

Ensembles normaux

par

J. LESCA et M. MENDÈS FRANCE (Bordeaux)

Introduction. Soit $A = (\lambda_n)$ une suite infinie de nombres réels; le nombre réel x est dit A -normal si la suite $xA = (x\lambda_n)$ est équirépartie (mod 1). On désigne par $B(A)$ l'ensemble des nombres A -normaux.

Nous établissons dans cet article deux résultats concernant les suites d'entiers. Soit S l'ensemble des suites croissantes d'entiers. Soit φ une application de \mathcal{N} dans \mathcal{N} . A étant dans S , on pose $\varphi(A) = (\varphi(\lambda_n))$. Nous démontrons:

THÉORÈME 1. *Si pour tout $A \in S$ les deux ensembles $B(\varphi(A))$ et $B(A)$ sont égaux, alors φ est nécessairement de la forme*

$$(1) \quad \varphi(z) = z + \text{const.}$$

pour $z \in \mathcal{N}$ suffisamment grand.

Ce résultat est "fin" en ce sens qu'il existe des fonctions φ ne vérifiant pas (1) et telles que cependant $B(\varphi(A)) = B(A)$ pour presque tous les $A \in S$ (on munit S d'une mesure qui est définie dans la seconde partie de l'article).

On montre en effet:

THÉORÈME 2. *Soit φ un polynôme non constant défini de \mathcal{Z} dans \mathcal{Z} . Pour presque tous les $A \in S$, on a l'égalité: $B(\varphi(A)) = \mathbf{R} - \mathbf{Q}$.*

En choisissant $\varphi(z) = z$, on voit que le théorème implique que $B(A) = \mathbf{R} - \mathbf{Q}$ presque partout: par conséquent pour tout polynôme φ non constant défini de \mathcal{Z} dans \mathcal{Z} , on a $B(\varphi(A)) = B(A)$ presque partout.

Remarque. Le théorème 2 signifie que l'application $B \circ \varphi$ définie de S dans $\mathfrak{P}(\mathbf{R})$ est presque partout constante. Peut-on caractériser les applications $\Psi: \mathcal{Z} \rightarrow \mathcal{Z}$ qui sont telles que $B \circ \Psi$ soit presque partout constantes? Ce problème est en rapport avec celui qui consiste à déterminer les A tels que $B(A) = \mathbf{R} - \mathbf{Q}$.

L'article est divisé en deux parties: la première concerne la démonstration du théorème 1, la seconde concerne la démonstration du théorème 2.

Démonstration du théorème 1

§ 1. Préliminaires. Nous identifions dans toute cette partie le tore \mathbf{R}/\mathbf{Z} au cercle T de longueur unité, orienté et muni d'une origine 0. Si x est un nombre réel, le symbole $\|x\|$ représente la distance de x à l'entier le plus voisin.

Soit φ une application de \mathbf{N} dans \mathbf{N} . Nous démontrons que si φ n'est pas de la forme $\varphi(z) = z + \text{const.}$ pour $z \in \mathbf{N}$ suffisamment grand, alors il existe $A \in \mathcal{S}$ tel que $B(\varphi(A)) \neq B(A)$. Nous sommes amenés à démontrer:

"Soit $U = (u_n)$ une suite croissante d'entiers qui satisfait à l'une des 5 conditions suivantes:

(a) $\varphi(u_n) - u_n$ prend une infinité de fois chacune des deux valeurs a et b ($a \neq b$),

(b) $\varphi(u_n) - u_n$ est non bornée et $\lim_{n \rightarrow \infty} \frac{\varphi(u_n)}{u_n} = 1$,

(c) $\varphi(u_n)/u_n$ tend vers l'infini avec n ,

(d) $\varphi(u_n)/u_n$ tend vers 2 quand n croît indéfiniment,

(e) pour tout entier $n > 0$, $\varphi(u_n) > u_n$ et il existe une constante $\eta \in]0, \frac{1}{2}]$ telle que

$$\eta \leq \|u_n/\varphi(u_n)\| \leq \frac{1}{2} - \eta.$$

Alors il existe une sous suite de A de U telle que $B(A) \neq B(\varphi(A))$."

