MATH. SCAND. 39 (1976), 251–266

# GENERALISATIONS DE CERTAINS THEOREMES DE ERDÖS–RENYI SUR LA THEORIE ADDITIVE DES NOMBRES[1]

NICOLAS SPALTENSTEIN

**Notations.**

Sauf indication contraire, nous appellerons « entiers » les éléments de $\mathsf{N}^*$.

Si $A$ et $B$ sont des sous-ensembles de $\mathsf{N}^*$, nous noterons:

$$\begin{aligned} s_n(A) &= \operatorname{Card}\{k \mid k \in A,\ k \leqq n\} \\ r_n(A,B) &= \operatorname{Card}\{(a,b) \mid (a,b) \in A \times B,\ a+b=n\} \\ r'_n(A,B) &= \operatorname{Card}\{(a,b) \mid (a,b) \in (A \times B) \cup (B \times A),\ a \leqq b,\ a+b=n\} \\ A+B &= \{a+b \mid a \in A,\ b \in B\}\,. \end{aligned}$$

De plus, si $p$ et $i \geqq 0$ sont des entiers, notons:

$$\begin{aligned} (p)A &= \{pa \mid a \in A\} \\ A_{p,i} &= \{a \in A \mid a \equiv i \pmod p\} \end{aligned}$$

Nous dirons que $A$ et $B$ sont compléments asymptotiques et nous noterons $A + B \sim \mathsf{N}^*$, si $\liminf_{n\to\infty} r_n(A,B) \neq 0$. Nous dirons que $A$ est une base asymptotiques si $A+A \sim \mathsf{N}^*$. Soient $E$ un ensemble et $A$ un sous-ensemble de $E$. Nous noterons $\varphi_A$ la fonction caractéristique du sous-ensemble $A$ de $E$, c'est-à-dire $\varphi_A(x)=1$ si $x \in A$, 0 si $x \in C_E A$.

Si $f$ et $g$ sont des applications de $\mathsf{N}^*$ dans $\mathsf{R}$, nous noterons $f(n) \ll g(n)$ (pour $n \to \infty$) s'il existe $c>0$ et un entier $n_0$ tels que $|f(n)| \leqq c|g(n)|$ pour tout entier $n \geqq n_0$.

## 1. Introduction.

Des théorèmes affirmant l'existence de sous-ensembles de $\mathsf{N}^*$ possédant certaines propriétés additives peuvent être démontrés par des méthodes probabilistes.

---

Reçu Septembre 5, 1975.

[1] Une partie des résultats ont été obtenus lors d'un travail de semestre à l'Ecole Polytechnique Fédérale de Lausanne.

En particulier, Erdös a démontré (voir [1]):

a) Il existe une base asymptotique $A$ telle que

$$\log n \ll r'_n(A, A) \ll \log n \quad \text{pour } n \to \infty .$$

Et Erdös et Rényi ont demontré ([2]):

b) Pour tout $\varepsilon > 0$, il existe un entier $g$ et une suite d'entiers $a_1 < a_2 < a_3 < \dots$ tels que:

i) $a_j \ll j^{2+\varepsilon}$

ii) $r'_n(\{a_1, a_2, \dots\}, \{a_1, a_2, \dots\}) \leqq g$ pour tout $n$.

On trouvera la démonstration de ces deux théorèmes dans l'ouvrage de Halberstam et Roth [3].

Je démontrerai d'abord le résultat suivant:

THEOREME 1. *Soit $\varphi$ l'une des fonctions* log, loglog, logloglog,.... *Il existe une base asymptotique $A$ telle que, si $p$ et $q$ sont des entiers premiers entre eux, et si $i$ et $j$ sont des entiers $\geqq 0$, on a*:

$$r_n((p)A, (q)A) \sim (pq)^{-\frac{1}{2}} \log n\varphi(n) \quad \textit{pour } n \to \infty$$

$$r_n(A_{p,i}, A_{q,j}) \sim (pq)^{-1} \log n\varphi(n) \quad \textit{pour } n \to \infty .$$

REMARQUE. Une première formulation était:

$$\log n\varphi(n) \ll r'_n(A) \ll \log n\varphi(n) \quad \text{pour } n \to \infty ,$$

$$(p)A + (q)A \sim \mathbf{N}^* \text{ et } A(p,i) + A(q,j) \sim \mathbf{N}^* \quad (\text{pour } (p,q) = 1) .$$

C'est à la suite d'une suggestion de M. le Professeur P. Erdös (à savoir qu'il devait être possible d'avoir $r'_n(A) \sim \log n\varphi(n)$) que le résultat a été mis sous la forme donnée ici.

Une légère modification des démonstrations de a) et b) telles qu'elles sont données dans [3], ainsi que de la démonstration du théorème 1 donnée ci-dessous, permet d'étendre ces résultats à des partitions de $\mathbf{N}^*$. On trouve ainsi:

THEOREME 2. *Il existe une partition $(A_i)_{i \geqq 1}$ de $\mathbf{N}^*$ en bases asymptotiques telles que*:

$$\forall i, j \in \mathbf{N}^*, \log n \ll r'_n(A_i, A_j) \ll \log n \quad \textit{pour } n \to \infty .$$

THEOREME 3. *Pour tout $\varepsilon > 0$, il existe un entier $g$ et une partition $(A_i)_{i \geqq 1}$ de $\mathbf{N}^*$ tels que*:

i) $\forall i \in \mathbf{N}^*$, *si* $A_i$ *est l'ensemble des points de la suite* $a_1 < a_2 < a_3 < \ldots$, *on a* $a_j \ll j^{2+\varepsilon}$

ii) $\forall k \in \mathbf{N}^*$, $\limsup_{n\to\infty} r'_n(\bigcup_{i=1}^k A_i, \bigcup_{i=1}^k A_i) \leqq g$.

THEOREME 4. *Soit* $\varphi$ *l'une des fonctions* log, log log, log log log, .... *Il existe une partition* $(A_i)_{i \geqq 1}$ *de* $\mathbf{N}^*$ *en bases asymptotiques telles que, si* $A$ *et* $B$ *sont des ensembles quelconques de la partition et si* $p, q, i \geqq 0, j \geqq 0$ *sont des entiers tels que* $(p, q) = 1$, *on ait*:

i) $r_n((p)A, (q)B) \sim (pq)^{-\frac{1}{2}} \log n\varphi(n)$ *pour* $n \to \infty$

ii) $r_n(A_{p,i}, B_{q,j}) \sim (pq)^{-1} \log n\varphi(n)$ *pour* $n \to \infty$.

