JOURNAL
DE
MATHÉMATIQUES
PURES ET APPLIQUÉES
FONDÉ EN 1836 ET PUBLIÉ JUSQU'EN 1874
PAR JOSEPH LIOUVILLE

J.-A. SERRET

Sur une question de théorie des nombres

Journal de mathématiques pures et appliquées 1re série, tome 15 (1850), p. 296.
<http://www.numdam.org/item?id=JMPA_1850_1_15__296_0>

SUR UNE QUESTION DE THÉORIE DES NOMBRES;

PAR M. J.-A. SERRET.

M. Kronecker a donné, dans le tome XXIX du Journal de M. Crelle, une démonstration simple et élégante de ce théorème :

Si p est un nombre premier, l'équation $\frac{x^p-1}{x-1}=0$ *est irréductible.*

La proposition sur laquelle repose cette démonstration est susceptible d'extension et peut alors s'énoncer ainsi :

Si p désigne un nombre premier et que $f(x)$ *soit un polynôme à coefficients entiers, tel que* $f(1)\equiv 1 \pmod p$, *on aura* $f(\alpha)f(6)\dots f(\omega)\equiv 1 \pmod p$, $\alpha, 6, \dots, \omega$ *étant les racines primitives de l'équation* $x^{p^\mu}-1=0$.

Pour le démontrer, posons

$$F_n(x)=f(x)f(x^2)f(x^3)\dots f\left(x^{p^n}\right)=A_0+A_1x+\dots,$$

remplaçons x par chaque racine de $x^{p^n}-1=0$, et ajoutons les résultats : on aura

$$(A)\quad\begin{cases}(p^n-p^{n-1})F_n(\alpha)+(p^{n-1}-p^{n-2})[F_{n-1}(\alpha_1)]^p+(p^{n-2}-p^{n-3})[F_{n-2}(\alpha_2)]^{p^2}+\dots\\ +(p^2-p)[F_2(\alpha_{n-2})]^{p^{n-2}}+(p-1)[F_1(\alpha_{n-1})]^{p^{n-1}}+[f(1)]^{p^n}\equiv 0 \pmod{p^n},\end{cases}$$

$\alpha, \alpha_1, \alpha_2, \dots, \alpha_{n-1}$ désignant des racines primitives des équations respectives

$$x^{p^n}-1=0,\quad x^{p^{n-1}}-1=0,\quad x^{p^{n-2}}-1=0,\dots,\quad x^p-1=0.$$

La congruence (A) sert à prouver que $F_n(\alpha)\equiv 1 \pmod p$, α étant une racine primitive de $x^{p^n}-1=0$. On le démontre immédiatement pour $n=1$; ensuite on voit aisément que, si cela a lieu pour $n=1, 2, \dots, \mu-1$, cela est vrai aussi pour $n=\mu$. Divisant ensemble les congruences $F_\mu(\alpha)\equiv 1$ et $F_{\mu-1}(\alpha_1)\equiv 1 \pmod p$, on a

$$f(\alpha)f(6)\dots f(\omega)\equiv 1 \pmod p,$$

où $\alpha, 6, \dots, \omega$ désignent les racines primitives de $x^{p^\mu}-1=0$.

De là on peut conclure que l'équation $\frac{x^{p^\mu}-1}{x^{p^{\mu-1}}-1}=X=0$ est irréductible, car si $X=f(x)\varphi(x)$, les coefficients de $f(x)$ et $\varphi(x)$ seront entiers, on aura $f(1)\varphi(1)=p$, d'où $f(1)=1$ et $\varphi(1)=p$; par suite, $\alpha, 6, \dots, \omega$ étant les racines de $X=0$, on aura $f(\alpha)f(6)\dots f(\omega)\equiv 1 \pmod p$, ce qui est absurde, car le premier membre est nul.

On déduit facilement de là que, quel que soit m, l'équation $x^m-1=0$ devient irréductible quand on l'a débarrassée de ses racines non primitives.