JEAN BASS

Construction d'une suite complètement équirépartie modulo 1. Applications

Séminaire Delange-Pisot-Poitou. Théorie des nombres, tome 14, n° 1 (1972-1973), exp. n° 6, p. 1-8
<http://www.numdam.org/item?id=SDPP_1972-1973__14_1_A4_0>

Séminaire DELANGE-PISOT-POITOU
(Théorie des nombres)
14e année, 1972/73, n° 6, 8 p.

13 novembre 1972

CONSTRUCTION D'UNE SUITE COMPLÈTEMENT ÉQUIRÉPARTIE modulo 1 . APPLICATIONS

par Jean BASS

1. Rappel et définitions.

On donne une suite A_1 , ... , A_n , ... de points appartenant au "cube fondamental" C^n de $\underset{\sim}{R}^n$ $(0 < x_1 < 1$, $0 < x_2 < 1$, ... , $0 < x_n < 1)$. On dit que cette suite est équirépartie dans le cube si, quel que soit le parallélipipède $\mathcal{P}$, intérieur à C^n , dont les côtés sont parallèles aux axes, la propriété suivante est vérifiée :

On considère les N premiers points A_1 , ... , A_N de la suite ; N' d'entre eux appartiennent à $\mathcal{P}$;

1° La proportion N'/N de ces points tend vers une limite, lorsque $N \to \infty$,

2° Cette limite est égale au volume de $\mathcal{P}$.

Si $\{A_n\}$ est une suite quelconque de points (non nécessairement contenus dans C^n), auxquels on associe la même suite modulo 1 , on parle alors d'une suite équirépartie modulo 1 . On dit qu'une suite de nombres réels x_1 , ... , x_n , ... est p-équirépartie modulo 1 si la suite $(x_n , x_{n+1} , \ldots , x_{n+p-1})$ est équirépartie dans C^p (modulo 1) . Une suite de nombres réels x_1 , ... , x_n , ... est complètement équirépartie modulo 1 si elle est p-équirépartie quel que soit $p \geqslant 1$.

On construit facilement des suites équiréparties, et même p-équiréparties. On utilise pour cela les théorèmes de H. WEYL dont voici les énoncés :

Théorème 1 : La suite x_n est équirépartie sur $(0 , 1)$ si et seulement si, pour toute fonction (réelle ou complexe) f , définie et Riemann-intégrable sur $(0 , 1)$,

$$\lim_{N\to\infty} \frac{1}{N} \sum_{n=1}^{N} f(x_n) = \int_0^1 f(x)\, dx .$$

Théorème 2 : La suite x_n est équirépartie modulo 1 si, et seulement si, quel que soit l'entier ℓ non nul,

$$\lim_{N\to\infty} \frac{1}{N} \sum_{n=1}^{N} \exp 2i\pi\ell x_n = 0 .$$

Théorème 3 : La suite x_n est p-équirépartie modulo 1 si, et seulement si, quels que soient les entiers m_1 , m_2 , ... m_p non tous nuls, la suite

$$m_1 x_n + m_2 x_{n+1} + \ldots + m_{n+p-1} x_{n+p-1}$$

est équirépartie modulo 1 .

Théorème 4 : Soit $P(x) = a_0 x^{\nu} + a_1 x^{\nu-1} + \dots + a_{\nu-1} x + a_{\nu}$ un polynôme à coefficients réels de degré $\nu \geqslant 1$.

Si a_0 est irrationnel, la suite $x_n = P(n)$ est ν-équirépartie modulo 1. Elle n'est pas $(\nu + 1)$-équirépartie.

Ce dernier théorème se démontre par récurrence ; tout se ramène au cas $\nu = 1$, pour lequel les moyennes $1/N \sum_{n=1}^{N} \exp 2i\pi\ell x_n$ se calculent élémentairement. On utilise le théorème suivant :

Théorème 5 : Si, pour tout entier h non nul, la suite $x_{n+h} - x_n$ est équirépartie modulo 1, alors la suite x_n est équirépartie modulo 1.

2. Suites complètement équiréparties.

Il est beaucoup plus difficile de construire des suites complètement équiréparties. On sait que la suite θ^n est complètement équirépartie modulo 1 pour presque tout $\theta > 1$ [KOKSMA - FRANKLIN], mais on ne connaît explicitement aucun θ valable.

La méthode suivante a été développée par les mathématiciens russes (POSTNIKOV et autres). On peut la décomposer en deux étapes.