Pour démontrer dans chacune des cinq hypothèses ci-dessus l'existence d'une telle sous-suite, nous faisons cinq démonstrations. Dans chacune on se donne à priori une sous suite (θ_n) équirépartie modulo 1 et on construit x et A de telle sorte que l'une des suites xA , $x\varphi(A)$ soit adjacente à (θ_n) (donc équirépartie modulo 1) et l'autre non partout dense modulo 1. Chaque fois x est obtenu comme intersection d'intervalles fermés emboîtés dont le diamètre tend vers 0. (Dans chaque cas, il est possible de construire, dans tout ouvert non vide de \mathbf{R} , conjointement à la suite A , un ensemble d'éléments x vérifiant les conditions ci-dessus, ensemble possédant la puissance du continu.)

Ceci démontre bien le théorème. En effet, supposons $(\varphi(u_n) - u_n)$ non constante à partir d'un certain rang:

(1) Si $(\varphi(n) - n)$ est bornée on a nécessairement la propriété (a) pour une suite U convenable.

(2) Si $(\varphi(n) - n)$ est non bornée supérieurement, il existe une suite U possédant l'une des propriétés (b), (c), (d), (e) précédentes.

(3) Si φ possède une valeur d'accumulation, le résultat final est facile.

(4) Si φ est décroissante et ne possède pas une valeur d'accumulation, on peut construire une sous-suite infinie U' telle que la restriction de

φ à U' soit injective et en déduire une suite U pour laquelle on a une des propriétés (a), (b), (c), (d), (e) lorsqu'on remplace φ par φ^{-1} , bien définie dans $\varphi(U')$.

§ 2. Cas (a). On suppose que l'application φ est telle qu'il existe une suite $U \in \mathcal{S}$ pour laquelle $\varphi(u_n) - u_n$ prend une infinité de fois chacune des deux valeurs a et b ($a \neq b$).

Conditions imposées. Construisons les intervalles fermés de \mathbf{R} , I_0, I_1, \dots et la suite $A = (\lambda_n) \in \mathcal{S}$ de sorte que

$$(1) x \in I_0 \Rightarrow \|(b-a)x\| \geq 1/4,$$

$$(2) I_0 \supset I_1 \supset I_2 \supset \dots,$$

$$(3) \lambda_n \text{ diam}(I_{n-1}) \geq 2 \quad (n \geq 1),$$

$$(4) x \in I_n \Rightarrow \|x\lambda_n - \theta_n\| \leq 1/n \quad (n \geq 1),$$

$$(5) \begin{cases} \|\theta_n\| \leq 3/8 \Rightarrow \varphi(\lambda_n) - \lambda_n = a, \\ \|\theta_n\| > 3/8 \Rightarrow \varphi(\lambda_n) - \lambda_n = b \quad (n \geq 1). \end{cases}$$

Les conditions ci-dessus résolvent le problème. En effet, si $x \in \bigcap_{n=0}^{\infty} I_n$, xA est équirépartie (mod 1) puisque d'après (4), cette suite est adjacente (mod 1) à (θ_n) . Par contre, $x\varphi(A)$ n'est pas dense (mod 1). En effet la suite $(\lambda_n + a)x$ est équirépartie (mod 1), mais d'après (1) et (5) la suite $x\varphi(A)$ diffère de la précédente: pour tout entier n , on a

$$\|x\varphi(\lambda_n) - ax\| \leq 3/8 + 1/n.$$

Construction: On construit dans l'ordre $I_0, \lambda_1, I_1, \lambda_2, \dots$. I_0 est choisi de façon à satisfaire la condition (1). Supposons que l'intervalle I_{n-1} soit construit. On choisit λ_n de façon à satisfaire (3) et (5). On construit enfin I_n de façon à vérifier la condition (4) et (2), ce qui est possible puisque $\lambda_n \text{ diam}(I_{n-1}) \geq 2$.

