Séminaire Delange-Pisot-Poitou.
Théorie des nombres

Jean-Marc Deshouillers

Quelques problèmes sur les bases d'entiers

Séminaire Delange-Pisot-Poitou. Théorie des nombres, tome 15, nº 1 (1973-1974), exp. nº 10, p. 1-5
<http://www.numdam.org/item?id=SDPP_1973-1974__15_1_A7_0>

Séminaire DELANGE-PISOT-POITOU
(Théorie des nombres)
15e année, 1973/74, n° 10, 5 p.

14 janvier 1974

QUELQUES PROBLÈMES SUR LES BASES D'ENTIERS

par Jean-Marc DESHOUILLERS

Le problème fondamental de la théorie additive des nombres est le suivant : Etant donnée une suite $\mathfrak{a}$ de nombres entiers positifs ou nuls, existe-t-il un entier h tel que tout entier soit somme d'au plus h éléments de $\mathfrak{a}$? S'il en est ainsi, on dit que la suite $\mathfrak{a}$ est une base d'entiers, et le plus petit entier h répondant à la question s'appelle l'ordre de la base.

Cette formulation est suggérée par diverses conjectures :

Conjecture de Fermat : Les nombres n-gonaux forment une base d'ordre n .

Conjecture de Waring : Les puissances n-ièmes forment une base.

Conjecture de Goldbach : Tout entier pair supérieur à 2 est une somme de deux nombres premiers. (Cet énoncé n'est pas exactement du même type que les précédents, mais admet des corollaires de ce genre ; e. g. : la suite $\mathcal{P}$, constituée par 0 , 1 et les nombres premiers, est une base (d'ordre 3).)

Les conjectures de Fermat et de Waring ont été résolues en tenant compte de la nature arithmétique des suites considérées. Au contraire, en montrant que $\mathcal{P}$ est une base, ŠNIRELMAN a introduit une notion de densité des suites d'entiers qui permet de montrer que certaines suites sont des bases : il définit la densité $\sigma(\mathfrak{a})$ d'une suite $\mathfrak{a}$ comme la borne inférieure du rapport $\#\{1 \leq a \leq N \; ; \; a \in \mathfrak{a}\}/N$ lorsque N parcourt $\mathbb{N}$. Il a démontré le résultat suivant.

THÉORÈME. - *Si* $0 \in \mathfrak{a}$, *on a* :

$$\sigma(h\mathfrak{a}) \geq 1 - (1 - \sigma\mathfrak{a})^h \; .$$

Si $0 \in \mathfrak{a}$ *et* $\sigma\mathfrak{a} \geq \frac{1}{2}$, *alors* $2\mathfrak{a} = \mathbb{N}$.

On en déduit aisément le corollaire suivant.

CRITERE (P). - *Si* $0 \in \mathfrak{a}$ *et* $\sigma(\mathfrak{a}) > 0$, $\mathfrak{a}$ *est une base*.

On peut remarquer que ce critère est le meilleur possible, dans le sens suivant :

Pour toute application φ de $\mathbb{N}^*$ dans $[0 , 1]$ telle que $\varphi(u)$ tende vers 0 lorsque n tend vers l'infini, il existe une suite $\mathfrak{a}$ contenant 0 et 1 qui ne soit pas une base et telle que, pour tout entier N , on ait

$$\#\{a \leq N \; ; \; a \in \mathfrak{a}\} > N.\varphi(N) \; .$$

Malheureusement, le critère (P) ne peut être directement appliqué pour démontrer que l'ensemble des carrés est une base ; on peut se demander si le fait que l'ensemble des carrés est une base ne provient pas du résultat plus général :

Est-il vrai que l'ensemble des carrés des éléments d'une base est une base ?

Cette formulation nous conduit au problème plus général suivant.

PROBLEME. - Quelles sont les fonctions f de $\underset{\sim}{N}$ dans $\underset{\sim}{N}$ telles que pour toute base $\mathcal{B}$, l'ensemble $\{f(b) ; b \in \mathcal{B}\}$ soit une base ?

1. Quelques résultats positifs.

On peut démontrer sans difficulté le résultat suivant.