LEMME. - On considère h nombres irrationnels indépendants $\theta_1, \dots, \theta_h$. Pour tout $s \leqslant h$, la suite

$$x^h = \{\theta_1, \dots, \theta_h ; 2\theta_1, \dots, 2\theta_h ; \dots ; n\theta_1, \dots, n\theta_h ; \dots\}$$

est s-équirépartie modulo 1.

Démonstration. - Soit x_j^h le j-ième terme de la suite x^h. On veut montrer que

$$\lim_{N\to\infty} \frac{1}{N} \sum_{j=1}^{N} \exp(2i\pi(m_1 x_j^h + \dots + m_s x_{j+s-1}^h)) = 0 .$$

On pose

$$A_1 = m_1 \theta_1 + \dots + m_s \theta_s ,$$

$$A_2 = m_1 \theta_2 + \dots + m_s \theta_{s+1} ,$$

$$\dots$$

$$A_{h-s+1} = m_1 \theta_{h-s+1} + \dots + m_s \theta_h ,$$

$$\dots$$

$$A_h = m_1 \theta_h + m_2 \theta_1 + \dots + m_s \theta_{s-1} .$$

On désigne par $\|A\|$ la distance de A à l'entier le plus proche. De l'inégalité

$$|\exp(2i\pi A) + \exp(4i\pi A) + \dots + \exp(2i\pi m A)| < \frac{1}{2\|A\|} ,$$

on déduit que

$$\left|\frac{1}{N} \sum_{j=1}^{N} \exp(2i\pi(m_1 x_j^h + \dots + m_s x_{j+s-1}^h))\right| < \frac{1}{2}\left(\frac{1}{\|A_1\|} + \dots + \frac{1}{\|A_h\|}\right) .$$

On conclut facilement.

Voici maintenant le théorème constructif.

THÉORÈME. - Soit $q_1, q_2, \dots, q_k, \dots$ la suite des nombres premiers. On pose d'autre part

$$r_k = \text{partie entière de } \exp(\log k)^3 , \quad \theta_k = \log q_k .$$

Alors la suite

$$\theta_1 , 2\theta_1 , \dots , r_1 \theta_1 ;$$
$$\theta_1 , \theta_2 , \dots , r_2 \theta_1 , r_2 \theta_2 ;$$
$$\dots$$
$$\theta_1 , \dots , \theta_h , \dots , r_h \theta_1 , \dots , r_h \theta_h ;$$
$$\dots$$

est complètement équirépartie modulo 1 .

Démonstration. - Soit x^h la suite

(1) $$\theta_1 , \dots , \theta_h , \dots , n\theta_1 , \dots , n\theta_h , \dots \quad (h \text{ fixe}).$$

On a montré dans le lemme, que

(2) $$\left|\sum_{j=1}^{n} \exp(2i\pi(m_1 x_j^h + \dots + m_s x_{j+s-1}^h))\right| < \frac{1}{2}\left(\frac{1}{\|A_1\|} + \dots + \frac{1}{\|A_h\|}\right) .$$

On va pouvoir aller plus loin en choisissant

(3) $$\theta_h = \log q_h .$$

Les nombres θ_h sont bien irrationnels et indépendants (toute combinaison linéaire à coefficients entiers d'un nombre fini de θ_h est non nulle, sauf si tous les coefficients sont nuls).

On a

(4) $$A_1 = m_1 \theta_1 + \dots + m_s \theta_s = \log(q_1^{m_1} \dots q_s^{m_s}) .$$

Les autres A_j ont des expressions analogues. Or les exposants $m_1 , \dots , m_s$ sont des entiers positifs, négatifs ou nuls.

A_j est donc le logarithme du quotient x/y de deux entiers, x correspondant aux $m_i > 0$, y aux $m_i < 0$. Comme les q_j sont premiers, les deux entiers x et y sont différents. $\log x/y$ est un nombre irrationnel. Or on sait alors minorer $\log x/y$. On utilise le théorème de Mahler.

THÉORÈME [MAHLER]. - Soient x et y deux entiers distincts ; soit z le plus grand. Il existe une constante numérique $c > 0$ telle que

(5) $$\|\log(x/y)\| > \exp(-c(\log z)^2) .$$

On peut ensuite remplacer z par une quantité plus grande. Le plus grand de x

et y est inférieur au produit de h facteurs q_h , avec comme exposant m le plus grand des $|m_j|$.

