Séminaire DELANGE-PISOT-POITOU
(Théorie des nombres)
14e année, 1972/73, n° 24, 7 p.

21 mai 1973

RÉSULTATS ET PROBLÈMES EN THÉORIE DES NOMBRES

par Paul ERDÖS

Rédigé par Jean-Louis NICOLAS

1. Un théorème de Van der Waerden et les fonctions $r_k(n)$.

Pour une étude plus détaillée, d'autres références et d'autres conjectures, on pourra voir [10] (p. 220-224) et [11] (p. 232). De façon générale, ces deux articles font le point sur plusieurs sujets de théorie des nombres et sont une mine inépuisable de conjectures et de problèmes ouverts. Comme autres recueils de problèmes, on pourra consulter aussi [12] et [13].

VAN DER WAERDEN a démontré le théorème suivant (cf. [32], [19], [23], et surtout [33] où l'auteur expose le cheminement de son raisonnement dans sa découverte du théorème).

THÉORÈME. - Si l'on fait une partition de l'ensemble $\mathbb{N}$ des entiers en deux classes, quel que soit l'entier k, une au moins des deux classes contient une progression arithmétique de k termes.

Définissons $f(k)$ comme le plus petit entier tel que, si l'on partage les nombres $1 \leq n \leq f(k)$ en deux classes arbitraires, l'une au moins contient une progression arithmétique de k termes. La majoration de $f(k)$ est un problème difficile, et la démonstration de VAN DER WAERDEN donne une majoration par quelque chose de beaucoup plus grand que

$$k^{k^{k^{\cdot^{\cdot^{\cdot}}}}} \quad k \text{ fois.}$$

BERLEKAMP [4] a donné pour $f(k)$ la minoration $f(k) \geq k2^k$ en partageant les entiers n, $1 \leq n \leq k2^k$, en deux classes ne contenant aucune progression arithmétique de k termes, à l'aide du corps fini à 2^k éléments.

Pour aborder la majoration de $f(k)$, on est amené à la définition suivante.

Définition. - On désigne par $r_k(n)$ le nombre maximum de termes d'une suite finie $(a_i)_{1 \leq i < \ell}$ vérifiant $1 \leq a_1 < a_2 < \ldots < a_\ell \leq n$ et ne contenant pas une progression arithmétique de k termes.

Une famille de plus de $r_k(n)$ nombres, tous plus petits que n, contient donc forcément une progression arithmétique de k termes et si, pour un certain n, on savait démontrer $r_k(n) < n/2$, cela donnerait pour $f(k)$ la majoration $f(k) < n$.

Exemples.

$r_3(5) = 4$ avec $(a_i) = 1 , 2 , 4 , 5$.

$r_3(14) = 8$ avec $(a_i) = 1 , 2 , 4 , 5 , 10 , 11 , 13 , 14$.

Propriété. - On a $r_k(n + n') \leq r_k(n) + r_k(n')$ (pour cela, et pour d'autres propriétés élémentaires de $r_k(n)$, cf. [14]).

BEHREND [2] a démontré l'existence de

$$c_k = \lim_{k\to\infty} \frac{r_k(n)}{n} .$$

Il a montré également que l'on avait " $c_k = 0$ pour tout k " ou bien " $\lim_{k\to\infty} c_k = 1$ " . En 1942, SALEM [28] a démontré que

$$r_3(n) > n^{1-(c/\log\log n)}$$

(On peut obtenir une minoration simple de $r_3(n)$ en constatant que la suite des nombres qui s'écrivent dans la base 3 avec uniquement les chiffres 0 et 2 ne contient pas trois termes en progression arithmétique). En 1946, BEHREND [3] a amélioré le résultat de SALEM en montrant :

$$r_3(n) > n^{1-(c/\sqrt{\log n})} .$$

D'autre part, ROTH [27] a majoré $r_3(n)$ obtenant :

$$r_3(n) < C \frac{n}{\log\log n} .$$

En 1968, SZEMEREDI [31], dans une démonstration compliquée, a montré que

$$\lim_{n\to\infty} \frac{r_4(n)}{n} = 0 .$$

Plus récemment, dans un article à paraître aux Acta Arithmetica, il a démontré que

$$\lim_{k\to\infty} \frac{r_k(n)}{n} = 0 \quad \text{pour tout } k .$$

Conjecture 1. - Si l'on peut démontrer

$$r_k(n) < \pi(n) = \text{nombre des nombres premiers} \leq n ,$$

cela entraîne qu'il existe k nombres premiers formant une progression arithmétique.

