REMARQUES SUR LES PROGRESSIONS ARITHMÉTIQUES

PAR

W. SIERPIŃSKI (WARSZAWA)

C. Zarankiewicz m'a posé récemment plusieurs problèmes concernant les progressions arithmétiques. Certains d'entre eux sont faciles à résoudre, néanmoins d'autres me semblent présenter des difficultés.

1. $q, q^2, q^3, \ldots$ étant une progression géométrique infinie de nombres distincts, peut-on toujours en extraire trois termes formant une progression arithmétique?

On démontre sans peine que c'est impossible si q est un nombre rationnel.

En effet, s'il était $q^n - q^m = q^p - q^n$, pour $m<n<p$, on aurait ou bien $q=0$, ce qui est impossible, les termes de la progression $q, q^2, \ldots$ étant distincts, ou bien $q^{p-m} - 2q^{n-m} + 1 = 0$. Or, cette équation a deux racines rationnelles au plus: 1 et -1, qui ne donnent pas de progression $q, q^2, \ldots$ aux termes distincts.

Cependant il existe des nombres irrationnels q tels que de la suite $q, q^2, \ldots$ on puisse extraire trois termes formant une progression arithmétique. Tel est, par exemple, le nombre $q = (\sqrt{5}-1)/2$, où les termes q^n, q^{n+1} et q^{n+3} forment une progression arithmétique (quel que soit le nombre naturel n).

P115. Existe-il un nombre irrationnel q tel qu'on puisse extraire de la suite $q, q^2, \ldots$ quatre termes formant une progression arithmétique?

2. On démontre sans peine qu'il n'existe aucune progression arithmétique infinie formée de carrés (de nombres naturels) distincts. Néanmoins, il existe trois carrés distincts formant une progression arithmétique, par exemple, les nombres $1^2, 5^2, 7^2$. Il est même facile de prouver qu'il y a une infinité de tels triples et de trouver tous les systèmes de trois nombres naturels x, z, y, où $x<z<y$, tels que $z^2 - x^2 = y^2 - z^2$, c'est-à-dire $x^2 + y^2 = 2z^2$.

En effet, si x, z, y sont de tels nombres, x et y sont soit tous les deux pairs, soit tous les deux impairs; on a donc $x+y=2u, x-y=2v$, où u et $v<u$ sont des nombres naturels, et on aboutit à l'équation de Pythagore $u^2+v^2=z^2$ qu'on sait résoudre en nombres naturels. u et v trouvés, il reste à poser $x=u+v$, $y=u-v$ pour avoir la solution de l'équation $x^2+y^2=z^2$. On calcule ainsi, par exemple, les triples $7^2, 13^2, 17^2$; $7^2, 17^2, 23^2$; $17^2, 25^2, 31^2$; $1^2, 29^2, 41^2$.

D'après Fermat il n'existe pas quatre (ou plus) carrés qui forment une progression arithmétique croissante[1]). Il n'existe pas trois carrés en progression arithmétique dont la différence serait un carré. En effet, si $y^2 - x^2 = u^2$ et $z^2 - y^2 = u^2$, on a $y^2 - u^2 = x^2, y^2 + u^2 = z^2$, d'où $y^4 - u^4 = (xz)^2$, et, comme Fermat l'a démontré par la méthode de la descente infinie, cette égalité est impossible pour x, y, z, u naturels; pour $x=0$ on obtient $y^2 = u^2$ et $z^2 = y^2 + u^2 = 2u^2$, ce qui est impossible pour z entier et u naturel[2]).

Il existe cependant des progressions arithmétiques infinies formées de carrés de nombres ordinaux transfinis croissants, par exemple,

$$\omega^2, (\omega\cdot 2)^2, (\omega\cdot 3)^2, \ldots,$$

car on a $[\omega(n+1)]^2 = (\omega n)^2 + \omega^2$ pour $n=1,2,\ldots$ Pareillement, pour $p=1,2,3,\ldots$, les nombres

$$\omega, (\omega\cdot 2)^p, (\omega\cdot 3)^p, \ldots$$

font une progression arithmétique infinie puisque

$$[\omega(n+1)]^p = (\omega\cdot n)^p + \omega^p \quad \text{pour} \quad n=1,2,\ldots$$

P116. Peut-on extraire de la suite infinie $1^3, 2^3, 3^3, \ldots$ une progression arithmétique formée de trois (ou plus) termes? Autrement dit, existe-il des solutions de l'équation $x^3+y^3=2z^3$ en nombres naturels distincts?

