a_0 TrQ\gamma y\gamma x + \\ \qquad\qquad TrP\mu x TrQ\gamma y + Tr \cdot P\mu y TrQ\mu x = 0 \end{cases}$$

$$\text{ou } a_0 = TrP = a_1 \quad b_0 = TrQ = a_1^{-1}$$

ou sur les lettres $x \in X$ γx coïncide avec $-\mu x$ d'où en explicitant les relations tirées de II.

$$\begin{cases} - \quad Tr(a_1^{-1}P + a_1 Q)\mu x\mu y = TrP\mu x TrQ\mu y + TrP\mu y TrQ\ \mu x \\ - \quad Tr(a_1^{-1}P + a_1 Q)\mu y\mu x = TrP\mu x TrQ\mu y + TrP\mu y TrQ\mu x \end{cases}$$

$$\text{ou } a_1^{-1}P + a_1 Q \neq \lambda I \quad \text{où} \quad \lambda \in \mathbb{R}^*.$$

Donc si α_1 est la valeur propre de μx qui intervient dans la récurrence liant les (a, x^n) et α_1 la valeur propre intervenant dans celle liant les (a, y^n) nous avons :

$$\begin{cases} - \quad Tr(a_1^{-1}P + a_1 Q)\mu x\mu y = 2\alpha_1\alpha_1' \\ - \quad Tr(a_1^{-1}P + a_1 Q)\mu y\mu x = 2\alpha_1\alpha_1' \end{cases}$$

Plus généralement soit f un mot de XX^* et soit fx (resp. fy) le nombre d'occurences de la lettre x (resp. y) dans le mot f d'où :

$$(a \sqcup\!\sqcup b, f) = (-1)^{|f|_y} \cdot TrP\mu x^{|f|_x} TrQ(\mu y)^{|f|_y} +$$
$$+(-1)^{|f|_x} \cdot TrP(\mu y)^{|f|_y} \cdot TrQ(\mu x)^{|f|_a} + (-1)^{|f|} a_1 TrQ\mu f + a_1^{-1} TrP\mu f +$$
$$+ \sum_{\substack{f' \neq x^{|f|_x}{}_{;y}{}^{|f|_y} \\ g'' \neq y^{|f|_y} \\ f' \neq f \\ g'' \neq f}} (-1)^{|g|} TrP\mu f' \cdot TrQ\mu y'' = 0$$

ou

$$\begin{cases} TrP(\mu f)^{|f|_x} = a_1 \alpha_1^{|f|_x} \\ TrP(\mu y)^{|f|_y} = a_1 \alpha_1^{|f|_y} \end{cases} \qquad \begin{cases} TrQ\mu x^{|f|_x} = a_1^{-1} \alpha_1^{|f|_x} \\ TrQ\mu y^{|f|_y} = a_1^{-1} \alpha_1'^{|f|_y} \end{cases}$$

d'où

$$(-1)^{|f|}a_1 TrQ\mu f + a_1^{-1}TrP\mu f +$$
$$+ \sum_{\substack{f'\neq x^{|f|_x},y^{|f|_y} \\ f'\neq f \\ g''\neq f}} (-1)^{|g''|}TrP\mu f' \cdot TrQ\mu g'' =$$
$$= \left[(-1)^{|f|_y-1} + (-1)^{|f|_x-1}\right]\alpha_1^{|f|_x} \cdot \alpha_1'^{|f|_y}$$

ou les mots f' et g'' sont strictement plus courts que le mot f dans toute décomposition restante d'où par récurrence :

$$(III) \quad Tr\Big((-1)^{|f|}a_1 Q + a_1^{-1}P\Big)\mu f = c\alpha_1^{|f|_x}\alpha_1'^{|f|_y} \text{ où } c = (-1)^{|f|} + 1$$

si $|f| = 2p$ d'après ce que nous avons vu précédemment :

$$a_1 Q + a_1^{-1}P \neq \lambda I \quad \text{où} \quad \lambda \in \mathbb{R}^*$$

donc l'expression (III) a un sens et permet d'affermer que : $\alpha_1^{|f|_x}\alpha_1^{|f|_y}$ est une valeur propre de la matrice μf si $|f| = 2p+1 \quad c = 0$. Supposons que le mot f s'écrive :

$$f = f'x$$

d'où

$$\Big[- TrP\mu f' \cdot TrQ\mu x = - \sum_{\substack{f_1\neq f' \\ f_1\neq x^{|f|_x},y^{|f|_y}}} (-1)^{(g_1'')}TrP\mu f_1 \cdot TrQ\mu g_1''$$

de même en examinant le mot : fx nous avons :

$$\begin{cases} Tr(a_1 Q + a_1^{-1}P)\mu f\mu x = 2\alpha_1^{|f|_x+1}\alpha_1'^{|f|_y} \\ Tr(a_1 Q + a_1^{-1}P)\mu f\mu x - TrP\mu f TrQ\mu x + \\ +(-1)^{|f|}TrP\mu x TrQ\mu f = C_1\alpha_1^{|f|_x+1}\alpha'^{|f|_y} \end{cases}$$

d'où

$$(-TrP\mu f)a_1^{-1}\alpha_1 - a_1\alpha_1 TrQ\mu f = d\alpha_1^{|f|_x+1}\alpha_1'^{|f|_y}$$

d'où :

$$Tr(-a_1^{-1}P - a_1 Q)\mu f = d\alpha_1^{|f|_x}\alpha_1'^{|f|_y}$$

donc $\alpha_1^{|f|_x}\alpha_1'^{|f|_y}$ est bien une valeur propre de la matric μf.

Soit $\mathcal{A}$ l'algèbre engendrée par la représentation μ dans $M_N(\mathbb{C})$ et soit A une matrice de $\mathcal{A}$.

D'où $Tr(a_1^{-1}Q + a_1P)$ A est un polynôme en α_1 et α_1' qui est une somme de monomes du genre :

$$\alpha_1^m \alpha_1'^{m'} \text{ (modulo les constantes)}$$

où m et m' sont des entiers qui ne dépendent que des occurences des matrices μx et μy dans les différents monomes intervenant dans l'écriture de la matrice A.

Donc l'algèbre $\mathcal{A}$ est réductible sur $\mathbb{C}$. Il existe donc une base de $M_N(\mathbb{C})$ dans laquelle toute matrice μf s'écrit :

$$\mu f = \begin{pmatrix} A_f & * \\ 0 & B_f \end{pmatrix}.$$

A_f étant une matrice carrée $p \times p$ $p \neq (N, 0)$

B_f étant une matrice carrée $(N-p) \times (N-p)$.

En tenant compte du fait que $\alpha_1^{|f|_x} \alpha_1'^{|f|_y}$ est une valeur propre de la matrice μf nous voyons que la représentation μ laisse stable un espace de dimension 1. Il existe donc une base de $M_N(\mathbb{C})$ dans laquelle les matrices μx et μy s'écrivent respectivement :

$$\mu x = \begin{pmatrix} \alpha_1 & * \\ 0 & B_x' \end{pmatrix} \quad \mu y = \begin{pmatrix} \alpha_2' & * \\ 0 & B_y' \end{pmatrix}$$

ce qui termine la démonstration du lemme 3 et aussi que la condition du théorème II est nécessaire.

Réciproque :

Soit $a = \sum_f (Trf\mu f)f$ une série rationnelle telle que la représentation μ qui lui est associée laisse stable un espace de dimension 1 et telle que pour toute lettre $x_i \in X$ la série rationnelle à une variable :

$$a_{x_i} = \sum_{n \geq 0} (a, x_i^n) T^n$$

est inversible pour le Shuffle ; alors la série a est inversible pour le Shuffle.

Démonstration :

Par récurrence sur la longueur des mots f démontrons que :

$$(a \sqcup\!\sqcup b, f) = 0 \quad \forall f \in XX^*$$

la série b étant définie sur les lettres de l'alphabet X par :

$$b = \sum_f (TrQ\gamma f)f \quad \text{où} \quad \gamma x_i = -\mu x_i \; \forall x_i \in X$$

$$\text{et } TrQ = (TrP)^{-1}$$

Prenons comme 1er vecteur de base le vecteur laissé stable par la représentation μ. Dans cette base la matrice μf s'écrit pour tout mot f de XX^*

$$\mu f = \begin{pmatrix} \mu_1 f & * \\ 0 & B_f \end{pmatrix}$$

la matrice P s'écrit dans cette base :

$$P = \begin{pmatrix} a_{11} & * \\ 0 & P' \end{pmatrix}$$

d'où $TrP\mu f = a_{11}\mu_1 f$

$$TrP' = 0 \quad TrP'B_f = 0 \; \forall f$$

la matrice Q s'écrit :

$$Q = \begin{pmatrix} a_{11}^{-1} & * \\ 0 & Q' \end{pmatrix}$$

où $TrQ\mu f = a_{11}^{-1}\mu_1 f$

$$TrQ' = 0 \quad \text{et} \quad TrQ'Bf = 0 \; \forall f$$

Soit x_i une lettre de l'alphabet X d'où

$$\begin{aligned} (a \sqcup\!\sqcup b, x_i) &= TrQTrP\mu x_i + TrPTrQ\gamma x_i \\ &= a_{11}^{-1}a_{11} \cdot \mu_1 x_i - a_{11}a_{11}^{-1}\mu_1 x_i = 0 \end{aligned}$$

soit f un mot de XX^* admettant la décomposition :

$$f = x_{i_1}x_{i_2}\cdots x_{i_n} \text{ en lettres de l'alphabet } X$$

soit x_ℓ une lettre de l'alphabet X d'où :

$$(a \sqcup\!\sqcup b, fx_\ell) = \sum_{0\le s\le n} (a, x_{j_1} - x_{j_s})(b, x_{j_{s+1}} - x_{j_{n-s}} x_\ell) +$$

$$+ \sum_{0\le s\le n} (a, x_{j_1} - x_{js} x_\ell)(b, x_{j_{s+1}} - x_{j_n})$$

$$= TrP \cdot TrQ \cdot \sum_{s\le n} \lambda_{j_1} \cdots \lambda_{j_s} (-1)^{n-s+1} \cdot \lambda_{j_{s+1}} \cdots \lambda_{j_{n-s}} \lambda_{x_e ll}$$

$$+TrPTrQ \cdot \textstyle\sum_{s\le n} \lambda_{j_1} \cdots \lambda_{j_s} \lambda_{x_\ell} (-1)^{n-s} \cdot \lambda_{j_{s+1}} \cdots \lambda_{j_{n-s}}$$

les λ_{j_i} sont les valeurs propres des matrices μx_{j_i}. En fait

$$\lambda_{j_i} = \mu_1 x_{j_i}$$

or par récurrence sur $|f|$ nous avons supposé que :

$$(a \sqcup\!\sqcup b, f) = 0$$

d'où

$$(a \sqcup\!\sqcup b, fx) = \lambda_{x_\ell}\Big(\textstyle\sum_{s\le n} \lambda_{j_1} - \lambda_{j_s}(-1)^{n-s+1} \cdot_{j_{s+1}} \cdots \lambda_{j_{n-s}}\Big) +$$

$$+\lambda_{x_\ell}\Big(\sum_{s\le n} \lambda_{j_1} - \lambda_{j_s}(-1)^{n-s} \lambda_{j_{s+1}} \cdots \lambda_{j_{n-s}}$$

$$= -\lambda x_\ell\Big(\sum_{s\le n} \lambda_{j_1} \cdots \lambda_s (-1)^{n-s} \lambda_{j_{s+1}} \cdots \lambda_{j_{n-s}}$$

$$- \sum_{s\le n} \lambda_{j_1} \cdots \lambda_{j_s} (-1)^{n-s} \lambda_{j_{s+1}} \cdots \lambda_{j_{n-s}}\Big)$$

$$= 0$$

ou $(a \sqcup\!\sqcup b, \varepsilon) = 1$. SI ε est le mot neutre de X^* ce qui termine la démonstration de la réciproque.

THÉORÈME III. — *Le Shuffle d'une série rationnelle et d'une série algébrique est algébrique.*

Démonstration :

Soit $a = \sum_f (a, f) f$ une série rationnelle et $b = \sum_f (b, f) f$ une série algébrique, on peut supposer a et b sans terme constant, car les séries :

$$a \sqcup\!\sqcup b \text{ et } [a - (a, \varepsilon)] \sqcup\!\sqcup (b - [b, \varepsilon]) \text{ sont de même nature.}$$

Soit $a = \sum_f (\mu f)_{1\mathbb{N}} f$ où μ est une représentation du monoïde libre X^* dans l'algèbre $M_N(\mathbb{R})$.

