François Dress

Théorie additive des nombres et problème de Waring

Séminaire de théorie des nombres de Bordeaux (1970-1971), exp. nº 26, p. 1-9
<http://www.numdam.org/item?id=STNB_1970-1971____A26_0>

Séminaire de Théorie des Nombres
Année 1970-1971 - exposé n° 28

18 Mai 1971

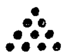
THÉORIE ADDITIVE DES NOMBRES
ET
PROBLÈME DE WARING

par

François DRESS

-:-:-:-

§. I. - INTRODUCTION HISTORIQUE

Depuis Pythagore, de très nombreux mathématiciens se sont intéressés aux propriétés "magiques" des nombres entiers, en particulier des nombres triangulaires, des nombres carrés, des nombres m -gonaux (les nombres triangulaires sont les entiers de la forme $n(n+1)/2$: nombre des éléments d'un triangle de points de base n ,  par exemple, les nombres carrés sont les carrés : nombres d'éléments d'un carré de points, etc...).

C'est Bachet qui semble avoir remarqué le premier, en 1621, que tout entier positif pouvait s'écrire comme somme de 4 carrés (certains étant éventuellement nuls), encore qu'il y ait quelques raisons de penser que Diophante connaissait déjà ce résultat empirique. Ensuite Fermat a noté, en 1936, que tout entier positif pouvait s'écrire comme somme de 3 nombres triangulaires, de 4 carrés, de m nombres m -gonaux (on s'apercevra plus tard que le résultat général n'est pas le meilleur possible).

Ainsi, pour les nombres triangulaires :

. . . .

$$12 = 10 + 1 + 1 = 6 + 6 + 0 = 6 + 3 + 3$$

$$13 = 10 + 3 + 0 = 6 + 6 + 1$$

$$14 = 10 + 3 + 1$$

$$15 = 15 + 0 + 0 = 6 + 6 + 3$$

$$16 = 15 + 1 + 0 = 10 + 6 + 0 = 10 + 3 + 3$$

. . . .

et pour les carrés :

. . . .

$$12 = 9 + 1 + 1 + 1 = 4 + 4 + 4 + 0$$

$$13 = 9 + 4 + 0 + 0 = 4 + 4 + 4 + 1$$

$$14 = 9 + 4 + 1 + 0$$

$$15 = 9 + 4 + 1 + 1$$

$$16 = 16 + 0 + 0 + 0 = 4 + 4 + 4 + 4$$

. . . .

Fermat avait ajouté, dans la lettre à Mersenne où il indiquait cette découverte, qu'il n'avait pas la place d'en donner la démonstration, mais qu'il y consacrerait un livre entier. Le livre ne fut jamais publié. . . On peut d'ailleurs douter que Fermat ait été en possession d'une démonstration correcte car des efforts infructueux furent déployés pendant plus d'un siècle, par Euler en particulier, pour tenter de résoudre ce problème. C'est finalement Lagrange, en 1770, qui en donna la première démonstration.

En même temps d'autres théorèmes empiriques, de nature additive également, étaient énoncés. Les deux plus célèbres sont le problème de Goldbach, formulé en 1742 dans une lettre à Euler : tout entier pair est-il somme de 2 nombres premiers ? et le problème de Waring, formulé en 1770 dans un livre (avec addition du "etc. . . " dans l'édition de 1782 !) : tout entier positif est-il somme de 9 cubes, de 19 bicarrés, etc. . . ?

Ces questions sont, malgré la simplicité de leur énoncé, extrêmement ardues et l'intervalle qui sépare l'énoncé empirique de sa démonstration se compte en dizaines d'années ou plus souvent en siècles (phénomène assez courant en arithmétique !).

§. II. - NOTIONS FONDAMENTALES EN THÉORIE ADDITIVE DES NOMBRES

En donnant le premier résultat partiel intéressant dans le problème de Godbach, Schnirelman esquissa, en 1930, un cadre général pour tous les problèmes additifs relatifs à des suites d'entiers.

Etant donné deux suites croissantes d'entiers scritement positifs $A = \{a_1 < a_2 < \dots\}$ et $B = \{b_1 < b_2 < \dots\}$, on appelle somme de A et B et on note $A + B$ la suite croissante obtenue en réordonnant l'ensemble $A \cup B \cup \{a_i + b_j \mid a_i \in A,\ b_j \in B\}$ (on convient parfois que $a_o = 0 \in A$, $b_o = 0 \in B$, auquel cas on considère simplement l'ensemble $\{a_i + b_j\}$).