§ 3. Cas (b). On suppose que $\varphi(u_n) - u_n$ est non bornée et que

$$\lim_{n \rightarrow \infty} \frac{\varphi(u_n)}{u_n} = 1.$$

Conditions imposées. Nous construisons une double suite d'intervalles réels

$$I_n = [x_n - l_n, x_n + l_n],$$

$$I'_n = [x'_n - l'_n, x'_n + l'_n]$$

conjointement à la suite λ_n .

Soit C l'ensemble des nombres x tels que la suite $x(\varphi(u_n) - u_n)$ soit dense (mod 1). Comme la suite $\varphi(u_n) - u_n$ est non bornée, on sait que C est de mesure pleine, donc partout dense.

On impose aux intervalles I_n, I'_n et à λ_n les conditions suivantes:

- (1) $I_0 \supset I'_0 \supset I_1 \supset I'_1 \supset I_2 \dots$,
- (2) $I'_{n-1} \varphi(\lambda_n) \geq 1$ ($n \geq 1$),
- (3) $\|x_n \varphi(\lambda_n) - \theta_n\| = 0$ ($n \geq 1$),
- (4) $I_n \varphi(\lambda_n) = 1/n$ ($n \geq 1$),
- (5) $x'_n \in C$ ($n \geq 0$),
- (6) $(x'_{n-1} - x_n) \varphi(\lambda_n) \leq 1/2$ ($n \geq 1$),
- (7) $(\varphi(\lambda_n) - \lambda_n) / \varphi(\lambda_n) \leq 1/n$ ($n \geq 1$),
- (8) $\begin{cases} \|(\varphi(\lambda_n) - \lambda_n) x'_{n-1}\| \leq 1/8 & \text{si } \|\theta_n\| \leq 1/2, \\ \|(\varphi(\lambda_n) - \lambda_n) x'_{n-1}\| \geq 3/8 & \text{si } \|\theta_n\| > 1/2 \end{cases}$ ($n \geq 1$).

Les conditions ci-dessus résolvent le problème. En effet, d'après (3) et (4), si x appartient à $\bigcap_n I_n$, la suite $x\varphi(A)$ est adjacente (mod 1) à la suite (θ_n) donc $x\varphi(A)$ est équirépartie (mod 1).

D'autre part, on a

$$\begin{aligned} x_n \lambda_n &= x_n \varphi(\lambda_n) + x_n (\lambda_n - \varphi(\lambda_n)) \\ &= x_n \varphi(\lambda_n) - (x_n - x'_{n-1}) (\varphi(\lambda_n) - \lambda_n) + x'_{n-1} (\varphi(\lambda_n) - \lambda_n). \end{aligned}$$

Les conditions (3), (7), (6) et (8) conduisent à l'inégalité

$$\|x_n \lambda_n\| \leq \frac{3}{8} + \frac{1}{2n}.$$

Ceci, compte tenu de (4), prouve que la suite $x\lambda$ n'est pas partout dense (mod 1).

Construction: On construit dans l'ordre

$$I_0, \lambda_1, x_1, I_1, x'_1, I'_1, \lambda_2, x_2, I_2, x'_2, I'_2, \dots$$

L'intervalle I_0 est pris arbitrairement. Supposons I_{n-1} construit et toutes les relations précédentes vérifiées. λ_n est construit de façon à satisfaire (2), (7) et (8). Ceci est possible car $x'_{n-1} \in C$. x_n est choisi de façon à satisfaire (3) et (6). I_n est construit de façon à satisfaire $I_n \subset I'_{n-1}$. x'_n est choisi dans l'intérieur de I_n de façon à satisfaire (5). Enfin I'_n est choisi suffisamment petit pour vérifier l'inclusion $I'_n \subset I_n$.

