SÉMINAIRE DE THÉORIE DES NOMBRES DE BORDEAUX

JEAN BÉSINEAU

Indépendance statistique d'ensembles liés à la fonction « Somme des chiffres »

Séminaire de théorie des nombres de Bordeaux (1970-1971), exp. n° 19, p. 1-20

<http://www.numdam.org/item?id=STNB_1970-1971____A19_0>

Séminaire de Théorie des Nombres
Année 1970-1971 - exposé n° 21

INDEPENDANCE STATISTIQUE D'ENSEMBLES LIES A LA FONCTION "SOMME DES CHIFFRES"

par

Jean BÉSINEAU

-:-:-:-

0 - INTRODUCTION ET PLAN DE L'ARTICLE

0-1 Introduction

a) Des problèmes de R. Salem, E.G. Straus et A.O. Gel'fond.

A la fin de [11] R. Salem pose (p.62-3) une question sur le comportement à l'infini de la transformée de Fourier d'une mesure portée par la somme de deux ensembles de Cantor. E.G. Straus, plus tard, conjecture le résultat arithmétique suivant qui résoud, en partie, le problème d'analyse harmonique de Salem. Soit g_1 , g_2 deux entiers $\geqslant 2$ premiers entre eux, s_{g_1} , s_{g_2} les "sommes des chiffres" en bases g_1 et g_2 (respectivement) : L'ensemble des entiers n tels que $s_{g_1}(n) \leqslant A$, $s_{g_2}(n) \leqslant B$ (A,B donnés) est fini. Toujours dans le même esprit, A.O. Gel'fond qui dans [5] avait obtenu des résultats sur la somme des chiffres, pose le problème suivant ([5], p.265) qu'il qualifie d'intéressant (*) : Démontrer que :

$$\text{card}\left\{n\leqslant x \ ; \ s_{g_1}(n)\equiv c_1 (\text{mod } m_1),\ s_{g_2}(n)\equiv c_2 (\text{mod } m_2)\right\} = \frac{x}{m_1\, m_2}+O(x^{\alpha}) \quad (0\leqslant\alpha<1)$$

si $(m_1 \ , \ g_1-1) = (m_2 \ , \ g_2-1) = 1$.

(*) Dans le même article Gel'fond pose deux autres problèmes, dont l'un est résolu par M. Olivier dans [10]

b) Ce sont des problèmes du genre de celui de Gel'fond qui seront ici résolus. Nous les énoncerons sous forme "d'indépendance" d'ensembles relativement à la densité d des suites d'entiers.

On a par exemple le résultat d'indépendance suivant :

$$d(s_{g_1}(n) \equiv c_1 (\mathrm{mod}\ m_1)\ ,\ s_{g_2}(n) \equiv c_2 (\mathrm{mod}\ m_2)) =$$

$$d(s_{g_1}(n) \equiv c_1 (\mathrm{mod}\ m_1)) \ .\ d(s_{g_2}(n) \equiv c_2 (\mathrm{mod}\ m_2)) = \frac{1}{m_1\ m_2}$$

si, et seulement si, les quatre nombres m_1 , m_2 , g_1-1 , g_2-1 sont premiers entre eux dans leur ensemble.

0-2 Notations fondamentales

Sauf indication contraire, nombre entier signifiera élément de $\mathbb{N}$ (entiers $\geqslant 0$) . Si $a \leqslant b$ sont deux entiers, $[a,b]$, $[a,b[$,... désignent les intervalles d'entiers, $a \leqslant n \leqslant b$, $a \leqslant n < b$,... Si $q < p$ toute somme $\sum_{k=p}^{q}$ devra être interprétée comme nulle. On désigne par $(a_1, a_2, \ldots, a_n)$ le p.g.c.d. de a_1 , a_2 ,..., a_n .

Si $g \geqslant 2$ est un entier donné (appelé base) , on sait que tout entier n s'écrit, et d'une seule façon, $n = \sum_{k=0}^{\infty} e_k(n) g^k$ où les fonctions e_k prennent leurs valeurs dans $[0,g-1]$. Pour n donné, les valeurs $e_k(n) = e_k$ sont les chiffres de n en base g :

Ils sont nuls dès que $k > \left[\frac{\mathrm{Log}\ n}{\mathrm{Log}\ g}\right]$ ($[x]$: plus grand entier $\leqslant x$).

Nous écrirons, classiquement, $n = \overline{e_\ell\ e_{\ell-1} \ldots e_1\ e_o}$ en autorisant éventuellement des "premiers" chiffres e_ℓ , $e_{\ell-1}$,... nuls (745 = 00745).

La fonction s_g , "somme des chiffres en base g" , est l'application $\mathbb{N} \to \mathbb{N}$ qui à $n = \sum_{k=0}^{\infty} e_k(n) g^k$ associe $s_g(n) = \sum_{k=0}^{\infty} e_k(n) = \sum_{k=0}^{\ell} e_k$.

Nous noterons plus simplement s pour s_g et s_1, s_2,..., pour s_{g_1}, s_{g_2},... (respectivement) s'il n'en résulte aucun risque de confusion.

0-3 Densité d'un ensemble d'entiers (rappel). Ensembles indépendants.

Rappelons que la densité d'une partie A de $\mathbb{N}$ est la limite, quand elle existe, $d(A) = \lim_{N\to\infty} \frac{\nu_A(N)}{N}$, où $\nu_A(N)$ est le nombre des éléments de A inférieurs à N.

On sait que d n'est pas une mesure de probabilité sur l'ensemble des suites ayant une densité ; cependant nous emploierons, pour énoncer certains résultats, le vocabulaire probabiliste : Par exemple, si deux parties A, B de $\mathbb{N}$ vérifient $d(A \cap B) = d(A).d(B)$, nous dirons que les ensembles A et B sont "indépendants".

0-4 Un mot des techniques employées et plan de l'article.