Si $f \in XX^*$ f admet la décomposition en lettres de X

$$f = x_{i_1} \cdots x_{i_n}$$

d'où $(a \sqcup\!\sqcup b, f) = \sum_{0 \le s \le n} (\mu x_{j1} \cdots \mu x_{j_s})_{1,N} (b, x_{js+1} - x_{jn})$.

Pour toute lettre $x \in X$, nous avons :

$$(I) \qquad \begin{aligned} (a \sqcup\!\sqcup b, xf) = & \sum_{0 \le s \le n} (\mu x \mu x_{j_1} \cdots \mu x_{js})_{1N} (b, x_{j_{s+1}} \cdots x_{j_n} + \\ & + \textstyle\sum_{0 \le s \le n} (\mu x_{j_1} \cdots \mu x_{j_s})_{1N} (b, x x_{j_{s+1}} \cdots x_{jn}) \end{aligned}$$

ou $(\mu x \mu x_{j_1} \cdots \mu x_{j_s})_{j,N} = \sum_{1 \le K \le N} (\mu x)_{1,K} (\mu x_{j_1} \cdots \mu x_{j_s})_{k,N}$.

En posant pour tout indice K $1 \le K \le N$.

$$a''_K = \sum_{f \in X^*} (\mu f)_{K,N} f \quad \text{et} \quad a'_K = a''_k \sqcup\!\sqcup b$$

la relation (I) s'écrit :

$$(a \sqcup\!\sqcup b, xf) = \sum_{1 \le K \le N} (\mu x)_{1,K} (a''_k \sqcup\!\sqcup b, f) + (a \sqcup\!\sqcup xb, xf).$$

Plus généralement pour tout indice K $1 \le K \le N$ nous avons :

$$(II) \qquad (a''_K \sqcup\!\sqcup b, xf) = \sum_{1 \le j' \le N} (\mu x)_{K,j'} (a''_{j'} \sqcup\!\sqcup b, f) + (a''_K \sqcup\!\sqcup xb, xf)$$

la série a étant rationnelle est solution du système linéaire suivant :

$$\begin{cases} p = (p_0 p_1 \cdots p_N) \text{ où pour tout } j \ 0 \le j \le N \\ p_j = q_{j_0} + \sum_{1 \le j' \le N} q_{j,j'} \cdot y_{j'} \\ q_{j,j'} = \sum_{x \in X} (\mu x)_{j,j'} \cdot x \\ q_{j_0} = \sum_{x \in X} (\mu x)_{jN} x \end{cases}$$

les $(y_j)_{1 \le j \le N}$ étant les variables pour lesquelles on fait les substitutions.

La série b étant algébrique est donc solution d'un système propre R à M variables (y''_j) $1 \leq j \leq M$ sur l'alphabet X. Soit

$$R = (R_1 R_2 \cdots R_M)\ [S(2)]$$

$$\text{où } (R_i, y_{j''}) = 0 \quad \forall\, 1 \leq i \leq M \quad 1 \leq j'' \leq M.$$

Donc tout série $a''_j \sqcup\!\sqcup b$ est une composante du système algébrique S à MN variables sur l'alphabet X où

$$S = (S_{ij})_{\substack{1 \leq i \leq N \\ 1 \leq j \leq M}}$$

$$\text{où } S_{ij} = p_i \sqcup\!\sqcup R_j$$

les variables étant écrites formellement :

$$y_{ij} = y'_i \sqcup\!\sqcup y''_j \quad 1 \leq i \leq N \quad 1 \leq j \leq M$$

ce qui signifie que l'on calcule le Shuffle des coefficients de y'_i et de y''_j dans les expressions S_{ij}.

Le système $(S_{ij})_{\substack{1 \leq i \leq N \\ 1 \leq j \leq M}}$ est un système propre. En effet :

$$p_i \in R^*_{rat} < X >$$

$$(R_i, y_{j'}) = 0 \quad \forall j, j' \quad 1 \leq j, j' \leq M$$

$$\text{d'où} (p_i \sqcup\!\sqcup R_j,\ y'_K \sqcup\!\sqcup y''_\ell) = 0 \quad \begin{matrix} \forall & 1 \leq i, K \leq N \\ \forall & 1 \leq j, \ell \leq M \end{matrix}$$

Donc pour tout indice K $a''_K \sqcup\!\sqcup b$ est algébrique. En particulier pour $K = 1$ la série $a \sqcup\!\sqcup b$ est algébrique.

Je remercie beaucoup M. le Professeur BENZAGHOU de l'Université d'Alger pour son aide. En effet dans le cas où l'algèbre des séries formelles est commutative, l'application ℓ définie de l'algèbre $A[X]$ munie du Shuffles dans l'algèbre $A[X]$ munie du produit de Cauchy m'a permis de simplifier les démonstrations. Les démonstrations que j'avais faites auparavant étaient basées sur la relation :

$$C_n^p = C_{n-1}^p + C_{n-1}^{p-1}.$$

Il reste à démontrer la conjecture suivante :

Si l'inverse pour le Shuffle d'une série algébrique est algébrique, alors cette série est rationnelle.

Il est connu qu'en caractéristique $p \neq 0$. Le Shuffle de deux séries algébriques est algébrique. En caractéristique zéro, le Shuffle de deux séries algébriques n'est pas algébrique.

BIBLIOGRAPHIE

[G(1)] K. GÉRARDIN. — *Thèse d'Etat*, Paris 7, (1979).

[S(1)] M.P. SCHÜZENBERGER. — On the definition of the family of automatic , *Inf. and control.* **4**, (1961), 245-250.

[S(2)] M.P. SCHÜZENBERGER. — On a theorem of Junsen, *Proceedings of the A.M.S.* **13, n° 6**, (1962), 885-890.

K. LAMÈCHE
12, rue Beccaria
75012 PARIS

DISTRIBUTION DES SOUS-SOMMES D'UNE PARTITION

Jean-Louis NICOLAS *

Nous désignerons par $p(n)$ le nombre de partitions sans restriction de n, et par $r(n,m)$ le nombre de partitions de n dont les sommants sont $\geq m$. Plus généralement si $A = \{a_1, \ldots, a_k\}$, nous noterons $r(n,A)$ le nombre de partitions de n dont aucun sommant n'appartient à A. Nous dirons qu'une partition de n :

$$n = n_1 + n_2 + \cdots + n_t$$

représente a, s'il existe une sous somme $n_{i_1} + n_{i_2} + \cdots + n_{i_j}$ égale à a. Nous définissons $R(n,a)$ comme le nombre de partitions de n qui ne représentent pas a.

On voit ainsi que :

$$r(n,m) = r(n, \{1,2,\ldots,n-1\})$$

$$R(n,a) \geq r(n,a+1) \tag{1}$$

$$R(n,a) \geq r(n, \{1,2,\ldots,[a/2],a\}) \tag{2}$$

en notant $[x]$ la partie entière de x.

Nous considérons aussi les partitions de n en sommants distincts. Dans ce cas les notations ci-dessus seront remplacées par $q(n)$, $\rho(n,m)$, $\rho(n,A)$, $Q(n,a)$.

Nous nous proposons dans cet exposé de faire le point sur les diverses quantités ci-dessus. Fin 1986, J. Dixmier a attiré notre attention sur ce sujet en voulant évaluer le nombre d'invariants des formes binaires (cf. [DNE]). Ce nombre est en effet minoré par le nombre de solutions d'une équation diophantienne proche de celles qui interviennent dans la théorie des partitions.

Au paragraphe 3, nous étudierons le nombre de couples de partitions de n sans sous-sommes communes (à part 0 et n).

* Ce travail a reçu l'aide du CNRS, Greco 060 (calcul formel), PRC Math-Info, PICS France USA n° 48b

Les résultats mentionnés ci-dessous sont en grande partie le fruit d'une collaboration avec J. Dixmier, P. Erdös et A. Sárközy.

1. Estimation de $r(n,m)$ et de $\rho(n,m)$

On définit $p(n,m)$ comme le nombre de partitions de n en sommants $\leq m$, ou ce qui revient au même comme le nombre de partitions de n en au plus m sommants.

On a :

$$\begin{aligned} r(n,m) &= r(n,m+1) + r(n-m,m) \\ r(n,n) &= 1 \end{aligned}$$

ce qui permet de calculer $r(n,m)$ par récurrence.

On a également (cf. [GGM], p. xiii) :

$$r(n,m) = \sum_{t=0}^{[n/m]} p(n-tm,t) \tag{3}$$

et il est facile de voir que

$$r(n,m) \leq p(n,[n/m]). \tag{4}$$

En utilisant (3), Gupta (cf. [G]) a donné une estimation asymptotique de $r(n,m)$ valide pour $n = O(m \log m)$.

J. Herzog a donné dans sa thèse (cf. [H1], p. 57) l'estimation valable pour $m = O(n^{3/8}(\log n)^{1/4})$:

$$\begin{aligned} \log r(n,m) = \pi\sqrt{\tfrac{2}{3}}\,\sqrt{n} - \tfrac{1}{2}m\log n + m\log m \\ -m\left(1+\log\tfrac{\sqrt{6}}{\pi}\right) + O\left(n^{1/4}\sqrt{\log n}\right). \end{aligned} \tag{5}$$

Ce résultat est obtenu comme application d'un théorème Taubérien.

Il est démontré dans ([DN1]), que l'on a uniformément pour $1 \leq m \leq n^{1/4}$

$$r(n,m) = p(n)\left(\frac{\pi}{\sqrt{6n}}\right)^{m-1}(m-1)!(1+O(m^2/\sqrt{n})). \tag{6}$$

Cette formule est étendue dans [DN2], où l'on montre que, pour $0 < \varepsilon < 1/3$ et $m \leq n^{1/3-\varepsilon}$, on a :

$$r(n,m) \sim p(n)(m-1)!\left(\frac{C}{2\sqrt{n}}\right)^{m-1}\exp\left(-\left(\frac{C}{8}+\frac{1}{2C}\right)\frac{m^2}{\sqrt{n}}\right), \tag{7}$$

où $C = \pi\sqrt{\frac{2}{3}}$.

Pour montrer la cohérence avec (5) rappelons la formule de Hardy-Ramanujan (cf. [HR]) :

$$p(n) \sim \frac{1}{4\sqrt{3}n} \exp(C\sqrt{n}). \tag{8}$$

Dans [ENS 1], il est démontré qu'il existe $\alpha > 0$ tel que quand $n \longrightarrow +\infty$, on a uniformément pour $1 \leq m \leq \alpha\sqrt{n}$

$$\exp\Big(O\Big(\frac{m^2}{\sqrt{n}}\Big)\Big) \leq \frac{r(n,m)}{p(n)\Big(\frac{\pi}{\sqrt{6n}}\Big)^{m-1}(m-1)!} \leq 1 + O\Big(\frac{1}{\sqrt{n}}\Big) \tag{9}$$

Enfin, dans [DN2], le cas $m \sim \lambda\sqrt{n}$ est étudié. Il est commode de poser pour x réel > 0 :

$$r(n,x) = r(n,\lceil x\rceil) \quad \text{et} \quad p(n,x) = p(n,[x]),$$

où $\lceil x\rceil = \min\{n\ ;\ n \in \mathbb{Z},\ n \geq x\}$; il est démontré que pour $\lambda > 0$ fixé il existe une fonction g telle que l'on ait pour $n \longrightarrow \infty$,

$$\log r(n, \lambda\sqrt{n}) \sim g(\lambda)\sqrt{n}. \tag{10}$$

La démonstration de (10) utilise (3) et les résultats de Szekeres (cf. [Sz1] et [Sz2])

$$\log p(n, \lambda\sqrt{n}) \sim f(\lambda)\sqrt{n}.$$

La fonction g est analytique pour $\lambda > 0$, vérifie une équation différentielle du second ordre, et il est donné dans [DN2] les développements asymptotiques de $g(\lambda)$ au voisinage de 0 et de l'infini, calculé par les systèmes de calcul forme MAPLE et MACSYMA.

