NOUVELLES ANNALES DE MATHÉMATIQUES

CHANSON

Solution de la question 316

Nouvelles annales de mathématiques 1re série, tome 17 (1858), p. 396-399

<http://www.numdam.org/item?id=NAM_1858_1_17__396_1>

SOLUTION DE LA QUESTION 316

(voir t. XV, p. 52)

PAR M. CHANSON,
Élève du lycée de Versailles (classe de M. Vannson).

Etant donnée la progression arithmétique

$$a, \quad a+r, \quad a+2r, \ldots, \quad a+nr$$

dans laquelle a et r sont premiers entre eux, faire voir qu'on peut y trouver un nombre illimité de termes premiers avec un nombre donné quelconque A.

Cela revient à dire qu'on peut choisir n d'une infinité de manières de sorte que $a+nr$ soit premier avec A.

Pour cela, je distingue trois cas :

1°. Celui où A est premier à la fois avec a et r.

Soit

$$A = b^{b'} c^{c'} d^{d'};$$

je n'ai qu'à poser

$$n = b^{\gamma} c^{z} d^{u},$$

γ, z, u pouvant d'ailleurs varier d'une infinité de manières. Je dis que A sera premier avec $a + nr$; car si un facteur premier de A divisait la somme $a + nr$ comme il divise une de ses parties nr (car n renferme par hypothèse tous les facteurs premiers de A), il diviserait l'autre partie a, ce qui est contre l'hypothèse, n étant premier avec a.

2°. A est premier avec un des nombres a et r seulement, avec a par exemple.

Soient

$$r = \alpha^{\alpha'} \beta^{\beta'}, \ldots, \quad A = \alpha^{\alpha''} \beta^{\beta''} \ldots b^{b'} c^{c'} d^{d'}, \ldots;$$

je n'ai qu'à prendre

$$n = b^{\gamma} c^{z} d^{u},$$

c'est-à-dire égal au produit de tous les facteurs premiers de A qui n'entrent pas dans r avec des exposants quelconques. Il est clair alors que A sera premier avec $a + nr$; car si α ou un facteur analogue (c'est-à-dire un des facteurs qui entrent dans r) divisait $a + nr$ divisant nr, il devrait diviser a, ce qui est contre l'hypothèse, parce que a est supposé premier avec r. Si c'était un des facteurs b, c qui n'entrent pas dans r qui divisât $a + nr$, on arriverait à la même absurdité.

Si A était premier avec r seulement, on raisonnerait de la même façon.

Passant donc au troisième cas, c'est-à-dire à celui où A n'est premier ni avec a ni avec r, alors si

$$r = \alpha^{\alpha'} \beta^{\beta'}, \ldots, \quad a = \gamma^{\gamma'} \delta^{\delta'}, \ldots, \text{ et } A = \alpha^{p} \ldots \gamma^{q} \ldots b^{b'} c^{c'} \ldots,$$

je choisis

$$n = b^{\gamma} c^{z} \ldots,$$

γ, z pouvant être quelconques. Je démontrerai comme

précédemment qu'aucun facteur de A ne peut diviser $a + nr$; car n ayant été choisi de la manière indiquée, ce facteur diviserait une des parties de la somme, et, par suite, diviserait l'autre, ce qui conduirait à une absurdité.

Note du Rédacteur. Dans les cas deuxième et troisième, quand A n'aura pas d'autres facteurs premiers que ceux qui entrent dans a et r, on aura $n = 1$, mais quand $a + \alpha r$ est premier à A, $a + (\alpha + k\mathrm{A})\, r$ l'est également; il y a donc encore dans $a + nr$ une *infinité* de nombres premiers à A.

L'avantage de la démonstration précédente est de ne pas supposer la résolution de l'équation indéterminée du premier degré à deux inconnues. Jacobi, dans l'introduction de son *Canon arithmeticus*, indique une démonstration qui suppose cette résolution, et qui peut donner l'expression générale des valeurs de n qui rendent $a + nr$ premier au nombre A.

On y lit :

« *Observo si* A *et* B *inter se primi sint, semper effici posse addendo ipsi* A *multiplum ipsius* B *ut prodeat numerus ad alium quemlibet* C *primus.* Sit enim B′ factor maximus ipsius C ad B primus sive $\frac{\mathrm{C}}{\mathrm{B}'}$ factor maximus communis ipsorum B et C ideoque primus ad numeros A, $\mathrm{A} + \alpha\mathrm{B}$; erit $\mathrm{A} + \alpha\mathrm{B}$ ad C primus, si ad B′ primus est; sub forma autem $\mathrm{A} + \alpha\mathrm{B}$ pro diversis ipsius α valoribus continentur numeri, qui respectu moduli B′ ad B primi residua quæcunque placet relinquunt; inde etiam forma $\mathrm{A} + \alpha\mathrm{B}$ continet numeros ad B′ primos, q. d. e.

Il y a ici omission ou erreur de copie.

Soient

$$\mathrm{B} = a^{\alpha} b^{\beta} c^{\gamma} \ldots \times p^{\lambda} q^{\mu} \ldots ,$$

$$\mathrm{C} = a^{\alpha'} b^{\beta'} c^{\gamma'} \ldots \times r^{\rho} s^{\sigma} \ldots ,$$

$a, b, c, \ldots; p, q, \ldots, r, s$ étant premiers, on aura

$$B' = r^{\rho} s^{\sigma} \ldots, \quad \frac{C}{B'} = a^{\alpha'} b^{\beta'} c^{\vartheta'} \ldots,$$

qui n'est pas le plus grand commun diviseur de C et B, mais bien un multiple de ce plus grand commun diviseur.