NOUVELLES ANNALES DE MATHÉMATIQUES

ANGELO GENOCCHI

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

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

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

## 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 $a, b, \ldots, k$; $m$ leur somme; $p$ un nombre premier, et faisons

$$M = \frac{1.2\ldots m}{(1.2\ldots a)(1.2\ldots b)\ldots(1.2\ldots k)},$$

je dis que si tous les nombres $a, b, \ldots, k$ 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 continuel $1.2\ldots N$, 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 $q + q' + q'' + \ldots$ et pour reste $r + r' + r'' + \ldots$ lorsqu'on aura

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

et, dans le cas contraire, donnera un quotient supérieur à $q + q' + q'' + \ldots$. 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

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

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

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

puis

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

d'où

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

Mais on aura en même temps

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

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

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

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

$$m_0 + m_1 + m_2 + \ldots$$

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

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

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,

$$a = p-1, \quad b = p(p-1), \quad c = p^2(p-1), \ldots, \quad k = p^{n-1}(p-1),$$

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

Cela posé, soit un polynôme

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

qui acquerra $p^n$ valeurs distinctes en donnant à chaque

---

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

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

et, par suite, $a$M est divisible par $m$. Il en sera de même de $b$M, $c$M,..., $k$M, en sorte que si $\omega$ désigne le plus grand commun diviseur des nombres $a, b, \ldots k$, alors $m$ divisera le produit $\omega$M. 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 *mième* 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*, 2e édition, p. 357.)

coefficient $a_i$ toutes les valeurs $0, 1, 2, 3, \ldots, p-1$. Élevons ce polynôme à la puissance $m$ et considérons un terme quelconque du résultat ordonné suivant les puissances de $x$. Si tous les coefficients $a_1, a_2, \ldots, a_n$ 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 $0^r + 1^r + 2^r + \ldots + (p-1)^r$, qui est, comme on sait, divisible par $p$. Enfin, si le terme qu'on considère renferme tous les coefficients $a_1, a_2, \ldots, a_n$ 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*, 25e 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

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

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

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

et, par conséquent,

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

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

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