

SÉMINAIRE DELANGE-PISOT-POITOU. THÉORIE DES NOMBRES

JEAN CHAUVINEAU

Théorème de Koksma pour les parties entières dans \mathbb{R} et dans \mathbb{Q}_p

Séminaire Delange-Pisot-Poitou. Théorie des nombres, tome 8, n° 1 (1966-1967),
exp. n° 7, p. 1-12

http://www.numdam.org/item?id=SDPP_1966-1967__8_1_A7_0

© Séminaire Delange-Pisot-Poitou. Théorie des nombres
(Secrétariat mathématique, Paris), 1966-1967, tous droits réservés.

L'accès aux archives de la collection « Séminaire Delange-Pisot-Poitou. Théorie des nombres » implique l'accord avec les conditions générales d'utilisation (<http://www.numdam.org/conditions>). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

Article numérisé dans le cadre du programme
Numérisation de documents anciens mathématiques
<http://www.numdam.org/>

THÉORÈME DE KOKSMA POUR LES PARTIES ENTIÈRES
 DANS $\underline{\mathbb{R}}$ ET DANS $\underline{\mathbb{Q}}_p$
 par Jean CHAUVINEAU

$\underline{\mathbb{N}}$, $\underline{\mathbb{Z}}$, $\underline{\mathbb{Q}}$, $\underline{\mathbb{R}}$, $\underline{\mathbb{Z}}_p$, $\underline{\mathbb{Q}}_p$ désignent les structures algébriques couramment représentées par ces lettres ($0 \notin \underline{\mathbb{N}}$, p premier); le groupe des unités de $\underline{\mathbb{Q}}_p$ est noté \underline{U}_p . Si $x \in \underline{\mathbb{Q}}_p$, on désigne par $|x|_p$ la valeur absolue p -adique de x , et on pose

$$v(x) = -\log_p |x|_p \quad \text{si } x \in \underline{\mathbb{Q}}_p^*, \quad v(0) = +\infty.$$

On se propose de montrer que le théorème métrique de Koksma concernant l'équirépartition (mod 1) s'étend aux suites des parties entières qui vont être définies, d'abord dans $\underline{\mathbb{R}}$, puis dans $\underline{\mathbb{Q}}_p$.

1. Notations et définitions utilisées dans $\underline{\mathbb{R}}$.

On désigne par \underline{r} un système de représentants du groupe quotient $\underline{\mathbb{R}}/\underline{\mathbb{Z}}$ des réels modulo 1; notamment, \underline{r} pourra être l'intervalle $\underline{r}_0 = [0, 1[$.

Tout $x \in \underline{\mathbb{R}}$ admet une décomposition unique

$$x = [x]_{\underline{r}} + \langle x \rangle_{\underline{r}} \quad \text{où } [x]_{\underline{r}} \in \underline{\mathbb{Z}}, \quad \langle x \rangle_{\underline{r}} \in \underline{r}$$

$[x]_{\underline{r}}$ s'appellera partie entière de x relative à \underline{r} .

On pose en particulier

$$[x]_{\underline{r}_0} = [x] \quad \text{et} \quad \langle x \rangle_{\underline{r}_0} = \langle x \rangle,$$

de sorte que

$$\langle x \rangle_{\underline{r}} \equiv \langle x \rangle \pmod{1}$$

$[x]$ et $\langle x \rangle$ sont dits respectivement partie entière et partie fractionnaire de x .

Enfin, on pose, pour tout $x \in \underline{\mathbb{R}}$:

$$e(x) = e^{2i\pi x}$$

d'où résultent, sur $\underline{\mathbb{R}}$, les inégalités

$$|e(x) - 1| \leq 2\pi \min(\langle x \rangle, 1 - \langle x \rangle) \leq 2\pi |x|.$$

Notre étude dans $\underline{\mathbb{R}}$ utilise deux définitions dues à I. WIVEN [4]. Soit une suite $(x_n)_{n \in \underline{\mathbb{N}}}$ de $\underline{\mathbb{Z}}$. Si $N \in \underline{\mathbb{N}}$, k entier ≥ 2 et $h = 0, 1, \dots, k-1$, on désigne par $(N, h, k)_x$ le nombre des n tels qu'on ait $1 \leq n \leq N$ et

$$x_n \equiv h \pmod{k}.$$

(a) La suite (x_n) de $\underline{\mathbb{Z}}$ est dite équirépartie [e. r.] \pmod{k} dans $\underline{\mathbb{Z}}$ si, et seulement si, pour tout $h = 0, 1, \dots, k-1$, on a

$$\lim_{N \rightarrow \infty} \frac{(N, h, k)_x}{N} = \frac{1}{k}.$$

Pour qu'il en soit ainsi, il faut et il suffit qu'on ait, pour tout $h = 1, \dots, k-1$:

$$\lim_{N \rightarrow \infty} \frac{1}{N} \sum_{1 \leq n \leq N} e\left(\frac{hx_n}{k}\right) = 0.$$

(b) La suite (x_n) de $\underline{\mathbb{Z}}$ est dite équirépartie [e. r.] dans $\underline{\mathbb{Z}}$ si, et seulement si, elle est e. r. \pmod{k} dans $\underline{\mathbb{Z}}$ pour tout entier $k \geq 2$.