Dans le cas des partitions sans répétition, la quantité $\rho(n,m)$ a été semble-t-il introduite pour la première fois dans [ES2], où il est démontré p. 433, que pour $m \leq n^{1/5}$, on a :

$$\rho(n,m) \sim q(n)2^{-m}, \tag{11}$$

en utilisant l'intégration complexe de la fonction génératrice. Rappelons ici que Hardy et Ramanujan ont donné pour $q(n)$ l'estimation :

$$q(n) \sim \frac{1}{4(3n^3)^{1/4}} \exp(\pi\sqrt{n/3}). \tag{12}$$

Dans [ENSz], il est démontré par des méthodes élémentaires que pour tout $n \geq 1$ et $1 \leq m \leq n$ on a :

$$\frac{q(n)}{2^{m-1}} \leq \rho(n,m) \leq \frac{1}{2^{m-1}} q\Big(n + \frac{m(m-1)}{2}\Big) \tag{13}$$

et

$$\rho(n,m) \leq \frac{1}{2^{m-2}} q\Big(n + \Big[\frac{m(m-1)}{4}\Big]\Big). \tag{14}$$

Il est aussi prouvé que pour $m = o\Big(\frac{n}{\log n}\Big)^{1/3}$, on a :

$$\rho(n,m) = (1+o(1))\frac{1}{2^{m-1}} q\Big(n + \Big[\frac{m(m-1)}{4}\Big]\Big). \tag{15}$$

Enfin, il est démontré que pour ε fixé, $0 < \varepsilon < 10^{-2}$, et $m \leq n^{3/8-\varepsilon}$, on a :

$$\rho(n,m) = (1+o(1))\frac{q(n)}{\prod\limits_{1 \leq j \leq m-1} \Big(1 + \exp\Big(-\frac{\pi j}{2\sqrt{3n}}\Big)\Big)}. \tag{16}$$

Dans [H2], J. Herzog a obtenu à l'aide d'un théorème taubérien l'estimation valable uniformément pour $m = o(\sqrt{n})$

$$\begin{aligned} \log \rho(n,m) = \pi\sqrt{\tfrac{n}{3}} - m\log 2 + \tfrac{\pi}{8\sqrt{3}}\tfrac{m^2}{\sqrt{n}} - \tfrac{\pi^2}{288}\tfrac{m^3}{n} \\ + O(m^4 n^{-3/2} + n^{1/4}\sqrt{\log n}). \end{aligned} \tag{17}$$

G. Freiman et J. Pitman, ont obtenu, dans [FP], par la méthode du col, une estimation valable pour :

$$1 \leq m \leq n(2\ \log n)^{-4}. \tag{18}$$

Soit $\sigma = \sigma(n,m)$ l'unique nombre réel tel que :

$$n = \sum_{j=m}^{n} \frac{j}{1+e^{\sigma j}}$$

et

$$B^2 = \sum_{j=m}^{n} \frac{j^2 e^{\sigma j}}{(1+e^{\sigma j})^2}.$$

Sous la condition (18), G. Freiman et J. Pitman démontrent :

$$\rho(n,m) \sim \frac{1}{\sqrt{2\pi B^2}} e^{\sigma n} \prod_{j=m}^{n} (1+e^{-j\sigma}). \tag{19}$$

Il est certainement possible, par une estimation précise de σ et B de déduire les formules (15) (16) et (17) de la formule (19). La même méthode devrait s'appliquer à $r(n,m)$.

Les méthodes utilisées pour étudier $r(n,m)$ et $\rho(n,m)$ se généralisent à $r(n,A)$ et $\rho(n,A)$. Dans [ENS1], il est démontré qu'il existe $\lambda_2 > 0$ tel que si $A = \{a_1, \ldots, a_k\}$ vérifie $s = a_1 + a_2 + \cdots + a_k \leq \lambda_2 n$ alors, quand $n \longrightarrow \infty$, on a :

$$\left(\exp\left(O\left(\frac{s}{\sqrt{n}}\right)\right)\right) \leq \frac{r(n,A)}{\left(\prod_{i=1}^{k} a_i\right) p(n) \left(\frac{\pi}{\sqrt{6n}}\right)^k} \leq 1 + O\left(\frac{1}{\sqrt{n}}\right). \tag{20}$$

Quant à $\rho(n,A)$, on trouve dans [ES3] le résultat suivant : Pour ε fixé, $0 < \varepsilon < 10^{-2}$, et pour k vérifiant $1 \leq k \leq n^{1/6-\varepsilon}$, on a :

$$\rho(n,A) = (1+o(1)) \frac{q(n)}{\prod_{1 \leq j \leq k} \left(1 + \exp\left(-\frac{\pi a j}{2\sqrt{3n}}\right)\right)}. \tag{21}$$

2. Estimation de $R(n,a)$ et de $Q(n,a)$

Premier cas : a fixé, $n \longrightarrow \infty$.

On désigne par $\Psi(a)$ la quantité $[a/2] + 1$. Dans [D1], J. Dixmier a démontré qu'il existe une constante $u(a)$ telle que :

$$R(n,a) \sim p(n) \left(\frac{\pi}{\sqrt{6n}}\right)^{\Psi(a)} u(a). \tag{22}$$

Les premières valeurs de $u(a)$ sont $u(1) = 1$, $u(2) = 4$, $u(3) = 3$, $u(4) = 16$. Une table de $u(a)$ pour $a \leq 20$ est donnée en appendice de [D1] et montre que $u(a)$ est croissante pour $3 \leq a \leq 20$. Mais nous verrons ci-dessous que cette propriété n'est pas vraie pour tout $a \geq 3$. La table montre aussi que $u(a)$ est un multiple de a pour $a \leq 20$. En fait, $u(a)$ est

divisible par le produit des diviseurs de a (cf. [D1], corollaire 4.26). De plus, J. Dixmier démontre dans [D1] que :

$$\text{(23)} \qquad \text{pour } a \text{ pair}, ([a/3]-1)!a^{a/6+3} \leq u(a) \leq 2^{a/2}a!/(a/2-1)!$$

$$\text{(24)} \qquad \text{pour } a \text{ impair}, ([a/3]-1)!a^{a/6+2} \leq u(a) \leq 2^{a/2}a!/(a/2)!$$

La différence de comportement de $u(a)$ entre les valeurs paires et impaires de a est précisée dans [D3] :

Lorsque a est impair tendant vers l'infini, $u(a)$ admet le développement asymptotique

$$\text{(25)} \qquad u(a) = (1.3.5. \ \ldots \ .a)(\alpha_0 + \frac{\alpha_1}{a} + \frac{\alpha_2}{a^2} + \frac{\alpha_3}{a^3} + \cdots)$$

où les α_i sont des entiers ≥ 0. On a $\alpha_0 = 1$, $\alpha_1 = 2$, $\alpha_2 = 24$.

Rappelons que :

$$\text{(26)} \qquad 1.3.5. \ \ldots \ .a = \frac{a^{a/2}}{e^{a/2}}\sqrt{2a}\Big(1 + \frac{1}{6a} + \cdots\Big).$$

Lorsque a est pair et $\geq a_0$, on a :

$$u(a) \leq \frac{a^{a/2}}{e^{a/2}} e^{-0.006a}.$$

La fonction $a \longmapsto u(a)$ oscille donc très rapidement lorsque a est grand. Par ailleurs les relations (23) et (24) entraînent que, pour a assez grand :

$$u(a) \geq \frac{a^{a/2}}{e^{a/2}} e^{-0.2a}.$$

Une étude similaire pourrait être faite pour $Q(n,a)$. Elle n'a, semble-t-il, pas encore été entreprise.

Deuxième cas : $1 \leq a \leq \lambda_0\sqrt{n}$.

Ce cas est étudié dans l'article [ENS1], où l'on montre : il existe $\lambda_0 > 0$, tel que, uniformément pour $1 \leq a \leq \lambda_0\sqrt{n}$, on a, lorsque $n \longrightarrow \infty$

$$\text{(27)} \qquad \log\Big(\frac{R(n,a)}{p(n)}\Big) \leq \Psi(a)\log\frac{\pi a}{\sqrt{6n}} + O(1/\sqrt{n})$$

et

$$\log\Big(\frac{R(n,a)}{p(n)}\Big) \geq \Psi(a)\log\frac{\pi a}{\sqrt{6n}} - \gamma_a a + O(a^2/\sqrt{n}) \tag{28}$$

avec $\gamma_a = 1/2$ si a est impair, et si a est pair

$$\gamma_a = \frac{1}{2} + \log 3 - \frac{7}{6}\log 2 + c\frac{\log a}{a} = 0.79\cdots + c\frac{\log a}{a}$$

où c est une constante.

Dans le cas des sommants distincts, la minoration suivante est démontrée dans [ENS1] : il existe $\lambda_1 > 0$, tel que, pour $1 \leq a \leq \lambda_1\sqrt{n}$ on ait :

$$\log\Big(\frac{Q(n,a)}{q(n)}\Big) \geq -\frac{a}{6}\log\frac{16}{3} + O(1 + a^2/\sqrt{n}). \tag{29}$$

Dans [ENS2], on donne la majoration : pour $a \leq \frac{3}{5}\sqrt{n}$, et n assez grand, on a :

$$\log\Big(\frac{Q(n,a)}{q(n)}\Big) \leq -a\log\frac{2}{\sqrt{3}} + \frac{\pi a^2}{8\sqrt{3n}} + O(1). \tag{30}$$

Les constantes figurant dans (29) et (30) valent :

$$\frac{1}{6}\log\frac{16}{3} = 0.279\ldots \quad \log\frac{2}{\sqrt{3}} = 0.144\ldots .$$

Troisième cas : $a \geq \lambda_2\sqrt{n}$.

Les résultats suivants figurent dans [ENS2] : Pour $n > n_0$, et $10^{18}\sqrt{n} \leq a \leq n^{5/7}$, on a :

$$Q(n,a) \leq q([n/2])\exp(4.10^5 a^{-1/3}n^{2/3}\log(a^{1/3}n^{-1/6})) \tag{31}$$

et

$$R(n,a) \leq p([n/2])\exp(4.10^5 a^{-1/3}n^{2/3}\log(a^{1/3}n^{-1/6})). \tag{32}$$

Pour $n > n_0$ et $n^{5/7} < a \leq n/2$, on a :

$$Q(n,a) \leq q([n/2])\exp(n^{1/2-1/30}) \tag{33}$$

et

$$R(n,a) \leq p([n/2]) \exp(n^{1/2-1/30}). \tag{34}$$

On déduit aisément des formules ci-dessus, que si $a = a(n)$ vérifie $a/\sqrt{n} \longrightarrow +\infty$ et $a \leq n/2$, on a :

$$Q(n,a) = q([n/2])^{1+o(1)} \tag{35}$$

et

$$R(n,a) = p([n/2])^{1+o(1)}. \tag{36}$$

Enfin, le résultat ci-dessous montre que l'influence de la parité de a que nous avons observée s'étend à celle de la divisibilité de a par les petits nombres : Soit $s(a)$ le plus petit entier naturel qui ne divise pas a. Pour n assez grand, $s(a) \geq 40\ 000$ et

$$\frac{7}{100} n^{1/2} s(a)^{3/2} \leq a \leq \frac{1}{40} n (s(a))^{-1}$$

on a

$$Q(n,a) \leq \exp(201 n^{1/2} s(a)^{-1/2} \log(s(a))) \tag{37}$$

et

$$R(n,a) \leq \exp(301 n^{1/2} s(a)^{-1/2} \log(s(a))) \tag{38}$$

Comme il est facile d'observer que :

$$Q(n,a) \geq q([(n-a)/s(a)] - 1)$$

et

$$R(n,a) \geq p([(n-a)/s(a)] - 1),$$

les formules (37) et (38) seraient optimales (à la constante près) si l'on enlevait le terme en $\log s(a)$.

La démonstration des formules (31) à (38) utilise des résultats de théorie additive des nombres (cf. [Sa1] et [Sa2]) et particulièrement le théorème

suivant : si une partie A de $\{1, 2, \ldots, N\}$ contient suffisamment d'éléments, l'ensemble des sous sommes de A contient une progression arithmétique assez longue (cf. [Sa2], théorème 4).

Quatrième cas : $\lambda_3 n \leq a \leq n/2$.

En utilisant également les théorèmes additifs, J. Dixmier démontre dans [D4] : soit λ_3 fixé, $0 < \lambda_3 \leq 1/2$ et r un entier fixé ≥ 1. Soit n tendant vers l'infini, et $a = a_n$ tel que $\lambda_3 n \leq a \leq n/2$.

On suppose que $s(a) = r + 1$. Alors :

(39i) si $a \geq n/(r+1)$, alors $\log R(n,a) \sim \log p(a)$;

(39ii) si $a \leq \frac{n}{(r+1)}$ et $r+1 \nmid n-a$, alors $R(n,a) \sim \log p(\frac{n}{r+1})$;

(39iii) si $\frac{n}{r+2} \leq a \leq \frac{n}{(r+1)}$ et $r+1 | n-a$, alors $\log R(n,a) \sim \log p(a)$;

(39iv) si $a \leq \frac{n}{r+2}$ et $r+1 | n-a$, alors $\log R(n,a) \sim \log p(\frac{n-a}{r+1})$.

