

LIONNET

**Note sur la somme des puissances semblables
de plusieurs nombres en progression
arithmétique, et sur quelques propriétés
des nombres premiers**

Nouvelles annales de mathématiques 1^{re} série, tome 1
(1842), p. 175-178

http://www.numdam.org/item?id=NAM_1842_1_1__175_1

© Nouvelles annales de mathématiques, 1842, tous droits réservés.

L'accès aux archives de la revue « Nouvelles annales de mathématiques » 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/>

NOTE

Sur la somme des puissances semblables de plusieurs nombres en progression arithmétique, et sur quelques propriétés des nombres premiers.

PAR M. LIONNET,

Professeur au Collège royal de Louis-le-Grand.

1. La formule, au moyen de laquelle on calcule la somme s_m des puissances entières du degré m de plusieurs nombres $a, b, c, \dots k, l$, en progression arithmétique est :

$$s_m = l^m + \frac{l^{m+1} - a^{m+1}}{(m+1)r} - \frac{m}{2}r(s_{m-1} - l^{m-1}) - \frac{m(m-1)}{2.3}r^2(s_{m-2} - l^{m-2}) - \text{etc.},$$

dans laquelle r désigne la raison de la progression. Nous allons reprendre la démonstration de cette formule, en y introduisant une légère modification, qui nous permettra de lui donner une forme plus simple.

On a les relations

$$b = a + r, \quad c = b + r, \quad d = c + r \dots \quad l = k + r,$$

d'où on déduit, par la formule du binôme,

$$b^{m+1} = a^{m+1} + \frac{m+1}{1} r a^m + \frac{(m+1)m}{1.2} r^2 a^{m-1} + \text{etc.} \dots + \frac{m+1}{1} r^m a + r^{m+1},$$

$$c^{m+1} = b^{m+1} + \frac{m+1}{1} r b^m + \frac{(m+1)m}{1.2} r^2 b^{m-1} + \text{etc.} \dots + \frac{m+1}{1} r^m b + r^{m+1},$$

.....

$$l^{m+1} = k^{m+1} + \frac{m+1}{1} r k^m + \frac{(m+1)m}{1.2} r^2 k^{m-1} + \text{etc.} \dots + \frac{m+1}{1} r^m k + r^{m+1}.$$

On a de même

$$(l+r)^{m+1} = l^{m+1} + \frac{m+1}{1} r l^m + \frac{(m+1)m}{1.2} r^2 l^{m-1} + \text{etc.} \dots + \frac{m+1}{1} r^m l + r^{m+1}.$$

Ajoutant ces égalités, et supprimant les termes $b^{m+1}, c^{m+1} \dots l^{m+1}$, communs aux deux membres de l'égalité résultante, il vient

$$(l+r)^{m+1} = a^{m+1} + \frac{m+1}{1} r s_m + \frac{(m+1)m}{1.2} r^2 s_{m-1} + \dots + \frac{m+1}{1} r^m s_1 + r^{m+1} s_0.$$

et, par suite,

$$(A) \dots s_m = \frac{(l+r)^{m+1} - a^{m+1}}{(m+1)r} - \frac{m}{2} r s_{m-1} - \frac{m(m-1)}{2.3} r^2 s_{m-2} - \text{etc.} \dots - r^{m-1} s_1 - \frac{r^m s_0}{m+1}.$$

Telle est la formule qu'il s'agissait d'obtenir.

2. THÉORÈME. *P étant un nombre premier plus grand que 2 et m un nombre entier compris entre 0 et P-1, la somme des puissances du degré m des nombres 1, 2, 3 ... P-1 est divisible par P.*

Pour appliquer la formule (A) au cas particulier des termes de la progression arithmétique $\div 1, 2, 3 \dots P-1$, il suffit d'y faire $a=1, r=1, l=s_0=P-1$. Alors elle devient

$$(B) \quad s_m = \frac{P(P^m-1)}{m+1} - \frac{m}{2} s_{m-1} - \frac{m(m-1)}{2 \cdot 3} s_{m-2} - \text{etc.} \dots - s_1.$$

Multipliant les deux membres de cette égalité par $1, 2, 3 \dots m(m+1)$, on aura

$$1.2.3 \dots m(m+1) s_m = 1.2.3 \dots m.P(P^m-1) - A_1 s_{m-1} \\ - A_2 s_{m-2} - \text{etc.} \dots - A_{m-1} s_1,$$

$A_1, A_2, A_3 \dots A_{m-1}$ étant des nombres entiers.

