PUBLICATIONS MATHEMATIQUES D'ORSAY

83.04

JOURNÉES ARITHMÉTIQUES (S.M.F.)

COLLOQUE HUBERT DELANGE

7 & 8 JUIN 1982

Université de Paris-Sud

Département de Mathématique

Bât. 425

91405 ORSAY France

PUBLICATIONS

MATHEMATIQUES

D'ORSAY

83.04

JOURNÉES ARITHMÉTIQUES (S.M.F.)

COLLOQUE HUBERT DELANGE

7 & 8 JUIN 1982

Université de Paris-Sud

Département de Mathématique

Bât. 425

91405 ORSAY France

COLLOQUE EN L'HONNEUR DE

HUBERT DELANGE

JOURNÉES ARITHMÉTIQUES (S.M.F.)

ORSAY, 7 & 8 JUIN 1982

Hubert DELANGE, professeur à l'Université de Paris-Sud a pris sa retraite le 1er octobre 1982.

Des journées arithmétiques ont été organisées, à cette occasion, les 7 et 8 juin 1982, à Orsay. Elles ont pu avoir lieu grâce à l'aide financière de la Société Mathématique de France, du C.N.R.S. et de l'Université Paris-Sud.

Ce colloque, dont Georges POITOU assurait la Présidence d'Honneur, a été ouvert par Jacques DENY. Un pot, réunissant les participants et les membres du laboratoire de Mathématiques d'Orsay, a été l'occasion, pour Jean-Pierre KAHANE, de saluer un fondateur d'Orsay et de lui témoigner l'estime qu'ont pour lui l'ensemble de ses collègues.

Un certain nombre de mathématiciens ont désiré s'associer à cette manifestation, soit en participant à ce colloque et en y faisant des exposés, soit en envoyant une contribution écrite. L'ensemble de ces travaux est réuni ici.

L'organisation matérielle de ces journées et de cette publication est l'oeuvre de Nicole Parvan, d'Anne-Marie Baillet et de Marcelle Bonnardel qui se sont acquittées de cette tâche avec compétence et gentillesse.

H. DABOUSSI

TABLE DES MATIÈRES

UNE PROPRIÉTÉ EXTRÉMALE DE SUITES AUTOMATIQUES

Jean-Paul ALLOUCHE et Michel COSNARD

INTRODUCTION.

Pour étudier les itérées d'une fonction unimodale d'un intervalle dans lui-même, deux types d'approches sont possibles :

- une approche topologique qui consiste à définir une relation d'équivalence sur l'ensemble des fonctions, de sorte que deux fonctions équivalentes aient même comportement itératif et qu'on sache étudier un représentant de chaque classe,
- une approche combinatoire (voir [3], [5], [6], [7], [8], [9], [10]) qui consiste à associer aux itérés successifs d'un point une suite à valeurs dans un ensemble fini, de sorte qu'une partie des propriétés du comportement itératif de la fonction se ramène à l'étude de certaines de ces suites.

Nous nous proposons, en adoptant ce second point de vue, de montrer le rôle particulier joué par certaines suites automatiques, baptisées q-miroir, et parmi elles par la suite de Thue-Morse ; puis nous donnerons une interprétation des résultats obtenus en termes de théorie des nombres.

Nous ne donnerons pas ici de démonstrations, on pourra les trouver dans [2] (voir aussi [1]).

I. - ORIGINE DU PROBLEME ; QUELQUES DEFINITIONS :

Fonctions unimodales :

Soit c un réel de $]0,1[$, on dit qu'une fonction f est unimodale si :

$$\begin{cases} f \text{ est continue de } [0,1] \text{ dans lui-même,} \\ f(1) = 0 \text{ et } f(c) = 1, \\ f \text{ est strictement croissante sur } [0,c[, \\ f \text{ est strictement décroissante sur }]c,1]. \end{cases}$$

Le codage ; itinéraire d'un point :

On définit γ par

$$\gamma(x) = \begin{cases} 0 & \text{si } x \in [0,c[, \\ 1 & \text{si } x \in]c,1], \\ \{0,1\} & \text{si } x = c. \end{cases}$$

Si x n'est pas un antécédent de c par l'une des f^n, on appelle itinéraire de x, et on note $\sigma_f(x)$ la suite $\sigma_f(x) = (\gamma(f^n(x)))_n$, c'est un élément de $\{0,1\}^{\mathbb{N}}$. Sinon il est possible de faire en sorte que $(\gamma(f^n(x)))_n$ soit formé d'au plus deux suites à valeurs dans $\{0,1\}$, on note alors $\sigma_f(x) = \{\sigma_f^-(x), \sigma_f^+(x)\}$ l'itinéraire de x.

Notations :

On munit $\{0,1\}^{\mathbb{N}}$ de l'ordre lexicographique, noté $\leq$, et induit par $0 < 1$.

On identifie $\{0,1\}^{\mathbb{N}}$ et $(\mathbb{Z}/2\mathbb{Z})^{\mathbb{N}}$, et on définit pour une suite A dans $\{0,1\}^{\mathbb{N}}$:

$$dA(n) = A(n+1),$$
$$\tau A(n) = \sum_{0 \leq j \leq n} A(j),$$
$$\bar{A}(n) = 1 + A(n).$$

THEOREME 1. *a) Soit A dans $\{0,1\}^{\mathbb{N}}$ telle que $A(0) = 1$, $A(1) = 0$, alors : il existe une fonction f unimodale telle que $A = \sigma_f(1)$ si et seulement si $\forall\, k \geq 0 \quad \overline{\tau A} \leq d^k(\tau A) \leq \tau A$; une telle suite A est dite maximale.*

b) Prenons A et f comme ci-dessus, et soit B dans $\{0,1\}^{\mathbb{N}}$ alors : il existe x dans $[0,1]$ tel que $B \in \sigma_f(x)$ si et seulement si $\forall\, k \geq 0$ $\overline{\tau A} \leq d^k(\tau B) \leq \tau A$; une telle suite B est dite A-admissible.

II. - ETUDE DE L'ENSEMBLE Γ :

D'après le théorème 1 a) ci-dessus, l'étude des suites maximales se ramène à l'étude de l'ensemble

$$\Gamma = \{A \in \{0,1\}^{\mathbb{N}} \ ; \ A(0) = A(1) = 1 \text{ et } \forall\, k \geq 0, \ \bar{A} \leq d^k A \leq A\} .$$

1°) Γ a la puissance du continu :

Plus précisément, soit $M \neq 1^\omega$ (1^ω est la suite constante égale à 1), alors $\Gamma \cap]M,1^\omega[$ a la puissance du continu.

En effet, si n est un entier supérieur ou égal à 3, les suites $1^n\ 0\ 1'\ 0\ 1'\ 0\ 1'...$, où $1'$ vaut 1 ou 11, sont dans Γ ; de plus, pour n assez grand, toute suite commençant par 1^n est dans l'intervalle $]M,1^\omega[$.

Ce résultat n'est pas nouveau puisqu'il figure implicitement dans [3].

2°) La suite de Thue-Morse :

La suite de Thue-Morse peut être définie comme le point fixe de la 2-substitution $0 \rightarrow 01$, $1 \rightarrow 10$ commençant par 0 (voir [4] par exemple), de sorte que cette suite commence par 01 10 1001 10010110.... .

Nous noterons L la première décalée de cette suite, de sorte que

$L = 110\ 1001\ 10010110\ \ldots$.

THEOREME 2. *Soit* A *une suite de* Γ, *telle que* $A < L$, *alors* A *est* 2^n*-périodique et* $d^{2^{n-1}} A = \bar{A}$.

Plus précisément $\Gamma \cap [0^\omega,L[= \{(1100)^\omega, (11010010)^\omega, \ldots\}$ *est un ensemble discret dénombrable dont* L *est le seul point d'accumulation (en particulier* L *est dans* Γ*).*

L'idée de la démonstration est donnée par les deux considérations "expérimentales" suivantes :

si une suite A est dans Γ et strictement inférieure à L, alors il existe un entier n au moins égal à 2, tel que $A(j) = L(j)$ pour j dans $[0,2^n-2]$ et $A(2^n-1) \neq L(2^n-1)$; par ailleurs, une suite vérifiant ces deux conditions est nécessairement périodique, de période 2^n ; (il est facile de se convaincre que si A est dans Γ et commence par 1100... par exemple, alors $A = (1100)^\omega$, c'est-à-dire 1100 1100 1100...).

Metropolis, Stein et Stein [8] ont les premiers construit les itinéraires correspondant aux premières suites 2^n-périodiques. Une démonstration rigoureuse du caractère universel de ce codage pour les suites périodiques a été obtenue par

Derrida, Gervois et Pomeau ([5]). Le fait que les suites (1100) , (11010010) ... sont consécutives dans Γ est explicite dans Collet Eckmann ([3]). Dans [7] Jonker utilise une application analogue à τ (l'intérêt de τ est que Γ est plus facile à étudier que $\tau^{-1}\Gamma$), et une suite λ qui joue le même rôle que L. Ce qui est nouveau ici, c'est l'identification de L comme étant la première décalée de la suite de Thue-Morse : L fait partie d'une classe de suites automatiques étudiées ci-dessous et qui permettent de généraliser le théorème 2.

3°) Les suites q-miroir et une généralisation du théorème 2 :

DEFINITION. *Soit* q *un entier supérieur ou égal à* 1, *on dit que la suite* Q *est* q-*miroir si :*

$$\begin{cases} \forall\ k \geq 0 \quad \forall\ j \in [0,\ q2^k - 2] \quad Q(q2^k + j) = \bar{Q}(j), \\ \forall\ k \geq 0 \quad Q(q2^k - 1) = 1 \end{cases}$$

Exemples : si $q = 3$ et $Q(0) = Q(1) = 1$, alors $Q = 111/001/000111/\ldots$,

si $q = 1$, alors $Q = L$,

si $q = 2$ et $Q(0) = 1$, alors $Q = L$.

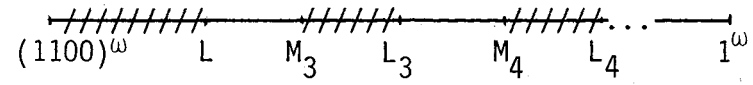
PROPOSITION. *Soit* Q *une suite* q-*miroir, alors* Q *n'est pas ultérieurement périodique, et elle est reconnue par un* 2-*automate (voir* [4]). *Plus précisément, la série formelle* $\sum_0^\infty Q(n)\ X^n$ *est quadratique sur* $\mathbb{Z}_{/2\mathbb{Z}}(X)$.

On peut alors donner une généralisation du théorème 2 ; pour $j \geq 3$ notons L_j la suite j-miroir telle que pour tout k dans [0,j-2], on ait $L_j(k) = 1$, et notons $M_j = (1^{j-1}0)^\omega$.

THEOREME 2'. *a) Les ensembles* $\Gamma \cap [(1100)^\omega, L[$ *et* $\Gamma \cap [M_j, L_j[$ *pour* $j \geq 3$ *sont discrets dénombrables ; les* L_j *sont dans* Γ.

Plus précisément, pour $j \geq 3$, $[M_j, L_j[\cap \Gamma = \{M_j, M_j^{(1)}, M_j^{(2)}, \ldots\}$ *où* $M_j^{(k)}$ *est* $2^k j$-*périodique, et où la suite* $(M_j^{(k)})_{k\geq 1}$ *croît vers* L_j.

b) Les ensembles $\Gamma \cap]L, M_3[$ *et* $\Gamma \cap]L_j, M_{j+1}[$ *pour* $j \geq 3$ *ont la puissance du continu.*



Les parties hachurées contiennent un nombre dénombrable d'éléments de Γ , les autres un nombre continu.

III. - LES ENSEMBLES Γ_A :

Soit A un élément de Γ , l'étude des suites $\tau^{-1}A$-admissibles se ramène d'après le théorème 1 b) à l'étude de l'ensemble $\Gamma_A = \{B \in \{0,1\}^{\mathbb{N}}$; $\forall\, k \geq 0$ $\bar{A} \leq d^k B \leq A\}$. Enonçons alors le théorème :

THEOREME 3. *a) Si l'on a* $A \in \Gamma$ *et* $A < L$, *alors* Γ_A *est dénombrable. Plus précisément, soit* B *un élément de* Γ_A, *alors ou bien* B *est l'une des suites* $(10)^\omega$ *ou* $(01)^\omega$, *ou bien il existe un entier* k *et un élément* U *de* Γ , *avec* $U \leq A$, *tels que* $d^k B = U$ *(en particulier* B *est ultérieurement périodique).*

b) Si A *est dans* Γ *et supérieur ou égal à* L, *alors* Γ_A *a la puissance du continu .*

Remarque : On peut énoncer un théorème "3'" en remplaçant L par L_j et en imposant à B des conditions supplémentaires.

IV. - RETOUR AUX ITERATIONS.

Traduisons les résultats précédents en termes d'itérations de fonctions unimodales ;

soit α une suite dans $\{0,1\}^{\mathbb{N}}$ et f une fonction unimodale telle que $\alpha = \sigma_f(1)$, alors :

- si $\tau\alpha < L$, pour chaque x de $[0,1]$ $f^n(x)$ est asymptotiquement périodique, de plus si la période de $\tau\alpha$ est 2^k, alors :
  - . f admet au moins un cycle d'ordre 2^i, quel que soit $i \leq k$,
  - . f peut admettre un cycle d'ordre 2^{k+1},
  - . f n'admet aucun cycle d'un autre ordre,

. quel que soit x, $(f^n(x))_n$ converge vers l'un de ces cycles.

- si $\tau\alpha = L$, f admet des cycles d'ordre 2^i, quel que soit l'entier i et au moins un Cantor invariant minimal C (C est une fermé non dénombrable, nulle part dense dans $[0,1]$, tel que $f(C) = C$, et quel que soit x dans C, l'ensemble des points d'accumulation de $f^n(x)$ est C).
De plus, quel que soit x dans $[0,1]$, $f^n(x)$ converge vers un cycle d'ordre 2^i ou vers un Cantor C (c'est-à-dire l'ensemble des points d'accumulation de $(f^n(x))_n$ est C).
- si $\tau\alpha > L$, f peut aussi admettre d'autres cycles et $(f^n(x))_n$ peut être une suite turbulente.

En particulier, soit f_μ une famille de fonctions unimodales admettant lorsque μ croît de 0 à μ_∞ une "cascade de Feigenbaum" (suite de bifurcations de cycles d'ordre 2^i en cycles d'ordre 2^{i+1}), alors $\tau(\sigma_{f_{\mu_\infty}}(1)) = L$ et $\tau(\sigma_{f_\mu}(1))$ décrit dans l'ordre l'ensemble $\{A \in \Gamma\ ;\ A < L\}$.

V. - TRADUCTION EN UN RESULTAT DE THEORIE DES NOMBRES.

THEOREME. *Notons pour un réel y, $\{y\}$ sa partie fractionnaire, et soit Γ' l'ensemble défini par :*

$$\Gamma' = \{x \in [0,1]\ ;\ \forall\, k \geq 0,\ 1 - x \leq \{2^k x\} \leq x\}.$$

La structure de Γ' peut être précisée de la manière suivante : pour $j \geq 2$, on pose $m_j = \frac{2^j - 2}{2^j - 1}$, et on définit ℓ_j par $\ell_2 = \sum_0^\infty \frac{L(n)}{2^{n+1}}$, $\ell_j = \sum_0^\infty \frac{L_j(n)}{2^{n+1}}$ pour $j \geq 3$; alors :

. les nombres ℓ_j et m_j sont dans Γ' ; de plus les ℓ_j sont transcendants.

. pour chaque j supérieur ou égal à 2, $\Gamma' \cap [m_j, \ell_j[$ ne contient que des rationnels, et le seul point d'accumulation de cet ensemble est ℓ_j.

. pour chaque j supérieur ou égal à 2, $\Gamma' \cap [\ell_j, m_{j+1}[$ a la puissance du continu.

En effet, si $x = \sum_{0}^{+\infty} \frac{A(n)}{2^{n+1}}$, x est dans Γ' si et seulement si A est dans Γ , ou $A = 10\ldots$ et quel que soit k entier $\tilde{A} \leq d^k A \leq A$. Il est alors immédiat que x est dans Γ' si et seulement si A est dans $\Gamma \cup \{(10)\}^{\omega}$. Enfin la transcendance des ℓ_j résulte du caractère automatique des suites L et L_j (voir [4] p. 410 par exemple).

On peut alors se poser la question de l'étude de l'ensemble

$\{x \in [0,1] \; ; \; \forall \, k \geq 0 \quad 1-x \leq \{a^k x\} \leq x\}$.

Si a est entier, en développant x en base a au lieu de la base 2, on peut obtenir des résultats analogues à ceux qui précèdent ; en revanche, si a est non entier, nous ne savons rien dire sur la structure de cet ensemble.

REFERENCES

[1] J.P. ALLOUCHE et M. COSNARD. Une propriété extrémale de la suite de Thue-Morse liée aux cascades de Feigenbaum. Séminaire de Théorie des Nombres de Bordeaux (1982) (à paraître).

[2] J.P. ALLOUCHE et M. COSNARD. (En préparation).

[3] P. COLLET et J.P. ECKMANN. Iterated maps on the interval as dynamical systems. Birkhäuser, Boston-Basel-Stuttgart (1980).

[4] G. CHRISTOL, T. KAMAE, M. MENDES FRANCE et G. RAUZY. Suites algébriques, automates et substitutions. Bull. Soc. Math. France 108, 1980, 401-419.

[5] B. DERRIDA, A. GERVOIS et Y. POMEAU. Iteration of endomorphisms on the real axis and representation of numbers". Ann. Inst. H. Poincaré, 29, (1978) 3, 305-356.

[6] J. GUCKENHEIMER. Sensitive dependance to initial conditions for one dimensional maps. Comm. Math. Phys. 70 (1979), 133-160.

[7] L. JONKER. Periodic orbits and kneading invariants. Proc. of the Lond. Math. Soc. Serie 3 (39) 1979.

[8] N. METROPOLIS, M.L. STEIN, P.R. STEIN. On finite limit sets for transformations on the unit interval. J. Comb. Theory A 15(1973) 25-44.

[9] J. MILNOR, P. THURSTON. On iterated maps of the interval I and II. Preprint, Princeton (1977).

[10] G. RAUZY. Itérations des endomorphismes d'un intervalle. Séminaire de Théorie des Nombres, Paris, 79-80, Séminaire Delange-Pisot-Poitou, Birkhäuser.

J.P. ALLOUCHE
Ecole Normale Supérieure
FONTENAY AUX ROSES

M. COSNARD
Laboratoire I.M.A.G.
GRENOBLE

MODULI r FOR WHICH THERE ARE MANY SMALL PRIMES CONGRUENT TO A MODULO r

*Paul T. BATEMAN and Carl POMERANCE**

§1. Introduction.

Suppose a is a given non-zero integer. In this note we show that there is an infinitude of positive integers r (relatively prime to a) for each of which there are many primes p not much larger than r and congruent to a modulo r. We prove two theorems of this type, in the second of which we impose the additional requirement that the ratios $(p-a)/r$ are also prime. The proof of each theorem consists of a straightforward application of the pigeon-hole principle and is based only on classical results in multiplicative number theory. Arguments of the sort given here were used in an essential way in [1].

Our theorems are as follows. Both theorems remain true when $k = 0$ but are trivial in that case.

THEOREM 1. *If a is a given non-zero integer and k is a given positive integer, there are infinitely many positive integers r coprime to a for which we can find $k+1$ distinct primes $p_0, p_1, \ldots, p_k$ satisfying*

$$p_i \equiv a \pmod{r}, \quad p_i < e\, k\, r \log r$$

for $i = 0, 1, \ldots, k$.

* The research of the second-named author was supported by a grant from the National Science Foundation.

THEOREM 2. *Suppose* $\lambda > e$. *If* a *is a given non-zero integer and* k *is a given positive integer, there are infinitely many positive integers* r *coprime to* a *for which we can find* $k + 1$ *distinct primes* $p_0, p_1, \ldots, p_k$ *satisfying*

$$p_i \equiv a \pmod{r},\ (p_i - a)/r \text{ is prime},\ p_i < \lambda k r \log r \log\log r$$

for $i = 0, 1, \ldots, k$.

It is not hard to see that the prime k-tuples conjecture would imply stronger results than these theorems, for example the assertion in which the inequalities for the primes p_i in Theorem 1 are replaced by the inequalities of the form $p_i < Akr$, where A is a constant depending only on a. However, the inequalities for the primes p_i given in these theorems are about the best that can be expected by simple averaging arguments, aside possibly for constant factors (possibly depending on a.) This optimality follows from the fact that the relative frequency of primes around r is about $1/\log r$ and the relative frequency of primes around $\log r$ is about $1/\log\log r$. More specifically, in the case of Theorem 1 the early primes congruent to a modulo r could be expected to lie about $r \log r$ apart, so that we could not expect to find k such primes until we reach numbers of the order of magnitude $k r \log r$. In the case of Theorem 2 the ratios $(p_i - a)/r$ are $O((\log r)^{1+\varepsilon})$ and so the extra condition that these ratios are primes introduces an extra factor $\log\log r$ in the preceding discussion. In the case of both Theorems 1 and 2 we do not guarantee that the results cannot be improved by a

numerical factor (possibly depending on a.) In fact, in the case of Theorem 2, the condition $\lambda > e$ could be replaced by the condition $\log \lambda > \phi(a)/a$, where, as usual, $\phi(a)$ denotes the number of positive integers not exceeding $|a|$ and coprime to a.

The authors would like to thank Paul Erdős for his interest in these theorems.

§2. Necessary Lemmas.

We require the following classical results from multiplicative number theory. As usual $\pi(y;m,\ell)$ denotes the number of primes not exceeding y which are congruent to ℓ modulo m. In Lemmas B1 and B2 (as in our two theorems) the letter a stands for a given non-zero integer.

LEMMA A. *If* $y \geq 3$, *then*

$$\pi(y;m,\ell) = \frac{1}{\phi(m)} \int_2^y \frac{du}{\log u} + O\left(\frac{y}{(\log y)^{100}}\right)$$

for all m *less than* $(\log y)^{3/2}$ *and all* ℓ *relatively prime to* m, *where the constant implied by the* O *symbol is absolute and effectively computable.*

The result of Lemma A follows from equation (36) of (3). The exponent 3/2 could be replaced by any number less than 2 and the exponent 100 could be replaced by any positive constant whatever.

LEMMA B1. *If* ρ *is a fixed number greater than* 1, *then for* $y \geq 3$ *we have*

$$\sum_{y<q\leq \rho y,\ (q,a)=1} \frac{1}{\phi(q)} = C_a \log \rho + O\left(\frac{\log y}{y}\right),$$

where

$$C_a = \frac{\phi(a)}{a} \prod_{p\nmid a} \left(1 + \frac{1}{p(p-1)}\right) > \frac{\phi(a)}{a}$$

and the constant implied by the O*-symbol depends on* a.

PROOF. By [2] we have

$$\sum_{1\le q\le y,\ (q,a)=1} \frac{1}{\phi(q)} = C_a \log y + D_a + O\left(\frac{\log y}{y}\right),$$

where C_a is as above, D_a is another constant depending on a, and the constant implied by the O-symbol depends on a. The stated result follows by subtraction.

LEMMA B2. *If ρ is a fixed number greater than 1, then for $y \ge 3$ we have*

$$\sum_{y<q\le \rho y,\ q \text{ prime}} \frac{1}{\phi(q)} = \frac{\log \rho}{\log y} + O\left(\frac{1}{(\log y)^2}\right),$$

where the constant implied by the O-symbol depends on ρ.

PROOF. From Lemma A with $m = 1$ we readily obtain by partial summation

$$\sum_{1\le q\le y,\ q \text{ prime}} \frac{1}{\phi(q)} = \sum_{1\le q\le y,\ q \text{ prime}} \frac{1}{q-1}$$

$$= \log\log y + b + O\left(\frac{1}{(\log y)^{99}}\right),$$

where b is a certain absolute constant. By subtraction we obtain

$$\sum_{y<q\le \rho y,\ q \text{ prime}} \frac{1}{\phi(q)} = \log\left(1 + \frac{\log \rho}{\log y}\right) + O\left(\frac{1}{(\log y)^{99}}\right),$$

from which the conclusion of the lemma follows.

§3. Proof of Theorem 1.

Let K be a large positive constant, to be specified later in terms of a. For large positive x let P be the set of primes p such that $x<p\le(K+1)x$, let Q be the set of integers q such that

$$(q,a) = 1,\ (1+\frac{1}{K})\ \frac{k\ \phi(a)}{C_a\ a}\ \log x < q \le (1+\frac{1}{K})\ \frac{ek\phi(a)}{C_a\ a}\ \log x,$$

and let M be the set of pairs (p,q) with $p \in P$, $q \in Q$, and $p \equiv a \pmod q$. We define a function f on M by putting $f(p,q) = (p-a)/q$. In view of the definitions of P and Q, the range of f is contained in the set R consisting of the integers r satisfying

$$(r,a) = 1,\ \frac{C_a\ a\ (x-a)}{(1+K^{-1})\ e\ k\ \phi(a)\log x} < r < \frac{C_a\ a\{(K+1)x-a\}}{(1+K^{-1})k\ \phi(a)\log x}.$$

By Lemma A the cardinality of M is given by

$$\begin{aligned}|M| &= \sum_{q\in Q} \{\pi(\ (K+1)\ x;\ q,a) - \pi(x;q,a)\} \\ &= \sum_{q\in Q} \{\frac{1}{\phi(q)} \int_x^{(K+1)x} \frac{du}{\log u} + O(\frac{x}{(\log x)^{100}})\} \\ &= \sum_{q\in Q} \frac{1}{\phi(q)} \{\frac{Kx}{\log x} + O(\frac{x}{(\log x)^2}\} + O(\frac{x}{(\log x)^{99}}).\end{aligned}$$

By Lemma B 1

$$\sum_{q\in Q} \frac{1}{\phi(q)} = C_a + O(\frac{\log\log x}{\log x}),$$

so that

$$|M| = C_a K \frac{x}{\log x} + O(\frac{x \log\log x}{(\log x)^2}).$$

On the other hand the cardinality of R satisfies

$$|R| = C_a K\{1 - \frac{1}{(K+1)e}\} \frac{x}{k \log x} + O(1).$$

Hence for large K we have $k|R| < |M|$, so that the function f must take on some value at least $k + 1$ times. Thus for sufficiently large x there exists an element r of R and $k + 1$ distinct pairs $(p_0,q_0), (p_1,q_1),\ldots,(p_k,q_k)$ in M such that

$$\frac{p_0 - a}{q_0} = \frac{p_1 - a}{q_1} = \ldots = \frac{p_k - a}{q_k} = r.$$

Clearly the primes p_i are distinct and $p_i \equiv a \pmod r$ for each i. Further

$$p_i = q_i\, r + a \leq (1 + \frac{1}{K}) \frac{e\phi(a)}{C_a\, a} k\, r \log x + a.$$

Since $\log r = \log x + O(\log\log x)$, we have

$$p_i < (1 + \frac{2}{K}) \frac{e\phi(a)}{C_a\, a} k\, r \log r$$

if x is sufficiently large. Since $C_a > \frac{\phi(a)}{a}$, we may take K large enough so that

$$(1 + \frac{2}{K}) \frac{1}{C_a} \leq \frac{a}{\phi(a)}.$$

Then the primes p_i satisfy the inequality of the theorem, provided of course that x is sufficiently large. Since r tends to infinity with x, there are infinitely many positive integers r for which the conclusion of the theorem holds.

§4. Proof of Theorem 2.

Let K be a large positive constant and let ρ be a constant greater than 1, both of which will be specified later. For large positive x let P be the set of primes p such that $x < p \leq (K + 1)\, x$, let Q be the set of primes q such that

$$k \log x \operatorname{loglog} x < q \leq \rho\, k \log x \operatorname{loglog} x,$$

and let M be the set of pairs (p,q) with $p \in P$, $q \in Q$, and $p \equiv a \pmod q$. We define a function f on M by putting $f(p,q) = (p - a)/q$. Clearly the range of f is contained in the set R consisting of the integers r satisfying

$$\frac{x - a}{k\, \rho \log x \operatorname{loglog} x} < r < \frac{(K + 1)\, x - a}{k \log x \operatorname{loglog} x}.$$

As in the proof of Theorem 1 the cardinality of M is given by

$$|M| = \sum_{q \in Q} \frac{1}{\phi(q)} \{\frac{K\, x}{\log x} + O(\frac{x}{(\log x)^2}\} + O(\frac{x}{(\log x)^{99}}).$$

By Lemma B2

$$\sum_{q \in Q} \frac{1}{\phi(q)} = \frac{\log \rho}{\log(k \log x \operatorname{loglog} x)} + O(\frac{1}{(\operatorname{loglog} x)^2}),$$

so that

$$|M| = K \log \rho \, \frac{x}{\log x \operatorname{loglog} x} + O(\frac{x \operatorname{logloglog} x}{\log x\, (\operatorname{loglog} x)^2}).$$

On the other hand the cardinality of R satisfies

$$|R| = (K + 1 - \frac{1}{\rho}) \, \frac{x}{k \log x \operatorname{loglog} x} + O(1).$$

Hence for large x we have $k|R| < |M|$, provided that $\rho > e$ and we choose K large enough so that

$$K(\log \rho - 1) > 1 - 1/\rho.$$

Accordingly for sufficiently large x there exists an element r of R and $k + 1$ distinct pairs $(p_0,q_0), (p_1,q_1),\cdots,(p_k,q_k)$ in M such that

$$\frac{p_0 - a}{q_0} = \frac{p_1 - a}{q_1} = \cdots = \frac{p_k - a}{q_k} = r.$$

Clearly the primes p_i are distinct, $p_i \equiv a \pmod r$ for each i, and $(p_i - a)/r = q_i$ is prime for each i. Further

$$p_i = q_i\, r + a \leq \rho\, k\, r \log x \operatorname{loglog} x + a.$$

Since $\log r = \log x + O(\operatorname{loglog} x)$, we have

$$p_i < \rho\, k\, r \log r \operatorname{loglog} r + O(r\, (\operatorname{loglog} r)^2)$$

if x is sufficiently large. If we now choose ρ so that $e < \rho < \lambda$, say, $\rho = (e + \lambda)/2$, and choose $K > (1 - \rho^{-1})/(\log \rho - 1)$, we have

$$p_i < \lambda\, k\, r \log r \operatorname{loglog} r,$$

provided of course that x is sufficiently large x. Since r tends to infinity with x, there are infinitely many positive integers r for which the conclusion of the theorem holds.

By redefining the set R to include only integers coprime to a, we could replace the condition $\lambda > e$ in Theorem 2 by the condition $\log \lambda > \phi(a)/a$.

§5. Some Related Conjectures.

If a is a non-zero integer and r is a positive integer coprime to a, let $p_k(r,a)$ denote the k-th prime number congruent to a modulo r and greater than r. Put

$$c(r,a) = \sup_k \frac{p_k(r,a)}{k\ r\ \log(k\ r)}.$$

Since $p_k(r,a) = O(k \log k)$ for fixed r and a by Lemma A, clearly $c(r,a)$ exists.

Theorem 1 asserts that if a and k are given, there are infinitely many r coprime to a for which

$$p_k(r,a)/\{k\ r\ \log(k\ r)\} < e.$$

However $c(r,a)$ considers the somewhat deeper question of bounding the ratio $p_k(r,a)/\{k\ r\ \log(k\ r)\}$ for all positive integral values of k while r and a remain fixed. The following conjectures about $c(r,a)$ seem reasonable to us.

CONJECTURE 1. *There is an absolute constant* c *for which there are infinitely many pairs of integers* r,a *such that*

$$0 < |a| < r, \quad (r,a) = 1, \quad \text{and} \quad c(r,a) \leq c.$$

Conjecture 2 is the more specific form of Conjecture 1 in which a is specified in advance.

CONJECTURE 2. *There is an absolute constant* c *such that, for any given non-zero integer* a, *there are infinitely many positive integers* r *coprime to* a *for which*

$$c(r,a) \leq c.$$

Conjecture 3 is a quantitative form of Conjecture 2 in which we assert (1) that, for any positive c, a positive fraction of the positive integers coprime to a have the property $c(r,a) \leq c$ and also (2) that, if c is large, the vast majority of the positive integers coprime to a have the property $c(r,a) \leq c$. In order to state this formally, we need the following notation. If a is a non-zero integer and $c \geq 0$, we let $N(a,c,x)$ denote the number of integers r satisfying

$$(r,a) = 1, \quad 1 \leq r \leq x, \quad c(r,a) \leq c.$$

CONJECTURE 3. *If a is a given non-zero integer, then*

$$f_a(c) = \lim_{x \to +\infty} x^{-1} N(a,c,x)$$

exists for every $c \geq 0$ and is a continuous function of c. Moreover $f_a(c) > 0$ for $c > 0$ and

$$\lim_{c \to +\infty} f_a(c) = \phi(a)/a.$$

Clearly Conjecture 3 implies Conjecture 2, which in turn implies Conjecture 1. While Conjecture 3 seems difficult, Conjectures 1 and 2 may be assailable.

REFERENCES

1. Paul T. Bateman, Carl Pomerance, and Robert C. Vaughan, On the size of the coefficients of the cyclotomic polynomial, to be published in the Proceedings of the Colloquium on Number Theory held in Budapest, Hungary, June 20-26, 1981.

2. E. Landau, On a Titchmarsh-Estermann sum, J. London Math. Soc. 11, 242-245 (1936).

3. A Page, On the number of primes in an arithmetic progression, Proc. London Math. Soc. (2) 39, 116-141 (1935).

University of Illinois at Urbana-Champaign

University of Georgia

SUR LA REPRÉSENTATION DES MULTIPLES D'UN ENTIER DANS UNE BASE

Jean COQUET

Summary. Let s *denote the function "sum of binary digits" and* h_1, h_2 *different odd integers. The sequence :* $n \mapsto x_1 s(h_1 n)+x_2 s(h_2 n)$ *is proved to be uniformly distributed modulo 1 if at least one of the real numbers* x_1, x_2 *is irrational. Fourier-Bohr spectrum and pseudo-randomness of related exponential sums are studied.*

I. INTRODUCTION

Dans cet article, $s_q(n)$ désigne la somme des chiffres de l'entier naturel n en base q, q entier ≥ 2. On note $e(u) = e^{2i\pi u}$ pour tout u réel.

Confirmant une conjecture de L. Moser et des observations numériques de I. Barrodale et R. Mac Leod, D.J. Newman [8] a montré que $s_2(3n)$ était plus souvent pair qu'impair :

$$\frac{1}{20} N^c \leq \sum_{n<N} (-1)^{s_2(3n)} \leq 5\, N^c \qquad \text{où} \qquad c = \frac{\text{Log } 3}{\text{Log } 4} .$$

Dans [6], I. Kátai a étudié les rapports entre $s_2(n)$ et $s_2(3n)$ montrant que :

$$\lim_{N\to\infty} 2^{-N} \text{ Card } \{n < 2^N \ ; \ s_2(3n) - s_2(n) < x\sqrt{\frac{N}{3}}\} = \Phi(x),$$

où Φ est la fonction de répartition gaussienne, résultat qu'il a généralisé récemment [4] avec L. Dringo à $s_2(hn) - s_2(n)$ où h est un entier impair différent de 1, en remplaçant $\frac{1}{\sqrt{3}}$ par une constante convenable.

La motivation de cet article est d'étudier la répartition modulo 1 de suites analogues.

THEOREME 1. Etant donnés des réels $x_1,\ldots,x_r$ *et des entiers positifs distincts* $h_1,\ldots,h_r$, *si la suite de terme général* $F(n) = e(\sum_{j=1}^{r} x_j s_q(h_j n))$ *n'est pas constante (autrement dit, identiquement égale à 1), elle a une valeur moyenne nulle.*

On en déduit le :

THEOREME 2. Etant donnés des réels x_1, x_2 *et des entiers positifs distincts* h_1, h_2 *non divisibles par* q, *la suite de terme général* $x_1 s_q(h_1 n) + x_2 s_q(h_2 n)$ *est équirépartie modulo 1 si (et seulement si) l'un au moins des réels* x_1, x_2 *est irrationnel.*

Une conséquence du théorème 2 est le résultat suivant qui fait intervenir à la fois la somme des chiffres s_q et le nombre de diviseurs premiers ω :

COROLLAIRE. Si l'un au moins des réels x, y *est irrationnel, la suite de terme général* $x\, s_q(n) + y\, \omega(n)$ *est équirépartie modulo 1.*

Avec les notations du théorème 1, on démontre aussi un résultat sur le spectre [9] qui permet de préciser le théorème 2.

THEOREME 3. Si la suite F^{q-1} *n'est pas identiquement égale à 1, le spectre de Fourier-Bohr de* F *est vide.*

Ce résultat suggère une étude du caractère pseudo-aléatoire [9] de F que nous faisons, pour simplifier les calculs, dans un cas particulier : $q = 3$, $h_1 = 2$, $h_2 = 1$. Dans ce cas, si le spectre de F est vide, F est pseudo-aléatoire comme le montre le théorème 4. Est-ce vrai dans le cas général ?

THEOREME 4. Si l'un au moins des réels $2x$, $2y$ *n'est pas entier relatif, la suite de terme général* $e(x\, s_3(2n) + y\, s_3(n))$ *est pseudo-aléatoire* [9]

II. PREUVE DU THEOREME 1.

On suppose que $\mu = \limsup_{N\to\infty} \frac{1}{N} \left| \sum_{n<N} F(n) \right|$ n'est pas nulle.