Cette minoration est valable à la fois pour $\|A_1\|$, $\|A_2\|$, ... , $\|A_h\|$. Donc

(6) $$|\sum_{j=1}^{n} \exp(2i\pi(m_1 x_j^h + \dots + m_s x_{j+s-1}^h))| < \frac{h}{2} \exp(+ c\, s^2\, m^2(\log q_1)^2) .$$

On prend maintenant les (hr_h) premiers termes de la suite x^h (on s'arrête à $n = r_h$). On prend successivement $h = 1 , 2 , \dots$ On constitue ainsi la suite α_j . On veut prouver qu'elle est complètement équirépartie modulo 1 , c'est-à-dire s-équirépartie quel que soit s . On étudie les moyennes

(7) $$\frac{1}{N} \sum_{\ell=1}^{N} \exp(2i\pi(m_1\, \alpha_\ell + \dots + m_s\, \alpha_{\ell+s-1})) .$$

Les exposants $m_1\, \alpha_\ell + \dots + m_s\, \alpha_{\ell+s-1}$ sont formés de termes appartenant à une ou plusieurs suites finies qui engendrent la suite α_j . A partir d'un certain rang, ils appartiennent à <u>une</u> ou à <u>deux</u> de ces suites. Les termes exceptionnels du début apportent à la moyenne (7) une contribution limite nulle. Ceux qui "chevauchent" deux suites sont de même négligeables, comme le montre un facile décompte. Il reste à examiner la contribution des termes dont les exposants sont constitués à partir d'une seule suite. Si l'on définit k par

$$r_1 + 2r_2 + \dots + kr_k < N \leq r_1 + 2r_2 + \dots + kr_k + (k+1)r_{k+1} ,$$

il suffit d'examiner, dans la somme $\sum_{j=1}^{N}$ de (7), les termes qui sont majorés par

(8) $$|\sum_{j=1}^{r_1}| + |\sum_{j=1}^{2r_2}| + \dots + |\sum_{j=1}^{kr_k}| + |\sum_{j=1}^{N-(r_1+\dots+kr_k)}| ,$$

chaque Σ étant respectivement associé à l'une des suites

$$x^1 \quad , \quad x^2 \quad , \dots , \quad x^k \quad , \qquad x^{k+1} \quad .$$

On trouve donc la majoration

(9) $$\frac{1}{2}[\exp(cs^2\, m^2(\log q_1)^2)+\dots+k \exp(cs^2\, m^2(\log q_k)^2)+(k+1)\exp(cs^2\, m^2(\log q_{k+1})^2)] .$$

On utilise maintenant une nouvelle propriété des nombres premiers (la première était purement arithmétique et élémentaire) ; il existe un nombre positif α^2 tel que

(10) $$q_j < \alpha^2\, j \log j .$$

On interprètera d'ailleurs très largement (10) sous la forme

$$q_j < \alpha^2\, j^2 .$$

Une succession de majorations faciles, sinon évidentes, montre que (9) est inférieur à

$$\exp(4c_1\, s^2\, m^2(\log k)^2) ,$$

où c_1 est une constante numérique (déduite de c).

Il faut maintenant diviser par N , et faire tendre N (ou k) vers l'infini. Or

$$N > r_1 + 2r_2 + \dots + kr_k > kr_k .$$

Si l'on choisit pour r_k un entier voisin de

$$\exp(\log k)^3 \ ,$$

et plus précisément la partie entière de $\exp(\log k)^3$, les conditions du théorème de Weyl sont vérifiées, ce qui démontre que la suite considérée est s-équirépartie quel que soit s .

Remarque. - On voit qu'on forme la suite α_j en prenant un certain nombre de termes d'une suite 1-équirépartie, puis un certain nombre de termes d'une suite 2-équirépartie, etc, le nombre de termes pris à chaque fois augmentant suivant une loi donnée. Mais cela ne réussit pas avec n'importe quelle suite. D'autre part, il arrive le plus souvent que nos connaissances actuelles sur les suites équiréparties ne permettent pas de démontrer qu'on obtient bien ainsi une suite complètement équirépartie. En prenant successivement un certain nombre de termes des suites

$$\theta_1 \ , \ 2\theta_1 \ , \ \ldots \ , \ n\theta_1 \ , \ \ldots$$
$$\theta_2 \ , \ 4\theta_2 \ , \ \ldots \ , \ n^2 \theta_2 \ , \ \ldots$$
$$\theta_3 \ , \ 8\theta_3 \ , \ \ldots \ , \ n^3 \theta_3 \ , \ \ldots$$

(θ_1 , θ_2 , θ_3 , ... irrationnels indépendants) qui sont respectivement 1-équirépartie, 2-équirépartie, 3-équirépartie, etc, on peut espérer qu'on obtient une suite complètement équirépartie. Mais on ne sait pas le démontrer. Pratiquement, seules les suites (scalaires ou vectorielles) multiples d'un même élément sont valables. C'est ce qui fait le succès de la démonstration ci-dessus, avec en outre un choix des irrationnels θ_j qui permet d'appliquer des minorations commodes au moment utile.