THÉORÈME 1. - Soient f une application de $\underset{\sim}{N}$ dans $\underset{\sim}{N}$ et α un nombre réel positif tel que

(i) $f(0) = 0$ et $f(1) = 1$,

(ii) $f(n) = \alpha n + O(1)$ lorsque n tend vers l'infini.

Alors l'image par f d'une base est une base.

Idée de la démonstration : Soient $\mathcal{A}$ une base et h son ordre ; on démontre que la suite $hf(\mathcal{A})$ est de densité asymptotique positive ; on en déduit que c'est une base, car elle contient 0 et 1.

2. Un critère pour les non-bases.

P. ERDÖS a proposé (communication privée) le critère suivant permettant de montrer qu'une suite d'entiers n'est pas une base.

CRITÈRE (N). - Soit $\mathcal{A}$ une suite d'entiers ; on suppose qu'il existe un nombre irrationnel α tel que :

$$\lim_{n\to\infty}(\{\alpha a_n\}) = 0 .$$

Alors, la suite $\mathcal{A}$ n'est pas une base.

Pour tout nombre réel positif ε, on posera :

$$\mathcal{A}'_\varepsilon = \{a_i \in \mathcal{A} ; \{\alpha a_i\} > \varepsilon\} \quad \text{et} \quad \mathcal{A}_\varepsilon = C_{\mathcal{A}}\, \mathcal{A}_\varepsilon .$$

On remarquera que $\mathcal{A}'_\varepsilon$ est un ensemble fini ; soit A'_ε un majorant de son cardinal.

Pour tout entier N, on a :

$$A(N) = A'_\varepsilon(N) + A_\varepsilon(N) \leq A'_\varepsilon + A_\varepsilon(N) \leq A'_\varepsilon + \#\{n \leq N ; \{\alpha n\} \leq \varepsilon\} .$$

De l'équirépartition modulo 1 de la suite αn, on déduit :

$$\limsup_{N\to\infty} \frac{A(N)}{N} \leq \limsup_{N\to\infty} \frac{1}{N} \#\{n \leq N ; \{\alpha n\} \leq \varepsilon\} \leq \varepsilon .$$

Cela démontre que la suite $\mathcal{A}$ a une densité asymptotique nulle, donc une densité de Šnirelman nulle.

Soit maintenant h un entier supérieur ou égal à 1. On suppose que la suite

h est de densité asymptotique nulle. On peut écrire :

$$(h+1)\mathfrak{a} = (\mathfrak{a}'_\varepsilon + h\mathfrak{a}) \cup (h+1)\mathfrak{a}_\varepsilon .$$

La suite $\mathfrak{a}'_\varepsilon + h\mathfrak{a}$, qui est la réunion d'un nombre fini de translatées de la suite $h\mathfrak{a}$, est de densité asymptotique nulle. Par ailleurs, tout entier m, élément de la suite $(h+1)\mathfrak{a}_\varepsilon$, satisfait la relation : $\{\alpha m\} \leq (h+1)\varepsilon$; on a donc

$$\limsup_{N\to\infty} \frac{1}{N} \#\{n \leq N \; ; \; n \in (h+1)\mathfrak{a}_\varepsilon\} \leq \limsup_{N\to\infty} \frac{1}{N} \#\{n \leq N \; ; \; \{\alpha n\} \leq (h+1)_\varepsilon\} \leq (h+1)\varepsilon .$$

La suite $(h+1)\mathfrak{a}_\varepsilon$ est donc de densité asymptotique inférieure à $(h+1)\varepsilon$ et il en est de même pour la suite $(h+1)\mathfrak{a}$ qui est incluse dans la réunion de $(h+1)\mathfrak{a}_\varepsilon$ et d'une suite de densité asymptotique nulle. Cela étant vrai pour tout nombre réel positif ε, la suite $h\mathfrak{a}$ est de densité asymptotique nulle.

On peut, de la même manière, démontrer le résultat suivant.

CRITÈRE (N'). - Soit $\mathfrak{a}$ une suite d'entiers ; on suppose qu'il existe un nombre irrationnel α tel que la suite $(\{\alpha a_n\})_{n\in N}$ n'ait qu'un nombre fini de points d'accumulations ; alors, la suite $\mathfrak{a}$ n'est pas une base.