Soit ρ une puissance de q assez grande pour que F ne soit pas constante sur l'ensemble $\{0, 1, \ldots, \rho-1\}$ et telle que $\rho > \text{Max}\,(h_1, \ldots, h_r)$. On utilise le développement des entiers naturels en base ρ :

$$n = \sum_{k=0}^{\infty} e_k(n)\, \rho^k \qquad \text{avec} \qquad 0 \leqslant e_k(n) < \rho \quad \text{pour tout entier } k.$$

Soit $\varepsilon > 0$ tel que $\left| \sum_{0\leqslant m<\rho} F(m) \right| \leqslant \rho - \varepsilon$. On choisit un entier $u > 0$ tel que $(1 - \rho^{-1})^u \leqslant \frac{\varepsilon}{2}\, \mu\rho^{-2}$. La densité asymptotique de l'ensemble E des entiers naturels pour lesquels $e_1(n), \ldots, e_u(n)$ sont tous non nuls, est majorée par $\frac{\varepsilon}{2}\, \mu\rho^{-2}$.

On partage $\mathbb{N} \setminus E$ en sous-ensembles

$$A_b = \{n \in \mathbb{N} \ ; \ b = \inf \{k \ ; \ 1 \leq k \leq u, \ e_k(n) = 0\}\} \ , \ 1 \leq b \leq u.$$

Tout entier n appartenant à A_b s'écrit $n = m + \rho^{b+1} n'$ avec $m < \rho^b$ de sorte que $s_q(h_j n) = s_q(h_j m) + s_q(h_j n')$ pour $1 \leq j \leq r$, donc $F(n) = F(m)F(n')$.

Ainsi, d(.) désignant la densité asymptotique,

$$\limsup_{N\to\infty} \frac{1}{N} \left| \sum_{\substack{n<N \\ n\in A_b}} F(n) \right| \leq \mu \, d(A_b).$$

Mais, pour b = 1, on a une majoration plus précise :

$$\limsup_{N\to\infty} \frac{1}{N} \left| \sum_{\substack{n<N \\ n\in A_1}} F(n) \right| \leq \mu d(A_1)(1-\varepsilon\rho^{-1}) = \mu(\rho^{-1}-\varepsilon\rho^{-2}).$$

En sommant, il vient :

$$\limsup_{N\to\infty} \frac{1}{N} \left| \sum_{n<N} F(n) \right| \leq d(E) + \mu(d(\mathbb{N}\setminus E)-\varepsilon\rho^{-2}) < \mu(1-\tfrac{\varepsilon}{2}\rho^{-2}).$$

Ainsi $\mu \leq \mu(1 - \frac{\varepsilon}{2}\rho^{-2})$, ce qui contredit l'hypothèse de départ.

III. THEOREME 2 ET COROLLAIRE

III.1. Preuve du théorème 2.

Pour simplifier, on pose $s_q = s$ et on note ν la valuation q-adique définie par $\nu(n) = \text{Max} \{k \in \mathbb{N} \ ; \ q^k \text{ divise } n\}$ pour $n \in \mathbb{Z}^*$. D'après le critère de Weyl et le théorème 1, il suffit de prouver la proposition suivante :

PROPOSITION 1. Si la suite de terme général $x_1 s(h_1 n) + x_2 s(h_2 n)$ *est à valeurs dans* $\mathbb{Z}$, x_1 *et* x_2 *sont rationnels.*

preuve : soit k entier assez grand pour que $q^k > \text{Max}\,(h_1, h_2)$.

$$s(h_i(q^{k+1}-1)) = s(h_i-1) + s(q^{k+1}-h_i) = s(h_i-1) + s(q^k-h_i) + q-1$$
$$= s(h_i(q^k-1)) + q-1.$$

L'hypothèse de la proposition entraîne donc que

① $$(q-1)(x_1+x_2) \in \mathbb{Z}$$

D'autre part, u et a étant deux entiers positifs tels que $q^a > u$,

$s(q^a-u) + s(u-1) = a(q-1)$ et $s(u) = s(u-1)+1 - (q-1)\nu(u)$

ce qui entraîne $s(q^a-u) + s(u) = 1 + (q-1)a - (q-1)\nu(u)$.

L'entier n étant fixé, on choisit a tel que $q^a > \text{Max}(h_1 n, h_2 n)$. L'égalité précédente donne :

$$(q-1)\nu(h_i n) = 1 + a(q-1) - s(h_i n) - s(q^a - h_i n)$$
$$= 1 + a(q-1) - s(h_i n) - s(h_i(q^a-n)) + s(h_i-1)$$
$$= a(q-1) - s(h_i n) - s(h_i(q^a-n)) + s(h_i)$$

D'après ① et l'hypothèse de la proposition

② $$(q-1)(x_1\nu(h_1 n) + x_2\nu(h_2 n)) \in \mathbb{Z} \quad \text{pour } n > 0.$$

Soit $d_i = (q, h_i)$. Si $d_1 < d_2$, $\nu(h_2 \frac{q}{d_2}) = 1$ et $\nu(h_1 \frac{q}{d_2}) = 0$. De ① et ② on déduit alors que $(q-1)x_1 \in \mathbb{Z}$ et $(q-1)x_2 \in \mathbb{Z}$.

Supposons maintenant que $(h_1,q) = (h_2,q) = d$ et notons $H_i = \frac{h_i}{d}$ de sorte que H_i est premier avec q. Supposons en outre que $H_1 < H_2$.

Avec $n = \frac{q}{d} N$ et $(N,q) = 1$,

$$x_1 s(h_1 n) + x_2 s(h_2 n) = x_1 s(H_1 N) + x_2 s(H_2 N).$$

On peut trouver un entier N et un entier a positifs tels que :

$$H_1 N < q^a < H_2 N < 2q^a \qquad \text{et} \qquad H_2 N \equiv q-1 \bmod q^2.$$

Alors $s(H_1 N(q^a + 1)) = 2s(H_1 N)$ et

$$s(H_2 N)(q^a+1)) = s(H_2 N + 1) + s(H_2 N - q^a) = 2s(H_2 N) - (q-1).$$

On conclut que $(q-1)x_1$ et $(q-1)x_2$ sont entiers.

III.2 Preuve du corollaire

Le corollaire est une conséquence immédiate du théorème 2 et du résultat suivant établi par Halasz et Vaughan [5], d'après une idée développée par H. Daboussi pour montrer à l'aide du grand crible que le spectre de Fourier-Bohr d'une suite multiplicative de module au plus égal à 1 est rationnel.

PROPOSITION 2. Soit Q un ensemble de nombres premiers tel que :

$$\sum_{p \in Q} \frac{1}{p} = + \infty .$$

Si une suite réelle f est telle que, pour tout couple (p,q) d'éléments de Q distincts, la suite de terme général f(pn) - f(qn) est équirépartie modulo 1, alors pour toute suite additive g, la suite f + g est équirépartie modulo 1.

III.3. Remarques

1. En adaptant convenablement la fin de la démonstration de la proposition 1, on démontre l'équirépartition de $\sum_{i=1}^{r} x_i s(h_i n)$, si les entiers h_i sont distincts et premiers avec q, et si l'un au moins des réels x_i est irrationnel.

2. L'équirépartition des suites envisagées au théorème 2 est uniforme. Rappelons qu'une suite λ de réels est équirépartie modulo 1 uniformément si, pour tout intervalle $I \subset [0,1[$,

$$\lim_{N\to\infty} \frac{1}{N} \text{Card } \{n \in \mathbb{N} \ ; \ t \leq n < N + t, \ \lambda(n) \in I + \mathbb{Z}\} = \ell(I),$$

uniformément par rapport à $t \in \mathbb{N}$, $\ell(I)$ étant la longueur de I.

3. A l'aide du théorème 1 et de la proposition 1, on montre le :

THEOREME 5. Etant donnés des entiers impairs distincts h_1 *et* h_2 *des entiers* b_1 *et* b_2 *au moins égaux à 2 et des entiers* a_1 *et* a_2 *quelconques, l'ensemble des entiers* n *tels que* $s_2(h_i n) \equiv a_i \bmod b_i$, $i \in \{1,2\}$, *a une densité asymptotique égale à* $(b_1,b_2)^{-1}$.

On peut aussi prouver le :

THEOREME 6. Etant donnés des entiers $b_1 \geq 2$, $b_2 \geq 2$, a_1, a_2 *quelconques, l'ensemble des entiers* n *tels que* $s_2(n) \equiv a_1 \bmod b_1$ *et* $\omega(n) \equiv a_2 \bmod b_2$, *a une densité asymptotique égale à* $(b_1 b_2)^{-1}$.

IV. PREUVE DU THEOREME 3.

IV.1. Un lemme.

x désignant un réel quelconque, il s'agit de montrer que la suite de terme général $G(n) = F(n)\, e(-xn)$ a une valeur moyenne nulle.

On pose $G_k(n) = G(q^k n)$ et

$$\mu = \operatorname*{Sup}_k \limsup_{N\to\infty} \frac{1}{N} \left| \sum_{n<N} G_k(n) \right|$$

Comme dans la démonstration du théorème 1, on suppose $\mu > 0$ et on désigne par ρ une puissance de q supérieure à Max $(h_1, \ldots, h_r)$ et assez grande pour qu'il existe un entier naturel $t < \rho$ tel que $F^{q-1}(t) \neq 1$. On pose $\rho = q^d$

LEMME 1. Il existe $\varepsilon > 0$ tel que pour tout $k \in \mathbb{N}$, on ait :

$$\operatorname{Inf} \left(\left| \sum_{m<\rho} G_k(m) \right|, \left| \sum_{m<\rho} G_{k+1}(m) \right| \right) \leq \rho - \varepsilon.$$

preuve : l'identité $F^{q-1}(m) = G_k^q(m)\, \overline{G_{k+1}(m)}$ entraîne

$$\operatorname{Max} \left(|1 - G_k(t)|, |1 - G_{k+1}(t)| \right) \geq \frac{1}{q+1} |(1 - F^{q-1}(t)|.$$

Le lemme en résulte.

IV.2. Fin de la démonstration

Pour tout $k \in \mathbb{N}$, on note $S_k = \{n \in \mathbb{N},\ e_{3k}(n) = e_{3k+2}(n) = 0\}$, où $n = \sum_{k=0}^{\infty} e_k(n)\, \rho^k$ est encore le développement de n en base ρ.

Puisque la densité de $\bigcup_{b<K} S_b$ vaut $1 - (1 - \rho^{-2})^K$, il existe un entier u tel que la densité de $S = \bigcup_{b\leq u} S_b$ soit minorée par $1 - \mu \frac{\varepsilon}{2} \rho^{-3}$. Supposons alors que :

③ $$\left| \sum_{m<\rho} G_{k+d}(m) \right| \lesssim \rho - \varepsilon$$

Les ensembles $T_o, T_1, \ldots, T_u$ définis par $T_o = S_o$ et pour $b > 0$ par $T_b = S_b \setminus \bigcup_{j<b} S_j$ forment une partition de S.

De plus, tout entier $n \in S_b$ s'écrit :

$$n = \rho^{3b+3} n_1 + \rho^{3b+1} n_2 + n_3 \text{ avec } n_2 < \rho \text{ et } n_3 < \rho^{3b},$$

de sorte que $G_k(n) = G_{k+d(3b+3)}(n_1)\, G_{k+d(3b+1)}(n_2)\, G_k(n_3)$,

ce qui entraine

④ $$\limsup_{N\to\infty} \frac{1}{N} \left| \sum_{\substack{n<N \\ n\in T_b}} G_k(n) \right| \lesssim \mu d(T_b).$$

De plus, ③ donne la majoration plus précise :

⑤ $$\limsup_{N\to\infty} \frac{1}{N} \left| \sum_{\substack{n<N \\ n\in S_o}} G_k(n) \right| \lesssim \mu(1 - \varepsilon\rho^{-1}) d(S_o) = \mu(\rho^{-2} - \varepsilon\rho^{-3})$$

④ et ⑤ donnent :

⑥ $$\limsup_{N\to\infty} \frac{1}{N} \left| \sum_{n<N} G_k(n) \right| \lesssim \mu(d(S) - \varepsilon\rho^{-3}) + d(\mathbb{N} \setminus S) < \mu(1 - \frac{\varepsilon}{2}\rho^{-3})$$

Lorsque ③ n'a pas lieu, le lemme 1 donne :

⑦ $$\left| \sum_{m<\rho} G_{k+d+1}(m) \right| \lesssim \rho - \varepsilon$$

Un raisonnement analogue avec les ensembles

$S'_k = \{n \in \mathbb{N} \ ; \ \left[\frac{n}{q}\right] \in S_k\}$ où $[.]$ désigne la partie entière,

donne à nouveau la majoration (6) .

On obtient ainsi une contradiction.

IV.3. Remarques

1. L'exemple de $F(n) = e(\frac{s(n)}{q-1}) = e(\frac{n}{q-1})$ montre que la conclusion du théorème 3 ne subsiste pas avec l'hypothèse du théorème 1.

2. A l'aide d'un résultat classique de Mendès-France [7], on déduit par exemple du théorème 3 et des résultats du paragraphe III le :

COROLLAIRE. Etant donnés des entiers impairs distincts $h_1,\ldots,h_r$ *, si l'un au moins des réels* $x_1,\ldots,x_r$ *est irrationnel, la suite de terme général* $\sum_{i=1}^{r} x_i s_2(h_i[n\sqrt{2}])$ *est équirépartie modulo 1.*

Ce théorème peut être comparé à celui obtenu dans [3], page 34.

V. PREUVE DU THEOREME 4

Si les nombres 2x et 2y sont entiers relatifs, $e(xs_3(2n) + ys_3(n) - 2xn-yn)$ est identiquement égale à 1. La suite considérée a alors un spectre non vide donc n'est pas pseudo-aléatoire [9]. La condition du théorème 4 est nécessaire.

On donne seulement les grandes lignes de la démonstration.

V.1. Relations de récurrence

On pose $F(n) = e(xs_3(2n) + ys_3(n))$ et $G(n) = e(xs_3(2n+1) + ys_3(n))$. Les relations de récurrence suivantes sont immédiates :

LEMME 2.. $F(3m) = F(m)$, $F(3m+1) = e(2x+y)F(m)$, $F(3m+2) = e(x+2y)G(m)$, $G(3m) = e(x)F(m)$, $G(3m+1) = e(y)G(m)$, $G(3m+2) = e(2x+2y)G(m)$.

A l'aide des suites périodiques "tronquées" $F \circ \rho_K$ et $G \circ \rho_K$ où $\rho_K(m)$ désigne le reste de m modulo 3^K, on démontre en suivant les arguments développés dans [2] l'existence des corrélations :

$$\alpha_1(t) = \lim_{N\to\infty} \frac{1}{N} \sum_{n<N} F(n+t)\overline{F(n)}$$

$$\alpha_2(t) = \lim_{N\to\infty} \frac{1}{N} \sum_{n<N} G(n+t)\overline{G(n)}$$

$$\beta_1(t) = \lim_{N\to\infty} \frac{1}{N} \sum_{n<N} F(n+t)\overline{G(n)}$$

$$\beta_2(t) = \lim_{N\to\infty} \frac{1}{N} \sum_{n<N} G(n+t)\overline{F(n)}$$

Le reste de la démonstration consiste à vérifier que :

⑧ $$\lim_{T\to\infty} \frac{1}{T} \sum_{t<T} |\alpha_1(t)|^2 = 0.$$

Les relations du lemme 2 se transmettent aux corrélations.

LEMME 3. Les relations suivantes ont lieu :

1) $\alpha_1(3u) = \frac{1}{3}(2\alpha_1(u) + \alpha_2(u))$

2) $\alpha_1(3u+1) = \frac{1}{3}(e(2x+y)\alpha_1(u) + e(-x+y)\beta_2(u) + e(-x-2y)\beta_1(u+1))$.

3) $\alpha_1(3u+2) = \frac{1}{3}(e(x+2y)\beta_2(u) + e(-2x-y)\alpha_1(u+1) + e(x-y)\beta_1(u+1))$.

4) $\alpha_2(3u) = \frac{1}{3}(\alpha_1(u) + 2\alpha_2(u))$.

5) $\alpha_2(3u+1) = \frac{1}{3}(e(-x+y)\beta_2(u) + e(2x+y)\alpha_2(u) + e(-x-2y)\beta_1(u+1))$.

6) $\alpha_2(3u+2) = \frac{1}{3}(e(x+2y)\beta_2(u) + e(x-y)\beta_1(u+1) + e(-2x-y)\alpha_2(u+1))$.

7) $\beta_1(3u) = \frac{1}{3}(e(-x)\alpha_1(u) + e(-x)\alpha_2(u) + e(2x)\beta_1(u))$.

8) $\beta_1(3u+1) = \frac{1}{3}(e(x+y)\alpha_1(u) + e(x+y)\alpha_2(u) + e(-2x-2y)\beta_1(u+1))$.

9) $\beta_1(3u+2) = \frac{1}{3}(e(2y)\beta_2(u) + 2e(-y)\beta_1(u+1))$.

10) $\beta_2(3u) = \frac{1}{3}(e(x)\alpha_1(u) + e(x)\alpha_2(u) + e(-2x)\beta_2(u))$.

11) $\beta_2(3u+1) = \frac{1}{3}(2e(y)\beta_2(u) + e(-2y)\beta_1(u+1))$.

12) $\beta_2(3u+2) = \frac{1}{3}(e(2x+2y)\beta_2(u) + e(-x-y)\alpha_1(u+1) + e(-x-y)\alpha_2(u+1))$.

preuve : à titre d'exemple, on vérifie la relation 6.

$$\alpha_2(3u+2) = \lim_{N\to\infty} \frac{1}{3N} \sum_{n<N} \sum_{0\leq a\leq 2} G(3n + a + 3u + 2)\,\overline{G(3n+a)}$$

$$= \frac{1}{3} \lim_{N\to\infty} \frac{1}{N} \sum_{n<N} \big(e(x+2y)G(n+u)\overline{F(n)} + e(x-y)F(n+u+1)\overline{G(n)} + e(-2x-y)G(n+u+1)\overline{G(n)}\big)$$

$$= \frac{1}{3}(e(x+2y)\beta_2(u) + e(x-y)\beta_1(u+1) + e(-2x-y)\alpha_2(u+1)).$$

On remarque que la suite $\alpha_o = \alpha_1 - \alpha_2$ vérifie :

$$\alpha_o(3u) = \frac{1}{3}\alpha_o(u), \quad \alpha_o(3u+1) = \frac{1}{3}e(2x+y)\alpha_o(u), \quad \alpha_o(3u+2) = \frac{1}{3}e(-2x-y)\alpha_o(u+1).$$

En faisant $u = 0$, on en déduit que $\alpha_o(0) = \alpha_o(1) = \alpha_o(2) = 0$. Par récurrence, on montre que α_o est identiquement nulle.

Dans la suite, on pose $\beta_o = \alpha_1 = \alpha_2$. Les corrélations β_o, β_1, β_2 se prolongent naturellement à $\mathbb{Z}$ de la manière suivante :

$$\beta_o(t) = \lim_{N\to\infty} \frac{1}{N} \sum_{-t\leq n<N} F(n+t)\overline{F(n)} \quad \text{pour} \quad t < 0$$

(et relations analogues pour β_1 et β_2).

On constate que $\beta_o(-u) = \overline{\beta_o(u)}$ et $\beta_2(-u) = \overline{\beta_1(u)}$ pour tout entier relatif u. Le lemme 3 se simplifie :

LEMME 4. Pour tout entier relatif u, *on a :*

1) $\beta_o(3u) = \beta_o(u)$

2) $\beta_o(3u+1) = \frac{1}{3}\left(e(2x+y)\beta_o(u) + e(-x-2y)\beta_1(u+1) + e(-x+y)\overline{\beta_1(-u)}\right)$.

3) $\beta_o(3u+2) = \frac{1}{3}\left(e(-2x-y)\beta_o(u+1) + e(x-y)\beta_1(u+1) + e(x+2y)\overline{\beta_1(-u)}\right)$.

4) $\beta_1(3u) = \frac{1}{3}\left(2e(-x)\beta_o(u) + e(2x)\beta_1(u)\right)$.

5) $\beta_1(3u+1) = \frac{1}{3}\left(2e(x+y)\beta_o(u) + e(-2x-2y)\beta_1(u+1)\right)$.

6) $\beta_1(3u+2) = \frac{1}{3}\left(2e(-y)\beta_1(u+1) + e(2y)\overline{\beta_1(-u)}\right)$.

V.2. Corrélations de corrélations

β_o est la corrélation de F, $2\beta_o + \beta_1 + \beta_2$ celle de F+G, $2\beta_o + i(\beta_2 - \beta_1)$ celle de F + iG. Ces suites sont transformées de Fourier de mesures boréliennes bornées positives sur le tore $\mathbb{T} = \mathbb{R}/\mathbb{Z}$. Ainsi, β_o, β_1, β_2 sont transformées de Fourier de mesures boréliennes bornées complexes sur le tore :

$$\beta_i(t) = \int_{\mathbb{T}} e(tx)\,d\Lambda_i(x) \quad \text{pour } t \in \mathbb{Z} \text{ et } i \in \{0, 1, 2\}.$$

Le théorème de convergence dominée montre l'existence des limites :

$$B_{ij}(v) = \lim_{N\to\infty} \frac{1}{2N} \sum_{-N\leq n<N} \beta_i(n+v)\,\overline{\beta_j(n)} \quad \text{et}$$

$$C_{ij}(v) = \lim_{N\to\infty} \frac{1}{2N} \sum_{-N\leq n<N} \beta_i(n+v)\,\beta_j(-n) \quad \text{pour } v \in \mathbb{Z}$$

Par exemple, $C_{01}(v) = \lim_{N\to\infty} \int_{\mathbb{T}^2} \left(\frac{1}{2N} \sum_{-N\leq n<N} e(nx-ny+vx)\,d\Lambda_0(x)\,d\Lambda_1(y)\right)$

$$= \int_{\mathbb{T}^2} e(vx)\,\delta(x,y)\,d\Lambda_0(x)\,d\Lambda_1(y) \quad \text{où } \delta(x,y) = \begin{cases} 1 \text{ si } x = y \\ 0 \text{ si } x \neq y \end{cases}$$

Les relations du lemme 4 se transmettent à leur tour aux quantités

$z_1 = B_{00}(0)$, $z_2 = B_{11}(0)$, $z_3 = e(3x)B_{10}(0)$, $z_4 = e(-3x-3y)B_{10}(1)$, $z_5 = e(-3y)C_{11}(1)$ comme suit :

LEMME 5.

1) $0 = -8z_1 + 2z_2 + z_3 + \overline{z_3} + z_4 + \overline{z_4} + z_5 + \overline{z_5}$

2) $0 = 4z_1 - 10z_2 + z_3 + \overline{z_3} + z_4 + \overline{z_4} + z_5 + \overline{z_5}$

3) $0 = 8z_1 + 4z_2 + [7 - 27e(-2x)]\,z_3 + z_4 + 3\overline{z_4} + 3z_5 + \overline{z_5}$

4) $0 = 8z_1 + 4z_2 + z_3 + 3\overline{z_3} + [7 - 27e(2x+2y)]\,z_4 + 3z_5 + \overline{z_5}$

5) $0 = 8z_1 + 4z_2 + 4z_3 + 4z_4 + [6 - 27e(2y)]\,z_5 + \overline{z_5}$

V.3. Fin de la démonstration

Les relations 1 et 2 du lemme 5 donnent $z_1 = z_2 = \frac{1}{6}(z_3+\overline{z_3}+z_4+\overline{z_4}+z_5+\overline{z_5})$. Les relations 3, 4, 5 deviennent :

$$0 = [9 - 27\, e(-2x)]\, z_3 + 2\overline{z_3} + 3z_4 + 5\overline{z_4} + 5z_5 + 3\overline{z_5}$$
$$0 = 3z_3 + 5\overline{z_3} + [9 - 27e(2x+2y)]\, z_4 + 2\overline{z_4} + 5z_5 + 3\overline{z_5}$$
$$0 = 6z_3 + 2\overline{z_3} + 6z_4 + 2\overline{z_4} + [8 - 27e(2y)]\, z_5 + 3\overline{z_5}$$

On se ramène ensuite à un système aux inconnues $\mathcal{R}ez_i$ et $\mathcal{I}z_i$ dont la seule solution est la solution nulle sous l'hypothèse du théorème 4. Ainsi $z_1 = 0$ ce qui prouve la relation (8) et le théorème.

V.4. Une application du théorème 4

En reprenant des arguments de Bésineau [1], on déduit du théorème 4 le :

COROLLAIRE. Si l'un au moins des réels x, y, z est irrationnel, la suite de terme général $x\, s_3(2n) + y\, s_3(n) + z\, s_2(n)$ *est équirépartie modulo 1.*

V.5. Remarques

1. Un calcul analogue pour $x\, s_2(3n) + y\, s_2(n)$ aurait nécessité l'emploi des 3 suites $F(n) = e(x\, s_2(3n) + y\, s_2(n))$, $G(n) = e(x\, s_2(3n+1) + y\, s_2(n))$, $H(n) = e(x\, s_2(3n+2) + y\, s_2(n))$ et conduit à des relations plus compliquées que celles du lemme 3.

2. L'introduction de G suggère l'étude de suites translatées :

THEOREME 7. La suite de terme général $\sum_{i=1}^{k} x_i s_3(n+a_i) + \sum_{j=1}^{\ell} y_j s_3(2n+b_j)$ *est équirépartie modulo 1 si (et seulement si) l'un au moins des réels* Σx_i, Σy_j *est irrationnel.*

La démonstration consiste à se ramener au cas $a_i < 2$, $b_j < 3$ puis au cas $a_i = 0$, $b_j < 3$.

3. On trouvera dans un article de Stolarsky [10] une étude des entiers pour lesquels $s_2(hn) \geq s_2(n)$ pour tout $h \in \mathbb{N}^*$

REFERENCES

[1] BESINEAU J. Indépendance statistique d'ensembles liés à la fonction "somme des chiffres". Acta Arithmetica 20 (1972), 401-416.

[2] COQUET J. Sur certaines suites pseudo-aléatoires. Acta Sci. Math. (Szeged) 40 (1978), 229-235.

[3] COQUET J. Sur certaines suites pseudo-aléatoires III. Monatshefte für Mathematik 90 (1980), 27-35.

[4] DRINGO L., KATAI I., Some remarks concerning the sum of digits of integers, Acta Math. Acad. Sci. Hung. 37 (1981), 165-172 .

[5] HALASZ G., VAUGHAN R.C., Communication privée.

[6] KATAI I., Change of the sum of digits by multiplication, Acta Sci. Math. (Szeged) 39 (1977), 319-328.

[7] MENDES FRANCE M. Les suites à spectre vide et la répartition modulo 1. Journal of Number Theory 5 (1973), 1-15

[8] NEWMAN D.J. On the number of binary digits in a multiple of three. Proc. A.M.S. 21 (1969), 719-721.

[9] RAUZY G., Propriétés statistiques des suites arithmétiques. P.U.F., Paris, Coll. Sup le Mathématicien 15 (1976).

[10] STOLARSKY K.B., Integers whose multiples have anomalous digital frequencies Acta Arithmetica 38 (1980), 117-128.

Jean COQUET
Département de Mathématique
Université de Valenciennes
59326 VALENCIENNES CEDEX

GAUSS SUMS AND FINITE FOURIER TRANSFORMS

Harold G. DIAMOND, Frank GERTH III, Jeffrey D. VAALER

Let $\mathbb{Z}_q$ denote the ring of residue classes of integers modulo q, and let $G(q) \subset \mathbb{Z}_q$ denote the multiplicative group of residue classes which are relatively prime to q. Here $q > 1$ and $|G(q)| = \varphi(q)$, where φ is Euler's function.

We define the (finite) Fourier transform of a function $f: \mathbb{Z}_q \to \mathbb{C}$ by

$$\hat{f}(n) = q^{-\frac{1}{2}} \sum_{m=1}^{q} f(m) e\left(\frac{-nm}{q}\right) , \tag{1}$$

where $e(x) = e^{2\pi i x}$. As is well known, f can be recovered from $\hat{f}$ by the inversion formula

$$f(m) = q^{-\frac{1}{2}} \sum_{n=1}^{q} \hat{f}(n) e\left(\frac{mn}{q}\right) . \tag{2}$$

If we identify each function $f: \mathbb{Z}^q \to \mathbb{C}$ with a point in the vector space $\mathbb{C}^q$, then the Fourier transform can be viewed as a linear transformation from $\mathbb{C}^q$ to $\mathbb{C}^q$ determined by the matrix

$$\mathcal{F}_q = \{q^{-\frac{1}{2}} e\left(\frac{-mn}{q}\right)\} , \qquad 1 \leq n,m \leq q .$$

The matrix giving the inverse transformation is

$$\mathcal{F}_q^{-1} = \{q^{-\frac{1}{2}} e\left(\frac{mn}{q}\right)\} .$$

Suppose that $f: \mathbb{Z}_q \to \mathbb{C}$ has support contained in $G(q)$, i.e. $f(m) = 0$ if $(m,q) > 1$. We are going to investigate how the Fourier transform reflects this special property of f. For example, can one recover f from the values of $\hat{f}$ restricted to $G(q)$? If we write

Research of the three authors was supported in part by grants from the National Science Foundation.

(3) $$\mathcal{F}_{G(q)} = \{q^{-\frac{1}{2}} e(\tfrac{-nm}{q})\}$$

for the $\varphi(q) \times \varphi(q)$ matrix where $1 \le n,m \le q$, $(n,q) = (m,q) = 1$, then an equivalent question is whether $\mathcal{F}_{G(q)}$ is an invertible matrix.

More generally, let H denote a multiplicative subgroup of $G(q)$ and let aH and bH be cosets of H in $G(q)$. If $f: \mathbb{Z}_q \to C$ is supported in the coset aH, can f be recovered from the values of $\hat{f}$ restricted to bH? The corresponding matrix question involves the $|H| \times |H|$ matrix

(4) $$\mathcal{F}_H^{(s)} = \{q^{-\frac{1}{2}} e(\tfrac{-snm}{q})\} ,$$

where $n,m \in H$ and $s = ab$, and asks if the matrix $\mathcal{F}_H^{(s)}$ is invertible.

We give a complete solution to this problem by determining those subgroups $H \subseteq G(q)$ for which $\mathcal{F}_H^{(s)}$ has an inverse. We also give inversion formulas analogous to (2). When $H = G(q)$ these formulas are particularly elementary and lead to some interesting inequalities and extremal functions.

In order to determine the matrices $\mathcal{F}_H^{(s)}$ that are invertible, we solve an equivalent problem on the nonvanishing of Gauss sums associated with H. Specifically, let $\gamma: H \to \{z \in \mathbb{C}: |z| = 1\}$ be a homomorphism. As usual, we call such a homomorphism γ a character of H, and we extend the domain of γ to $\mathbb{Z}_q$ by setting $\gamma(m) = 0$ if $m \notin H$. We write Γ_H for the set of all characters γ and note that $|\Gamma_H| = |H|$. It is easy to show that every $\gamma \in \Gamma_H$ has the form

$$\gamma(m) = \begin{cases} \chi(m) & \text{if } m \in H \\ 0 & \text{if } m \notin H \end{cases}$$

for some Dirichlet character χ.

The Fourier transform of $\gamma \in \Gamma_H$ is the function $\hat{\gamma}$ determined by the formula

$$\hat{\gamma}(n) = q^{-\frac{1}{2}} \sum_{m=1}^{q} \gamma(m) e\left(\frac{-nm}{q}\right) . \tag{5}$$

Aside from the factor $q^{-\frac{1}{2}}$, the right side of (5) is a Gauss sum associated with the character γ of the group H. The connection between Gauss sums and matrices $\mathscr{F}_H^{(s)}$ is provided by the following result.

Theorem 1. Let H denote a multiplicative subgroup of $G(q)$. Then for each integer s with $(s,q) = 1$ we have

$$\det \mathscr{F}_H^{(s)} = \pm \prod_{\gamma \in \Gamma_H} \hat{\gamma}(s) , \tag{6}$$

where the $\pm$ sign depends only on H. Moreover, if the expression in (6) is nonzero for some integer s, $(s,q) = 1$, then it is nonzero for every such integer.

We sketch a proof of this theorem here; full proofs of this and subsequent results are given in [2]. The first assertion of the theorem is established by showing that each character γ is an eigenfunction with eigenvalue $\hat{\gamma}(s)$ of the matrix $K\mathscr{F}_H^{(s)}$. Here $K = \{k_{mn}\}$, $m \in H$, $n \in H$, is the $|H| \times |H|$ matrix satisfying

$$k_{mn} = \begin{cases} 1 & \text{if } mn \equiv 1 \mod q \\ 0 & \text{if } mn \not\equiv 1 \mod q . \end{cases}$$

The determinant of K is ± 1 since K is a permutation matrix.

The second assertion of the theorem is proved by noting that

$$\det \mathcal{F}_H^{(s)} = q^{-|H|/2} \sum_{\pi} \operatorname{sgn}(\pi) e\left(\frac{-s}{q} \sum_{h \in H} h\pi(h)\right) ,$$

where π ranges over all permutations of the elements of H. Ignoring the $q^{-|H|/2}$ factor, the right side of the last equation is a polynomial with integer coefficients evaluated at $e(-s/q)$. Such a polynomial vanishes at one primitive q-th root of unity if and only if it vanishes at every primitive q-th root of unity.

For certain special subgroups H the value of $\hat{\gamma}(s)$ can be explicitly determined, cf. [1]. In view of Theorem 1, the invertibility of $\mathcal{F}_H^{(s)}$ is equivalent to the nonvanishing of the product in (6). Some special cases of nonvanishing of Gauss sums have been considered before [3,4,5,6].

We shall characterize subgroups $H \subset G(q)$ for which Gauss sums are nonvanishing. For this we define $v = v(q)$ to be the number defined by

$$v(q) = \begin{cases} \prod_{p|q} p & \text{if } 8 \nmid q \\ 2 \prod_{p|q} p & \text{if } 8 \mid q . \end{cases}$$

We then set

$$U(q) = \{m \in \mathbb{Z}_q : m \equiv 1 \bmod v\}$$

and note that $U(q)$ is a multiplicative subgroup of $G(q)$ as well as a coset of an additive subgroup of $\mathbb{Z}_q$.

Theorem 2. Let H denote a multiplicative subgroup of $G(q)$. Then

$$\prod_{\gamma \in \Gamma_H} \hat{\gamma}(s) \neq 0$$

for each $s \in G(q)$ if and only if $H \cap U(q) = \{1\}$.

We note that $U(q)$ is trivial if q is square free, so $\mathcal{F}_H^{(s)}$ is invertible for all subgroups $H \subseteq G(q)$ and all $s \in G(q)$ if q is square free. Also, it follows at once that $\mathcal{F}_H^{(s)}$ is not invertible for any $s \in G(q)$ in case $H = G(q)$ for q a number divisible by the square of a prime.

A rather easy calculation shows that $\hat{\gamma}_0(1) = 0$, where γ_0 denotes the principal character, whenever $H \cap U(q) \neq \{1\}$. The converse is more difficult; it is proved with the aid of the following result.

Lemma. Let p be an odd prime, $(m,p) = 1$, ζ a primitive p^α-th root of unity for some fixed $\alpha \geq 1$, and ω a primitive m-th root of unity. Suppose that

$$1 \leq \ell_1 < \ell_2 < \ldots < \ell_J \leq p^\alpha$$

are integers with $J \leq p - 1$. Then the numbers $\{\zeta^{\ell_j} : 1 \leq j \leq J\}$ are linearly independent over $\mathbb{Q}(\omega)$.

We now give the inverse of $\mathcal{F}_H^{(s)}$ in case it exists. For each coset sH we define $W_{sH} : \mathbb{Z}_q \to \mathbb{C}$ by

$$W_{sH}(m) = q^{\frac{1}{2}} |H|^{-1} \sum_{\gamma \in \Gamma_H} \gamma(m\tilde{s}) / \hat{\gamma}(s) , \tag{7}$$

where $s\tilde{s} \equiv 1 \bmod q$. (A small calculation shows that W_{sH} depends only on the coset sH and not on the coset representative s.)

Theorem 3. Let $H \subseteq G(q)$ and $H \cap U(q) = \{1\}$. Let $s = ab$ with $(s,q) = 1$. Suppose that $f: \mathbb{Z}_q \to \mathbb{C}$ is supported in the coset aH and its Fourier transform $\hat{f}$ is defined by (1). Then for all integers $m \in \mathbb{Z}_q$ we have

$$f(m) = q^{-\frac{1}{2}} \sum_{n \in bH} \hat{f}(n) W_{sH}(mn) \tag{8}$$

and for all integers $\ell \in \mathbb{Z}_q$

$$\hat{f}(\ell) = q^{-\frac{1}{2}} \sum_{n \in bH} \hat{f}(n) \hat{W}_{sH}(\ell \tilde{n}) \ , \tag{9}$$

where $n\tilde{n} \equiv 1 \bmod q$. Moreover, the inverse of the matrix $\mathcal{F}_H^{(s)}$ is

$$\{q^{-\frac{1}{2}} W_{sH}(smn)\} \ , \quad m,n \in H \ .$$

Formula (8) is deduced from the definition of W and the orthogonality of characters. Formula (9) follows from (8) upon taking Fourier transforms.

We note a few consequences of these relations. If the values of $\hat{f}$ on bH are given, then $\hat{f}$ can be extended to all of $\mathbb{Z}_q$ by (9) in such a way that f has support contained in aH. Also, if $f: \mathbb{Z}_q \to \mathbb{C}$ has support contained in aH, then one can bound $|f(m)|$ by an expression depending on $|\hat{f}(n)|$ only for values of n in bH. For example, if $|\hat{f}(n)| \leq A$ for all n in bH, then

$$|f(m)| \leq q^{-\frac{1}{2}} A \sum_{n \in bH} |W_{sH}(mn)| \tag{10}$$

for all $m \in aH$.