3. On démontre sans peine qu'il n'existe aucun système de trois nombres naturels croissants m, n, p tels que les nombres $m!, n!, p!$ forment une progression arithmétique.

En effet, soient m, n, p des nombres naturels et $m<n<p$: on a $p>2$. S'il était $n! - m! = p! - n!$, on aurait

$$\frac{n!}{m!} - 1 = \frac{n!}{m!}\left(\frac{p!}{n!} - 1\right). \tag{1}$$

Or, comme $n<p$, on a $p!/n! \geqslant p > 2$, d'où $p!/n! - 1 > 1$, et la formule (1) donne $(n!/m!) - 1 > n!/m!$, ce qui est impossible.

K. Roth a démontré récemment[3]) un théorème duquel il résulte facilement que si $u_1, u_2, \ldots$ est une suite infinie croissante de nombres naturels, dont on ne peut extraire aucune progression arithmétique de trois

---

[1]) Cf. L. E. Dickson, *History of the theory of numbers*, vol. II, New York 1934, p. 440 et 635.

[2]) Cf. A. Errera, *A propos d'un système diophantien et de la méthode de Fermat*, Comptes Rendus du Congrès de l'Association Française pour l'Avancement des Sciences, Tunis, Mai 1951.

[3]) K. Roth, *Sur quelques ensembles d'entiers*, Comptes Rendus de l'Académie des Sciences de Paris 234 (1952), p. 388.

termes, on a

$$\lim_{n\to\infty}\frac{f(n)}{n}=0,$$

où $f(n)$ désigne le nombre des indices k tels que $u_k\leqslant n$.

4. Parmi les nombres irrationnels de la suite infinie $\sqrt{1},\sqrt{2},\sqrt{3},\ldots$ on peut en choisir une infinité qui forment une progression arithmétique. Tels sont par exemple les nombres $\sqrt{2(2k-1)^2}=\sqrt{2}(2k-1)$, où $k=1,2,\ldots$

5. On démontre sans peine qu'il n'existe aucune progression arithmétique infinie dont les termes soient des nombres premiers distincts. En effet, dans la progression arithmétique $ak+b$ $(k=0,1,2,\ldots)$, où a est un nombre naturel >1 et b un entier $\geqslant 0$, le terme $a(a+b+1)+b=(a+1)(a+b)$ est un nombre composé.

P117. Existe-t-il pour chaque n naturel une progression arithmétique formée de n nombres premiers distincts?

Pour $n=3$ telle est la suite $3,5,7$; pour $n=5$ la suite $5,11,17,23,29$; pour $n=6$ la suite $7,37,67,97,127,157$; pour $n=10$ la suite $199,409,619,829,1039,1249,1459,1669,1879,2089$ [4]).

On pourrait étudier la fonction $g(x)$, où, pour x réel, $g(x)$ désigne le nombre maximal de termes d'une progression arithmétique formée de nombres premiers distincts $\leqslant x$. On a $g(1)=0$, $g(2)=1$ et on trouve

$$g(x)=\begin{cases}2 & \text{pour} \quad 3\leqslant x<7,\\ 3 & \text{pour} \quad 7\leqslant x<23,\\ 4 & \text{pour} \quad 23\leqslant x<29,\\ 5 & \text{pour} \quad 29\leqslant x<157,\\ 6 & \text{pour} \quad 157\leqslant x<1307,\\ 7 & \text{pour} \quad 1307\leqslant x<1669,\\ 8 & \text{pour} \quad 1669\leqslant x<1879,\\ 9 & \text{pour} \quad 1879\leqslant x<2089,\end{cases}$$

et $g(2089)=10$.

On peut démontrer [5]) que, p étant un nombre premier, si p nombres premiers $\neq p$ forment une progression arithmétique croissante, la différence de cette progression est divisible par tout nombre premier $\leqslant p$.

[4]) Cf. V. Thébault, *Sur les nombres premiers impairs*, Comptes Rendus de l'Académie des Sciences de Paris 218 (1944), p. 223. Voir aussi Scripta Mathematica 13 (1947), p. 162.