3. Quelques résultats négatifs.

Nous nous proposons d'utiliser le critère (N), pour démontrer le résultat suivant.

THÉORÈME 2. - Il existe une base $\mathfrak{B}$ (d'ordre 3), telle que la suite constituée par les carrés des éléments de $\mathfrak{B}$ ne soit pas une base.

Ce théorème se déduit de la proposition 1 ci-dessous.

PROPOSITION 1. - On pose $\rho = (1+\sqrt{5})/2$. Pour tout nombre réel positif ε, la suite $\mathfrak{a}_\varepsilon = \{n \; ; \; \{\rho n^2\} \leq \varepsilon\}$ est une base asymptotique d'ordre 3 (tout entier supérieur à $(12/\varepsilon)^{27}$ est somme d'au plus trois éléments de $\mathfrak{a}_\varepsilon$).

Commençons par démontrer que le théorème 2 s'en déduit. On pose

$$\mathfrak{B} = \{n \in \underset{\sim}{N} \; ; \; \{\rho n^2\} \leq 12 n^{-1/27}\} ;$$

d'après le critère (N), la suite $\mathfrak{B}^{(2)} = \{b^2 \; ; \; b \in \mathfrak{B}\}$ n'est pas une base, et d'après la proposition 1, $\mathfrak{B}$ est une base d'ordre au plus trois.

Pour démontrer la proposition 1, nous utiliserons les trois lemmes suivants :

LEMME 1. - Soient P un nombre entier supérieur à 160, h un entier non nul, et α un nombre réel ; on a :

$$\left|\sum_{n=1}^{P} e(\rho h n^2 + \alpha n)\right| \leq 7P^{1/2}(1 + |h|^{1/2}) \quad \text{si} \quad |h| < \frac{3P^{1/2}}{4} .$$

Ce lemme s'obtient aisément en combinant l'inégalité fondamentale de van der CORPUT (cf. [1]) et le lemme 8a de VINOGRADOV (cf. [3], p. 24).

LEMME 2. - Soient P un entier positif, u et v deux entiers, et h un entier non nul ; on a :

$$|\sum_{n_1=u+1}^{u+P} \sum_{n_2=v+1}^{v+P} e(2\rho h n_1 \, n_2)| \leqslant 7P^{3/2}(1 + |h|^{1/2}) .$$

C'est un cas particulier du lemme 10b de VINOGRADOV ([3], p. 29).

LEMME 3 (J. F. KOKSMA [2]). - Soient a et b deux entiers positifs $(a < b)$, θ un nombre réel positif inférieur à 1, M un entier supérieur à 200, f_1, f_2 et f_3, trois applications de $[a , b[\times [a , b[$ dans $\underset{\sim}{R}$, on note :

$$S = S(a,b,\theta) = \#\{(n_1,n_2) \; ; \; a \leqslant n_i < b \, , \{f_j(n_1,n_2)\} \leqslant \theta \qquad (j = 1,2,3)\} .$$

On pose :

$$Ph_j = \begin{cases} 30|h_j|^{-1} & \text{si } h_j \neq 0 \\ 2 & \text{si } h_j = 0 \end{cases}$$

$$T = \sum^*_{(h_1,h_2,h_3)} |\sum_{n_1=a}^{b-1} \sum_{n_2=a}^{b-1} e(\sum_{j=1}^{3} h_j \, f_j(n_1 \, , n_2))| Ph_1 \, Ph_2 \, Ph_3 ,$$

où la première somme est étendue aux triplets non nuls (h_1 , h_2 , h_3) tels que $0 \leqslant |h_j| \leqslant M$; on a :

$$|S - \theta^3(b - a)^2| \leqslant T + (b - a)^2 \frac{1200}{M} .$$

Soit ε un nombre réel positif inférieur à 1, et N un entier supérieur à $(\frac{12}{\varepsilon})^{27}$; on va montrer qu'il existe deux entiers n_1, n_2 satisfaisant les relations :

$$(R) \qquad \begin{cases} 1 \leqslant n_1 \leqslant [\frac{N}{2}] = P \\ 1 \leqslant n_2 < [\frac{N}{2}] = P \\ \{\rho n_1^2\} \leqslant \varepsilon \quad \{\rho n_2^2\} \leqslant \varepsilon \quad \{\rho(N - n_1 - n_2)^2\} \leqslant \varepsilon . \end{cases}$$

Il est clair que la proposition 1 sera alors démontrée (en effet, on a : $N = (N - n_1 - n_2) + n_1 + n_2$).