Le pas suivant consiste à construire une famille $(\Pi_t)_{t\in D}$ de partitions de $\mathbf{N}^*$, où $D$ est un sous-ensemble dénombrable de $]0, 1[$, de telle sorte que des propriétés analogues à celles des théorèmes 2 à 4 soient vérifiées pour chaque partition $\Pi_t$ et entre les diverses partitions. On pose alors

$$d(x, y) = \inf\{t \mid x \equiv y \pmod{\Pi_t}\} .$$

Une telle construction peut être faite de telle sorte que $d$ soit une distance pour laquelle les boules ont des propriétés additives convenables.

THEOREME 5. *Soit* $D$ *un sous-ensemble dénombrable dense dans* $]0, 1[$, *symétrique par rapport à* $\frac{1}{2}$. *Soit* $\theta: \mathbf{N}^* \to ]0, \infty[$ *une fonction croissante divergente. Alors il existe une distance ultramétrique sur* $\mathbf{N}^*$, *pour laquelle le diamètre de* $\mathbf{N}^*$ *vaut* 1, *et qui vérifie les propriétés suivantes*:

1°) *Si* $B$ *est une boule ouverte ou fermée de rayon* $r \in ]0, 1]$ *on a pour tout* $\varepsilon > 0$: $n^{r-\varepsilon} \ll s_n(B) \ll n^{r+\varepsilon}$ *pour* $n \to \infty$.

2°) *Si* $r \in ]0, 1] \backslash D$, *les boules ouvertes de rayon* $r$ *sont égales aux boules fermées correspondantes.*

3°) *Si* $A$ *et* $B$ *sont deux boules (ouvertes ou fermées) de rayons respectifs* $r, s \in ]0, 1]$, *on a*:

i) $r + s < 1 \Rightarrow \limsup_{n\to\infty} r'_n(A, B) \leqq 1/(1 - r - s)$

ii) $r + s > 1 \Rightarrow A + B \sim \mathbf{N}^*$

iii) *si* $r, s \in D$ *et si* $A$ *et* $B$ *sont des boules fermées, on a*:
$r + s = 1 \Rightarrow \log n \ll r'_n(A, B) \ll \log n$ *pour* $n \to \infty$

iv) *si* $A$ *ou* $B$ *est une boule ouverte, on a*:
$r + s = 1 \Rightarrow r'_n(A, B) \ll \theta(n)$ *pour* $n \to \infty$.

Le théorème 5 est susceptible de nombreuses variantes.

## 2. Correspondance entre suites entières et espaces de probabilité.

Soient, pour tout $i \in \mathbf{N}^*$, $(\Omega_i, \Sigma_i, P_i)$ un espace de probabilité et $E_i$ un sous-ensemble $\Sigma_i$-measurable de $\Omega_i$. Considérons l'espace de probabilité $(\Omega, \Sigma, P)$ produit de la famille $(\Omega_i, \Sigma_i, P_i)_{i \geqq 1}$. A tout $\omega = (\omega_1, \omega_2, \ldots) \in \Omega$, on peut faire correspondre un sous-ensemble $A(\omega)$ de $\mathbf{N}^*$ tel que $\varphi_{A(\omega)}(i) = \varphi_{E_i}(\omega_i)$ pour tout entier $i$, c'est-à-dire:

$$A(\omega) = \{i \mid \omega_i \in E_i\} .$$

Par la suite, c'est toujours à l'espace $(\Omega, \Sigma, P)$ qu'il sera fait référence, et lorsque des sous-ensembles de $\mathbf{N}^*$ seront associés aux éléments de $\Omega$, ce sera toujours de la manière décrite ci-dessus.

Supposons maintenant que pour chaque entier $i$, nous avons une partition de $\Omega_i$ en ensembles $\Sigma_i$-mesurables:

$$\Omega_i = \bigcup_{n=1}^{\infty} E(i,n), \qquad E(i,n) \cap E(i,m) = \emptyset \qquad \text{si } m \neq n .$$

Soit, pour tout entier $n$ et tout $\omega \in \Omega$, $A_n(\omega)$ le sous-ensemble de $\mathbf{N}^*$ déduit de la suite $(E(i,n))_{i \geqq 1}$. Alors pour tout $\omega \in \Omega$ les ensembles $A_n(\omega)$ forment une partition de $\mathbf{N}^*$:

$$\mathbf{N}^* = \bigcup_{n=1}^{\infty} A_n(\omega), \qquad A_n(\omega) \cap A_m(\omega) = \emptyset \qquad \text{si } m \neq n .$$

Soit, pour tout $i \in \mathbf{N}^*$, $(F(i,n))_{n \geqq 1}$ une seconde partition de $\Omega_i$ en sous-ensembles $\Sigma_i$-mesurables. On suppose qu'il existe une partition $(J_n)_{n \geqq 1}$ de $\mathbf{N}^*$ telle que:

$$\forall i, n \in \mathbf{N}^*, \qquad E(i,n) = \bigcup_{j \in J_n} F(i,j) .$$

Soit pour tout entier $n$ et pour tout $\omega \in \Omega$, $B_n(\omega)$ le sous-ensemble de $\mathbf{N}^*$ déduit de $(F(i,n))_{i \geqq 1}$. Alors, pour tout $\omega \in \Omega$, la partition $(B_n(\omega))_{n \geqq 1}$ de $\mathbf{N}^*$ est plus fine que $(A_n(\omega))_{n \geqq 1}$.