On voit par là que si l'on suppose chacune des sommes $s_1, s_2 \dots s_{m-1}$ divisible par P , il en sera de même du produit $1, 2, 3 \dots m(m+1) s_m$; mais, par hypothèse, on a $m < P-1$, et, par suite, $m+1 < P$; donc, le nombre premier P ne divise aucun des facteurs du produit $1, 2, 3 \dots m(m+1)$; donc, il divise s_m . D'ailleurs, puisqu'on suppose $P > 2$, la somme s' , ou $\frac{P(P-1)}{2}$, est divisible par P ; donc, en vertu de ce qui précède, s_2 est aussi divisible par P ; s_1 et s_2 étant divisibles par P , il en sera de même de la somme s_3 , et ainsi de suite jusqu'à s_{P-2} inclusivement.

3. THÉORÈME. *P étant un nombre premier plus grand que 2 et m un nombre entier compris entre 0 et P-1, la somme P_m des produits m à m des nombres 1, 2, 3 ... P-1 est divisible par P.*

En effet, les nombres $P_1, P_2, P_3 \dots P_m$ et ceux qu'on a désignés précédemment par $s_1, s_2, s_3 \dots s_m$ sont liés entre eux par la relation connue

$$(C) \quad s_m - P_1 s_{m-1} + P_2 s_{m-2} - \text{etc.} \dots \mp P_{m-1} s_1 = \mp m P_m,$$

dans laquelle on donne au second membre le signe — ou le signe +, suivant que m est pair ou impair. Or, en vertu du théorème précédent, chacun des nombres $s_1, s_2 \dots s_m$ est divisible par P ; donc, $m P_m$ et, par suite, P_m est aussi divisible par P .

4. THÉORÈME. *P étant un nombre premier, le produit 1, 2, 3... (P-1) augmenté de l'unité est divisible par P; et réciproquement, tout nombre P, qui satisfait à cette condition, est premier.*

1° Car, si l'on conçoit le produit des P-1 binômes (1+1), (1+2), (1+3), ... [1+(P-1)] [1+(P-2)] [1+(P-3)], ordonné suivant les puissances décroissantes de leur premier terme 1, on aura l'égalité

$1.2.3... (P-1). P = 1 + P_1 + P_2 + P_3 + \dots + P_{P-2} + 1.2.3... (P-1)$, dans laquelle P_1, P_2, \dots, P_{P-2} ont la même signification que dans la démonstration du théorème précédent; or, en vertu de ce théorème, chacun des nombres P, P_1, \dots, P_{P-2} est divisible par P; d'ailleurs, le produit $1, 2, 3 \dots (P-1) P$ est aussi divisible par P; donc, il en est de même de $1, 2, 3 \dots (P-1) + 1$.

2° Soit L un diviseur de P, inférieur à P. Ce nombre L sera l'un des facteurs 1, 2, 3... P-1; donc, il divisera leur produit; d'ailleurs L, étant diviseur de P, divise aussi le nombre $1, 2, 3 \dots (P-1) + 1$, qui est multiple de P; donc $L=1$; donc le nombre P n'admet pour diviseurs que P et l'unité; donc, il est premier.

Ce théorème, dont *Waring* attribue l'énoncé à *Jean Wilson*, et le théorème précédent ont été démontrés, pour la première fois, par *Lagrange* (Nouveaux mémoires de l'Académie de Berlin, année 1774). Lorsqu'on prouve d'abord, comme l'a fait *Lagrange*, que tous les produits $P_1, P_2, P_3 \dots P_{P-2}$ sont divisibles par P, il est facile de démontrer ensuite, au moyen de la formule (C), que chacune des sommes $s_1, s_2, s_3, \dots, s_{P-2}$ est aussi divisible par P. En suivant une autre marche, nous avons eu pour objet de mettre les démonstrations de ces théorèmes plus à la portée des élèves.