The function W_{sH} can be characterized as the unique function on $\mathbb{Z}_q$ satisfying

(11) the support of W_{sH} is contained in the coset sH,

(12) $\hat{W}_{sH}(1) = q^{\frac{1}{2}}$,

(13) if $n \in H \setminus \{1\}$, then $\hat{W}_{sH}(n) = 0$.

It is easy to verify that W_{sH} given by (7) satisfies these three conditions.

For the case $H = G(q)$, q square free, we can give another representation of $W_{G(q)}$ which does not involve characters. Here there is only one coset, so we can simplify the notation and write $W_{G(q)} = W$. If d is a positive divisor of q, we define $\bar{d}$ to be the unique integer, $1 \leq \bar{d} \leq q/d$, which satisfies $d\bar{d} \equiv 1 \bmod q/d$.

Theorem 4. For q square free the function W defined by (7) has the finite Fourier series representation

$$W(m) = \sum_{d|q} \mu(d) e(d\bar{d}m/q) , \tag{14}$$

where μ denotes the Möbius function, and the product representation

$$W(m) = \prod_{p|q} \{e(\tfrac{m}{p}(\overline{q/p})) - 1\} . \tag{15}$$

One can verify by inspection that W as given by (14) satisfies (11), (12), and (13). Formula (15) follows from (14) by multiplication and use of the identity

$$\sum_{p|d} (q/p)(\overline{q/p}) \equiv (q/d)(\overline{q/d}) \mod q ,$$

valid for any $d|q$.

We conclude by giving, as an application of these results, a closed form expression for the sum occurring in (10). We have from (15)

$$\sum_{m=1}^{q} |W(m)| = \sum_{m \in G(q)} \prod_{p|q} |2\, i \sin\{\frac{\pi m}{p}(\overline{q/p})\}| \ .$$

If we write $q = p_1 p_2 \cdots p_r$, we have $G(q) \cong G(p_1) \times G(p_2) \times \ldots \times G(p_r)$, and we can express the last sum as

$$2^{\omega(q)} \prod_{p|q} \sum_{\ell \in G(p)} |\sin\{\frac{\pi \ell}{p}(\overline{q/p})\}| \ .$$

Here $\omega(q) = r$, the number of prime divisors of q. Since $(\overline{q/p}, p) = 1$, $\ell(\overline{q/p})$ runs through $G(p)$ as ℓ does, and upon summing $\sin(\pi\ell/p)$ we obtain

$$\sum_{m=1}^{q} |W(m)| = 2^{\omega(q)} \prod_{p|q} \cot \frac{\pi}{2p} \ .$$

References

1. B.C. Berndt and R. Evans, The determination of Gauss sums, Bull. of Amer. Math. Soc. (New Series) 5 (1981), pp. 107-129.

2. H.G. Diamond, F. Gerth III, and J.D. Vaaler, Gauss sums and Fourier analysis on multiplicative subgroups of $\mathbb{Z}_q$, submitted for publication.

3. R. Evans, Generalized cyclotomic periods, Proc. of Amer. Math. Soc. 81 (1981), pp. 207-212.

4. L. Fuchs, Ueber die Perioden, welche aus den Wurzeln der Gleichung $\omega^n = 1$ gebildet sind, wenn n eine zusammengesetzte Zahl ist, J. Reine Angew. Math. 61 (1863), pp. 374-386.

5. E. Kummer, Theorie der idealen Primfaktoren der complexen Zahlen, welche aus den Wurzeln der Gleichung $\omega^n = 1$ gebildet sind, wenn n eine zusammengesetzte Zahl ist, Math. Abh. Kon. Akad. Wiss. Berlin (1856), pp. 1-47; Collected Papers, vol. 1, Springer-Verlag, Berlin and New York, 1975, pp. 583-629.

6. H. Weber, Lehrbuch der Algebra, 3rd edition, vol. 2, Chelsea, New York, 1961.

Harold G. Diamond
Department of Mathematics
University of Illinois
Urbana, Illinois 61801 and
The University of Texas

Frank Gerth III
Jeffrey D. Vaaler
Department of Mathematics
The University of Texas
Austin, Texas 78712

SUR UNE SOMME LIÉE À LA FONCTION DE MÖBIUS

Exposé par François DRESS

(travail de F. DRESS, H. IWANIEC & G. TENENBAUM)

1. UNE FONCTION CORIACE ...

On commence par considérer la fonction arithmétique

$$M(n,z) := \sum_{\substack{d \mid n \\ d \le z}} \mu(d)$$

qui n'est pas trop mal connue. Elle est souvent nulle et de toute façon pas très grande. Voici quelques résultats :

- pour presque tout n et pour tout $\varepsilon > 0$,
$$\sum_{k=1}^{n} \frac{1}{k} M(n,k)^2 \le (2+\varepsilon)^{\omega(n)} \quad \text{(Erdös et Hall [3])} ;$$
- densité $\{n \mid M(n,z) \neq 0\} << (\log z)^{-\gamma_0}$

avec $\gamma_0 = 1 - \frac{e}{2} \log 2 \# 0.0579$ (Erdös et Hall [3]), puis

$\gamma_0 = 1 - \frac{\log(e \log 2)}{\log 2} \# 0.0860$ (Tenenbaum [6]).

Les choses se compliquent beaucoup lorsque l'on étudie le maximum

$$M(n) := \max_{z} |M(n,z)| .$$

Les résultats connus se limitent finalement à :

- pour tout n, $M(n) \le \sqrt{\frac{2}{\pi}} \frac{2^{\omega(n)}}{\sqrt{\omega(n)}}$ (avez-vous reconnu le théorème de Sperner ?),
- pour presque tout n et pour tout $\varepsilon > 0$, $M(n) \le (\alpha+\varepsilon)^{\omega(n)}$, le dernier

record pour α étant $(3/e)^{\log 2/\log 3}$ ## 1.0641 (Hall et Tenenbaum [4]).

Et quiconque démontrera que, pour presque tout n, $M(n) \geq 2$, aura une place de choix au club des Möbiusophiles !

2. TROIS VALEURS POUR UNE SOMME.

Revenons à la fonction $M(n,z)$ et intéressons-nous à l'estimation de $\sum_{n\leq x} M(n,z)^2$ (qui est utilisée par exemple dans la nouvelle démonstration du théorème de Bombieri-Vinogradov par Vaughan [7]) :

$$\sum_{n\leq x} M(n,z)^2 = \sum_{n\leq x} \sum_{\substack{a,b\mid n \\ a,b\leq z}} \mu(a)\,\mu(b) = \sum_{a,b\leq z} \mu(a)\,\mu(b) \left[\frac{x}{[a,b]}\right] \quad *$$

$$= xS(z) + O(z^2),$$

où

$$S(z) := \sum_{m,n\leq z} \frac{\mu(m)\mu(n)}{[m,n]} .$$

Malgré la présence des termes diagonaux $\frac{1}{m}$, on peut espérer une limite finie pour $S(z)$, avec la bonne raison heuristique que $\sum_{a,b\leq x} \mu(a)\mu(b) \frac{x}{[a,b]} = 1$.

THEOREME. *Lorsque* x *tend vers l'infini, la somme* $S(x)$ *définie ci-dessus tend vers une limite* L *et l'on a les trois expresssions :*

$$L = C \sum_{j=1}^{\infty} \log\frac{j+1}{j} \sum_{m,n\leq j} \frac{\mu(m)\mu(n)}{mn} \prod_{p\mid mn} \frac{1}{(1+\frac{1}{p}-\frac{1}{p^2})}$$

où

$$C = \prod_p (1 - \frac{2}{p^2} + \frac{1}{p^3}) \# 0.4282495$$

$$L = \frac{6}{\pi^2} \sum_{j=1}^{\infty} \log\frac{j+1}{j} \sum_{m,n\leq j} \frac{\mu(mn)}{mn} \prod_{p\mid mn} \frac{1}{(1+\frac{1}{p})}$$

$$L = \frac{1}{\pi}\int_0^{\infty} \prod_p (1-\frac{1}{p})\,(1+\frac{|1-p^{it}|^2-1}{p})\,\frac{dt}{t^2} = \frac{1}{\pi}\int_0^{\infty} |\zeta(1+it)|^{-2} \prod_p \frac{p^2-2cp+2c-1}{p^2-2cp+1}\,\frac{dt}{t^2}$$

$(c = \cos(t \log p))$.

---

* et trois significations pour la notation [ ]: numéro de référence, partie entière, et p.p.c.m.

Trois valeurs pour une somme, mais hélas pas de valeur numérique certaine. Si l'on écrit la première expression $L = \sum_{j=1}^{\infty} a(j)$, la démonstration (cf. ci-dessous) fait apparaître que les termes $a(j)$ sont positifs ; on obtient donc des minorations de L et les trois valeurs :

$$\sum_{1}^{1030} a(j) = 0.44069352...$$

$$\sum_{1}^{2060} a(j) = 0.44071426...$$

$$\sum_{1}^{4120} a(j) = 0.44072359...$$

suggèrent $L \neq 0.4407$. Mais la seule majoration connue a été calculée par Hall [5] et est très loin de la valeur espérée : $L < 0.947$ (une amélioration substantielle de la majoration nécessiterait une minoration explicite de $|\zeta(1+it)|$, et il semble que les spécialistes n'en possèdent actuellement aucune intéressante en stock).

3. GRANDES LIGNES DE LA DEMONSTRATION.

$$\text{PRIMO} \quad L = C \sum_{j=1}^{\infty} \log\frac{j+1}{j} \sum_{m,n\le j} \frac{\mu(m)\mu(n)}{mn} \prod_{p\mid mn} \left(\frac{1}{1+\frac{1}{p}-\frac{1}{p^2}}\right).$$

On commence par manipuler $S(x)$:

$$S(x) = \sum_{m,n\le x} \frac{\mu(m)\mu(n)}{[m,n]} = \sum_{m,n\le x} \frac{\mu(m)\mu(n)}{mn} (m,n)$$

$$(m,n) \uparrow \sum_{d\mid(m,n)} \varphi(d)$$

$$= \sum_{d\le x} \varphi(d) \sum_{\substack{d\mid m \\ d\mid n \\ m,n\le x}} \frac{\mu(m)\mu(n)}{mn}$$

$$\frac{\mu(m)\mu(n)}{mn} \uparrow \sum_{\substack{m'\le X/d \\ n'\le X/d \\ (m',d)=1 \\ (n',d)=1}} \frac{\mu(d)\mu(m')\mu(d)\mu(n')}{dm'dn'} = \sum_{d\le n} \frac{\varphi(d)}{d^2} m\left(d, \frac{X}{d}\right)^2 ,$$

où $m(d,y) = \mu(d) \sum_{\substack{n\le y \\ (n,d)=1}} \frac{\mu(n)}{n}$ alias $\sum_{n\le y} \frac{\mu(dn)}{n}$.

Toute majoration raisonnable de $m(d,y)$, par exemple

$|m(d,y)| <<_\varepsilon \prod_{p|d} (1+p^{-1+\varepsilon})\ e^{-c\sqrt{\log y}}$ $(0<\varepsilon<1)$, convient pour continuer.

On écrit alors

$$S(X) = \sum_{\sqrt{x}<d\le x} \frac{\varphi(d)}{d^2}\, m\,(d,\tfrac{x}{d})^2 + o(1)$$

$$= \sum_{j=1}^{\infty} a(j,x),$$

où $$a(j,x) = \sum_{\max(\sqrt{x},\frac{x}{j+1})<d\le\frac{x}{j}} \frac{\varphi(d)}{d^2}\, m(d,j)^2 .$$

D'une part $a(j,x) <<_\varepsilon \frac{1}{j}\, e^{-2c\sqrt{\log j}}$, d'où l'on déduit l'existence de la limite.

D'autre part on démontre, via une expression du style $a(j,x) = \sum_{m,n\le j} \frac{\mu(m)\mu(n)}{mn}\,(\ldots)$ et une méthode analogue à celle du lemme 2 de [1] que, lorsque n tend vers l'infini, $a(j,x)$ tend vers

$$a(j) = \prod_p (1-\frac{2}{p^2}+\frac{1}{p^3}) \log\frac{j+1}{j} \sum_{m,n\le j} \frac{\mu(m)\mu(n)}{mn} \prod_{p|mn} (\frac{1}{1+\frac{1}{p}-\frac{1}{p^2}}),$$

ce qui termine la démonstration de la première expression de L.

SECUNDO $$L = \frac{6}{\pi^2} \sum_{j=1}^{\infty} \log\frac{j+1}{j} \sum_{m,n\le j} \frac{\mu(mn)}{mn} \prod_{p|mn} (\frac{1}{1+\frac{1}{p}}).$$

On manipule de nouveau $S(x)$, mais de façon différente :

$$S(x) = \sum_{m,n\le x} \frac{\mu(m)\mu(n)}{[m,n]} = \sum_{\substack{d\le x \\ m'\le x/d \\ n'\le x/d \\ (m',n')=1}} \frac{\mu(dm')\mu(dn')}{dm'n'} = \sum_{d\le x} \frac{\mu^2(d)}{d} \sum_{\substack{m,n\le x/d \\ (m,n)=1 \\ (m,d)=1 \\ (n,d)=1}} \frac{\mu(m)\mu(n)}{mn} = \sum_{d\le x} \frac{\mu^2(d)}{j} \sum_{\substack{m,n\le x/d \\ (mn,d)=1}} \frac{\mu(mn)}{mn}.$$

Cette "amorce" différente étant effectuée, on poursuit la démonstration exactement

comme précédemment, avec au bout la deuxième expression de L.

$$\text{TERTIO} \qquad L = \frac{1}{\pi} \int_0^{\infty} \prod_p (1 - \frac{1}{p}) (1 + \frac{|1-p^{it}|^2 - 1}{p}) \frac{dt}{t^2} .$$

On effectue un retour aux sources pour considérer la fonction définie au début $M(n,z)$ (pour $z = e^u$). Et on introduit la fonction complètement multiplicative $n \longmapsto f(n\,;\,\sigma,t)$ définie par $f(p\,;\,\sigma,t) = |1-p^{-\sigma-it}|^2$. On peut alors relier ces deux fonctions par une formule de Plancherel :

$$\int_0^{\infty} M(n,e^u)^2 \, e^{-2\sigma u} \, du = \frac{1}{2\pi} \int_{-\infty}^{+\infty} f(n\,;\,\sigma,t) \, \frac{dt}{\sigma^2+t^2} .$$

On se rappelle que $\sum_{n \le x} M(n,e^u)^2 = x\, S(e^u) + O(e^{2u})$, on montre sans difficulté que, lorsque x tend vers l'infini

$$\sum_{n \le x} f(n\,;\,\sigma,t) \sim x \prod_p (1 + \frac{|1-p^{-\sigma-it}|^2 - 1}{p}),$$

et on en déduit la relation asymptotique

$$x \int_0^{\infty} S(e^u) e^{-2\sigma u} \, du + O(\int_0^{\infty} e^{-2(\sigma-1)u} du) \sim \frac{x}{\pi} \int_0^{\infty} \prod_p (1 + \frac{|1-p^{-\sigma-it}|^2 - 1}{p}) \frac{dt}{\sigma^2 + t^2} ,$$

valable pour $\sigma > 1$. La fin de la démonstration consiste à faire tendre x vers l'infini et surtout à se donner le droit de passer à la limite pour $\sigma = 0$.

BIBLIOGRAPHIE

[1] H. DELANGE. Sur les fonctions arithmétiques multiplicatives. Ann. Sci. Ecole Norm. Sup. (3) 78 (1961), 273-304.

[2] F. DRESS, H. IWANIEC & G. TENENBAUM. Sur une somme liée à la fonction de Möbius. J. reine angew. Math. (à paraître).

[3] P. ERDÖS & R.R. HALL. On the Möbius function. J. reine angew. Math., 315 (1980), 121-126.

[4] R.R. HALL & G. TENENBAUM. On the average and normal orders of Hooley's Δ-function. J. London Math. Soc. (à paraître).

[5] R.R. HALL. A majoration of an integral related to Riemann's zeta function. (Unpublished personal communication).

[6] G. TENENBAUM. Sur la probabilité qu'un entier possède un diviseur dans un intervalle donné (soumis pour publication).

[7] R.C. VAUGHAN. An elementary method in prime number theory. Acta Arithm., 37 (1980), 111-115.

F. DRESS
U.E.R. de Mathématique
Université de Bordeaux I
351, Cours de la Libération

33405 TALENCE Cedex

A NEW INEQUALITY IN THE THEORY OF ADDITIVE ARITHMETIC FUNCTIONS

P.D.T.A. ELLIOTT

I shall begin with

THEOREM. *Let* $a > 0, b, A > 0$, B *be integers for which* $\Delta = aB - Ab \neq 0$. *Then the inequality*

$$\sum_{\substack{q \le x \\ (q, aA\Delta)=1}} \frac{1}{q} |f(q) - F(x) \log q|^2 \ll \sup_{x < y \le x^C} \frac{1}{y} \sum_{x < n \le y} |f(an+b) - f(An+B)|^2$$

holfd for all additive functions $f(\ )$, *and all* $x \ge 2$. *Here*

$$F(x) = \sum_{x^{1/2} < q \le x} \frac{f(q)}{q} \Big/ \sum_{x^{1/2} < q \le x} \frac{\log q}{q},$$

q *denotes a (typical) prime-power, and the constant* C *depends at most upon* a, A, b *and* B.

Remarks. $\ll$ denotes the symbol of Vinogradov, so that $r \ll S$ means

$$|r| \le C_0 S$$

for some constant C_0. In the above case it depends at most upon a, A, b and B. Probably, if the inequality is asserted only to hold for x large enough depending upon a, A, b and B, then an obsolute value could be given for C.

There are supplementary inequalities involving those prime-powers which do have factors in common with aA, and also $|F(x)|^2$. I shall not go into those here.

Before giving some indication of the proof, I will give some applications.

Erdös (Annals of Math., 1946) proved that if

$$f(n+1) - f(n) \longrightarrow 0, \quad n \longrightarrow \infty,$$

then for some constant D,

$$f(n) = D \log n$$

must hold. Many other proofs of this result were later given. Here I note that

in his paper Erdös conjectured that from

$$f(n+1) - f(n) \leq \text{constant}$$

one could establish the existence of a constant D so that

$$f(n) = D \log n + O(1)$$

uniformly for all $n \geq 1$. This conjecture of Erdös was established by Wirsing in 1968, by a method altogether different from that of Erdös.

The method used to establish the above theorem is once again different. In particular L^2-norm inequalities are considered, since the dual of an L^2-norm inequality is generally another inequality involving L^2-norms.

In this same period of the sixties, Katai asked for a characterisation of those additive functions for which

$$f(an+b) - f(An+B) \longrightarrow c_1 ,$$

for some finite number c_1, as $n \longrightarrow \infty$.

The inequality of the theorem allows us to conclude from this assumption the uniform boundedness of the sums

$$\sum_{\substack{q \leq x \\ (q, aA\Delta)=1}} \frac{1}{q} |f(q) - F(x) \log q|^2 , \quad x \geq 2.$$

In particular $|F(x)|$ is bounded. By letting x increase through a suitable sequence of values, we obtain a constant F so that the series

$$\sum_{(q, aA\Delta)=1} \frac{1}{q} |f(q) - F \log q|^2$$

converges. In particular those primes p for which $|f(p) - F \log p|$ is large, say at least one in value, have

$$\Sigma' \frac{1}{p}$$

convergent. Such a thin sequence of primes is readily handled by a sieve method, and one deduces that for all q which are prime to $aA\Delta$,

$$f(q) = D \log q,$$

when D is a constant depending upon F.

For example, if

$$f(3n+1) - f(3n+2) \longrightarrow 0, \quad n \longrightarrow \infty,$$

then for some constant D,

$$f(n) = D \log n$$

holds for all n which are not divisible by 3.

In another direction, consider the following result of Erdös and Kac (1939) :

If $f(\ )$ is strongly additive, $|f(p)| \leq 1$,

$$A(N) = \sum_{p \leq N} \frac{f(p)}{p}, \quad B(N) = \left(\sum_{p \leq N} \frac{|f(p)|^2}{p}\right)^{\frac{1}{2}} \geq 0,$$

and $B(N)$ is unbounded with N, then

$$\frac{1}{N} \sum_{\substack{n \leq N \\ f(n)-A(N) \leq zB(N)}} 1 \Longrightarrow \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{z} e^{-u^2/2} du, \quad N \to \infty,$$

where the frequency approaches the normal law in the usual weak convergence sense of measure theory.

I shall not consider here the ramifications of this result in the Probabilistic Theory of Numbers, but refer only to the monograph of Kubilius, and my book, volumes 239, 240 of the Springer Grundlehren series, 1979/80.

Suppose now that $\beta(x) > 0$ is a function which satisfies $\beta(x) \to \infty$ as $x \to \infty$, and

$$\lim_{x \to \infty} \frac{\beta(x^y)}{\beta(x)} = 1$$

for each fixed $y > 0$. Then a necessary and sufficient condition for the frequency

$$\frac{1}{[x]} \sum_{\substack{n \leq x \\ f(n+1)-f(n) \leq z\beta(x)}} 1$$

to approach some (limiting) distribution as $x \longrightarrow \infty$, in such a way that the mean and variance of this frequency also converge to the mean and variance of the limit law, is that there be a constant D so that

$$\frac{1}{\beta(x)^2} \sum_{\substack{p \leq x \\ f(p)-D \log p \leq u\beta(x)}} \frac{(f(p)-D \log p)^2}{p} \to G(u), \quad x \longrightarrow \infty$$

for some non-decreasing function $G(u)$ of bounded total variation. Here the more

difficult part is the necessity of the weak convergence to G(u). An application of the theorem allows the use of a compactness argument so that one can introduce the machinery of the theory of probability.

Now a third application. Let m_1 be an integer which is prime to 3. Clearly one can always obtain a product representation of the form

$$m_1^v = \prod_{i=1}^{s} (3n_i + 1)^{\varepsilon_i}$$

where v, n_i are positive integers, and each ε_i has one of the values ± 1. Likewise if $(m_2,5) = 1$ then one can obtain a representation

$$m_2^v = \prod_{i=1}^{s} (5n_i + 2)^{\varepsilon_i}.$$

Much more interesting, and not at all obvious, is that these representations can be obtained simultaneously, with the same values of n_i, ε_i, s and v. Moreover, the same value of v can be held for every choice of m_1 and m_2.

To establish this let Q_1 be the (multiplicative) group of the positive rational numbers. We form $Q_1 \oplus Q_1 = Q_2$, the direct sum of two copies of Q_1. Let G be the subgroup of Q_2 generated by the elements $3n+1 \oplus 5n+2$, $n = 1,2,\ldots$, and let Γ be the quotient group Q_2/G.

The group Q_2/G is shown to be finite by considering homomorphisms of it into various groups, and proving that they are essentially trivial. For example, one is reduced to the application of propositions of the type :

If f_1, f_2 *are real-valued completely-additive functions which satisfy*

$$f_1(3n+1) + f_2(5n+2) = 0$$

for all integers $n \geq 1$,

$$f_1(m) = 0 \quad \text{if} \quad (m,3) = 1$$

$$f_2(m) = 0 \quad \text{if} \quad (m,5) = 1.$$

Such a result may be deduced from the inequality of the theorem.

The proof of the main theorem involves several ideas. I shall state here two ingredients.

LEMMA 1. *Let* $\frac{1}{2} < \sigma < 1$. *Let* $D \geq 1$, t *be integers. Then the inequality*

$$\sum_{\log x < p \leq Q} \max_{(r,p)=1} \max_{y \leq x} \Big| \sum_{\substack{n \leq y \\ n \equiv r \pmod p \\ n \equiv t \pmod D}} \frac{f(n)}{n^\sigma}\left(1 - \frac{n}{y}\right) - \frac{1}{p-1} \sum_{\substack{n \leq y \\ (n,p)=1 \\ n \equiv t \pmod D}} \frac{f(n)}{n^\sigma}\left(1 - \frac{n}{y}\right)\Big|^2$$

$$\ll \left(\frac{x^{2(1-\sigma)}}{\log x} + Q^{\mu(\sigma)}\right) \sum_{q \leq x} \frac{|f(q)|^2}{q}$$

holds for all additive functions f, *for all* $x \geq 2$. *Here* $\mu(\sigma)$ *is an explicit but complicated function of* σ, *which satisfies*

$$\min_{\frac{1}{2} < \sigma < 1} \mu(\sigma) < 8.$$

As is usual p *denotes a prime,* q *a prime-power.*

Important features of this inequality are that it holds with no a-piori bounds on f, and the presence of the factor $1/\log x$. For a wide range of values of Q the term $x^{2(1-\sigma)}/\log x$ cannot be replaced by anything smaller. This result looks, of course, like the well-known Bombieri-Vinogradov theorem, but it is an "abstract-norm" inequality, whereas their result takes advantage of the special properties of prime numbers.

LEMMA 2. *Let*

$$\sum_{x^{d_1} < p \leq x^{d_2}} \frac{1}{p} |f(p) - \alpha(x) + \alpha(\tfrac{x}{p})| = o(\rho(x))$$

as $x \longrightarrow \infty$. *Here* $\rho(x) > 0$ *is to satisfy*

$$\limsup_{x \to \infty} \frac{\rho(x^y)}{\rho(x)} < \infty$$

for each fixed $y > 0$; d_1 *and* d_2 *are (fixed) positive reals ; and*

$$\alpha(x) = \sum_{p \leq x} \frac{f(p)}{p} .$$

Then there is a decomposition

$$\alpha(x) = U(x) + V(x)$$

where for $y > 0$

$$U(x^y) = yU(x) + o(\rho(x)), \quad V(x^y) = V(x) + o(\rho(x))$$

hold as $x \longrightarrow \infty$.

In particular we may conclude that

$$\sum_{x^{d_1} < p \le x^{d_2}} \frac{1}{p} |f(p) - U(x) \log p| = o(\rho(x)).$$

The proof of the main theorem is rather complicated, but one might hope to apply it to other problems which involve additive arithmetic functions.

Imperial College, London
and Boulder, Colorado.

UNE NOUVELLE MAJORATION DE LA FONCTION $\pi_2(x)$.

Etienne FOUVRY

Dans ce travail, on expose un article fait en collaboration avec H. Iwaniec ([8]).

I. INTRODUCTION.

La lettre p désignant toujours un nombre premier, on note

$$\pi_2(x) = \#\ \{p\ ;\ p \le x,\ p+2 \text{ premier}\}.$$

La célèbre conjecture sur les nombres premiers jumeaux est de montrer que

$$\pi_2(x) \longrightarrow +\infty \quad \text{pour} \quad x \longrightarrow +\infty .$$

Une conjecture plus précise est de prouver l'équivalence (pour $x \longrightarrow +\infty$) :

$$\pi_2(x) \sim 2 \prod_{p>2} \left(1 - \frac{1}{(p-1)^2}\right) \frac{x}{\log^2 x} \ := P(x) .$$

La majoration asymptotique :

$\forall\ \varepsilon > 0$ on a $\qquad \pi_2(x) \le (1+\varepsilon)\ P(x) \quad \text{pour} \quad x > x_0(\varepsilon)$

semble déjà très difficile à obtenir. Les améliorations successives de la majoration de $\pi_2(x)$ rendent bien compte des progrès effectués dans les méthodes de crible et dans la répartition des nombres premiers.

En 1920, Brun obtenait comme application de son crible, la formule :

$$\pi_2(x) \ll P(x)(\log\log x)^2 \tag{1}$$

(on retient plutôt ce résultat sous la forme :

"La série des inverses des nombres premiers jumeaux est convergente").

Un peu plus tard, il obtenait le bon ordre de grandeur, en démontrant :

$$\pi_2(x) \ll P(x). \tag{2}$$

En 1949, Selberg, grâce à son crible parvenait à :

$$\forall\ \varepsilon > 0 \qquad \pi_2(x) \le (8+\varepsilon)\ P(x) \quad \text{pour} \quad x > x_0(\varepsilon). \tag{3}$$

(On se reportera à [9] par une bibliographie complète).

Chacune des majorations (1), (2) et (3) est obtenue en criblant l'ensemble

$\{n(n+2)\ ;\ n \le x\}$ et ne nécessite aucun théorème profond sur la suite des nombres premiers.

Il n'en est plus de même si on part de l'ensemble

$$\mathcal{A} = \{p + 2\ ;\ p \le x\}$$

car on doit connaître la répartition des nombres premiers dans les progressions arithmétiques. Ainsi en 1960, Wang ([14]) obtenait, sous l'hypothèse de Riemann généralisée, l'inégalité

(4) $\quad \forall\ \varepsilon > 0, \qquad \pi_2(x) \le (4+\varepsilon)\ P(x) \quad \text{pour} \quad x > x_0(\varepsilon).$

En 1965, Bombieri et Davenport ([1]) retrouvaient l'inégalité (4), sans recourir à l'hypothèse de Riemann généralisée (voir aussi [13] pour un résultat intermédiaire). Leur démonstration repose essentiellement sur le théorème de Bombieri-Vinogradov ([9]), résultat très puissant sur la répartition, en moyenne, des nombres premiers dans les progressions arithmétiques :

Pour tout A , *il existe* B = B(A) *tel qu'on ait*

$$(5) \qquad \sum_{q \le x^{1/2}(\log x)^{-B}} \max_{y \le x} \max_{(a,q)=1} \left|\pi(x\,;q,a) - \frac{\pi(x)}{\varphi(q)}\right| = O_A(x(\log x)^{-A}).$$

Le coefficient 4, dans la formule (4), semblait difficile à améliorer, puisqu'il est directement lié à l'exposant 1/2 de (5). Toutefois, Chen ([2], voir aussi [12]) parvint à la formule

$\forall\ \varepsilon > 0, \qquad \pi_2(x) \le (3{,}9171 + \varepsilon)\ P(x) \quad \text{pour} \quad x \ge x_0(\varepsilon).$

Sa démonstration utilise des arguments proches de ceux apparaissant dans celle du théorème de Chen ([9] chap. 11).

On montre

THEOREME 1 ([6], [8]) ; *Pour tout* $\varepsilon > 0$, *on a pour* $x > x_0(\varepsilon)$ *l'inégalité :*

$$(6) \qquad \pi_2(x) \le \left(\frac{64}{17} + \varepsilon\right) P(x).$$

(Le coefficient $\frac{64}{17}$ (= 3,7647...) pourrait sans doute être amélioré en utilisant les idées de [2]).

II. APERCU DE LA DEMONSTRATION DE (6).

Par le crible de Selberg, appliqué à la suite $\mathscr{A}$, on parvient, en simplifiant à l'extrême, à la majoration :

$$\pi_2(x) \leq 2\left(\frac{\log x}{\log D} + \varepsilon\right) P(x) + R(\mathscr{A},D) \tag{7}$$

avec

$$R(\mathscr{A},D) = \sum_{\substack{q \leq D \\ (q,2)=1}} \left|\pi(x\,;\,q,-2) - \frac{\pi(x)}{\varphi(q)}\right| .$$

La formule (5) permet de choisir $D = x^{\frac{1}{2}-\varepsilon}$, conduisant ainsi à (4). On voit que toute amélioration de l'exposant $\frac{1}{2}$, se répercute aussitôt sur la majoration de $\pi_2(x)$. Une étude plus précise montre que $R(\mathscr{A},D)$ vaut en fait (toujours en simplifiant):

$$R(\mathscr{A},D) = \sum_{\substack{q_1 \leq \sqrt{D} \\ (q_1q_2,2)=1}} \sum_{q_2 \leq \sqrt{D}} \lambda_{q_1}\lambda_{q_2}\left(\pi(x\,;\,q_1q_2\,,-2) - \frac{\pi(x)}{\varphi(q_1q_2)}\right) \tag{8}$$

avec $|\lambda_q| \leq 1$. Cette souplesse plus grande du terme reste, ne permet pas encore, pour l'instant, de prendre des valeurs de $D > x^{\frac{1}{2}-\varepsilon}$. Mais le crible de Rosser-Iwaniec ([11]) fournit un terme reste beaucoup plus intéressant, puisque pour toute écriture $D = D_1D_2$ $(D_1 \geq 1,\ D_2 \geq 1)$ on retrouve la formule (7) avec

$$R(\mathscr{A},D) = \sum \lambda_{q_1}(D_1)\,\lambda_{q_2}(D_2)\left(\pi(x\,;\,q_1q_2,\,-2) - \frac{\pi(x)}{\varphi(q_1q_2)}\right) \tag{9}$$

avec $|\lambda_{q_i}(D_i)| \leq 1$ $(i = 1$ ou $2)$.

Pour $D_1 = D_2 = D^{1/2}$, on retrouve (8).

On a besoin de quelques définitions :

Soit $\lambda : \mathbb{N}^* \to \mathbb{C}$, on dit que λ est de <u>niveau</u> D $(D \geq 1)$ et <u>d'ordre fini</u> si on a

$$d > D \Rightarrow \lambda(d) = 0$$

et s'il existe un entier $\varkappa$ tel qu'on ait

$$|\lambda(d)| \leq \tau_\varkappa(d)$$

($\tau_\varkappa(d)$ est le nombre de décomposition de l'entier d en $d = d_1 \ldots d_\varkappa$).

On dit que λ de niveau D est bien factorisable, si pour toute décomposition $D = D_1D_2$ $(D_1, D_2 \geq 1)$, il existe μ et ν de niveaux D_1 et D_2 et d'ordre finis vérifiant $\lambda = \mu * \nu$.

D'après les formules (7) et (9), il est facile de voir que le théorème 1 est la conséquence du théorème 2 suivant :

THEOREME 2 : *Si* $\lambda(q)$ *est bien factorisable de niveau* $Q = x^{\frac{17}{32} - \varepsilon}$ $(\varepsilon > 0)$, *on a, pour tout* A *l'inégalité :*

$$(10) \qquad \sum_{(q,a)=1} \lambda(q)(\pi(x\,;\,q,a) - \frac{\pi(x)}{\varphi(q)}) = O_{A,\varepsilon}\,(x(\log x)^{-A})$$

uniformément pour $|a| \leq (\log x)^A$.

Ce théorème constitue, en un certain sens, une amélioration du théorème de Bombieri-Vinogradov. A cause du problème de l'uniformité en a, on en peut rien déduire sur le nombre de solutions de l'équation $2N = p_1 + p_2$.

La démonstration du théorème 2 est longue, nous n'en dégagerons que les idées principales.

Par l'identité d'Heath-Brown ([10]) et la définition de $\lambda(q)$, la démonstration de (10) se ramène à prouver que la somme

$$(11) \qquad E = \sum_{r\leq R} \alpha_r \sum_{s\leq S} \beta_s \Big(\sum_{\substack{m\leq M \\ mn\equiv a[rs]}} \gamma_m \sum_{n\leq N} \delta_n - \frac{1}{\varphi(rs)} \sum_{\substack{m\leq M \\ (mn,rs)=1}} \gamma_m \sum_{n\leq N} \delta_n \Big)$$

vérifie

$$E = O_A(MN(\log MN)^{-A}) .$$

On peut supposer, pour simplifier, les inégalités

$$|\alpha_r|,\ |\beta_s|,\ |\gamma_m|,\ |\delta_n| \leq 1.$$

Les nombres R et S vérifient $RS = Q$, et seront choisis de manière optimale en fonction de M et N.

Les nombres M et N sont liés par la relation $MN = x$, et la suite (δ_n) se répartit bien dans les progressions arithmétiques, elle vérifie :

$$\sum_{n\le y, n\equiv b[k]} \delta_n = \frac{1}{\varphi(k)} \sum_{n\le y,(n,k)=1} \delta_n + O_B(y(\log y)^{-B})$$

pour tout B, et pour tout entier b premier avec k. (Pour $\delta_n = \Lambda(n)$, on reconnaît le théorème de Siegel-Walfisz).

Le problème est alors de calculer, en fonction de M et N, une "sorte d'exposant de répartition" de la convolée des suites (γ_m) et (δ_n). Cette situation a été l'objet de [4], [5] et [7], et a été traitée par un calcul de dispersion.

Par une interversion de sommations, la relation (11) devient

$$E = \sum_r \alpha_r \sum_m \gamma_m (\sum_s \beta_s \sum_n \delta_n - \ldots)$$

et par l'inégalité de Cauchy-Schwarz on a

$$E^2 \le RM \sum_r \sum_s (\sum_s \beta_s \sum_n \delta_n - \ldots)^2.$$

Après avoir développé le carré, on arrive à

$$E^2 \le RM(W - 2V + U)$$

où U, V et W sont définis à partir de six variables de sommation :

$$r,\ m,\ s,\ s',\ n \text{ et } n'.$$

Chacune des expressions U, V et W doit être exprimée comme somme d'un terme principal et d'un terme d'erreur, en effet après une interversion de sommations, on rencontre une somme S de la forme suivante :

$$S = \sum_{\substack{M<m\le 2M \\ tm\equiv b[k]}} 1 \qquad (k > M).$$

(Les nombres b, t et k sont définis à partir de r, s, s', n et n').
En notant $\{y\}$ la partie fractionnaire du réel y et par $\bar{t}$ l'inverse de t modulo k, on voit que S vérifie

$$S = \frac{M}{k} + \{\frac{M - b\bar{t}}{k}\} - \{\frac{2M - b\bar{t}}{k}\}. \tag{12}$$

Le terme M/k est le terme principal. La contribution des différents termes principaux est traitée par le grand crible, d'une façon analogue à la démonstration du théorème de Barban-Davenport-Halberstam. Le point délicat de la démonstration est l'étude de la contribution des parties fractionnaires de (12). On ne peut se contenter de la majorer par 1, on les développe en série de Fourier, pour parvenir à des sommes de Kloosterman. Il faut alors tenir compte des différentes compensations en

sommant sur les variables r, s, s', n et n', autrement dit, on gagne davantage en appliquant les résultats récents de Deshouillers et Iwaniec sur les sommes des Kloosterman en moyenne ([3]) qu'en utilisant la majoration classique de Weil.