Dans [5] Gel'fond démontre ses résultats par des calculs de "sommes d'exponentielles". Michel Mendès-France qui avait déjà dans sa thèse [7] étudié des fonctions pseudo-aléatoires liées à la fonction somme des chiffres, retrouve ([8]) par ses techniques (de fonctions pseudo-aléatoires) certains résultats de Gel'fond pour des fonctions plus générales que la fonction somme des chiffres (fonctions qui sont d'ailleurs g-additives au sens donné par Gel'fond dans [5]) .

Ce sont aussi des techniques de fonctions pseudo-aléatoires que nous utiliserons.

Dans la partie I, nous définirons (I-1) les ensembles et suites à caractère presque-périodique dont nous donnerons quelques exemples, puis dans I-2 , nous rappellerons et préciserons des définitions et des propriétés des fonctions pseudo-aléatoires.

La partie II est consacrée à des fonctions liées aux s_g , dont on démontre qu'elles sont pseudo-aléatoires ou périodiques . (théorèmes 1 et 2).

Dans la partie III, on démontre d'abord le théorème 3 : Ce théorème contient (en gros) les résultats d'indépendance qui sont ensuite analysés. On termine par un résultat d'équirépartition.

PREMIERE PARTIE

I-1 SUITES ET ENSEMBLES A CARACTERES B-PRESQUE-PERIODIQUES (c.p.p.)

I-1-1 Si l'on plonge l'espace $\mathcal{N}$ des fonctions $\phi : \mathbb{N} \to \mathbb{N}$ (d'entiers à valeurs entières) bornées en moyenne ($\limsup_{N\to\infty} \frac{1}{N} \sum_{k=0}^{N-1} \phi(k) < +\infty$) dans l'espace $\mathcal{M}_1 = \mathcal{M}$ de Besicovitch-Marcinkiewicz (des fonctions complexes d'entiers de valeur absolue bornée en moyenne), on peut démontrer en adaptant le procédé constructif [6] de Marcinkiewicz que $\mathcal{N}$ est complet.
(La B-norme dans $\mathcal{M}$ est définie par : $\| f \| = \limsup_{N\to\infty} \frac{1}{N} \sum_{k=0}^{N-1} |f(k)|$. De fait, il s'agit seulement d'une semi-norme qui devient une norme dans l'espace $\mathcal{M}/_{(0)}$ où (0) est l'ensemble des fonctions dont la valeur absolue est nulle en moyenne).

I-1-2 Soit $\mathcal{B} \subset \mathcal{N}$ la partie de $\mathcal{N}$ constituée des fonctions B-presque-périodiques (B-p.p.) (c'est-à-dire qui appartiennent à la B-adhérence de l'ensemble des polynômes trigonométriques (sommes finies d'éléments $ae^{i\omega n}$, a complexe, ω réel)).
On peut voir que $\mathcal{B}$ est B-complet.

L'espace $\mathcal{C}$ des fonctions caractéristiques $\chi : \mathbb{N} \to \{0,1\}$ B-presque-périodiques (qui est une partie de $\mathcal{B}$) est aussi B-complet.

I-1-3 Par analogie avec l'espace $\{0,1\}^{\mathbb{N}}$ dont les éléments sont des fonctions caractéristiques, nous appellerons tout élément $\phi \in \mathbb{N}^{\mathbb{N}}$ une fonction caractéristique <u>généralisée</u> :
Notons qu'à toute $\phi \in \mathbb{N}^{\mathbb{N}}$ on peut associer la suite d'entiers, finie ou infinie, croissante au sens large, ainsi décrite :

$$(\underbrace{0,\ldots,0}_{\phi(0)} \ , \ \underbrace{1,\ldots,1}_{\phi(1)} \ , \ \ldots \ , \ \underbrace{q,\ldots,q}_{\phi(q)} \ ,\ldots)$$

En particulier cette correspondance associe, bijectivement, l'ensemble des fonctions caractéristiques (strictes) et les suites strictement croissantes ou si l'on veut les ensembles d'entiers.

Définition 1 : Nous dirons qu'une *suite* (croissante) d'entiers (finie ou infinie) est à caractère B-presque-périodique (en abrégé c.p.p.) si sa fonction caractéristique généralisée est B-presque-périodique.

Si un *ensemble* d'entiers a une fonction caractéristique B-p.p. nous dirons aussi que cet *ensemble* est B-p.p.

PROPOSITION 1. L'espace $\mathcal{B}$ (resp. $\mathcal{C}$) des fonctions caractéristiques généralisées (resp. des fonctions caractéristiques) B-presque-périodiques est B-complet.

I-1-4 Sur l'ensemble des fonctions $\phi \in \mathcal{M}$ ayant une moyenne :

$$M\phi = \lim_{N \to \infty} \frac{1}{N} \sum_{k=0}^{N-1} \phi(k)$$, l'inégalité (immédiate)

$|M\phi - M\psi| \leq \| \phi - \psi \|$ montre que M est (uniformément) continue. Comme il est connu que les fonctions B-presque-périodiques ont une moyenne, M est continue sur $\mathcal{B}$ ou $\mathcal{C}$.

Pour une fonction caractéristique, la moyenne est la densité de la suite ou de l'ensemble associé. Finalement, en identifiant dans le langage, suites (resp. ensembles) c.p.p., avec leurs fonctions caractéristiques, nous pouvons énoncer :

PROPOSITION 2. L'opérateur moyenne M est continu sur $\mathcal{B}$ ou $\mathcal{C}$. L'opérateur moyenne est continu sur l'ensemble des suites c.p.p. La densité d est continue sur la famille des ensembles c.p.p.

Nous utiliserons l'énoncé amoindri suivant :

COROLLAIRE. Soit (E_ν) une suite d'ensembles c.p.p. de fonctions caractéristiques χ_ν . Si (χ_ν) B-converge vers χ , fonction caractéristique de E , alors E est c.p.p. et $d(E_\nu) \to d(E)$.