2. Théorème de Koksma dans $\underline{\mathbb{R}}$.

2.1 Désignons par \mathcal{A} l'algèbre de Boole des réunions finies d'intervalles quelconques (éventuellement ponctuels) de $\underline{\mathbb{R}}$. Soient $E \in \mathcal{A}$, $F \in \mathcal{A}$, et soit ω un réel > 0 ; on dira que E et F sont congrus $\pmod{\omega}$, et on écrira $E \equiv F \pmod{\omega}$, si et seulement s'il existe une partition finie de E en intervalles quelconques I_h , une partition finie de F en intervalles quelconques J_h , et une suite finie d'entiers rationnels a_h , où $h = 1, \dots, H$, telles qu'on ait

$$I_h = J_h + a_h \omega \quad \text{pour tout } h = 1, \dots, H.$$

Dans ces conditions, les ensembles E et F , qui sont évidemment mesurables au sens de Riemann [mesurables- \mathbb{R}], ont des mesures- \mathbb{R} égales.

LEMME 1. - Soit \underline{r} un système de représentants de $\underline{\mathbb{R}}/\underline{\mathbb{Z}}$ tel que $\underline{r} \in \mathcal{A}$; pour que la suite (x_n) de $\underline{\mathbb{R}}$ soit e. r. $\pmod{1}$ dans $\underline{\mathbb{R}}$, il faut et il suffit que, pour tout entier $k \geq 2$, la suite $([kx_n]_{\underline{r}})$ soit e. r. \pmod{k} dans $\underline{\mathbb{Z}}$.

Notons d'abord qu'on a $\underline{r} \equiv (0, 1[\pmod{1}$, et \underline{r} est de mesure 1.

Nécessité. - Supposons que la suite (x_n) soit e. r. (mod 1) dans $\underline{\mathbb{R}}$; pour cela, il faut et il suffit que la suite $(\langle x_n \rangle_{\underline{\mathbb{R}}})$ soit e. r. dans $\underline{\mathbb{R}}$, donc encore que la suite $(k\langle x_n \rangle_{\underline{\mathbb{R}}})$ soit e. r. dans $k\underline{\mathbb{R}}$.

La partition \mathcal{P} de $\underline{\mathbb{R}}$ en k ensembles $\underline{\mathbb{R}} + k\underline{\mathbb{Z}} + \ell$, où $\ell = 0, 1, \dots, k-1$, fournit une partition de $k\underline{\mathbb{R}}$ en k ensembles $A(\ell) \in \mathcal{A}$ respectivement congrus (mod k) à $\underline{\mathbb{R}} + \ell$. Fixons ℓ , et considérons les $k\langle x_n \rangle_{\underline{\mathbb{R}}}$ qui sont répartis dans $A(\ell)$, de mesure 1 ; puisque $A(\ell) \equiv \underline{\mathbb{R}} + \ell \pmod{k}$, les $[k\langle x_n \rangle_{\underline{\mathbb{R}}}]_{\underline{\mathbb{R}}}$ correspondants sont tous congrus à $\ell \pmod{k}$. Dès lors, l'équirépartition des $k\langle x_n \rangle_{\underline{\mathbb{R}}}$ dans $k\underline{\mathbb{R}}$, de mesure k , entraîne l'équirépartition (mod k) des $[k\langle x_n \rangle_{\underline{\mathbb{R}}}]_{\underline{\mathbb{R}}}$ dans $\underline{\mathbb{Z}}$.

Mais on a

$$[k\langle x_n \rangle_{\underline{\mathbb{R}}}]_{\underline{\mathbb{R}}} = [kx_n - k[x_n]_{\underline{\mathbb{R}}}]_{\underline{\mathbb{R}}} = [kx_n]_{\underline{\mathbb{R}}} - k[x_n]_{\underline{\mathbb{R}}} \equiv [kx_n]_{\underline{\mathbb{R}}} \pmod{k}.$$

Donc enfin, la suite $([kx_n]_{\underline{\mathbb{R}}})$ est e. r. (mod k) dans $\underline{\mathbb{Z}}$.

