
ANNALES DE MATHÉMATIQUES PURES ET APPLIQUÉES.

GERGONNE

Réflexions sur le même problème

Annales de Mathématiques pures et appliquées, tome 5 (1814-1815), p. 322-327

http://www.numdam.org/item?id=AMPA_1814-1815__5__322_1

© Annales de Mathématiques pures et appliquées, 1814-1815, tous droits réservés.

L'accès aux archives de la revue « Annales de Mathématiques pures et appliquées » implique l'accord avec les conditions générales d'utilisation (<http://www.numdam.org/conditions>). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

Article numérisé dans le cadre du programme
Numérisation de documents anciens mathématiques
<http://www.numdam.org/>

Réflexions sur le même problème ;

Par M. GERGONNE.

I. La question proposée revient évidemment à la suivante : *Trouver un nombre de n chiffres qui , retranché de son carré , donne un reste qui ait au moins n zéros à sa droite ?*

Soit x le nombre cherché , et soit généralement B la base du système de numération relativement auquel on se propose de résoudre le problème ; en désignant par y un nombre entier indéterminé , l'équation de ce problème sera

$$x^2 - x \text{ ou } x(x-1) = B^n y ;$$

x ne devant pas avoir plus de n chiffres.

On satisfait d'abord généralement à cette équation , quel que soit B , en posant $y=0$, d'où

$$x=0 \text{ ou } x=1 .$$

Ainsi , dans tout système de numération , tout nombre terminé par n zéros ou par l'unité précédée de $n-1$ zéros , a toutes ces puissances terminées aussi par n zéros ou par l'unité précédée de $n-1$ zéros , respectivement ; ce qui est d'ailleurs évident. Nous ne nous occuperons donc plus à l'avenir de ces deux solutions.

Pour parvenir à la découverte des autres , remarquons d'abord que x , et à plus forte raison $x-1$, étant moindre que B^n , ne sauraient , ni l'un ni l'autre , être divisibles par ce diviseur ; et , comme d'ailleurs ces deux nombres x et $x-1$ sont nécessairement premiers entre eux , ils ne sauraient être divisibles , respectivement , que par deux nombres aussi premiers entre eux.

Soit donc supposé

$$B^n = pq ;$$

p et q étant deux facteurs premiers entre eux , différens de B^n et de l'unité. B^n étant le plus petit des nombres de $n+1$ chiffres ; il s'ensuit que p et q seront l'un et l'autre moindres que x et $x-1$; en choisissant donc x de manière que l'un des deux soit divisible par p et l'autre par q , on remplira les conditions du problème , puisqu'on aura l'une ou l'autre des équations

$$\frac{x}{p} \cdot \frac{x-1}{q} = y , \quad \frac{x}{q} \cdot \frac{x-1}{p} = y .$$

dont les premiers membres sont entiers, par l'hypothèse, et qui ont pour second membre un nombre entier indéterminé.

Posant donc

$$\left. \begin{array}{l} x=pt, \\ x-1=qu; \end{array} \right\} \text{ ou } \left\{ \begin{array}{l} x=qt; \\ x-1=pu; \end{array} \right.$$

l'élimination de x donnera

$$pt-qu=1 \quad \text{ou} \quad qt-pu=1.$$

Ayant donc trouvé un système de valeurs de t et u satisfaisant à l'une ou à l'autre de ces deux équations, on aura ensuite

$$x=pt \quad \text{ou} \quad y=qt,$$

et le problème sera résolu.

On voit par là qu'outre les solutions communes à tous les systèmes de numération déjà mentionnés, le problème admettra encore deux fois autant de solutions qu'il y aura de manières de décomposer B^n en deux facteurs premiers entre eux, différents de lui-même et de l'unité.

Soit supposé

$$B=a^\alpha b^\beta c^\gamma \dots \dots x \quad \text{d'où} \quad B^n=a^{n\alpha} b^{n\beta} c^{n\gamma} \dots \dots$$

$a, b, c, \dots \dots$ étant des nombres premiers inégaux, au nombre de m . Il est évident qu'il y aura autant de manières de décomposer B^n en deux facteurs premiers entre eux, dont aucun ne soit l'unité, qu'il y aurait de manières d'exécuter cette décomposition sur le simple produit

$$abc \dots \dots gh,$$

aussi de m facteurs. Or, soit Z_{m-1} ce nombre de décompositions pour le produit de $m-1$ facteurs

$$abc \dots \dots g,$$

en introduisant le m^{me} facteur h , on pourra l'introduire indifféremment

remment, pour chaque décomposition, dans le premier ou dans le second facteur, ou bien encore le prendre à lui seul pour un facteur; ce qui prouve qu'on doit avoir $Z_m = 2Z_{m-1} + 1$; ce qui donne, en général,

$$Z_m = 2^m C - 1;$$

mais, lorsque $m=2$, on a évidemment $Z_m=1$, donc $C=\frac{3}{2}$, et par conséquent

$$Z_m = 2^{m-1} - 1;$$

le nombre des solutions, autres quē les deux mentionnées ci-dessus sera donc

$$2Z_m = 2^m - 2,$$

en y joignant donc ces deux-là, leur nombre total s'élèvera à 2^m ; m indiquant combien la base B a de sortes de facteurs premiers.