I-1-5 Exemples d'ensembles et de suites c.p.p.

a) Citons d'abord les suites de densité nulle, les progressions arithmétiques et leurs réunions finies car leur fonction caractéristique est périodique.

Si ϕ_1 , ϕ_2 sont des fonctions caractéristiques généralisées B-p.p., $a_1 \phi_1 + a_2 \phi_2$ (a_1 , $a_2 \in \mathbb{N}$) , $\mathrm{Inf}(\phi_1 , \phi_2)$, $\mathrm{Sup}(\phi_1 , \phi_2)$ le sont aussi.

b) La suite $n \mapsto [\alpha n + \beta]$ où $\alpha > 0$ est un nombre réel est c.p.p. (c'est un ensemble c.p.p. si $\alpha > 1$).

c) Soit (a_n) une suite (finie ou infinie) d'entiers telle que $\Sigma \frac{1}{a_n} < +\infty$: L'ensemble E des multiples (resp. F des non multiples) des a_n est c.p.p.

Démonstration : Soit E_ν l'ensemble des multiples des $a_1, a_2, \ldots, a_\nu$; χ_ν , χ les fonctions caractéristiques de E_ν , E (respectivement). On a $\chi \geq \chi_\nu$ et $1 = \chi(k) > \chi_\nu(k) = 0$ seulement si k est multiple d'un des $a_{\nu+1}$, $a_{\nu+2}$,... ce qui permet d'écrire :

$$\frac{1}{N} \sum_{k=0}^{N-1} |\chi(k) - \chi_\nu(k)| \leq \left[\frac{N}{a_{\nu+1}}\right] + \left[\frac{N}{a_{\nu+2}}\right] + \ldots$$

donc $\| \chi - \chi_\nu \| \leq \sum_{n=\nu+1}^{\infty} \frac{1}{a_n}$ qui tend vers 0 si $\nu \to \infty$, donc puisque χ_ν est périodique , χ est c.p.p.

L'ensemble F_ν des non multiples de a_1 , $a_2, \ldots, a_\nu$ et l'ensemble F des non multiples de tous les a_n, ont pour fonctions caractéristiques $\phi_\nu = 1 - \chi_\nu$, $\phi = 1 - \chi$ donc $\| \phi - \phi_\nu \| = \| \chi - \chi_\nu \| \to 0$ et d'après le corollaire (§ I-1-4) F est c.p.p. et $d(F_\nu) \to d(F)$.

Si les a_n sont premiers entre eux deux à deux, ceci montre que $d(F) = \prod (1 - \frac{1}{a_n})$ (car il est connu que $d(F_\nu) = \prod_{n=1}^{\nu} (1 - \frac{1}{a_n})$).

En particulier, si $a_n = p_n^r$ où p_n est le n^e nombre premier, et r un entier ≥ 2 , F est l'ensemble Q_r des entiers "r-free" qui est donc c.p.p. et dont on retrouve la densité

$$\prod (1 - \frac{1}{p_n^r}) = \frac{1}{\zeta(r)} \qquad (\zeta : \text{fonction de Riemann}) .$$

d) Signalons enfin que l'ensemble G suivant, que Gel'fond utilise dans son théorème III de [5] est c.p.p. : Soit $k \geq 1$, $r \geq 2$ deux entiers ; G est l'ensemble des entiers n tels que n, n+1,..., n+k soient r-free.

I-2 - FONCTIONS $f : \mathbb{N} \to \mathbb{C}$ PSEUDO-ALEATOIRES. REMARQUES SUR L'EQUI-REPARTITION

I-2-1 Soit $f : \mathbb{N} \to \mathbb{C}$. Sa corrélation γ_f (notée plus simplement γ si cela ne présente pas d'ambiguïté) est la fonction $\mathbb{N} \to \mathbb{C}$, si elle existe, définie par :

$$\gamma(p) = \lim_{N \to \infty} \frac{1}{N} \sum_{k=0}^{N-1} \overline{f(k)}\ f(k+p).$$

$f \in \mathcal{M}$ est dite pseudo-aléatoire (en abrégé p.a.) si γ existe et est nulle en moyenne quadratique : $M|\gamma|^2 = 0$ (*)

On a alors essentiellement les résultats suivants :

a) Une fonction p.a. est nulle en moyenne.

b) Le produit d'une fonction p.a. par une fonction B^2-presque-périodique est nul en moyenne.

c) Ajoutons la proposition suivante :

PROPOSITION 3. Le produit d'une fonction p.a. bornée par une fonction B-presque-périodique est de moyenne nulle.

Démonstration : Soit f p.a. bornée, $\|f\|_\infty = \mathrm{Sup}\{|f(k)| ; k \in \mathbb{N}\} = m$ soit ϕ une fonction B-p.p. et P un polynôme trigonométrique tel que $\|\phi - P\| \leq \varepsilon$ ($\varepsilon > 0$ donné).

(*) Cette définition est celle de J.P. Bertrandias. J. Bass qui le premier a introduit les fonctions p.a. prenait la condition plus restrictive (mais finalement très "voisine"): $\gamma(p) \to 0$ si $p \to \infty$. Il se trouve, comme l'a démontré M. Mendès-France dans sa thèse [7], que la fonction $e^{2i\pi \frac{s(n)}{g}}$ (s : somme des chiffres en base g) , que nous utiliserons dans la suite, est p.a. au sens de Bertrandias, pas au sens de Bass.

L'inégalité $\left|\frac{1}{N}\sum_{k=0}^{N-1}(f(\phi-P))(k)\right| \leqslant \|f\|_\infty \ \|\phi - P\|$

implique $\limsup_{N\to\infty}\left|\frac{1}{N}\sum_{k=0}^{N-1}(f\phi)(k)\right| \leqslant m\,\varepsilon$, qui démontre la proposition 3 puisque cette dernière inégalité est vraie pour tout $\varepsilon > 0$.