Exemple numérique. - $199 + 210\ell$ avec $0 \leq \ell \leq 9$ est une progression arithmétique de 10 termes. D'après A. SCHINZEL, le record serait une progression arithmétique de 16 nombres premiers.

Conjecture 2. - Si la suite infinie $a_1 < a_2 < \ldots$ ne contient pas une progression arithmétique de 3 termes, alors $\sum_{i=1}^{\infty} 1/(a_i) < +\infty$. La conjecture de Goldbach (cf. PRACHAR, [22], p. 177) "tout nombre pair est somme de deux nombres premiers" entraîne, pour un nombre premier p_1 , que $2p_1 = p_2 + p_3$. CHOWLA [7] a démontré, sans hypothèse, qu'il existe une infinité de triplets de nombres premiers en progression arithmétique, mais l'on a

$$\sum_{p \text{ premier}} \frac{1}{p} = +\infty .$$

Cette conjecture peut être rapprochée de [15], où il est démontré qu'une suite $a_1 < a_2 \dots$, telle que $a_n \neq a_{n_1} + a_{n_2} + \dots + a_{n_i}$, vérifie $\sum_i \frac{1}{a_i} < +\infty$.

Conjecture 3. - Soit $f(n)$ une fonction quelconque de $\underset{\sim}{N}$ dans $\{+1 , -1\}$. Montrer que, pour tout C , il existe d et m tels que :

$$|\sum_{k=1}^{m} f(kd)| > C$$

ou mieux, montrer qu'il existe une constante c_1 telle que

$$\max_{md \leqslant n} |\sum_{k=1}^{m} f(kd)| > c_1 \log n$$

(La fonction f partage les entiers en deux classes, et dire que $|\sum_{k=1}^{m} f(kd)|$ est grand signifie que la progression arithmétique $(kd)_{1 \leqslant k \leqslant m}$ est située en grande partie dans l'une des classes).

Signalons enfin que, dans des travaux non publiés, DAVIES [Université de Leicester (Grande-Bretagne] avec l'hypothèse du continu, et BAUMGARTNER [Université de Hanover, N. H. (Etats-Unis)] sans hypothèse, ont partagé les réels en deux parties, dont l'une ne contient pas une progression arithmétique de 3 termes et l'autre ne contient pas une progression arithmétique infinie.

2. Différence entre deux nombres premiers consécutifs.

Soit p_n le n-ième nombre premier. On pose $d_n = p_{n+1} - p_n$. Pour une étude plus détaillée de cette question, on pourra se reporter à [10] (p. 200 et suivantes), [11] (p. 222 et suivantes) et à [21] ou [22] (chapitre V, § 5).

De l'égalité $\sum_{k=1}^{n} d_k = p_n - p_1 \sim n \log n$, on déduit que

$$\overline{\lim} \frac{d_n}{\log n} \geqslant 1 \quad \text{et} \quad \underline{\lim} \frac{d_n}{\log n} \leqslant 1 .$$

Le meilleur résultat connu sur les grandes valeurs de d_n est : Pour une infinité de valeurs de n , on a, en posant $\log_2(n) = \log \log n$, etc.,

$$d_n > C \frac{\log n \log_2 n \log_4 n}{(\log_3 n)^2} ,$$

RANKIN [24] l'a montré avec $C = \frac{1}{3} - \varepsilon$; SCHÖNHAGE [30] et RANKIN [25] l'ont amélioré avec $C = e^{\gamma} - \varepsilon$, où γ est la constante d'Euler.