On peut en particulier effectuer les sommes $A + A = 2A$, $A + A + A = 3A$, $A + \dots + A = hA$, ... On dit alors que la suite A est une <u>base</u> des entiers (d'ordre $\leq h$) s'il existe h tel que $hA = \mathbb{N}$ (A est exactement d'ordre h si $(h-1)A \subsetneqq \mathbb{N}$). On peut également définir la notion de base relativement à une sous-suite de $\mathbb{N}$ (les entiers pairs dans le problème de Goldbach, par exemple).

Etant donné une suite $A = \{a_k\}$, on définit la fonction $A(n) = \sum_{1 \leq a_k \leq n} 1 =$ nombre des a_k compris entre 1 et n. On définit ensuite la <u>densité de Schnirelman</u> de la suite A par :

$$d(A) = \inf_n \frac{A(n)}{n} .$$

Cette définition appelle deux remarques. Primo, on a $1 \in A$ dès que $d(A) > 0$. Secundo, la notion de densité de Schnirelman est très différente de celle, classique, de densité asymptotique, définie par $\liminf \frac{A(n)}{n}$. En particulier, $d(A) = 1$ équivaut à $A = \mathbb{N}$, tandis que d. asympt. $(A) = 1$ équivaut à "presque tous les entiers appartiennent à A". Indiquons enfin une notion intermédiaire, "tous les entiers assez grands appartiennent à A", fréquemment utilisée en théorie additive (théorème de Vinogradov sur les entiers impairs sommes de 3 nombres premiers, constantes $G(k)$ du problème de Waring).

§. III. - THEORÈMES DE SCHNIRELMAN ET DE MANN

La densité de Schnirelman est un outil remarquable pour prouver que certaines suites sont des bases. Il ne faut pas cependant en attendre plus que des résultats d'existence, avec au mieux une majoration délirante de l'ordre (2.10^{10} pour les nombres premiers, nettement pire dans le problème de Waring par la méthode de Linnik et Khintchine, par exemple), en raison de l'influence très pathologique des premiers termes de la suite (et comme "premiers" n'est jamais que le contraire de "à l'infini", cela peut entraîner fort loin ... !).

Les principaux théorèmes en la matière sont les suivants :

THÉORÈME. (Schnirelman [2] 1930). $d(A+B) \geq d(A) + d(B) - d(A)d(B)$.

La démonstration, que nous ne donnerons pas ici, est fort simple et s'appuie, modulo la minoration $\forall n[A(n) \geq n.\, d(A)]$, sur un dénombrement très banal.

LEMME. $d(A) + d(B) \geq 1 \Rightarrow A+B = \mathbb{N}$.

Une simple affaire de tiroirs tout aussi banale.

COROLLAIRE. Toute suite de densité de Schnirelman strictement positive est une base.

En effet, l'inégalité de Schnirelman peut s'écrire

$$(1-d(A+B)) \leq (1-d(A))(1-d(B)).$$

Il s'ensuit, en particulier, que $(1-d(hA)) \leq (1-d(A))^h \leq \frac{1}{2}$ si $d(A) > 0$ et $h \geq h_o$. Et le lemme précédent entraîne immédiatement que $2h_oA = \mathbb{N}$.

Schnirelman [2] a ainsi prouvé que la suite $P = \{1\} \cup \{$nombres premiers$\}$ était une base en démontrant par une méthode de crible que $d(2P) > 0$.

THÉORÈME (Mann [5], 1942). $d(A+B) \geq \min(d(A)+d(B), 1)$.

La démonstration de ce théorème est assez ardue et il faut ajouter qu'il représente en un sens le meilleur résultat possible. Si l'on a par exemple (k étant un entier ≥ 2)

$$A = B = (1, k+1, 2k+1, \ldots),$$

alors

$$A + B = (1, 2, k+1, k+2, 2k+1, 2k+2, \ldots),$$

cependant que l'on a $d(A) = d(B) = \frac{1}{k}$ et $d(A+B) = \frac{2}{k} = d(A) + d(B)$.

§. IV. - <u>COMPOSANTES ESSENTIELLES</u>

Une conséquence des théorèmes de Schnirelman et de Mann est qu'une suite M de densité strictement positive augmente la densité de toute suite A telle que $0 < d(A) < 1$: $d(A+M) > d(A)$.