Suffisance. - Posant, pour k entier ≥ 2 et $h = 1, \dots, k-1$:

$$S_N(h, k) = \frac{1}{N} \sum_{1 \leq n \leq N} e\left(\frac{h}{k} [kx_n]_{\underline{\mathbb{R}}}\right)$$

$$S'_N(h, k) = \frac{1}{N} \sum_{1 \leq n \leq N} e(hx_n) \left(e\left(-\frac{h}{k} \langle kx_n \rangle_{\underline{\mathbb{R}}}\right) - 1 \right)$$

et, pour $h \in \underline{\mathbb{N}}$:

$$\sigma_N(h) = \frac{1}{N} \sum_{1 \leq n \leq N} e(hx_n)$$

on a

$$S_N(h, k) = \sigma_N(h) + S'_N(h, k)$$

d'où

$$|\sigma_N(h)| \leq |S_N(h, k)| + |S'_N(h, k)|.$$

Puisqu'il appartient à \mathcal{A} , le système de représentants $\underline{\mathbb{R}}$ est borné ; posant $M = \sup_{t \in \underline{\mathbb{R}}} |t|$, on obtient

$$|S'_N(h, k)| \leq \frac{1}{N} \sum_{1 \leq n \leq N} |1 - e\left(\frac{h}{k} \langle kx_n \rangle_{\underline{\mathbb{R}}}\right)| \leq \frac{1}{N} \sum_{1 \leq n \leq N} \frac{2\pi h}{k} |\langle kx_n \rangle_{\underline{\mathbb{R}}}| \leq \frac{2\pi h M}{k}$$

de sorte que

$$|\sigma_N(h)| \leq |S_N(h, k)| + \frac{2\pi h M}{k}.$$

Si la suite $([kx_n]_{\mathbb{R}})$ est e. r. (mod k) dans \mathbb{Z} pour tout entier $k \geq 2$, alors, pour tout $h \in \mathbb{N}$ et pour tout entier $k > h$, on a

$$\lim_{N \rightarrow \infty} S_N(h, k) = 0,$$

et la limite supérieure de $|\sigma_N(h)|$ quand $N \rightarrow \infty$ est au plus égale à $\frac{2\pi h M}{k}$; cela exige, puisque, h étant fixé, k est arbitrairement grand, qu'on ait

$$\lim_{N \rightarrow \infty} \sigma_N(h) = 0 \quad \text{pour tout } h \in \mathbb{N},$$

et la suite (x_n) est e. r. (mod 1) dans \mathbb{R} .

2.2 Ce lemme étant établi, soit I un intervalle de \mathbb{R} et soit une suite (f_n) d'applications dérivables de I dans \mathbb{R} ; on pose $F_{m,n} = f_m - f_n$. Introduisons les deux conditions suivantes :

(K1) Pour tout couple d'entiers naturels (m, n) , où $m \neq n$, la fonction $F'_{m,n}$ est monotone et de signe constant sur I .

(K2) Il existe un réel $c > 0$ tel que, pour tout couple d'entiers naturels (m, n) , où $m \neq n$, on ait $|F'_{m,n}(x)| \geq c$ pour tout $x \in I$.

On sait [3] que, si ces conditions sont satisfaites, alors la suite $(f_n(x))$ de \mathbb{R} est e. r. (mod 1) pour presque tous les $x \in I$, c'est-à-dire sauf pour ceux qui appartiennent à une partie de I dont la mesure de Lebesgue [mesure- \mathcal{L}] est nulle, et il en est de même de la suite $(\frac{f_n(x)}{k})$, où k entier ≥ 2 . Dès lors, soit $\mathcal{A} \in \mathcal{A}$; d'après le lemme 1 (nécessité de la condition), pour tout entier $k \geq 2$, la suite $([f_n(x)]_{\mathbb{R}})$ est e. r. (mod k) dans \mathbb{Z} pour presque tous les $x \in I$. Puisqu'une réunion dénombrable d'ensembles de mesure- \mathcal{L} nulle est elle-même de mesure- \mathcal{L} nulle, il en résulte que l'ensemble des $x \in I$, tels que la suite $([f_n(x)]_{\mathbb{R}})$ ne soit pas e. r. dans \mathbb{Z} , a une mesure- \mathcal{L} nulle, et le théorème de Koksma dans \mathbb{R} peut être complété comme suit :

THÉORÈME 1. - Soit \mathcal{r} un système de représentants de \mathbb{R}/\mathbb{Z} tel que $\mathcal{r} \in \mathcal{A}$, soit I un intervalle de \mathbb{R} et soit une suite (f_n) d'applications dérivables de I dans \mathbb{R} ; si I et f_n vérifient les conditions (K1) et (K2), alors, pour presque tous les $x \in I$, la suite $(f_n(x))$ est e. r. (mod 1) dans \mathbb{R} et la suite $([f_n(x)]_{\mathbb{R}})$ est e. r. dans \mathbb{Z} .

3. Notations et définitions utilisées dans \mathbb{Q}_p .

L'ensemble des rationnels qui, après réduction, ont pour dénominateur une puissance entière ≥ 0 de p sera noté $\mathbb{Q}_{(p)}$.