I-2-2 Soit $k \mapsto u(k)$ une suite réelle, $n \mapsto q_n$ une suite d'entiers c.p.p., dont la fonction caractéristique est non nulle en moyenne.

PROPOSITION 4. Si pour tout $\ell \geq 1$, la fonction $k \mapsto e^{2i\pi\ell u(k)}$ est p.a. (J.P. Bertrandias dit alors que la suite $(u(k))$ est p.a.), alors la suite $n \mapsto u(q_n)$ est équirépartie modulo 1.

En effet, si ϕ est la fonction caractéristique (généralisée) de (q_n) , la fonction $k \mapsto \phi(k)\, e^{2i\pi\ell u(k)}$ est de moyenne nulle d'après la proposition 3. On en déduit aisément (critère de Weyl) le résultat.

Cette proposition 4 améliore, par exemple, les résultats d'équirépartition liés au critère de Van der Corput.

DEUXIEME PARTIE

II - DES FONCTIONS LIEES A LA "SOMME DES CHIFFRES" QUI SONT PSEUDO-ALEATOIRES OU PERIODIQUES.

Notations : α , $\alpha_1, \ldots, \alpha_\nu$ sont des nombres réels. Les fonctions f, $f_1, \ldots, f_\nu$ sont définies par $f(n) = e^{2i\pi\alpha s(n)}$, $f_j(n) = e^{2i\pi\alpha_j s_j(n)}$ où s, $s_1, \ldots, s_\nu$ sont les sommes des chiffres en bases g, $g_1, \ldots, g_\nu$ respectivement.

Nous démontrerons essentiellement dans cette partie les deux théorèmes suivants :

THEOREME 1. La fonction $f(n) = e^{2i\pi\alpha s(n)}$ est pseudo-aléatoire si $\alpha(g-1)$ est non entier, périodique dans le cas contraire (et alors de moyenne 1 ou 0 , suivant que α est entier ou non).

THEOREME 2. Si les entiers g_1 , g_2,..., g_ν sont deux à deux premiers entre eux, la fonction $(f_1 \cdot f_2 \cdot \ldots \cdot f_\nu)(n) = \prod_{j=1}^{\nu} e^{2i\pi\alpha_j s_j(n)}$ est pseudo-aléatoire si l'un au moins des nombres $\alpha_j(g_j-1)$ est non entier, périodique dans le cas contraire (et alors de moyenne 1 ou 0 suivant que $\alpha_1+\ldots+\alpha_\nu$ est entier ou non) .

Evidemment le théorème 1 est un cas particulier du théorème 2 (pour $\nu = 1$) : Nous traitons le théorème 1 à part, parcequ'il nous apparaît fondamental et sa démonstration autonome. Le théorème 2 est une conséquence du théorème 1 au regard d'autres considérations : Disons tout de suite que les propriétés relatives au produit $f_1 \cdot f_2 \cdot \ldots \cdot f_\nu$ ($\nu \geq 2$) seront établies pour $\nu = 2$ et immédiatement généralisées à $\nu > 2$.

Nous utiliserons pour établir les théorèmes 1 et 2 une relation fondamentale relative à s et les lemmes qui suivront.

II-1 Relation fondamentale relative à la "somme des chiffres" (s en base g)

Si $n = kg^m + r$, m entier , $0 \leq r \leq g^m-1$

on a : $\boxed{s(n) = s(kg^m + r) = s(k) + s(r)}$

$\boxed{f(n) = f(kg^m + r) = f(k).f(r)}$ $\quad (f(n) = e^{2i\pi\alpha s(n)})$

II-2 LEMME 1.

Soit g $\geq$ 2 , s la "somme des chiffres" en base g : Pour p entier donné, il existe une partition de $\mathbb{N}$ en progressions arithmétiques P_m , $m \geq 1$, telles que $s(n+p)-s(n)=\lambda_m$ reste constant si n décrit P_m .

Démonstration :

Ecrivons : $p = \overline{a_\ell \dots a_1}\, a_0 \quad (a_\ell > 0)$

$q = g^{\ell+1} - p$

$n = \overline{e_k\, e_{k-1} \dots e_\ell \dots e_0}$, ou aussi

$n = \lambda g^{\ell+1} + n_1$, avec $0 \leqslant n_1 = \overline{e_\ell \dots e_0} < g^{\ell+1}$

a) Si $o \leqslant n_1 < q$ on voit aisément que $s(n+p)-s(n) = s(n_1+p)-s(n_1)$.

Donc si n décrit l'une des q progressions arithmétiques $n_1 + g^{\ell+1}\mathbb{N}$ $(0 \leqslant n_1 < q)$, $s(n+p)-s(n) = s(n_1+p) - s(n_1)$ est constant.

b) Supposons maintenant $q \leqslant n_1 = \overline{e_\ell \dots e_1\, e_0} < g^{\ell+1}$

b_1) si $0 \leqslant e_{\ell+1} \leqslant g-2$, c'est-à-dire si n décrit l'une des $p(g-1)$ progressions arithmétiques

$$n_1 + ag^{\ell+1} + g^{\ell+2}\mathbb{N} \quad , (0 \leqslant a \leqslant g-2) ,$$

on peut voir que $s(n+p)-s(n) = s(n_1+p) - s(n_1)$ est constant.

b_2) si $e_{\ell+1} = g-1$ et $0 \leqslant e_{\ell+2} \leqslant g-2$, c'est-à-dire si n décrit l'une des $p(g-1)$ progressions arithmétiques

$$n_1 + (g-1)g^{\ell+1} + ag^{\ell+2} + g^{\ell+3}\mathbb{N} \quad , (0 \leqslant a \leqslant g-2)$$

$s(n+p)-s(n) = s(n_1+p) - s(n_1) - (g-1)$ est constant

b_3) Et de façon générale, si n décrit l'une des $p(g-1)$ progressions arithmétiques

$$n_1 + (g-1)g^{\ell+1} + \dots + (g-1)g^{\ell+h} + ag^{\ell+h+1} + g^{\ell+h+2}\mathbb{N} \quad , (0 \leqslant a \leqslant g-2)$$

$s(n+p) - s(n) = s(n_1 + p) - s(n_1) - h(g-1)$ est constant

Comme les progressions mises en évidence constituent une partition de $\mathbb{N}$ (évident) le lemme est démontré.