Mais il existe des suites de densité nulle qui possèdent également cette propriété (par exemple la suite des carrés des entiers : Khintchine [3]). Toute suite possédant cette propriété s'appelle une <u>composante essentielle.</u>

Erdös a démontré que toute base était une composante essentielle ou, plus précisément, le résultat suivant ([4], 1936) :

THÉORÈME. <u>Si</u> B <u>est une base d'ordre</u> h <u>alors</u>, <u>pour toute suite</u> A <u>telle que</u> $0 < d(A) < 1$, <u>on a</u> $d(A+B) \geq d(A) + \frac{d(A)(1-d(A))}{2h}$.

Cette inégalité a été améliorée, mais pas très sensiblement. De fait, on a montré que l'inégalité $d(A+B) \geq d(A) + \frac{d(A)(1-d(A))}{h}$ était fausse.

Après ce théorème d'Erdös, la question qui se pose naturellement est de savoir s'il existe des composantes essentielles qui ne soient pas des bases (ni, a fortiori, des suites de densité positive). Il en existe un exemple trivial :

$$M = (2, 3, 4, 5, \ldots) .$$

M n'est pas une base car $1 \notin M$ ni $1 \notin hM$ pour tout h , mais $d(A+M) = 1 > d(A)$ dès que $d(A) > 0$, car alors $1 \in A$ et $A + M = \mathbb{N}$.

Le premier exemple "intéressant" de composante essentielle M qui ne soit pas une base est dû à Linnik ([6], 1942). Cet exemple satisfait $M(n) = o(x^{\varepsilon})$ pour tout $\varepsilon > 0$ mais il n'est pas constructible avec des méthodes "élémentaires".

Stöhr et Wirsing ([10], 1956) ont donné un exemple élémentaire vérifiant seulement $M(n) = o(n)$. Leur construction est fondée sur un résultat précédent de Stöhr montrant qu'il est possible d'obtenir des base B_h d'ordre h , vérifiant $B_h(n) = o(n)$ et augmentant uniformément la densité de toute suite de densité positive (i. e. $d(A) > 0 \Rightarrow d(A+B_h) \geq d(A) + \frac{d(A)(1-d(A))}{2}$ pour toute B_h) .

§. V. - GÉNÉRALITÉS SUR LE PROBLÈME DE WARING

Nous en avons déjà vu l'énoncé : pour $k = 2, 3, 4, \ldots$, la suite des puissances k-ièmes est-elle une base ? La réponse est affirmative, et l'on désigne traditionnellement par $g(k)$ l'ordre de cette base. Pour les premières valeurs de k , l'évidence empirique conduit à conjecturer les valeurs suivantes :

$$g(2) = 4 \quad , \quad g(3) = 9 \quad , \quad g(4) = 19 \ .$$

En exceptant le théorème des 4 carrés de Lagrange, la première démonstration d'existence, dans le cas particulier des bicarrés, est due à Liouville, en 1859, avec la majoration $g(4) \leq 53$.

Puis on s'apercevra assez vite que, moyennant une identité algébrique "convenable" (que l'on découvrira effectivement pour les petites valeurs de k), l'existence de $g(k)$ entraîne celle de $g(2k)$, avec une majoration du style $g(2k) \leq a_k\, g(k) + b_k$.

Par contre, les valeurs impaires de k posent des problèmes délicats, car les identités ont alors une tendance fâcheuse à fournir des sommes de puissances k-ièmes dont certaines sont négatives ! Enfin Maillet réussit en 1895, à démontrer l'existence dans le cas des cubes, et donne la majoration $g(3) \leq 21$.

De nouveaux cas sont résolus, les majorations sont petit à petit améliorées, puis Hilbert ([1], 1909), démontre le théorème général d'existence de $g(k)$. Le théorème de Hilbert ne donnant aucune majoration explicite, la course aux majorations continue donc, et continue toujours... mais surtout pour une autre constante dont nous allons parler maintenant.