§ 4. Cas (c). On suppose que $\frac{\varphi(u_n)}{u_n}$ croît indéfiniment.

Conditions imposées. Nous construisons deux suites d'intervalles fermés $I_1, I_2, \dots, I'_0, I'_1, \dots$ et une suite $A = (\lambda_n) \in S$ tels que

- (1) $I_0 \subset I_1 \subset I'_1 \subset I_2 \subset I'_2 \subset \dots$,
- (2) $\lambda_n \text{ diam}(I'_{n-1}) \geq 2$ ($n \geq 1$),
- (3) $\varphi(\lambda_n) / \lambda_n > n$ ($n \geq 1$),

$$(4) \ x \in I_n \Rightarrow \|x\lambda_n - \theta_n\| \leq 1/n \ (n \geq 1),$$

$$(5) \ x \in I'_n \Rightarrow \|x\varphi(\lambda_n)\| \leq 1/4 \ (n \geq 1).$$

Les conditions imposées résolvent le problème. En effet, si $x \in \bigcap_n I_n$, alors d'après (4), la suite $x\lambda$ est adjacente (mod 1), à la suite (θ_n) . $x\lambda$ est donc équirépartie (mod 1). Par contre, la suite $x\varphi(A)$ qui vérifie (5) n'est pas dense modulo 1.

Construction: On construit dans l'ordre

$$I'_0, \lambda_1, I_1, I'_1, \lambda'_1, \lambda_2, I_2, I'_2, \dots$$

I'_0 est un intervalle non vide arbitraire. I'_{n-1} étant supposé construit, on construit λ_n suffisamment grand pour satisfaire (2) et (3). Compte tenu de (2), il est possible de construire I_n inclus dans I'_{n-1} de sorte que (4) soit vérifié. Enfin I'_n est un intervalle incluant I_n et qui vérifie (5): ceci est rendu possible par les conditions (4) et (3).

§ 5. Cas (d). On suppose que $\frac{\varphi(u_n)}{u_n}$ tend vers 2.

On définit la suite (η_n) par

$$\begin{cases} 0 \leq \eta_n \leq 1/4, \\ 2\eta_n \equiv \theta_n \pmod{1} \quad (n \geq 0). \end{cases}$$

Par une construction analogue à celles des paragraphes précédents, on détermine une sous-suite A de U et $x \in \mathbf{R}$ tels que la suite $x\lambda$ soit adjacente (mod 1) à la suite (η_n) . $x\lambda$ est donc non équirépartie (mod 1). Par ailleurs, la suite $x\varphi(A)$ est adjacente à (θ_n) donc $x \in B(\varphi(A))$.

§ 6. Cas (e). On suppose que pour tout entier n , $\varphi(u_n) > u_n$ et il existe $\eta \in]0, \frac{1}{2}]$ telle que

$$\eta \leq \left\| \frac{u_n}{\varphi(u_n)} \right\| \leq \frac{1}{2} - \eta.$$

Établissons un résultat préliminaire.

LEMME. Soient $\eta \in]0, \frac{1}{2}]$ et $\alpha \in \mathbf{R}$ tels que

$$\eta \leq \|\alpha\| \leq \frac{1}{2} - \eta.$$

Il existe un entier $r = r(\eta)$ tel que: Pour tout β réel, il existe des entiers u et v tels que

$$\begin{cases} |u| < r, \\ |v| < r, \\ \|au - \beta\| \leq 1/6, \\ \|av - \beta\| \geq 1/3. \end{cases}$$

Démonstration. Soit $r = \left[\frac{1}{2\eta} \right] + 2$. Considérons les $2r + 1$ points de $T = \mathbf{R}/\mathbf{Z}$:

$$S_r = \{0, \pm a, \pm 2a, \dots, \pm ra\}.$$

Montrons que le plus grand arc connexe de $T - S_r$ a une longueur d au plus égale à $1/3$ (le lemme est bien une conséquence de ce dernier résultat).