D'autre part, on sait que, pour n assez grand, on a :

$$d_n < n^{\tau} ,$$

MONTGOMERY [20] (p. 131) donne pour τ la valeur $\frac{3}{5} + \varepsilon$. Huxley aurait très récemment montré que l'on peut prendre $\tau = \frac{7}{12} + \varepsilon$. Rappelons que l'hypothèse de Riemann donne, pour τ , la valeur $\frac{1}{2} + \varepsilon$ (cf. PRACHAR [22], p. 320-324) et que CRAMER a conjecturé

$$\overline{\lim} \frac{d_n}{(\log n)^2} = 1 .$$

Pour les petites valeurs de d_n , la conjecture la plus probable est l'existence d'une infinité de nombres premiers jumeaux, i. e. $\underline{\lim}\, d_n = 2$. Le meilleur résul-

tat est dû à BOMBIERI et DAVENPORT ([5] voir aussi [9]) qui démontrent

$$\underline{\lim}\ \frac{d_n}{\log n} < 0{,}455\ .$$

P. ERDÖS [16] a démontré que

$$\overline{\lim}\ \min(d_n\ ,\ d_{n+1})/\log n = +\infty\ .$$

Conjecture 1. - $\underline{\lim}\ \max(d_n\ ,\ d_{n+1})/\log n < 1$.

Conjecture 2. - $\overline{\lim}\ \min(d_n\ ,\ d_{n+1}\ ,\ d_{n+2})/\log n = +\infty$.

Comme $\overline{\lim}\ d_n = +\infty$, il existe une infinité de n tels que $d_{n+1} > d_n$. ERDÖS et TURAN [17] ont montré qu'il existe une infinité de n tels que $d_n > d_{n+1}$.

Conjecture 3. - Existe-t-il une infinité de n tels que

$$d_{n+2} > d_{n+1} > d_n\ ?$$

Conjecture 4. - Y a-t-il une infinité de n tels que

$$d_{n+1} = d_n\ ?$$

Conjecture 5.(primée 500 francs, et entrainée par la conjecture 3 ou la conjec-4). - Montrer qu'il n'existe pas d'entier N tel que, pour $n \geqslant N$, le graphe de d_n soit en dents de scie, i. e. :

$$d_N < d_{N+1}$$
$$d_{N+1} > d_{N+2}$$
$$d_{N+2} < d_{N+3}$$
$$\ldots$$

3. Le problème de Romanoff (cf. [11], p. 230).

ROMANOFF a démontré (cf. [27] et [23], p. 168-173) que les nombres de la forme $2^k + p$, k entier, p premier et plus petits que x , sont en quantité supérieure à cx . P. ERDÖS a montré [18] que le nombre de solutions de l'équation $2^k+p=n$ est supérieur à $c \log\log n$ pour une suite infinie d'entiers n . Dans le même article, il démontre l'existence d'une progression arithmétique infinie de nombres impairs qui ne s'écrivent pas $2^k + p$. C'est cette question qui a amené P. ERDÖS à s'intéresser aux systèmes de congruences recouvrants.

Conjecture 1. - 105 est tel que $105 - 2^k$ est premier pour tout k . Montrer que 105 est le plus grand nombre ayant cette propriété.

Conjecture 2. - Existe-t-il un entier k tel que tout nombre s'écrive

$$p + 2^{n_1} + \ldots + 2^{n_i} \quad \text{avec} \quad i \leqslant k\ ?$$

LINNIK a démontré qu'il existe un entier k' tel que tout entier s'écrive $p + q + 2^{n_1} + \ldots + 2^{n_i}$ avec $i \leqslant k'$, p et q premiers. SCHINZEL a trouvé une infinité de nombres impairs qui ne s'écrivent pas sous la forme $p + 2^{n_1} + 2^{n_2}$, et GALLAGHER a montré très récemment que, pour tout $\varepsilon > 0$, il existe k tel que la

densité inférieure des nombres $p + 2^{n_1} + \ldots + 2^{n_k}$ soit supérieure à $1 - \varepsilon$. Signalons enfin que la conjecture 1 du paragraphe 4 sur les systèmes de congruences recouvrant avec des modules $\geq c$ entraîne l'existence d'une infinité de nombres qui ne s'écrivent pas sous la forme $q_c + 2^n$, où q_c est un nombre ayant au plus c facteurs premiers.

