Séminaire DELANGE-PISOT-POITOU
(Théorie des nombres)
15e année, 1973/74, n° 1, 4 p.

15 octobre 1973

METHODES PROBABILISTES EN THEORIE DES NOMBRES

par Paul ERDÖS

Rédigé par Jean-Louis NICOLAS

1. Etablir des conjectures.

Les méthodes probabilistes permettent d'établir des conjectures en théorie des nombres. C'est ainsi que CRAMER [1], observant que, pour presque toutes les suites a_n vérifiant $a_n \sim n \log n$, on avait

$$\overline{\lim} \frac{a_{n+1} - a_n}{(\log n)^2} = 1$$

a conjecturé que l'on avait pour p_n la suite des nombres premiers

$$\overline{\lim} \frac{p_{n+1} - p_n}{(\log n)^2} = 1 .$$

Les meilleurs résultats sur la différence $p_{n+1} - p_n$ sont très loin de cette conjecture : HUXLEY [10] a démontré que, pour tout $\varepsilon > 0$, on avait

$$p_{n+1} - p_n = O(p_n^{(7/12)+\varepsilon}) ,$$

et d'autre part RANKIN [13] a montré que, pour tout $\varepsilon > 0$, l'inégalité

$$p_{n+1} - p_n \geq (e^{\gamma} - \varepsilon)\log p_n \frac{(\log \log p_n)(\log \log \log \log p_n)}{(\log \log \log p_n)^2}$$

était vérifiée une infinité de fois (γ est la constante d'Euler).

2. Fonction de répartition.

Le livre de références est celui de KUBILIUS [11] dont l'introduction fait un très bon historique de la question et qui donne de nombreuses références, dont 9 articles de H. DELANGE qui a contribué à l'étude de ces problèmes.

Définition. - On dit qu'une fonction f de $\underline{N}$ dans $\underline{R}$ a une fonction de répartition F, si, pour tout x réel, on a :

$$\lim \frac{1}{x} \operatorname{card}\{n \in \underline{N} ; \ f(n) \leq x\} = F(x) .$$

DAVENPORT [2] a montré que $\sigma(n)/n$, où $\sigma(n)$ est la somme des diviseurs de n, a une fonction de répartition continue (cf. aussi [15]). SCHOENBERG a montré que $\varphi(n)/n$, où φ est l'indicateur d'Euler, a aussi une fonction de répartition [14].

Une fonction est dite additive, si, pour m et n premiers entre eux, on a $f(mn) = f(m) f(n)$, et fortement additive si on a toujours $f(mn) = f(m) f(n)$. ERDÖS et WINTNER [5] ont démontré qu'une fonction arithmétique additive a une fonction de répartition si, et seulement si, les séries

$$\sum_{p \text{ premier}} \frac{f'(p)}{p} \quad \text{et} \quad \sum_{p \text{ premier}} \frac{(f'(p))^2}{p}$$

sont convergentes, avec $f'(p) = f(p)$ si $f(p) < 1$, et $f'(p) = 1$ si $f(p) > 1$ (cf. [11], théorème 4.5, p. 74).

En 1936, ERDÖS [4] a démontré : Soit $\omega(n)$ le nombre de diviseurs premiers de n, on a

$$\frac{1}{x}\,\mathrm{card}\{n \leq x \ ; \ \omega(n) \geq \log\log n\} = \frac{1}{2}\ .$$

Ce résultat a été généralisé avec KAC [6] grâce au théorème central limite des probabilités et au crible de Brun.