A cause de la symétrie, on peut toujours supposer que $\eta \leq a \leq \frac{1}{2} - \eta$. Considérons les deux cas:

1er cas: $a \leq \frac{1}{3}$. Alors, compte tenu du fait que $2ra > 1$, il est clair que $d \leq a \leq \frac{1}{3}$.

2e cas: $\frac{1}{3} < a \leq \frac{1}{2} - \eta$. Considérons les points

$$a, 3a, 5a, \dots, sa \quad (s = r \text{ ou } r-1)$$

et leurs symétriques

$$-a, -3a, \dots, -sa.$$

Ces points sont distants de $\frac{1}{3}$ au moins et 2η au plus. Compte tenu du fait que le nombre de ces points est au moins r et de l'inégalité $2(r-1)\eta \geq 1$, il est clair qu'on a: $d \leq \frac{1}{3}$.

Le lemme étant établi, nous construisons les suites de nombres réels $(\gamma_n), (\gamma_n^{(0)}), (l_n)$ et les suites d'entiers $U = (u_n)$ et $A = (\lambda_n)$ telles que $A \subset U$. On pose $I_n = [\gamma_n - l_n, \gamma_n + l_n]$. On rappelle qu'il existe η tel que

$$(1) \eta \leq \left\| \frac{u_n}{\varphi(u_n)} \right\| \leq \frac{1}{2} - \eta.$$

Conditions imposées:

$$(2) I_0 \supset I_1 \supset I_2 \supset \dots,$$

$$(3) \varphi(\lambda_n) l_{n-1} \geq r + 2 \quad (r = r(\eta), \text{ voir le lemme ci-dessus}), \quad (n \geq 1),$$

$$(4) (\varphi(\lambda_n)) \text{ est une suite croissante,}$$

$$(5) \|\varphi(\lambda_n) \gamma_n^{(0)} - \theta_n\| = 0 \quad (n \geq 1),$$

$$(6) |\varphi(\lambda_n) \gamma_n^{(0)} - \varphi(\lambda_n) \gamma_{n-1}| \leq 1/2 \quad (n \geq 1),$$

$$(7) \gamma_n = \gamma_n^{(0)} + u_n / \varphi(\lambda_n) \quad (n \geq 1),$$

$$(8) u_n \leq r \quad (n \geq 1),$$

$$(9) l_n \varphi(\lambda_n) = 1/n \quad (n \geq 1),$$

$$(10) \begin{cases} \|\lambda_n \gamma_n - \theta_n\| \leq 1/6 & \text{si } \|\theta_n\| \leq 1/4, \\ \|\lambda_n \gamma_n - \theta_n\| \geq 1/3 & \text{si } \|\theta_n\| > 1/4 \quad (n \geq 1). \end{cases}$$

Les conditions imposées résolvent le problème. En effet, si x appartient à $\bigcap_n I_n$, alors la suite $x\varphi(A)$ est adjacente modulo 1 à θ_n d'après (5), (7) et (9); la suite $x\varphi(A)$ est donc équirépartie (mod 1).

Par ailleurs, d'après (9), (10) et compte tenu du fait que $\lambda_n < \varphi(\lambda_n)$:

$$\|x\lambda_n\| \leq \frac{5}{12} + \frac{1}{n}.$$

La suite $x\mathcal{A}$ n'est donc pas équirépartie (mod 1).