On désigne par \mathbb{r}_p un système de représentants du groupe quotient $\mathbb{Q}_p/\mathbb{Z}_p$ des p -adiques modulo 1, qui est isomorphe au groupe $\mathbb{Q}_{(p)}/\mathbb{Z}$; notamment, \mathbb{r}_p pourra être l'ensemble $\mathbb{r}_{p,0} = (0, 1[\cap \mathbb{Q}_{(p)}$.

Tout $x \in \mathbb{Q}_p$ admet une décomposition unique

$$x = [x]_{\mathbb{r}_p} + \langle x \rangle_{\mathbb{r}_p} \quad \text{où } [x]_{\mathbb{r}_p} \in \mathbb{Z}_p, \quad \langle x \rangle_{\mathbb{r}_p} \in \mathbb{r}_p$$

$[x]_{\mathbb{r}_p}$ s'appellera partie entière de x relative à \mathbb{r}_p .

En particulier, posant $[x]_{\mathbb{r}_{p,0}} = [x]_p$ et $\langle x \rangle_{\mathbb{r}_{p,0}} = \langle x \rangle_p$, de sorte que

$$\langle x \rangle_{\mathbb{r}_p} \equiv \langle x \rangle_p \pmod{1}$$

on obtient la décomposition unique

$$x = [x]_p + \langle x \rangle_p \quad \text{où } [x]_p \in \mathbb{Z}_p, \quad \langle x \rangle_p \in \mathbb{r}_{p,0}$$

$[x]_p$ et $\langle x \rangle_p$ sont dits respectivement partie entière p -adique et partie principale p -adique de x .

On a, pour $x_1, x_2, y \in \mathbb{Q}_p$:

$$\langle (x_1 + x_2)y \rangle_p \equiv \langle x_1 y \rangle_p + \langle x_2 y \rangle_p \pmod{1}$$

et $x \mapsto \langle xy \rangle_p$, où $y \in \mathbb{Q}_p$, est un homomorphisme continu du groupe additif \mathbb{Q}_p dans le groupe additif \mathbb{R}/\mathbb{Z} ; de plus on a:

$$(x_1 - x_2)y \in \mathbb{Z}_p \implies \langle x_1 y \rangle_p = \langle x_2 y \rangle_p \quad \text{pour } x_1, x_2, y \in \mathbb{Q}_p$$

et

$$\langle xy \rangle_p = \langle x \langle y \rangle_p \rangle_p \quad \text{pour } x \in \mathbb{Z}_p, \quad y \in \mathbb{Q}_p.$$

Enfin on pose, pour tout $x \in \mathbb{Q}_p$:

$$e_p(x) = e^{2i\pi \langle x \rangle_p}.$$

Si $x \in \mathbb{Q}_{(p)}$, alors on a $[x] = [x]_p$ et $\langle x \rangle = \langle x \rangle_p$, donc aussi $e(x) = e_p(x)$.

Notre étude dans \mathbb{Q}_p utilise d'abord deux définitions qui sont les analogues p -adiques des définitions de I. NIVEN mentionnées au paragraphe 1.

Soit une suite $(x_n)_{n \in \mathbb{N}}$ de \mathbb{Z}_p . Si $N \in \mathbb{N}$, $\alpha \in \mathbb{Z}_p$, $k \in \mathbb{N}$, on distingue par $(N, \alpha, k)_x$ le nombre des n tels qu'on ait $1 \leq n \leq N$ et $x_n \in \alpha + p^k \mathbb{Z}_p$.

(a) La suite (x_n) de \mathbb{Z}_p est dite équirépartie d'ordre k [k-e. r.] dans \mathbb{Z}_p si, et seulement si, pour tout $\alpha \in \mathbb{Z}_p$, on a

$$\lim_{N \rightarrow \infty} \frac{(N, \alpha, k)_x}{N} = \frac{1}{p^k}.$$

Pour qu'il en soit ainsi, il faut et il suffit qu'on ait, pour tout $h = 1, \dots, p^k - 1$:

$$\lim_{N \rightarrow \infty} \frac{1}{N} \sum_{1 \leq n \leq N} e_p \left(\frac{hx_n}{p^k} \right) = 0.$$

(b) La suite (x_n) de \mathbb{Z}_p est dite équirépartie [e. r.] dans \mathbb{Z}_p si, et seulement si, elle est k -e. r. dans \mathbb{Z}_p pour tout $k \in \mathbb{N}$.

D'autre part, nous introduisons la notion d'équirépartition (mod 1) dans \mathbb{Q}_p : La suite (x_n) de \mathbb{Q}_p est dite équirépartie [e. r.] (mod 1) dans \mathbb{Q}_p si, et seulement si, la suite $(\langle x_n \rangle_p)$ est e. r. dans $(0, 1)$.