## 3. Démonstration des théorèmes 1 à 4.

*Dans tout ce paragraphe, nous supposerons donnés pour tout entier i deux sous-ensembles $\Sigma_i$-mesurables $E_i$ et $F_i$ de $\Omega_i$, et nous noterons $\alpha_i = P_i(E_i)$, $\beta_i = P_i(F_i)$. $A(\omega)$ et $B(\omega)$ (ou A et B, si aucune confusion n'est à craindre) seront les sous-ensembles de $\mathbf{N}^*$ déduits respectivement des suites $(E_i)_{i \geqq 1}$ et $(F_i)_{i \geqq 1}$. Nous noterons $s_n$ (resp. $r_n, r_n'$) l'application: $\Omega \to \mathbf{R}$, définie par $s_n(\omega) = s_n(A(\omega))$ (resp. $r_n(\omega) = r_n(A(\omega), B(\omega))$, $r_n'(\omega) = r_n'(A(\omega), B(\omega))$).*

*Soient, pour* $i<n$, $f_{i,n}$ *la fonction definie par*

$$f_{i,n}(\omega) = \varphi_{E_i}(\omega_i)\varphi_{F_{n-i}}(\omega_{n-i}), \qquad où\ \omega = (\omega_1, \omega_2, \ldots)\,,$$

*et* $g_{i,n} = \max(f_{i,n}, f_{n-i,n})$. *Posons enfin*:

$$m_n = \sum_{k=1}^{n} \alpha_k$$

$$\lambda_n = \sum_{k\leqq n/2} E(g_{k,n})$$

$$\lambda'_n = \sum_{k\leqq n/2} \frac{E(g_{k,n})}{1-E(g_{k,n})} \qquad si\ E(g_{k,n})<1\ pour\ tout\ entier\ k\leqq n/2\,.$$

Si $\alpha_n \to 0$ et $\beta_n \to 0$, $\lambda'_n$ est toujours défini pour $n$ assez grand, et $\lambda_n \sim \lambda'_n$. $s_n$, $r_n$ et $r'_n$ sont des variables aléatoires sur $(\Omega, \Sigma, P)$. Pour $i \neq j$, les événements $\{i \in A(\omega)\}$ et $\{j \in B(\omega)\}$ sont indépendants. Pour tout entier $n$, on a $m_n = E(s_n)$, $\lambda_n = E(r'_n)$.

Tous les lemmes de ce paragraphe, à l'exception du lemme 5, sont donnés sans démonstration. Les démonstrations sont essentiellement les mêmes que celles données par Halberstam et Roth pour les résultats correspondants dans [3].

LEMME 1 (voir [3, lemme 10, p. 144]). *Supposons que* $m_n \to \infty$. *Alors* $s_n(\omega) \sim m_n$ *presque sûrement.*

LEMME 2 (voir [3, lemme 14, p. 148]). *Soient* $f_1, f_2, \ldots, f_m$ *des variables aléatoires indépendantes ne prenant que les valeurs* 0 *et* 1, *et telles que* $E(f_i)<1$ $(1 \leqq i \leqq m)$. *Soient*:

$$L = \sum_{i=1}^{m} E(f_i)$$

$$L' = \sum_{i=1}^{m} \frac{E(f_i)}{1-E(f_i)}\,.$$

*Alors pour tout entier* $d \geqq 0$, *on a*:

$$P\left(\sum_{i=1}^{m} f_i = d\right) \leqq e^{-L}\frac{(L')^d}{d!}\,.$$

COROLLAIRE. *Si* $\lambda'_n$ *est défini, on a pour tout entier* $d \geqq 0$:

$$P(r'_n = d) \leqq e^{-\lambda_n}\frac{(\lambda'_n)^d}{d!}\,.$$

LEMME 3 (voir [3, lemme 11, p. 144]). *Soient* $\varphi$ *l'une des fonctions* log, log log, log log log,... *et* $\alpha$, $\beta$, $c$, $c'$, $c''$, $d$, $d'$, $d''$, $\varrho$, *des constantes telles que*: $\alpha>0$, $\beta>0$, $0<c<1$, $0<d<1$, $c'\geqq 0$, $d'\geqq 0$, $c''\geqq 0$, $d''\geqq 0$, $0\leqq\varrho\leqq 1$. *On suppose que pour* $i\to\infty$:

$$\alpha_i \sim \alpha\frac{(\log i)^{c'}(\varphi(i))^{c''}}{i^c}, \qquad \beta_i \sim \beta\frac{(\log i)^{d'}(\varphi(i))^{d''}}{i^d}.$$

*Alors, pour* $n\to\infty$:

i) $$\sum_{k<\varrho n}\alpha_k\beta_{n-k} \sim \alpha\beta\left(\int_0^\varrho t^{-c}(1-t)^{-d}\,dt\right)\frac{(\log n)^{c'+d'}(\varphi(n))^{c''+d''}}{n^{c+d-1}}$$

ii) $$m_n \sim \frac{\alpha}{1-c}(\log n)^{c'}(\varphi(n))^{c''}n^{1-c}.$$

iii) *Si* $A=\{a_1,a_2,\dots\}$ *avec* $a_1<a_2<\dots$, *et si* $c'=c''=0$, *on a presque sûrement*:

$$a_j \sim \left(\frac{1-c}{\alpha}j\right)^{1/(1-c)} \qquad \textit{pour } j\to\infty.$$

LEMME 4 (voir [3, lemme 17, p. 149]). *Si* $0<v\leqq x\leqq u$, *alors*

i) $$\sum_{d\geqq u}\frac{x^d}{d!}\leqq\left(\frac{ex}{u}\right)^u$$

ii) $$\sum_{d\leqq v}\frac{x^d}{d!}\leqq\left(\frac{ex}{v}\right)^v.$$

LEMME 5. *Soit* $\varphi$ *l'une des fonctions* log, log log, log log log,.... *Supposons que pour* $i\to\infty$:

$$\alpha_i \sim \alpha\frac{(\log i)^{c'}(\varphi(i))^{c''}}{i^c}$$

$$\beta_i \sim \beta\frac{(\log i)^{d'}(\varphi(i))^{d''}}{i^d}$$

*où* $\alpha$, $\beta$, $c$, $c'$, $c''$, $d$, $d'$, $d''$, *sont des constantes telles que* $\alpha>0$, $\beta>0$, $0<c<1$, $c+d=1$, $c'\geqq 0$, $d'\geqq 0$, $c'+d'=1$, $c''\geqq 0$, $d''\geqq 0$, $c''+d''=1$, *et soit*

$$k = \alpha\beta\int_0^1 t^{-c}(1-t)^{-d}\,dt.$$

*Alors, pour presque tout* $\omega\in\Omega$, *si* $p$, $q$, $i\geqq 0$, $j\geqq 0$ *sont des entiers tels que* $(p,q)=1$, *on a*:

i) $r_n((p)A, (q)B) \sim kp^{-d}q^{-c}\log n\varphi(n)$

ii) $r_n(A_{p,i}, B_{q,j}) \sim k(pq)^{-1}\log n\varphi(n)$ .