[5]) Voir, par exemple, mon livre *Teoria liczb*, Monografie Matematyczne 19, Warszawa-Wrocław 1950, p. 490, Exercise 9.

Il en résulte, par exemple, que si 11 nombres premiers >11 forment une progression arithmétique croissante, sa différence est divisible par 2310.

Si $p_{25}=97$ nombres premiers >97 font une progression arithmétique croissante, sa différence est divisible par

$$p_1p_2\ldots p_{25}=210\,p_5p_6\ldots p_{25}>210\cdot 10^{21}>10^{23}.$$

Il est donc pratiquement impossible, à l'état actuel de la science, de trouver 100 nombres premiers distincts qui forment une progression arithmétique. On ne sait même pas si une telle progression existe.

6. Je vais démontrer les deux théorèmes suivants:

THÉORÈME 1. *On peut supprimer dans la suites de tous les nombres naturels une suite infinie croissante plus vite qu'une suite infinie croissante arbitraire donnée d'avance, de sorte que l'ensemble des nombres naturels qui restera ne contienne aucune progression arithmétique infinie.*

Démonstration. Soit $u_1,u_2,\ldots$ une suite infinie croissante arbitraire de nombres naturels.

Il existe, comme on le sait, pour tout n naturel, des nombres naturels p_n et q_n bien déterminés par n, tels que

$$n=2^{p_n-1}(2q_n-1).$$

Posons, pour $n=1,2,\ldots$,

$$v_n=p_nu_n^2+q_n.$$

La suite infinie v_n $(n=1,2,\ldots)$ de nombres naturels croît plus rapidement que la suite u_n $(n=1,2,\ldots)$ puisqu'on a $v_n>u_n^2$ pour $n=1,2,\ldots$

Soit maintenant $ak+b$ $(k=1,2,\ldots)$ une progression arithmétique donnée, où a et b sont des nombres naturels. Posons $n=2^{a-1}(2b-1)$; on aura $p_n=a,q_n=b$, donc $v_n=p_nu_n^2+q_n=au_n^2+b$ est un terme de la suite $ak+b$ $(k=1,2,\ldots)$. La suite $v_1,v_2,\ldots$ a donc des termes communs avec toute progression arithmétique infinie. Si l'on supprime les nombres $v_1,v_2,\ldots$ de la suite $1,2,3,\ldots$ la suite de nombres naturels qui restera ne contiendra aucune progression arithmétique infinie. Le théorème 1 est ainsi démontré.

Remarque. Evidemment, si une suite $\{v_n\}$ de nombres naturels contient un terme commun avec toute progression arthmétique infinie croissante de nombres naturels, elle en contient une infinité. Cette remarque étant valable aussi par rapport aux progressions $ak+b$ $(k=0,1,2,\ldots)$, où $(a,b)=1$, le théorème bien connu de Lejeune-Dirichlet sur la progression arithmétique équivaut à la proposition suivante (qu'on pourrait regarder comme plus faible que ce dernier):

Toute progression arithmétique $ak+b$ $(k=0,1,2,\ldots)$, où a et b sont des nombres naturels premiers entre eux, contient au moins un nombre premier [6]).

THÉORÈME 2. *u_n $(n=1,2,\ldots)$ étant une suite infinie croissante de nombres naturels, il existe toujours une suite infinie de nombres naturels v_n $(n=1,2,\ldots)$, croissant plus rapidement que la suite u_n $(n=1,2,\ldots)$, de laquelle on peut extraire des progressions arithmétiques finies aussi longues que l'on veut.*

Démonstration. Soit u_n $(n=1,2,\ldots)$ une suite infinie croissante de nombres naturels. Posons $v_1=u_1$. Soit k un nombre naturel et supposons avoir déjà défini tous les nombres v_n pour $n\leqslant k^2$. Posons

$$v_{k^2+i}=i\cdot(2k)!\,u_{(k+1)^2} \quad \text{pour} \quad i=1,2,3,\ldots,2k+1. \tag{2}$$

Les nombres v_n se trouvent ainsi définis pour $k^2<n\leqslant(k+1)^2$. Ils sont donc définis par induction pour tout n naturel, et on voit que la suite infinie v_n $(n=1,2,\ldots)$ est croissante.

Il résulte de (2) que les termes v_{k^2+i} $(i=1,2,\ldots,2k+1)$ forment une progression arithmétique. On peut donc extraire de la suite infinie v_n $(n=1,2,\ldots)$ une progression arithmétique de $2k+1$ termes, donc aussi longue que l'on veut.