Pour qu'il en soit ainsi, il faut et il suffit, puisque $e_p(h \langle x_n \rangle_p) = e_p(hx_n)$, qu'on ait, pour tout $h \in \mathbb{N}$:

$$\lim_{N \rightarrow \infty} \frac{1}{N} \sum_{1 \leq n \leq N} e_p(hx_n) = 0.$$

4. Théorème de Koksma dans \mathbb{Q}_p .

4.1. LEMME 2. - Soit \underline{r}_p un système de représentants de $\mathbb{Q}_p/\mathbb{Z}_p$ inclus dans un système de représentants \underline{r} de \mathbb{R}/\mathbb{Z} tel que $\underline{r} \in \mathcal{A}$; pour que la suite (x_n) de \mathbb{Q}_p soit e. r. (mod 1) dans \mathbb{Q}_p , il faut et il suffit que, pour tout $k \in \mathbb{N}$, la suite $([p^k x_n]_{\underline{r}_p})$ soit k -e. r. dans \mathbb{Z}_p .

Nécessité. - Supposons que la suite (x_n) soit e. r. (mod 1) dans \mathbb{Q}_p ; pour cela, il faut et il suffit que la suite $(\langle x_n \rangle_{\underline{r}_p})$ soit e. r. dans \underline{r} , donc encore que la suite $(p^k \langle x_n \rangle_{\underline{r}_p})$ soit e. r. dans $p^k \underline{r}$.

La partition \mathcal{P} de \mathbb{R} en p^k ensembles $\underline{r} + p^k \mathbb{Z} + \ell$, où

$$\ell = 0, 1, \dots, p^k - 1,$$

fournit une partition de $p^k \mathbb{R}$ en p^k ensembles $A(\ell) \in \mathcal{A}$ respectivement congrus (mod p^k) à $\underline{r} + \ell$. Fixons ℓ , et considérons les $p^k \langle x_n \rangle_{\underline{r}_p}$ qui sont répartis

dans $A(\ell)$, de mesure 1; puisque $A(\ell) \equiv \underline{r} + \ell \pmod{p^k}$, les $[p^k \langle x_n \rangle_{\underline{r}_p}]_{\underline{r}}$ correspondants sont tous congrus à $\ell \pmod{p^k}$. Dès lors, l'équirépartition des $p^k \langle x_n \rangle_{\underline{r}_p}$ dans $p^k \mathbb{R}$, de mesure p^k , entraîne l'équirépartition (mod p^k) des $[p^k \langle x_n \rangle_{\underline{r}_p}]_{\underline{r}}$ dans \mathbb{Z} .

Or, si $t \in \mathbb{Q}(p)$, on a $[t]_{\underline{r}} = [t]_{\underline{r}_p}$; donc ici

$$[p^k \langle x_n \rangle_{\underline{r}_p}]_{\underline{r}} = [p^k \langle x_n \rangle_{\underline{r}_p}]_{\underline{r}_p}$$

de sorte que l'équirépartition (mod p^k) des $[p^k \langle x_n \rangle_{\underline{r}_p}]_{\underline{r}}$ dans \mathbb{Z} équivaut à l'équirépartition d'ordre k des $[p^k \langle x_n \rangle_{\underline{r}_p}]_{\underline{r}_p}$ dans \mathbb{Z}_p .

Mais on a :

$$[p^k \langle x_n \rangle_{\underline{r}_p}]_{\underline{r}_p} = [p^k x_n - p^k [x_n]_{\underline{r}_p}]_{\underline{r}_p} = [p^k x_n]_{\underline{r}_p} - p^k [x_n]_{\underline{r}_p} \in [p^k x_n]_{\underline{r}_p} + p^k \mathbb{Z}_p.$$

Donc enfin, la suite $([p^k x_n]_{\underline{r}_p})$ est k -e. r. dans \mathbb{Z}_p .

Suffisance. - Posant ici, pour $k \in \mathbb{N}$ et $h = 1, \dots, p^k - 1$:

$$S_{\mathbb{N}}(h, k) = \frac{1}{N} \sum_{1 \leq n \leq N} e_p\left(\frac{h}{p^k} [p^k x_n]_{\underline{r}_p}\right)$$

$$S_{\mathbb{N}}^!(h, k) = \frac{1}{N} \sum_{1 \leq n \leq N} e_p(hx_n) \left(e\left(-\frac{h}{p^k} \langle p^k x_n \rangle_{\underline{r}_p}\right) - 1 \right)$$

et pour $h \in \mathbb{N}$:

$$\sigma_{\mathbb{N}}(h) = \frac{1}{N} \sum_{1 \leq n \leq N} e_p(hx_n)$$

on a

$$S_{\mathbb{N}}(h, k) = \sigma_{\mathbb{N}}(h) + S_{\mathbb{N}}^!(h, k)$$

d'où

$$|\sigma_{\mathbb{N}}(h)| \leq |S_{\mathbb{N}}(h, k)| + |S_{\mathbb{N}}^!(h, k)|.$$

