NOUVELLES ANNALES DE MATHÉMATIQUES

B. FINCK

Observations sur le théorème de M. Lamé, relativement au plus grand commun diviseur, et nouvelle démonstration de ce théorème

Nouvelles annales de mathématiques 1re série, tome 4 (1845), p. 71-74

<http://www.numdam.org/item?id=NAM_1845_1_4__71_0>

OBSERVATIONS

sur le théorème de M. Lamé, relativement au plus grand commun diviseur, et nouvelle démonstration de ce théorème.

PAR B. FINCK,
Docteur ès sciences, professeur de mathématiques à Strasbourg.

—

J'ai donné dans les *Nouvelles Annales*, un théorème pour déterminer une limite du nombre des opérations de la recherche du plus grand commun diviseur de deux nombres. Ce théorème a trouvé place dans la seconde partie de mon arithmétique, pages 57 et 58. J'en rappellerai l'énoncé : *si* B *est le plus petit des deux nombres, et qu'on cherche le plus petit nombre entier* n, *qui rend* $2^n > \frac{B+1}{2}$, 2n *sera une limite du nombre des opérations*. On peut conclure de là, qu'il suffit que $n+1$ soit $> \frac{\log(B+1)}{\log 2}$, et, si c est le nombre des chiffres de B, il suffit que $n+1 > \frac{c}{0,3}$, car $\log 2 > 0,3$. De là pour $2n$, la limite $\frac{2c}{0,3} - 2$ ou $\frac{20}{3}c - 2$.

M. Lamé donne la limite plus simple $5c$, et il se sert à cet effet de la série 1, 2, 3, 5, 8..., dont les premiers termes sont 1, 2, chacun des autres étant la somme des deux précédents. J'ai considéré dans mon arithmétique, page 128, la même série dans un but analogue. Ici je la remplacerai par une autre; mais il faut reprendre les choses de plus haut, et d'abord, je dis que si B est égal au $n^{ième}$ terme de la série

1, 2, 3, 5, 8, etc. (1)

il n'y aura jamais plus de n opérations, et si B est $<$ que ce $n^{ième}$ terme, il y aura moins de n opérations.

En effet, soient R_1, R_2... les restes ; φ_1, φ_2... les quotients. Il vient :

$$\left.\begin{aligned} A &= B\varphi_1 + R_1 \\ B &= R_1\varphi_1 + R_2, \text{ etc.} \end{aligned}\right\} (2).$$

Remarquons que si on prend dans (1) deux termes consécutifs, pour en chercher le plus grand commun diviseur, les restes seront précisément les termes précédents de (1), et le nombre des opérations sera le rang du plus petit des deux termes, dont on chercherait le plus grand commun diviseur. D'ailleurs, les quotients et le dernier diviseur auraient leurs valeurs minima, savoir : 2 pour le dernier quotient, et 1 pour tous les autres et le dernier diviseur. Par conséquent, si A et B donnent lieu à n opérations, il s'ensuit que B $\begin{matrix}=\\>\end{matrix}$, au $n^{ième}$ terme de (1). En effet, si les quotients et le dernier diviseur ont leurs valeurs minima, les nombres R_{n-1}, R_{n-2},... R_1, B seront les n premiers termes de (1), et auront aussi chacun sa plus petite valeur. Donc, dans tout autre cas, B sera $>$ le terme de rang n.

Donc si B $=$ le terme de rang n, il n'y a pas plus de n opérations, et à fortiori si B est $<$ que ce terme. La détermination du maximum du nombre des opérations revient donc à celle du rang du terme qui dans (1) est égal, ou immédiatement supérieur à B.