J. Dixmier considère aussi dans [D4] le cas $n = 2a$. Plus précisément, il donne un développement asymptotique de $R(2n, n)$ suivant les puissances de $n^{-1/2}$. Soit $R''(2n)$ le nombre de partitions de $2n$ qui ne représentent pas n, et ayant une part $> n$. On a :

$$R''(2n) = \sum_{i=0}^{n-1} p(i)$$

et il est possible (cf. [DN1]) d'obtenir, un développement asymptotique :

$$R''(2n) = p(n)\Big(\frac{\sqrt{6}}{\pi}\sqrt{n} + \beta_0 + \frac{\beta_1}{\sqrt{n}} + \frac{\beta_2}{n} + \cdots\Big). \tag{40}$$

Soit $R'(2n) = R(2n,n) - R''(2n)$ le nombre de partitions de $2n$ qui ne représentent pas n, et dont les parts sont $< n$. Lorsque n est pair, J. Dixmier prouve :

$$R'(2n) = p(n)\Big(\frac{\pi}{\sqrt{6n}} + \frac{\alpha_2}{n} + \frac{\alpha_3}{n^{3/2}} + \cdots\Big) \tag{41}$$

et lorsque n est impair :

$$R'(2n) = p(n)\Big(1 + \frac{\pi}{\sqrt{6n}} + \frac{\alpha_2}{n} + \frac{\alpha_3}{n^{3/2}} + \cdots\Big). \tag{42}$$

Les coefficients α_i sont les mêmes dans (41) et (42). Le "1" supplémentaire dans (42) correspond aux partitions dont toutes les parts sont paires.

Cinquième cas : $a \sim \lambda\sqrt{n}$.

Il est démontré que dans [DN2] que si a est impair et $a \sim \sqrt{n}$, on a :

$$\log R(n,a) \geq 2.0138\sqrt{n}. \tag{43}$$

La même méthode permet de déterminer une fonction φ telle que si a est impair, et $a \sim \lambda\sqrt{n}$, on ait :

$$\log R(n,a) \geq \varphi(\lambda)\sqrt{n}. \tag{44}$$

Il est conjecturé dans [ENS2] que (44) est optimal lorsque a est impair. Lorsque a est pair, la situation semble moins claire.

J. Dixmier démontre dans [D4] que, pour $\varepsilon > 0$, il existe $\delta < 1$ tel que, pour n assez grand on a :

$$\varepsilon\sqrt{n} \leq a \leq n - \varepsilon\sqrt{n} \Longrightarrow R(n,a) \leq p(n)^{\delta}. \tag{45}$$

Par la même méthode, un résultat similaire peut être démontré en remplaçant $R(n,a)$ par $Q(n,a)$ et $p(n)$ par $q(n)$.

Remarque : Une table numérique de $R(n,a)$ figure dans [ENS1] et une table de $Q(n,a)$ dans [ENS2].

3. Couples de partitions additivement indépendantes

Nous dirons que deux partitions τ_1 et τ_2 du même entier naturel n sont additivement indépendantes si leurs sous-sommes (excepté 0 et n) sont distinctes, autrement dit s'il n'existe aucun entier naturel a, $1 \leq a \leq n-1$ représenté simultanément par τ_1 et τ_2.

Nous désignerons par $G(n)$ (resp. $H(n)$) le nombre de couples de partitions (resp. partitions sans répétitions) additivement indépendantes. Si l'on choisit pour τ_1 (resp. τ_2) la partition avec un seul sommant égal à n, pour tout choix de τ_2 (resp. τ_1), τ_1 et τ_2 seront additivement indépendantes, ce qui démontre

$$\begin{aligned} G(n) &\geq 2p(n) - 1 \\ H(n) &\geq 2q(n) - 1. \end{aligned}$$

Le tableau ci-dessous permet de calculer $G(7) = 41$.

σ_i	Sous-sommes $\neq 0$ et 7	$\{j; \sigma_i$ et σ_j add.ind.$\}$	Nombres de j
$\sigma_1 = 7$	$\emptyset$	$1 \cdots 15$	15
$\sigma_2 = 6+1$	1,6	1,3,5,9	4
$\sigma_3 = 5+2$	2,5	1,2,5,8	4
$\sigma_4 = 5+1+1$	1,2,5,6	1,5	2
$\sigma_5 = 4+3$	3,4	1,2,3,4	4
$\sigma_6 = 4+2+1$	1,2,3,4,5,6	1	1
$\sigma_7 = 4+1+1+1$	1,2,3,4,5,6	1	1
$\sigma_8 = 3+3+1$	1,3,4,6	1,3	2
$\sigma_9 = 3+2+2$	2,3,4,5	1,2	2
$\sigma_{10} = 3+2+1+1$	1,2,3,4,5,6	1	1
$\sigma_{11} = 3+1+1+1+1$	1,2,3,4,5,6	1	1
$\sigma_{12} = 2+2+2+1$	1,2,3,4,5,6	1	1
$\sigma_{13} = 2+2+1+1+1$	1,2,3,4,5,6	1	1
$\sigma_{14} = 2+1+1+1+1+1$	1,2,3,4,5,6	1	1
$\sigma_{15} = 1+1+1+1+1+1+1$	1,2,3,4,5,6	1	1
		Total =	41

Notons que les partitions $\sigma_6, \sigma_7, \sigma_{10}$ à σ_{15} sont "pratiques", c'est-à-dire représentent tout nombre entre 0 et 7. Dans [ES1], il est démontré que $\widetilde{p}(n)$, le nombre de partitions pratiques de n, vérifie $\widetilde{p}(n) \sim p(n)$, autrement dit, lorsque $n \longrightarrow \infty$, presque toutes les partitions sont pratiques. Dans [DN1], on trouvera un développement asymptotique de $\widetilde{p}(n)/p(n)$.

Dans [ENS3], on donne les estimations suivantes pour $G(n)$ et $H(n)$. Pour tout entier k, il existe des coefficients $\alpha_1, \alpha_2, \ldots, \alpha_k$ tels que

$$G(n) = 2p(n)\Big(1 + \frac{\alpha_1}{\sqrt{n}} + \frac{\alpha_2}{n} + \cdots + \frac{\alpha_k}{n^{k/2}} + O\Big(\frac{1}{n^{(k+1)/2}}\Big)\Big)$$

On a :

$$\alpha_1 = \frac{\pi}{\sqrt{6}} = 1.28\cdots, \quad \alpha_2 = \frac{17}{12}\pi^2 - 1 = 12.98\cdots$$

$$\alpha_3 = \frac{1}{\sqrt{6}}\left(\frac{337}{36}\pi^3 - \frac{1019}{48}\pi + \frac{3}{2\pi}\right) = 91.46\cdots$$

$$\alpha_4 = \frac{7889}{864}\pi^4 - \frac{12115}{288}\pi^2 + \frac{509}{24} + \frac{3}{4\pi^2} = 495.53\cdots$$

$$\alpha_5 = 10450.82 \qquad \alpha_6 = 43427.98 \qquad \alpha_7 = -848498.0$$

$$\alpha_8 = 7.67\ 10^7 \qquad \alpha_9 = -1.897\ 10^9 \qquad \alpha_{10} = 4.42\ 10^{10}$$

$$\alpha_{11} = -7.28\ 10^{11} \qquad \alpha_{12} = 1.23\ 10^{13} \qquad \alpha_{13} = -4.04\ 10^{14}$$

$$\alpha_{14} = 2.53\ 10^{16} \qquad \alpha_{15} = -1.42\ 10^{18} \qquad \alpha_{16} = 6.51\ 10^{19}$$

$$\alpha_{17} = -2.53\ 10^{21}.$$

Les coefficients ci-dessus ont été calculés à l'aide du système de calcul formel MAPLE.

Il existe un nombre réel c tel que

$$H(n) = cq(n)\left(1 + O\left(\frac{\log^2 n}{\sqrt{n}}\right)\right). \tag{47}$$

La valeur de c vérifie : $13.83 \leq c \leq 14.29$.

La différence entre (46) et (47) s'explique par la différence de comportement de $r(n,m))$ et de $\rho(n,m)$. Si l'on choisit pour τ_1 la partition $1+(n-1)$, et pour τ_2 une partition sans 1, τ_1 et τ_2 seront des partitions additivement indépendantes. De tels couples, il y en a $r(n,2)$ ou $\rho(n,2)$. Or, d'après (6),

$$r(n,2) \sim \frac{\pi}{\sqrt{6n}}p(n) = o(p(n))$$

tandis que, d'après (11),

$$\rho(n,2) \sim \frac{1}{2}q(n).$$

Désignons par $\pi(h)$ (resp. $\pi'(h)$) l'ensemble des partitions de h (resp. l'ensemble des partitions en sommants distincts).

Si σ est une partition, on appelle $\mathcal{P}(\sigma)$ l'ensemble des sous sommes non nulles de σ. Le point de départ des formules (46) et (47) est que pour tout $\varepsilon > 0$, on a

$$G(n) = 2 \sum_{h=0}^{3000\sqrt{n}\log n} \sum_{\sigma\in\pi(h)} R(n,\mathcal{P}(\sigma)) + O_\varepsilon(p(n)^{1/\sqrt{2}+\varepsilon}) \tag{48}$$

et

$$H(n) = 2 \sum_{h=0}^{3000\sqrt{n}} \sum_{\sigma \in \pi'(h)} \rho(n, \mathcal{P}(\sigma)) + O_\varepsilon(q(n)^{1/\sqrt{2}+\varepsilon}). \tag{49}$$

La démonstration de (49) est la même que celle de (48). Pour démontrer (48), on commence par minorer $G(n)$: Pour tout $h_0 < n/2$, on a :

$$G(n) = 2 \sum_{h=0}^{h_0} \sum_{\sigma \in \pi(h)} R(n, \mathcal{P}(\sigma)) - E(h_0). \tag{50}$$

Cette formule est assez simple : à $\sigma \in \pi(h)$ on associe $\tau_1 \in \pi(n)$ qui est formée des parts de σ auxquelles on ajoute la part $n - h$. Si τ_2 est une partition quelconque de n dont les sous sommes ne sont pas dans $\mathcal{P}(\sigma)$, alors le couple (τ_1, τ_2) est additivement indépendant, et de même le couple (τ_2, τ_1). Ceci justifie le terme principal dans le membre de droite de (50). $E(h_0)$ compte le nombre des couples (τ_1, τ_2) comptés deux fois dans le procédé ci-dessus, c'est-à-dire pour lesquels il existe h_1 et h_2, $0 \leq h_1 \leq h_0$, $0 \leq h_2 \leq h_0$, $\sigma_1 \in \pi(h_1)$ $\sigma_2 \in \pi(h_2)$ tels que

$$\tau_1 = \sigma_1 + (n - h_1); \quad \tau_2 = \sigma_2 + (n - h_2)$$

et $\mathcal{P}(\sigma_1) \cap \mathcal{P}(\sigma_2) = \emptyset$. On a la majoration

$$E(h_0) \leq \Big(\sum_{h=0}^{h_0} p(h)\Big)^2 \leq ((h_0 + 1)p(h_0))^2$$

qui, par (8), prouve avec (50) la minoration dans (48).

Pour la majoration, on dit qu'une partition $\tau \in \pi(n)$ a la propriété (51) si

$$\tau \text{ a au moins } \sqrt{n}/100 \text{ parts distinctes inférieures à } 100\sqrt{n}. \tag{51}$$

Par un argument combinatoire assez grossier, on peut montrer que le nombre de partitions de n pour lesquelles (51) n'est pas vrai est $O((p(n))^{1/4})$. Le nombre de couples (τ_1, τ_2) de partitions de n tels que τ_1 et τ_2 ne vérifient pas (51) est $O((p(n))^{1/2})$, et est donc inclus dans le terme d'erreur de (48).

Supposons maintenant que τ_2 soit une partition de n dont tous les sommants sont inférieurs à $n - 3000\sqrt{n}\log n$. Il est assez facile de voir que τ_2 représente un nombre a vérifiant

$$a_1 = 1500\sqrt{n}\log n \leq a < a_2 = n - 1500\sqrt{n}\log n.$$

Le nombre de choix possibles pour τ_1, tel que le couple (τ_1, τ_2) soit additivement indépendant, est donc au plus (car τ_1 ne doit pas représenter a)

$$\sum_{a_1 \leq a \leq a_2} R(n,a) \tag{52}$$

et les formules (32) et (34) permettent de majorer (52) par $O((p(n))^{(1/\sqrt{2}+\varepsilon)}$.

Si, de plus, τ_1 vérifie (51), grâce aux théorèmes de théorie additive des nombres (cf. [Sa1] et [Sa2]) déjà utilisés pour démontrer les formules (31) à (38), on peut montrer que le nombre de partitions τ_2 tels que le couple (τ_1, τ_2) soit additivement indépendant est $O((p(n))^{1/\sqrt{2}+\varepsilon})$.

