NOUVELLES ANNALES DE MATHÉMATIQUES

HERMITE

Un théorème de Fermat

Nouvelles annales de mathématiques 1re série, tome 12 (1853), p. 45-46

<http://www.numdam.org/item?id=NAM_1853_1_12__45_1>

UN THÉORÈME DE FERMAT;

D'APRÈS M. HERMITE.

(Journal de Mathematiques, tome XIII, page 15; 1848.)

1. *Lemme.* Lorsqu'un nombre premier est de la forme $\dot{4}+1$, il existe un carré qui, augmenté de 1, donne une somme divisible par ce nombre premier.

2. *Lemme.* Le nombre fractionnaire $\frac{a}{b}$ étant converti en fraction continue, on trouve toujours deux réduites consécutives dont les dénominateurs sont, l'un inférieur, et l'autre supérieur à $\sqrt{b}$.

3. THÉORÈME DE FERMAT. *Un nombre premier de la forme* $\dot{4}+1$ *est toujours la somme de deux carrés.*

Démonstration. Soit p ce nombre premier, on a donc (*lemme* 1)

$$a^2+1=\dot{p};$$

$\frac{a}{p}$ étant converti en fraction continue, on arrive à deux réduites consécutives $\frac{m}{n}$, $\frac{m'}{n'}$, où $n<\sqrt{p}$ et $n'>p$ (*lemme* 2). Donc, d'après la théorie connue,

$$\frac{a}{p}=\frac{m}{n}+\frac{\varepsilon}{nn'} \quad \text{où} \quad \varepsilon<1;$$

on en déduit

$$na-mp=\varepsilon.\frac{p}{n'},$$

$$(na-mp)^2=p.\frac{p}{n'^2}.\varepsilon^2;$$

$\frac{p}{n^2}$ et ε^2 sont des fractions; donc

$$(na - mp)^2 < p;$$

mais

$$n^2 < p;$$

donc

$$(na - mp)^2 + n^2 < 2p,$$

ou bien

$$n^2(a^2 + 1) - p(2anm - m^2p) < 2p.$$

$a^2 + 1$ est un multiple de p, l'expression à gauche est donc un multiple de p moindre que $2p$. Donc

$$(na - mp)^2 + n^2 = p. \qquad \text{C. Q. F. D.}$$

4. Euler a démontré que la décomposition du nombre premier $p = 4 + 1$ ne peut se faire que d'une seule manière (*voir* tome VII, page 38); et, d'après la formule de Gauss (*voir* tome IX, page 307), lorsqu'un nombre ne peut se décomposer que d'une seule manière en deux carrés, il est premier.