On notera que le procédé qui vient d'être schématisé ci-dessus est employé dans d'autres circonstances. Il l'a été par MARCINKIEWICZ pour démontrer que l'espace $\mathfrak{M}^p$ (de BESICOVITCH) est complet. $\mathfrak{M}^p$ est l'espace des classes de fonctions complexes f définies sur $\underset{\sim}{R}$ telles que

$$\limsup_{T \to \infty} \frac{1}{2T} \int_{-T}^{T} |f(t)|^p \, dt < \infty \ , \qquad p \geqslant 1 \ .$$

Si l'on se donne une suite de Cauchy f_n dans $\mathfrak{M}^p$ (préalablement normé), on construit explicitement sa limite, qui est la juxtaposition

d'un morceau de f_1 pour $|t| < t_1$

d'un morceau de f_2 pour $|t_1| < |t| < t_2$

d'un morceau de f_3 pour $|t_2| < |t| < t_3$

etc, où t_1 , t_2 , t_3 , ... est une suite croissante bien choisie de nombres positifs.

3. Application.

On appelle fonction pseudo-aléatoire, une fonction f définie sur $\underset{\sim}{R}$, à valeurs réelles ou complexes, telle que les moyennes

$$Mf = \lim_{T\to\infty} \frac{1}{2T} \int_{-T}^{T} f(t)\, dt \ ,$$

$$\gamma(\tau) = M\overline{f}(t)\, f(t+\tau) = \lim_{T\to\infty} \frac{1}{2T} \int_{-T}^{T} \overline{f}(t)\, f(t+\tau)\, dt$$

existent, et que

$$\lim_{\tau\to\infty} \gamma(\tau) = 0 \ .$$

$\gamma(\tau)$ est la <u>fonction de corrélation de</u> f .

Les suites 2-équiréparties permettent de construire des fonctions pseudo-aléatoires. Soit h une fonction réelle ou complexe, définie et intégrable sur $(0,1)$, et telle que

$$\int_0^1 h(x)\, dx = 0 \ .$$

Soit x_n une suite 2-équirépartie. La fonction en escalier, égale à

$$\begin{array}{ll} 0 & \text{si} \quad t < 0 \ , \\ h(x_n) & \text{si} \quad 0 \leqslant n < t < n+1 \ , \end{array}$$

est pseudo-aléatoire.

En effet, on utilise d'abord un théorème général, dû à N. WIENER. Si g est une fonction en escalier, constante sur chaque intervalle $[n\ ,\ n+1]$, sa fonction de corrélation $\gamma(\tau)$ est représentée par une fonction affine dans chaque intervalle $[n\ ,\ n+1]$.

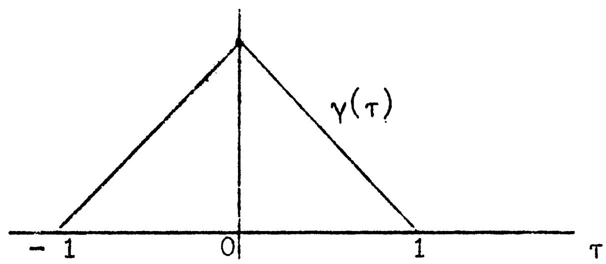
Or si τ est un entier p , on a

$$\gamma(p) = \lim_{N\to\infty} \frac{1}{N} \sum_{n=1}^{N} h(x_n)\, h(x_{n+p}) \ .$$

D'après le premier théorème de Weyl, cette moyenne est nulle pour $p \neq 0$ (produit de deux intégrales nulles), et égale à

$$\int_0^1 |h(x)|^2\, dx \quad \text{si} \quad p = 0 \ .$$

D'où $\gamma(\tau)$



D'autre part, la convolution $f = K * g$ d'une fonction pseudo-aléatoire g par un noyau intégrable sur $\underset{\sim}{R}$ est une fonction pseudo-aléatoire, qui est régularisée par le noyau.