BIBLIOGRAPHIE

[1] E. BOMBIERI and H. DAVENPORT. Small differences between prime numbers, Proc. Roy. Soc. Ser. A (293) 1966, 1-18.

[2] J.R. CHEN. On the Goldbach's problem and the sieve methods, Sci. Sin. 21 (1978), 701-739.

[3] J.M. DESHOUILLERS and H. IWANIEC. Kloosterman sums and the Fourier coefficients of cusps, Inv. Math. (à paraître).

[4] E. FOUVRY. Répartition des suites dans les progressions arithmétiques, Acta Arith. (à paraître).

[5] E. FOUVRY. Répartition des suites dans les progressions arithmétiques. Résultats du type Bombieri-Vinogradov avec exposant supérieur à 1/2, Thèse de Doctorat d'Etat ès Sciences, Université de Bordeaux I (1981).

[6] E. FOUVRY. Autour du théorème de Bombieri-Vinogradov, (en préparation).

[7] E. FOUVRY and H. IWANIEC. On a theorem of Bombieri-Vinogradov type, Mathematika 27 (1980), 135-172.

[8] E. FOUVRY and H. IWANIEC. Primes in arithmetic progressions, Acta Arith. (à paraître).

[9] H. HALBERSTAM and H.E. RICHERT. Sieve Methods, Academic Press, London New-York, 1974.

[10] D.R. HEATH-BROWN. Sieve identities and gaps between primes, Journées arithmétiques de Metz, à paraître dans Astérisque.

[11] H. IWANIEC. A new form of the error term in the linear sieve, Acta Arith. 37 (1980), 307-320.

[12] C.B. PAN. On the upper bound of the number of ways to represent an even integer as a sum of two primes, Sci. Sin. 23 (1980), 1368-1377.

[13] C.D. PAN. A new application of the Ju. V. Linnik large sieve method, Acta Math. Sinica 14 (1964), 597-606.

[14] Y. WANG. On the representation of a large integer as a sum of a prime and an almost prime, Acta Math. Sinica 10 (1960), 168-181 et Chinese Math. 1 (1962), 181-195.

Etienne FOUVRY
U.E.R. de Mathématiques et d'Informatique
Université de Bordeaux I
351, Cours de la Libération
33405 TALENCE CEDEX

AN EXTENSION OF THE METHOD OF MOMENTS FOR ADDITIVE FUNCTIONS

A. GHOSH*

1. If one were to draw up a list of theorem that illustrate the abiding charm of number theory, then surely one would include the beautiful result of Hardy and Ramanujan [7] that almost all integers n have about $\log\log n$ prime divisors.

In his doctoral dissertation (of which only fragments were ever published) Turan [10] gave a new proof by exploiting the probabilistic aspects of the problem; and then, in 1940, Erdős and Kac [5] demonstrated the fruitfulness of Turan's point of view in their famous theorem that $\omega(n)$, the number of distinct prime divisors of n, conforms (after suitable normalization) to the Central Limit Theorem and the values it assumes are distributed according to the Gaussian Law. Later, Kac [8] described this result as an instance of "primes playing a game of chance."

Let

$$\sigma_N(x) = \frac{1}{N}\,\mathrm{card}\{n : 1 \le n \le N,\ \frac{\omega(n) - \log\log N}{\sqrt{\log\log N}} < x\}.$$

then $\sigma_N(x)$ is a distribution function and

$$(1)\qquad \lim_{N\to\infty} \sigma_N(x) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{x} e^{-\frac{1}{2}t^2}\,dt$$

is the precise statement of the Erdős-Kac Theorem. Their proof involved applying the Central Limit Theorem itself to a truncation of $\omega(n)$, and then bridging the gap between $\omega(n)$ and its truncation by means of Brun's sieve. Kac also suggested that a more straightforward approach and one "closest in spirit to the traditional lines of probability theory", would be to compute the associated moments

* This article was prepared and delivered as a lecture at the Colloque Delange, June 1982, by H. Halberstam.

$$\mu_k(N) = \int_{-\infty}^{\infty} x^k d\sigma_N(x) = \frac{1}{N} \sum_{n=1}^{N} \left(\frac{\omega(n) - \log\log N}{\sqrt{\log\log N}}\right)^k$$

and prove, for each $k = 1,2,3,\ldots$ that

$$(2) \qquad \mu_k = \lim_{N\to\infty} \mu_k(N) = (2\pi)^{-\frac{1}{2}} \int_{-\infty}^{\infty} x^k e^{-\frac{1}{2}x^2}\, dx = \begin{cases} \dfrac{k!}{(\frac{1}{2}k)!\, 2^{\frac{1}{2}k}}, & k \text{ even}, \\ 0, & k \text{ odd}. \end{cases}$$

By a classical lemma of Čebyčev - the method of moments - (1) would then follow at once.

This approach has the added appeal that (2) yields a whole family of striking asymptotic formulae. Cases $k=1$ and 2 were already explicitly present in Turan's pioneering work - the case $k=2$ leads directly to a proof of the Hardy-Ramanujan Theorem - but (2) was first proved in 1953 by Delange [2] (who was not aware at the time of Kac's desideratum).

When k is odd, $\mu_k = 0$ - in other words, there is then present a marked cancellation effect. It is therefore appropriate to ask whether anything can be said about the corresponding absolute moments, about

$$\sum_{n=1}^{N} |\omega(n) - \log\log N|,$$

for example. The purpose of this note is to answer this question. Indeed, it is perhaps a little surprising that one can prove even that

THEOREM. For each real number $\kappa > 0$,

$$\sum_{n=1}^{N} |\omega(n) - \log\log N|^{\kappa} \sim \frac{2^{\frac{1}{2}\kappa}}{\sqrt{\pi}} \Gamma\left(\frac{\kappa+1}{2}\right) N (\log\log N)^{\frac{1}{2}\kappa} \text{ as } N \to \infty.$$

We shall suppose in the sequel that N is a sufficiently large positive integer.

2. Our approach is to calculate the real absolute moments by expressing them in terms of 'even integer' moments μ_{2k}. For this (2) alone is not sufficient - we require a result for μ_{2k} that is uniform in k; fortunately such a result may readily be extracted from Delange [3]: Write $L = \log\log N$ and

$$F(n) = (\omega(n) - L)L^{-\frac{1}{2}}, \qquad 1 \leq n \leq N.$$

Then

$$(3) \qquad \mu_{2k}(N) = \frac{1}{N}\sum_{n=1}^{N} F(n)^{2k} = \mu_{2k} + O((Ak)^{4k}L^{-\frac{1}{2}})$$

where A is, here and throughout, a 'generic' positive absolute constant.

The cases $0 < \kappa \leq 1$ and $\kappa > 1$ require slightly different treatment, and we shall deal here in detail only with the case $\kappa > 1$.

Let m be the unique non-negative integer such that $2m + 1 < \kappa \leq 2m + 3$, so that we may write

$$\kappa = 2m + 1 + \theta, \qquad 0 < \theta \leq 2.$$

Let

$$D = \int_0^{\infty} \frac{(\sin t)^4}{t^{2+\theta}}\,dt = \int_0^{T} \frac{(\sin t)^4}{t^{2+\theta}}\,dt + O(T^{-1-\theta})$$

for any $T > 0$ (T to be chosen later). Throughout, constants implied by use of the O-notation depend at most on κ.

[For $0 < \kappa \leq 1$, the appropriate starting point is

$$D = \int_0^{\infty} \frac{(\sin t)^2}{t^{1+\kappa}}\,dt. \qquad]$$

Then, for any α,

$$(4) \qquad |\alpha|^K = \frac{|\alpha|^{2m}}{D} \left\{ \int_0^T \frac{(\sin |\alpha| t)^4}{t^{2+\theta}} \, dt + O(T^{-1-\theta}) \right\}.$$

Moreover, by Taylor's Theorem

$$(5) \qquad (\sin x)^4 = \sum_{r=2}^{R} a_r x^{2r} + O\left\{ \frac{(4|x|)^{2R+2}}{(2R+2)!} \right\}$$

where

$$(6) \qquad |a_r| < \frac{1}{8} \frac{4^{2r}}{(2r)!} \qquad (r=2,3,\ldots)$$

and R is a parameter to be chosen later. Combining (4) and (5) we obtain

$$|\alpha|^K = \frac{1}{D} \int_0^T \sum_{r=2}^{R} a_r t^{2r} |\alpha|^{2m+2r} \frac{dt}{t^{2+\theta}} + O\left\{ \frac{(4T)^{2R+1-\theta}}{(2R+2)!R} |\alpha|^{2m+2R+2} + |\alpha|^{2m} T^{-1-\theta} \right\}.$$

Now take $|\alpha| = |F(n)|^K$, sum over n from 1 to N and divide by N:

$$\mu_K^*(N) = \frac{1}{N} \sum_{n=1}^{N} |F(n)|^K = \frac{1}{D} \int_0^T \sum_{r=2}^{R} a_r t^{2r} \mu_{2m+2r}(N) \cdot \frac{dt}{t^{2+\theta}}$$

$$+ O\left\{ \frac{(4T)^{2R+1-\theta}}{(2R+3)!} \mu_{2m+2R+2}(N) + T^{-1-\theta} \mu_{2m}(N) \right\}.$$

Hence, by (3), we obtain after some straightforward calculation

$$(7) \qquad \mu_K^*(N) = \frac{1}{D} \int_0^T \sum_{r=2}^{R} a_r \mu_{2m+2r} t^{2r} \cdot \frac{dt}{t^{2+\theta}} + O((AR)^{5R} T^{-1-\theta} e^{T^2} L^{-\frac{1}{2}})$$

$$+ O\left\{ \frac{(4T)^{2R+1-\theta}}{(2R+3)!} \mu_{2m+2R+2} + T^{-1-\theta} \right\}.$$

It is straightforward to check that

$$\mu_{2m+2R+2} \leq (2m+1)^{R+1}\,\mu_{2m}\mu_{2R+2} \leq (2m+1)^{R+1}\mu_{2m}(3R)^{R} = O((AR)^{R}), \quad \text{so that}$$

(7) becomes

$$\mu_K^*(N) = \frac{1}{D}\int_0^T \sum_{r=2}^{R} a_r\mu_{2m+2r}\,t^{2r}\cdot\frac{dt}{t^{2+\theta}} + O\Big\{T^{-1-\theta}(1+(AR)^{5R}e^{T^2}L^{-\frac{1}{2}}) + (\tfrac{A}{R})^{R+3}\,T^{2R+1-\theta}\Big\}. \tag{8}$$

We are now ready to deal with the leading term, and here, in a sense, we reverse the direction of the preceding argument. We know that

$$\mu_{2k} = \sqrt{\frac{2}{\pi}}\int_0^\infty x^{2k}\,e^{-\frac{1}{2}x^2}\,dx,$$

and therefore, by (5),

$$\sum_{r=2}^{R} a_r\mu_{2m+2r}\,t^{2r} = \sqrt{\frac{2}{\pi}}\int_0^\infty x^{2m}\,e^{-\frac{1}{2}x^2}\left\{\sum_{r=2}^{R} a_r(tx)^{2r}\right\}dx$$

$$= \sqrt{\frac{2}{\pi}}\int_0^\infty x^{2m}\,e^{-\frac{1}{2}x^2}\,(\sin tx)^4\,dx + O\left\{\frac{(4t)^{2R+2}}{(2R+2)!}\mu_{2m+2R+2}\right\}.$$

Now multiply by $D^{-1}\,t^{-2-\theta}$, integrate with respect to t from 0 to T, and interchange the order of integration (justified by absolute convergence). Then the leading term in (8) contributes

$$\sqrt{\frac{2}{\pi}}\int_0^\infty x^{2m}\,e^{-\frac{1}{2}x^2}\,\frac{1}{D}\left\{\int_0^T \frac{\sin^4(xt)}{t^{2+\theta}}\,dt\right\}dx + O((\tfrac{A}{R})^{R+3}\,T^{2R+1-\theta})$$

$$= \sqrt{\frac{2}{\pi}} \int_0^\infty x^{2m} e^{-\frac{1}{2}x^2} (x^{K-2m} + O(T^{-1-\theta})) \, dx + O((\frac{A}{R})^{R+3} T^{2R+1-\theta})$$

$$= \frac{2^{\frac{1}{2}K}}{\sqrt{\pi}} \Gamma(\frac{K+1}{2}) + O(T^{-1-\theta} + (\frac{A}{R})^{R+3} T^{2R+1-\theta})$$

by (4). Hence (8) becomes

$$(9) \qquad \mu_K^*(N) = \frac{2^{\frac{1}{2}K}}{\sqrt{\pi}} \Gamma(\frac{K+1}{2}) + O(T^{-1-\theta}(1 + (AR)^{5R} e^{T^2} L^{-\frac{1}{2}}) + (\frac{A}{R})^{R+3} T^{2R+1-\theta}).$$

It remains only to choose T and R. Let $T = (R/A)^{\frac{1}{2}}$ and $R = \frac{1}{10} \frac{\log L}{\log \log L}$. Then

$$\mu_K^*(N) = \frac{2^{\frac{1}{2}K}}{\sqrt{\pi}} \Gamma(\frac{K+1}{2}) + O((\frac{\log \log L}{\log L})^{\frac{1}{2}}), \qquad L = \log \log N,$$

which is a little more precise than the statement of the Theorem.

3. Erdös and Kac actually proved their theorem for the more general class of real strongly additive functions

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

which satisfy

(10) $\quad f(p) = O(1)$

and

(11) $$\sum_{p\le N} \frac{f^2(p)}{p} \to \infty \quad \text{as} \quad N \to \infty.$$

Writing

$$A_r(N) = \sum_{p\le N} \frac{f(p)^r}{p} \qquad (r=1,2),$$

our method extends without new complications to proving that, for each real number $\kappa > 0$,

(12) $$\lim_{N\to\infty} \frac{1}{N} \sum_{n=1}^{N} \left| \frac{f(n) - A_1(N)}{A_2(N)^{1/2}} \right|^{\kappa} = \frac{2^{\frac{1}{2}\kappa}}{\sqrt{\pi}} \Gamma\left(\frac{\kappa+1}{2}\right).$$

if f is a real strongly additive function satisfying (10) and (11). Indeed, it is clear from the details of the method that we could weaken (10) somewhat and still obtain (12).

H. N. Shapiro [9] proved the Erdös-Kac Theorem subject to (11) and the (analogue of the) Lindeberg condition

(13) for every $\varepsilon > 0$, $$\lim_{N\to\infty} A_2(N)^{-1} \sum_{\substack{p\le N \\ |f(p)|>\varepsilon A_2(N)^{1/2}}} \frac{f^2(p)}{p} = 0.$$

Moreover, Delange and Halberstam [4] showed that the moments associated with f behave in accordance with (2) if (11) and (13) hold and if also (cf (10))

$$(14) \qquad f(p) = O(A_2(p)^{1/2}) \ ;$$

but that this is false if one assumes only (11) and (13). It is very likely that (12) holds also for the Delange-Halberstam class of additive functions.

It should be mentioned in conclusion that the extension of the method of moments described above has been used with success also in the study of zeros of the Riemann zeta function (Ghosh [6]), and could be applied to the results about character sums in Davenport and Erdös [1], if ever anything were to be gained by so doing.

References

1. H. Davenport and P. Erdös, The distribution of quadratic and higher residues, Publ. Math. Debrecen 2, (1952), 252-265.

2. H. Delange, Sur le nombre des diviseurs premiers de n, C. R. Acad. Sci. (Paris), 237(1953), 542-4.

3. H. Delange, Sur un theoreme d'Erdös et Kac, Acad. Roy. Belg. Bull. Cl. Sci. (5) 42(1956), 130-44.

4. H. Delange and H. Halberstam, A note on additive functions, Pacific J. Math. 7(1957), 1551-6.

5. P. Erdös and M. Kac, The Gaussian Law of errors in the theory of additive number theoretic functions, Amer. J. Math. 62(1940), 738-42.

6. A. Ghosh, On Riemann's zeta function-sign changes of S(T), Recent Progress in Analytic Number Theory, Vol. I, Academic Press, London, 1981.

7. G. H. Hardy and S. Ramanujan, The normal number of prime factors of a number n, Quart. J. Math. (Oxford) 48(1917), 76-92.

8. M. Kac, Statistical Independence in Probability, Analysis & Number Theory, Carus Monograph No. 12, A. M. A., John Wiley 1959.

9. H. N. Shapiro, Distribution functions of additive arithmetic functions, Proc. Nat. Acad. Sci. USA, 42(1956), 426-30.

10. P. Turan, On a theorem of Hardy and Ramanujan, J. London Math. Soc. 9 (1934), 274-6.

On random multiplicative functions

by

G. HALASZ

Let $f(p)$ (p prime) be independent random variables taking the values $+1$ and -1 with probability $1/2$ each. We extend them to a multiplicative function by defining

$$f(n) = \begin{cases} \prod_{p|n} f(p) & \text{if } n \text{ is square free,} \\ 0 & \text{otherwise.} \end{cases}$$

A. Wintner [1] proved that

$$M(x) \overset{\text{def.}}{=} \sum_{n\le x} f(n) = O(x^{1/2+\varepsilon}), \neq O(x^{1/2-\varepsilon})$$

for every positive ε with probability 1 as a heuristic support for the Riemann hypothesis, the latter being equivalent to the first estimation for the special function with $f(p) \equiv -1$, the Moebius function. A deeper aspect of the problem is to find out how the number-theoretic dependence among $f(n)$ effects the magnitude, compared especially with the case of $f(n) = \pm 1$ being independent for all n when the exact order of magnitude $\sqrt{x \log\log x}$ is known by the law of the iterated logarithm. P. Erdös therefore proposed to give more precise estimations showing (unpublished, see [2]) as a first step that

$$M(x) = O(\sqrt{x}\,\log^{c_1} x), \neq O(\sqrt{x}/\log^{c_2} x) \tag{1}$$

with probability 1. Here and in what follows $c_1, c_2, \ldots$ are, unless otherwise stated, positive universal constants that could be given numerically. In the present paper we replace both these constants by arbitrary positive numbers.

THEOREM. (i) $M(x) = O(\sqrt{x}\, e^{c_3 \sqrt{\log\log x \log\log\log x}})$,

(ii) $M(x) \neq O(\sqrt{x}\, e^{-c_4 \sqrt{\log\log x \log\log\log x}})$

with probability 1.

Apart from the three times iterated logarithm in (i) -it will be outlined after the proof of Lemma 3 how to drop it by more careful calculation- these bounds seem to be the best our method can yield. Unfortunately they are still too weak to make a comparison with the law of the iterated logarithm. Surprisingly, the "logarithmic average"

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

is, as $\sigma \longrightarrow 1/2+0$, much smaller for our random multiplicative function than for $f(n)$ independent for all n as can easily be established.

Our problem can also be interpreted in the theory of orthogonal series. Realizing $f(p)$ as the Rademacher functions, $f(n)$ will be the Walsh system of functions in a number-theoretic reordering. In Wintner's and Erdös's upper bounds the ordering does not yet come into play -(1) in fact following for any $c_1 > 3/2$ from a theorem of Rademacher and Menchov concerning general orthogonal series- but it plays an important role in all the other results.

Proof of Theorem, (i). We shall show in Lemma 1 below that $M(x)$ changes little in short intervals :

$$\max_{x_{k-1}<x\le x_k} |M(x) - M(x_k)| = O(\sqrt{x_k})$$

almost surely, where $x_k = [e^{k^{c_6}}]$ with some $0 < c_6 < 1$. It therefore suffices to prove

$$\int_{x_{k-1}}^{x_k} M(x)dx = O(x_k - x_{k-1})\sqrt{x_k}\; e^{c_3\sqrt{\log\log x_k \log\log\log x_k}} \tag{2}$$

almost surely.

In each $f(n)$ built up from $f(p)$'s we separate primes $p \le z$ from those $p > z$, the parameter z to be specified later. Introducing the notations

$$M_1(x) = \sum_{\substack{m\le x \\ p\mid m \Rightarrow p\le z}} f(m), \qquad \sum_r^* = \sum_{\substack{r>z \\ p\mid r\Rightarrow p>z \\ r \text{ square free}}}$$

this leads to the decompositions

$$M(x) = M_1(x) + \sum_r^* f(r) M_1\left(\frac{x}{r}\right) \overset{\text{def.}}{=} M_1(x) + M_2(x), \tag{3}$$

$$\int_{x_{k-1}}^{x_k} M(x)dx = \int_{x_{k-1}}^{x_k} M_1(x)dx + \int_{x_{k-1}}^{x_k} M_2(x)dx, \tag{4}$$

where

$$\int_{x_{k-1}}^{x_k} M_2(x)dx = \sum_{r\le x_k}^* f(r) \int_{x_{k-1}}^{x_k} M_1\left(\frac{x}{r}\right)dx \overset{\text{def.}}{=} \sum_{r\le x_k}^* b_r f(r) \qquad (b_r = b(r,k,z)). \tag{5}$$

The advantage of this formula will be apparent later.

Observe that for $f(p)$ occuring in $M_1(x)$, hence in b_r we have $p \le z$, while for $f(p)$ occuring in $f(r)$ of $\sum^*$ we have $p > z$. These two being completely independent sets of random variables, we can, for the time being, fix the values $f(p)$ for $p \le z$, i.e. consider b_r as (deterministicly) constant coefficients. Note also that since r in $\sum^*$ is composed of primes $p > z$, the number of its prime divisors $\Omega(r)$ is limited and it is thus useful for (5) to apply Lemma 2 below :

$$E\left(\left|\sum_{r\le x_k}^* b_r f(r)\right|^{\ell} \mid f(p) \text{ fixed for } p\le z\right) \le \left(\sum_{r\le x_k}^* b_r^2 (\ell-1)^{\Omega(r)}\right)^{\ell/2} \tag{6}$$

for any even integer $\ell \ge 2$. (E stands for expectation). Markov's inequality implies for the conditional probability

$$\begin{aligned} &\text{Prob}\left(\left|\sum_{r\le x_k}^* b_r f(r)\right| > (x_k - x_{k-1})\sqrt{x_k}\, R \mid f(p) \text{ fixed for } p \le z\right) \\ &\le \frac{1}{R^{\ell}} \left(\frac{\sum_{r\le x_k}^* b_r^2 (\ell-1)^{\Omega(r)}}{(x_k - x_{k-1})^2 x_k}\right)^{\ell/2} \overset{\text{def.}}{=} \frac{D_k^{\ell/2}}{R^{\ell}} \qquad (D_k = D(k,z)). \end{aligned} \tag{7}$$

R is to be chosen later.

Using first the Cauchy-Schwarz inequality in the definition (5) of b_r ,

$$b_r^2 \le (x_k - x_{k-1}) \int_{x_{k-1}}^{x_k} M_1^2(\tfrac{x}{r})\, dx \le (x_k - x_{k-1}) x_k \int_{x_{k-1}/r}^{x_k/r} \frac{M_1^2(u)}{u}\, du,$$

$$\sum_{r \le x_k}^{*} b_r^2 (\ell-1)^{\Omega(r)} \le (x_k - x_{k-1}) x_k \sum_{r \le x_k} (\ell-1)^{\Omega(r)} \int_{x_{k-1}/r}^{x_k/r} \frac{M_1^2(u)}{u} du = (x_k - x_{k-1}) x_k \int_1^{x_k/z} \frac{M_1^2(u)}{u} \sum_{\frac{x_{k-1}}{u} < r \le \frac{x_k}{u}}^{*} (\ell-1)^{\Omega(r)},$$

the upper limit x_k/z coming from $r > z$ in $\sum^*$. The sum will be estimated in an elementary way in Lemma 3, (ii) below (taking $a = x_{k-1}/u$, $b = x_k/u \ge z$), giving for the quantity D_k defined in (7)

$$D_k \le \frac{1}{\log z} \left(c_{12} \frac{\log x_k}{\log z}\right)^{\ell-1} \int_1^{x_k/z} \frac{M_1^2(u)}{u^2}\, du, \tag{8}$$

provided that

$$z \ge e^{\left(\frac{x_k}{x_k - x_{k-1}}\right)^{\delta}} \tag{9}$$

with some fixed $\delta > 0$.

We can now explain the aim of our introductory steps. The last integral, since we expect $M_1(u)$ to be of the order about $\sqrt{u}$, is only a logarithm in magnitude not changing its order in a whole range

$$\sqrt{Y} < x_k \le Y : \tag{10}$$

$$D_k \le \frac{1}{\log z} \left(c_{12} \frac{\log Y}{\log z}\right)^{\ell-1} \int_1^{Y} \frac{M_1^2(u)}{u^2}\, du$$

independently of the many k in our range (fixing Y for the time being) and a trivial estimate of the integral will therefore suffice : letting now $f(p)$ for $p \le z$, too, be random variables we calculate the expectations

$$E\, M_1^2(u) = \sum_{\substack{m \le u \\ p \mid m \Rightarrow p \le z \\ m \text{ square free}}} 1 \le u,$$

$$E \frac{1}{\log z} \left(c_{12} \frac{\log Y}{\log z}\right)^{\ell-1} \int_1^{Y} \frac{M_1^2(u)}{u}\, du \le (c_{12} h)^{\ell} \quad \left(h \overset{\text{def.}}{=} \frac{\log Y}{\log z}\right) \tag{11}$$

and apply Markov's inequality to get with probability

$$1 - \frac{1}{R} \tag{12}$$

$$D_k \le (c_{12} h)^{\ell} R \tag{13}$$

for all k in the range (10) simultaneously.

If so, the right hand side of (7) becomes

$$\frac{D_k^{\ell/2}}{R^{\ell}} \le \frac{(c_{12}h)^{\ell^2/2}}{R^{\ell/2}} \le e^{-\frac{\log^2 R}{16\log(c_{12}h)}}$$

with the optimal choice $\ell = 2[\frac{\log R}{4\log(c_{12}h)}]$, provided that

$$\frac{\log R}{4\log(c_{12}h)} \ge 3. \tag{14}$$

(7) holds only for a single k. We discard all the events, at most $(\log Y)^{1/c_6}$ in number, (recall $x_k = [e^{k^{c_6}}]$), featuring in it corresponding to our range (10) of total conditional probability at most

$$(\log Y)^{1/c_6} e^{-\frac{\log^2 R}{16\log(c_{12}h)}}.$$

The condition (13) of this conditional probability is fulfilled with probability (12) and we see that with probability

$$(1-\frac{1}{R})\ (1 - (\log Y)^{1/c_6} e^{-\frac{\log^2 R}{16\log(c_{12}h)}})$$

we have for (5)

$$\left| \int_{x_{k-1}}^{x_k} M_2(x)dx \right| \le (x_k - x_{k-1})\sqrt{x_k}\ R \tag{15}$$

for all k in the range (10).

The first term of (4) is estimated trivially using Markov's inequality :

$$E\left(\int_{x_{k-1}}^{x_k} M_1(x)dx\right)^2 \le (x_k - x_{k-1})\int_{x_{k-1}}^{x_k} E\, M_1^2(x)dx \le (x_k - x_{k-1})^2 x_k e^{-h},$$

since

$$E\, M_1^2(x) = \sum_{\substack{m\le x \\ p|m \Rightarrow p\le z \\ m \text{ square free}}} 1 \le x_k e^{-h} \quad (z > c_{11},\ h \ge 2c_{11},\ x \le x_k) \tag{16}$$

by Lemma 3, (i) below, noting that $\log x_k/\log z \ge (1/2)\log Y/\log z = h/2$ according to the definition of h in (11), hence

$$\text{Prob}\left(\left|\int_{x_{k-1}}^{x_k} M_1(x)dx\right| \ge (x_k - x_{k-1})\sqrt{x_k}\right) \le e^{-h}$$

for a single k.

Discarding all these events of total probability at most

$$(\log Y)^{1/c_6}\, e^{-h},$$

we have

$$\left|\int_{x_{k-1}}^{x_k} M_1(x)dx\right| < (x_k - x_{k-1})\sqrt{x_k}$$

for all k in the range (10) simultaneously and combined with (15) we get for (4)

$$\left|\int_{x_{k-1}}^{x_k} M(x)dx\right| \le (x_k - x_{k-1})\sqrt{x_k}\,(R+1) \tag{17}$$

for all k in $\sqrt{Y} < x_k \le Y$ simultaneously with probability

$$1 - \left[\frac{1}{R} + (\log Y)^{1/c_6}\left(e^{-\frac{\log^2 R}{16\log(c_{12}h)}} + e^{-h}\right)\right].$$

In order to optimize this quantity let us e.g. choose $h = \log^2 R$ and in order to supress the power of $\log Y$ with a possibly small R set $\log R = \sqrt{(33/c_6)\log\log Y \log\log\log Y}$. We then get for the exceptional probability in the square bracket the upper bound

$$\frac{1}{R} + (\log Y)^{-1/c_6} \le \frac{2}{R} < e^{-c_5\sqrt{\log\log Y \log\log\log Y}} \tag{18}$$

for Y large enough. h defines z in (11) as

$$\log z = \frac{\log Y}{h} = \frac{\log Y}{(33/c_6)\log\log Y \log\log\log Y}$$

and as for $x_k = \left[e^{k^{c_6}}\right] \le Y$

$$\frac{x_k}{x_k - x_{k-1}} \sim \frac{1}{c_6}(\log x_k)^{(1-c_6)/c_6} \le \frac{1}{c_6}(\log Y)^{(1-c_6)/c_6},$$

we see that condition (9) is satisfied with e.g. $\delta = c_6$, while conditions (14), $z > c_{11}$ and $h > 2c_{11}$ in (16) are obviously satisfied.

Putting our choice of R into (17) and letting Y run through a sequence Y_s with $Y_{s-1} = \sqrt{Y_s}$, e.g. $Y_s = e^{2^s}$ we get (2) with any $c_3 > \sqrt{33/c_6}$ from the Borel-Cantelli lemma since the sum of the exceptional probabilities as estimated in (18) is finite.

Q.e.d.

LEMMA 1. *Let* $x_k = [e^{k^{c_6}}]$. *With suitable* $0 < c_6 < 1$ *we have*

$$\max_{x_{k-1}<x\le x_k} |M(x) - M(x_{k-1})| = \max_{x_{k-1}<x\le x_k} \Big|\sum_{x_{k-1}<n\le x} f(n)\Big| = O(\sqrt{x_k})$$

with probability 1.

In fact we could add any fixed negative power of $\log x_k$ as a factor to the right by further decreasing the value of c_6.

Proof. This is based on evaluating

$$E\Big(\sum_{u<n\le v} f(n)\Big)^4 = \sum_{u<\ell,m,n,r\le v} E\, f(\ell)f(m)f(n)f(r) = \sum_{\substack{u<\ell,m,n,r\le v \\ \ell mnr \text{ a complete square} \\ \ell,m,n,r \text{ square free}}} 1 .$$

We write s^2, $u^2 < s \le v^2$, for the complete square and observe that $\ell | s^2$ implies $\ell | s$, $s \overset{\text{def.}}{=} \ell\ell'$, $u^2/v < \ell' < v^2/u$, ℓ being square free. Noting also

$$\sum_{\substack{m,n,r \\ mnr=\frac{s^2}{\ell}=\ell\ell'^2}} 1 \le d^2(\ell\ell'^2) \le d^2(\ell)d^4(\ell')$$

owing to elementary properties of the divisor function $d(n) = \sum_{\substack{m,r \\ mr=n}} 1$, we obtain

$$E\Big(\sum_{u<n\le v} f(n)\Big)^4 \le \Big(\sum_{u<\ell\le v} d^2(\ell)\Big)\Big(\sum_{u^2/v<\ell'<v^2/u} d^4(\ell')\Big) \le \Big(\sum_{u^2/v<\ell<v^2/u} d^4(\ell)\Big)^2.$$

One way of estimating the sum here is to use Hölder's inequality and the elementary estimate

$$\sum_{\ell\le x} d^\alpha(\ell) = O(x \log^{2^\alpha - 1} x)$$

with $x = v^2/u$, $\alpha = 12$: assuming also $u+1 < v \le 2u$,

$$\sum_{u^2/v<\ell<v^2/u} d^4(\ell) < \Big(\sum_{\ell<v^2/u} d^{12}(\ell)\Big)^{1/3}\Big(\frac{v^2}{u} - \frac{u^2}{v} + 1\Big)^{2/3} < c_7 v^{1/3}(v-u)^{2/3}\log^{1365} v.$$

We could almost get $(v-u)$ but the exponent $2/3 > 1/2$ is just as good.

Markov's inequality implies for $x_{k-1} \le u < v \le x_k$

$$\text{Prob}\Big(\Big|\sum_{u<n\le v} f(n)\Big| > \frac{\sqrt{x_k}}{\log x_k}\Big) \le c_7^2\Big(\frac{v-u}{x_k}\Big)^{4/3} \log^{c_8} x_k.$$

Keeping k fixed temporarily we apply this result, in a nowadays standard way, to $u = x_{k-1} + (s-1)2^m$, $v = x_{k-1} + s2^m \le x_k$ for all possible choices of $s \ge 1$, $m \ge 0$, $s2^m \le x_k - x_{k-1}$. Summing the bounds for the corresponding probabilities,

$$c_7^2 \log^{c_8} x_k \sum_{2^m \le x_k - x_{k-1}} \left(\frac{2^m}{x_k}\right)^{4/3} \frac{x_k - x_{k-1}}{2^m} < c_9 \left(\frac{x_k - x_{k-1}}{x_k}\right)^{4/3} \log^{c_8} x_k .$$

With the exception of an event of this probability

$$\left| \sum_{u < n \le v} f(n) \right| \le \frac{\sqrt{x_k}}{\log x_k}$$

simultaneously for all the above intervals (u,v).

By dyadic decomposition every interval (x_{k-1}, x) $(x \le x_k)$ is the union of such intervals corresponding to different m and we find that

$$\max_{x_{k-1} < x \le x_k} \left| \sum_{x_{k-1} < n \le x} f(n) \right| < \frac{\sqrt{x_k}}{\log 2} ,$$

since m has at most $\log(x_k - x_{k-1})/\log 2 + 1$ different values. This then will follow almost surely for k large enough from the Borel-Cantelli lemma as for the above exceptional probability we have, when $x_k = \left[e^{k^{c_6}}\right]$,

$$\frac{x_k - x_{k-1}}{x_k} \sim \frac{c_6}{k^{1-c_6}} ,$$

$$c_9 \left(\frac{x_k - x_{k-1}}{x_k}\right)^{4/3} \log^{c_8} x_k < \frac{c_{10}}{k^{(4/3)(1-c_6) - c_8 c_6}} = \frac{c_{10}}{k^{5/4}} ,$$

choosing $c_6 = 1/16(c_8 + 4/3)$,

$$\sum \frac{1}{k^{5/4}} < +\infty ,$$

and the proof of Lemma 1 is completed.

We have made, in the course, a rather rough estimation of the 4^{th} moment as far as powers of logarithm are concerned. Some power is, however, indispensable and this makes it impossible to simply use this natural device of 4^{th} moments to prove our Theorem containing only $\log^{\varepsilon}$. In the present situation, however, we have taken sufficiently short intervals $x_k - x_{k-1} \sim x_k / \log^K x_k$ to cancel the effect of the logarithm.

Next we prove (6) in a different, but obviously equivalent, formulation in order to emphasize its independence of primes and our ordering of the Walsh system.

LEMMA 2. *With points* ω *of a countable set* Ω *we associate independent random variables* ξ_ω *taking* +1 *and* -1 *with probability* 1/2 *each. For any finite subset* A *we put* $\eta_A = \prod_{\omega\in A} \xi_\omega$ *and denote by* c_A *arbitrary constant coefficients. We have for every even integer* $\ell \geq 2$

$$E\Big|\sum_A c_A\,\eta_A\Big|^\ell \leq \Big(\sum_A |c_A|^2\,(\ell-1)^{|A|}\Big)^{\ell/2}$$

where A *runs through all finite sets* $A\subset\Omega$; $|A|$ *stands for the number of elements in* A.

This result, as we have learned long after completing the work published here, had been proved earlier by A. Bonami even for every real $\ell \geq 2$; see [3] where she gives various methods for proving this and related results. We present our different

Proof. This goes by induction on ℓ . Suppose we know that

$$|E\prod_{i=1}^{\ell}\Big(\sum_A c_A^{(i)}\,\eta_A\Big)| \leq \prod_{i=1}^{\ell}\sqrt{\sum_A |c_A^{(i)}|^2(\ell-1)^{|A|}} \tag{19}$$

for arbitrary ℓ sets of ceofficients $c_A^{(i)}$, where ℓ is an integer, even or odd. We deduce the inequality for ℓ+1. For ℓ=2 it is just the Cauchy-Schwarz inequality, the η_A being orthogonal and the lemma then follows as the special case $c_A^{(i)} = c_A$ $(1\leq i\leq \ell/2)$, $c_A^{(i)} = \bar{c}_A$ $(\ell/2 < i \leq \ell)$ when ℓ is even.

Now, multiplying out and separating $i = \ell + 1$,

$$E\prod_{i=1}^{\ell}\Big(\sum_A c_A^{(i)}\eta_A\Big) = \sum_B c_B^{(\ell+1)} \sum_{A_1,\dots,A_\ell} c_{A_1}^{(1)}\dots c_{A_\ell}^{(\ell)}\, E\,\eta_B\eta_{A_1}\dots\eta_{A_\ell} = \sum_B c_B^{(\ell+1)} \sum_{A_1,\dots,A_\ell}{}' c_{A_1}\dots c_{A_\ell},$$

where in $\sum'$ $(A_1,\dots,A_\ell)$ runs through all ℓ-tuples of finite sets which cover points $\omega\in B$ an odd number of times, points $\omega\notin B$ an even number of times.

