ANNALES
DE MATHÉMATIQUES
PURES ET APPLIQUÉES.

FRÉDÉRIC SARRUS

Questions résolues. Démonstration de la fausseté du théorème énoncé à la page 320 du IX.e volume de ce recueil

Annales de Mathématiques pures et appliquées, tome 10 (1819-1820), p. 184-187
<http://www.numdam.org/item?id=AMPA_1819-1820__10__184_0>

QUESTIONS RÉSOLUES.

Démonstration de la fausseté du théorème énoncé à la page 320 du IX.e volume de ce recueil ;

Par M. FRÉDÉRIC SARRUS.

LE théorème dont il s'agit consiste en ce que tout nombre impair $2n+1$ serait ou ne serait pas premier, suivant que l'un des deux nombres 2^n-1, 2^n+1 serait ou ne serait pas divisible par $2n+1$.

En cherchant à démontrer cette proposition, je l'ai trouvée en défaut pour le nombre 341.

On a, en effet,

$$2^5-1=31\ ,\quad 2^5+1=33\ ;\quad \text{d'où}\quad 2^{10}-1=31.33=341.3\ ;$$

donc

$$2^{10}=341.3+1\ ,$$

et par suite

$$2^{170}=(341.3+1)^{17}\ ,$$

si

si l'on développe le second membre de cette équation, tous les termes de son développement excepté le dernier 1 seront divisibles par 341 ; de sorte qu'on peut écrire

$$2^{170}=341k+1 ,$$

k désignant un nombre entier ; or, de là résulte

$$2^{170}-1=341k ;$$

ainsi, $2^{170}-1$ est divisible par 341, bien que ce nombre ne soit pas premier.

Il est donc certain que l'une des deux formules 2^n-1 et 2^n+1 peut être divisible par le nombre impair $2n+1$, sans que ce nombre soit premier ; mais il n'en demeure pas moins certain que, lorsque ce nombre est premier, il divise nécessairement l'une ou l'autre de ces deux formules ; ce qu'on peut prouver assez simplement comme il suit.

Soit p un nombre premier quelconque, on aura

$$2^p=(1+1)^p=1+\frac{p}{1}+\frac{p}{1}\cdot\frac{p-1}{2}+\ldots\ldots+\frac{p}{1}\cdot\frac{p-1}{2}+\frac{p}{1}+1 ;$$

d'où

$$2^p-2=\frac{p}{1}+\frac{p}{1}\cdot\frac{p-1}{2}+\frac{p}{1}\cdot\frac{p-1}{2}\cdot\frac{p-2}{3}+\ldots$$

$$+\frac{p}{1}\cdot\frac{p-1}{2}\cdot\frac{p-2}{3}+\frac{p}{1}\cdot\frac{p-1}{2}+\frac{p}{1} :$$

Tous les termes du second membre de cette équation sont, comme l'on sait des nombres entiers. De plus, ils sont tous divisibles par p, qui ne saurait se trouver au dénominateur d'aucun d'eux, donc 1.° lorsque p est premier

$$\frac{2^p-2}{p}$$

est un nombre entier.

Supposons présentement que le nombre premier p soit un nombre impair de la forme $2n+1$, en substituant dans la formule elle deviendra

$$\frac{2(2^{2n}-1)}{2n+1} = \frac{2.(2^n-1)(2^n+1)}{2n+1};$$

or, 2 ne pouvant être divisible par le nombre premier impair $2n+1$, il faut que ce soit le produit $(2^n-1)(2^n+1)$, et par suite l'un ou l'autre de ses facteurs 2^n-1, 2^n+1 qui soit divisible par ce diviseur.

N'aurons-nous donc rien de plus simple que le théorème de Wilson, pour juger, *à priori*, si un nombre donné est ou n'est pss premier? Il nous paraît du moins que son procédé est susceptible d'abréviations notables. Dabord comme tout nombre composé a toujours au moins un diviseur premier moindre que la racine du quarré le plus approchant en plus; on voit que N étant un nombre donné, et g, h deux nombres premiers consécutifs, tels que $g^2 < N$ et $h^2 > N$; si l'on fait le produit $P = 1.2.3.5.7.11....g$ des nombres premiers, jusqu'à g inclusivement; suivant que P et N auront ou n'auront pas un commun diviseur, N sera composé au premier : on peut même, dans ce produit, supprimer les facteurs 2.3.5, attendu que ces facteurs se reconnaissent dans un nombre à la première inspection.

Ainsi, par exemple, puisque 400 est le quarré de 20, il suffira, pour reconnaître si un nombre inférieur à 400 ou même à 441 est composé ou premier, de chercher s'il a ou n'a pas un diviseur commun avec $32323 = 7.11.13.17.19$.

A la vérité, ceci suppose qu'on a une table des nombres premiers qui s'étend au moins jusqu'à $\sqrt{N}$; mais si l'on était privé d'une pareille table, on en serait seulement réduit à substituer au produit des nombres premiers le produit $7.11.13.17.19\,23.25.29.31.35.37\ldots\ldots$ des nombres de la forme $6n \mp 1$ qui, comme l'on sait, comprend tous les nombres premiers (*).

(*) Nous nous sommes assurés que la loi dont M. Sarrus vient de démontrer la fausseté se soutient pour les 70 premiers nombres naturels ; peut-être même se soutient-elle beaucoup au-delà ; et c'en est assez pour montrer quel fond on doit faire sur l'*induction*, même en mathématiques.

Il serait curieux de savoir quel est le plus petit nombre composé pour lequel elle est en défaut ; et quelle est la forme générale des nombres pour laquelle elle est fausse.

Nous saisissons cette occasion pour observer que, dans l'impression du mémoire de M. Sarrus, inséré à la pag. 33 de ce volume, il s'est glissé diverses erreurs, dont une très-grave et de nature à le rendre inintelligible : en voici la correction.

Page 37, ligne 3, pour $+a_n \frac{\mathrm{d}A_m}{\mathrm{d}a_m}$; *lisez* : $+a_n \frac{\mathrm{d}A_m}{\mathrm{d}a_n}$.

ligne 7 ; pour 2^{α}, *lisez* : 2α.

Page 48, lignes 4, 5, 6, 8 ; les premiers membres qui sont a_1, $2a_1$, $3a_1$, ... na_1, doivent être a_1A_1, $2a_1A_2$, $3a_1A_3$, ... na_1A_n.

Page 49, ligne 3, au dernier terme ; $n+a$, *lisez* : $n+2$.

J. D. G.