Il est facile à prouver que

$$\lim_{n\to\infty}\frac{v_n}{u_n}=+\infty.$$

Le théorème 2 se trouve ainsi démontré.

Il est enfin à remarquer que Van der Waerden a démontré la proposition suivante:

k et l étant des nombres naturels donnés, il existe toujours un nombre naturel $n=n(k,l)$ tel que si l'on décompose l'ensemble $\{1,2,3,\ldots,n\}$ en k ensembles disjoints quelconques (parmi lesquels peuvent se trouver aussi des ensembles vides), au moins un de ces ensembles contient une progression arithmétique de l nombres distincts.

Une démonstration élémentaire de cette proposition a été trouvée par M. A. Loukomskaja [7]).

Or, si l'on décompose l'ensemble N de tous les nombres naturels en deux ensembles disjoints, A et B, il peut arriver qu'aucun de ces ensembles ne contienne de progression arithmétique infinie. Zarankiewicz a trouvé une telle décomposition $N=A+B$, où, de tous trois nombres naturels consécutifs, un au moins appartient à l'ensemble A, un au moins à l'ensemble B, et où ni A ni B ne contient de progression arithmétique infinie. De tels ensembles A et B peuvent être définis comme il suit

Soit A (respectivement B) l'ensemble de tous les nombres naturels n pour lesquels le nombre $n+E\sqrt{n}$ est impair (respectivement pair).

Soit n un nombre naturel. On a

$$\sqrt{n+2}-\sqrt{n}=\frac{2}{\sqrt{n+2}+\sqrt{n}}<1,$$

d'où il résulte que de trois nombres $E\sqrt{n}$, $E\sqrt{n+1}$ et $E\sqrt{n+2}$, au moins deux sont égaux. Si $E\sqrt{n}=E\sqrt{n+1}$, on a

$$n+1+E\sqrt{n+1}-(n+E\sqrt{n})=1,$$

d'où il résulte que l'un des nombres $n+E\sqrt{n}$ et $n+1+E\sqrt{n+1}$ est impair, l'autre pair, donc qu'un des nombres n et $n+1$ appartient à A, l'autre à B. Si $E\sqrt{n+1}=E\sqrt{n+2}$, on conclut pareillement que l'un des nombres $n+1$ et $n+2$ appartient à A et l'autre à B.

Soit maintenant $ak+b$ $(k=0,1,2,\ldots)$ une progression arithmétique, où a et b sont des nombres naturels. Posons

$$m=a\cdot 4ab^2+b, \qquad n=a(4ab^2-2b)+b;$$

les nombres n et m sont évidemment des termes de la progression $ak+b$ $(k=0,1,2,\ldots)$. On a

$$(2ab)^2<m=(2ab)^2+b<(2ab)^2+4ab+1=(2ab+1)^2,$$

d'où $2ab<\sqrt{m}<2ab+1$, ce qui prouve que

$$E\sqrt{m}=2ab \quad \text{et} \quad m+E\sqrt{m}=(2ab)^2+2ab+b. \tag{3}$$

D'autre part, on a

$$(2ab-1)^2=(2ab)^2-4ab+1<(2ab)^2-2ab+b=n<(2ab)^2,$$

d'où $2ab-1<\sqrt{n}<2ab$, ce qui prouve que

$$E\sqrt{n}=2ab-1 \quad \text{et} \quad n+E\sqrt{n}=(2ab)^2+b-1. \tag{4}$$

On a ainsi, d'après (3) et (4), $m+E\sqrt{m}-(n+E\sqrt{n})=2ab+1$, d'où il résulte que l'un des nombres $m+E\sqrt{m}, n+E\sqrt{n}$ est impair, l'autre pair, donc que l'un des nombres m,n appartient à A tandis que l'autre à B.

La progression $ak+b$ $(k=0,1,2,\ldots)$ a donc des termes dans A et des termes dans B; elle ne peut donc être contenue ni dans A ni dans B. Les ensembles A et B ont donc les propriétés désirées.

[6]) Cf. mon livre cité *Teoria liczb*, p. 526.

[7]) Cf. А. Я. Хинчин, *Три жемчужины теории чисел*, Москва-Ленинград 1948, p. 8-13.