Possibilité de la construction. On construit dans l'ordre γ_0, l_0 (et par suite I_0), λ_1 (et par suite l_1), $\gamma_1^{(0)}, u_1$ (et par suite γ_1 et I_1), $\lambda_2, \dots, \lambda_n$ (et par suite l_n), $\gamma_n^{(0)}, u_n$ (et par suite γ_n et I_n), λ_{n+1}, \dots

γ_0 et l_0 sont arbitraires. Supposons construits tous les éléments d'indice inférieurs à $n > 0$. On choisit λ_n suffisamment grand pour réaliser (3) et (4). Les conditions (5) et (6) déterminent $\gamma_n^{(0)}, u_n$ se construit de la façon suivante:

Le premier membre des inégalités (10) s'écrit en vertu de (7)

$$\left\| \lambda_n \gamma_n^{(0)} + u_n \frac{\lambda_n}{\varphi(\lambda_n)} - \theta_n \right\|.$$

Il est clair, d'après le lemme précédent et (1) qu'on peut construire u_n de sorte que (8) et (10) soient vérifiés. On peut alors écrire d'après (6), (7) et (8):

$$\|\gamma_{n-1} - \gamma_n\| \leq \|\gamma_{n-1} - \gamma_n^{(0)}\| + \|\gamma_n^{(0)} - \gamma_n\| \leq \frac{1}{2\varphi(\lambda_n)} + \frac{r}{\varphi(\lambda_n)} \leq \frac{r+1}{\varphi(\lambda_n)}.$$

Compte tenu de (3), I_n est bien inclus dans I_{n-1} .

Démonstration du théorème 2

Soit S la famille des suites croissantes $A = (\lambda_n)$ d'entiers positifs. A $A \in S$, on associe la fonction caractéristique $\varepsilon(A) = (\varepsilon_n(A))$ définie par

$$\varepsilon_n(A) = \begin{cases} 1 & \text{si } n \in A, \\ 0 & \text{si } n \notin A, \quad n = 1, 2, 3, \dots \end{cases}$$

La bijection ε ainsi construite permet de transporter la mesure de Haar normalisée de $D = \{0, 1\}^{\mathbf{N}}$ sur l'espace S . Dorénavant, nous supposons S muni de cette mesure.

Soit $\delta = (\delta_n)$ une suite infinie de nombres complexes. On dit que δ est une suite pseudo-aléatoire si

(i) pour tout $p \in \mathbf{Z}$, la limite

$$\gamma(p) = \lim_{n \rightarrow \infty} \frac{1}{n} \sum_{k=1}^n \bar{\delta}_k \delta_{k+p}$$

existe,

$$(ii) \lim_{p \rightarrow \infty} \gamma(p) = 0$$

(voir [1], [2] et [3]).

Nous admettrons les cinq lemmes suivants qui sont classiques.

LEMME 1. Si δ est une suite pseudo-aléatoire et si f est une fonction presque périodique, alors

$$\lim_{n \rightarrow \infty} \frac{1}{n} \sum_{k=1}^n \delta_k f(k) = 0.$$

En particulier, une fonction pseudo-aléatoire a une moyenne nulle (voir [2]).

Soit T l'opérateur de translation dans C^N . T est donc défini par $T(\delta_n) = (\delta_{n+1})$. On définit les itérées de T par $T^p(\delta_n) = (\delta_{n+p})$ pour $p \in \mathbb{Z}$.

LEMME 2. Soit $\delta \in C^N$ une suite telle que les limites suivantes existent:

$$\bar{M}(\delta) = \lim_{n \rightarrow \infty} \frac{1}{n} \left| \sum_{k=1}^n \delta_k \right|,$$

$$M(\delta \cdot T^p \delta) = \lim_{n \rightarrow \infty} \frac{1}{n} \sum_{k=1}^n \delta_k \delta_{k+p} = \gamma(p), \quad p = 0, 1, 2, \dots$$

Alors:

$$|\bar{M}(\delta)|^2 \leq M(|\gamma|).$$

En particulier si $\lim_{p \rightarrow \infty} \gamma(p) = 0$, alors $\bar{M}(\delta) = 0$.

Soient a et b deux lettres. On dit qu'un élément $\theta \in \{a, b\}^N$ est normal si pour tout entier $s > 0$, les 2^s s -uples de $\{a, b\}^s$ apparaissent chacun avec la fréquence 2^{-s} dans la suite θ . Si l'on munit $\{a, b\}^N$ de la mesure habituelle (produit infini de la mesure de Bernoulli), on sait que

LEMME 3 (E. Borel). Presque tous les éléments de $\{a, b\}^N$ sont normaux.