Demonstration. Il suffit de démontrer que i) et ii) sont vraies avec probabilité 1.

a) la propriété i) est vraie presque sûrement. Soient $p$ et $q$ deux entiers avec $(p,q)=1$. Considérons un entier $n$. Soit $\varrho_n$ (resp. $\varrho_n'$) le nombre de décompositions $n=px+qy$ où $x \in A$, $y \in B$, avec $x<y$ (resp. $y<x$). Considérons deux nombres $x_0, y_0$ tels que $1 \leqq x_0 \leqq q$, $1 \leqq y_0 \leqq p$, et posons $i_0=px_0+qy_0$. Nous allons considérer les nombres entiers $n \geqq i_0$ tels que $n \equiv i_0 \pmod{pq}$.

Soit $n$ un tel nombre. Il existe un unique entier $\mu \geqq 0$ tel que $n=i_0+\mu pq$. Les solutions entières de l'équation $n=px+qy$ sont

$$x = x_0+\nu q, \qquad y = y_0+(\mu-\nu)p, \qquad 0 \leqq \nu \leqq \mu .$$

La condition $x<y$ devient

$$\nu < \mu\frac{p}{p+q}+\frac{y_0-x_0}{p+q} .$$

Posons, pour $\nu \geqq 0$, $\mu \geqq 0$:

$$\bar{\alpha}_\nu = \alpha_{x_0+\nu q}, \qquad \bar{\beta}_\nu = \beta_{y_0+\nu p} ,$$

$$\bar{\lambda}_\mu = \sum_{\nu<M_\mu} \bar{\alpha}_\nu \bar{\beta}_{\mu-\nu}$$

$$\bar{\lambda}_\mu' = \sum_{\nu<M_\mu} \frac{\bar{\alpha}_\nu \bar{\beta}_{\mu-\nu}}{1-\bar{\alpha}_\nu \bar{\beta}_{\mu-\nu}}$$

où $M_\mu=(p\mu+y_0-x_0)/(p+q)$. En appliquant le lemme 2, on trouve

$$(1) \qquad P(\varrho_{i_0+\mu pq}=d) \leqq e^{-\bar{\lambda}_\mu}\frac{(\bar{\lambda}_\mu')^d}{d!} .$$

Or on déduit facilement du lemme 3 que

$$(2) \qquad \bar{\lambda}_\mu \sim \bar{\lambda}_\mu' \sim \alpha\beta p^{-d}q^{-c}\left(\int_0^{p/(p+q)} t^{-c}(1-t)^{-d}\,dt\right)\log\mu\,\varphi(\mu) .$$

Il suffit maintenant de montrer, pour prouver que i) est vraie presque sûrement, que pour tout $\varepsilon>0$, les séries

$$(3) \qquad \sum_{\mu=0}^{\infty} P(\varrho_{i_0+\mu pq} > (1+\varepsilon)\bar{\lambda}_\mu')$$

$$(4) \qquad \sum_{\mu=0}^{\infty} P(\varrho_{i_0+\mu pq} < (1-\varepsilon)\bar{\lambda}'_\mu)$$

sont convergentes, car alors $\varrho_n + \varrho'_n \sim kp^{-d}q^{-c}\log(n)\varphi(n)$ presque sûrement, d'où le résultat cherché.

En appliquant (1) et le lemme 4, on trouve

$$P(\varrho_{i_0+\mu pq} > (1+\varepsilon)\bar{\lambda}'_\mu) = \sum_{d>(1+\varepsilon)\bar{\lambda}'_\mu} P(\varrho_{i_0+\mu pq} = d)$$

$$\leqq e^{-\bar{\lambda}_\mu} \sum_{d>(1+\varepsilon)\bar{\lambda}'_\mu} \frac{(\bar{\lambda}'_\mu)^d}{d!} \leqq e^{-\bar{\lambda}_\mu}\left(\frac{e}{1+\varepsilon}\right)^{(1+\varepsilon)\bar{\lambda}'_\mu}.$$

D'où, en appliquant (2):

$$\log\left(P(\varrho_{i_0+\mu pq} > (1+\varepsilon)\bar{\lambda}'_\mu)\right) \leqq -2(1+o(1))\log\mu$$

ce qui assure la convergence de la série (3). La convergence de la série (4) se démontre de façon similaire.

b) On démontre de façon similaire que ii) est vraie presque sûrement.

Demonstration du theoreme 1. On prend pour $(\Omega_i, \Sigma_i, P_i)$ l'intervalle $[0,1]$ muni de la mesure de Lebesgue sur les boréliens. Soit

$$\alpha = \pi^{-\frac{1}{2}} = \left(\int_0^1 (t(1-t))^{-\frac{1}{2}}\,dt\right)^{-\frac{1}{2}},$$

et soit $i_0$ assez grand pour que $\varphi(i_0)$ soit défini et positif. On prend:

$$E_i = F_i = \left[0, \alpha\left(\frac{\log i\varphi(i)}{i}\right)^{\frac{1}{2}}\right] \cap [0,1] \qquad \text{pour } i \geqq i_0$$

$$E_i = F_i = \varnothing \qquad \text{pour } i < i_0 .$$

On a alors $A(\omega) = B(\omega)$ pour tout $\omega$. Le lemme 5 s'applique et permet d'affirmer que pour presque tout $\omega \in \Omega$, $A(\omega)$ vérifie les propriétés désirées, ce qui démontre le théorème.

