

E. PROUHET

Irréductibilité de l'équation

**$X = 1 + x + \dots + x^{p-1} = 0$, p étant
un nombre premier**

Nouvelles annales de mathématiques 1^{re} série, tome 9
(1850), p. 348-349

http://www.numdam.org/item?id=NAM_1850_1_9__348_0

© Nouvelles annales de mathématiques, 1850, 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/>

 IRRÉDUCTIBILITÉ

de l'équation $X = 1 + x + \dots + x^{p-1} = 0$, p étant un nombre premier

(voir t. VIII, p. 419),

PAR M. E. PROUHET.

I. Lemme 1. Les diviseurs de X ne peuvent être que de la forme $\dot{p} + 1$, pour toute valeur entière de x qui n'est pas $p + 1$. (Théorème connu.)

Lemme 2. Une congruence de degré n ne peut avoir plus de n racines, lorsque le module est premier. (Théorème connu.)

THÉORÈME. X ne peut être divisible par un polynôme de degré moindre, à coefficients entiers.

Démonstration. Si un pareil diviseur $\varphi(x)$ pouvait exister, on aurait, d'après le lemme 1,

$$\begin{aligned}\varphi(0) &= \dot{p} + 1, & \varphi(2) &= \dot{p} + 1, \\ \varphi(3) &= \dot{p} + 1, \dots, & \varphi(p-1) &= \dot{p} + 1,\end{aligned}$$

et, dès lors, la congruence

$$\varphi(x) - 1 = \dot{p},$$

de degré inférieur à $p - 1$, aurait $p - 1$ racines, ce qui est contraire au lemme 2. Donc, etc.

Démonstration du lemme 1.

II. Soit θ un diviseur premier de X , en sorte que

$$X = \dot{\theta};$$

on aura

$$X(x-1) = x^p - 1 = \dot{\theta}.$$

Puisque p est un nombre premier, si $x - 1$ n'est pas $\dot{\theta}$, x^p est la première puissance de x qui soit $\dot{\theta} + 1$. Donc,

d'après le théorème de Fermat, p est un diviseur de $\theta - 1$, et l'on a, par conséquent,

$$\theta \equiv 1 \pmod{p}. \quad \text{C. Q. F. D.}$$

La démonstration précédente est en défaut quand $x - 1 = \theta$; mais cela ne peut arriver que si $\theta = p$; en effet, on a identiquement

$$\begin{aligned} x^p - 1 &= (x - 1 + 1)^p - 1 \\ &= (x - 1)^p + \dots + \frac{p(p-1)}{1 \cdot 2} (x - 1)^2 + p(x - 1), \end{aligned}$$

et, par suite,

$$X = (x - 1)^{p-1} + \dots + \frac{p(p-1)}{1 \cdot 2} (x - 1) + p.$$

Ce qui montre que X et $x - 1$ ne peuvent avoir d'autre facteur commun que p , et même que X ne peut jamais être divisible par p^2 .