Il restera à compter les couples additivement indépendants (τ_1, τ_2) avec τ_1 vérifiant (51) et τ_2 ayant un sommant $n - h$, avec $h \leq 3000\sqrt{n}\log n$. Clairement le nombre de ces couples est majoré par

$$\sum_{0 \leq h \leq 3000\sqrt{n}\log n} \sum_{\sigma \in \pi(h)} R(n, \mathcal{P}(\sigma)). \tag{53}$$

Et comme on doit considérer de façon symétrique les couples (τ_1, τ_2) où τ_1 a un grand sommant $n - h$, et τ_2 vérifie (51), il faut multiplier (53) par 2, pour obtenir (48).

Pour démontrer (46) à partir de (48), on observe d'abord (puisque $h \in \mathcal{P}(\sigma)$) que

$$\sum_{\sigma \in \pi(h)} R(n, \mathcal{P}(\sigma)) \leq \sum_{\sigma \in \pi(h)} R(n,h) = p(h)R(n,h).$$

On prouve ensuite

$$\sum_{h=2k}^{3000\sqrt{n}\log n} p(h)R(h,h) = O(p(n)n^{-(k+1)/2})$$

en utilisant les formules (8), (22), (27) et (45).

D'après [D1], on peut écrire

$$\sum_{h=0}^{2k-1} \sum_{\sigma \in \pi(h)} R(n, \mathcal{P}(\sigma)) = \sum_{i=0}^{d} b_i p(n-i)$$

où les nombres d, et b_i peuvent être calculés.

Enfin d'après Hardy et Ramanujan (cf. [DN1]) on a le développement asymptotique d'ordre s quelconque, pour μ fixé

$$\frac{p(n-\mu)}{p(n)} = 1 + \sum_{i=1}^{s} \beta_i n^{-i/2} + O(n^{-(s+1)/2})$$

avec en particulier :

$$\beta_1 = -\frac{C\mu}{2}, \quad \beta_2 = \mu + \frac{C^2\mu^2}{8}, \quad C = \pi\sqrt{2/3}.$$

Pour démontrer (47) à partir de (49), on observe similairement que

$$\sum_{\sigma \in \pi'(h)} \rho(n, \mathcal{P}(\sigma)) \leq q(h) Q(n, h)$$

et l'on prouve

$$\sum_{5 \log n < h \leq 3000\sqrt{n} \log n} q(h) Q(n, h) = O(q(n) \log n / \sqrt{n})$$

en utilisant les formules (12), (30) et (35).

L'évaluation de

$$S_1 = \sum_{0 \leq h \leq 5 \log n} \sum_{\sigma \in \pi'(h)} \rho(n, \mathcal{P}(\sigma))$$

est plus délicate. On observe d'abord que comme σ est une partition sans répétition de h, $\mathcal{P}(\sigma)$ est un ensemble contenu dans $\{1, \ldots, h(h+1)/2\}$. Soit P un ensemble d'entiers naturels ≥ 1. On définit $\mathcal{W}(h, P)$ comme l'ensemble des parties $\mathcal{A} \subset \{1, 2, \ldots, h\}$ telles que les sous sommes de $\mathcal{A}$ ne rencontrent pas P. Si $S(\mathcal{A})$ est la somme des éléments de $\mathcal{A}$, on a alors

$$\rho(n, P) = \sum_{\mathcal{A} \in \mathcal{W}(h,P), S(\mathcal{A}) \leq n} \rho(n - S(\mathcal{A}), h+1). \tag{54}$$

Comme $S(\mathcal{A}) \leq \frac{h(h+1)}{2} = O(\log^2 n)$, la formule (13) nous donne

$$\rho(n - S(\mathcal{A}), h+1) = \frac{1}{2^h} q(n)\Big(1 + O\Big(\frac{\log^2 n}{\sqrt{n}}\Big)\Big) \tag{55}$$

et, par (54) et (55), S_1 devient :

$$S_1 = q(n)\Big(\sum_{0 \leq h \leq 5 \log n} z(h) 2^{-h}\Big)\Big(1 + O\Big(\frac{\log^2 n}{\sqrt{n}}\Big)\Big) \tag{56}$$

avec

$$z(h) = \sum_{\sigma \in \pi'(h)} \mathrm{Card}(\mathcal{W}(h, \mathcal{P}(\sigma))). \tag{57}$$

On démontre ensuite que

$$z(h) \leq q(h) 3^{h/2} \tag{58}$$

et l'on pose

$$c/2 = \sum_{h=0}^{\infty} z(h) 2^{-h}.$$

Par (12) et (58), la série ci-dessus est convergente, et le reste vérifie

$$\sum_{h > 5 \log n} z(h) 2^{-h} = O\Big(\sum_{h > 5 \log n} \exp(-h/10)\Big) = O\Big(\frac{1}{\sqrt{n}}\Big).$$

La formule (56) donne alors

$$S_1 = \frac{c}{2} q(n)\Big(1 + O\Big(\frac{\log^2 n}{\sqrt{n}}\Big)\Big)$$

ce qui achève la preuve de (47).

Le calcul numérique de c a été fait par M. Deléglise. Le calcul de $z(h)$ par (57) est très lent et a été effectué pour $h \leq 40$ en plusieurs jours d'ordinateurs SUN 3/80. On obtient

$$z(40) 2^{-40} = 0.842\ 10^{-3}$$

tandis que la majoration (58) donne :

$$z(40) 2^{-40} \leq q(40)(\sqrt{3}/2)^{40} = 3.53.$$

Il a donc fallu améliorer la majoration théorique ci-dessus pour obtenir la valeur de c avec une précision pas trop mauvaise. On trouvera dans [ENS3] les calculs détaillés de cette majoration, ainsi que des tables numériques des diverses fonctions utilisées.

BIBLIOGRAPHIE

[D1] J. DIXMIER. — *Sur les sous-sommes d'une partition*, Mémoire de la SMF, n° 35, supplément au Bull. SMF 116, 1988.

[D2] J. DIXMIER. — Sur les sous-sommes d'une partition II, *Portugaliae Mathematica* **46**, (1989), 137-154.

[D3] J. DIXMIER. — Sur les sous-sommes d'une partition III, *Bull. Sci. Math.* **113**, (1989), 125-149.

[D4] J. DIXMIER. — Partitions avec sous-sommes interdites, *Bull. Soc. Math. Belgique* **42**, (1990), 477-500.

[D5] J. DIXMIER. — Proof of a conjecture by Erdös and Graham concerning the problem of Frobenius, *J. Number Theory* **34**, (1990), 198-209.

[DEN] J. DIXMIER, P. ERDÖS, et J.-L. NICOLAS. — Sur le nombre d'invariants fondamentaux des forme binaires, *C.R. Acad. Sci. Paris* **305, Série I**, (1987), 319-322.

[DN1] J. DIXMIER et J.-L. NICOLAS. — Partitions without small parts, Colloquia Math. Soc. János Bolyai, *Number Theory, Budapest (Hungary)* **51**, (1987), 9-33.

[DN2] J. DIXMIER et J.-L. NICOLAS. — Partitions sans petits sommants, *Number Theory, Budapest (Hungary)* , (1990), 121-152.

[ENS1] P. ERDÖS, J.-L. NICOLAS et A. SÁRKÖZY. — On the number of partitions of n without a given subsum (I), *Discrete Mathematics* **75**, (1989), 155-166.

[ENS2] P. ERDÖS, J.-L. NICOLAS et A. SÁRKÖZY. — On the number of partitions of n without a given subsum (II), *Analytic Number Theory, Proceedings of a Conference in Honor of Paul T. Bateman, Progress in Mathematics, Birkhäuser* **85**, (1990), 205-234.

[ENS3] P. ERDÖS, J.-L. NICOLAS et A. SÁRKÖZY. — *On the number of pairs of partitions of n without common subsums*, à paraître dans Colloquium Mathematicum.

[ENSz] P. ERDÖS, J.-L. NICOLAS et M. SZALAY. — Partitions into parts which are unequal and large, *Number Theory, Ulm 87 édité par H.P. Schickewei et E. Wirsing, Springer Verlag Lecture Note* **1380**, (1987), 19-30.

[ES1] P. ERDÖS et M. SZALAY. — On some problems of J. Dénes and P. Turán, *Studies in pure Math. to the memory of P. Turán, Editor P. Erdös, Budapest* , (1983), 187-212.

[ES2] P. ERDÖS et M. SZALAY. — On the statistical theory of partitions, *Coll. Math. Soc. János Bolyai, Topics in classical number theory, Budapest* **34**, (1981), 397-450.

[ES3] P. ERDÖS et M. SZALAY. — On some problems of the statistical theory of partitions, *Coll. Math. Soc. János Bolyai, Number theory, Budapest (Hungary)* **51**, (1987), 93-110.

[FP] G. FREIMAN et J. PTIMAN. — *Partitions into distinct large parts*, preprint.

[G] H. GUPTA. — A formula in partitions, *J. Indian Math. Soc. (N.S.)* **6**, (1942), 115-117.

[GGM] H. GUPTA, C.E. GWYTHER et J.C.P. MILLER. — *Table of partitions*, Cambridge University Press, 1962.

[H1] J. HERZOG. — *Gleichmässige asymptotische für parameterabhängige Partionenfunktionen, Thesis*, Université J.W. Goethe, Frankfurt am Main, 1987.

[H2] J. HERZOG. — *On partitions into distinct parts* $\geq Y$, préprint.

[HR] G.H. HARDY et S. RAMANUJAN. — Asymptotic formulae in combinatory analysis, *Proc. London Math. Soc.* (2), 17, 1918, 75-115. (Aussi dans Collected Papers de S. Ramanujan, Cambridge University Press 1927, 276-309, réimprimé par Chelsea, 1962.

[Sa1] A. SÁRKÖZY. — Finite addition theorems, *J. Number Theory* **32**, (1989), 114-130.

[Sa2] A. SÁRKÖZY. — Finite additions theorem II, à paraître, *J. Number Theory*.

[Sz1] G. SZEKERES. — An asymptotic formula in the theory of partitions, *Quart. J. Math. Oxford* **2**, (1951), 85-108.

[Sz2] G. SZEKERES. — Some asymptotic formulae in the theory of partitions II, *Quart. J. Math. Oxford* **4**, (1953), 96-111.

Jean-Louis NICOLAS
Mathématiques, Bât. 101
Université Claude Bernard, Lyon 1
F-69622 VILLEURBANNE CEDEX

FINITE ADDITION THEOREMS, III

A. SÁRKÖZY

1. Throughout this paper we use the following notations : the cardinality of the finite set $\mathcal{S}$ is denoted by $|\mathcal{S}|$. $\mathcal{A}$, $\mathcal{B}$,... denote finite or infinite sets of non–negative integers, and the counting functions of their *positive parts* are denoted by $A(n)$, $B(n)$,..., so that, e.g., $A(n) = |\mathcal{A} \cap \{1,2,\ldots,n\}|$. $\mathcal{A}+\mathcal{B}$ denotes the set of the distinct non–negative integers that can be represented in the form $a+b$ with $a \in \mathcal{A}$, $b \in \mathcal{B}$. We write $\mathcal{A}+\mathcal{A} = 2\mathcal{A}$ and $k\mathcal{A} = \mathcal{A}+(k-1)\mathcal{A}$ for $k = 3,4,\ldots$. An arithmetic progression will be sait homogeneous if it consists of the consecutive multiples of a non–zero number, i.e., it is of the form kd, $(k+1)d,\ldots,\ell d$ (where $d \neq 0$).

2. In Part I [5] of this paper, I proved the following theorem (improving on a result of Nathanson and mine [4]) :

THEOREM 1. — *Assume that k, N are positive integers, $\mathcal{A} \subset \{1,2,\ldots,N\}$ and*

$$|\mathcal{A}| > \frac{N}{k}+1 .$$

Then there are integers d, ℓ, m such that $d \leq k-1$, $\ell < 118k$ and

$$\{(m+1)d,(m+2)d,\ldots,(m+N)d\} \subset \ell\mathcal{A} .$$

In other words, this theorem says that if $\mathcal{A} \subset \{1,2,\ldots,N\}$ and $|\mathcal{A}| \geq 2$, then there is an $\ell < c\frac{N}{|\mathcal{A}|}$ such that $\ell\mathcal{A}$ contains a homogeneous arithmetic progression of length N. (In several applications one needs the fact that this arithmetic progression is homogeneous.)

In Part II [6] of this paper, I studied subset sums, i.e., sums of the form $\sum_{a\in\mathcal{A}} \varepsilon_a a$ where $\varepsilon_a = 0$ or 1.