Lemme 6 (voir [3, preuve du théorème 1, p. 150]). *Supposons qu'il existe une constante $\gamma > 1$ telle que pour $n \to \infty$, $\lambda_n \sim \lambda'_n \sim \gamma \log n$. Alors, pour $n \to \infty$, on a*

$$\log n \ll r_n(\omega) \ll \log n \quad \text{presque sûrement}.$$

Lemme 7 (voir [3, preuve du théorème 2, p. 151]). *Soit $\delta > 0$ un nombre réel, et soit $\varphi$ l'une des fonctions* log, loglog, logloglog ... *Supposons que*

$$\lambda_n \sim \lambda'_n \sim k(\log n)^{c'}(\varphi(n))^{c''}n^{-\delta} \qquad \textit{pour } n \to \infty,$$

*où* $c' \geqq 0$, $c'' \geqq 0$, $k > 0$ *sont des constantes arbitraires. Soit* $K$ *un entier tel que* $K\delta > 1$. *Alors la série*:

$$\sum_{n=1}^{\infty} P(r'_n \geqq K)$$

*est convergente.*

Nous pouvons maintenant démontrer les théorèmes 2 à 4. Pour cela, nous partirons chaque fois de la même construction:

CONSTRUCTION (I) soit, pour tout entier $i$, $(\Omega_i, \Sigma_i, P_i)$ l'intervalle $[0,1]$ muni de la mesure de Lebesgue sur les boréliens. Soit $(a_i)_{i \geqq 1}$ une suite de nombres réels strictement positifs. Posons, pour tout entier $i$ et pour tout entier $n$:

$$E(i,n) = [(n-1)a_i, na_i[ \cap [0,1] .$$

Pour tout $\omega \in \Omega$ et pour tout entier $n$, soit $A_n(\omega)$ le sous-ensemble de $\mathbf{N}^*$ associé à la suite $(E(i,n))_{i \geqq 1}$. Alors pour tout $\omega \in \Omega$, la famille $(A_n(\omega))_{n \geqq 1}$ est une partition de $\mathbf{N}^*$.

DEMONSTRATION DU THEOREME 2. On considère la construction (I) où les nombres $(a_i)_{i \geqq 1}$ sont choisis de telle sorte que:

$$a_i \sim \left(\frac{\log i}{i}\right)^{\frac{1}{2}} .$$

Comme $\frac{1}{2}\int_0^1 (t(1-t))^{-\frac{1}{2}} dt = \frac{1}{2}\pi > 1$, le lemme 3 montre que le lemme 6 s'applique à $A_m(\omega)$, $A_n(\omega)$ pour $m, n \in \mathbf{N}^*$. Comme il n'y a qu'un nombre dénombrable de couples $(m,n) \in \mathbf{N}^* \times \mathbf{N}^*$, on en déduit que pour presque tout $\omega \in \Omega$, la partition $(A_n(\omega))_{n \geqq 1}$ de $\mathbf{N}^*$ remplit les conditions désirées, ce qui démontre le théorème.

DEMONSTRATION DU THEOREME 3. Considérons la construction (I) où:

$$a_i = i^{((2+\varepsilon)^{-1}-1)} .$$

Les lemmes 1 et 3 indiquent que si $m \in \mathbf{N}^*$ et si $A_m(\omega) = \{b_1, b_2, \ldots\}$ avec $b_1 < b_2 < \ldots$, on a pour presque tout $\omega \in \Omega$,

$$b_j \sim (j/(2+\varepsilon))^{2+\varepsilon} \ll j^{2+\varepsilon} .$$

Soient maintenant $\delta = \varepsilon/(2+\varepsilon)$ et $g$ un entier tel que $(g+1)\delta > 1$.

Si $k$ est un entier quelconque, on a:

$$P\left(i \in \bigcup_{j \leqq k} A_j(\omega)\right) \sim k i^{((2+\varepsilon)^{-1}-1)} \quad \text{pour } i \to \infty .$$

Les lemmes 3 et 7 montrent alors que pour presque tout $\omega \in \Omega$, la partition $(A_n(\omega))_{n \geqq 1}$ vérifie les conditions désirées.

DEMONSTRATION DU THEOREME 4. Soit $\alpha = \pi^{-\frac{1}{2}}$, et considérons la construction (I) dans le cas où:

$$a_i \sim \alpha \left( \frac{\log i\varphi(i)}{i} \right)^{\frac{1}{2}} \quad \text{pour } i \to \infty .$$

Le lemme 5 montre que pour presque tout $\omega \in \Omega$, la partition $(A_n(\omega))_{n \geqq 1}$ de $\mathbf{N}^*$ remplit les conditions désirées.

## 4. Démonstration du théorème 5.

Soit $(c_i)_{i \geqq 1}$ une famille de points distincts de $]0,1[$. Soient $l, m$ et $n$ des entiers (resp. $m$ et $n$; $l$ et $n$).

Nous considérerons par la suite la condition (I) ci-dessous (resp. (II); (III)):

$$\text{(I)} \quad \begin{aligned} & l < m,\ n < m, \\ & c_l < c_m < c_n \\ & c_l = \max \{c_h \mid c_h < c_m,\ h < m\} \\ & c_n = \min \{c_h \mid c_h > c_m,\ h < m\} \end{aligned}$$

$$\text{(II)} \quad \begin{aligned} & n < m,\ c_m < c_n, \\ & c_n = \min \{c_h \mid h < m\} \end{aligned}$$

$$\text{(III)} \quad \begin{aligned} & c_l < c_n, \\ & c_l = \max \{c_h \mid c_h < c_n,\ h \leqq \max (l, n)\} \\ & c_n = \min \{c_h \mid c_h > c_l,\ h \leqq \max (l, n)\} . \end{aligned}$$

LEMME 8. *Soit* $(c_i)_{i \geqq 1}$ *une famille de points distincts de* $]0,1[$ *telle que* $C = \{c_1, c_2, c_3, \ldots\}$ *soit dense dans* $[0,1]$. *On suppose que pour tout élément* $c \in C$, *on a aussi* $1 - c \in C$. *Si* $l, m$ *et* $n$ *sont des entiers vérifiant la condition* (I), *on suppose que* $2c_m > c_l + c_n$, *et si* $m$ *et* $n$ *vérifient la condition* (II), *on suppose que* $2c_m > c_n$ *et que* $c_m + c_p < 1$ *pour tout entier* $p \leqq m$. *De plus, si* $c_m = \max \{c_h \mid h \leqq m\}$, *alors il existe* $p \leqq m$ *tel que* $c_m + c_p > 1$. *Soit* $\theta: \mathbf{N}^* \to\ ]0, \infty[$ *une fonction croissante telle que* $\lim_{n \to \infty} \theta(n) = \infty$.