4. Système de congruences recouvrant.

Pour une étude plus complète de la question, et d'autres références, cf. [1] (p. 408-409), [10] (p. 235), et aussi A. SCHINZEL [29] qui met en rapport cette question avec la réductibilité de certains polynômes.

Définition. - On dit qu'un système de congruences $a_i \pmod{m_i}$, avec $m_1 < m_2 < \ldots < m_k$, est recouvrant si, pour tout entier n, il existe au moins un indice i tel que

$$n \equiv a_i \mod m_i .$$

Exemple 1. - $0 \pmod 2$, $0 \pmod 3$, $1 \pmod 4$, $1 \pmod 6$, $11 \pmod{12}$.

Exemple 2. - $0 \pmod 2$, $0 \pmod 3$, $1 \pmod 4$, $7 \pmod 8$, $11 \pmod{12}$, et $19 \pmod{24}$. Pour d'autres exemples, cf. [8].

Conjecture 1. - Pour tout c donné, existe-t-il un système de congruences recouvrant vérifiant $c \leqslant m_1 < m_2 < \ldots < m_k$? CHOI [6] a trouvé un système de congruences recouvrant dont les modules sont tous $\geqslant 20$.

Conjecture 2. - Existe-t-il un système recouvrant dont tous les modules soient impairs ?

Conjecture 3. - On dit qu'un entier m est recouvrant s'il existe un système de congruences recouvrant dont tous les modules sont des diviseurs de m (Ainsi 12 est recouvrant d'après l'exemple 1). Montrer que, pour tout $c > 0$, il existe un entier m qui ne soit pas recouvrant et qui vérifie $(\sigma(m))/m > c$ avec

$$\sigma(m) = \sum_{d|m} d .$$

Lorsque $c = 2$, on peut voir que $m = 70$ n'est pas recouvrant.

BIBLIOGRAPHIE

[1] ATKIN (A. O. L.) and BIRCH (B. J.) [Editors]. - Computers in number theory. Proceedings of the Science research council Atlas symposium [2. 1969. Oxford]. - London, New York, Academic Press, 1971.

[2] BEHREND (F.). - On sequences of integers containing no arithmetic progression, Cas. Mat. Fys., t. 67, 1938, p. 235-238.

[3] BEHREND (F.). - On sets of integers which contain no three terms in arithmetic progression, Proc. Nat. Acad. Sc. U. S. A., t. 32, 1946, p. 331-332.

[4] BERLEKAMP (E. R.). - A construction for partitions which avoid long arithmetic progression, Can. Math. Bull., t. 11, 1968, p. 409-414.

[5] BOMBIERI (E.) and DAVENPORT (H.). - Small differences between prime numbers, Proc. Roy. Soc., London, Series A, t. 293, 1966, p. 1-18.

[6] CHOI (S. L. G.). - Covering the set of integers by congruence classes of distinct moduli, Math. of Comp., Washington, t. 25, 1971, p. 885-895.

[7] CHOWLA (S. D.). - There exists an infinity of 3-combinations of primes in A. P., Proc. Lahore philos. Soc., t. 6, 1944, p. 15-16.

[8] CHURCHHOUSE (R. F.). - Covering sets and systems of congruences, "Computers in mathematical research", p. 20-36. - Amsterdam, North-Holland publishing Company, 1968.

[9] DAVENPORT (H.). - Multiplicative number theory. - Chicago, Markham publishing Company, 1967 (Lectures in advanced Mathematics, 1).

[10] ERDÖS (P.). - Some recent advances and current problems in number theory, "Lectures on modern mathematics". Edited by T. L. Saaty, Vol. 3, p. 196-244. - New York, J. Wiley and Sons, 1965.

[11] ERDÖS (P.). - Some unsolved problems, Publ. Math. Inst. Hung. Acad. Sc., t. 6, 1961, p. 221-254.