We consider $A_i' = A_i \cap B$ and make them disjoint by the usual procedure : $A_1'' = A_1'$, $A_2'' = A_2' \setminus A_1''$, $A_3'' = A_3' \setminus (A_1'' \cup A_2'')$ and so son. The sets A_i cover B -(an odd non-negative number is ≥ 1)- thus the A_i'' form a disjoint decomposition

of B. Fixing this decomposition, in other words summing in $\sum'$ first only for those $(A_1,\dots,A_\ell)$ which yield the same decomposition $A_1'',\dots,A_\ell''$ we find for this summation $\sum''$

$$\Big|\sum''_{A_1,\dots,A_\ell} c_{A_1}^{(1)}\dots c_{A_\ell}^{(\ell)}\Big| \le E\prod_{i=1}^{\ell}\Big(\sum b_A^{(i)}\eta_A\Big),$$

where $b_A^{(i)} = |c_{A\cup A_i''}^{(i)}|$ if $A\cup A_i'' = \emptyset$ and 0 otherwise ; to see this the right hand side, when multiplied out, contains beside possibly other positive terms all terms

$$b_{A_1\setminus A_1''}^{(1)}\dots b_{A_\ell\setminus A_\ell''}^{(\ell)} E\,\eta_{A_1\setminus A_1''}\dots\eta_{A_\ell\setminus A_\ell''} = |c_{A_1}^{(1)}\dots c_{A_\ell}^{(\ell)}| E\,\eta_{A_1\setminus A_1''}\dots\eta_{A_\ell\setminus A_\ell''}$$

with $A_1,\dots,A_\ell$ occuring on the left hand side and this last expectation is in fact 1, since the sets $A_i\setminus A_i''$ $(i = 1,\dots,\ell)$ cover each point an even number of times : if $\omega\notin B$, then $\omega\notin A_i''$ $(i = 1,\dots,)$ and ω is covered by $A_i\setminus A_i''$ as many times as by A_i ; if on the other hand $\omega\in B$, then $\omega\in A_i''$ for precisely one value of i, thus ω is covered by $A_i\setminus A_i''$ one time less than by A_i, again an even number of times.

Hence we can apply our induction hypothesis (19) :

$$E\prod_{i=1}^{\ell}\Big(\sum b_A^{(i)}\eta_A\Big) \le \prod_{i=1}^{\ell}\sqrt{\sum_A |b_A^{(i)}|^2(\ell-1)^{|A|}} = \prod_{i=1}^{\ell}\sqrt{\sum_{D\supset A_i''}|c_D^{(i)}|^2(\ell-1)^{|D|-|A_i''|}}$$

$$= \prod_{i=1}^{\ell}\sqrt{m^{(i)}(A_i'')(\ell-1)^{-|A_i''|}}$$

with the notation

$$m^{(i)}(A) = \sum_{\substack{D\\ D\supset A}} |c_D^{(i)}|^2\,(\ell-1)^{|D|}.$$

Still keeping B fixed we sum now for all the possible $\ell^{|B|}$ disjoint decompositions $A_1'',\dots,A_\ell''$ of B using the Cauchy-Schwarz inequality :

$$\Big|\sum'_{A_1,\dots,A_\ell} c_{A_1}^{(1)}\dots c_{A_\ell}^{(\ell)}\Big|^2 \le \ell^{|B|}\sum_{A_1'',\dots,A_\ell''}\prod_{i=1}^{\ell} m^{(i)}(A_i'')(\ell-1)^{-|A_i''|}.$$

The inequality $|ab| \le \alpha|a|^2/2 + |b|^2/2\alpha$ implies with $\alpha = u\,\ell^{|B|}$

$$|c_B^{(\ell+1)} \sum_{A_1,\dots,A_\ell}{}' c_{A_1}^{(1)} \dots c_{A_\ell}^{(\ell)}| \le \frac{u}{2} |c_B^{(\ell+1)}|^2 \ell^{|B|} + \frac{1}{2u} \sum_{A_1'',\dots,A_\ell''} \prod_{i=1}^{\ell} m^{(i)}(A_i'')(\ell-1)^{-|A_i''|}.$$

Summing finally for B, introducing the notation

$$I_i = \sum_A |c_A^{(i)}|^2 \ell^{|A|} \quad (i = 1,\dots,\ell+1)$$

the first term gives $(u/2)I_{\ell+1}$ and the second

$$\frac{1}{2u} \sum_{A_1'',\dots,A_\ell''} \prod_{i=1}^{\ell} m^{(i)}(A_i'')(\ell-1)^{-|A_i''|} \le \frac{1}{2u} \prod_{i=1}^{\ell} \Big(\sum_A m^{(i)}(A)(\ell-1)^{-|A|}\Big),$$

summation on the left being extended over all tuples of ℓ disjoint sets $A_1'',\dots,A_\ell''$.

Here

$$\sum_A m^{(i)}(A)(\ell-1)^{-|A|} = \sum_A (\ell-1)^{-|A|} \sum_{D\supset A} |c_D^{(i)}|^2 (\ell-1)^{|D|} = \sum_D |c_D^{(i)}|^2 (\ell-1)^{|D|} \sum_{A\subset D} (\ell-1)^{-|A|}$$

$$= \sum_D |c_D^{(i)}|^2 \ell^{|D|} = I_i.$$

Collecting our estimations we get

$$|E \prod_{i=1}^{\ell+1} \Big(\sum_A c_A^{(i)} \eta_A\Big)| \le \frac{u}{2} I_{\ell+1} + \frac{1}{2u} \prod_{i=1}^{\ell} I_i = \prod_{i=1}^{\ell+1} \sqrt{I_i}$$

with the optimal choice $u = \sqrt{(\prod_{i=1}^{\ell} I_i)/I_{\ell+1}}$ what we had to prove.

The following lemma is partly known (in much stronger form), starting from the work of N. de Bruijn and partly standard.

LEMMA 3. *Let* $\gamma = \log b/\log z$. *Using again the notation*

$$\sum_r^* = \sum_{\substack{p|r \Rightarrow p>z \\ r \text{ square free}}} r$$

and also $\sum_*$ *for the same summation with* $p \le z$, *we have*

(i) $$\sum_{n\le b}^* 1 \le b\, e^{-\gamma}$$

for $z,\ \gamma > c_{11}$;

(ii) $$\sum_{a<r\le b}^* \ell^{\Omega(r)} \le \frac{b-a}{\log b}(c_{12}\gamma)^{\ell}$$

for $\ell \ge 1,\ z > e^{(\frac{b}{b-a})^{\delta}}$ $(\delta > 0)$ *and* $c_{12} = c_{12}(\delta)$.

Proof, (i). With $\gamma \geq 2$ we first look at

$$\sum_{\frac{b}{z}<n\leq b}{}^{*} 1 \leq \frac{1}{\log \frac{b}{z}} \sum_{\frac{b}{z}<n\leq b}{}^{*} \log n \leq \frac{2}{\log b} \sum_{m}{}^{*} \sum_{\substack{p\leq z \\ \frac{b}{z}<mp\leq b}} \log p \leq \frac{c_{13}\, b}{\log b} \sum_{m>\frac{b}{z^2}}{}^{*} \frac{1}{m}$$

by Chebyshev's elementary estimation $\sum_{p\leq u} \log p = O(u)$ which, by the way, he obtained from essentially the same formula that we have just used. This device of turning a strong average into a logarithmic one has also been used by E. Wirsing and H. Delange for general multiplicative functions and a similar thing happens also in the proof of our Theorem, (i).

Now, with $v = b/z^2$, $\beta \leq 1$

$$\sum_{m>v}{}^{*} \frac{1}{m} \leq \frac{1}{v^{1-\beta}} \sum_{m=1}^{\infty}{}^{*} \frac{1}{m^{\beta}} = \frac{1}{v^{1-\beta}} \prod_{p\leq z} \left(1+\frac{1}{p^{\beta}}\right) \leq e^{-(1-\beta)\log v + \sum_{p\leq z} \left(\frac{1}{p^{\beta}} - \frac{1}{p}\right) + \log\log z + c_{14}},$$

where we have made use of the elementary asymptotics

$$h(u) \overset{\text{def.}}{=} \sum_{p\leq u} \frac{1}{p} = \log\log u + O(1).$$

This latter also implies by partial summation

$$\sum_{p\leq z} \left(\frac{1}{p^{\beta}} - \frac{1}{p}\right) = \int_2^z (u^{1-\beta}-1)\,dh(u) = \int_1^z \frac{u^{1-\beta}-1}{u\log u}\,du + O(z^{1-\beta}) = \int_0^{(1-\beta)\log z} \frac{e^t-1}{t}\,dt + O(z^{1-\beta}) = O(z^{1-\beta})$$

and we get

$$\sum_{m>v}{}^{*} \frac{1}{m} \leq e^{-(1-\beta)\log v + c_{15} z^{1-\beta} + \log\log z} \leq \log z\; e^{-(\gamma-2)\log\frac{\gamma-2}{c_{15}} + \gamma - 2} \leq c_{16} \log z\, e^{-2\gamma}$$

with the optimal choice of β given by the equation $\log v/\log z = \gamma-2 = c_{15} z^{1-\beta}$.

Collecting our estimates,

$$\sum_{\frac{b}{z}<n\leq b}{}^{*} 1 \leq \frac{c_{13}\, b}{\log b}\, c_{16} \log z\, e^{-2\gamma} \leq c_{17}\, b\, e^{-2\gamma},$$

trivially holding for $\gamma \leq 2$. Using this with b/z, b/z^2... and so on as b with corresponding values $\gamma-1$, $\gamma-2$,...,

$$\sum_{n\leq b}{}^{*} 1 \leq c_{17} \sum_{k=0}^{\infty} \frac{b}{z^k}\, e^{-2(\gamma-k)} \leq 2c_{17}\, b\, e^{-2\gamma}$$

for $z > 2e^2$ and Lemma 3, (i) follows.

(ii) The same formula as above leads to the inequality

$$\sum_{a<r\le b}^{*} \ell^{\Omega(r)} \le \frac{1}{\log a} \sum_{m\le \frac{b}{z}}^{*} \ell^{\Omega(m)+1} \sum_{\frac{a}{m}<p\le\frac{b}{m}} \log p.$$

Here we can use the prime number theorem with a logarithmic remainder to get $\sum_{u<p\le v} \log p \le c_{18}(v-u)$, provided that $v-u \ge v/\log^{1/\delta} v$ $(c_{18} = c_{18}(\delta))$. With $u = a/m$, $v = b/m$ this condition takes the form $\log(b/m) \ge (b/(b-a))^{\delta}$ and this is certainly fulfilled if $\log z \ge (b/(b-a))^{\delta}$ which is assumed in the lemma. We get further

$$\le \frac{1}{\log a} c_{18}\ell(b-a) \sum_{m\le b}^{*} \frac{\ell^{\Omega(m)}}{m} \le \frac{c_{18}\ell(b-a)}{\log a} \prod_{z<p\le b} (1+\frac{\ell}{p}) \le \frac{c_{18}\ell(b-a)}{\log a} e^{\ell \sum_{z<p\le b} \frac{1}{p}}$$

$$\le \frac{c_{18}\ell(b-a)}{\log a} e^{\ell \log(c_{19}\gamma)}$$

proving Lemma 3, (ii).

The three times iterated log factor in Theorem, (i) comes from the large factor $(c_{12}\gamma)^{\ell}$ in Lemma 3, (ii) which in turn comes from $\sum_{z<p\le b} \frac{1}{p}$. We can, however, restrict these primes to ranges $\sum_{z<p\le z^2} \frac{1}{p} = O(1)$ by decomposing $M(x)$ into a greater number of parts than in (3) according to e.g. the sequence $z_j = e^{2^j}$;

$$M(x) = \sum_{z_{j_o}<z_j\le x^2} \sum_{\substack{r\le x \\ p\mid r \Rightarrow z_{j-1}<p\le z_j}} f(r) \sum_{\substack{m\le \frac{x}{r} \\ p\mid m \Rightarrow p\le z_{j-1}}} f(m) + \sum_{\substack{n\le x \\ p\mid n \Rightarrow p\le z_{j_o}}} f(n) .$$

Estimating the inner double sums for each j separately the same way as in our Theorem enables one to drop the three times iterated logarithm.

Proof of Theorem, (ii). A natural idea we have been unable to implement of estimating the integral of (8) non-trivially would be to use generating Dirichlet series ; (see [4] for an attempt). But this is how we get our lower bound.

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

converges for $\sigma = \mathrm{Re}\, s > 1/2$ as follows already from Wintner's upper bound. Its connection with $M(x)$ is given by the partial integration

$$F(s) = \int_1^\infty \frac{dM(x)}{x^s} = s\int_1^\infty \frac{M(x)}{x^{s+1}}\,dx\ .$$

Cutting the range of integration by $x_0 = \exp(1/\sqrt{\sigma-1})$ we get for $|t| = |\mathrm{Im}\, s| \le 2$, say,

$$|F(s)| \le 3\Big(\max_{x\ge 1}\frac{|M(x)|}{\sqrt{x}}\int_1^{x_0}\frac{dx}{x^{\sigma+1/2}} + \max_{x\ge x_0}\frac{|M(x)|}{\sqrt{x}}\int_1^\infty \frac{dx}{x^{\sigma+1/2}}\Big)$$

$$\le 3\Big(\max_{x\ge 1}\frac{|M(x)|}{\sqrt{x}}\cdot\frac{1}{\sqrt{\sigma-1/2}} + \max_{x\ge x_0}\frac{|M(x)|}{\sqrt{x}}\cdot\frac{1}{\sigma-1/2}\Big).$$

Suppose Theorem, (ii) were false. This would imply with positive probability uniformly for $|t| \le 2$, $\sigma \to 1/2+0$, with the notation $L = \log 1/(\sigma-1/2)$,

$$F(s) = O\big(e^{L/2} + e^{L-c_2\sqrt{(L/2)\log(L/2)}}\big).$$

The connection with primes is given by the Euler product representation

$$F(s) = \prod_p\Big(1+\frac{f(p)}{p^s}\Big) = e^{\sum_p \frac{f(p)}{p^s} - (1/2)\sum_p \frac{1}{p^{2s}} + \sum_{k=3}^\infty \sum_p \frac{(-1)^{k+1}f^k(p)}{k\,p^{ks}}}\ .$$

This is valid for $\sigma > 1$ by absolute convergence. The second and third parts converge absolutely even for $\sigma > 1/2$ while the first sum converges there by Kolmogorov's theorem, $f(p)$ being independent and $\sum 1/p^{2\sigma} < \infty$. The exponential formula thus extends to the half-plane $\sigma > 1/2$.

The third part is uniformly bounded in this half-plane. The second part, by a similar exponential formula for the Riemann zeta function, equals

$$\frac{1}{2}\log\xi(2s) - \frac{1}{2}\sum_{k=2}^\infty \sum_p \frac{1}{k\,p^{2ks}}$$

and is also uniformly bounded e.g. in the domain $\sigma > 1/2$, $1 \le t \le 2$ avoiding the pole at $s = 1/2$ of $\xi(2s)$. We infer

$$(20)\qquad \max_{1\le t\le 2}\ \mathrm{Re}\sum_p \frac{f(p)}{p^s} = \max_{1\le t\le 2}\sum_p f(p)\,\frac{\cos(t\log p)}{p^\sigma} \le L - (c_2/2)\sqrt{L\log L}$$

as $\sigma \to 1/2 + 0$ with positive probability.

We shall show later that with x defined by $\sigma-1/2 = 1/\log x$ (then $L = \log\log x$) the contribution of terms $p > x$ is negligible as is the error made by replacing σ

by 1/2 for $p \le x$. Our first aim is, therefore, to prove

$$\max_{1\le t\le 2} \sum_{p\le x} f(p)\,\frac{\cos(t\log p)}{\sqrt{p}} > L - c_{20}\sqrt{L\log L} \quad (L=\log\log x)$$

almost surely for $x \to \infty$ through some sequence, a contradiction if $c_2 > 2\,c_{20}$.

We have to split up the sum into smaller parts. The next lemma explains why.

LEMMA 4.

$$\Big|\sum_{y<p\le x} \frac{\cos(\alpha\log p)}{p}\Big| \le \frac{c_{21}}{\alpha\log y} \quad (1/\log y \le \alpha \le 4).$$

Proof. The quantity is

$$\int_y^x \cos(\alpha\log u)\,dh(u),$$

where

$$h(u) \overset{\text{def.}}{=} \sum_{p\le u}\frac{1}{p} = \log\log u + C + g(u), \quad g(u) = O\Big(\frac{1}{\log^2 u}\Big) \tag{21}$$

as follows from the prime number theorem with a logarithmic remainder by partial summation.

First,

$$\int_y^x \cos(\alpha\log u)\,d\log\log u = \int_{\log y}^{\log x}\frac{\cos(\alpha u)}{u}\,du = \int_{\alpha\log y}^{\alpha\log x}\frac{\cos u}{u}\,du = O\Big(\frac{1}{\alpha\log y}\Big)$$

$$(\alpha\log y \ge 1).$$

Secondly,

$$\int_y^x \cos(\alpha\log u)\,dg(u) = [g(u)]_y^x + \alpha\int_y^x g(u)\,\frac{\sin(\alpha\log u)}{u}\,du = O\Big(\frac{1}{\log y}\Big) \qquad (0\le\alpha\le 4)$$

proving Lemma 4.

We define accordingly

$$\varphi(t) = \sum_{y<p\le x} f(p)\,\frac{\cos(t\log p)}{\sqrt{p}} \quad (1\le t\le 2).$$

The correlation

$$E\varphi(t)\varphi(\tau) = \sum_{y<p\le x}\frac{\cos(t\log p)\cos(\tau\log p)}{p} = \frac{1}{2}\sum_{y<p\le x}\frac{\cos((t-\tau)\log p)+\cos((t+\tau)\log p)}{p}$$

measures the independence of values taken at a distance $\alpha = |t-\tau|$. The proof of the lemma shows that this correlation would be rather large for $0 \le \alpha \le 1/\log y$ while it decreases more rapidly for $\alpha \ge 1/\log y$. Thus forced to take y large we can

then apply to our sub-sum essentially the same method as in [5] based on the almost independence of values taken at distant points.

We take a non negative function

$$k(x) = \begin{cases} 1 & x \geq M+1, \\ 0 & x \leq M, \end{cases}$$

M will be given later and consider for an arbitrary set $S \subset [1,2]$ the random variable

$$\eta = \int_S k(\varphi(t))dt \leq |\{t : t \in S, \varphi(t) \geq M\}|; \tag{22}$$

($|\ \ |$ of a set means its Lebesgue measure).

We wish to show that with large probability η is large, i.e. $\varphi(t)$ is large on a large set. With a view of applying Chebyshev's inequality for this purpose we calculate the first and second moments of η using what is called the characteristic function method in probability.

Accordingly we introduce the Laplace transform

$$K(w) = \int_M^\infty k(x)e^{-wx}dx \qquad (\mathrm{Re}\ w > 0)$$

that we shall only consider on the line $\mathrm{Re}\, w = 1$.

We have

$$|K(w)w^r| = \left|\int_M^{M+1} k^{(r)}(x)e^{-wx}dx\right| \leq c_{22} \quad (r = 1,\ldots,6, \quad M \geq 0)$$

provided that $|k^{(r)}(x)| \leq c_{22}$ $(r = 1,\ldots,6)$ and we fix $k(x)$ between M and $M+1$ with this property, implying

$$\int_{(1)} |K(w)\, w^4||dw| \leq c_{23} \tag{23}$$

integrated on the vertical line $\mathrm{Re}\, w = 1$.

We also have

$$k(x) = \frac{1}{2\pi i}\int_{(1)} K(w)e^{wx}dw,$$

$$k(\varphi(t)) = \frac{1}{2\pi i}\int_{(1)} K(w)e^{w\varphi(t)}dw,$$

$$E\eta = \frac{1}{2\pi i}\int_S\int_{(1)} K(w)E\, e^{w\varphi(t)}dw\, dt\,. \tag{24}$$

Here, $f(p)$ being independent,

$$Ee^{w\varphi(t)} = \prod_{y<p\leq x} E\, e^{wf(p)\frac{\cos(t\log p)}{\sqrt{p}}} = \prod_{y<p\leq x} \mathrm{ch}\left(\frac{w\cos(t\log p)}{\sqrt{p}}\right).$$

As $\operatorname{ch} z = \exp(z^2/2 + O(|z|^4))$ for $|z| \le 1$, we have for $|w| \le \sqrt{y}$

$$\operatorname{ch}\left(\frac{w\cos(t\log p)}{\sqrt{p}}\right) = \frac{w^2\cos^2(t\log p)}{2p} + O\left(\frac{|w|^4}{p^2}\right) = \frac{w^2}{4p} + \frac{w^2\cos(2t\log p)}{4p} + O\left(\frac{|w|^4}{p^2}\right)$$

and by Lemma 4 $(2 \le \alpha = 2t \le 4)$, introducing for simplicity

$\Delta = \log\log x - \log\log y$ $\left(= \sum_{y<p\le x} 1/p + O(1/\log y)\right)$ and estimating rather roughly

$$Ee^{w\varphi(t)} = e^{\frac{w^2}{4}\sum_{y<p\le x}\frac{1}{p} + O\left(\frac{|w|^2}{\log y}\right) + O\left(\frac{|w|^4}{y}\right)} = e^{w^2\Delta/4} + O\left(\frac{w^4}{\log y}\, e^{\Delta/4}\right),$$ recalling

$|w| \ge \operatorname{Re} w = 1$, provided that $|w| \le (\log y)^{1/4}$. For $\operatorname{Re} w = 1$, $|w| \ge (\log y)^{1/4}$ we only use the trivial

$$\left|\prod_{y<p\le x} \operatorname{ch}\left(\frac{w\cos(t\log p)}{\sqrt{p}}\right)\right| \le \prod_{y<p\le x} \operatorname{ch}\left(\frac{1}{\sqrt{p}}\right) \le c_{24}e^{\Delta/2}.$$

Splitting the inner integral of (24) accordingly,

$$\int_{\substack{(1)\\ |w|\le(\log y)^{1/4}}} K(w)Ee^{w\varphi(t)}dw - \int_{\substack{(1)\\ |w|\le(\log y)^{1/4}}} K(w)e^{w^2\Delta/4}dw + O\left(\frac{e^{\Delta/4}}{\log y}\right)\int_{(1)} |K(w)w^4||dw|,$$

$$\int_{\substack{(1)\\ |w|\ge(\log y)^{1/4}}} K(w)Ee^{w\varphi(t)}dw = O(e^{\Delta/2}) \int_{\substack{(1)\\ |w|\ge(\log y)^{1/4}}} |K(w)|\,|dw|\,.$$

The error made in the main term when integration is extended to the whole line $\operatorname{Re} w = 1$ can be included into the last $O(\ )$ term which in turn is inferior to the last but one $O(\ )$ term, $\Delta/4$ to be replaced in it by $\Delta/2$. Using for it our preliminary estimation (23) and integrating the formula thus arisen at the same time with respect to t (of which the formula does not depend),

$$E\eta = |S|\left(\frac{1}{2\pi i}\int_{(1)} K(w)e^{w^2\Delta/4}\,dw + O\left(\frac{e^{\Delta/2}}{\log y}\right)\right). \tag{25}$$

Here, by Plancherel's formula, the integral becomes

$$\frac{1}{\sqrt{\pi\Delta}}\int_M^\infty k(x)e^{-\frac{x^2}{\Delta}}dx \ge \frac{1}{\sqrt{\pi\Delta}}\, e^{-\frac{(M+2)^2}{\Delta}} \ge c_{25}\, e^{-\frac{M^2}{\Delta} - (1/2)\log\Delta}$$

and

$$E\eta \ge (c_{25}/2)\,|S|e^{-\frac{M^2}{\Delta} - (1/2)\log\Delta} \tag{26}$$

for we shall have

(27) $$0 \le M \le \Delta, \quad \log y \ge e^{2\Delta}, \quad \Delta \ge c_{26} .$$

Next,

$$\eta^2 = \int_S\int_S k(\varphi(t))k(\varphi(\tau))dtd\tau$$

(28) $$E\eta^2 = \int_S\int_S E\, k(\varphi(t))k(\varphi(\tau))dtd\tau$$

$$k(\varphi(t))k(\varphi(\tau)) = \frac{1}{(2\pi i)^2}\int_{(1)}\int_{(1)} K(w)K(z)e^{w\varphi(t)+z\varphi(\tau)}dwdz$$

$$E\, k(\varphi(t))k(\varphi(\tau)) = \frac{1}{(2\pi i)^2}\int_{(1)}\int_{(1)} K(w)K(z) \prod_{y<p\le x} ch\left(\frac{w\cos(t\log p)+z\cos(\tau\log p)}{\sqrt{p}}\right).$$

Similarly and as roughly as above the product will be

$$e^{\frac{1}{2}\sum_{y<p\le x}\frac{(w\cos(t\log p)+z\cos(\tau\log p))^2}{p}+O\left(\frac{(|w|+|z|)^4}{y}\right)} = e^{w^2\Delta/4+z^2\Delta/4+O\left(\frac{(|w|+|z|)^4}{|t-\tau|\log y}\right.}$$

$$= e^{w^2\Delta/4+z^2\Delta/4}+O\left(\frac{(|w|+|z|)^4}{|t-\tau|\log y}\, e^{\Delta/2}\right)$$

by Lemma 4 with $\alpha = 2t,\ 2\tau,\ t+\tau$ and $|t-\tau|$, provided that $|w|,\ |z| \le (|t-\tau|\log y)^{1/4}$.

For other w, z on $\mathrm{Re}\, w = \mathrm{Re}\, z = 1$ we only use the trivial

$$\left|\prod_{y<p\le x} ch\left(\frac{w\cos(t\log p)+z\cos(\tau\log p)}{\sqrt{p}}\right)\right| \le \prod_{y<p\le x} ch\left(\frac{2}{\sqrt{p}}\right) \le c_{27}\, e^{2\Delta} .$$

We see similarly as in the one dimensional case

$$Ek(\varphi(t))k(\varphi(\tau)) = \frac{1}{(2\pi i)^2}\int_{(1)}\int_{\substack{(1)\\ |w|,|z|\le(|t-\tau|\log y)^{1/4}}} K(w)K(z)e^{w^2\Delta/4+z^2\Delta/4}\, dwdz$$

$$+ O\left(\frac{e^{\Delta/2}}{|t-\tau|\log y}\right)\int_{(1)}\int_{(1)} |K(w)K(z)|\,(|w|+|z|)^4\,|dw||dz|$$

$$+ O(e^{2\Delta})\int_{(1)}\int_{\substack{(1)\\ \max(|w|,|z|)\ge(|t-\tau|\log y)^{1/4}}} |K(w)K(z)|\,|dw||dz|$$

$$= \left(\frac{1}{2\pi i}\int_{(1)} K(w)e^{w^2\Delta/4}\, dw\right)^2 + O\left(\frac{e^{2\Delta}}{|t-\tau|\log y}\right) \qquad (|t-\tau|\log y \ge 1).$$

For $|t-\tau|\log y \le 1$ we cannot but use the trivial estimate :

$$E\, k(\varphi(t))k(\varphi(\tau)) \le \frac{c_{27}e^{2\Delta}}{(2\pi)^2}\int_{(1)}\int_{(1)}|K(w)K(z)||dw||dz| \le c_{28}\, e^{2\Delta}\ .$$

When integrated with respect to t and τ in (28) separately for $|t-\tau|\log y \ge 1$ and ≤ 1, our results yield

$$E\eta^2 \le |S|^2\Big(\frac{1}{2\pi i}\int_{(1)}K(w)e^{w^2\Delta/4}dw\Big)^2 + O\Big(|S|\,\frac{e^{2\Delta}\log(|S|\log y)}{\log y}\Big) + O\Big(|S|\,\frac{e^{2\Delta}}{\log y}\Big).$$

Replacing the integral by $E\eta$ according to (25),

$$E\eta^2 \le \Big(E\eta + O\Big(|S|\frac{e^{\Delta/2}}{\log y}\Big)\Big)^2 + O\Big(|S|\frac{e^{2\Delta}\log(|S|\log y)}{\log y}\Big) = (E\eta)^2 + O\Big(|S|\frac{e^{2\Delta}\log(|S|\log y)}{\log y}\Big)$$

$$(|S|\log y \ge 2)$$

for trivially $E\eta \le |S| \le 1$. We have thus found for the variance of η

$$E\,\eta^2 - (E\eta)^2 = O\Big(|S|\frac{e^{2\Delta}\log(|S|\log y)}{\log y}\Big)\ .$$

Let us apply now Chebyshev's inequality combined with the lower bound for $E\eta$ in (26)

$$\text{Prob.}(\eta < (1/2)E\eta) = O\Big(|S|\frac{e^{2\Delta}\log(|S|\log y)}{(E\eta)^2\log y}\Big) = O\Big(\frac{e^{5\Delta}\log(|S|\log y)}{|S|\log y}\Big) \le e^{-\Delta}$$

for we shall have $|S|\log y \ge \exp(7\Delta)$. By the definition (22) of η, using again the lower bound (26) of $E\eta$,

$$\text{Prob.}\ \Big(|\{t : t\in S,\ \varphi(t) \ge M\}| < |S|e^{-\frac{M^2}{\Delta} - \log\Delta}\Big) \le e^{-\Delta},$$

provided that

$$|S|\log y \ge e^{7\Delta}\ ,\ 0 \le M \le \Delta\ ,\ \Delta \ge c_{29}. \tag{29}$$

If so, our previous conditions (27) will also be fulfilled.

We shall define a sequence y_k $(k = 0,1....)$, corresponding blocks

$$\varphi_k(t) = \sum_{y_{k-1}<p\le y_k} f(p)\,\frac{\cos(t\log p)}{\sqrt{p}} \qquad (k = 1,2,...),$$

corresponding sequences $\Delta_k = \log\log y_k - \log\log y_{k-1}$, M_k and a sequence of sets $S_k \subset [1,2]$ with

$$|S_k| = |S_{k-1}|e^{-\frac{M_k^2}{\Delta_k} - \log\Delta_k}\ .$$

With k_0 to be specified later we apply our result for $S = S_{k_0-1} = [1,2]$, $y = y_{k_0-1}$, $x = y_{k_0}$, $\varphi(t) = \varphi_{k_0}(t)$, $\Delta = \Delta_{k_0}$, $M = M_{k_0}$. It gives us with probability $1 - \exp(-\Delta_{k_0})$ a random set $S_{k_0} \subset S_{k_0-1}$ of measure

$$|S_{k_0}| = |S_{k_0-1}|\, e^{-\frac{M_{k_0}^2}{\Delta_{k_0}} - \log \Delta_{k_0}}$$

on which $\varphi_{k_0}(t) \geq M_{k_0}$. This random set depends on $f(p)$ for $p \leq y_{k_0}$ which are independent of $f(p)$ for $p > y_{k_0}$, so we can fix this set and take it as our S for the next block $\varphi(t) = \varphi_{k_0+1}(t)$. Our result again gives us with conditional probability $1 - \exp(-\Delta_{k_0+1})$ a random set $S_{k_0+1} \subset S_{k_0}$ (depending only on $f(p)$ for $p \leq y_{k_0+1}$) of measure

$$|S_{k_0+1}| = |S_{k_0}|\, e^{-\frac{M_{k_0+1}^2}{\Delta_{k_0+1}} - \log \Delta_{k_0+1}}.$$

on which $\varphi_{k_0+1}(t) \geq M_{k_0+1}$ and so on. We see that on S_k $\varphi_\ell(t) \geq M_\ell$ for all $k_0 \leq \ell \leq k$ and thus

$$\sum_{p \leq y_k} f(p)\, \frac{\cos(t \log p)}{\sqrt{p}} = \sum_{\ell=k_0}^{k} \varphi_\ell(t) + O(1) \geq \sum_{\ell=1}^{k} M_\ell + O(1) \tag{30}$$

($O(1)$ depends on k_0) on a set S_k of measure

$$|S_k| = \prod_{\ell=k_0}^{k} e^{-\frac{M_\ell^2}{\Delta_\ell} - \log \Delta_\ell}$$

for all k simultaneously with probability

$$\prod_{k=k_0}^{\infty} (1 - e^{-\Delta_k}).$$

We have to satisfy first of all the condition

$$|S_{k-1}| \log y_{k-1} \geq e^{7\Delta_k}. \tag{31}$$

Recalling the definitions of our sequences this can be rewritten as

$$\sum_{\ell=1}^{k_0-1} \Delta_\ell + \sum_{\ell=k_0}^{k-1} \left(\Delta_\ell - \frac{M_\ell^2}{\Delta_\ell} - \log \Delta_\ell\right) \geq 7\Delta_k, \quad (\text{let } \log\log y_0 = 0).$$

Here $\Delta_\ell - M^2/\Delta_\ell \geq \Delta_\ell - M_\ell$ if $0 \leq M_\ell \leq \Delta_\ell$ and it is reasonable to set $\Delta_\ell - M_\ell = 2 \log \Delta_\ell$. The inequality will then certainly be fulfilled if we set

$$\sum_{\ell=1}^{k-1} \log \Delta_\ell = 7\, \Delta_k \qquad (k = 2,3,\ldots),$$

i.e. $\Delta_2 = (1/7) \log \Delta_1$, $\Delta_k = \Delta_{k-1} + (1/7)\log \Delta_{k-1}$ $(k = 2,3,\ldots)$. Starting this recurrence with Δ_1 large enough, all the remaining conditions $0 \leq M_k \leq \Delta_k$, $\Delta_k \geq c_{29}$ of (29) will also be satisfied.

We easily see that $\Delta_k \sim (1/7) k \log k$; alternatively we could define Δ_k a priori as e.g. $(1/8)\, k \log k$ and verify the requirements for $k \geq k_0$, k_0 large enough. We have

$$\log\log y_k = \sum_{\ell=1}^{k} \Delta_\ell \sim (1/14)\, k^2 \log k,$$

$$\log\log y_k - \sum_{\ell=1}^{k} M_\ell = \sum_{\ell=1}^{k} (\Delta_\ell - M_\ell) = 2 \sum_{\ell=1}^{k} \log \Delta_\ell \sim 2k \log k \sim \sqrt{28 \log\log y_k \log\log\log y_k}$$

implying in (30)

$$\sum_{p \leq x} f(p)\, \frac{\cos(t \log p)}{\sqrt{p}} \geq L - \sqrt{29 L \log L} \qquad (L = \log\log x) \tag{32}$$

as $x = y_k \to \infty$ for t belonging to a set $S_k \subset [1,2]$ of measure

$$|S_k| > \frac{1}{\log x} \tag{33}$$

(see (31)) almost surely, letting $k_0 \to \infty$, since $\sum_{k=1}^{\infty} \exp(-\Delta_k) < +\infty$.

It remains to examine the difference of the quantities in (32) and (20) for $\sigma = \sigma_k = 1/2 + 1/\log x = 1/2 + 1/\log y_k$:

$$\rho(t) = \sum_{p \leq x} f(p)\, \frac{\cos(t \log p)}{\sqrt{p}} (1 - p^{1/2-\sigma}) - \sum_{p > x} f(p)\, \frac{\cos(t \log p)}{p^\sigma}\,. \tag{34}$$

A standard real variable technique will suffice here.

We have for $v \geq 0$

$$\int_1^2 e^{v\rho(t)} dt \geq e^{vM} \,|\{t : t \in [1,2],\ \rho(t) \geq M\}|$$

and calculate

$$E \int_1^2 e^{v\rho(t)}\, dt = \int_1^2 E\, e^{v\rho(t)} dt.$$

Now,

$$Ee^{v\rho(t)} = \prod_{p\le x} \mathrm{ch}\left(\frac{v\cos(t\log p)}{\sqrt{p}}\,(1-p^{1/2-\sigma})\right) \prod_{p>x} \mathrm{ch}\left(\frac{v\cos(t\log p)}{p^{\sigma}}\right)$$

$$\le e^{\frac{v^2}{2}\sum_{p\le x}\frac{(1-p^{1/2-\sigma})^2}{p} + \frac{v^2}{2}\sum_{p>x}\frac{1}{p^{2\sigma}}}.$$

The first sum is, for $\sigma = 1/2 + 1/\log x$,

$$\le (\sigma-1/2)^2 \sum_{p\le x}\frac{\log^2 p}{p} \le c_{30},$$

and the second, using only a bounded remainder in (21)

$$= \int_x^{\infty} u^{1-2\sigma}\, dh(u) = \int_x^{\infty} \frac{du}{u^{2\sigma}\log u} + O(1) = \int_2^{\infty} \frac{e^{-u}}{u}\, du + O(1) \le c_{31}.$$

We deduce

$$E\int_1^2 e^{v\rho(t)}dt \le e^{(c_{30}+c_{31})v^2/2}$$

and by Markov's inequality

$$\mathrm{Prob.}(|\{t : t\in[1,2],\ \rho(t)\ge M\}| > 1/\log x) \le \mathrm{Prob.}\left(\int_1^2 e^{v\rho(t)}dt \ge \frac{e^{vM}}{\log x}\right)$$

$$\le \log x\, e^{c_{32}v^2 - vM} = \frac{1}{\log x}$$

choosing $v = M/2c_{32}$ optimally and $M = \sqrt{8c_{32}L}$.