*Pour tout entier* $m$, *soit* $\psi_m: \mathbf{N}^* \to \mathbf{R}$, *la fonction définie par*:

$$\psi_m(i) = \begin{cases} 1 & si\ i = 1 \\ \left( \dfrac{\log i}{i} \right)^{c_m} & si\ i \neq 1 \end{cases}$$

*Alors il existe une famille d'espaces de probabilité* $(\Omega_i, \Sigma_i, P_i)_{i \geq 1}$, *des ensembles* $A(i,k,m)$ *($i,k,m$ entiers), et une suite d'entiers* $R_1 < R_2 < R_3 < \dots$ *tels que:*

(a) *Pour tout entier $i$ et pour tout entier $m$, la famille* $(A(i,k,m))_{k \geq 1}$ *est une partition de* $\Omega_i$ *en sous-ensembles* $\Sigma_i$*-mesurables. Si* $P_i(A(i,k,m)) = 0$, *alors* $A(i,k,m) = \varnothing$. *L'ensemble* $J_{i,m} = \{k \mid A(i,k,m) \neq \varnothing\}$ *est fini.*

b) *Pour tout couple $(l,n)$ d'entiers vérifiant la condition* (III), *il existe une partition* $(J_k)_{k \geq 1}$ *de* $\mathbf{N}^*$ *telle que:*

$$\forall i \in \mathbf{N}^*, \ \forall k \in \mathbf{N}^*, \qquad A(i,k,l) = \bigcup_{j \in J_k} A(i,j,n) .$$

*On a de plus pour tout $k \in \mathbf{N}^*$, les propriétés suivantes: Notons* $J = J_k$ *et*

$$I_i = \{j \in J \mid A(i,j,n) \neq \varnothing\} .$$

*Soit* $I'_i$ *l'ensemble* $I_i$ *privé de son plus grand élément. Alors il existe un entier* $i_0$ *et une fonction* $i \mapsto \varepsilon(i) > 0$ *définie pour* $i \geq i_0$, *avec* $\lim_{i \to \infty} \varepsilon(i) = 0$, *tels que:*

1°) $I_{i_0} = \bigcup_{i \leq i_0} I_i$.

2°) *Pour* $i \geq i_0$, *on a* $I_i = I_{i+1}$ *ou* $I_i = I'_{i+1}$. *Soit, pour* $i \geq i_0$, $N(i) = \mathrm{Card}\,(I_i)$. *Alors:*

$$\left| N(i) - \frac{\psi_l(i)}{\psi_n(i)} \right| \leq 3 \qquad \forall i \geq i_0 .$$

3°) *Pour* $i \geq i_0$ *et* $j \in I_i$, *on a:*

$$P_i(A(i,j,n)) \leq (1 + \varepsilon(i)) \psi_n(i) .$$

4°) *Pour* $i \geq i_0$ *et* $j \in I'_i$, *on a:*

$$P_i(A(i,j,n)) \geq (1 - \varepsilon(i)) \psi_n(i) .$$

c) *Si l'on a:* $c_m = \max\{c_h \mid h \leq m\}$, *alors*

$$P(A(i,k,m)) \leq \frac{1}{m} \qquad \text{pour tout entier } i \leq m .$$

d) *Si* $c_n = \min\{c_h \mid h \leq n\}$, *alors:*

$$A(i,1,n) = \Omega_i \qquad \text{pour tout entier } i \leq n .$$

*Soit* $I_i = \{k \mid A(i,k,n) \neq \varnothing\}$, *et soit* $I'_i$ *l'ensemble* $I_i$ *privé de son plus grand élément. Alors il existe un entier* $i_0$ *et une fonction* $i \mapsto \varepsilon(i) > 0$, *avec* $\lim_{i \to \infty} \varepsilon(i) = 0$, *tels que les relations* 1°) *à* 4°) *du point* b) *soient vérifiées (en remplaçant* $\psi_l(i)$ *par* 1 *dans* 2°)).

e) *Soit* $(\Omega, \Sigma, P)$ *l'espace de probabilité produit de la famille* $(\Omega_i, \Sigma_i, P_i)_{i \geq 1}$.

*Pour tout $\omega \in \Omega$, notons $A(k,m)(\omega)$ le sous-ensemble de $\mathbf{N}^*$ correspondant à la famille $(A(i,k,m))_{i \geqq 1}$.*

*Si $p$ et $q$ sont deux entiers, notons:*

$$K(p,q) = \bigcup_{i \leqq q} \{k \mid A(i,k,p) \neq \emptyset\}$$

*Alors, si $m$ est un entier tel qu'il existe un entier $u \leqq m$ avec $c_u + c_m > 1$, on a les propriétés suivantes:*

1°) *Soit $B_i = \bigcup_{k \in K(v,m)} A(i,k,v)$ où $v$ est l'unique entier tel que*

$$c_v = \min\{c_u \mid c_u + c_m > 1, u \leqq m\} .$$

*Soit, pour tout $\omega \in \Omega$, $B(\omega)$ le sous ensemble de $\mathbf{N}^*$ correspondant à la famille $(B_i)_{i \geqq 1}$, et soit:*