En 1909 également, Wieferich prouve que $g(3) = 9$, cependant que Landau montre qu'il existe N_o tel que tout entier supérieur à N_o soit somme d'au plus 8 cubes. En d'autres termes, la valeur de $g(3)$ dépend d'un nombre fini d'entiers - en fait 23 et 239 - qui sont seuls à exiger 9 cubes, et ne réflète nullement les propriétés "à l'infini". Plus généralement on est amené à définir $G(k)$ le minimum de p, tel que tout entier suffisamment grand soit somme d'au plus p puissances k-ièmes. La disproportion entre les deux constantes est énorme : on sait actuellement que $g(k)$ est équivalent à 2^k, tandis que l'on dispose pour $G(k)$ de majorations de l'ordre de $k \operatorname{Log} k$.

Pour en terminer avec le problème de Waring, on notera que Hardy et Littlewood en 1920, puis Vinogradov en 1924, ont introduit des méthodes analytiques extrêmement puissantes qui permettent d'obtenir des résultats numériques remarquables ; cependant qu'une démonstration du théorème de Hilbert par la méthode de Schnirelman (il existe ℓ_k tel que $d(\ell_k A^{(k)}) > 0$, $A^{(k)}$ étant la suite $\{1, 2^k, 3^k, \ldots\}$) a été trouvée en 1943 par Linnik ([7]), puis améliorée par Khintchine ([8]).

§. VI. - PROBLÈMES DIVERS

L'imagination des mathématiciens s'est donnée libre cours pour poser, et parfois résoudre, de nombreux problèmes en théorie additive des nombres.

On en donnera juste un exemple (Lorentz, [9]) :

THEORÈME. A toute suite A on peut associer une suite B qui vérifie :

- tous les entiers assez grands appartiennent à $A+B$;
- $B(n) \leq c \sum_{k=1}^{n} \frac{\log A(k)}{A(k)}$.

Si $d(A) = \delta > 0$ par exemple, on en déduit $\frac{\log A(k)}{A(k)} \leq \frac{\log \delta k}{\delta k}$ (car $A(k) \geq \delta k$), et donc que la suite B est assez rare : $B(n) \leq c' \log^2 n$ (inégalité qui ne peut être améliorée, comme l'a montré Erdös par des arguments probabilistes, (i. e. en mettant une mesure sur l'espace des suites).

-:-:-:-

BIBLIOGRAPHIE HISTORIQUE

[1] HILBERT. - Beweis für die Darstellbarkeit der ganzen Zahle durch eine feste Anzahl n-ter Potenzen (Waringsches Problem). Math. Ann. t. 67, 1909, p. 281-300.

[2] SCHNIRELMAN. - Sur les propriétés additives des nombres [en russe], Izv. Donetz polytech. in. ta., t. 14, 1930, p. 3-28.

[3] KHINTCHINE. - Über ein metrisches Problem der additiven Zahlentheorie, Mat. Sbornik, N. S., t. 40, 1933, p. 180-189.

[4] ERDÖS. - On the arithmetical density of the sum of two sequences, one of which forms a basis for the integers, Acta Arithm., Warszawa, t. 1, 1936, p. 197-200.

[5] MANN. - A proof of the fundamental theorem on the density of sums of sets of positive integers, Annals of Math., 2e série, t. 43, 1942, p. 523-527.

[6] LINNIK. - On Erdös's theorem on the addition of numerical sequences, Mat. Sbornik, N. S., t. 52, 1942, p. 67-78.

[7] LINNIK. - Solution élémentaire du problème de Waring d'après la méthode de Schnirelman [en russe], Mat. Sbornik, N. S., t. 54, 1943, p. 225-230.

[8] KHINTCHINE. - Trois théories liées en théorie des nombres, Fizmatgiz, 1948.

[9] LORENTZ. - On a problem of additive number theory, Proc. Amer. Math. Soc., t. 5, 1954, p. 838-841.

[10] STÖHR und WIRSING. - Beispiele von wesentlichen Komponenten, die keine Basen sind, J. für reine und angew. math., t. 196, 1956, p. 96-98.

OUVRAGES

[11] KHINTCHINE. - Three pearls in the theory of numbers. - Rochester, Graylock Press, 1952.

[12] HALBERSTAM and ROTH. - Sequences. Vol. 1, Oxford, at the Clarendon Press, 1966.

[13] OSTMANN. - Additive Zahlentheorie. Berlin, Göttingen, Heidelber, Springer-Verlag, 1956 (Ergebnisse der Mathematik und ihrer Grenzgebiete. Neue Folge. Heft 11).

-:-:-:-

François DRESS
U.E.R. de Mathématiques
et d'Informatique
Université de Bordeaux 1
351, cours de la Libération
33 - T A L E N C E