

ANGELO GENOCCHI

Solution de la question 293 (J.-A. Serret)

Nouvelles annales de mathématiques 1^{re} série, tome 14
(1855), p. 241-245

http://www.numdam.org/item?id=NAM_1855_1_14__241_0

© Nouvelles annales de mathématiques, 1855, 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/>

SOLUTION DE LA QUESTION 293 (J.-A. SERRET)

(voir t. XIII, p. 314);

PAR M. ANGELO GENOCCHI.

Je m'appuierai sur la proposition suivante :

Lemme. Soient n nombres entiers $a, b, \dots, k$; m leur somme; p un nombre premier, et faisons

$$M = \frac{1 \cdot 2 \dots m}{(1 \cdot 2 \dots a)(1 \cdot 2 \dots b) \dots (1 \cdot 2 \dots k)};$$

je dis que si tous les nombres $a, b, \dots, k$ sont divisibles par $p - 1$. et forment une somme $m < p^n - 1$, M sera divisible par p .

Pour le démontrer, j'observe : 1° que l'exposant de p , dans tout produit continu $1 \cdot 2 \dots N$, est la somme des quotients entiers q_1, q_2, q_3 , etc., obtenus en divisant successivement N par p, p^2, p^3 , etc., ou, ce qui revient au même, en divisant N , puis q_1 , puis q_2 , etc., par p (LEGENDRE, *Théorie des nombres*, t. I, p. 10); 2° que si plusieurs nombres étant divisés par p donnent les quotients q, q', q'' , etc., et les restes r, r', r'' , etc., leur somme, divisée également par p , donnera pour quotient $q + q' + q'' + \dots$ et pour reste $r + r' + r'' + \dots$ lorsqu'on aura

$$r + r' + r'' + \dots < p,$$

et, dans le cas contraire, donnera un quotient supérieur à $q + q' + q'' + \dots$. Il s'ensuit que pour obtenir une valeur de M non divisible par p , p devant alors monter à la même puissance dans le numérateur et dans le dénomi-

nateur de M , on aura à considérer les équations

$$\begin{aligned} m &= \mu_0 p + m_0, & \mu_0 &= \mu_1 p + m_1, & \mu_1 &= \mu_2 p + m_2, \dots, \\ a &= \alpha_0 p + a_0, & \alpha_0 &= \alpha_1 p + a_1, \dots, \\ b &= \beta_0 p + b_0, & \beta_0 &= \beta_1 p + b_1, \dots, \\ k &= \chi_0 p + k_0, & \chi_0 &= \chi_1 p + k_1, \dots, \end{aligned}$$

formées avec les quotients et les restes positifs ou nuls qu'on trouve en divisant par p , et il faudra supposer

$$\mu_0 = \alpha_0 + \beta_0 + \dots + \chi_0, \quad m_0 = a_0 + b_0 + \dots + k_0,$$

puis

$$\begin{aligned} \mu_1 &= \alpha_1 + \beta_1 + \dots + \chi_1, & m_1 &= a_1 + b_1 + \dots + k_1, \\ \mu_2 &= \alpha_2 + \beta_2 + \dots + \chi_2, & m_2 &= a_2 + b_2 + \dots + k_2, \\ & \dots\dots\dots \end{aligned}$$

d'où

$$m_0 + m_1 + m_2 + \dots = \sum a_i + \sum b_i + \dots + \sum k_i.$$

Mais on aura en même temps

$$\begin{aligned} m &= m_0 + m_1 p + m_2 p^2 + \dots, \\ a &= a_0 + a_1 p + a_2 p^2 + \dots, \\ & \dots\dots\dots \end{aligned}$$

D'ailleurs, si a est divisible par $p - 1$, il en sera de même de la somme $\sum a_i$, puisqu'on trouve

$$\begin{aligned} a &= a_1(p-1) + a_2(p^2-1) + a_3(p^3-1) + \dots \\ &= a_0 + a_1 + a_2 + a_3 + \dots; \end{aligned}$$

cette remarque s'applique aussi à $\sum b_i, \dots, \sum k_i$. Donc, en vertu de l'équation précédente, la somme

$$m_0 + m_1 + m_2 + \dots$$

ne sera pas inférieure à $n(p-1)$. Or les restes m_i sont tous inférieurs à p ; donc le nombre de ceux qui ne sont pas nuls sera au moins égal à n : d'où l'on conclut que la valeur de m doit contenir des puissances de p supérieures à p^{n-2} . Si elle contient seulement p^{n-1} , les coefficients m_i seront tous égaux à $p-1$, sans quoi leur somme serait $< n(p-1)$, et l'on aura

$$m = (p-1)(1 + p + p^2 + \dots + p^{n-1}) = p^n - 1;$$

si la valeur de m contient p^n ou des puissances supérieures, m sera plus grand que $p^n - 1$. Donc enfin, si M n'est pas divisible par p , le nombre m ne sera pas inférieur à $p^n - 1$. C. Q. F. D.