$$A(\omega) = \bigcup_{k \in K(m,m)} A(k,m)(\omega) .$$

*Alors:*

$$\sum_{h > R_m} P(r'_h(A(\omega), B(\omega)) > \theta(R_m)) < 2^{-m} .$$

2°) *S'il existe un entier $n < m$ tel que*

$$c_n = \min\{c_h \mid c_h > c_m, h < m\} ,$$

*alors pour tout $k \in K(m,m)$, il existe un entier $j$ tel que:*

$$A(i,k,m) = A(i,j,n) \quad \textit{pour } i \leqq R_m .$$

Demonstration. On prend pour $(\Omega_i, \Sigma_i, P_i)$ l'intervale $[0,1]$ muni de la mesure de Lebesgue sur les boreliens. On montre que s'il existe des ensembles $A(i,k,p)$ et des entiers $R_p$ ($i \in \mathbf{N}^*$, $k \in \mathbf{N}^*$, $1 \leqq p < m$) tels que les relations a) à e) soient vérifiées, on peut construire des ensembles $A(i,k,m)$ et un entier $R_m$ tels que ces relations soient toujours vérifiées. Si $c_m > c_l$ pour tout $l < m$, il s'agit simplement de subdiviser les ensembles $A(i,k,l)$ et d'utiliser une bijection $\mathbf{N}^* \times \mathbf{N}^* \to \mathbf{N}^*$. Dans les autres cas, par exemple s'il existe des entiers $l, n$ tels que $l, m$ et $n$ vérifient la condition (I), les sous-ensembles $A(i,k,m)$ sont des réunions finies de sous-ensembles $A(i,k,n)$ contenus dans un même $A(i,k,l)$. Ceci peut être fait de manière convenable en utilisant en particulier la remarque suivante. Soient $0 < a < b$ des nombres réels tels que $a + b \leqq 1$. Soit $(x_i)_{i \geqq 1}$ une suite de points de $]0, \infty[$, croissante pour $i > i_0$, telle que

$$\lim_{i \to \infty} x_i = \infty \quad \text{et} \quad \lim_{i \to \infty} (x_{i+1} - x_i) = 0 .$$

Soit $i \mapsto N(i)$ une application de $\mathbf{N}^*$ dans $\mathbf{N}^*$ telle que pour $i > i_0$,

$$0 \leqq N(i+1) - N(i) \leqq 1 \quad \text{et} \quad |N(i) - x_i^{a+b}| \leqq 3 .$$

Alors il existe un entier $i_1$ et une application $i \mapsto K(i)$ de $\mathbf{N}^*$ dans $\mathbf{N}^*$ tels-que, en posant $M(i) = [N(i)/K(i)]$, on ait pour $i > i_1$:

1) $0 \leqq K(i+1) - K(i) \leqq 1$.

2) Si $M(i+1) \neq M(i)$, alors $M(i+1) = M(i) + 1$, $K(i+1)M(i+1) = N(i+1)$ et si $j$ est un entier tel que $M(j) > M(i+1)$, alors $K(j) > K(i)$.

3) Si $K(i+1) \neq K(i)$, alors $M(i+1) = M(i)$ et si $j$ est le plus grand entier tel que $K(j) = K(i+1)$, alors $N(j) - N(i) > M(i) + 1$.

4) $|K(i) - x_i^b| \leqq 2$ et $|M(i) - x_i^a| \leqq 2$.

On utilise aussi le lemme 7 pour determiner $R_m$.

Demonstration du theoreme 5. Ce théorème résulte du lemme 8 où l'on prend $C = D$. Il est toujours possible en effet de numéroter les éléments de $D = \{c_1, c_2, \ldots\}$ de telle sorte que les hypothèses du lemme 11 soient remplies. On a donc une famille $(\Omega_i, \Sigma_i, P_i)_{i \geqq 1}$ d'espaces de probabilité, des sous-ensembles $A(i,k,m)$ ($i,k,m$ entiers) et une suite d'entiers $(R_m)_{m \geqq 1}$ vérifiant les propriétés énoncées au lemme 8. Nous reprendrons dans la suite les notations introduites dans l'énoncé de ce lemme.

Pour tout $\omega \in \Omega$ on a les deux propriétés suivantes:

1°) pour tout entier $m$, la famille $(A(k,m)(\omega))_{k \geqq 1}$ est une partition de $\mathbf{N}^*$

2°) si l'on a $c_m < c_n$, la partition $(A(k,n)(\omega))_{k \geqq 1}$ est plus fine que la partition $(A(k,m)(\omega))_{k \geqq 1}$.

Si $t = 1 - c_m$, nous noterons $\pi_t(\omega)$ la partition $(A(k,m)(\omega))_{k \geqq 1}$.

Si $p$ et $q$ sont des entiers quelconques, et si $\omega \in \Omega$, notons:

$$d_\omega(p,q) = \inf \{ t \in D \mid p \equiv q \pmod{\pi_t(\omega)} \} .$$

On a toujours $d_\omega(p,q) < 1$ en vertu du fait que $D$ est dense et de la propriété d) du lemme 8.

On a bien sûr $d_\omega(p,q) = d_\omega(q,p)$, et, si $r$ est un entier, on a:

$$d_\omega(p,q) \leqq \max \{ d_\omega(p,r), d_\omega(r,q) \} .$$

Enfin, si $d_\omega(p,q) = 0$, on a presque sûrement $p = q$. En effet, supposons que $p \neq q$. Soit $\varepsilon > 0$. Il existe un entier $m$ tel que

$$c_m = \max \{ c_h \mid h \leqq m \}, \quad m\varepsilon > 1 \text{ et } p \leqq m .$$

On a alors, en vertu de la propriété c) du lemme 8:

$$\begin{aligned} P(d_\omega(p,q)=0) &\leqq P(p\equiv q \pmod{\pi_{1-c_m}(\omega)}) \\ &= \sum_{k=1}^{\infty} P_p(\omega_p \in A(p,k,m))P_q(\omega_q \in A(q,k,m)) \\ &\leqq \sum_{k=1}^{\infty} \frac{1}{m} P_q(\omega_q \in A(q,k,m)) < \varepsilon . \end{aligned}$$

$\varepsilon$ étant arbitraire, on en déduit que $P(d_\omega(p,q)=0)=0$. Il résulte de ce qui précède que pour presque tout $\omega \in \Omega$, $d_\omega$ est une distance sur $\mathbf{N}^*$, qui est de plus ultramétrique.

Dans ce qui suit, nous noterons $\Omega'$ l'ensemble des $\omega \in \Omega$ tels que $d_\omega$ est une distance.

Soit $\varepsilon > 0$, et $m$ et $k$ des entiers. Comme $P_i(A(i,k,m)) \sim (\log i/i)^{c_m}$ pour $i \to \infty$, on déduit des lemmes 1 et 3 que pour presque tout $\omega \in \Omega$:

$$n^{1-c_m-\varepsilon} \ll s_n(A(k,m)(\omega)) \ll n^{1-c_m+\varepsilon} \quad \text{pour } n \to \infty .$$

Ceci a comme conséquence que pour presque tout $\omega \in \Omega'$, on a pour toute boule $B$ ouverte ou fermée et de rayon $n \leqq 1$

$$n^{r-\varepsilon} \ll s_n(B) \ll n^{r+\varepsilon} \quad \text{pour } n \to \infty .$$

Comme on a toujours $d_\omega(p,q) < 1$, on déduit de ce dernier fait que pour presque tout $\omega \in \Omega'$, le diamètre de $\mathbf{N}^*$ vaut 1.