On montre aussi les deux résultats suivants:

LEMME 4. Si $\delta \in \{-1, +1\}^N$ est normal, alors $\delta^{(p)} = \delta \cdot T^p \delta$ est normal, $p = 1, 2, \dots$ (voir [4]).

LEMME 5. Une suite normale $\delta \in \{-1, +1\}^N$ est pseudo-aléatoire (voir [4]).

Avant d'attaquer — à proprement parler — la démonstration, on établit la proposition suivante:

PROPOSITION. Soit $\delta \in \{-1, +1\}^N$ une suite normale. Soit φ un polynôme à coefficients réels. Alors

$$\lim_{n \rightarrow \infty} \frac{1}{n} \sum_{k=1}^n \delta_k \exp 2i\pi\varphi(k) = 0.$$

Ce résultat se montre par récurrence: si le degré du polynôme φ est 0, l'égalité découle des lemmes 1 et 5 par exemple.

Admettons la proposition pour des polynômes de degré $\nu - 1$ ($\nu \geq 1$ entier). Soit ψ un polynôme de degré ν :

Considérons la fonction f :

$$f(n) = \delta_n \exp 2i\pi\psi(n).$$

La moyenne

$$\limsup_{n \rightarrow \infty} \frac{1}{n} \left| \sum_{k=1}^n \overline{f(k)} f(k+p) \right|$$

s'écrit:

$$\limsup_{n \rightarrow \infty} \frac{1}{n} \left| \sum_{k=1}^n \delta_k \delta_{k+p} \exp 2i\pi(\psi(k+p) - \psi(k)) \right|.$$

Le lemme 4 montre que la suite $\delta \cdot T^p \delta$ est normale ($p = 1, 2, \dots$). Par ailleurs $\psi(\cdot + p) - \psi(\cdot)$ est un polynôme de degré $\nu - 1$ donc par hypothèse de récurrence, la moyenne est nulle. Enfin, du lemme 2, il découle que

$$\lim_{n \rightarrow \infty} \frac{1}{n} \sum_{k=1}^n \delta_k \exp 2i\pi\psi(k) = 0.$$

Soit $A \in \mathcal{S}$ et soit $\varepsilon(A)$ sa fonction caractéristique sur N . Il est bien clair que

$$\sum_{j=1}^{\lambda_n} \varepsilon_j(A) = n.$$

Supposons que $\varepsilon(A) \in \mathcal{D}$ soit normale. Alors les lemmes 1 et 5 impliquent que

$$\lim_{n \rightarrow \infty} \frac{1}{n} \sum_{k=1}^n (2\varepsilon_k(A) - 1) = 0.$$

Done

$$\frac{1}{\lambda_n} \sum_{k=1}^{\lambda_n} \varepsilon_k(A) = \frac{n}{\lambda_n} \rightarrow \frac{1}{2}.$$

Ainsi si $\varepsilon(A)$ est normale, alors $\lambda_n \sim 2n$.

LEMME 6. Soit φ un polynôme à coefficients réels et soit $A \in \mathcal{S}$. Si $\varepsilon(A)$ est normale, alors

$$B(\varphi(A)) = B(\varphi(N)).$$

En effet, soit x un nombre réel. Considérons la somme de Weyl

$$\sigma_n = \frac{1}{n} \sum_{j=1}^n \exp 2i\pi x \varphi(\lambda_j),$$

soit:

$$\sigma_n = \frac{1}{n} \sum_{j=1}^{\lambda_n} \varepsilon_j(\lambda) \exp 2i\pi x \varphi(j).$$

Comme $\varepsilon(\lambda)$ est par hypothèse normale, on a $\lambda_n \sim 2n$. Par ailleurs, la proposition établie au paragraphe précédent conduit à l'estimation

$$\frac{1}{\lambda_n} \sum_{j=1}^{\lambda_n} (2\varepsilon_j(\lambda) - 1) \exp 2i\pi x \varphi(j) = o(1).$$