On utilise le lemme 3, avec les notations :

$f_1(n_1 \, , n_2) : = \rho n_1^2$,

$f_2(n_1 \, , n_2) : = \rho n_2^2$,

$f_3(n_1 \, , n_2) : = \rho(N - n_1 - n_2)^2$,

$a : = 1$,

$b : = [\frac{N}{2}] = P$,

$\theta : = \varepsilon$.

Il nous faut donc évaluer les sommes

$$T_{h_1,h_2,h_3} = |\sum_{n_1=1}^{P} \sum_{n_2=1}^{P} e(\rho(h_1 \, n_1^2 + h_2 \, n_2^2 + h_3(N - n_1 - n_2)^2)| .$$

Considérons trois cas :

(a) $h_1 + h_3 \neq 0$; on a alors :

$$T_{h_1,h_2,h_3} \leqslant \sum_{n_2=1}^{P} \left|\sum_{n_1=1}^{P} e(\rho(h_1+h_3)\, n_1^2 + \beta n_1)\right| \leqslant 10P^{3/2}(1 + M^{1/2})$$

d'après le lemme 1.

(b) $h_2 + h_3 \neq 0$; on obtient la même majoration de façon similaire.

(c) $h_3 = - h_1 = - h_2$; d'après le lemme 2, on a :

$$T_{h_1,h_2,h_3} = \left|\sum_{n_1=1}^{P} \sum_{n_2=1}^{P} e(2\rho h_3(n_1 - N)(n_2 - N))\right| \leqslant 10P^{3/2}(1 + M^{1/2}) .$$

On pose alors $M = P^{1/9}$ (loisible si $N > 1,1.10^{21}$) , on obtient :

$$T_{h_1,h_2,h_3} \leqslant 88P^{17/9} .$$

Avec les notations du lemme de Koksma, on a : $|S - \varepsilon^3 P^2| \leqslant 1288\, P^{17/9}$. Si P est supérieur à $\frac{1}{2}(12/\varepsilon)^{27}$, S est non nul, c'est-à-dire qu'il existe deux entiers n_1 , n_2 satisfaisant les conditions (R) ; la proposition 1 est donc démontrée.

Remarquons que la même méthode permet de démontrer que, pour toute fonction "assez régulière" f telle que $\lim_{x\to\infty} \frac{f(x)}{x} = +\infty$ (e. g. $f(n) = [n^c]$, $c > 1$; $f(n) = [n \log n]$), il existe une base $\mathfrak{B}$ telle que $f(\mathfrak{B})$ ne soit pas une base.

On mentionnera enfin, sans démonstration, le résultat encore plus surprenant suivant :

THÉORÈME 3. - Il existe une suite $\mathfrak{a}$ qui n'est pas une base, telle que l'ensemble des carrés des éléments de $\mathfrak{a}$ constitue une base.

La démonstration (assez compliquée) de ce résultat, qui utilise la "méthode du cercle", sera publiée ultérieurement.

BIBLIOGRAPHIE

[1] CORPUT (J. G. van der). - Neue zahlentheorische Abschätzungen, Math. Z., t. 29, 1929, p. 397-426.

[2] KOKSMA (J. F.). - Some theorems on Diophantine inequalities, Math. Centrum, Amsterdam, Scriptum n° 5, 1950, 52 p.

[3] VINOGRADOV (I. M.). - The method of trigonometrical sums in the theory of numbers. - London, Interscience Publishers, 1954.

(Texte reçu le 25 février 1974)

Jean-Marc DESHOUILLERS
[E. R. A. du C. N. R. S. n° 362]
U. E. R. de Math. et Inform.
Université de Bordeaux I
351 cours de la Libération
33405 TALENCE
et
Centre de Mathématiques
Ecole Polytechnique
17 rue Descartes
75230 PARIS CEDEX 05