THÉORÈME (ERDÖS-KAC). - Soit f une fonction fortement additive vérifiant $|f(p)| \leq M$ pour tout p premier, et telle que les séries

$$\sum_{p \text{ premier}} \frac{f(p)}{p} \quad \text{et} \quad \sum_{p \text{ premier}} \frac{f(p)^2}{p}$$

soient divergentes. On pose

$$A(x) = \sum_{p<x} \frac{f(p)}{p} \quad \text{et} \quad B(x) = \Big(\sum_{p<x} \frac{f(p)^2}{p}\Big)^{\frac{1}{2}}\ .$$

Alors on a :

$$\lim \frac{1}{x}\,\mathrm{card}\{n \leq x \ ; \ f(n) \leq A(x) + tB(x)\} = G(t)\ ,$$

où

$$G(t) = \frac{1}{2\pi}\int_{-\infty}^{t} \exp(-x^2/2)\,dx\ .$$

La démonstration se trouve dans KUBILIUS ([11], théorème 4.2, p. 61). Elle est basée sur le fait qu'une fonction fortement additive est la somme de variables aléatoires X_p qui valent $f(p)$ avec la probabilité $\frac{1}{p}$, et 0 avec la probabilité $(1 - \frac{1}{p})$.

3. Comportement de $f(n)$ par rapport à $f(n+1)$.

Si f est une fonction additive qui satisfait aux conditions du théorème de Erdös-Kac, on peut montrer (LEVÊQUE [12]) que $f(n)$ et $f(n+1)$ se comportent comme des variables indépendantes. En particulier, si $d(n)$ est le nombre de diviseurs de n, l'ensemble des n vérifiant $d(n+1) > d(n)$ a pour densité $1/2$; et de même pour $\omega(n)$, le nombre de diviseurs premiers de n (ERDÖS [3]). On ne sait rien dire sur les entiers n tels que $\omega(n+1) = \omega(n)$.

Si l'on choisit pour f la fonction fortement additive, définie par $f(p) = \log p$, alors $f(n) = \log n$, et on a toujours $f(n+1) > f(n)$. Par contre, si l'on choisit $f(p) = p$ ou $f(p) = (\log p)^{\alpha}$ avec $\alpha > 0$, $\alpha \neq 1$, on ne peut rien dire sur la densité des n tels que $f(n+1) > f(n)$, car les grands nombres premiers sont décisifs.

Soit $g(n)$ une fonction donnée. On pose $f(n) = p$, où p est le plus petit diviseur de n vérifiant $p > g(n)$. Si, pour tout $\varepsilon > 0$, $g(n) = o(n^{\varepsilon})$, alors les n, tels que $f(n+1) > f(n)$, ont pour densité $1/2$. Mais si $g(n) = n^{c}$, $c > 0$, on ne sait rien.

Rappelons qu'une fonction additive et croissante est proportionnelle à $\log n$. Une fonction f , vérifiant

$$\lim_{n\to\infty} f(n+1) - f(n) = 0 ,$$

est aussi proportionnelle à $\log n$. Enfin WIRSING [16] a récemment démontré que si f additive vérifiait

$$f(n+1) - f(n) \leq C ,$$

on avait $f(n) = a \log n + g(n)$ avec $g(n)$ borné.

4. Problèmes de base additive d'ordre 2 .

Pour ce genre de problème, voir le livre de HALBERSTAM et ROTH ([9], chapitre 3).

Etant donnée une suite (a_i) , on appelle $g(n)$ le nombre de représentations $n = a_i + a_j$. SIDON avait demandé s'il était possible de trouver une suite (a_i) telle que $g(n) > 0$ pour tout n assez grand, mais telle que $g(n) = O(n^\varepsilon)$ pour tout ε . ERDÖS [7] a résolu ce problème par un argument probabilistique, et a même démontré que, pour presque toutes les suites, on avait :

$$c_1 \log n \leq g(n) \leq c_2 \log n .$$

Mais on ne connait pas de suite explicite pour laquelle ces inégalités sont vérifiées. On ne sait pas non plus s'il existe une suite telle que

$$\lim_{n\to\infty} g(n)/\log n = c > 0 .$$

- CONJECTURE (primée 1000 francs suisses). - Pour toute suite, telle que $g(n) > 0$ à partir d'un certain rang, on a $\overline{\lim}\, g(n) = \infty$. Peut-être a-t-on

$$\overline{\lim} \frac{g(n)}{\log n} > 0 .$$

Une conjecture plus forte est la suivante. Pour toute suite (a_k) , vérifiant $a_k < ck^2$, on a $\overline{\lim}\, g(n) = \infty$.