II-3 LEMME 2. Soit $\{P_m ; m \geqslant 1\}$ la partition précédente, λ_m la valeur fixe de $s(n+p)-s(n)$ si n décrit P_m, $d(P_m)$ la densité de P_m: La fonction $n \mapsto e^{2i\pi\alpha s(n)}$ a une corrélation donnée par

$$\gamma(p) = \sum_{m\geqslant 1} d(P_m) e^{2i\pi\alpha\lambda_m},$$ où le deuxième membre est sommable.

Démonstration :

a) Notons d'abord que les progressions P_m sont de la forme $a_m + g^{r_m}\mathbb{N}$, avec $0 \leqslant a_m < g^{r_m}$. On en déduit que :

$$\mathrm{card}(P_m \cap [0,N-1]) = \frac{N-1}{g^{r_m}} + \varepsilon_m \quad \text{avec } |\varepsilon_m| \leqslant 1$$

b) Le nombre des P_m telles que $P_m \cap [0,N-1] \neq \emptyset$ est $O(\mathrm{Log}\ N)$. En effet ces progressions doivent vérifier $a_m \leqslant N-1$, ce qui a lieu pour au plus $K = q + p(g-1)(\rho(N) - \rho(p))$ suites, où $\rho(N) = \left[\frac{\mathrm{Log}\ N}{\mathrm{Log}\ g}\right] + 1$ est le "nombre de chiffres" de N. (Il suffit d'examiner les a_m sous les rubriques a) b) du lemme 1). Ceci montre que $K = O(\mathrm{Log}\ N)$ et par suite le résultat annoncé.

c) Posons $\gamma_N(p) = \frac{1}{N}\sum_{k=0}^{N-1} e^{2i\pi\alpha(s(n+p)-s(n)}$ $\quad(\gamma(p) = \lim_{N\to\infty} \gamma_N(p))$

on a : $\gamma_N(p) = \frac{1}{N} \sum_{P_m \cap [0,N-1] \neq \emptyset} \left(\frac{N-1}{g^{r_m}} e^{2i\pi\alpha\lambda_m} + \varepsilon_m e^{2i\pi\alpha\lambda_m}\right)$

(notations précédentes). Donc d'après b) on a :

$$\gamma_N(p) = \frac{N-1}{N} \sum_{P_m \cap [0,N-1] \neq \emptyset} \frac{e^{2i\pi\alpha\lambda_m}}{g^{r_m}} + \frac{O(\mathrm{Log}\ N)}{N}$$

d) Le nombre des P_m, telles que $r_m = r$ (constant), est borné (il vaut q ou $p(g-1)$). Il s'ensuit que $\sum_{m\geqslant 1} \frac{1}{g^{r_m}} e^{2i\pi\alpha\lambda_m}$ est sommable.

e) De c) et d) on déduit que si $N \to \infty$: $\gamma_N(p) \to \sum_{m \geq 1} \frac{1}{g^{r_m}} e^{2i\pi\alpha\lambda_m}$, ce qui démontre le lemme 2 .

Remarque : Pour p = 1 la formule trouvée s'écrit

$$\gamma(1) = \frac{g-1}{g} e^{2i\pi\alpha} \sum_{k=0}^{\infty} \frac{e^{2i\pi k\alpha(1-g)}}{g^k}$$ qui donne l'expression

simplifiée : $\gamma(1) = \frac{g-1}{ge^{-2i\pi\alpha} - e^{2i\pi\alpha g}}$. Par des calculs analogues on peut aussi obtenir pour $\gamma(p)$ une expression simplifiée, mais malheureusement encore bien compliquée. De toutes façons, nous ne l'utiliserons pas.

II-4 Lemme 3 Soit g_1 , g_2 deux entiers ≥ 2 , f_1 , f_2 les fonctions définies par $f_1(k) = e^{2i\pi\alpha_1 s_1(k)}$, $f_2(k) = e^{2i\pi\alpha_2 s_2(k)}$, p un entier donné, $\{P_m ; m \geq 1\}$ (resp. $\{Q_n ; n \geq 1\}$) la partition associée à p pour g_1 (resp. pour g_2) comme dans le lemme 1 . On a :

$$\gamma_{f_1 f_2}(p) = \sum_{m,n} d(P_m \cap Q_n) e^{2i\pi\alpha_1\lambda_m} e^{2i\pi\alpha_2\mu_n}$$

(λ_m , μ_n : notations évidentes) où le deuxième membre est sommable.

Démonstration : On répète à peu près celle du lemme 2 .

Le nombre des progressions P_m , Q_n de raisons $g_1^{r_m}$, $g_2^{t_n}$ vérifiant $r_m = r$, $t_m = t$ (r,t donnés) est borné si (r,t) décrit $\mathbb{N}^2$, disons par C. Puisque $P_m \cap Q_n$ est contenu dans P_m et Q_n , on a : $d(P_m \cap Q_n) \leq \mathrm{Inf}\left(\frac{1}{g_1^{r_m}}, \frac{1}{g_2^{t_n}}\right)$

Comme d'autre part $\left(\inf\left(\frac{1}{g_1^r}, \frac{1}{g_2^t}\right)\right)_{(r,t)\in\mathbb{N}^2}$ est sommable , il en est de même de $(d(P_m \cap Q_n))_{(m,n)\in\mathbb{N}^2}$

$$\left(\sum_{m,n} d(P_m \cap Q_n) \leq C \sum_{r,t} \inf\left(\frac{1}{g_1^r}, \frac{1}{g_2^t}\right)\right)$$

II-5 LEMME 4. : Si g_1 , g_2 sont premiers entre eux , on a :

$$\boxed{\gamma_{f_1 f_2} = \gamma_{f_1} \cdot \gamma_{f_2}}$$

En effet $g_1^{r_m}$, $g_2^{t_n}$, raisons de P_m et Q_n , sont alors deux nombres premiers entre eux et, par suite $d(P_m \cap Q_n) = d(P_m).d(Q_n)$.