[12] ERDÖS (P.). - Quelques problèmes de la théorie des nombres. - Genève, L'Enseignement mathématique (Monographies de l'enseignement mathématique, 6, p. 81-135).

[13] 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).

[14] ERDÖS (P.) and TURAN (P.). - On some sequences of integers, J. London. math. Soc., t. 11, 1936, p. 261-264.

[15] ERDÖS (P.). - Some remarks on number theory, III [en hongrois, avec un résumé en anglais], Mat. Lapok, t. 13, 1962, p. 28-38. [Pour une traduction, cf. BENKOVSKI and ERDÖS, Math. of Comp. (à paraître).]

[16] ERDÖS (P.). - Problems and results on the differences of consecutive primes, Publ. Math., Debrecen, t. 1, 1949, p. 33-37.

[17] ERDÖS (P.) and TURAN (P.). - On some sequences of integers, Bull. Amer. math. Soc., t. 54, 1948, p. 371-378.

[18] ERDÖS (P.). - On integers of the form $2^k + p$, Summa Brasil. Math., t. 2, 1950, p. 113-123.

[19] KHINČIN (A. Ja.). - Three pearls of number theory. Translated from the 2nd (1948) russian edition. - Rochester, Graylock Press, 1952.

[20] MONTGOMERY (H. L.). - Topics in multiplicative number theory. - Berlin, Springer-Verlag, 1971 (Lecture Notes in Mathematics, 227).

[21] NICOLAS (J.-L.). - Répartition des nombres premiers, Séminaire Delange-Pisot-Poitou : Théorie des nombres, 9e année, 1967/68, groupe d'étude n° G6, 4 p.

[22] PRACHAR (K.). - Primzahlverteilung. - Berlin, Springer-Verlag, 1957 (Grundlehren der mathematischen Wissenschaften, 91).

[23] RADO (R.). - Studien zur Combinatorik, Math. Z., t. 36, 1933, p. 424-480.

[24] RANKIN (R. A.). - The difference between consecutive prime numbers, J. London math. Soc., t. 13, 1938, p. 242-247.

[25] RANKIN (R. A.). - The difference between consecutive prime numbers, V, Proc. Edimburgh math. Soc., t. 13, 1963, p. 29-30.

[26] ROMANOFF (N. P.). - Über einige Satze der additiven Zahlentheorie, Math. Annalen, t. 109, 1934, p. 668-678.

[27] ROTH (K. F.). - On certain sets of integers, J. London math. Soc., t. 28, 1953, p. 104-109.

[28] SALEM (R.) and SPENCER (D. C.). - On sets of integers which contain no three terms in an arithmetical progression, Proc. Nat. Acad. Sc. U. S. A., t. 28, 1942, p. 561-563 ; et "Oeuvres mathématiques" de R. SALEM, p. 252-254. - Paris, Hermann, 1967.

[29] SCHINZEL (A.). - Reducibility and irreducibility of polynomial and covering systems of congruences, Acta Arithm., Warszawa, t. 13, 1967, p. 91-101.

[30] SCHÖNHAGE (A.). - Eine Bemerkung zur Konstruktion grosser Primzahllucken, Arch. der Math., Basel, t. 14, 1963, p. 29-30.

[31] SZEMEREDI (E.). - On sets of integers containing no four elements in arithmetic progression, Acta Math. Acad. Sc. Hung., t. 20, 1969, p. 89-104.

[32] VAN DER WAERDEN (B. L.). - Beweis einer Baudet'schen Vermutung, Neiuw Archief voor Wiskunde, t. 15, 1928, p. 212-216.

[33] VAN DER WAERDEN (B. L.). - How the proof of Baudet's conjecture was found, "Studies in pure mathematics". Papers in combinatorial theory, analysis, ... presented to Richard Rado, p. 251-260. - London and New York, Academic Press, 1971.

(Texte reçu le 15 octobre 1973)

Paul ERDÖS
Magyar Tudomanyos Akademia
Matematikai Kutato Intezete
Réaltanoda u 13-15
BUDAPEST V (Hongrie)