In this paper, my goal is to study $k\mathcal{A}$ in the case when $k \ll N/|\mathcal{A}|$ so that Theorem 1 cannot be applied. A simple consideration shows that in this case, we cannot expect that the sum set $k\mathcal{A}$ (with $k \ll N/|\mathcal{A}|$) should contain a complete arithmetic progression of length N. Instead, the best

that we may hope is that there is an arithmetic progression of length N which contains at least $\left(\min\left(1, ck\frac{|\mathcal{A}|}{N}\right)\right)N$ elements of $k\mathcal{A}$, moreover, we have to give up the requirement that this arithmetic progression should be homogeneous. In fact, we will prove

THEOREM 2. — *Assume that k, N are positive integers, $\mathcal{A}$ is a finite set of positive integers with*

$$|\mathcal{A}| \geq 2 \tag{1}$$

and $\mathcal{A} \subset \{1, 2, \ldots, N\}$. Then there is an integer m and a positive integer d such that

$$d < 2\frac{N}{|\mathcal{A}|} \tag{2}$$

and

$$|\{m+d, m+2d, \ldots, m+Nd\} \cap k\mathcal{A}| \geq \left(\min\left(1, \frac{1}{800}k\frac{|\mathcal{A}|}{N}\right)\right)N. \tag{3}$$

Note that for $|\mathcal{A}| = 1$, the left hand side of (3) is $\leq |k\mathcal{A}| = 1$, while the right hand side is $= N$ for $k \geq 800N$. This shows that the condition (1) is necessary.

The example $\mathcal{A} = \left\{p, 2p, \ldots, \left[\frac{N}{p}\right]p\right\}$, $k = p$ (where p is prime) shows that (2) is the best possible apart from the constant factor 2.

Moreover, for $\mathcal{A} = \{1, 2\}$, the left hand side of (3) is $\leq |k\mathcal{A}| = |\{k, k+1, \ldots, 2k\}| = k+1$ and this is $\sim \frac{1}{2}k\frac{|\mathcal{A}|}{N} \cdot N$ for $k \longrightarrow +\infty$. Thus for $N > k+1$ and $k \longrightarrow +\infty$, the left hand side of (3) is less than $\left(\min\left(1, \left(\frac{1}{2}+\varepsilon\right)\frac{|\mathcal{A}|}{N}\right)\right)N$. This shows that (3) is the best possible apart form the constant $\frac{1}{800}$ on the right hand side and, in fact, this constant cannot be replaced by a number greater than $1/2$.

Finally, if p is a prime, k is a positive integer with $k \leq p-1$ and $\mathcal{A}$ is defined by $\mathcal{A} = \{n : n \equiv 1 \pmod{p},\ 1 \leq n \leq N\}$, than all the elements of $k\mathcal{A}$ are $\equiv k \not\equiv 0 \pmod{p}$ and thus

$$|\{(m+1)d, (m+2)d, \ldots, (m+N)d\} \cap k\mathcal{A}| \leq \left[\frac{N}{p}\right] + 1 \leq |\mathcal{A}| + 1$$

for all integers m, d (> 0). This inequality shows that, in fact, the arithmetic progression $\{m+d, m+2d, \ldots, m+Nd\}$ on the left hand side of (3) cannot be replaced by a homogeneous one.

3. The rest of this paper will be devoted to the proof of Theorem 2. The proof uses some elements of the proof of Theorem 1, however, certain modifications and further ideas are needed.

We shall need the following special case of a theorem of Dyson [1] (it also follows from Mann's theorem [3]) :

LEMMA 1. — *Assume that h, n are positive integers, $\mathcal{C} \subset \{0, 1, 2, \ldots, n\}$, $0 \in \mathcal{C}$. Let $\mathcal{D} = h\mathcal{C}$. If δ is a positive real number such that $C(m) \geq \delta m$ for $m = 1, 2, \ldots, n$, then*

$$\frac{D(m)}{m} \geq \min(1, h\delta) \quad \textit{for} \quad m = 1, 2, \ldots, n \, .$$

We need two more lemmas :

LEMMA 2. — *Assume that M, k are positive integers, δ is a positive real number, $\mathcal{A} \subset \{1, 2, \ldots, M\}$,*

$$|\mathcal{A}| \geq \delta M, \tag{4}$$

and there is a positive integer a^* such that both $a^* \in \mathcal{A}$ and $a^* + 1 \in \mathcal{A}$ hold. Then there is an integer n such that

$$|\{n+1, n+2, \ldots, n+M\} \cap k\mathcal{A}| \geq (\min(1, k\delta/6))M. \tag{5}$$

Proof : The case $k = 1$ is trivial, thus we may assume that

$$k \geq 2 \, . \tag{6}$$

First we will show that there is an integerg u (with $0 \leq u < M$) such that

$$A(u+m) - A(u) \geq \frac{\delta}{2} m \quad \text{for all} \quad 1 \leq m \leq M \, . \tag{7}$$

To prove this, assume that in contrary to the assertion there is no u with this property. Define the sequence $z_0 < z_1 < \cdots < z_t$ of non–negative integers by the following recursion :

Let $z_0 = 0$. Assume that z_i has been defined for some $i \geq 0$. Then we define z_{i+1} in the following way : If $z_i \geq M$ then we end the construction, i.e., let $i = t$. If $z_i < M$, then, by our indirect assumption, z_i cannot be chosen as u in (7), thus there is an integer m_i with

$$1 \leq m_i \leq M \tag{8}$$

and

$$A(z_i + m_i) - A(z_i) < \frac{\delta}{2} m_i \ . \tag{9}$$

Let $z_{i+1} = z_i + m_i$. By (8) we have

$$z_{i+1} = z_i + m_i < M + M = 2M \ . \tag{10}$$

If follows from (10) and the construction that

$$M \leq z_t < 2M \ . \tag{11}$$

By (9) and (11) we have

$$A(M) = A(z_t) = \sum_{i=0}^{t-1} (A(z_{i+1}) - A(z_i)) < \sum_{i=0}^{t-1} \tfrac{\delta}{2}(z_{i+1} - z_i) = \\ = \tfrac{\delta}{2}(z_t - z_0) = \tfrac{\delta}{2} z_t < \delta M$$

which contradicts (4) and this completes the proof of the existence of a u satisfying (7).

Let u be a fixed integer satisfying (7), and let $\mathcal{B} = \{0\} \cup \{b : 1 \leq b \leq M,\ u + b \in \mathcal{A}\}$. Then by (7) we have

$$B(M) \geq \frac{\delta}{2} m \quad \text{for all} \quad 1 \leq m \leq M \ . \tag{12}$$

Let $\ell = [k/2]$. Then $\ell \geq 1$ and

$$\ell \geq k/3 \tag{13}$$

by (6). Let $C = \ell\mathcal{B}$. By Dyson's theorem and (13), $0 \in \mathcal{B}$ and (12) imply

$$C(M) \geq (\min(1, \ell\delta/2))M \geq \min((1, k\delta/6))M \ . \tag{14}$$

Now we will show that

$$b \in \mathcal{B} \text{ implies } b + u + a^* + 1 \in 2\mathcal{A} \ . \tag{15}$$

Assume first that $b = 0$. Then (7) (with $m = 1$) and $\delta > 0$ imply that $u + 1 \in \mathcal{A}$ so that

$$b + u + a^* + 1 = 0 + u + a^* + 1 = (u + 1) + a^* \in \mathcal{A} + \mathcal{A} = 2\mathcal{A}$$

so that (15) holds in this case. Assume now that $b > 0$, $b \in \mathcal{B}$. Then by the definition of $\mathcal{B}$ we have $u + b \in \mathcal{A}$. Thus we have

$$b + u + a^* + 1 = (u + b) + (a^* + 1) \in \mathcal{A} + \mathcal{A} = 2\mathcal{A}$$

which completes the proof of (15).

Let $m = \ell(u + a^* + 1)$. We will show that

$$0 < c \leq M,\ c \in \mathcal{C} \text{ imply } m + c \in (2\ell)\mathcal{A} \ . \tag{16}$$

In fact, if $c \in \mathcal{C} = \ell\mathcal{B}$, then c can be written in the form

$$c = b_1 + b_2 + \cdots + b_\ell \quad (\text{where } b_i \in \mathcal{B} \text{ for } i = 1, 2, \ldots, \ell) \ .$$

Thus we have

$$m + c = \ell(u + a^* + 1) + (b_1 + b_2 + \cdots + b_\ell) =$$

$$= (b_1 + u + a^* + 1) + (b_2 + u + a^* + 1) + \cdots + (b_\ell + u + a^* + 1)$$

where, by (15), every term belongs to $2\mathcal{A}$ so that

$$m + c \in \ell(2\mathcal{A}) = (2\ell)\mathcal{A}$$

which proves (16).

It follows from (14) and (16) that

$$|\{m+1,m+2,\dots,m+M\}\cap(2\ell)\mathcal{A}|\geq|\{1,2,\dots,M\}\cap\mathcal{C}|= \tag{17}$$
$$=C(M)\geq(\min(1,k\delta/6))M\ .$$

Thus if $k=2[k/2]=2\ell$, then (5) holds with m in place of n. If $k=2[k/2]+1=2\ell+1$, then for an $a'\in\mathcal{A}$ we have

$$k\mathcal{A}=\mathcal{A}+2\ell\mathcal{A}\supset\{a'\}+(2\ell)\mathcal{A}$$

whence

$$|\{a'+m+1,a'+m+2,\dots,a'+m+M\}\cap k\mathcal{A}|\geq \tag{18}$$
$$\geq|\{a'+m+1,a'+m+2,\dots,a'+m+M\}\cap(\{a'\}+(2\ell)\mathcal{A})|=$$
$$=|\{m+1,m+2,\dots,m+M\}\cap(2\ell)\mathcal{A}|\ .$$

By (17) and (18), (5) holds with $a'+m$ in place of n and this completes the proof of the lemma.

LEMMA 3. — *Assume that h, g are positive integers, $\mathcal{A}$ is a set of positive integers and it is the union of $t(\geq 1)$ disjoint infinite arithmetic progressions of difference g :*

$$\mathcal{A}=\bigcup_{i=1}^{t}\{a_i,a_i+g,a_i+2g,\dots\}\ (\text{where } a_i\not\equiv a_j\ (\mathrm{mod}\,g)\ \text{for}\ i\neq j)\ .$$

Then there is a divisor g' of g such that $h\mathcal{A}$ is the union of u disjoint infinite arithmetic progressions of difference g : $h\mathcal{A}=\bigcup_{i=1}^{u}\{e_i,e_i+g',e_i+2g',\dots\}$ where

$$\frac{u}{g'}\geq h\frac{t}{g}-\frac{h-1}{g'}\ .$$

This is Lemma 4 in [5] and, in fact, it is a trivial consequence of Kneser's theorem [2].

4. Completion of the proof of Theorem 2. Let us write $\mathcal{A}=\{a_1,a_2,\dots,a_y\}$ so that, by (1),

$$y=|\mathcal{A}|\geq 2\ . \tag{19}$$

Clearly,

$$(k-1)\{a_1\}+\mathcal{A}\subset\{(k-1)a_1+1,(k-1)a_1+2,\dots,(k-1)a_1+N\}\cap k\mathcal{A}$$

thus for $k\leq 800$ we have

$$|\{(k-1)a_1+1,(k-1)a_1+2,\dots,(k-1)a_1+N\}\cap k\mathcal{A}|\geq$$
$$\geq|(k-1)\{a_1\}+\mathcal{A}|=|\mathcal{A}|\geq\tfrac{k}{800}|\mathcal{A}|$$

so that (2) and (3) hold with $m=(k-1)a_1$, $d=1$. Thus in the rest of the proof we may assume that

$$k>800\,. \tag{20}$$

Let $g=\min\limits_{1\leq i<y}(a_{i+1}-a_i)$, and let a' denote an integer with

$$a'\in\mathcal{A},\quad a'+g\in\mathcal{A}\,. \tag{21}$$

Clearly we have

$$N>a_y-a_1=\sum_{i=1}^{y-1}(a_{i+1}-a_i)\geq g(y-1),$$

hence, in view of (19),

$$g<\frac{N}{y-1}\leq\frac{N}{y/2}=\frac{2N}{|\mathcal{A}|}\,. \tag{22}$$

We will show that (3) holds with a d satisfying

$$d|g \tag{23}$$

ane then in fact, (2) will follow from (22) and (23).