Si on pose comme précédemment $M = \sup_{t \in \mathbb{T}} |t|$, on trouve ici $|S_N^!(h, k)| \leq \frac{2\pi h M}{p^k}$, de sorte que

$$|\sigma_N(h)| \leq |S_N(h, k)| + \frac{2\pi h M}{p^k}.$$

Si la suite $([p^k x_n]_{\mathbb{R}_p})$ est k -e. r. dans \mathbb{Z}_p pour tout $k \in \mathbb{N}$, alors, pour tout $h \in \mathbb{N}$ et pour tout entier $k > \frac{\log h}{\log p}$, on a

$$\lim_{N \rightarrow \infty} S_N(h, k) = 0,$$

et la limite supérieure de $|\sigma_N(h)|$ quand $N \rightarrow \infty$ est au plus égale à $\frac{2\pi h M}{p^k}$; cela exige, puisque, h étant fixé, k est arbitrairement grand, qu'on ait :

$$\lim_{N \rightarrow \infty} \sigma_N(h) = 0 \quad \text{pour tout } h \in \mathbb{N},$$

et la suite (x_n) est e. r. (mod 1) dans \mathbb{Q}_p .

4.2. Ce lemme étant établi, soit B une boule de \mathbb{Q}_p et soit une suite (f_n) d'applications continues de B dans \mathbb{Q}_p ; on pose $F_{m,n} = f_m - f_n$. Soit d'autre part E un ensemble de couples d'entiers naturels (m, n) contenant la diagonale de $\mathbb{N} \times \mathbb{N}$; on pose, pour tout $N \in \mathbb{N}$:

$$E_N = \text{card} \{(m, n) \in E \mid m \leq N \text{ et } n \leq N\}.$$

Introduisons les deux conditions suivantes :

(C1) A tout couple d'entiers naturels $(m, n) \notin E$ est associé un entier rationnel $\lambda_{m,n}$ tel qu'on ait, pour $x \in B$, $y \in B$:

$$|F_{m,n}(x) - F_{m,n}(y)|_p = p^{\lambda_{m,n}} |x - y|_p$$

et tel que $\lambda_{m,n} \rightarrow +\infty$ quand $\max(m, n) \rightarrow \infty$.

(C2) La série de terme général $\frac{E_N}{N^2}$ est convergente.

On sait ([1], chap. 5) que, si ces conditions sont satisfaites, alors la suite $(f_n(x))$ de \mathbb{Q}_p est e. r. (mod 1) dans \mathbb{Q}_p pour presque tous les $x \in B$, c'est-à-dire sauf pour ceux qui appartiennent à une partie de B dont la mesure de Haar [mesure- \mathcal{H}] est nulle, et il en est de même de la suite

$$\left(\frac{f_n(x)}{p^k}\right), \quad \text{où } k \in \mathbb{N}.$$

Dès lors, soient $\underline{r} \in \mathcal{A}$ et $\underline{r}_p \subset \underline{r}$; d'après le lemme 2 (nécessité de la condition), pour tout $k \in \underline{\mathbb{N}}$, la suite $([f_n(x)]_{\underline{r}_p})$ est k-e. r. dans $\underline{\mathbb{Z}}_p$ pour presque tous les $x \in B$. Il en résulte que l'ensemble des $x \in B$ tels que la suite $([f_n(x)]_{\underline{r}_p})$ ne soit pas e. r. dans $\underline{\mathbb{Z}}_p$ a une mesure- μ nulle, et le théorème de Koksma dans $\underline{\mathbb{Q}}_p$ peut être complété comme suit :

THÉORÈME 2. - Soit \underline{r}_p un système de représentants de $\underline{\mathbb{Q}}_p/\underline{\mathbb{Z}}_p$ inclus dans un système de représentants \underline{r} de $\underline{\mathbb{R}}/\underline{\mathbb{Z}}$ tel que $\underline{r} \in \mathcal{A}$, soit B une boule de $\underline{\mathbb{Q}}_p$ et soit une suite (f_n) d'applications continues de B dans $\underline{\mathbb{Q}}_p$; si E, B, f_n vérifient les conditions (C1) et (C2), alors, pour presque tous les $x \in B$, la suite $(f_n(x))$ est e. r. (mod 1) dans $\underline{\mathbb{Q}}_p$ et la suite $([f_n(x)]_{\underline{r}_p})$ est e. r. dans $\underline{\mathbb{Z}}_p$.

5. Applications du théorème de Koksma dans $\underline{\mathbb{Q}}_p$.

Il est entendu que, dans ce dernier paragraphe, \underline{r}_p est de la forme que lui assigne le théorème 2.

(a) Démontrons d'abord le corollaire suivant.