The sum of the probabilities $1/\log x = 1/\log y_k$ is finite and we see that almost surely for $x = y_k$ large enough the set where $\rho(t) \ge \sqrt{8\, c_{32}L}$ has measure $\le 1/\log x$. But (32) holds on a larger set (33) so that there exists a t satisfying both (32) and $\rho(t) < \sqrt{8\, c_{32}\, L}$ implying by the definition (34) of $\rho(t)$

$$\sum_p f(p)\,\frac{\cos(t\log p)}{p^{\sigma}} \ge L - \sqrt{29L\log L} - \sqrt{8\, c_{32}\, L}$$

contradicting (20) for $c_2 > 2\sqrt{29}$. The proof of Theorem, (ii) is concluded.

REFERENCES

[1] A. WINTNER. Random factorizations and Riemann's hypothesis, Duke Math. J. 11 (1944), 267-275.

[2] P. ERDÖS. Some unsolved problems, Magyar Tu. Akad. Mat. Kut. Int. Közl. 6 (1961), 221-254.

[3] A. BONAMI. Etude des coefficients de Fourier des fonctions de $L^p(G)$, Annales de l'Institut Fourier de l'Université de Grenoble, XX, 2 (1970), 335-402.

[4] G. HALASZ and L. CARLESON. On an integral equation, Techn. Report, Mittag-Leffler Institut (1978), n° 10.

[5] G. HALASZ. On a result of Salem and Zygmund concerning random polynomials, Studia Sci. Math. Hung. 8 (1973), 369-377.

G. HALASZ

BUDAPEST

HONGRIE

WEIGHTED SIEVES

H. HALBERSTAM and H.-E. RICHERT

1. Introduction Let $\mathscr{A}$ be a finite integer sequence and $\mathscr{P}$ a set of primes. Following the notation of [4], let $\mathscr{A}_d = \{a \in \mathscr{A}: a \equiv 0 \bmod d\}$, so that $\mathscr{A}_1 = \mathscr{A}$; and write

$$P(z) = \prod_{\substack{p<z \\ p\in\mathscr{P}}} p, \qquad P(z_1,z) = P(z)/P(z_1) = \prod_{\substack{z_1\le p<z \\ p\in\mathscr{P}}} p \qquad (2 \le z_1 \le z).$$

The classical sifting function

$$S(\mathscr{A}, \mathscr{P}, z) = |\{a \in \mathscr{A}: (a, P(z)) = 1\}|$$

has been intensively studied and much is known about it for a wide range of sieve problems. Later we shall need to recall some of this information.

If $S(\mathscr{A}, \mathscr{P}, z)$ is large then $\mathscr{A}$ contains many elements all of whose prime factors from $\mathscr{P}$ are at least as large as z; if $\mathscr{P}$ has been properly chosen this may allow us to infer that $\mathscr{A}$ contains many elements having few prime factors. However, if <u>this</u> is the kind of result we want, then experience has shown that we do better with a <u>weighted</u> sifting function of type

$$H(\mathscr{A}, \mathscr{P}, z_1, z_2) = \sum_{\substack{a\in\mathscr{A} \\ (a,P(z_1))=1}} \gamma((a, P(z_1,z_2)))$$

where $\gamma(n) \le 1$ always and $\gamma(n)$ is so chosen that at $n = (a, P(z_1,z_2))$, $\gamma(n) > 0$ implies that a has few prime factors from $\mathscr{P}$ between z_1 and z_2.

Since any a counted in H has no prime factors from $\mathscr{P}$ below z_1, an inequality showing H to be large again leads, indirectly, to the conclusion that $\mathscr{A}$ has many elements having few prime factors (again, provided that $\mathscr{P}$ has been properly chosen); but now we often attain better results because, roughly speaking, we may take z_2 larger when estimating H from below than z when working with S. The study of weighted sieves, though hardly new, is still at rather an experimental stage. First of all, we do not know how to construct optimal weights γ; neither have we found the best way to estimate the associated H from below. (Of course, these two problems are closely connected; but later we shall

see that one may have a 'good' weight and still not be sure of the best way of dealing with H.)

When it comes to interpreting arithmetically what it means for H to be large it is important to know that we may assume any a counted in H with a positive weight to be squarefree with respect to the primes (of $\mathscr{P}$) between z_1 and z_2. In practice it is usually possible (though not necessarily trivial) to show that

$$\sum_{\substack{z_1 \le p < z_2 \\ p \in \mathscr{P}}} \sum_{\substack{a \in \mathscr{A} \\ a \equiv 0 \bmod p^2}} 1$$

is small compared with H, so that we shall make this assumption here. And while we introduce one assumption we may as well take the opportunity to introduce several others; for, while generality is one of the hallmarks of sieve theory, we have necessarily to impose some restrictions on $\mathscr{A}$ and $\mathscr{P}$.

Let X be a convenient approximation to $|\mathscr{A}|$, and for each $p \in \mathscr{P}$ let $\omega(p)/p$ $(0 \le \omega(p) < p)$ be the "probability" that p divides an element of $\mathscr{A}$ in the sense that $\frac{\omega(p)}{p} X$ approximates $|\mathscr{A}_p|$. We let $\omega(p) = 0$ if $p \notin \mathscr{P}$ (normally the right way to choose $\mathscr{P}$ is to require that no prime from the complement of $\mathscr{P}$ can ever divide an element of $\mathscr{A}$) and assume that $\omega(p)$ is, on average over $\mathscr{P}$, 1 (in some weak sense - cf. condition $\Omega_2(1,A)$ of [4] with $A \ge 1$ a constant for simplicity; and see F/N connected with (4.15) below.) We form the multiplicative function $\omega(d) = \prod_{p|d} \omega(p)$ on the squarefree integers d, and we assume the "events" {a in $\mathscr{A}$ is divisible by p in $\mathscr{P}$} to be "quasi-independent" in that the remainders

$$R_d = |\mathscr{A}_d| - \frac{\omega(d)}{d} X \tag{1.1}$$

are small on average (in some precise sense) over divisors d of $P(z_2)$ that

are less than y (see (4.4) below). This y is our basic parameter. We suppose it to be large, and write

$$\max_{a\in\mathcal{A}} |a| \le y^g .$$

Finally (for the present!) let

$$V(z) = \prod_{p<z} (1 - \frac{\omega(p)}{p}),$$

and use $\nu(n)$, $\Omega(n)$ to denote respectively the number of distinct prime factors of n and the number of prime factors of n counted according to multiplicity.

We shall now sketch the first and simplest weighted sieve, invented by Kuhn. Let b be a positive integer and

$$\gamma(n) = 1 - \frac{1}{b+1} \sum_{p|n} 1$$

Then $\gamma(n) \le 1$ always and $\gamma(n) > 0$ implies for squarefree n that n has at most b prime factors. Suppose we want to sift out $\mathbf{P}_r$'s in $\mathcal{A}$, with $r \ge 2$.

Write

$$z_1 = y^V , \quad z_2 = y^U$$

where

$$U > \max(V, \frac{g}{r+1}).$$

Let $a \in \mathcal{A}$ have $\gamma((a, P(y^V,y^U))) > 0$ and be counted in $H(\mathcal{A}, \mathcal{P}, y^V,y^U)$; also, remember that a is squarefree with respect to the primes of $\mathcal{P}$ between y^V, y^U by assumption. If a has ℓ such prime factors between y^V and y^U , and if $\Omega(a) \ge r+1$,

then

$$y^g > |a| \ge y^{\ell V+(r+1-\ell)U} = y^{(r+1)U-\ell(U-V)} \ge y^{(r+1)U-b(U-V)}$$

and this is impossible if $(r+1)U - b(U-V) \ge g$, that is, if we take

$$b = [\frac{(r+1)U - g}{U-V}] .$$

With this choice of b, therefore, we may conclude that $\Omega(a) \le r$ whenever $\gamma((a, P(y^V, y^U))) > 0$; and the latter must hold for some $a \in \mathcal{A}$, indeed for many a's, if we can show that, for some admissible choice of parameters,

$$H(\mathcal{A}, \mathcal{P}, y^V, y^U) \gg XV(y).$$

Finally, to arrive at such an inequality we observe that

$$H = S(\mathcal{A}, \mathcal{P}, y^V) - \frac{1}{b+1} \sum_{y^V \le p < y^U} S(\mathcal{A}_p, \mathcal{P}, y^V)$$

and we then apply classical S-theory to estimate H from below.

2. Logarithmic weights

A choice of γ that is always superior to Kuhn's is

$$\gamma(n) = 1 - \frac{1}{(r+1)U-g} \sum_{p \mid n} (U - \frac{\log p}{\log y})$$

first proposed by Ankeny and developed in Richert [7]. Here, if $(a, P(y^V)) = 1$ and $\Omega(a) \ge r+1$,

$$\gamma((a,P(y^V,y^U))) \le \frac{1}{(r+1)U-g} \left\{ (r+1)U-g-\sum_{p \mid a} (U - \frac{\log p}{\log y}) \right\}$$

$$\le \frac{1}{(r+1)U-g} \left\{ (r+1)U - g - U\Omega(a) + \frac{\log |a|}{\log y} \right\} \le 0$$

so that $\gamma((a, P(y^V,y^U))) > 0$ implies that $\Omega(a) \le r$. Moreover, here

$$H(\mathcal{A}, \mathcal{P}, y^V, y^U) = S(\mathcal{A}, \mathcal{P}, y^V) - \frac{1}{(r+1)U-g} \sum_{y^V \le p < y^U} (U - \frac{\log p}{\log y}) S(\mathcal{A}_p, \mathcal{P}, y^V)$$

and so may be estimated from below, as in the Kuhn case, by classical S-theory.

A defect of both these weights is that the corresponding H-sums do contain negative weights. In Halberstam, Heath-Brown and Richert [3] we introduced therefore the modified logarithmic weight

$$\gamma(n) = \{1 - \frac{1}{(r+1)U-g} \sum_{p \mid n} (U - \frac{\log p}{\log y})\}^+ ,$$

where

$$\{x\}^+ = \max(x,0)$$

and we managed to analyse the associated H in terms of S-functions. The general theory of this weighted sieve still needs to be worked out, but for P_2's in short intervals we obtained good results.

However, there is a second defect, even in this improved approach, arising from the analysis in terms of S-functions: we estimate those appearing with a positive sign from below and those with a negative sign from above, extreme measures that a prior cancellation or smoothing might conceivably avoid. Putting this in more radical form, we might ask whether there is not, for each weighted sieve function H, a lower bound theory analogous to that for S. In two important papers [1] and [2] Greaves has had some success in this direction; and in this paper we sketch an improved as well as more versatile weighted sieve of Greaves' type.

3. A new weighted sieve

Introduce, in addition to U and V, two further parameters E and T, such that $E \le V$ and $U \le T$; more precisely, put

$$E_0 = \max(E, \tfrac{1}{3}(1-T)) \tag{3.1}$$

and require that

$$E_0 \le V \le \tfrac{1}{4}, \quad \tfrac{1}{2} \le U \le T < 1, \tag{3.2}$$

also that

$$U + 3V \ge 1. \tag{3.3}$$

Eventually, in an application, all these parameters have numerical values; but for the theoretical calculations beforehand it is important to insist that V is positive and bounded away from zero. Define*, for $p \in \mathscr{P}$,

---

*When $E_0 = E$, $w(p)$ has, at least for $p \ge y^V$, the more familiar look

$$1 - w(p) = \frac{1}{T-E}\left(T - \frac{\log p}{\log y}\right).$$

$$w(p) = \begin{cases} \frac{1}{T-E}\left(\frac{\log p}{\log y} - E\right), & y^{\frac{1}{4}} \le p < y^U, \\ \frac{1}{T-E}\left(\frac{\log p}{\log y} - E_0\right), & y^V \le p < y^{\frac{1}{4}}, \\ 0, & p < y^V. \end{cases} \tag{3.4}$$

Note that, by (3.2), $0 \le w(p) < 1$ always. We have defined $w(p)$ on $\mathcal{P}$ for $p < y^U$ only, but it is in order, or course, if we wish, to extend it to $p < y^T$. Indeed, this can strengthen our method in at least one respect, as we shall point out presently. But first, define

$$\gamma(n) = \{1 - \sum_{\substack{p \mid n \\ p \in \mathcal{P}}} (1 - w(p))\}^+ \tag{3.5}$$

and observe that, by (3.4), $\gamma(n) = 0$ unless $(n, P(y^V)) = 1$. Hence we may write the weighted sifting function H more simply in the form

$$H(\mathcal{A}, \mathcal{P}, y^V, z) = \sum_{a \in \mathcal{A}} \gamma((a, P(z))), \quad y^V < z \le y^T \tag{3.6}$$

Since

$$\{x_1 - x_1\}^+ \ge \{x_1\}^+ - \{x_2\}^+ ,$$

we have

$$\begin{aligned} H(\mathcal{A}, \mathcal{P}, y^V, y^T) &\ge H(\mathcal{A}, \mathcal{P}, y^V, y^U) - \sum_{a \in \mathcal{A}} \sum_{\substack{p \mid a \\ (a, P(y^V))=1, \; y^U \le p < y^T}} (1 - w(p)) \\ &= H(\mathcal{A}, \mathcal{P}, y^V, y^U) - \sum_{y^U \le p < y^T} (1 - w(p))\, S(\mathcal{A}_p, \mathcal{P}, y^V). \end{aligned} \tag{3.7}$$

Inequality (3.7) transfers the basic combinatorial idea of Iwaniec-Laborde [6] to our new configuration; but we shall make no use of this innovation in the present account. Let it be said that our definition of $w(p)$ follows Greaves [1] closely but involves two new parameters as well as a new sifting function and in this way affords us greater flexibility.

Suppose for the moment that we can prove that

$$H(\mathcal{A}, \mathcal{P}, y^V, y^T) > 0. \tag{3.8}$$

What does this mean arithmetically? To simplify matters suppose here that $T = U$. By (3.8) there exists an element $a \in \mathcal{A}$, necessarily coprime with

$P(y^V)$, such that

$$0 < \{1 - \sum_{p|a, p<y^T} (1 - w(p))\}^+ . \tag{3.9}$$

Since $E \leqslant E_o$, we have, by (3.4),

$$1 - w(p) \geq \frac{1}{T-E} (T - \frac{\log p}{\log y}), \quad y^V \leq p < y^T,$$

and we note that $T - \frac{\log p}{\log y} \leq 0$ for $p \geqslant y^T$. Then, by (3.9),

$$\begin{aligned} 0 < T-E - \sum_{\substack{p|a \\ p<y^T}} (T - \frac{\log p}{\log y}) &\leqq T-E - \sum_{p|a} (T - \frac{\log p}{\log y}) \\ &\leq T-E - T\Omega(a) + \frac{\log |a|}{\log y} \\ &\leq T-E - T\Omega(a) + g, \end{aligned}$$

so that

$$\Omega(a) < 1 + \frac{g-E}{T} .$$

Hence, if

$$g \leq rT + E, \tag{3.10}$$

(3.9) implies that $\Omega(a) \leq r$.

Our main problem is to prove (3.8) or something better. For this purpose write (note that our W differs from Greaves')

$$W(d) = \sum_{t|d} \mu(t)\, \gamma(t), \qquad d|P(y^U), \tag{3.11}$$

so that, by Moebius inversion.

$$\gamma(n) = \sum_{d|n} \mu(d)\, W(d), \qquad n|P(y^U),$$

and so H may be re-written in the form

$$H(\mathcal{A}, \mathcal{P}, y^V, y^U) = \sum_{d|P(y^U)} \mu(d)\, W(d)\, |\mathcal{A}_d| \tag{3.12}$$

This will be our starting point; but first we introduce some other convenient notations. Let

$$H_q(\mathcal{A}, \mathcal{P}, y^V, z) = \sum_{d|P(z)} \mu(d) W(qd)\, |\mathcal{A}_{qd}|, \qquad (q, P(z)) = 1, \tag{3.13}$$

so that $H_1(\mathcal{A}, \mathcal{P}, y^V, z) = H(\mathcal{A}, \mathcal{P}, y^V, z)$. Then

$$H_q(\mathcal{A}, \mathcal{P}, y^V, z) = \sum_{a \in \mathcal{A}_q} \gamma_q((a, P(z))), \qquad (q, P(z)) = 1, \tag{3.14}$$

where

$$\gamma_q(n) = \sum_{d|n} \mu(d)W(qd), \quad \gamma_1(n) = \gamma(n). \tag{3.15}$$

Let $p(n)$ and $q(n)$ denote respectively the least and largest prime factors of $n > 1$, and put $p(1) = \infty$, $q(1) = 1$. On the set of positive divisors of $P(y^U)$ introduce an arithmetic function $\chi(.)$, requiring at this stage only that $\chi(1) = 1$; and define

$$\chi(1) = 0, \quad \bar{\chi}(n) = \chi(\tfrac{n}{p(n)}) - \chi(n) \quad \text{if} \quad n > 1.$$

It is easy to verify that

$$1 = \chi(d) + \sum_{\substack{t|d \\ q(d/t)<p(t)}} \bar{\chi}(t) \tag{3.16}$$

and from this we readily derive the important identity

$$\sum_{d|P(z)} \mu(d)\phi(d) = \sum_{d|P(z)} \mu(d)\chi(d)\phi(d) + \sum_{d|P(z)} \mu(d)\bar{\chi}(d) \sum_{t|P(p(d))} \mu(t)\phi(dt) \tag{3.17}$$

valid for any arithmetic function $\phi(.)$. Applying this identity in (3.12), with $z = y^U$ and $\phi(d) = W(d)|\mathscr{A}_d|$, we obtain

$$H(\mathscr{A}, \mathscr{P}, y^V, y^U) = \sum_{d|P(y^U)} \mu(d)\chi(d)W(d)|\mathscr{A}_d| + \sum_{d|P(y^U)} \mu(d)\bar{\chi}(d)\, H_d(\mathscr{A}, \mathscr{P}, p(d)). \tag{3.18}$$

Lemma 1 Suppose that $d|P(y^U)$ and that $n|P(p(d))$. Then

$$\gamma_d(n) \geq 0 \quad \text{if} \quad \nu(d) = 2 ; \tag{3.19}$$

and

$$\gamma_d(n) = \begin{cases} 1 - \sum_{p|d} w(p) \geq 0, & n = 1, \\ w(p), & n = p, \\ 0, & \nu(n) \geq 2, \end{cases} \qquad \text{if} \quad \nu(d) > 2 \tag{3.20}$$

provided that

$$d < y, \quad q(d/q(d))^3\, q(d) < y. \tag{3.21}$$

In particular, by (3.14), $H_d(\mathscr{A}, \mathscr{P}, y^V, (p(d)) \geq 0$ for every $d|P(y^U)$ with $\nu(d) \geq 2$ that satisfies (3.21).

We shall not prove this result here; but as some indication of its line of reasoning let us prove (what is implicit in the proof of the Lemma) that

$$W(d) = 1 - \sum_{p|d} w(p), \quad d|P(y^U), \tag{3.22}$$

when d=1, d is prime or, if $\nu(d) \geq 2$, when d satisfies (the second inequality in) (3.21). We do, in any case, require this result. We argue as follows:

By (3.11) and (3.5), $W(1) = \gamma(1) = 1$ and $W(p) = 1 - \gamma(p) = 1 - w(p)$. Now suppose $\nu(d) \geq 2$ and put $d = p_1 p_2 \cdots p_\nu$ $(p_1 > p_2 > \ldots > p_\nu)$; then, according to (3.21), $p_2^3 p_1 < y$. Hence $p_2 < y^{\frac{1}{4}}$ (so that only $p_1 \geq y^{\frac{1}{4}}$ is possible) and $p_1 p_2 < y^{\frac{1}{3}(1+2U)} \leq y^{\frac{1}{3}(1+2T)}$. It follows from (3.4) that

$$w(p_1) + w(p_2) \geq \frac{1}{T-E}\left(\frac{\log p_1 p_2}{\log y} - E - E_0\right) < 1$$

since, by (3.1), $T + 3E_0 \geq 1$; and this tells us that $\gamma(p_1 p_2) = \{w(p_1) + w(p_2) - 1\}^+ = 0$ by (3.5). But (3.5) implies also that if $t|d$ then $\gamma(d) \leq \gamma(t)$. In particular, $\gamma(d) \leq \gamma(p_1 p_2) = 0$, so that $\gamma(d) = 0$. Furthermore, if $t|d$ and $\nu(t) \geq 2$, then t also satisfies (3.21) and therefore $\gamma(t) = 0$. Hence the only t's contributing in (3.11) are $t = 1$ and the prime values of t; and this proves (3.22) under the given conditions.

Lemma 1 and the subsequent argument imply that

$$H(\mathcal{A}, \mathcal{P}, y^V, y^U) \geq \sum_{d|P(y^U)} \mu(d)\chi(d) |\mathcal{A}_d| \left(1 - \sum_{p|d} w(p)\right) \tag{3.23}$$

provided that

$$d|P(y^U), \quad \chi(d) \neq 0, \quad \nu(d) \geq 2 \Rightarrow (3.21), \tag{3.24}$$

and

$$\mu(d)\,\bar{\chi}(d)\begin{cases} = 0, & \mu(d) = -1, \\ \geq 0, & \mu(d) = 1, \end{cases} \quad d \mid P(y^U) \; ; \tag{3.25}$$

and these two requirements are satisfied if χ is chosen from the Rosser-Iwaniec upper sieve.

Introduce the arithmetic functions $\chi_y^{\pm}(\cdot)$: Let $\chi_y^{\pm}(1) = 1$, and if $n = p_1 \cdots p_\nu$ $(p_1 > \ldots > p_\nu, \nu \geq 1)$ let

$$\chi_y^{\pm}(n) = \eta_y^{\pm}(p_1)\,\eta_y^{\pm}(p_1p_2)\cdots\,\eta_y^{\pm}(p_1p_2\cdots p_\nu) \tag{3.26}$$

where

$$\eta_y^{+}(m) = \begin{cases} 1, & \nu(m) \text{ even} \\ 1, & \nu(m) \text{ odd } \&\; p^2(m)m < y, \\ 0, & \text{otherwise} \end{cases} \qquad \eta_y^{-}(m) = \begin{cases} 1, & \nu(m) \text{ odd} \\ 1, & \nu(m) \text{ even } \&\; p^2(m)m < y \\ 0, & \text{otherwise.} \end{cases} \tag{3.27}$$

Then (3.23) holds with $\chi = \chi_y^-$, for (cf (3.25))

$$\mu(d)\bar{\chi}_y^-(d) = \mu(d)\chi_y^-\left(\frac{d}{p(d)}\right)(1 - \eta_y^-(d)) = \begin{cases} 0, & \nu(d) \text{ odd} \\ 0, & \nu(d) \text{ even } \&\; p^2(d)d < y \\ \chi_y^-(d/p(d)), & \nu(d) \text{ even } \&\; p^2(d)d \geq y. \end{cases}$$

Also, if $d \mid P(y^U)$ and $\nu(d) \geq 2$, then $\chi_y^-(d) \neq 0$ implies that $\chi_y^-(d) = 1$; writing $d = p_1 \cdots p_\nu$ $(p_1) > \ldots > p_\nu, \nu \geq 2)$, this means that $\eta_y^-(p_1p_2) = 1$, i.e. that $p_2^3 p_1 < y$, and that $\eta_y^-(p_1p_2\cdots p_{2[\nu/2]}) = 1$. When ν is even $p_\nu^3 p_{\nu-1}\cdots p_1 < y$ clearly implies $d < y$, and when ν is odd $p_{\nu-1}^3 p_{\nu-2}\cdots p_1 < y$ leads to $d < y$ too. Thus we have arrived at the important inequality

$$H(\mathcal{A},\mathcal{P},y^V,y^U) \geq \sum_{d \mid P(y^U)} \mu(d)\chi_y^-(d)\,|\mathcal{A}_d|\,\left(1 - \sum_{p \mid d} w(p)\right) \tag{3.28}$$

by following closely the model of the Rosser-Iwaniec treatment of $S(\mathcal{A},\mathcal{P},z)$. There is one respect in which we probably fail to match the success of that model: in going from (3.18) (with $\chi = \chi_y^-$) to (3.28) we have discarded some non-negative terms and it may be that in so doing we have omitted a worthwhile positive contribution to H.

4. The inequality (3.28)

By (1.1), inequality (3.28) implies that

$$H(\mathcal{A},\mathcal{P},y^V,y^U) \geq XG(\mathcal{A},\mathcal{P},y^V,y^U) + R(\mathcal{A},\mathcal{P},y^V,y^U) = XG + R, \tag{4.1}$$

where

$$G = G(\mathcal{A},\mathcal{P},y^V,y^U) = \sum_{d\mid P(y^U)} \mu(d)\chi_y^-(d)\,\frac{\omega(d)}{d}\quad (1 - \sum_{p\mid d} w(p)). \tag{4.2}$$

and

$$R = R(\mathcal{A},\mathcal{P},y^V,y^U) = \sum_{d\mid P(y^U)} \mu(d)\chi_y^-(d)R_d\quad (1 - \sum_{p\mid d} w(p)). \tag{4.3}$$

The remainder sum can, in favorable circumstances, be analysed with greater precision, but in this exposition we note merely that

$$|R| \leq \sum_{\substack{d\mid P(y^U)\\ d<y}} |R_d|\ , \tag{4.4}$$

and that, with the right choice of y, R will play the role of an error term. Our main business is with G. Write

$$T^{\pm}(x,z) = \sum_{d\mid P(z)} \mu(d)\chi_x^{\pm}(d)\,\frac{\omega(d)}{d}\ , \tag{4.5}$$

sums familiar from Rosser-Iwaniec theory. Then

$$G = T^-(y,y^U) - \sum_{p<y^U} w(p) \sum_{\substack{d\mid P(y^U)\\ p\mid d}} \mu(d)\chi_y^-(d)\,\frac{\omega(d)}{d}\ . \tag{4.6}$$

In the second sum write d uniquely in the form $d = d_2pd_1$, where $d_2\mid P(p)$ and $d_1\mid P(p^+, y^U)$ (p^+ being the successor of p in $\mathcal{P}$); and observe that

$$\chi_y^-(d) = \chi_y^-(d_1)\chi_{y/d_1}^{(-)^{\nu(d_1)+1}}(pd_2) = \chi_y^-(d_1)\eta_{y/d_1}^{(-)^{\nu(d_1)+1}}(p)\,\chi_{y/(pd_1)}^{(-)^{\nu(d_1)}}(d_2).$$

Then

$$G = T^-(y,y^U) + \sum_{p<y^U} w(p)\,\frac{\omega(p)}{p} \sum_{d\mid P(p^+,y^U)} \mu(d)\eta_{y/d}^{(-)^{\nu(d)+1}}(p)\,\chi_y^-(d)\,\frac{\omega(d)}{d}\,T^{(-)^{\nu(d)}}(\tfrac{y}{pd},p); \tag{4.7}$$

in the double sum on the right, when $d > 1$ we deduce from $\eta_{y/d}^{(-)^{\nu(d)+1}}(p)\chi_y^-(d) = 1$

that, necessarily, $p < y^{1/4}$ (more precisely, we deduce $p^3 d < y$ when $\nu(d)$ is odd and $p(d)^2 d < y$ when $\nu(d)$ is even). The analysis of G in terms of the functions $T^{\pm}$ allows us to use known information about them. First of all, there is the Buchstab identity

$$T^{+}(x,z_2) = T^{\pm}(x,z_1) - \sum_{z_1 \le p < z_2} \frac{\omega(p)}{p} T^{\mp}(\tfrac{x}{p},p), \qquad 2 \le z_1 \le z_2, \tag{4.8}$$

with the additional condition $p^3 < x$ in the '+' case, and then we have (Iwaniec [5]), for $x \ge z \ge 2$,

$$T^{+}(x,z) = V(z)\{F(\tfrac{\log x}{\log z}) + O(\log^{-\frac{1}{3}} x)\}, \tag{4.9}$$

$$T^{-}(x,z) = V(z)\{f(\tfrac{\log x}{\log z}) + O(\log^{-\frac{1}{3}} x)\}, \tag{4.10}$$

where

$$F(s) = \frac{2e^{\gamma}}{s} \ (0 < s \le 3), \qquad f(s) = \begin{cases} 0, & s \le 2, \\ \frac{2e^{\gamma}}{s}\log(s-1), & 2 \le s \le 4, \end{cases} \tag{4.11}$$

and

$$\begin{cases} sF(s) - s_o F(s_o) = \int_{s_o}^{s} f(t-1)dt, \\ sf(s) - s_o f(s_o) = \int_{s_o}^{s} F(t-1)dt, \end{cases} \qquad 2 \le s_o \le s, \tag{4.12}$$

where the first formula in (4.12) is true even for $s_0 \ge 1$. Apply (4.8) (with $x = y$, $z_1 = y^{\frac{1}{4}}$; $z_2 = y^U$) to the first term on the right of (4.7), and in the second sum use the remark immediately following (4.7). We obtain at once

$$G = T^{-}(y,y^{\frac{1}{4}}) - \sum_{y^{\frac{1}{4}} \le p < y^U} (1-w(p)) \frac{\omega(p)}{p} T^{+}(\tfrac{y}{p}, p) + G_o, \tag{4.13}$$

say, where

$$G_o = \sum_{y^V \le p < y^{\frac{1}{4}}} w(p) \frac{\omega(p)}{p} \sum_{d \mid P(p^+, y^U)} \mu(d)\, \eta_{y/d}^{(-)^{\nu(d)+1}}(p) \chi_y^{-}(d) \frac{\omega(d)}{d} T^{(-)^{\nu(d)}}(\tfrac{y}{pd}, p). \tag{4.14}$$

Apply (4.8) again, this time with $z_1 = x^{1/3}$: we see by (4.10) and (4.11) that $T^+(x,z_2)$ and $T^+(x,x^{1/3})$ are approximately equal if $z_2 \geq x^{1/3}$. Writing[†]

$$\sigma^+(x) = T^+(x,x^{\frac{1}{3}}) = V(x)\{2e^{\gamma} + O(\log^{-\frac{1}{3}} x)\} \tag{4.15}$$

by (4.9) and (4.11), we derive from (4.13) that

$$G = T^-(y,y^{\frac{1}{4}}) - \sum_{y^{\frac{1}{4}} \leq p < y^U} (1-w(p)) \frac{\omega(p)}{p} \sigma^+(\tfrac{y}{p}) + G_o + O((\log y)^{-\frac{1}{3}}) \tag{4.16}$$

since $p \geq (y/p)^{1/3}$ in the second expression on the right of (4.13).

The asymptotic formulae (4.9) and (4.10) may be applied in the expression for G_0, (4.14), since $y/(pd) > p$ in each term (see again the remark following (4.7)), but this will lead to little progress in itself because F and f are known explicitly only for small values of ξ (cf. (4.11)). Fortunately the functions $T^{\pm}$ may be expressed in terms of functions σ^+ by means of the following

LEMMA 2 (REDUCTION LEMMA): Suppose that

$$\frac{\log x}{\log z} \ll 1 ;$$

then

$$T^{(-)^\nu}(x,z) = \sum_{\substack{t \mid P(z,x) \\ q(t)\ x/t \\ \nu(t) \equiv \nu \bmod 2}} \frac{\omega(t)}{t} \sigma^+(\tfrac{x}{t}) + O(V(z)\log^{-\frac{1}{3}} z), \quad \nu = 0,\ 1,$$

provided that $x > 1$, $z \geq 2$ when $\nu = 0$, and $2 \leq \varkappa < x^{\frac{1}{2}}$ when $\nu = 1$.

[†] We use here and later that $V(z_1)/V(z_2) = (\log z_2/\log z_1)(1 + O(\frac{1}{\log z_1}))$, $2 \leq z_1 \leq z_2$, reflecting that $\omega(p)$ is 1 on average.

The proof depends on iterations of (4.8). In a continuous form this result occurs for the first time in an unpublished manuscript of Siebert, and is to be found also in Greaves [1].

We substitute from Lemma 2 in the expression (4.14) for G_0. To simplify the exposition we omit error terms from here on and indicate their hidden presence by means of the symbol $\cong$; details of all these calculations will, in any case, appear elsewhere. Then

$$G_o \cong \sum_{y^V \le p < y^{\frac{1}{4}}} w(p) \frac{\omega(p)}{p} \sum_{\substack{d \mid P(p^+, y^U) \\ \nu(d) \text{ odd} \Rightarrow p^3 d\, y}} \mu(d) \chi_y^-(d) \frac{\omega(d)}{d} \sum_{\substack{t \mid P(p^+, y/pd) \\ \nu(t) \equiv \nu(d) \bmod 2 \\ q(t)\, t < y/(pd)}} \frac{\omega(t)}{n} \sigma^+\left(\frac{y}{pdt}\right).$$

In the inner double sum the term corresponding to $d = t = 1$ is simply $\sigma^+(y/p)$, and the terms with $\gcd(d,t) > 1$ altogether contribute no more than an admissible error term. For the remaining terms with $\gcd(d,t) = 1$ write $dt = n$; we obtain, after careful combinations of summation conditions,

$$G_o \cong \sum_{y^V \le p < y^{\frac{1}{4}}} w(p) \frac{\omega(p)}{p} \{\sigma^+\left(\frac{y}{p}\right) + \sum_{\substack{1 < n \mid P(p^+, y^U) \\ \nu(n) \text{ even}}} \frac{\omega(n)}{n} \sigma^+\left(\frac{y}{pn}\right) \sum_{\substack{d \mid n \\ q(n/d) < y/(pn)}} \mu(d) \chi_y^-(d) \quad .$$

Here a curious and possibly significant result comes to our aid.

LEMMA 3. Suppose that $1 < n \mid P(p^+, y^U)$ and that $\nu(n)$ is even. Then

$$\sum_{\substack{d \mid n \\ q(n/d) < y/(pn)}} \mu(d) \chi_y^-(d) = \begin{cases} -\chi_y^-(n), & p(n) < y/(pn), \\ 0, & \text{otherwise.} \end{cases}$$

With this result to hand, we obtain

$$G_o \cong \sum_{y^V \le p < y^{\frac{1}{4}}} w(p) \frac{\omega(p)}{p} \{\sigma^+\left(\frac{y}{p}\right) - \sum_{\substack{1 < n \mid P(p^+, y^U) \\ p(n) < y/(pn) \\ \nu(n) \text{ even}}} \chi_y^-(n) \frac{\omega(n)}{n} \sigma^+\left(\frac{y}{pn}\right)\} \quad . \tag{4.17}$$

Combining (4.16) and (a precise version of) (4.17) we arrive at

$$G = T^-(y,y^{\frac14}) - \sum_{y^{\frac14}\le p<y^U} (1-w(p))\,\frac{\omega(p)}{p}\,\sigma^+(\tfrac{y}{p}) + \sum_{y^V\le p<y^{\frac14}} w(p)\,\frac{\omega(p)}{p}\,\sigma^+(\tfrac{y}{p})$$

$$- \sum_{y^V\le p<y^{\frac14}} w(p)\,\frac{\omega(p)}{p} \sum_{\substack{1<n\,|\,P(p^+,y^U)\\ p(n)<y/(pn)\\ \nu(n)\ \text{even}}} \bar\chi_y^-(n)\,\frac{\omega(n)}{n}\,\sigma^+(\tfrac{y}{pn}) + O(V(y)\log^{-\frac13} y). \tag{4.18}$$

Writing G_1 for the fourth expression on the right of (4.18), (4.10), (4.11) and (4.15) combined with straightforward Stieltjes integration yield

$$G = \frac{2e^\gamma V(y)}{T-E}\{T\log\tfrac1U + (1-T)\log\tfrac{1}{1-U} - \log\tfrac43 - E\log 3 + \int_V^{\frac14}(1-\tfrac{E_o}{x})\tfrac{dx}{1-x}\}$$

$$- G_1 + O(V(y)\log^{-\frac13} y). \tag{4.19}$$

We take a closer look at G_1. Suppose $\nu(n) = 2k$, $k \ge 1$. The conditions $y^V \le p$, $p(n) < y/(pn)$, $\nu(n) = 2k$ together imply that $q(n)p^{2k+1} < y$, that is, $q(n) < y^{1-(2k+1)V} \le y^{1-3V}$, and this is a more stringent requirement than $q(n) < y^U$, in view of (3.3). Hence

$$G_1 = \sum_{y^V\le p<y^{\frac14}} w(p)\,\frac{\omega(p)}{p} \sum_{k\ge1} \sum_{\substack{p<p(n)<y/(pn)\\ \nu(n)=2k}} \mu^2(n)\,\bar\chi_y^-(n)\,\frac{\omega(n)}{n}\,\sigma^+(\tfrac{y}{pn})\ ;$$

and the same argument shows that, actually,

$$k < \frac{1}{2V} - 1$$

in this summation. For example, if $V \ge \frac16$, there is only the term $k = 1$ in the sum over k, and if $V \ge \frac18$ there are only two terms, corresponding to $k = 1$ and 2. One can show by (4.15) and Stieltjes integration that

$$G_1 = \frac{2e^\gamma V(y)}{T-E}\{\int_V^{\frac14}(1-\tfrac{E_o}{x})\,h(x)dx + O(\tfrac{1}{\log y})\} \tag{4.20}$$

where

$$(4.21)\qquad h(x)=\sum_{k\geq 1} h_{2k}(x),\quad h_{2k}(x)=\int_{\substack{x<x_{2k}<\ldots<x_1\\ x_{2k}<1-x-x_1-\ldots-x_{2k}\\ 3x_{2i}+\ldots+x_1<1\ \forall i<k\\ 3x_{2k}+\ldots+x_1\geq 1}} \frac{dx_1\ldots dx_{2k}}{x_1\ldots x_{2k}}\ \frac{1}{1-x-x_1-\ldots-x_{2k}}\ .$$

Hence, by (4.19),

$$(4.22)\qquad G=\frac{2e^{\gamma}V(y)}{T-E}\left\{T\log\frac{1}{U}+(1-T)\log\frac{1}{1-U}-\log\frac{4}{3}-E\log 3+\int_V^{\frac14}\frac{x-E_o}{x}\psi(x)dx\right\}$$
$$+O(V(y)(\log y)^{-\frac13})$$

where

$$\psi(x)=\frac{1}{1-x}-h(x),\quad 0<x\leq\frac14,$$

and, according to Greaves [1], $\psi(x)$ is increasing and has a unique zero $V_0 = 0{\cdot}074\ 368\ \ldots\ (= 1/13{\cdot}446\ldots)$, so that

$$\psi(x)\geq 0\quad\text{for}\quad x\geq V_o\ .$$

Let

$$(4.23)\qquad \alpha(V)=\int_V^{\frac14}\psi(x)dx,\quad \beta(V)=\int_V^{\frac14}\psi(x)\frac{dx}{x}\ .$$

Greaves [1] carried out the difficult computation to show that

$$\alpha(V_o)=0.150\ 5528\ldots,\quad \beta(V_o)=0.876\ 95\ldots,$$

suggesting V_0 to be the optimal choice of V in his sieve. This is not always the case, especially when one works with our more flexible system of parameters and uses ancillary sieve devices such as the bilinear

form of R and/or the Iwaniec-Laborde extension (cf. (3.7)). For example, for P_2's in short intervals a value of V close to $1/6$ is better. Accordingly we record here the values

$$\alpha(\tfrac{1}{6}) = 0.098\ 580\ldots, \qquad \beta(\tfrac{1}{6}) = 0.474\ 533\ldots$$

and recall, in the light of an earlier remark, that

$$h(x) = h_2(x) = \frac{x}{1-x}\int_2^{\frac{1}{x}-2} \frac{\log(t-1)}{2-(t+2)x}\,dt, \quad \tfrac{1}{6} \leq x \leq \tfrac{1}{4}$$

Summing up, we have shown that

$$H(\mathscr{A},\mathscr{P},y^V,y^U) \geq \frac{2e^\gamma}{T-E}\,XV(y)\,\{T\log\frac{1}{U} + (1-T)\log\frac{1}{1-U} - (\log\tfrac{4}{3} - \alpha(V)) - E\log 3 - E_o\,\beta(V) + O((\log y)^{-\frac{1}{3}})\}$$

$$- \sum_{\substack{d\mid P(y^U)\\ d<y}} |R_d|,$$

subject to (3.1), (3.2) and (3.3), as well as $0 \leq \omega(p) < p$ and $\Omega_2(1,A)$.