Donc $\gamma_{f_1 f_2}(p) = \sum_{m,n} d(P_m).\, d(Q_n) e^{2i\pi\alpha_1\lambda_m}\, e^{2i\pi\alpha_2\mu_n} = \gamma_{f_1}(p).\gamma_{f_2}(p)$

Remarque : Ce lemme s'étend immédiatement au suivant .

Si g_1 , g_2,..., g_ν sont premiers entre eux deux à deux :

$$\gamma_{f_1.f_2.\ \ldots\ .f_\nu} = \gamma_{f_1} \cdot \gamma_{f_2} \cdot \ \ldots\ \cdot \gamma_{f_\nu}$$

DEMONSTRATION DU THEOREME 1 .

Les techniques de démonstration de II-6 et II-7 sont inspirées de la thèse de M. Mendès-France ([7] p.46-48) que, par moments, elles démarquent de très près.

II-6 Pour $f(n) = e^{2i\pi\alpha s(n)}$, γ vérifie la récurrence suivante :
si $0 \leqslant r \leqslant g-1$

$$\boxed{(1)\quad \gamma(gn+r) = \left[\frac{g-r}{g}\,\gamma(n) + \frac{r}{g}\,e^{-2i\pi\alpha g}\,\gamma(n+1)\right]\, e^{2i\pi\alpha r}}$$

Démonstration : Soit $p = gn + r$, $0 \leqslant r \leqslant g-1$

$$k = k_1 g + a \ , \quad 0 \leqslant a \leqslant g-1$$

$$S_N = \sum_{k=0}^{gN-1} \overline{f(k)}\, f(k+p) = \sum_{a=0}^{g-1} \sum_{k_1=0}^{N-1} \overline{f(k_1 g+a)}\ f((k_1+n)g+a+r)$$

On a tenant compte de II-1.

$$S_N = \sum_{a=0}^{g-r-1} \overline{f(a)}\ f(a+r) \sum_{k_1=0}^{N-1} \overline{f(k_1)} f(k_1+n) +$$

$$+ \sum_{a=g-r}^{g-1} \overline{f(a)} f(a+r-g) \sum_{k_1=0}^{N-1} \overline{f(k_1)} f(k_1 + n + 1)$$

Donc $S_N = (g-r)e^{2i\pi\alpha r} \sum_{k_1=0}^{N-1} \overline{f(k_1)} f(k_1+n) +$

$$+ re^{2i\pi\alpha(r-g)} \sum_{k_1=0}^{N-1} \overline{f(k_1)} f(k_1+n+1)$$

Divisant des deux côtés par gN et faisant tendre N vers l'infini , on obtient (1) .

II-7 On sait qu'une fonction γ de corrélation est de type positif et on démontre alors (Wiener) qu'elle a elle même une corrélation Γ. Remarquons que $\Gamma(0) = M|\gamma|^2$, donc que f est p.a. si $\Gamma(0) = 0$.

On peut évidemment trouver pour Γ une formule de récurrence par le procédé précédemment employé : Nous emploierons ce procédé uniquement à partir de $\Gamma(0)$ et $\Gamma(1)$, ce qui sera suffisant pour conclure .

$$\text{On a } \Gamma(0) = \lim_{N \to \infty} \frac{1}{gN} \sum_{k=0}^{gN-1} |\gamma(k)|^2$$

On écrit $\sum_{k=0}^{gN-1} |\gamma(k)|^2 = \sum_{r=0}^{g-1} \sum_{n=0}^{N-1} |\gamma(gn + r)|^2$. Et traduisant $\gamma(gn + r)$ par la formule (1) , on établit que :

$$(2) \quad \Gamma(0) = \frac{1}{2}\left(\Gamma(1)e^{-2i\pi\alpha g} + \overline{\Gamma(1)}\ e^{2i\pi\alpha g}\right)$$

De même en partant de $\Gamma(1) = \lim_{N \to \infty} \frac{1}{gN} \sum_{k=0}^{gN-1} \overline{\gamma(k)}\ \gamma(k+1)$,

on établit en tenant compte de (1) et (2) que :

$$(3) \quad g\Gamma(1)\ e^{-2i\pi\alpha} = \frac{g+1}{2}\ \Gamma(1)e^{-2i\pi\alpha g} + \frac{g-1}{2}\ \overline{\Gamma(1)}\ e^{2i\pi\alpha g}$$

II-8 <u>Si</u> $\alpha(g-1)$ <u>n'est pas entier</u> , $f(n) = e^{2i\pi\alpha s(n)}$ <u>est pseudo-aléatoire</u>. En effet, posons $\Gamma(1)e^{-2i\pi\alpha g} = x + iy$.

(3) montre, en posant $\theta = 2\pi\alpha(g-1)$ pour simplifier l'écriture, que x et y vérifient :

$$\begin{cases} x(1-\cos\theta) + y\sin\theta = 0 \\ x\sin\theta + y(\cos\theta - \frac{1}{g}) = 0 \end{cases},$$

système qui admet exclusivement la solution nulle $x = y = 0$, si son déterminant $(1+\frac{1}{g})(\cos\theta - 1)$ est non nul, c'est-à-dire si $\cos\theta = \cos 2\pi\alpha(g-1) \neq 1$. Ceci a lieu si $\alpha(g-1)$ est non entier : A ce moment $\Gamma(1)$ est nul, donc aussi $\Gamma(0)$ d'après (2) et f est bien p.a.