COROLLAIRE. - Soit une suite (a_n) de $\underline{\mathbb{Q}}_p$ telle que $\lim_{n \rightarrow \infty} v(a_n) = -\infty$; s'il existe un couple réel (c, s) vérifiant $c \geq 0$ et $0 \leq s < 1$, tel qu'à partir d'un certain rang en m et d'un certain rang en n , on ait :

$$|m - n| > c \max(m^s, n^s) \implies v(a_m) \neq v(a_n)$$

alors, pour presque tous les $x \in \underline{\mathbb{Q}}_p$, la suite $n \mapsto a_n x$ est e. r. (mod 1) dans $\underline{\mathbb{Q}}_p$ et la suite $n \mapsto [a_n x]_{\underline{r}_p}$ est e. r. dans $\underline{\mathbb{Z}}_p$.

Prenant $f_n(x) = a_n x$, on a :

$$|F_{m,n}(x) - F_{m,n}(y)|_p = p^{\lambda_{m,n}} |x - y|_p$$

en posant $\lambda_{m,n} = -v(a_m - a_n)$.

Si $v(a_m) \neq v(a_n)$, on a

$$\lambda_{m,n} = -\min(v(a_m), v(a_n)) \rightarrow +\infty \text{ quand } \max(m, n) \rightarrow \infty.$$

Ainsi (C1) est vérifiée en prenant

$$E = \{(m, n) \mid v(a_m) = v(a_n)\} .$$

Comme par hypothèse

$$v(a_m) = v(a_n) \implies |m - n| \leq c \max(m^s, n^s)$$

pour disons, $m > m_0$ et $n > n_0$, on voit que

$$E \subset F = \{(m, n) \mid m \leq m_0 \text{ ou } n \leq n_0 \text{ ou } |m - n| \leq c \max(m^s, n^s)\} .$$

Supposons $1 \leq m, n \leq N$; le nombre des couples (m, n) vérifiant la première condition indiquée est $m_0 N$; de même, celui des couples (m, n) vérifiant la seconde est $n_0 N$; enfin, celui des couples (m, n) vérifiant la troisième est **au plus égal** à $N(2cN^s + 1) = O(N^{s+1})$. Donc on a, avec des notations évidentes

$$E_N \leq F_N = O(N^{s+1})$$

et (C2) est vérifiée, puisque $s < 1$.

En particulier, appliquant ce corollaire avec $s = 0$, $c = p - 1$, on voit que, pour presque tous les $x \in \mathbb{Q}_p$, la suite

$$n \longmapsto \frac{x}{(\alpha + 1)^k (\alpha + 2)^k \dots (\alpha + n)^k}$$

où $k \in \mathbb{N}$, $\alpha \in \mathbb{Z}_p$, $-\alpha \notin \mathbb{N}$, est e. r. (mod 1) dans \mathbb{Q}_p et la suite associée

$$n \longrightarrow \left[\frac{x}{(\alpha + 1)^k (\alpha + 2)^k \dots (\alpha + n)^k} \right]_{\mathbb{Z}_p}$$

est e. r. dans \mathbb{Z}_p .

(b) Soit $f_n(x) = xn^k \alpha^n$, où $k \in \mathbb{Z}$, $\alpha \in \mathbb{Q}_p - \mathbb{Z}_p$. On a

$$|F_{m,n}(x) - F_{m,n}(y)|_p = p^{\lambda_{m,n}} |x - y|_p ,$$

en posant $\lambda_{m,n} = -v(m^k \alpha^m - n^k \alpha^n)$.

Si $kv(m) + mv(\alpha) \neq kv(n) + nv(\alpha)$, on a

$$\lambda_{m,n} = -\min(kv(m) + mv(\alpha), kv(n) + nv(\alpha)) .$$

Puisque $v(n) = O(\log n)$ et $v(\alpha) \leq -1$, on voit que $\lambda_{m,n} \rightarrow +\infty$ quand $\max(m, n) \rightarrow \infty$. Ainsi (C1) est vérifiée en prenant

$$E = \{(m, n) \mid (m - n)v(\alpha) = k(v(n) - v(m))\}.$$

Supposons $1 \leq m, n \leq N$ et $(m - n)v(\alpha) = k(v(n) - v(m))$; à un choix de m et de $v(n)$ correspond au plus une seule valeur de n ; comme les valeurs possibles de m sont $1, 2, \dots, N$ et les valeurs possibles de $v(n)$ sont $0, 1, \dots, \lfloor \frac{\log N}{\log p} \rfloor$, on a

$$E_N \leq N(\lfloor \frac{\log N}{\log p} \rfloor + 1) = O(N \log N)$$

et (C2) est vérifiée. Ainsi, pour presque tous les $x \in \mathbb{Q}_p$, la suite $n \mapsto xn^k \alpha^n$, où $k \in \mathbb{Z}$, $\alpha \in \mathbb{Q}_p - \mathbb{Z}_p$, est e. r. (mod 1) dans \mathbb{Q}_p et la suite associée $n \mapsto [xn^k \alpha^n]_{\mathbb{Z}_p}$ est e. r. dans \mathbb{Z}_p .