II. Lorsqu'on a trouvé un nombre dont les n derniers chiffres à droite se reproduisent perpétuellement à la droite de toutes ses puissances, il est évident qu'à plus forte raison ses n' derniers chiffres à droite, n' étant moindres que n , se reproduiront aussi perpétuellement à la droite de toutes ses puissances. Les solutions du problème, pour la valeur n , donnent donc en même temps *des solutions*, pour la valeur n' , moindre que n ; puis donc que, par ce qui précède le nombre des solutions pour chaque valeur de n est toujours le même et ne dépend que de m , il sera le même pour n' que pour n , et conséquemment les solutions pour la valeur n donneront *toutes les solutions* pour la valeur n' .

Ainsi, lorsqu'on voudra avoir les solutions pour plusieurs valeurs de n ; au lieu de monter successivement de plus petites valeurs à la plus élevée, il sera incomparablement préférable d'attaquer directement le problème pour cette dernière; puisque les solutions qu'on obtiendra renfermeront implicitement toutes les autres.

Appliquons ces généralités à notre système de numération ; et cherchons à résoudre le problème, dans ce système, pour les 20 premières valeurs de n . Pour cela nous poserons sur-le-champ $n=20$. Nous avons d'ailleurs $B=10=2.5$, d'où $B^n=2^{20}.5^{20}$; et nous n'aurons conséquemment que le seul système de valeurs

$$p=2^{20}, \quad q=5^{20};$$

en sorte qu'il faudra résoudre successivement les deux équations indéterminées

$$2^{20}.t-5^{20}.u=1, \quad 5^{20}.t-2^{20}.u=1;$$

ou du moins chercher les plus petits nombres qui y satisfont ; en posant ensuite

$$x=2^{20}.t, \quad x=5^{20}.t.$$

Or, on a

$$2^{20}=1\ 048\ 576,$$

$$5^{20}=94\ 956\ 806\ 640\ 625.$$

Si l'on cherche le plus grand commun diviseur entre ces deux nombres, les quotiens successifs seront

90949470, 5, 1, 1, 1, 3, 1, 1, 3, 1, 1, 1, 1, 10, 1, 12 :

A l'aide de ces quotiens, sauf le dernier, on trouvera, pour la dernière fraction convergente vers $\frac{5^{20}}{2^{20}}$,

$$\frac{7385006028926}{81199}.$$

On conclura de là, par les théories connues (*), que le plus petit système de valeurs de t et u , dans l'équation

(*) Voyez le 2.^e volume de l'*Algèbre* d'Euler, ou la *Théorie des nombres* de M. Legendre.

$$2^{20} \cdot t - 5^{20} \cdot z = 1$$

est

$$t = 7385006028926 ,$$

$$z = 81199 ;$$

que par conséquent, pour l'équation

$$5^{20} \cdot t - 2^{20} \cdot z = 1 ,$$

ce plus petit système de valeurs est

$$t = 2^{20} - 81199 ,$$

$$z = 5^{20} - 7385006028926 .$$

On aura donc

$$x = 2^{20} \cdot 7385006028926 ;$$

$$x = 5^{20} \cdot (2^{20} - 81199) = 10^{20} - 5^{20} \cdot 81199 ;$$

On trouvera ainsi que tous les nombres et les seuls nombres dont un certain nombre des derniers chiffres à droite seront les mêmes, que dans l'un quelconque des quatre nombres

$$\dots\dots\dots 00000 \ 00000 \ 00000 \ 00000 ,$$

$$\dots\dots\dots 00000 \ 00000 \ 00000 \ 00001 ,$$

$$\dots\dots\dots 07743 \ 74008 \ 19871 \ 09376 ,$$

$$\dots\dots\dots 92256 \ 25991 \ 82128 \ 90625 ,$$

auront aussi les mêmes derniers chiffres à droite, en même nombre, à toutes leurs puissances.

On traiterait d'une manière analogue le cas où l'on exigerait seulement que les terminaisons des puissances successives fussent périodiques (*).

(*) Le Rédacteur a reçu postérieurement de M. Durrande une autre solution du même problème, qui rentre pour le fond dans celles qui viennent d'être mentionnées.