On y parviendrait au moyen du terme général de (1), traitée comme une série récurrente : mais ce terme n'étant pas maniable, je remplacerai la série (1) par une autre. Cette série (1) se rapporte à la fraction continue

$$1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \ldots}}}$$

dont les réduites sont

$$\frac{1}{1}, \frac{2}{1}, \frac{3}{2}, \frac{5}{3}, \frac{8}{5}, \text{ etc.} \qquad (3)$$

Parmi ces réduites, j'en prends une qui soit de rang impair : $\frac{8}{5}$, ainsi que chacune des suivantes, convient : je dirai tout à l'heure pourquoi $\frac{3}{2}$ ne convient pas. Je forme la série géométrique

$$1, \frac{8}{5}, \left(\frac{8}{5}\right)^2, \left(\frac{8}{5}\right)^3, \ldots \qquad (4)$$

sauf le premier terme, chacun des autres est $<$ que son correspondant pris dans (1); on peut s'en convaincre pour le deuxième et le troisième; pour les suivants, dans (1) chacun se déduit du précédent au moyen d'un multiplicateur égal à l'une des réduites (3), à partir de $\frac{5}{3}$; aucune de ces réduites n'est moindre que $\frac{8}{5}$ raison de la série (4); donc, etc.

Il s'ensuit que si B $\underset{<}{=}$ que le $n^{ième}$ terme de (4), B est $<$ que le $n^{ième}$ terme de (1). Donc, si B $\underset{<}{=}$ que $\left(\frac{8}{5}\right)^x$, qui est le terme de rang $x+1$ dans (4), B est $<$ que le terme de rang $x+1$ dans (1), et il y aura au plus x opérations; mais B sera $\underset{<}{=} \left(\frac{8}{5}\right)^x$, si x est un nombre entier au moins égal à $\frac{\log B}{\log 8 - \log 5} = \frac{\log B\ldots}{0{,}204\ldots}$. Soit c le nombre des chiffres de B; log. B est ainsi $< c$; il s'ensuit, que le maximum du nombre des opérations est le nombre entier immédiatement supérieur à $\frac{c}{0{,}204}$, nombre entier qui ne surpasse pas $\frac{c}{0{,}2}$ ou $5c$.

J'ajoute que la formule $\frac{\log B}{0{,}204}$ donnera souvent une limite

moindre ; c'est ainsi que si B=15 3, elle donne $\frac{2,184}{0,204}$ ou 11. au lieu de 15.

J'ai dit que la réduite $\frac{3}{2}$ ne convient pas pour raison de la série auxiliaire ; cela tient à ce que $\log \frac{3}{2} = 0,176$ et la limite serait $\frac{c}{0,176}\left(\text{ou } \frac{\log B}{0,176}\right)$, qui conduirait à $6c$.

Chacune des réduites de rang impair qui suivent $\frac{8}{5}$ donne un log. plus grand que 0,204, mais on y gagnerait peu de chose ; car ces réduites sont toutes moindres que $\frac{1+\sqrt{5}}{2}$, valeur de la fraction continue citée ; or $\frac{1+\sqrt{5}}{2}$ a pour log. une quantité qui reste au-dessous de 0,209, de sorte que le dénominateur de log. B, ne peut s'élever jusqu'à 0,209.

Si on emploie des quotients excédants, chaque reste est moindre que la moitié du précédent, diminué préalablement d'une unité, et ces restes successifs ont pour maxima $\frac{B-1}{2}$, $\frac{B-1-2}{2^2}$, $\frac{B-1-2-2^2}{2^3}$, ... $\frac{B-1-2-\ldots-2^{n-1}}{2^n} = \frac{B-2^n+1}{2^n}$.

Si donc ce dernier est <2, l'opération est terminé à la $n^{ième}$ division ; de là

$$B-2^n+1 < 2^{n+1} \text{ ou } B+1 < 2^n.3,$$

et

$$2^n > \frac{B+1}{3}, \text{ ou } n > \frac{l.(B+1)-l.3}{l.2}.$$

On peut donc prendre ce nombre pour limite, ou si l'on veut $\frac{l.(B+1)}{l.2} - 1$, ou encore $\frac{10}{3}\, l.\,(B+1) - 1$, nombre plus simple que la limite donnée par M. Binet. (*Compte rendu*. n° 19 du 2me semestre 1844.)