Par suite

$$\sigma_n = \frac{1}{\lambda_n} \sum_{j=1}^{\lambda_n} \exp 2i\pi x \varphi(j) + o(1).$$

φ étant un polynôme, on sait que lorsque l'entier p tend vers l'infini, la moyenne

$$\frac{1}{p} \sum_{j=1}^p \exp 2i\pi x \varphi(j)$$

tend vers une limite. Donc:

$$\sigma_n = \lim_{p \rightarrow \infty} \frac{1}{p} \sum_{j=1}^p \exp 2i\pi x \varphi(j) + o(1).$$

Cette égalité prouve bien la double implication

$$x \in B(\varphi(N)) \Leftrightarrow x \in B(\varphi(\lambda)), \quad \text{C.Q.F.D.}$$

En particulier, si φ est un polynôme non constant défini de \mathbf{Z} dans \mathbf{Z} , on sait que $B(\varphi(N)) = \mathbf{R} - \mathbf{Q}$. Cette remarque, associée aux lemmes 3 et 6, prouve le théorème 2.

Travaux cités

- [1] J. Bass, *Suites uniformément denses, moyennes trigonométriques, fonctions pseudo-aléatoires*, Bull. Soc. Math. France, 87 (1959), p. 1-69.
- [2] J. P. Bertrandias, *Suites pseudo-aléatoires et critères d'équirépartition modulo un*, Compositio Math. 16 (1965), p. 23-28.
- [3] J. Cigler, *The fundamental theorem of Van der Corput on uniform distribution and its generalizations*, Compositio Math. 16 (1965), p. 29-34.
- [4] M. Mendès France, *Nombres normaux. Applications aux fonctions pseudo-aléatoires*, Journal d'Analyse Math. 20 (1967), p. 1-56.

Reçu le 26. 7. 1969

A note on the least prime in an arithmetic progression with a prime difference

by

YOICHI MOTOHASHI (Tokyo)

Let $P(k, l)$ be the least prime in the arithmetic progression $n \equiv l \pmod{k}$, where $(k, l) = 1$. The estimate of $P(k, l)$ is one of the most important problems in the theory of numbers, and so many results have been obtained. But it seems that the following fact has not been observed before.

THEOREM. For any fixed l there exist infinitely many primes q such that

$$P(q, l) < c(\varepsilon) q^{\vartheta + \varepsilon},$$

where $\vartheta = 2e^{1/4}(2e^{1/4} - 1)^{-1} = 1.63773\dots$

We will prove this in detail only in the case $l = 1$, but the general case is merely an easy extension.

Let us consider the product

$$\prod_{p \leq N} (p-1),$$

where p runs over all primes not exceeding large N . Defining $\pi(N, k)$ to be the number of primes not exceeding N and $\equiv 1 \pmod{k}$, we have

$$(1) \quad \sum_{q^a < N} \pi(N, q^a) \log q = \sum_{p \leq N} \log p + O\left(\sum_{p \leq N} p^{-1}\right) \\ = N + O(N \exp(-c(\log N)^{1/2})),$$

where the sum of the left side is taken over prime q and integer $a \geq 1$.

Now

$$(2) \quad \sum_{q^a < N} \pi(N, q^a) \log q \\ = \left\{ \sum_{\substack{q \leq N^{1/2}(\log N)^{-B} \\ a=1}} + \sum_{\substack{N^{1/2}(\log N)^{-B} < q \leq N^{\frac{1}{2}} \\ a=1}} + \sum_{\substack{N^{\frac{1}{2}} < q < N \\ a=1}} + \sum_{\substack{q^a < N \\ a \geq 2}} \right\} \pi(N, q^a) \log q \\ = \Sigma_1 + \Sigma_2 + \Sigma_3 + \Sigma_4, \text{ say,}$$