Montrons que pour presque tout $\omega \in \Omega'$, la distance $d_\omega$ vérifie la propriété 2°) de l'énoncé du théorème. Il suffit en fait de montrer que si $p$ et $q$ sont des entiers distincts, on a alors $d_\omega(p,q) \in D$ pour tout $\omega \in \Omega'$. En supposant $p \neq q$, on a aussi $d_\omega(p,q) \neq 0$, ce qui veut dire qu'il existe un entier $u$ tel que

$$p \not\equiv q \pmod{\pi_{1-c_u}(\omega)} .$$

Il existe d'autre part toujours un entier $v$ tel que $p \equiv q \pmod{\pi_{1-c_v}(\omega)}$ et tel qu'il existe $h \leqq v$ avec $c_h + c_v > 1$. Soient $w = \max(u,v,p,q)$ et $l$ l'unique entier tel que

$$c_l = \max\{c_h \mid p \equiv q \pmod{\pi_{1-c_h}(\omega)}, h \leqq w\} .$$

En vertu de la partie 2°) du point e) du lemme 8, on peut alors construire une suite d'entiers $m_1 < m_2 < \ldots$ tels que $c_{m_i} \to c_l$ pour $i \to \infty$ et tels que pour tout entier $i$,

$$p \not\equiv q \pmod{\pi_{1-c_{m_i}}(\omega)} .$$

On a donc $d_\omega(p,q) = 1 - c_l \in D$.

Le point 2°) de l'énoncé est donc vérifié par $d_\omega$ pour tout $\omega \in \Omega'$, et de plus les boules fermées de rayon $r \in D$ s'identifient aux ensembles de la partition $\pi_r(\omega)$ pour tout $r \in D$.

Montrons que pour presque tout $\omega \in \Omega'$, la distance $d_\omega$ vérifie la partie i) de 3°). Comme $D$ est dense il suffit de le vérifier pour $r, s \in D$ et pour les boules fermées, qui sont égales à des ensembles $A(k,m)(\omega)$ pour $k$ et $m$ bien choisis. Ce résultat découle alors du fait que $D$ est dénombrable et des lemmes 3 et 7.

Les lemmes 3 et 6 montrent que pour presque tout $\omega \in \Omega'$, $d_\omega$ vérifie la condition iii) du point 3°). La condition ii) en découle car $D$ est dense.

En résumé, on a montré jusqu'ici que pour presque tout $\omega \in \Omega$, $d_\omega$ est une distance qui vérifie toutes les conditions voulues, à l'exception de la partie iv) du point 3°).

Nous allons maintenant montrer qu'il existe un sous-ensemble $E$ de $\Omega'$, de mesure non nulle, tel que pour tout $\omega \in E$, $d_\omega$ remplit la condition iv) du point 3°). Soit

$$M = \{m \mid \exists u \leqq m \text{ avec } c_u + c_m > 1\} .$$

Pour tout $m \in M$, considérons les sous-ensembles $A(\omega)$ et $B(\omega)$ de $\mathbf{N}^*$ définis dans la partie 1°) du point e) du lemme 8, que nous noterons ici $A_m(\omega)$ et $B_m(\omega)$ respectivement.

Soit:

$$E = \Omega' \setminus \bigcup_{m \in M} \bigcup_{h > R_m} \{\omega \mid r'_h(A_m(\omega), B_m(\omega)) > \theta(R_m)\} .$$

On a bien $P(E) > 0$ en vertu de la partie 1°) du point e) du lemme 8. Considérons un élément $\omega \in E$. Il suffit de démontrer que la distance $d_\omega$ vérifie la condition désirée dans deux cas:

1°) $X$ et $Y$ sont des boules ouvertes de rayons respectifs $r$ et $s$, avec $r+s=1$ ($r, s \in ]0,1[$).

Soient $i = \min X$, $j = \min Y$. Pour $m$ assez grand, il existe des entiers $u_m$ et $v_m$ tels que:

$$c_{u_m} = \min\{c_h \mid 1 - c_h < r,\ h \leqq m\}$$

$$c_{v_m} = \min\{c_h \mid 1 - c_h < s,\ h \leqq m\} .$$

Pour $m \to \infty$, on a $1 - c_{u_m} \to r$, $1 - c_{v_m} \to s$, et

$$X = \bigcup_m B(i, 1 - c_{u_m}), \qquad Y = \bigcup_m B(j, 1 - c_{v_m})$$

(où $B(x, \varrho)$ désigne la boule ouverte de centre $x$ et de rayon $\varrho$). On montre alors, en utilisant la définition de $E$ et le point e) du lemme 8, qu'il existe un entier $m_0$ tel que pour $m > m_0$ et $n > R_{m_0}$:

$$r'_n(B(i, 1 - c_{u_m}), B(j, 1 - c_{v_m})) \leqq \theta(n) ,$$

ce qui achève la démonstration dans ce cas particulier.

2°) $X$ est une boule ouverte de rayon $r \in D$, $Y$ est une boule fermée de rayon $s=1-r \in D$.

Ce cas se traite de facon similaire au cas 1°).

Il résulte de ce qui précède que l'ensemble des $\omega \in \Omega$ tels que $d_\omega$ remplisse toutes les conditions demandées dans le théorème 5 a une mesure non nulle, ce qui démontre le théorème.

## REFERENCES

1. P. Erdös, *On a problem of Sidon in additive number theory*, Acta Univ. Szeged 15 (1953/54), 255–259.
2. P. Erdös et A. Rényi, *Additive properties of random sequences of positive integers*, Acta Arith. 6 (1960), 83–110.
3. H. Halberstam et K. F. Roth, *Sequences*, vol. I, At the Clarendon Press, Oxford, 1966.

MATHEMATICS INSTITUTE
UNIVERSITY OF WARWICK
COVENTRY, ENGLAND