For $i=0,\ \pm1,\ \pm2,\dots$, write $\mathcal{A}(i)=\{a:a\in\mathcal{A},\ a\equiv i\ (\mathrm{mod}\,g)\}$. Assume that $\mathcal{A}$ meets exactly t distinct residue classes modulo g, and denote the least elements of $\mathcal{A}$ in these residue classes by $d_1,d_2,\dots,d_t$, so that $d_1\in\mathcal{A}$, $d_2\in\mathcal{A},\dots,d_t\in\mathcal{A}$ and

$$\begin{aligned}&\mathcal{A}=\bigcup_{j=1}^{t}\mathcal{A}(d_j),\ \mathcal{A}(d_j)\neq\emptyset\text{ for }1\leq j\leq t\\&\text{and }d_j\not\equiv d_{j'}\ (\mathrm{mod}\,g)\text{ for }1\leq j<j'\leq t\,.\end{aligned} \tag{24}$$

We may assume that $|\mathcal{A}(d_1)| \geq |\mathcal{A}(d_2)| \geq \cdots \geq |\mathcal{A}(d_t)|$ so that

$$|\mathcal{A}| = \sum_{j=1}^{t} |\mathcal{A}(d_j)| \leq t|\mathcal{A}(d_1)| \,. \tag{25}$$

Write $\mathcal{D} = \{d_1, d_2, \ldots, d_t\}$. Then we have

$$\mathcal{D} \subset \mathcal{A} \,. \tag{26}$$

Let

$$\mathcal{P} = (\mathcal{A}(d_1) + \{a'\}) \cup \{d_1 + a' + g\} \,. \tag{27}$$

By (21),

$$\mathcal{A}(d_1) + \{a'\} \subset \mathcal{A} + \mathcal{A} = 2\mathcal{A}$$

and

$$d_1 + a' + g \in \mathcal{A}(d_1) + \{a' + g\} \subset \mathcal{A} + \mathcal{A} = 2\mathcal{A}$$

so that

$$\mathcal{P} \subset 2\mathcal{A} \,. \tag{28}$$

Moreover, we have

$$\mathcal{P} \subset \left\{d_1 + a', d_1 + a' + g, \ldots, d_1 + a' + \left[\frac{N - d_1}{g}\right] g\right\} \,. \tag{29}$$

It follows from (26) and (28) that

$$\mathcal{D} + \left[\frac{k-1}{2}\right] \mathcal{P} \subset \mathcal{A} + \left[\frac{k-1}{2}\right] \cdot 2\mathcal{A} = \left(2\left[\frac{k-1}{2}\right] + 1\right) \mathcal{A} \,. \tag{30}$$

Let

$$Q = \{n : d_1 + a' + (n-1)g \in \mathcal{P}\} \,. \tag{31}$$

By (27), we have

$$\begin{aligned} |\mathcal{A}(d_1)| + 1 = |\mathcal{A}(d_1) + \{a'\}| + |\{d_1 + a' + g\}| \geq |Q| \geq \\ \geq |\mathcal{A}(d_1) + \{a'\}| = |\mathcal{A}(d_1)| \end{aligned} \tag{32}$$

and

$$\{1,2\} \subset Q\ . \tag{33}$$

It follows from (29) that

$$Q \subset \left\{1,2,\dots,\left[\frac{N-d_1}{g}\right]+1\right\} \subset \{1,2,\dots,\left[\frac{N}{g}\right]+1\}\ . \tag{34}$$

We have to distinguish two cases.

5. In this section, we will study

CASE 1. Assume that

$$k|\mathcal{A}(d_1)| \le 180\frac{N}{g}\ . \tag{35}$$

By (33) and (34), we may apply Lemma 2 with $\left[\frac{N}{g}\right]+1$, $\left[\frac{k-1}{2}\right]$, Q and 1 in place of M, k, $\mathcal{A}$ and a^*, respectively. We obtain that there is an integer m such that

$$\begin{aligned}\left|\left\{m+1,m+2,\dots,m+\left[\frac{N}{g}\right]+1\right\}\cap\left[\frac{k-1}{2}\right]Q\right| \ge \\ \ge \left(\min\left(1,\left[\frac{k-1}{2}\right]\frac{|Q|}{6([N/g]+1)}\right)\right)\left(\left[\frac{N}{g}\right]+1\right)\ .\end{aligned} \tag{36}$$

By (32) and (35), here we have

$$\left[\frac{k-1}{2}\right]\frac{|Q|}{6([N/g]+1)} \le \frac{k}{2}\frac{|\mathcal{A}(d_1)|+1}{6([N/g]+1)} \le \frac{k|\mathcal{A}(d_1)|}{6([N/g]+1)} \le \frac{180}{6} = 30\ . \tag{37}$$

It follows from (20), (32), (36) and (37) that

$$\begin{aligned}\left|\left\{m+1,m+2,\dots,m+\left[\frac{N}{g}\right]+1\right\}\cap\left[\frac{k-1}{2}\right]Q\right| \ge \frac{1}{30}\left[\frac{k-1}{2}\right]\frac{|Q|}{6} \ge \\ \ge \frac{1}{30}\cdot\frac{9}{20}k\cdot\frac{|\mathcal{A}(d_1)|}{6} = \frac{1}{400}k|\mathcal{A}(d_1)|\ .\end{aligned} \tag{38}$$

Clearly, $n = n_1 + n_2 + \dots + n_{[(k-1)/2]} \in \left[\frac{k-1}{2}\right]Q$ (where n_1, $n_2,\dots,n_{[(k-1)/2]} \in Q$) if and only if $\left[\frac{k-1}{2}\right](d_1+a'-g)+ng \in \left[\frac{k-1}{2}\right]\mathcal{P}$. Thus it follows from (38) that writing $m' = \left[\frac{k-1}{2}\right](d_1+a'-g)+mg$, we have

$$\begin{aligned}\left|\left\{m'+g,m'+2g,\dots,m'+\left(\left[\frac{N}{g}\right]+1\right)g\right\}\cap\left[\frac{k-1}{2}\right]\mathcal{P}\right| = \\ = \left|\left\{m+1,m+2,\dots,m+\left[\frac{N}{g}\right]+1\right\}\cap\left[\frac{k-1}{2}\right]Q\right| \ge \frac{1}{400}k|\mathcal{A}(d_1)|\ .\end{aligned} \tag{39}$$

Write

$$\mathcal{R} = \mathcal{D} + \left(\{m'+g, m'+2g, \dots, m'+([N/g]+1)g\} \cap \left[\frac{k-1}{2}\right]\mathcal{P}\right).$$

Then by (30),

$$\mathcal{R} \subset \left(2\left[\frac{k-1}{2}\right]+1\right)\mathcal{A}. \tag{40}$$

By $\mathcal{D} \subset \{1,2,\dots,N\}$, for $r \in \mathcal{R}$ clearly we have

$$1+m'+g \le r \le N+m'+([N/g]+1)g \le N+m'+N+g = 2N+m'+g$$

so that

$$\mathcal{R} \subset \{m'+g+1,\ m'+g+2,\dots,m'+g+2N\}. \tag{41}$$

If $d, d' \in \mathcal{D}$, $d \neq d'$ and $p,p' \in \left(\left\{m'+g, m'+2g, \dots, m'+\left(\left[\frac{N}{g}\right]+1\right)g\right\} \cap \left[\frac{k-1}{2}\right]\mathcal{P}\right)$, then

$$d \not\equiv d' \pmod{g} \quad \text{and} \quad p \equiv p' \pmod{g}$$

whence

$$d+p \neq d+p'.$$

Thus by (25) and (39) we have

$$|\mathcal{R}| = |\mathcal{D}| \cdot \left|\left\{m'+g, m'+2g, \dots, m'+\left(\left[\frac{N}{g}\right]+1\right)g\right\} \cap \left[\tfrac{k-1}{2}\right]\mathcal{P}\right| \ge \tag{42}$$

$$\ge t \cdot \tfrac{1}{400}k|\mathcal{A}(d_1)| \ge \tfrac{1}{400}k|\mathcal{A}|.$$

By the pigeon hole principale, it follows from (40), (41) and (42) that

$$\left|\{m'+g+\varepsilon N+1, m'+g+\varepsilon N+2, \dots, m'+g+\varepsilon N+N\} \cap \left(2\left[\tfrac{k-1}{2}\right]+1\right)\mathcal{A}\right| > \tfrac{1}{800}k|\mathcal{A}| \tag{43}$$

holds with either $\varepsilon = 0$ or $\varepsilon = 1$.

If k is odd, then $2\left[\frac{k-1}{2}\right]+1=k$ so that by (43), (3) holds with $m'+g+\varepsilon N$ and 1 in place of m and d, respectively. If k is even, then $2\left[\frac{k-1}{2}\right]+1=k-1$. Thus by (43),

$$\begin{aligned}
&|\{m'+g+\varepsilon N+a_1+1, m'+g+\varepsilon N+a_1+2,\dots,m'+g+\\
&\qquad +\varepsilon N+a_1+N\}\cap k\mathcal{A}|\geq\\
&\geq\Big|\{m'+g+\varepsilon N+a_1+1, m'+g+\varepsilon N+a_1+2,\dots,m'+g+\\
&\qquad +\varepsilon N+a_1+N\}\cap\Big(\Big(2\Big[\tfrac{k-1}{2}\Big]+1\Big)\mathcal{A}+\{a_1\}\Big)\Big|=\\
&=\Big|\{m'+g+\varepsilon N+1, m'+g+\varepsilon N+2,\dots,m'+\\
&\qquad +g+\varepsilon N+N\}\cap\Big(2\Big[\tfrac{k-1}{2}\Big]+1\Big)\mathcal{A}\Big|>\tfrac{1}{800}k|\mathcal{A}|
\end{aligned}$$

so that again, (3) holds with $m'+g+\varepsilon N+a_1$ and 1 in place of m and d, respectively, and this completes the proof in Case 1.

6. Assume now that

CASE 2.

$$k|\mathcal{A}(d_1)|>180\frac{N}{g}\,. \tag{44}$$

First we will show that there is an integer z with

$$\Big\{z+g, z+2g,\dots,z+\Big[\frac{1}{30}k|\mathcal{A}(d_1)|\Big]g\Big\}\subset 2\Big[\frac{k}{4}\Big]\mathcal{A}\,. \tag{45}$$

By (44) and $g<N$ we have

$$\Big[\frac{1}{30}k|\mathcal{A}(d_1)|\Big]\geq\frac{1}{30}k|\mathcal{A}(d_1)|-1>6\frac{N}{g}-1>6\Big[\frac{N}{g}\Big]-1>\Big[\frac{N}{g}\Big]+1\,. \tag{46}$$

By (33), (34) and (46), we may apply Lemma 2 with $\left[\frac{1}{30}k|\mathcal{A}(d_1)\right]$, $\left[\frac{k}{4}\right]$, Q and 1 in place of M, k, $\mathcal{A}$ and a^*, respectively. We obtain that there is an integer m such that

$$\begin{aligned}
&\Big|\Big\{m+1, m+2,\dots,m+\Big[\tfrac{1}{30}k|\mathcal{A}(d_1)|\Big]\Big\}\cap\Big[\tfrac{k}{4}\Big]Q\Big|\geq\\
&\geq\Big(\min\Big(1,\tfrac{[k/4]}{6}\frac{|Q|}{[\frac{1}{30}k|\mathcal{A}(d_1)|]}\Big)\Big)\cdot\Big[\tfrac{1}{30}k|\mathcal{A}(d_1)|\Big]\,.
\end{aligned} \tag{47}$$

By (20) and (32), here we have

$$\frac{[k/4]}{6}\frac{|Q|}{[\frac{1}{30}k|\mathcal{A}(d_1)|]} > \frac{k}{30}\frac{|\mathcal{A}(d_1)|}{[\frac{1}{30}k|\mathcal{A}(d_1)|]} = 1 .$$

Thus it follows from (47) that

$$\left|\left\{m+1, m+2, \dots, m+\left[\frac{1}{30}k|\mathcal{A}(d_1)|\right]\right\} \cap \left[\frac{k}{4}\right]Q\right| \geq \left[\frac{1}{30}k|\mathcal{A}(d_1)|\right]$$

whence

$$\left\{m+1, m+2, \dots, m+\left[\frac{1}{30}k|\mathcal{A}(d_1)|\right]\right\} \subset \left[\frac{k}{4}\right]Q .$$

By (28) and (31), this implies that, writing $m' = \left[\frac{k}{4}\right](d_1 + a' - g) + mg$, we have

$$\left\{m'+g, m'+2g, \dots, m'+\left[\frac{1}{30}k|\mathcal{A}(d_1)|\right]g\right\} \subset \left[\frac{k}{4}\right]\mathcal{P} \subset 2\left[\frac{k}{4}\right]\mathcal{A}$$

which completes the proof of (45).