Dans les problèmes non linéaires, on rencontre des fonctions qui sont composées de fonctions pseudo-aléatoires continues f par des fonctions imposées. Il arrive que ces fonctions puissent être développées en série suivant les puissances de f. Le problème essentiel est de savoir si f^n est pseudo-aléatoire. Or, si $f = K * g$,

$$f^n(t) = \int K(s_1) \dots K(s_n)\, g(t - s_1) \dots g(t - s_n)\, ds_1 \dots ds_n .$$

On est donc conduit à étudier les produits de n translatées d'une fonction pseudo-aléatoire $g(t)$, définie par

$$g(t) = h(x_n) \quad \text{si} \quad 0 < n < t < n + 1 ,$$
$$g(t) = 0 \quad \text{si} \quad t < 0 .$$

Mais les propriétés d'un produit de n translatées de g exigent que la suite x_n soit n-équirépartie. S'il y a une suite infinie de puissances de f, n n'est pas limité. C'est pour cette raison que la suite x_n doit être complètement équirépartie modulo 1.

On démontre que $f^n(t)$ est la somme d'une fonction pseudo-aléatoire, et d'une fonction périodique de période 1, définie par

$$\lim_{N\to\infty} \frac{1}{N} \sum_{q=1}^{N} f^n(t + q) ,$$

(et qui peut dans certains cas se réduire à une constante).

Ce résultat est surtout utile pour construire des fonctions réelles. Car, dans ce cas, la partie périodique existe toujours, quitte à se réduire à une constante. Le résultat est même vrai pour les puissances d'une fonction de la forme $g(t)$ ci-dessus. Si cependant $g(t)$ ne prend que les valeurs 1 et -1 (exemple : $h(t)=1$ pour $0 < t < \frac{1}{2}$, $h(t) = -1$ pour $\frac{1}{2} < t < 1$), alors $g^2(t) = 1$ et se réduit à sa partie périodique (constante) ainsi que toutes les puissances paires de g.

Lorsque h est complexe, la partie périodique peut complètement disparaître. Exemple : $g(t) = \exp 2i\pi x_n$.

Remarque. - Ces résultats sont une adaptation locale détaillée d'un théorème de JACOBS-BERTRANDIAS, suivant lequel :

Toute fonction $\mathfrak{M}^p$ faiblement presque-périodique se décompose d'une manière unique en une somme d'une fonction $\mathfrak{M}^p$ presque-périodique et d'une fonction $\mathfrak{M}^p$-pseudo-aléatoire.

BIBLIOGRAPHIE

[1] BASS (J.). - Suites uniformément denses, moyennes trigonométriques, fonctions pseudo-aléatoire, Bull. Soc. math. France, t. 87, 1959, p. 1-64.

[2] BASS (J.). - Les fonctions pseudo-aléatoires. - Paris, Gauthier-Villars, 1962 (Mémorial des Sciences mathématiques, 153).

[3] BASS (J.). - Cours de mathématiques, Tome III. - Paris, Masson, 1971.

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

[5] FRANKLIN (J. N.). - Deterministic simulation of random processes, Math. of Comput., t. 17, 1963, p. 28-59.

[6] KOKSMA (J. K.). - Ein mengentheoretischer Satz über die Gleichverteilung modulo Eins , Compos. Math., Groningen, t. 2, 1953, p. 250-258.

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

[8] MAHLER (K.). - On the approximation of logarithms of algebraic numbers, Phil. Trans. royal Soc. London, t. 245, 1953, p. 371-398.

[9] POSTNIKOV (A. G.). - Modèle arithmétique de processus stochastique [en russe], Trudy Mat. Inst. Steklova, t. 57, 1960, 84 p.

[10] VO-KHAC Khoan. - Etude des fonctions quasi-stationnaires et de leurs applications aux équations différentielles opérationnelles, Bull. Soc. math. France, Mémoire 6, 1966, 175 p. (Thèse Sc. math. Paris, 1965).

[11] WEYL (H.). - Über die Gleichverteilung von Zahlen modulo Eins , Math. Annalen, t. 77, 1916, p. 313-352.

[12] WIENER (N.). - Generalized harmonic analysis, Acta Math., Uppsala, t. 55, 1930, p. 117-258.

(Texte reçu le 17 mai 1973)

Jean BASS
24 rue Ferdinand Jamin
92340 BOURG LA REINE