II-9 Supposons $\alpha(g-1) = m$ entier : $\alpha = \frac{m}{g-1}$. Il est connu que pour tout n, $s(n) \equiv n \pmod{(g-1)}$: c'est le principe de la preuve par 9 ; donc $f(n) = e^{2i\pi\frac{m}{g-1}s(n)} = e^{2i\pi\frac{m}{g-1}n}$.

C'est une fonction périodique de moyenne 1 ou 0 suivant que $\frac{m}{g-1} = \alpha$ est entier ou non.

Les paragraphes II-8 et II-9 démontrent le théorème 1.

II-10 DEMONSTRATION DU THEOREME 2

Soit g_1, g_2 deux nombres $\geqslant 2$, premiers entre eux,

$f_1(n) = e^{2i\pi\alpha_1 s_1(n)}$, $f_2(n) = e^{2i\pi\alpha_2 s_2(n)}$

On a puisque $|\gamma_{f_1 f_2}(p)| \leqslant 1$ pour tout p et que $\gamma_{f_1 f_2}$ a une moyenne (puisque c'est une fonction de corrélation (Wiener)) :

$$(M|\gamma_{f_1 f_2}|^2)^2 \leqslant (M|\gamma_{f_1 f_2}|)^2 \leqslant M|\gamma_{f_1}|^2 \cdot M|\gamma_{f_2}|^2,$$

La dernière inégalité étant due au lemme 4 et à l'inégalité de Cauchy-Schwarz. Donc si l'une des fonctions f_1, f_2 est p.a., c'est-à-dire, si l'un au moins des nombres $\alpha_2(g_1-1)$, $\alpha_2(g_2-1)$ est non entier $f_1 f_2$ est p.a.

Si $\alpha_1(g_1-1) = m_1$ et $\alpha_2(g_2-1) = m_2$ sont entiers,

$$(f_1 f_2)(n) = e^{2i\pi\frac{m_1}{g_1-1}n} e^{2i\pi\frac{m_2}{g_2-1}n} = e^{2i\pi(\alpha_1+\alpha_2)n}$$

qui est périodique, de moyenne 1 ou 0 suivant que $\alpha_1 + \alpha_2$ est entier ou non.

Le théorème 2 est donc démontré pour $\nu = 2$. Il est clair, au regard de la remarque du paragraphe II-5 , qu'il est aussi valable pour $\nu > 2$.

TROISIEME PARTIE

III - RESULTATS D'INDEPENDANCE ET D'EQUIREPARTITION

III-1 Soit $g_1,\ldots, g_\nu$, ν entiers premiers entre eux deux à deux, $c_1,\ldots, c_\nu$, $m_1,\ldots, m_\nu$ des entiers tels que $(m_j , g_j-1) = 1$, $j = 1, 2,\ldots, \nu$, A_j les ensembles $\{n ; s_j(n) \equiv c_j \pmod{m_j}\}$, E un ensemble c.p.p.

THEOREME 3. Les ensembles E, $A_1\ldots, A_\nu$ sont indépendants :

$$d(E\cap A_1\cap \ldots\cap A_\nu) = d(E).d(A_1)\ldots.d(A_\nu) = \frac{d(E)}{m_1\, m_2 \ldots m_\nu}$$

Démonstration : Sous les hypothèses indiquées le théorème 2 permet d'affirmer que les fonctions

$$(f_1\ldots f_\nu)(n) = e^{2i\pi \frac{k_1}{m_1} s_1(n)} \ldots e^{2i\pi \frac{k_\nu}{m_\nu} s_\nu(n)}$$

sont pseudo-aléatoires si

$$0 \leqslant k_1 \leqslant m_1-1,\ldots, 0 \leqslant k_\nu \leqslant m_\nu -1 , (k_1,\ldots,k_\nu) \neq (0,\ldots,0).$$

Donc, si χ est la fonction caractéristique (B-p.p.) de E, on a (proposition 3, § I-2-1) les $m_1 \ldots m_\nu-1$ relations

$$\frac{1}{N} \sum_{n=0}^{N-1} \chi(n)\, e^{2i\pi \frac{k_1}{m_1} s_1(n)} \ldots e^{2i\pi \frac{k_\nu}{m_\nu} s_\nu (n)} \to 0$$

En multipliant ces relations respectivement par $e^{-2i\pi\frac{k_1}{m_1} c_1} \ldots e^{-2i\pi\frac{k_\nu}{m_\nu} c_\nu}$,

On a :

$$\frac{1}{N}\sum_{n=0}^{N-1}\chi(n)e^{2i\pi k_1\frac{s_1(n)-c_1}{m_1}}\ldots e^{2i\pi k_\nu\frac{s_\nu(n)-c_\nu}{m_\nu}}\to 0.$$

Comme d'autre part : $\frac{1}{N}\sum_{n=0}^{N-1}\chi(n)\to d(E)$,

il vient, en sommant membre à membre , les $m_1\, m_2 \ldots m_\nu$ relations obtenues , si χ_{A_j} est la fonction caractéristique de A_j :

$$(m_1\ldots m_\nu)M(\chi\chi_{A_1}\ldots\chi_{A_\nu}) = d(E) \text{ , c'est-à-dire}$$

$$d(E\cap A_1\cap\ldots\cap A_\nu) = \frac{d(E)}{m_1\ldots m_\nu}$$

Faisant dans cette relation $E = \mathbb{N}$ et $m_\ell = 1$ pour $\ell \neq j$, on a : $d(A_i) = \frac{1}{m_i}$. Cette dernière affirmation combinée avec le résultat précédent démontre entièrement le théorème 3 .