7. Let us write

$$h = \left[\frac{1}{180}\frac{k|\mathcal{A}(d_1)|g}{N}\right] .$$

Then by (44),

$$h \geq 1 . \tag{48}$$

Moreover, it follows from (22) that

$$h \leq \frac{1}{180}\frac{k|\mathcal{A}(d_1)|g}{N} < \frac{1}{180}k|\mathcal{A}(d_1)| \cdot \frac{2}{|\mathcal{A}|} \leq \frac{1}{90}k . \tag{49}$$

Let us write

$$\mathcal{E} = \bigcup_{i=1}^{t}\{d_i, d_i+g, d_i+2g, \dots\} .$$

By Lemma 3, there is a divisor g' of g such that $h\varepsilon$ is the union of u disjoint infinite arithmetic progression of difference g' :

$$h\mathcal{E} = \bigcup_{i=1}^{u}\{e_i, e_i+g', e_i+2g', \dots\} \tag{50}$$

where

$$\frac{u}{g'} \geq h\frac{t}{g} - \frac{h-1}{g'} . \tag{51}$$

Again, we have to distinguish two cases. In this section, we will study

CASE 2. a) Assume that

$$\frac{u}{g'} > \frac{h}{2}\frac{t}{g} . \tag{52}$$

Since $h\mathcal{E}$ is the union of u disjoint infinite arithmetic progressions of difference g' and $g'|g$, thus $h\mathcal{E}$ is the union of $u \cdot \frac{g}{g'}$ disjoint infinite arithmetic progressions of difference g. Denote the set of the least elements of these arithmetic progressions by $\mathcal{F}$ so that

$$|\mathcal{F}| = u \cdot \frac{g}{g'} \tag{53}$$

and

$$f, f' \in \mathcal{F} \quad \text{implies} \quad f \not\equiv f' \,(\mathrm{mod}\, g) . \tag{54}$$

Moreover, it follows from the definitions of ε and $\mathcal{F}$ that

$$\mathcal{F} \subset h\mathcal{D} . \tag{55}$$

By (49) we have

$$2\left[\frac{k}{4}\right] + h < \frac{k}{2} + \frac{k}{2} = k . \tag{56}$$

It follows from (26), (45), (55) and (56) that

$$\begin{aligned} &\left\{z+g, z+2g, \ldots, z+\left[\tfrac{1}{30}k|\mathcal{A}(d_1)|\right]g\right\} + \mathcal{F} + \\ &+\left\{\left(k-2\left[\tfrac{k}{4}\right]-h\right)a_1\right\} \subset \\ &\subset 2\left[\tfrac{k}{4}\right]\mathcal{A} + h\mathcal{D} + \left(k-2\left[\tfrac{k}{4}\right]-h\right)\mathcal{A} \subset \\ &\subset 2\left[\tfrac{k}{4}\right]\mathcal{A} + h\mathcal{A} + \left(k-2\left[\tfrac{k}{4}\right]-h\right)\mathcal{A} = k\mathcal{A} . \end{aligned} \tag{57}$$

By (25), (44), (52), (53) and (54), the cardinality of the sum set in (57) is

$$\left|\left\{z+g, z+2g, \dots, z+\left[\tfrac{1}{30}k|\mathcal{A}(d_1)|\right]g\right\}+\mathcal{F}+\right.$$

$$(58)\quad \left.+\left\{\left(k-2\left[\tfrac{k}{4}\right]-h\right)a_1\right\}\right| =$$

$$= \left[\tfrac{1}{30}k|\mathcal{A}(d_1)|\right]|\mathcal{F}| > \tfrac{1}{50}k|\mathcal{A}(d_1)|u\tfrac{g}{g'} > \tfrac{1}{100}hkt|\mathcal{A}(d_1)| \geq \tfrac{1}{100}hk|\mathcal{A}| .$$

Moreover, by (55), $\mathcal{F} \subset \{1, 2, \dots, hN\}$. Thus writing $z' = z+\left(k-2\left[\frac{k}{4}\right]-h\right)a_1$, all the elements of the sum set in (57) are greater, than z', and, by (48), they do not exceed

$$z' + \left[\frac{1}{30}k|\mathcal{A}(d_1)|\right]g + hN \leq z' + \frac{1}{30}k|\mathcal{A}(d_1)|g + hN =$$

$$= z' + 6\cdot\frac{1}{180}\frac{k|\mathcal{A}(d_1)|g}{N}\cdot N + hN \leq z' + 3hN + hN = z' + 4hN .$$

Thus it follows from (57) and (58) that

$$|\{z'+1, z'+2, \dots, z'+4hN\} \cap k\mathcal{A}| > \frac{1}{100}hk|\mathcal{A}| .$$

By the pigeon hole principle, this implies that there is a positive integer i such that $i \leq 4h$ and

$$|\{z'+(i-1)N+1, z'+(i-1)N+2, \dots, z'+iN\} \cap k\mathcal{A}| >$$
$$> \tfrac{1}{4h}\cdot\tfrac{1}{100}hk|\mathcal{A}| = \tfrac{1}{400}k|\mathcal{A}| ,$$

so that (3) holds with $m = z'+(i-1)N$, $d = 1$ and this completes the proof in Case 2.a).

8. Assume finally that

CASE 2. b)

$$(59)\qquad \frac{u}{g'} \leq \frac{h}{2}\frac{t}{g} .$$

It follows from (51) and (59) that

$$\frac{h}{2}\frac{t}{g} \geq \frac{u}{g'} \geq h\frac{t}{g} - \frac{h-1}{g'} ,$$

whence

$$\frac{h}{2}\frac{t}{g} \leq \frac{h-1}{g'} < \frac{h}{g'}$$

so that

$$\frac{t}{2} \leq \frac{g}{g'} . \tag{60}$$

Consider the set $\mathcal{E}$ defined in Section 7. By (50), $h\mathcal{E}$ is the non–empty union of disjoint infinite arithmetic progressions of difference g'. Consider one of these arithmetic progressions, say, $\{e_1, e_1+g', e_1+2g', \ldots\}$. By the definition of $\mathcal{E}$, for each element $e_1 + jg'$ of this progression there is an integer $d^{(j)}$ such that, by (26),

$$d^{(j)} \in h\mathcal{D} \subset h\mathcal{A} \tag{61}$$

and

$$d^{(j)} \equiv e_1 + jg' \pmod{g} . \tag{62}$$

Define z by (45). It follows from (45), (56) and (61) that

$$\begin{aligned} &\left\{z+g, z+2g, \ldots, z+\left[\tfrac{1}{30}k|\mathcal{A}(d_1)|\right]g\right\} + \left\{d^{(1)}, d^{(2)}, \ldots, d^{(g/g')}\right\} + \\ &+\left(k-2\left[\tfrac{k}{4}\right]-h\right)\{a_1\} \subset 2\left[\tfrac{k}{4}\right]\mathcal{A} + h\mathcal{A} + \left(k-2\left[\tfrac{k}{4}\right]-h\right)\mathcal{A} = k\mathcal{A} . \end{aligned} \tag{63}$$

Let z' denote the greatest integer with

$$z' < z + g + hN + \left(k - 2\left[\frac{k}{4}\right] - h\right)a_1 \tag{64}$$

and

$$z' \equiv z + e_1 + \left(k - 2\left[\frac{k}{4}\right] - h\right)a_1 \pmod{g'} , \tag{65}$$

and write

$$v = \left[\frac{(\left[\frac{1}{30}k|\mathcal{A}(d_1)|\right]-1)g - hN}{g'}\right] .$$

Then by (25), (44), (60) and $g' \leq g < N$ we have

$$\begin{aligned} v &\geq \tfrac{1}{g'}\left(\left(\tfrac{1}{30}k|\mathcal{A}(d_1)|-2\right)g - hN\right) - 1 \\ &\geq \tfrac{1}{g'}\left(\left(\tfrac{1}{30}k|\mathcal{A}(d_1)|-3\right)g - hN\right) > \\ &> \tfrac{N}{g'}\left(\tfrac{1}{60}k|\mathcal{A}(d_1)|\tfrac{g}{N} - \tfrac{1}{180}\tfrac{k|\mathcal{A}(d_1)|g}{N}\right) = \tfrac{1}{90}k|\mathcal{A}(d_1)|\tfrac{g}{g'} \geq \\ &\geq \tfrac{1}{180}k|\mathcal{A}(d_1)|t \geq \tfrac{1}{180}k|\mathcal{A}| . \end{aligned} \tag{66}$$

Now we will prove that

(67)
$$\{z'+g', z'+2g', \dots, z'+vg'\} \subset$$
$$\subset \left\{z+g, z+2g, \dots, z+\left[\tfrac{1}{30}k|\mathcal{A}(d_1)|\right]g + \left\{d^{(1)}, d^{(2)}, \dots, d^{(g/g')}\right\} + \right.$$
$$\left. + \left(k - 2\left[\tfrac{k}{4}\right] - h\right)\{a_1\}\right.$$

It suffices to show that for every $1 \le i \le v$ there is a j such that

(68)
$$z'+ig'-d^{(j)}-\left(k-2\left[\frac{k}{4}\right]-h\right)a_1 \in \left\{z+g, z+2g, \dots, z+\left[\frac{1}{30}k|\mathcal{A}(d_1)|\right]g\right\}.$$

By (65),

$$z'+ig'-\left(k-2\left[\frac{k}{4}\right]-h\right)a_1 \equiv z'-\left(k-2\left[\frac{k}{4}\right]-h\right)a_1 \equiv z+e_1 \pmod{g'}.$$

Thus by $g'|g$ and (62), there is a j such that

$$z'+ig'-\left(k-2\left[\frac{k}{4}\right]-h\right)a_1 \equiv z+e_1+jg' \equiv z+d^{(j)} \pmod{g}$$

whence

$$z'+ig'-d^{(j)}-\left(k-2\left[\frac{k}{4}\right]-h\right)a_1 \equiv z \pmod{g}. \tag{69}$$

Moreover, by (61) and the definition of z' we have

$$z'+ig'-d^{(j)}-\left(k-2\left[\frac{k}{4}\right]-h\right)a_1 \ge$$
$$\ge \left(z+g+hN+\left(k-2\left[\frac{k}{4}\right]-h\right)a_1-g'\right)+g'-hN- \tag{70}$$
$$\left(k-2\left[\frac{k}{4}\right]-h\right)a_1 = z+g$$

and, by (64),

$$z'+ig'-d^{(j)}-\left(k-2\left[\frac{k}{4}\right]-h\right)a_1 <$$
$$< \left(z+g+hN+\left(k-2\left[\frac{k}{4}\right]-h\right)a_1\right)+vg'-1-\left(k-2\left[\frac{k}{4}\right]-h\right)a_1 \tag{71}$$
$$= z+g+hN+vg'-1 <$$
$$< z+g+hN+\frac{\left(\left[\frac{1}{30}k|\mathcal{A}(d_1)|\right]-1\right)g-hN}{g'}g' = z+\left[\tfrac{1}{30}k|\mathcal{A}(d_1)|\right]g.$$

(68) follows from (69), (70) and (71) and this completes the proof of (67).

By (63) and (67) we have

$$\{z' + g', z' + 2g', \dots, z' + vg'\} \subset k\mathcal{A} .$$

By (66), it follows that

$$|\{z' + g', z' + 2g', \dots, z' + Ng'\} \cap k\mathcal{A}| \geq \min(N, v) \geq$$
$$\geq \min\left(N, \tfrac{1}{180}k|\mathcal{A}|\right) = \left(\min\left(1, \tfrac{1}{180}k\tfrac{|\mathcal{A}|}{N}\right)\right)N$$

so that (3) holds with z' and g' in place of m and d, respectively, and this completes the proof of Theorem 2.

REFERENCES

[1] F. DYSON. — A theorem on the densities of sets of integers, *J. London Math. Soc.* **20**, (1945), 8–14.

[2] M. KNESER. — Abschätzungen der asymptotischen Dichte von Summenmengen, *Math. Zeit.* **58**, (1953), 459–484.

[3] H.B. MANN. — A proof of the fundamental theorem on the density of sums of sets of positive integers, *Ann. of Math.* **32**, (1942), 523–527.

[4] M.B. NATHANSON and A. SÁRKÖZY. — Sumsets containing long arithmetic progressions and powers of 2, *Acta Arithmetica* **54**, (1989), 147–154.

[5] A. SÁRKÖZY. — Finite addition theorems, I, *J. Number Theory* **32**, (1989), 114–130.

[6] A. SÁRKÖZY. — Finite addition theorems, II, *J. Number Theory*, to appear.

A. SÁRKÖZY
Mathematical Institute
of the Hungarian Academy of Sciences
1053 Budapest, Reáltanoda u. 13–15
HONGRIE

N° d'impression 1301
1er trimestre 1992