Finally, we report that the preceding analysis can be extended to sieve problems of dimension κ, $\frac{1}{2} \leq \kappa \leq 1$; and that in the case $\kappa = 1$ it can be made to incorporate a bilinear form of R a la Iwaniec. Using the latter, we are able, for example, to obtain many new results concerning almost primes in short intervals. These results, as well as details of the preceding exposition, will be published elsewhere. A first paper will appear in the Proceedings of the Number Theory Colloquium held by the Banach Institute in Warsaw in the fall of 1982.

References

1. G. Greaves, A weighted sieve of Brun's type, Acta Arith. 40(1982), 297-332.

2. _____, Rosser's sieve with weights, Recent Progress in Analytic Number Theory, Vol. I, Academic Press, London, 1981, 61-68.

3. H. Halberstam, D. R. Heath-Brown & H.-E. Richert, Almost primes in short intervals, ibid, 69-102.

4. H. Halberstam and H.-E. Richert, Sieve Methods, Academic Press, London, 1974.

5. H. Iwaniec, Rosser's sieve, Acta Arith. 36(1980), 171-202.

6. H. Iwaniec & P. Laborde, P_2's in short intervals, Ann. Inst. Fourier (Grenoble), 31(1981), 37-56.

7. H.-E. Richert, Selberg's sieve with weights, Mathematica 16(1969), 1-22.

Mathematics department
University of Illinois
Urbana, Illinois, USA

Mathematics Department
University of Ulm
Ulm, West Germany

SPIRALES

M. MENDES FRANCE

§ 1. INTRODUCTION.

Ce texte est un compte-rendu d'un travail fait conjointement avec Y. Dupain et C. Tricot et dont le détail paraîtra ultérieurement [3].

La spirale exponentielle $\rho = e^{-\theta}$ évoque la croissance biologique alors que la spirale $\rho = (\log(2+\theta))^{-1}$ évoque plutôt les tourbillons de von Karman dans les fluides turbulents. La première est liée à la notion d'ordre et la seconde au désordre et à la complexité.

Suivant l'idée de B. Mandelbrot [6], nous mesurons la complexité par la dimension. Quelle dimension ? Nous discuterons deux d'entre elles, l'une bien connue, la dimension de Kolmogorov, l'autre qui nous est personnelle et que nous appelons la dimension de Steinhaus.

§ 2. DIMENSION DE KOLMOGOROV.

Soit E un ensemble borné dans $\mathbb{R}^2$. Soit $N(\varepsilon)$ le nombre minimal de boules de rayon $\varepsilon > 0$ nécessaires pour recouvrir E. Si E est un segment de droite, on voit que

$$N(\varepsilon) \asymp \frac{1}{\varepsilon} \quad \text{quand} \quad \varepsilon \searrow 0$$

et si E est un rectangle,

$$N(\varepsilon) \asymp \left(\frac{1}{\varepsilon}\right)^2 .$$

Les exposants 1 et 2 de ε^{-1} traduisent les dimensions respectives du segment et du rectangle. Cette remarque conduit à la définition suivante de la dimension de Kolmogorov :

$$\bar{d}_K(E) = \limsup_{\varepsilon \searrow 0} \frac{\log N(\varepsilon)}{\log \varepsilon^{-1}}$$

$$\underline{d}_K(E) = \liminf_{\varepsilon \searrow 0} \frac{\log N(\varepsilon)}{\log \varepsilon^{-1}} .$$

En cas d'égalité, on notera $d_K(E)$ la valeur commune.

Il est clair que

$$0 \le \underline{d}_K(E) \le \bar{d}_K(E) \le 2$$

et pour tout couple (α,β), $0 \le \alpha \le \beta \le 2$ il existe un ensemble E tel que $\underline{d}_K(E) = \alpha$, $\bar{d}_K(E) = \beta$.

Soit $\alpha > 0$. On définit les spirales S_α

$$\rho = (\theta+1)^{-\alpha} \quad (\theta > 0)$$

et $S_{\log}$

$$\rho = (\log(\theta+2))^{-1}.$$

Un calcul tout à fait élémentaire indique que

$$d_K(S_\alpha) = \max \{1, \frac{2}{1+\alpha}\}$$

$$d_K(S_{\log}) = 2.$$

(Méthode : remplacer la spirale par des cercles concentriques).

On voit en particulier que la spirale $S_{\log}$ a tendance à recouvrir un voisinage infiniment petit de l'origine.

§ 3. DIMENSION DE STEINHAUS.

Soit D une droite du plan x,y :

$$x \cos\theta + y \sin\theta - \rho = 0, \ \theta \in \mathbb{R}/2\pi\mathbb{Z} , \ \rho \in \mathbb{R}$$

où l'on a identifié les deux couples

$$(\rho,\theta) = (-\rho, \theta+\pi).$$

L'ensemble des droites est donc un ruban de Möbius M qu'on suppose muni de la mesure de Lebesgue $dD = d\rho d\theta$. (Je remercie R. Gay qui m'a indiqué la structure de Möbius de l'ensemble des droites).

Dans le plan x,y on se donne une courbe rectifiable Γ . Soit $\Omega(\Gamma) \subset M$ l'ensemble des droites D qui intersectent Γ et soit m_k la mesure de l'ensemble

$$M_k = \{D \in \Omega(\Gamma)/\text{card}(\Gamma \cap D) = k\} \quad (k = 1,2,3,\ldots).$$

Un théorème célèbre de Steinhaus [8], [9] énonce que

$$\sum_{k=1}^{\infty} k\, m_k = 2|\Gamma|$$

où $|\Gamma|$ représente la longueur de Γ, et que

$$\sum_{k=1}^{\infty} m_k = |\partial K|,$$

longueur de la frontière de l'enveloppe convexe de Γ.

Considérons maintenant une courbe plane Γ, bornée dans $\mathbb{R}^2$, localement rectifiable, de longueur infinie mais telle que $m_\infty = 0$. Pour une telle courbe,

$$\sum_{k=1}^{\infty} m_k < \infty$$

et

$$\sum_{k=1}^{\infty} k\, m_k = +\infty.$$

La première inégalité montre que $m_k \longrightarrow 0$. Il se peut qu'il existe un exposant α (nécessairement > 1) pour lequel

$$|\Gamma|^{(\alpha)} = \sum_{k=1}^{\infty} k(m_k)^{\alpha} < \infty.$$

(Exercice : Supposez que

$$m_k = \begin{cases} \nu^{-2} & \text{si } k = 2^{\nu},\ \nu = 0,1,2,\ldots \\ k^{-2} & \text{sinon.} \end{cases}$$

Alors la série $|\Gamma|^{(\alpha)}$ diverge pour tout $\alpha > 0$).

Le nombre

$$m_k = \int_{M_k} d\rho d\theta$$

est de dimension 1 au sens des physiciens ($d\theta$ est sans dimension et $d\rho$ est unidimensionnel). Donc, $(m_k)^{\alpha}$ et $|\Gamma|^{(\alpha)}$ sont de dimension α. Le nombre

$$d_S(\Gamma) = \inf\{\alpha > 1 \ / \ |\Gamma|^{(\alpha)} < \infty\}$$

s'appelle la dimension de Steinhaus de Γ. Si $|\Gamma|^{(\alpha)}$ diverge pour tout α, on pose $d_S(\Gamma) = +\infty$.

Ainsi, la dimension de Steinhaus d'une courbe est égale à 1 dès que Γ est de longueur finie.

On remarquera que $d_S(\Gamma)$, calculé à partir du nombre de points d'intersection de Γ avec une famille de droites mesure la "complexité" de Γ alors que $d_K(\Gamma)$ mesure ce qu'il semble naturel d'appeler la dimension.

La dimension de Steinhaus d'une spirale se calcule aisément. On trouve en particulier

$$d_S(S_\alpha) = \max \{1, \frac{2}{1+\alpha}\}$$
$$d_S(S_{log}) = 2$$

si bien que pour ces spirales, les dimensions de Kolmogorov et de Steinhaus coïncident. Ce résultat s'étend à une grande famille de spirales (voir [3]) :

THEOREME. *Soit* S_f *la spirale* $\rho = f(\theta)$ *où la fonction* f *est réelle, définie, continue pour* $\theta \geq 0$, *tendant vers* 0 *pour* θ *infini, convexe. Alors* $d_S(S_f) = \bar{d}_K(S_f)$.

Remarque 1. La condition entraîne l'inégalité

$$d_S(S_f) \leq 2.$$

Remarque 2. Outre les phénomènes de la nature (escargots, turbulence, spirales se rencontrent dans l'étude de la répartition modulo 1 liées aux sommes de Weyl. On consultera à ce propos les articles de Dekking, Mendes France [1], Deshouillers [2] et Lehmer [5].

REFERENCES

[1] F.M. DEKKING, M. MENDES FRANCE. Uniform distribution modulo one : a geometrical viewpoint. Jour. für die reine und angew. Mathem. 329, 1981, 143-153.

[2] J.M. DESHOUILLERS. Courbes associées aux sommes de Weyl.

[3] Y. DUPAIN, M. MENDES FRANCE, C. TRICOT. Dimension des spirales. A paraître.

[4] A.N. KOLMOGOROV, Y.M. TIHOMINOV. ε-entropy and ε-capacity of sets in functional spaces. Amer. Math. Soc. Translations 17, série 2, 1961, 277-364.

[5] D.H. LEHMER. Incomplete Gauss sums, Mathematika, 23, 1976, 125-135.

[6] B.B. MANDELBROT. Fractals, form, chance and dimension, Freeman 1977.

[7] M. MENDES FRANCE. Chaotic curves, Luminy symposium on Oscillations sept. 1981, édité par J. Demongeot, Springer-Verlag Lecture Notes in Biomathematics, à paraître.

[8] L. SANTALO. Integral geometry and geometric probability. Encyclopedia of Math. Addison Wesley 1976.

[9] H. STEINHAUS. Length, shape, area, Colloq. Math. 3, 1954, 1-13.

M. MENDES FRANCE
U.E.R. de Mathématique
Université Bordeaux I
351, Cours de la Libération

33405 TALENCE Cedex

L'ÉQUIRÉPARTITION DES VALEURS DE $\sigma_k(n)$.

W. NARKIEWICZ

On dit qu'une suite d'entiers $a_1, a_2, \ldots, a_n, \ldots$ est faiblement équirépartie modulo N si

1°. $\#\{n : (a_n, N) = 1\} = \infty$,

2°. $\forall\, j$ tel que $(j,N) = 1$,

$$\lim_{x\to\infty} \frac{\#\{n \le x : a_n \equiv j \pmod N\}}{\#\{n \le x : (a_n, N) = 1\}} = \frac{1}{\varphi(N)},$$

où φ est la fonction d'Euler.

Pour $k \ge 1$, soit $\sigma_k(n)$ la somme des puissances k-ièmes des diviseurs positifs de n.

En utilisant un critère d'équirépartition démontré par moi dans Acta Arithmetica 12 (1967), p. 269-279, J. Sliwa a montré que la suite $\{\sigma_1(n)\}$ est faiblement équirépartie modulo N si, et seulement si, N n'est pas divisible par 6. L'utilisation du même critère dans le cas général semblait difficile et ce n'est que récemment que l'on a obtenu des résultats difinitifs.

En 1980 Fomenko a observé que, pour chaque k, les valeurs de $\sigma_k(n)$ sont faiblement équirépartie modulo p pour tout nombre premier $p \ge p(k)$. Ce résultat est maintenant un cas particulier du théorème suivant (Litovskii Mat. Sbornik, 22, 1982, p. 135-145) :

Si f est une fonction multiplicative à valeurs entières telle que l'on ait, pour chaque p premier, $f(p) = V(p)$, où V est un polynôme qui n'est pas de la forme

$$V(x) = C\, V_1^k(x), \quad \text{avec} \quad V_1 \in \mathbb{Z}[X] \quad \text{et} \quad k \ge 2,$$

alors la suite $\{f(n)\}$ est faiblement équirépartie modulo N pour chaque N qui n'est divisible par aucun nombre premier appartenant à un certain ensemble fini $E(V)$.

Dans Journal für die reine und angewandte Mathematik, 323, 1981, p. 200-212, j'ai donné une méthode effective pour déterminer cet ensemble. Comme $\sigma_k(p) = 1+p^k$, on peut prendre $V(X) = 1 + X^k$ et ce théorème s'applique.

On peut poser le problème de déterminer l'ensemble $M(f)$ de tous les entiers N tels que la suite $\{f(n)\}$ soit faiblement équirépartie modulo N. Dans le cas général on ne connaît pas d'algorithme fini pour cela, mais, dans le cas de σ_k, la situation est meilleure. J'ai démontré l'existence d'un tel algorithme pour σ_k, où $k \geq 3$, dans un article qui doit paraître dans Acta Arithmetica.

L'utilisation de cet algorithme nécessite l'emploi d'un ordinateur, mais pour $k = 3$ on peut se débarasser de toute technique et on arrive à

$$M(\sigma_3) = \{N : 2 \nmid N \text{ et } 7 \nmid N\} \cup \{N : 2/N \text{ et } 3 \nmid N\}.$$

Le cas où $k = 2$ est plus compliqué, mais, avec F. Rayner, nous avons déterminé $M(\sigma_2)$ (Monatshefte für Mathematik, sous presse) :

$$M(\sigma_2) = \{N : 8 \nmid N,\ 12 \nmid N,\ 15 \nmid N,\ 28 \nmid N,\ 42 \nmid N,\ 66 \nmid N\}$$
$$\cup \{N : 40/N \text{ et, } \forall\ p \text{ premier} \geq 7 \text{ tel que } p/N,\ 2/\text{ordre}_p 4\ \}.$$

Comme on voit, la situation est ici beaucoup plus compliquée que pour $k = 3$.

J'ignore la structure de $M(\sigma_k)$ pour $k \geq 4$, mais, si k est un nombre premier, on peut montrer que la partie impaire de $M(\sigma_k)$ est

- soit l'ensemble de tous les entiers impairs (dans le cas où $k \equiv 1 \pmod 4$ ou bien $k \equiv 3 \pmod 4$ et $2k+1$ est un nombre composé),
- soit $\{N : 2 \nmid N \text{ et } 2k+1 \nmid N\}$ (dans le cas où $k \equiv 3 \pmod 4$ et $2k+1$ est premier).

C'est un résultat obtenu par E. Dobrowolski et moi-même et qui va paraître dans Colloquium Mathematicum.

Je termine en indiquant une conjecture de Rayner basée sur une expérimentation numérique :

Si k est un nombre premier impair et $2k+1$ est un nombre composé,

$$M(\sigma_k) = \{N : 6 \nmid N\}.$$

W. NARKIEWICZ
Wroclaw University, Mathematics
WROCLAW (Pologne)

AUTOUR DE FORMULES DUES À A. SELBERG

Jean-Louis NICOLAS

I. INTRODUCTION.

Désignons par $\Omega(n) = \sum_{p^a \| n} a$ le nombre de diviseurs de n comptés avec leur multiplicité. On définit :

$$\mathcal{N}(x,k) = \{n \leq x \mid \Omega(n) = k\}$$

$$N(x,k) = \text{Card}\,\mathcal{N}(x,k)$$

$$\mathcal{S}(x,k) = \{n \leq x \mid \Omega(n) \geq k\}$$

$$S(x,k) = \text{Card}\, S(x,k).$$

Dans tout cet article on écrira ℓ à la place de log log x.

En 1900, E. LANDAU a démontré comme corollaire du théorème des nombres premiers que, pour k fixé,

$$N(x,k) \sim \frac{x}{\log x} \frac{(\log\log x)^{k-1}}{(k-1)!} = \frac{x}{\log x} \frac{\ell^{k-1}}{(k-1)!}$$

(cf. [Lan], § 56) . Cette formule avait été conjecturée par Gauss (cf. [Ell], Introduction). En 1917, Hardy et Ramanujan dans leur célèbre mémoire "The normal number of prime factors of a number n" ont donné une majoration de $N(x,k)$ (cf. [Ram]).

En 1953, L.G. Sathe (cf. [Sat]) explicitait une fonction f telle que, pour $k \leq (2-\varepsilon)\ell$, on ait :

$$N(x,k) \sim f(k/\ell) \frac{\ell^{k-1}}{(k-1)!} \frac{x}{\log x}$$

étendant ainsi un résultat de P. Erdös qui avait considéré le cas $k-\ell = O(\sqrt{\ell})$; (cf. [Erd]).

A la suite de l'article de L.G. Sathe, A. Selberg démontrait la formule (cf. [Sel]) :

(1) $$\sum_{n\le x} z^{\Omega(n)} = xzF(z)(\log x)^{z-1} + O(x(\log x)^{\mathrm{Re}\, z-2}) \quad \text{où} \quad x \ge 2,$$

$$F(z) = \frac{1}{\Gamma(z+1)} \prod_p (1 - 1/p)^z (1 - z/p)^{-1}$$

est une fonction holomorphe dans $|z| < 2$, et où le "O" est uniforme dans tout disque $|z| \le R$, avec $R < 2$.

La formule (1) permettait à A. Selberg de retrouver le résultat de L.G. Sathe, et de préciser le comportement de $N(x,k)$ lorsque $(2-\varepsilon)\ell \le k \le B\ell$. Il signale notamment que

$$N(x,k) \sim C(x \log x)/2^k$$

pour $(2+\varepsilon)\ell \le k \le B\ell$, où B est un nombre réel arbitraire.

La formule (1) a été généralisée de plusieurs façons par H. Delange (cf. [Del]).

En 1978, G. Kolesnik et E.G. Strauss, ont donné (cf. [Kol]) une estimation asymptotique de $N(x,k)$ sous la forme d'une somme double, mais dont les termes sont difficilement comparables. P. Erdös et Sarközy ont démontré dans [Sar] :

$$S(x,k) = O((x \log x)k^4/2^k)$$

uniformément pour tout x et k. Et K. Norton (cf. [Nor 3]) a donné

$$S(x,k) = O((x \log x)\sqrt{\ell}/2^k)$$

ainsi que

$$S(x,k) >> (x \log x)2^{-k}(\varepsilon/\log\log\log x)^3$$

pour $2\ell - \sqrt{2\ell} \le k \le (1-\varepsilon)(\log x)/\log 2$ et x assez grand.

Nous démontrerons :

THEOREME. *Pour tout* $\varepsilon > 0$ *et pour tout* $\eta > 0$, *on a uniformément pour* $x \ge e$ *et* $(2+\varepsilon)\ell \le k \le (\log x)/\log 2 - \eta$

$$N(x,k) = C(x/2^k)\log(x/2^k)(1 + O(\log\log(3x/2^k))^{-1/4})$$

avec

$$C = (1/4)\prod_{p>2}(1 + 1/(p(p-2))) = 0{,}378694.$$

La démonstration du théorème repose sur la formule :

(2) $$N(x,k) = \sum_{m=0}^{k} N'(x/2^{k-m}, m)$$

où $N'(y,m) = \text{card}\{n \le y,\ n \text{ impair},\ \Omega(n) = m\}$.

La formule (2) s'obtient en regroupant les $n \in \mathcal{N}(x,k)$ qui sont divisibles exactement par la même puissance de 2.

On évalue ensuite $N'(y,m)$ grâce à une extension de la formule de Selberg (cf. lemme 2), qui permet d'évaluer $\sum_{\substack{n\le x \\ n\equiv 1 \bmod 2}} z^{\Omega(n)}$. On remarque enfin que dans la sommation de la formule (1) les termes les plus importants sont ceux pour lesquels m est voisin de 2ℓ ; en quelque sorte, l'élément normal de $\mathcal{N}(x,k)$, lorsque $k \ge (2+\varepsilon)\ell$, s'écrit $n = 2^a n'$ avec n' impair et $\Omega(n') \sim 2\ell$.

Cette démonstration marche lorsque $k \le (\log x)(\frac{1}{\log 2} - \varepsilon)$. Il est facile de voir que, si $k > (\log x)/\log 3$, alors tout élément de $\mathcal{N}(x,k)$ est certainement pair, et même divisible par une certaine puissance de 2, ce qui permet de nous ramener au cas précédent.

II. QUELQUES LEMMES.

LEMME 1. *Soit* a *un nombre réel fixé. On a, lorsque* $x \to +\infty$:

$$e^{-x} \sum_{m \ge x+x^{3/4}+a} \frac{x^m}{m!} = O(1/x)$$

et

$$e^{-x} \sum_{m \le x-x^{3/4}+a} \frac{x^m}{m!} = O(1/x).$$

Démonstration. On utilise les majorations suivantes : (cf. [Hal], p. 149)

$$\sum_{m\ge m_0} \frac{x^m}{m!} \le \left(\frac{ex}{m_0}\right)^{m_0} ; \qquad 0 < x \le m_0$$

$$\sum_{m\le m_1} \frac{x^m}{m!} \le \left(\frac{ex}{m_1}\right)^{m_1} ; \qquad 0 < m_1 \le x \quad .$$

On pose $m_0 = x(1+u)$ avec $u = x^{-1/4} + ax^{-1}$, et en utilisant le développement limité

$$(1+u)(1 - \log(1+u)) = 1 - u^2/2 + o(u^2)$$

on obtient pour la première quantité la majoration

$$\exp(-x\,\frac{u^2}{2}\,(1 + o(1))).$$

La deuxième majoration est similaire.

LEMME 2 (Formule de Selberg pour les nombres impairs).

On a :

$$\sum_{\substack{n\le x\\ n\equiv 1 \bmod 2}} z^{\Omega(n)} = xz\left(1-\frac{z}{2}\right) F(z)(\log x)^{z-1} + xO(\log x)^{\operatorname{Re} z-2}$$

où le "O" est uniforme pour $|z| \le R < 2$, *et la fonction* $(1-z/2)\,F(z)$ *est holomorphe pour* $|z| < 3$.

Démonstration. H. Delange a donné ([Del], p. 136) une formule de Selberg pour une progression arithmétique quelconque. Cependant, on peut donner ici une démonstration rapide. On a :

$$\sum_{\substack{n\le x\\ n \text{ pair}}} z^{\Omega(n)} = \sum_{n'\le x/2} z^{1+\Omega(n')}$$

et par (1) :

$$= z\{\frac{x}{2}\, zF(z)\,(\log \tfrac{x}{2})^{z-1} + O(\tfrac{x}{2}(\log \tfrac{x}{2}))^{\operatorname{Re} z-2}\}$$

$$= z^2 \frac{x}{2} F(z)(\log x)^{z-1} + O(x(\log x)^{\operatorname{Re} z-2}) .$$

En observant que :

$$\sum_{\substack{n\le x\\ n\equiv 1 \bmod 2}} z^{\Omega(n)} = \sum_{n\le x} z^{\Omega(n)} - \sum_{\substack{n\le x\\ n \text{ pair}}} z^{\Omega(n)} ,$$

et en appliquant (1), on démontre le lemme.

LEMME 3. *Soit* $f(z)$ *une fonction holomorphe dans* $|z| \le R$ *et vérifiant* $f(0) \neq 0$. *Soit* $t > 0$ *et*

$$f(z)e^{tz} = a_0 + a_1 z + \ldots + a_k z^k + \ldots .$$

Alors on a, pour $k < tR$:

$$|a_k - f(k/t)\, t^k/k!| \le 2M \left(\frac{t^k}{k!}\right)\left(\frac{k}{t^2}\right)$$

où $M = \sup_{|z|\le R} |f''(z)|$.

Démonstration. On écrit, pour $k \neq 0$:

$$a_k = \frac{1}{2i\pi} \int_\gamma \frac{f(z)e^{tz}}{z^{k+1}}\, dz$$

où γ est le cercle de centre 0 et de rayon $r = k/t$. On a ensuite :

$$f(z) = f(r) + (z-r)\, f'(r) + (z-r)^2\, \Phi(z)$$

et la fonction Φ est holomorphe pour $|z| \leq R$. Un calcul simple montre que :

$$(z-r)^2\, \Phi(z) = \int_r^z (z-w)\, f''(w)dw$$

et que

$$|\Phi(z)| \leq M/2 .$$

On a alors :

$$a_k = \frac{1}{2i\pi} \{\int_\gamma \frac{f(r)e^{tz}}{z^{k+1}}\, dz + \int_\gamma \frac{(z-r)f'(r)e^{tz}}{z^{k+1}}\, dz + \int_\gamma \frac{(z-r)^2\, e^{tz}\, \Phi(z)}{z^{k+1}}\, dz\}.$$

La première intégrale vaut $f(r)\, t^k/k!$; la seconde est nulle; la troisième est majorée par $\frac{M}{2\pi\ r^{k-2}} J$, avec

$$J = \int_{-\pi}^{\pi} (1-\cos\ \theta)e^{k\cos\theta} d\theta .$$

Or,

$$J = 2\int_0^{\pi} (1-\cos\ \theta)e^{k\cos\theta} d\theta \leq 2\int_0^{\frac{\pi}{2}} (1-\cos\ \theta)e^{k\cos\theta}\, d\theta + (\pi+2)$$

$$\leq 2\int_0^1 \frac{1-u}{\sqrt{1-u^2}}\, e^{ku}\, du + (\pi+2) \leq 2\int_0^1 \sqrt{1-u}\ \ e^{ku}\, du + (\pi+2)$$

$$= 2\, e^k\, k^{-3/2} \int_0^k e^{-v}\, \sqrt{v}\, dv + (\pi+2)$$

$$\leq 2\, \Gamma(3/2)\, e^k\, k^{-3/2} + (\pi+2) \leq 4e^k\, k^{-3/2} .$$

On obtient donc :

$$|a_k - f(r)\, t^k/k!| \leq \frac{4M}{2\pi} \frac{t^{k-2}}{k^{k-2}}\, e^k\, k^{-3/2} .$$

En utilisant la formule de Stirling sous la forme :

$$k! \leq k^k\, e^{-k}\, \sqrt{2\pi k}\quad \exp(1/12k) \leq 2{,}73\, k^k\, e^{-k}\ \sqrt{k} ,$$

on achève la démonstration du lemme.

LEMME 4. *Soit* $\chi(n)$ *la fonction qui vaut* 1 *si* n *est impair, et* 0 *si* n *est pair. On a alors, pour* z *réel, vérifiant* $1 \leq z < 3$,

$$\sum_{n\leq x} \chi(n)\, z^{\Omega(n)} \leq x \prod_{3\leq p\leq x} (1 + \frac{z-1}{p-z})$$

et pour tout $\rho < 3$, *on a :*

$$N'(x,k) \leq C_\rho\, \frac{x(\log\ x)^{\rho-1}}{\rho^k}$$

pour tout $x \geq 1$ *et* $k \geq 1$.

Démonstration. On écrit :

$$\chi(n)\, z^{\Omega(n)} = \sum_{d|n} h(d)$$

où $h(d)$ est la fonction multiplicative à valeurs positives ou nulles définies par :

$$h(p^\alpha) = \chi(p) z^\alpha (1-1/z).$$

On a ensuite :

$$\begin{aligned}
\sum_{n\leq x} \chi(n) z^{\Omega(n)} &= \sum_{n\leq x} \sum_{d|n} h(d) \leq x \sum_{d\leq x} \frac{h(d)}{d} \\
&\leq x \prod_{p\leq x} \{1 + \frac{h(p)}{p} + \ldots + \frac{h(p^\alpha)}{p^\alpha} + \ldots\} \\
&= x \prod_{p\leq x} (1 + \chi(p)(1 - \frac{1}{z})(\sum_{\alpha\geq 1} (\frac{z}{p})^\alpha)) \\
&= x \prod_{3\leq p\leq x} (1 + \frac{z-1}{p-z}).
\end{aligned}$$

On peut majorer $N'(x,k)$ en observant :

$$z^k N'(x,k) \leq \sum_{n\leq x} \chi(n)\, z^{\Omega(n)} ,$$

ce qui donne, pour $z = \rho$,

$$\begin{aligned}
N'(x,k) &\leq \rho^{-k} x \prod_{3\leq p\leq x} (1 + \frac{\rho-1}{p-\rho}) \\
&\leq \frac{x}{\rho^k} \exp \sum_{3\leq p\leq x} \frac{\rho-1}{p-\rho} \\
&\leq \frac{x}{\rho^k} \exp (\sum_{3\leq p\leq x} \frac{1}{p} + (\frac{\rho}{p(p-\rho)}))(\rho-1) .
\end{aligned}$$

Et en utilisant la relation

$$\sum_{p\leq x} \frac{1}{p} = \log\log x + O(1)$$

on obtient l'égalité annoncée.

Remarquons que, par une méthode similaire, K. Norton obtient une majoration meilleure cf. [Nor 3])

$$N'(x,k) = O\left(\frac{x(\log x)^2}{3^k} \sqrt{\log\log x}\right).$$

PROPOSITION. (Evaluation de $N'(x,k)$). *On a, pour* $\rho < 3$,

$$N'(x,k) = O\left(\frac{x}{\log x}\,\frac{\ell^{k-1}}{(k-1)!}\right) \tag{3}$$

uniformément pour $k \le \rho\ell$. *De plus, pour*

$$2\ell - 2\ell^{3/4} \le k \le 2\ell + 2\ell^{3/4} \tag{4}$$

on a :

$$N'(x,k) = \frac{Cx}{2\log x}\,\frac{\ell^{k-1}}{(k-1)!}\,(1+O(\ell^{-1/4})) \tag{5}$$

où la constante C *est celle qui figure dans le théorème.*

Démonstration. Le lemme 2 nous dit que :

$$\sum_{\substack{n\le x\\ n\equiv 1 \bmod 2}} z^{\Omega(n)} = xz(1-z/2)\,F(z)\,(\log x)^{z-1} + Q(x,z) \tag{6}$$

où $Q(x,z)$ est holomorphe pour $|z| < 3$, et pour chaque $R<2$, il existe $M(R) > 0$ tel que

$$|Q(x,z)| \le M(R)\,x(\log x)^{\mathrm{Re}\,z-2} \quad \text{pour} \quad x \ge 2 \quad \text{et} \quad |z| \le R. \tag{7}$$

Le coefficient de z^k dans (6) est $N'(x,k)$. On a donc :

$$N'(x,k) = a_k(x) + b_k(x)$$

où $a_k(x)$ et $b_k(x)$ sont les coefficients de z^k dans les développements en série entière de $xz(1-z/2)\,F(z)\,(\log x)^{z-1}$ et de $Q(x,z)$.

D'après une inégalité classique de Cauchy, il résulte de (7) que pour $R<2$,

$$|b_k(x)| \le M(R)\,x(\log x)^{R-2}\,R^{-k} \quad \text{pour} \quad x \ge 2.$$

La formule (3) résulte pour $k \le 9\ell/5$ du théorème de Sathe, car il est clair que $N'(x,k) \le N(x,k)$. Pour $9/5 \le k \le \rho\ell$, on choisit $R = 9/5$, et on pose $r = k/\ell$. On a :

$$\begin{aligned} |b_k(x)| &\le M(9/5)\,x(\log x)^{-1/5}\,(9/5)^{-k} \\ &\le M(9/5)\,x\exp(-1/5 - r\log 9/5)\ell\,. \end{aligned}$$

On a d'autre part, d'après la formule de Stirling :

$$\frac{\ell^{k-1}}{(k-1)!} \gg \frac{\ell^k}{k!} \gg \left(\frac{\ell}{k}\right)^k \frac{e^k}{\sqrt{\ell}}$$

ce qui entraîne

$$\frac{1}{\log x}\,\frac{\ell^{k-1}}{(k-1)!} \gg \exp((-r\log r + r - 1)\,\ell - (1/2)\log \ell).$$

La fonction $r \longmapsto -r\log r + r - 1 + r\log(9/5) + 1/5$ pour $r \in [9/5, 3]$ présente un minimum en $r = 3$. On en déduit :

$$b_k(x) = O\Big(\frac{x}{(\log x)^{1,6}}\,\frac{\ell^{k-1}}{(k-1)!}\Big).$$

L'estimation de $a_k(x)$ se fait par le lemme 3, en remarquant que $F(0) \neq 0$. On achève ainsi de démontrer (3). On obtient (5), en observant que si l'on pose

$$F_1(z) = (1-z/2)\,F(z) = \frac{1}{2^z\,\Gamma(z+1)} \prod_{p\geq 3} (1-1/p)^z\,(1-z/p)^{-1}.$$

On a lorsque k vérifie (4)

$$F_1((k-1)/\ell) = F_1(2)\,(1 + O(\ell^{-1/4}))$$

et

$$F_1(2) = C/2.$$

III. DEMONSTRATION DU THEOREME LORSQUE $k < \log x$.

On remarque d'abord que l'hypothèse $k < \log x$ entraîne :

$$x \geq x/2^k \geq x^{1-\log 2}$$

$$\log x \geq \log(x/2^k) \geq (1-\log 2)\log x$$

$$\log\log(x/2^k) = \ell + O(1).$$

On choisit $\rho = 5/2$ et on découpe la somme (2) :

$$N(x,k) = S_1 + S_2 + S_3 + S_4$$

où les intervalles de sommation sont :

pour S_1 : $m \leq 2\ell - (2\ell)^{3/4} = m_0$

pour S_2 : $m_0 < m \leq 2\ell + (2\ell)^{3/4} = m_1$

pour S_3 : $m_1 < m \leq \rho\ell$

pour S_4 : $\rho\ell < m \leq k$.

La somme S_4 pouvant éventuellement être vide.

a) Majoration de S_4.

D'après le lemme 4, on a :

$$S_4 = \sum_{\rho\ell<m\le k} N'(x2^{m-k}, m)$$

$$\le C_\rho \sum_{\rho\ell<m\le k} x2^{m-k}(\log x)^{\rho-1}\,\rho^{-m}$$

$$\ll \frac{x}{2^k}(\log x)^{\rho-1} \sum_{\rho\ell<m} (2/\rho)^m$$

$$\ll x2^{-k}(\log x)^{\rho-1}(2/\rho)^{\rho\ell} = x2^{-k}(\log x)^{\rho-1+\rho\log(2/\rho)}$$

$$= O(x2^{-k}(\log x)^{0,95}), \quad \text{puisque} \quad \rho = 2,5.$$

b) Majoration de S_1. On a

$$S_1 = \sum_{m\le m_0} N'(x2^{m-k}, m)$$

et par (3),

$$S_1 = O\Big(\sum_{m\le m_0} \frac{2^m \ell^{m-1}}{(m-1)!} \frac{x}{2^k \log(x/2^k)}\Big)$$

et par le lemme 1

$$S_1 = O\Big(\frac{x \log x}{2^k \log\log x}\Big) .$$

c) Majoration de S_3. On obtient la même majoration que pour S_1 en appliquant (3), puis le lemme 1.

d) Estimation de S_2. On a :

$$S_2 = \sum_{m_0\le m\le m_1} N'(x2^{m-k}, m).$$

On veut appliquer (5). On doit vérifier que :

$$2\log\log(x2^{m-k}) - 2(\log\log(x2^{m-k}))^{3/4} \le m \le 2\log\log(x2^{m-k}) + 2(\log\log(x2^{m-k}))^{3/4}.$$

Ceci résulte de

$$\log\log(x2^{m-k}) = \ell + O(1).$$

On obtient alors, par (5)

$$N'(x2^{m-k}, m) = \frac{Cx}{2\log(x2^{m-k})}\, 2^{m-k}\, \frac{(\log\log(x2^{m-k}))^{m-1}}{(m-1)!}\,(1+O(\ell^{-1/4})).$$

En posant $\ell_1 = \log\log(x2^{-k})$ et $\ell_2 = \log\log(x2^{(2+\varepsilon)\ell-k})$ et en remarquant que $\log(x2^{m-k}) = \log(x2^{-k})(1+O(\ell/\log x))$, on encadre S_2 par deux sommes de la forme :

$$i = 1, 2 : \qquad \frac{C\,x}{2^k \log(x2^{-k})}\,(1 + O(\ell^{-1/4}))\sum_{m_0<m\le m_1}\frac{(2\ell_i)^{m-1}}{(m-1)!}$$

qui valent, par le lemme 1 :

$$\frac{C\,x}{2^k \log(x2^{-k})}\; e^{2\ell_i}(1+O(\ell^{-1/4})).$$

Or

$$e^{2\ell_1} = \log^2(x2^{-k})$$

et

$$e^{2\ell_2} = (\log(x2^{-k}) + (2+\varepsilon)\ell \log 2)^2$$
$$= \log^2(x2^{-k})(1+O(\ell/\log x)).$$

On obtient donc :

$$S_2 = \frac{Cx}{2^k}\log(x2^{-k})(1 + O(\ell^{-1/4}))$$

et compte tenu des majorations de S_1, S_3, S_4, cela démontre le théorème lorsque $(2+\varepsilon)\ell \le k \le \log x$.