Remarque. Si m était égal à $p^n - 1$, on pourrait prendre, par exemple,

$$\begin{aligned} a &= p-1, & b &= p(p-1), & c &= p^2(p-1), \dots, \\ & & k &= p^{n-1}(p-1), \end{aligned}$$

et alors M ne serait pas divisible par p (*).

Cela posé, soit un polynôme

$$X = a_1 + a_2 x + a_3 x^2 + \dots + a_n x^{n-1},$$

qui acquerra p^n valeurs distinctes en donnant à chaque

(*) En représentant M par $(a, b, \dots, k)$, on a identiquement

$$a(a, b, \dots, k) = m(a-1, b, \dots, k),$$

et, par suite, aM est divisible par m . Il en sera de même de bM , cM , ..., kM , en sorte que si ω désigne le plus grand commun diviseur des nombres $a, b, \dots, k$, alors m divisera le produit ωM . Ce théorème a été donné par M. Cauchy (*Comptes rendus*, t. XII, p. 707). On en déduit que si m est une puissance du nombre premier p , toutes les valeurs de M , c'est-à-dire tous les coefficients du développement de la *même* puissance d'un polynôme, autres que 1, sont multiples de p : d'où résulte immédiatement un *lemme* employé souvent dans la théorie des *congruences irréductibles*, savoir que, $f(x)$ étant un polynôme à coefficients entiers, on a

$$[f(x)]^{p^n} \equiv f(x^{p^n}) \pmod{p}.$$

(SERRET, *Algèbre supérieure*, 2^e édition, p. 357.)

coefficient a_i toutes les valeurs $0, 1, 2, 3, \dots, p-1$. Élevons ce polynôme à la puissance m et considérons un terme quelconque du résultat ordonné suivant les puissances de x . Si tous les coefficients $a_1, a_2, \dots, a_n$ n'entrent pas dans ce terme, s'il y manque par exemple a_1 , alors, en ajoutant les p valeurs de X^m qui correspondent aux p valeurs de a_1 et à une combinaison déterminée des autres coefficients, on trouvera p fois ce même terme. Si dans ce terme l'un, a_i , des coefficients est élevé à un exposant r , qui ne soit pas divisible par $p-1$, dans la somme des mêmes valeurs de X^m ce terme acquerra pour facteur la somme $0^r + 1^r + 2^r + \dots + (p-1)^r$, qui est, comme on sait, divisible par p . Enfin, si le terme qu'on considère renferme tous les coefficients $a_1, a_2, \dots, a_n$ élevés à des exposants divisibles par $p-1$, il sera affecté d'un coefficient numérique M , qui, en vertu du lemme, sera divisible par p tant qu'on aura $m < p^n - 1$. On conclut de là que, si m est plus petit que $p^n - 1$, la somme de toutes les valeurs de X^m ne renferme que des termes ayant p pour facteur. Ainsi, dans ce cas, $\sum X^m$ égale un multiple de p .

On voit immédiatement pour $n = 1$ et pour $n = 2$ que cette égalité n'a plus lieu lorsque $m = p^n - 1$, et, pour s'en assurer, en général, on peut avoir recours à la théorie des *congruences irréductibles* exposées dans la nouvelle édition de l'*Algèbre supérieure*, 25^e leçon. En effet, on démontre qu'il existe toujours une fonction entière $F(x)$ du degré n à coefficients entiers, pour laquelle on ne saurait avoir *identiquement*

$$\varphi(x)\psi(x) = F(x) + p\chi(x),$$

$\varphi(x), \psi(x), \chi(x)$ désignant trois polynômes à coefficients entiers; et qu'alors, pour chaque valeur de x , zéro

excepté, on peut poser

$$f(x)F(x) = X^m - 1 + p\chi(x);$$

f et χ désignant des polynômes à coefficients entiers, m étant égal à $p^n - 1$, et en supposant que le coefficient de x^n dans $F(x)$ soit réduit à l'unité. Il s'ensuit que, si l'on prend pour x une racine de l'équation $F(x) = 0$, on aura, pour ces $p^n - 1$ valeurs de X , la congruence

$$X^m \equiv 1 \pmod{p},$$

et, par conséquent,

$$\sum X^m \equiv p^n - 1 \equiv -1 \pmod{p},$$

et qu'ainsi $\sum M^m$ ne sera pas multiple de p .

Si l'on suppose que x représente un nombre entier quelconque, on verra aisément que $\sum X^m$ sera toujours multiple de p , excepté dans le cas de $n = 1$ et $m = p - 1$.