(c) Soit $f_n(x) = \gamma(n!)^h x^n$, où $\gamma \in \mathbb{Q}_p^*$, $h \in \mathbb{Z}$, et soit B_k une boule de rayon $\frac{1}{p^{k+2}}$ contenue dans la couronne $p^k U_p$, où $k \in \mathbb{Z}$. Prenons $x \in B_k$, $y \in B_k$, $x \neq y$, et formons

$$\frac{F_{m,n}(x) - F_{m,n}(y)}{x - y} = \gamma \frac{(m!)^h (x^m - y^m)}{x - y} - \gamma \frac{(n!)^h (x^n - y^n)}{x - y}.$$

On obtient, dans ces conditions :

$$v\left(\frac{x^n - y^n}{x - y}\right) = v(n) + (n - 1)k$$

d'où

$$v\left(\frac{(n!)^h (x^n - y^n)}{x - y}\right) = hv(n!) + v(n) + (n - 1)k,$$

soit $\varphi(n)$. Dès lors, si $\varphi(m) \neq \varphi(n)$, on a

$$|F_{m,n}(x) - F_{m,n}(y)|_p = p^{\lambda_{m,n}} |x - y|_p$$

en posant

$$\lambda_{m,n} = -v(\gamma) - \min(\varphi(m), \varphi(n)).$$

Or on voit que

$$\varphi(n) = n\left(k + \frac{h}{p-1}\right) + O(\log n).$$

Supposons $k < -\frac{h}{p-1}$; alors $\lambda_{m,n} \rightarrow +\infty$ quand $\max(m, n) \rightarrow \infty$. Ainsi (C1) est vérifiée en prenant

$$E = \{(m, n) \mid \varphi(m) = \varphi(n)\} .$$

La condition indiquée s'écrit explicitement

$$v\left(\frac{(n!)^h}{(m!)^h} \frac{n}{m}\right) = (m-n)k$$

où le premier membre est de la forme $\frac{(n-m)h}{p-1} + O(\log \max(m, n))$; elle s'écrit donc encore

$$m - n = O(\log \max(m, n)) .$$

Supposant $1 \leq m, n \leq N$; il en résulte qu'on a ici

$$E_N = O(N \log N)$$

et (C2) est vérifiée.

Le résultat de KOKSMA s'applique donc à presque tous les $x \in B_k \subset p^k \mathbb{U}_p$ quel que soit $k < -\frac{h}{p-1}$, c'est-à-dire finalement à presque tous les $x \in \mathbb{Q}_p - p^K \mathbb{Z}_p$, où K est l'entier rationnel défini par $K-1 < -\frac{h}{p-1} \leq K$.

Ainsi :

Soient $\gamma \in \mathbb{Q}_p^*$, $h \in \mathbb{Z}$ et soit K le plus petit entier rationnel $\geq -\frac{h}{p-1}$; pour presque tous les $x \in \mathbb{Q}_p - p^K \mathbb{Z}_p$, la suite $n \mapsto \gamma(n!)^h x^n$ est e. r.

(mod 1) dans \mathbb{Q}_p et la suite $n \mapsto [\gamma(n!)^h x^n]_{r_p}$ est e. r. dans \mathbb{Z}_p .

Le cas $h = 0$, d'où $K = 0$, étend aux parties entières un résultat remarquable obtenu par Mme F. BERTRANDIAS ([1], chap. 5) : soit $\gamma \in \mathbb{Q}_p^*$; pour presque tous les $x \in \mathbb{Q}_p - \mathbb{Z}_p$, la suite $n \mapsto \gamma x^n$ est e. r. (mod 1) dans \mathbb{Q}_p et la suite $n \mapsto [\gamma x^n]_{r_p}$ est e. r. dans \mathbb{Z}_p .

BIBLIOGRAPHIE

- [1] BERTRANDIAS (Françoise). - Ensembles remarquables d'adèles algébriques, Bull. Soc. math. France, Mémoire n° 4, 1965, VI + 98 p. (Thèse Sc. math. Paris, 1965).
- [2] CHAUVINEAU (Jean). - Complément au théorème métrique de Koksma dans \mathbb{R} et dans \mathbb{Q}_p , C. R. Acad. Sc. Paris, t. 260, 1965, p. 6252-6255.
- [3] KOKSMA (Jurjen F.). - Ein mengentheoretischer Satz über die Gleichverteilung modulo Eins, Compos. Math., Groningen, t. 2, 1935, p. 250-258.
- [4] NIVEN (Ivan). - Uniform distribution of sequences of integers, Trans. Amer. math. Soc., t. 98, 1961, p. 52-61.