IV. DEMONSTRATION DU THEOREME LORSQUE $k > \log x$.

On observe d'abord que, si $n \in \mathcal{N}(x,k)$, et si l'on écrit $n = 2^a n'$ avec n' impair (ce qui entraîne $\Omega(n') \le (\log n')/\log 3$), on a, lorsque $k > \log x$:

$$k = a + \Omega(n') \le a + (\log n')/\log 3 \le a + \log(x/2^a)/\log 3$$

ce qui implique :

$$a > (k \log 3 - \log x)/\log(3/2)$$

et donc $a \ge a_0$, en posant :

$$a_0 = [(k \log 3 - \log x)/\log(3/2)]$$

où $[u]$ désigne la partie entière de u. On a donc :

$$a_0 = ((k \log 3 - \log x)/\log(3/2)) - \theta$$

avec $0 \le \theta < 1$. Tous les éléments de $\mathcal{N}(x,k)$ sont donc multiples de 2^{a_0}, et l'on a :

$$N(x,k) = N(x2^{-a_0}, k - a_0). \tag{8}$$

On veut appliquer le résultat du paragraphe précédent au membre de droite de (8). On doit donc vérifier :

(9) $$k - a_0 \le \log(x2^{-a_0})$$

et

(10) $$(2+\varepsilon)\log\log(x2^{-a_0}) \le k - a_0.$$

Soit λ un nombre réel. On a :

(11) $$\lambda \log(x2^{-a_0}) - (k-a_0) = \frac{\lambda \log 3 - 1}{\log(3/2)} (\log x - k \log 2) - \theta(1 - \lambda \log 2).$$

En choisissant $\lambda = 1$ et si $k \le (\log x)/(\log 2) - 2$, on constate que le deuxième membre de (11) est positif ce qui entraîne (9). En choisissant $\lambda = 1/\log 3$, le deuxième membre de (11) est maintenant négatif et l'on a :

$$k - a_0 \ge \frac{1}{\log 3} \log(x2^{-a_0}) \ge 3 \log\log(x2^{-a_0}),$$

cette dernière inégalité ayant lieu si $\log(x2^{-a_0}) \ge 6$. Or comme

(12) $$\log x - a_0 \log 2 = \frac{\log 3}{\log(3/2)}(\log x - k \log 2) + \theta \log 2$$

$$\ge \frac{(\log 2)(\log 3)}{\log(3/2)} \left(\frac{\log x}{\log 2} - k\right),$$

on a $\log(x2^{-a_0}) \ge 6$ dès que $k \le \frac{\log x}{\log 2} - 4$, et cela entraîne (10), car on peut se limiter dans le théorème à $\varepsilon \le 1$.

Nous avons démontré au paragraphe III, pour $\varepsilon > 0$, l'existence d'une constante K_ε telle que, pour $x \ge 3$ et k vérifiant $(2+\varepsilon)\ell \le k \le \log x$, on ait :

$$|N(x,k) - Cx2^{-k} \log(x2^{-k})| \le K_\varepsilon \frac{x2^{-k}\log(x2^{-k})}{(\log\log(3x\,2^{-k}))^{1/4}}.$$

On applique cette formule au membre de droite de (8) et on constate qu'elle est encore valable pour $k \le (\log x)/(\log 2) - 4$, puisque la quantité $x2^{-k}$ ne change pas quand on remplace x par $x2^{-a_0}$ et k par $k-a_0$. Enfin, lorsque

$$\frac{\log x}{\log 2} - 4 < k < \frac{\log x}{\log 2} - \eta,$$

(8) et (12) montrent que $N(x,k)$ est borné, et $x2^{-k}$ aussi, et le théorème est démontré en augmentant éventuellement la constante K_ε.

Remarques. L'exposant 1/4 qui figure dans le terme de reste du théorème peut être remplacé par tout nombre $< 1/2$. D'autre part la méthode de Selberg permet d'obtenir un reste meilleur si on se limite à $k \le B\ell$. Rappelons que cette méthode consiste

à écrire dans (1) :

$$F(z) = \frac{C}{2-z} + G(z)$$

avec G holomorphe dans le disque $|z| < 3$, et à écrire $N(x,k)$ comme une somme de 3 termes, dont le premier est le coefficient de z^k dans

$$x\, z\, \frac{C}{2-z}\, (\log x)^{z-1}$$

et vaut donc :

$$\frac{Cx}{2^k \log x} \sum_{j=0}^{k-1} \frac{(2\ell)^j}{j!} .$$

Le deuxième s'évalue en appliquant le lemme 3 à la fonction G, et le troisième se majore par l'inégalité de Cauchy, comme dans la proposition 1. On peut ainsi prouver que :

PROPOSITION 2. *Pour tout* $r > 2$, *et* $B > r$, *il existe* $\delta > 0$ *tel que pour tout* k *vérifiant* $r\ell \le k \le B\ell$, *on ait :*

$$N(x,k) = C(x \log x)2^{-k}(1 + O(\log x)^{-\delta}).$$

Pour $2 < r \le 3$ *on peut choisir pour* δ *n'importe quelle valeur vérifiant* $\delta < 2 + r(\log r - \log 2 - 1)$. *Pour* $3 < r < \frac{2}{\log 3/2} = 4{,}93$ *on peut choisir* $\delta < r \log(3/2) - 1$; *pour* $r > \frac{2}{\log 3/2}$, *on peut choisir* $\delta < 1$.

REFERENCES

[Del] H. DELANGE. Sur des formules de Atle Selberg. Acta Arithmetica, XIX 1971, p. 105-146.

[Ell] P.D.T.A. ELLIOTT. Probabilistic number theory I et II. Springer Verlag 1980, Grundlehren der mathematischen Wissenschaften, n° 239-240.

[Erd] P. ERDÖS. On the integers having exactly K prime factors. Ann of Math. (2), 49, 1948, p. 53-66.

[Hal] H. HALBERSTAM and K.F. ROTH. Sequences. Oxford 1966.

[Kol] G. KOLESNIK and E.G. STRAUSS. On the distribution of integers with a given number of prime factors. Acta Arithmetica, 37, 1980, p. 181-199.

[Lan] E. LANDAU. Handbuch der Lehre von der Verteilung der Primzahlen. Chelsea Publishing Company, 1953.

[Nic] P. ERDÖS et J.L. NICOLAS. Sur la fonction : nombre de facteurs premiers de n. L'Enseignement Mathématique, t. 27, 1981, p. 3-27.

[Nor 1] K.K. NORTON. On the number of restricted prime factors of an integer. I, Illinois J. Math. 20, 1976, p. 681-705.

[Nor 3] K.K. NORTON. On the number of restricted prime factors of an integer. III, à paraître à l'Enseignement Mathématique.

[Ram] S. RAMANUJAN. Collected Papers. Chelsea publishing Company, 1962.

[Sar] P. ERDÖS and A. SARKÖZY. On the number of prime factors of integers. Acta Sci. Math. 42, 1980, p. 237-246.

[Sat] L. G. SATHE. On a problem of Hardy on the distribution of integers having a given number of prime factors. J. Indian Math. Soc. 17, 1953, p. 63-141 ; 18, 1954 ; p. 27-81.

[Sel] A. SELBERG. Note on a paper by L.G. SATHE. J. Indian Math. Soc. 18, 1954, p. 83-87.

J.L. NICOLAS
Département de Mathématiques
Université de Limoges
123, Avenue Albert Thomas

87060 LIMOGES Cedex

POLYNÔMES TRIGONOMETRIQUES ET "MOYENNES CROISEES"

B. SAFFARI (Orsay)

Tout le contenu des paragraphes 2 et suivants [à propos des fonctions définies sur l'intervalle [a,b] muni de la mesure dx/(b-a)] est valable sans modification pour tout espace de probabilité. Néanmoins nous nous restreindrons ici au cadre de l'intervalle [a,b] pour suivre à la lettre l'exposé oral. La mesure de Lebesgue d'un ensemble S sera notée mes S.

1 - Etant donnés deux nombres strictement positifs u et v, leur moyenne pondérée d'ordre p (réel quelconque) par rapport aux "masses" respectives $\lambda > 0$ et $\mu > 0$ est :

$$(1) \qquad M_p(u,v\,;\lambda,\mu) = \begin{cases} \left(\dfrac{\lambda u^p + \mu v^p}{\lambda+\mu}\right)^{1/p} & \text{si } p \neq 0 \\ (u^{\lambda} v^{\mu})^{1/(\lambda+\mu)} & \text{si } p = 0\ . \end{cases}$$

C'est une fonction continue et non-décroissante de p. Pour $\lambda = \mu$, ceci est la moyenne "ordinaire" d'ordre p :

$$M_p(u,v) = \begin{cases} \left(\dfrac{u^p + v^p}{2}\right)^{1/p} & \text{si } p \neq 0 \\ \sqrt{uv} & \text{si } p = 0\ . \end{cases}$$

Lorsque $\lambda = v$, $\mu = u$ (c'est-à-dire quand chacun des nombres u et v est affecté d'une masse égale à l'autre nombre), je propose d'appeler la moyenne pondérée (1) la "moyenne croisée" (en anglais : "cross-mean") d'ordre p de u et v :

$$M_p^*(u,v) = \begin{cases} \left(\dfrac{vu^p + uv^p}{u+v}\right)^{1/p} & \text{si } p \neq 0 \\ (u^v v^u)^{1/(u+v)} & \text{si } p = 0. \end{cases}$$

Au paragraphe 3 j'indiquerai la raison qui m'a conduit à considérer cette "moyenne croisée" (3), qui semble à priori être un objet pour le moins artificiel. Signalons, bien que nous n'ayons pas à nous en servir ici, que Z. PÁLES me fit récemment

observer que $M_p^*(u,v)$ correspond au cas $\alpha = -1$ de la "generalized power mean"

$$M_p(u,v)_\alpha = \left(\frac{u^{\alpha+p} + v^{\alpha+p}}{u^\alpha + v^\alpha}\right)^{1/p}$$

étudiée en détail dans des articles récents par Z. DAROCZY, L. LOSONCZI et lui-même, principalement dans des revues hongroises. Inversement on retrouve les "generalized power means" à l'aide des moyennes croisées, car

$$M_p(u,v)_\alpha = (M^*_{-p/\alpha}(u^{-\alpha},v^{-\alpha}))^{-1/\alpha} \qquad (\text{si } \alpha \neq 0) .$$

2 - Soit $f : [a,b] \longrightarrow \mathbb{R}$ une fonction mesurable et bornée non identiquement nulle presque partout, mais de valeur moyenne nulle :

$$\int_a^b f(x)dx = 0 , \tag{4}$$

de sorte que les nombres

$$H := \sup \operatorname{ess} f \qquad \text{et} \qquad h := -\inf \operatorname{ess} f$$

sont strictement positifs. Pour $p > 0$, posons

$$\|f\|_p = \left(\frac{1}{b-a}\int_a^b |f(x)|^p dx\right)^{1/p} .$$

Une observation ancienne (et triviale) est que

$$h \geq \frac{1}{2}\|f\|_1 . \tag{5}$$

Ceci fut en particulier utilisé par divers auteurs (K.F. ROTH [6], S.K. PICHORIDES [4],...) pour remarquer que, dans le cas $[a,b] = [0,2\pi]$ et

$$f(x) = \sum_{k=1}^{N} \cos n_k x \qquad (\text{les } n_k \text{ entiers, } 0 < n_1 < \ldots < n_N),$$

les divers résultats relatifs à la conjecture de LITTLEWOOD (minorations de $\|f\|_1$ en fonction de N) fournissaient des résultats quant au "problème de ANKENY-CHOWLA" (minorations de h en fonction de N).

Il est facile de voir que, f n'étant pas nulle presque partout, l'inégalité (5) est stricte. En remplaçant f par $-f$, celle-ci devient $H > \frac{1}{2}\|f\|_1$. D'où :

(6) $$\|f\|_1 < 2\min(H,h) .$$

Comme $2Hh/(H+h) < 2\min(H,h)$, je me demandai si l'inégalité grossière (6) ne pourrait pas être remplacée par

(7) $$\|f\|_1 \leq \frac{2Hh}{H+h} ,$$

vu que j'avais déjà observé que certaines inégalités classiques pouvaient être améliorées en remplaçant des expressions analogues au second membre de (6) par les moyennes harmoniques correspondantes. En vérité la démonstration de (7) est très facile. La voici :

Preuve de (7) : On peut supposer sans perte que $[a,b] = [0,1]$. Posons :

$$A = \{x \in [0,1] : f(x) \geq 0\} \quad \text{et} \quad \theta = \text{mes } A ;$$
$$B = \{x \in [0,1] : f(x) < 0\} \quad \text{donc} \quad 1-\theta = \text{mes } B ;$$
$$f^+(x) = \max(f(x),0) \quad \text{et} \quad f^-(x) = \max(-f(x),0) .$$

Il résulte de (4) que

(8) $$\|f\|_1 = 2\int_A f^+(x)dx = 2\int_B f^-(x)dx .$$

Or

(9) $$\int_A f^+(x)dx \leq \theta H \quad \text{et} \quad \int_B f^-(x)dx \leq (1-\theta)h ,$$

donc, d'après (8) et (9),

(10) $$\|f\|_1 \leq 2\min(\theta H, (1-\theta)h) .$$

Le maximum sur $[0,1]$ de la fonction $t \longrightarrow \min(tH, (1-t)h)$ est $Hh/(H+h)$ [atteint en $t = h/(H+h)$]. Donc (10) implique (7). Enfin (9) permet de caractériser les cas d'égalité, que nous énonçons dans le cas général d'un intervalle $[a,b]$ quelconque :
Pour que (7) soit une égalité, il faut et il suffit que

$$\frac{1}{b-a}\,\text{mes}\{x \in [a,b] : f(x) = \xi\} = \begin{cases} h/(H+h) & \text{si } \xi = H \\ H/(H+h) & \text{si } \xi = -h \\ 0 & \text{si } \xi \neq H \text{ et } \neq -h . \end{cases}$$

C'est par exemple le cas pour la fonction valant H sur $[a,c]$ et $-h$ sur $]c,b]$, où $c = a + (b-a)h/(H+h)$.

3 - Par ailleurs j'avais déjà observé, lors d'une étude sur les polynômes triogonométriques sans terme constant (donc de valeur moyenne nulle) de la forme

$$(11) \qquad \sum_{k=1}^{n} (a_k \cos kt + b_k \sin kt) \qquad \text{sur } [0,2\pi] ,$$

que pour toute fonction f vérifiant (4) on a

$$(12) \qquad \|f\|_2 \leq \sqrt{Hh} ,$$

avec des résultats plus précis pour les polynômes trigonométriques (11) quand on tient compte du degré : par exemple le second membre de (12) peut alors être remplacé par

$$(13) \qquad \sqrt{Hh}\,(1 - \tfrac{c}{n}) \qquad (c : \text{constante absolue} > 0) .$$

J'étais intrigué par la similarité entre (7) et (12), les seconds membres étant respectivement les moyennes harmonique et géométrique de H et h. Des personnes à qui je fis part de cette observation suggérèrent, vu le fait que les seconds membres de (7) et (12) sont respectivement $M_{-1}(H,h)$ et $M_0(H,h)$ [cf. la relation (2) ci-dessus], la conjecture suivante :

CONJECTURE. Pour toute f vérifiant (4) et pour tout p réel ≥ 1,

$$(14) \qquad \|f\|_p \leq M_{p-2}(H,h) .$$

Je pus prouver que (14) est vraie pour $p \geq 2$, mais qu'elle est fausse pour $1 < p < 2$. [Pour $p = 1$, elle est vraie d'après (7). Je montrai en outre que (14) est également vraie pour $0 \leq p < 1$]. C'est au cours de cette démonstration que je fus conduit à définir, accessoirement, la moyenne croisée (3). En effet, il résulte facilement de (7) que

$$(15) \qquad \|f\|_p \leq M_p^*(H,h) \qquad \text{pour tout } p \geq 1.$$

[Pour le voir, il suffit de reprendre la démonstration de (7) : on a

$$\|f^+\|_p^p \leq H^{p-1}\|f^+\|_1 = \frac{1}{2}H^{p-1}\|f\|_1 ,$$

$$\|f^-\|_p^p \leq h^{p-1}\|f^-\|_1 = \frac{1}{2}h^{p-1}\|f\|_1 ,$$

En ajoutant, et en utilisant (7), on a bien (15)]. Il ne restait plus qu'à essayer de majorer $M_p^*(H,h)$ par $M_{p-2}(H,h)$. Je prouvai le lemme suivant (qui est facile, mais pas entièrement trivial) :

LEMME. Nous avons, pour tout p réel et pour tous $u>0$, $v>0$,

$$(16) \qquad M_p^*(u,v)\begin{cases} \geq M_{p-2}(u,v) & \text{si } 1\leq p\leq 2 \\ \leq M_{p-2}(u,v) & \text{pour tous les autres } p\in\mathbb{R}. \end{cases}$$

Si $p\neq 1$ et $p\neq 2$, l'égalité n'a lieu que pour $u=v$. [Si $p=1$ ou $p=2$, (16) est évidemment une égalité pour tous $u>0$ et $v>0$].

Je dispose actuellement de quatre démonstrations différentes de (16) : une par moi-même, via les "règles de LAGUERRE" [5]; une par R.C. VAUGHAN [8], par un calcul direct; une par J. PEYRIERE [3], via une utilisation intéressante de propriétés de fonctions hyperboliques; une par J. MARION [2], grâce à une remarque (souvent utile) que, pour des raisons diverses, j'appelle le "lemme de DELANGE" [1] : Soit φ une fonction réelle définie et continue sur $[c,+\infty[$, dérivable sur $]c,+\infty[$, vérifiant $\varphi(c)>0$ et $\varphi(x)>0$ pour x suffisamment grand. Supposons que chaque fois que φ s'annule en un $x_0\in]c,+\infty[$, alors $\varphi'(x_0)$ garde un signe constant (non nul). Alors φ ne s'annule jamais, c'est-à-dire que $\varphi(x)>0$ pour tout $x\geq c$.

Ces diverses démonstrations seront exposées en détail ailleurs. Observons que la véracité de (14) pour $p\geq 2$ résulte de (15) et de la seconde inégalité (16), mais que sa fausseté pour $1<p<2$ ne résulte évidemment pas de la première inégalité (16). Néanmoins il est facile d'établir directement la fausseté de (14) pour $1<p<2$ et le fait que, pour un tel p, la plus petite valeur de q telle que l'on ait toujours

$$\|f\|_p \leq M_q(H,h)$$

est $q=0$.

4 - Extension de (14) au cas $0\leq p\leq 1$. La véracité de (14) pour $p=1$ n'est pas une "singularité". On peut en effet voir que (14) reste vrai pour $0<p\leq 1$, grâce à un argument autre que l'inégalité (15) (laquelle n'est pas valable si $p<1$). En

effet supposons (sans perte) que $[a,b] = [0,1]$, et définissons A, B et θ comme au paragraphe 2 [démonstration de (7)]. Si $0<p<1$, alors d'après l'inégalité de Hölder :

$$\int_A |f(x)|^p dx \leq (\int_A |f(x)|dx)^p (\int_A dx)^{1-p} = R^p \theta^{1-p} ,$$

$$\int_B |f(x)|^p dx \leq (\int_B |f(x)|dx)^p (\int_B dx)^{1-p} = R^p (1-\theta)^{1-p} ,$$

où $R := \int_A |f(x)|dx = \int_B |f(x)|dx$. D'où :

$$(17) \qquad \int_0^1 |f(x)|^p dx \leq R^p(\theta^{1-p} + (1-\theta)^{1-p}) = (H_0 h_0^p + h_0 H_0^p)/(H_0 + h_0)$$

où $H_0 := R/\theta$ et $h_0 = R/(1-\theta)$. Donc, d'après (17) et (16),

$$(18) \qquad \|f\|_p \leq M_p^*(H_0,h_0) \leq M_{p-2}(H_0,h_0).$$

Or, pour <u>tout</u> $q \in \mathbb{R}$ fixé, $M_q(u,v)$ est une fonction croissante de u et de v. Comme $H_0 \leq H$ et $h_0 \leq h$ [cf. (9)], on obtient donc, d'après (18) :

$$\|f\|_p \leq M_{p-2}(H,h) \qquad \text{pour } 0<p<1 ,$$

ce qui est l'inégalité (14) étendue au cas $0<p<1$. (<u>N.B.</u> Pour traiter le cas $0<p<1$, l'utilisation de $M_{p-2}(H_0,h_0)$ et de l'inégalité $M_{p-2}(H_0,h_0) \leq M_{p-2}(H,h)$ était ici indispensable, et nous n'aurions pas pu comparer directement $M_p^*(H_0,h_0)$ et $M_p^*(H,h)$. En effet, contrairement aux moyennes ordinaires, $M_p^*(u,v)$ <u>n'est pas</u> dans ce cas une fonction monotone de u et de v). D'autre part l'inégalité (15) n'est pas nécessairement vraie lorsque $0<p<1$.

L'inégalité (14) reste donc également valable pour $p=0$ à condition de poser

$$\|f\|_0 = \lim_{p\to 0+} \|f\|_p = \exp(\frac{1}{b-a} \int_a^b \log|f(x)|dx)$$

(noter que $\|f\|_p$ est une fonction croissante de p). Ce cas $p=0$ est particulièrement intéressant, vu le lien avec la "mesure de Mahler" d'un polynôme. Quant à l'extension de (14) aux p négatifs, elle sera étudiée ultérieurement dans une version plus détaillée du présent texte.

5 - <u>REMARQUES</u>.

a) <u>Un cas particulier intéressant</u>. L'inégalité (14), qui est donc vraie pour tout $p \geq 0$ (<u>sauf</u> ceux tels que $1<p<2$), devient pour $p=3$:

$$\|f\|_3 \leq \frac{H+h}{2} = \frac{1}{2}\omega(f)$$

où $\omega(f) =$ sup ess f - inf ess f est l'oscillation (essentielle) de f. On a ainsi :

$$2\|f\|_3 \leq \omega(f) \leq 2\|f\|_\infty \qquad \text{pour toute } f \text{ de moyenne nulle,}$$

le facteur 2 étant évidemment optimal dans les deux cas.

b) Polynômes trigonométriques. Malgré le titre de l'exposé, nous n'avons guère parlé ici de polynômes trigonométriques, mais comptons le faire dans un travail reprenant ces questions de façon détaillée. Bornons-nous à indiquer ici que, lorsque f est de la forme (11), on peut affiner les inégalités (14) et (15) en multipliant le second membre par un facteur < 1 (et dépendant du degré n). La forme optimale d'un tel facteur n'est pas connue. En particulier l'expression (13) qui s'obtient grâce à l'utilisation du théorème de FEJER-RIESZ ([7] et [9]) sur la représentation des polynômes trigonométriques ≥ 0, n'est pas optimale. D'autre part on peut obtenir des améliorations intéressantes moyennant des hypothèses appropriées sur les fréquences.

c) L'idée d'une certaine extension de (14) aux fonctions à valeurs complexes a été suggérée par J. PEYRIÈRE. Elle sera développée dans la rédaction détaillée évoquée ci-dessus.

RÉFÉRENCES

[1] H. DELANGE, communication privée, janvier 1975.

[2] J. MARION, communication privée, juin 1979.

[3] J. PEYRIÈRE, communication privée, août 1979.

[4] S.K. PICHORIDES, Norms of Exponential Sums, Publications Mathématiques d'Orsay, 1976.

[5] G. POLYA and G. SZEGÖ, Problems and Theorems in Analysis, Volume II, Springer, 1976.

[6] K.F. ROTH, On cosine polynomials corresponding to sets of integers, Acta Arithmetica XXIV (1973), p. 87-98.

[7] W. RUDIN, Fourier Analysis on Groups, Interscience, 1962.

[8] R.C. VAUGHAN, communication privée, juillet 1979.

[9] L. FEJÉR, Über trigonometrische Polynome, J. Reine Angew. Math. 146 (1916) p. 53-82.

B. SAFFARI
Bâtiment 425 (Mathématiques)
Université de Paris-Sud
91405 ORSAY CEDEX

FRANCE

SUR LES ENSEMBLES DE MULTIPLES

G. TENENBAUM

Soit $\mathscr{A}$ une suite d'entiers et $\mathscr{B}=\mathscr{B}(\mathscr{A})$ l'ensemble des multiples de $\mathscr{A}$, soit

$$\mathscr{B}(\mathscr{A}) := \{ma : m \in \mathbb{N}, a \in \mathscr{A}\} .$$

Une même suite $\mathscr{B}$ peut être engendrée par plusieurs suites $\mathscr{A}$. L'intersection de toutes les suites $\mathscr{A}$ engendrant $\mathscr{B}$ est encore une suite engendrant $\mathscr{B}$. Elle est caractérisée par la propriété qu'aucun de ses éléments n'en divise un autre : on dit qu'elle est primitive. Un exemple important de suite primitive finie est

$$\mathscr{A}(T) := \{a : T < a \leq 2T\} ;$$

un exemple de suite primitive infinie est fourni par l'ensemble des entiers ayant exactement k facteurs premiers comptés avec leur ordre de multiplicité.

Les résultats classiques concernant les ensembles de multiples sont exposés dans le livre d'Halberstam et Roth [5]. Un des théorèmes fondamentaux est le Théorème de Davenport et Erdös démontré en 1937 [2] :

THEOREME (Davenport-Erdös). *Quelle que soit la suite $\mathscr{A}$, l'ensemble des multiples $\mathscr{B}(\mathscr{A})$ possède une densité logarithmique $\delta\mathscr{B}(\mathscr{A})$, égale à sa densité asymptotique inférieure $d\mathscr{B}(\mathscr{A})$.*

Au début des années trente, on avait même conjecturé que tout ensemble de multiple possède une densité asymptotique, mais Besicovitch a montré en 1934 que ce n'est pas le cas [1]. Sa démonstration repose sur le fait que

$$\liminf_{T\to\infty} d(T) = 0 \tag{1}$$

où $d(T)$ désigne la densité asymptotique de $\mathscr{B}(\mathscr{A}(T))$. Ayant prouvé (1), il construit un contre-exemple de la façon suivante. Un nombre positif ε étant donné, on peut toujours trouver une suite $\{T_k : k = 1,2,3,\ldots\}$ tendant vers l'infini et satisfaisant aux deux conditions suivantes

(i) $$d(T_k) \le \varepsilon 2^{-k-1}$$

(ii) $$\sup_{x \ge T_{k+1}} B_k(x)/x \le 2\, d(T_k)$$

pour tout $k \ge 1$, où $B_k(x)$ désigne le cardinal de $\mathscr{B}(\mathscr{A}(T_k)) \cap [1,x]$. On pose alors $\mathscr{A} := \bigcup_{k=1}^{\infty} \mathscr{A}(T_k)$ et $\mathscr{B} := \mathscr{B}(\mathscr{A})$. Notant $B(x) := \operatorname{card} \mathscr{B} \cap [1,x]$, on voit que $B(2T_k) \ge T_k - 1$, et donc que la densité supérieure $\bar{d}\mathscr{B}$ de $\mathscr{B}$ est au moins égale à $\frac{1}{2}$. De plus,

$$B(T_{k+1}) \le \sum_{j=1}^{k} B_j(T_{k+1}) \le \varepsilon\, T_{k+1} \sum_{j=1}^{k} 2^{-j} \le \varepsilon\, T_{k+1} ,$$

d'où $\underline{d}\mathscr{B} \le \varepsilon$. Comme ε est arbitrairement petit, on obtient bien le résultat annoncé.

En 1935, Erdös a précisé la relation (1) en établissant que $d(T) \longrightarrow 0$ lorsque $T \longrightarrow \infty$ [3], sa démonstration fournit même la majoration $d(T) \ll (\log\log T)^{-1/2}$. En utilisant un autre de ses articles [4], j'ai montré en 1976 [7] que l'on a pour T infini

$$d(T) = (\log T)^{-\delta + o(1)}$$

avec

$$\delta := 1 - \frac{\log(e \log 2)}{\log 2} = 0{,}086071\ldots .$$

Le théorème général suivant [9] fournit un encadrement plus précis.

THEOREME 1. *Désignons par* $H(x,y,z)$ *le nombre des entiers au plus égaux à* x *ayant au moins un diviseur dans l'intervalle* $]y,z]$. *Sous l'hypothèse*

(2) $$1 < 2y \le z \le \sqrt{x}$$

et en notant $u := \min(\frac{1}{2}, \frac{\log z/y}{\log y})$, *on a*

(3) $$x\, u^{\delta} L_1(\tfrac{1}{u}) \le H(x,y,z) \le x\, u^{\delta} L_2(\tfrac{1}{u})$$

avec

$$L_1(v) := \exp\{-c_1 \sqrt{\log v \log\log v}\} ,$$

$$L_2(v) := c_2 \log\log v (\log v)^{-1/2} .$$

De plus, dans le cas où $z \ll y$, *on peut supprimer, quitte à modifier* c_2, *le facteur* $\log\log v$ *dans* $L_2(v)$.

On trouvera également dans [9] une étude asymptotique de $H(x,y,z)$ lorsque $y < z < 2y$ et lorsque $\log y = o(\log z)$. En choisissant $y = \frac{1}{2} z = T$ et en faisant tendre x vers l'infini, on obtient par le théorème 1

$$(4) \qquad \frac{\exp\{-c\sqrt{\log\log T \log\log\log T}\}}{(\log T)^{\delta}} \ll d(T) \ll \frac{1}{\sqrt{\log\log T}\,(\log T)^{\delta}} \; ;$$

de plus le même encadrement est valable pour $\frac{1}{x} H(x,T,2T) = \frac{1}{x} \operatorname{card} \mathscr{B}(\mathscr{A}(T)) \cap [1,x]$ dès que $x \geq 4T^2$. Il s'ensuit que le contre-exemple de Besicovitch peut être construit avec, par exemple, la suite définie par

$$T_k = \exp\exp k/\varepsilon \qquad (k = 1,2,3,\ldots)$$

pour ε assez petit. La situation change lorsque l'on restreint la vitesse de croissance de T_k. Considérons, pour $\lambda > 0$, la suite définie par

$$T_k = \exp k^{\lambda} \qquad (k = 1,2,3\ldots)$$

et notons

$$\mathscr{A}_\lambda := \bigcup_{k=1}^{\infty} \mathscr{A}(T_k),$$

$$\mathscr{B}_\lambda := \mathscr{B}(\mathscr{A}_\lambda).$$

Lorsque $\lambda > 1/\delta$, le produit $\prod_{k=1}^{\infty} (1-d(T_k))$ est convergent ; on déduit alors facilement d'une inégalité de Behrend que $d\,\mathscr{B}_\lambda$ existe et que l'on a

$$d\,\mathscr{B}_\lambda \leq 1 - \prod_{k=1}^{\infty} (1-d(T_k)) < 1.$$

A l'opposé, pour $\lambda < 1$, on a $\mathscr{A}_\lambda = \mathbb{N} \setminus \{0,1,2\}$, et donc $d\mathscr{B}_\lambda = 1$. Erdös a conjecturé l'existence d'une valeur $\lambda_0 > 1$ telle que $d\mathscr{B}_\lambda = 1$ pour $\lambda < \lambda_0$. Dans l'article [6] en commun avec R.R. Hall, nous établissons cette conjecture ; plus précisément, on a le résultat suivant :

THEOREME 2. *Soit* $\lambda_0 = 1{,}314578\ldots$ *la racine de l'équation*

$$\lambda_0 \log(1 - \frac{1}{2\lambda_0}) + 2\lambda_0 - 2 = 0.$$

Alors $d\mathscr{B}_\lambda = 1$ *pour* $\lambda < \lambda_0$.

Dans le même travail, nous conjecturons que $d\mathscr{B}_\lambda = 1$ pour $\lambda < \lambda_1 = 1/(1-\log 2) = 3{,}258891\ldots$, et que $d\mathscr{B}_\lambda < 1$ pour $\lambda > \lambda_1$. L'argument heuristique conduisant à cette conjecture est le suivant : les diviseurs de n occupent l'échelle logarithmique $[0, \log n]$, dont la réunion des intervalles $]T_k, 2T_k]$ couvre une longueur équivalente à $\log 2\ (\log n)^{1/\lambda}$, soit une proportion d'environ $\log 2\ (\log n)^{(1/\lambda)-1}$; il est raisonnable de penser que la condition $d\mathscr{B}_\lambda = 1$ n'est réalisée que si ce nombre est au moins égal à $1/\tau(n)$ pour presque tout n ; comme l'ordre normal de $\tau(n)$ est $(\log n)^{\log 2 + o(1)}$, on obtient bien la valeur λ_1 annoncée.

La démonstration du théorème 2 utilise la notion d'équirépartition modulo 1 sur les diviseurs. On dit qu'une fonction arithmétique réelle f est équirépartie modulo 1 sur les diviseurs (en abrégé erd) si

$$\Delta(n\,;f) := \sup_{0\le u<v\le 1} |\mathrm{card}\{d|n : f(d) \in [u,v[(\mathrm{mod}\ 1)\} - (v-u)\tau(n)|$$

est $o(\tau(n))$ pour presque tout n. Un critère pour que f soit erd est que l'on ait pour x infini [8]

$$\sum_{k<x} \Big| \sum_{\substack{n<x \\ n\equiv 0 (\mathrm{mod}\ k)}} \frac{e(\nu f(n))}{n\ 4^{\Omega(n)}} = o(\sqrt{\log x})$$

pour tout entier non nul ν, où $\Omega(n)$ désigne le nombre des facteurs premiers de n, comptés avec leur ordre de multiplicité. Ce critère est utilisé dans [8] pour prouver que $f(d) = (\log d)^\alpha$ est erd pour tout $\alpha > 0$; le Théorème 2 découle d'une estimation adéquate de la discrépence dans le cas $\alpha = 1/\lambda$. En effet, pour montrer l'existence d'un d et d'un k tels que

$$\exp(k^\lambda) < d \le \exp(k^\lambda + \log 2)$$

soit

$$k < (\log d)^{1/\lambda} \le k + \frac{\log 2 - \theta}{\lambda\ k^{\lambda-1}}$$

où $\theta = \theta(k,\lambda)$ est ≥ 0, il suffit de prouver que

$$\Delta(n;f) = o((\log n)^{\frac{1-\lambda}{\lambda}} \tau(n)). \tag{5}$$

Dans [6] nous montrons que

$$\Delta(n\,;f) \ll_\varepsilon \tau(n)^{\gamma+\varepsilon} \tag{6}$$

avec $\gamma := (\log(4-2/\lambda))/\log 4$, lorsque n parcourt une suite de densité logarithmique unité. Pour $\lambda < \lambda_0$, (6) implique (5), d'où $\delta\mathscr{B}_\lambda = 1$. D'après le théorème de Davenport-Erdös, il s'ensuit que $d\mathscr{B}_\lambda = 1$.

BIBLIOGRAPHIE

[1] A.S. BESICOVITCH. On the density of certain sequences of integers, Math. Annalen 110 (1934), 336-341.

[2] H. DAVENPORT et P. ERDÖS. On sequences of positive integers, Acta Arithm. 2 (1937), 147-151.

[3] P. ERDÖS. Note on sequences of integers no one of which is divisible by any other, J. London Math. Soc. 10 (1935), 126-128.

[4] P. ERDÖS. Sur une inégalité asymptotique en théorie des nombres (en russe) Vestnik Leningrad Univ., Serija Mat. Mekh. i Astr. 13 (1960), 41-49.

[5] H. HALBERSTAM et K.F. ROTH, Sequences, Oxford (1966).

[6] R.R. HALL et G. TENENBAUM. Les ensembles de multiples et la densité divisorielle, à paraître.

[7] G. TENENBAUM. Sur la répartition des diviseurs, Sém. Delange-Pisot-Poitou, 17 (1975 / 76) n° G 14.

[8] G. TENENBAUM. Sur la densité divisorielle d'une suite d'entiers, J. Number Theory, à paraître.

[9] G. TENENBAUM. Sur la probabilité qu'un entier possède un diviseur dans un intervalle donné, Compositio Math., à paraître.

G. TENENBAUM
U.E.R. de Mathématiques
Université de Bordeaux I
351, Cours de la Libération

F - 33405 TALENCE

N° D'IMPRESSION 612
3EME TRIMESTRE 1983