5. Problème de Erdös et Moser.

Etant donné x , trouver $k = f(x)$ le nombre maximum d'entiers $a_1 < a_2 < \ldots < a_k < x$ tels que les sommes $\sum_{i=1}^{k} \varepsilon_i a_i$, où ε_i vaut 0 ou 1 , soient toutes distinctes.

Si l'on prend $x = 2^k$ et $a_i = 2^{i-1}$, on voit que $f(2^k) \geq k$. Si l'on prend $x = 8$, les nombres 3 , 5 , 6 , 7 forment une meilleure famille. CONWAY et GUY ont un exemple numérique non publié de 24 nombres inférieurs à 2^{22} ayant la propriété.

Par une méthode probabiliste, MOSER et ERDÖS [8] ont montré

$$f(x) \leq \frac{\log x}{\log 2} + \frac{\log \log x}{2 \log 2} + c .$$

CONJECTURE. - Montrer que $f(x) < (\log x/\log 2) + c$, et trouver un exemple numérique avec $f(2^k) \geq k + 3$.

BIBLIOGRAPHIE

[1] CRAMER (H.). - On the order of magnitude of the difference between consecutive prime numbers, Acta Arithmetica, Warszawa, t. 2, 1937, p. 23-46.

[2] DAVENPORT (H.). - Uber numeri abundantes, Sitzungsber. Akad. Berlin, 1933, p. 830-837.

[3] ERDÖS (P.). - On a problem of Chowla and some related problems, Proc. Cambridge philos. Soc., t. 32, 1936, p. 530-540.

[4] ERDÖS (P.). - Note on the number of prime divisors of integers, J. London math. Soc., t. 12, 1937, p. 308-314.

[5] ERDÖS (P.) and WINTNER (A.). - Additive arithmetic functions and statistical independance, Amer. J. of Math., t. 61, 1939, p. 713-722.

[6] ERDÖS (P.) and KAC (M.). - The Gaussian law of errors in the theory of additive number theoretic functions, Amer. J. of Math., t. 62, 1940, p. 738-742.

[7] ERDÖS (P.). - On a problem of Sidon in additive number theory, Acta Scient. Math., Szeged, t. 15, 1954, p. 255-259.

[8] ERDÖS (P.). - Problems and results in additive number theory, "Colloque sur la théorie des nombres [1955. Bruxelles]", p. 127-137. - Liège, G. Thone ; Paris, Masson, 1956 (Centre belge de Recherches mathématiques).

[9] HALBERSTAM (H.) and ROTH (K. F.). - Sequences. - Oxford, at the Clarendon Press, 1966.

[10] HUXLEY (M. N.). - The distribution of prime numbers. Large sieves and zero-density theorems. - Oxford, at the Clarendon Press, 1972 (Oxford mathematical Monographs).

[11] KUBILIUS (J.). - Probabilistic methods in the theory of numbers, vol. 11. Translations of mathematical Monographs.

[12] LEVÊQUE (W. J.). - On the size of certain number theoretic functions, Trans. Amer. math. Soc., t. 66, 1949, p. 440-463.

[13] RANKIN (R. A.). - The difference between consecutive prime numbers, V, Proc. Edimburgh math. Soc., t. 13, 1963, p. 331-332.

[14] SCHOENBERG (I. J.). - On asymptotic distributions of arithmetical functions, Trans. Amer. math. Soc., t. 39, 1936, p. 315-330.

[15] WALL (C. R.). - Density bounds for the sum of divisors function, "The theory of arithmetic functions [1971. Kalamazoo]", p. 283-287. - Berlin, Springer-Verlag, 1972 (Lecture Notes in Mathematics, 251).

[16] WIRSING (E.). - A characterization of $\log n$ as an additive arithmetic function, "Symposia Mathematica, vol. 4 : Teoria dei numeri [1968. Roma], p. 45-57. - London and New York, Academic Press, 1970 (Istituto nazionale di Alta Matematica).

(Texte reçu le 24 juin 1974)

Paul ERDÖS
Magyar Tudomanyos Akademia
Matematikai Kutoto Intezete
Realtanoda u. 13-15
BUDAPEST V (Hongrie)