ANALYSE DES RESULTATS

III-2 Une seule base intervient

1) Si l'on fait $\nu = 1$, posant $g_1 = g$ et $A = \{n; s_g(n)\equiv c(\text{mod } m)\}$, on a si $(m,g-1) = 1$ l'indépendance :

$$d(E\cap A) = d(E).d(A) \quad \left(= \frac{d(E)}{m}\right) .$$

Ce théorème traduit pour $E = a\mathbb{N} + b$ ($a > 0$, b entiers) , Q_r , G (cf. I-1-5, c et d) les théorèmes I, II, III de Gel'fond dans [5] . Enonçons le pour $E = Q_r$: L'ensemble des entiers n "r-free", tels que $s_g(n) \equiv c$ (mod m) a une densité qui vaut $\frac{1}{m\zeta(r)}$. L'ensemble des entiers "r-free" et l'ensemble des entiers n tels que $s_g(n)\equiv c$ (mod m) sont indépendants.

2) Si m et $g-1$ ne sont pas premiers entre eux, certaines fonctions intervenant dans la démonstration du théorème 3 ne sont pas pseudo-aléatoires, mais dans ce cas on peut évaluer (aisément) leur moyenne même si on les multiplie par la fonction caractéristique de la progression arithmétique $a\mathbb{N} + b$.

On peut obtenir les résultats suivants :

si $(a,m,g-1) = 1$: $d((a\mathbb{N}+b)\cap A) = d(a\mathbb{N}+b).d(A) = \frac{1}{am}$

si $(a,m,g-1) = \delta > 1$: $\begin{cases} \text{si } b-c \not\equiv 0 \pmod{\delta} : (a\mathbb{N}+b)\cap A = \emptyset \\ \text{si } b-c \equiv 0 \pmod{\delta} : d((a\mathbb{N}+b)\cap A) = \frac{\delta}{am} \\ \qquad\qquad\qquad\qquad = \delta.d(a\mathbb{N}+b).d(A) \end{cases}$.

III-3 Deux ou plusieurs bases interviennent.

1) Enonçons d'abord le théorème : $d(Q_2\cap A_1\cap A_2) = \frac{1}{m_1 m_2 \zeta(2)}$.

L'ensemble des entiers n "square-free" tels que $s_{g_1}(n) \equiv c_1 \pmod{m_1}$, $s_{g_2}(n) \equiv c_2 \pmod{m_2}$, avec $(g_1,g_2) = (m_1,g_1-1) = (m_2,g_2-1) = 1$, a une densité qui vaut $\frac{6}{m_1 m_2 \pi^2}$.

2) Pour $E = \mathbb{N}$ (en suivant une remarque analogue à II-2,2)) on peut démontrer que si $(m_j , g_j -1) = \delta_j$, on a l'indépendance : $d(A_1\cap \ldots\cap A_\nu) = d(A_1) \ldots d(A_\nu)$, si et seulement si les δ_j sont premiers entre eux deux à deux . (Pour $\nu = 2$, ce résultat est celui qui est cité dans O-1-b) .

Disons, au vu de la formule d'indépendance précédente, que les fonctions $s_1,\ldots, s_\nu$ sont "indépendantes".

III-4 Toujours dans les mêmes conditions : $g_1,\ldots,g_\nu$ sont deux à deux premiers entre eux, on établit aisément le résultat suivant (cf. proposition 4 de I-2-2) :

Si (q_n) est une suite d'entiers c.p.p., dont la fonction caractéristique est de moyenne non nulle, alors, la suite $n \mapsto \sum_{j=1}^{\nu} \alpha_j s_j(q_n)$ est équirépartie modulo 1 si, et seulement si, l'un des α_j au moins est irrationnel.

Ce résultat pour $\nu = 1$, $q_n = n$, était déjà donné par Michel Mendès-France dans sa thèse [7] .

-:-:-:-

REFERENCES

[1] BASS J. Espaces de Besicovitch, Fonctions presque-périodiques, Fonctions pseudo-aléatoires. Bull. Soc. Math. de France, 91, 1963, p. 39-61.

[2] BERTRANDIAS J.P. Espaces de fonctions bornées et continues en moyenne asymptotique d'ordre p. Bull. Soc.Math. France Mémoire 5, 1966, p. 1-106 (thèse Paris 1964).

[3] BERTRANDIAS J.P. Suites pseudo-aléatoires et critères d'équi-répartition modulo 1. Compositio mathematica. vol 16 Fasc. 1,2 p 23-28 , 1964.

[4] BÉSINEAU J. Sur un problème de Gel'fond relatif à la fonction "somme des chiffres". C.R. Acad.Sc.Paris t.272, p.453-456 - 1971.

[5] GEL'FOND A.O. Sur les nombres qui ont des propriétés additives et multiplicatives données. Acta Arithmetica. XIII, 1968, p. 259-265.

[6] MARCINKIEWICZ J. Une remarque sur les espaces de Besicowitch C.R. Acad. Sc. Paris 208, 1939, p. 157-159.

[7] MENDÈS-FRANCE M. Nombres normaux. Applications aux fonctions pseudo-aléatoires. Journal d'analyse mathématique (Jérusalem) 20, 1967, p. 1-56 (thèse , Paris 1966).

[8] MENDÈS-FRANCE M. Séminaire Delange-Pisot-Poitou, 8e année, 1966-67 , fasc 1 exposé 8 (Institut Henri Poincaré Paris 1968)

[9] MENDÈS-FRANCE M. Les suites à spectre vide et la répartition modulo 1. A paraître dans "Journal of number theory".

[10] OLIVIER M. Sur la représentation en base g des nombres premiers. (à paraître).

[11] SALEM R. Algebraic numbers and Fourier analysis H. M. M. 1963.

-:-:-:-

Jean BESINEAU
Université de Pau
Faculté des Sciences Exactes
Département de Mathématiques
Avenue Philippon
64 - P A U