NOUVELLES ANNALES DE MATHÉMATIQUES

Théorème sur la somme de deux carrés ; d'après Euler

Nouvelles annales de mathématiques 1re série, tome 12 (1853), p. 46-47

<http://www.numdam.org/item?id=NAM_1853_1_12__46_1>

THÉORÈME SUR LA SOMME DE DEUX CARRÉS;

D'APRÈS EULER.

THÉORÈME. *$a^2 + b^2$ n'a aucun diviseur premier de la forme $4n - 1$, à moins que a et b aient un tel diviseur pour facteur commun.*

Démonstration. a et b n'étant pas divisibles par $4n - 1$, il s'ensuit (Fermat) que $a^{4n-2} - b^{4n-2}$ sera divisible par le nombre premier $4n - 1$; donc $a^{4n-2} + b^{4n-2}$ ne sera pas divisible par ce nombre premier. Mais $a^2 + b^2$ est un facteur de $a^{4n-2} + b^{4n-2}$; donc, etc. (*Correspondance mathématique et physique*, t. I, p. 116. Lettre à Goldbach, de Berlin, 6 mars 1742).

Dans la même Lettre, on trouve cette simple démonstration du théorème de Fermat.

1. *Lemme.* p étant un nombre premier, on a

$$(a+b)^p - a^p - b^p = \dot{p}. \tag{1}$$

2. *Lemme.* Si

$$a^p - a = \dot{p},$$

on aura aussi

$$(a+1)^p - (a+1) = \dot{p}.$$

Démonstration. Dans la congruence (1), faisons

$$b = 1,$$

il vient

$$(a+1)^p - a^p - 1 = \dot{p},$$

ou bien

$$(a+1)^p - (a+1) - (a^p - a) = \dot{p};$$

mais, par hypothèse,

$$a^p - a = \dot{p}.$$

Donc, etc.

3. Théorème de Fermat. p étant un nombre premier, on a

$$a^p - a = \dot{p}.$$

Démonstration. On a

$$1^p - 1 = \dot{p};$$

donc, d'après le lemme 2,

$$2^p - 2 = \dot{p}, \quad 3^p - 3 = \dot{p}, \quad \text{etc.}$$