NOUVELLES ANNALES DE MATHÉMATIQUES

M. CHALAUX

Tout nombre premier de la forme $4n + 1$ est une somme de deux carrés

Nouvelles annales de mathématiques 4^e série, tome 17 (1917), p. 305-308

<http://www.numdam.org/item?id=NAM_1917_4_17__305_0>

[19c]

TOUT NOMBRE PREMIER DE LA FORME $4n+1$ EST UNE SOMME DE DEUX CARRÉS ;

PAR M. M. CHALAUX,
Capitaine d'Artillerie.

1. On démontre souvent cette proposition célèbre en établissant tout d'abord le théorème suivant :

Tout diviseur d'une somme de deux carrés premiers entre eux est lui-même une somme de deux carrés.

Je vais montrer qu'il suffit de s'appuyer sur le lemme plus particulier que voici, dont la démonstration est plus simple :

Si un nombre premier, somme de deux carrés, divise une somme de deux carrés premiers entre eux, le quotient est lui-même une somme de deux carrés premiers entre eux.

Soient en effet $p = a^2 + b^2$ le nombre premier considéré, $A^2 + B^2$ la somme de deux carrés premiers entre eux qu'il divise, m le quotient

$$(1) \qquad pm = (a^2 + b^2)m = A^2 + B^2,$$

a et b étant évidemment premiers entre eux, l'équation indéterminée

$$ax + by = A$$

admet une infinité de solutions en nombres entiers

données par les formules

$$x = x_0 + b\lambda, \tag{2}$$

$$y = y_0 - a\lambda, \tag{3}$$

le couple (x_0, y_0) constituant une solution particulière, λ étant un entier arbitraire.

Posons

$$bx_0 - ay_0 = C_0,$$

$$bx - ay = C = C_0 + (a^2 + b^2)\lambda. \tag{4}$$

On a les identités

$$(a^2 + b^2)(x_0^2 + y_0^2) = A^2 + C_0^2, \tag{5}$$

$$(a^2 + b^2)(x^2 + y^2) = A^2 + C^2. \tag{6}$$

On tire de (1) et (5)

$$B^2 - C_0^2 = (B - C_0)(B + C_0) \equiv 0 \qquad [\mathrm{mod}\,(a^2 + b^2)];$$

$a^2 + b^2 = p$ étant premier divise donc au moins l'un des nombres $B - C_0$, $B + C_0$. Comme, dans l'égalité (1), B n'intervient que par son carré, on peut supposer que c'est $B - C_0$. Soit alors

$$B - C_0 = (a^2 + b^2)\mu,$$

μ étant entier. Si l'on fait dans les formules (2) et (3)

$$\lambda = \mu,$$

il vient, d'après (4),

$$C = B,$$

et, d'après (6),

$$\frac{A^2 + B^2}{a^2 + b^2} = x^2 + y^2.$$

D'autre part, x et y sont premiers entre eux, car un diviseur commun de ces nombres *diviserait* aussi A

et B, en vertu des égalités

$$ax + by = A, \qquad bx - ay = B,$$

et A et B sont supposés premiers entre eux. Le lemme est donc complètement établi.

2. Cela posé, le théorème sur les nombres premiers de la forme $4n + 1$ s'établit aisément, par une méthode de récurrence.

Tout d'abord, il résulte des éléments de la théorie des résidus quadratiques que tout nombre premier $4n + 1$ divise une somme de deux carrés premiers entre eux, et qu'au contraire un nombre premier $4n + 3$ ne divise jamais une pareille somme (cela revient à dire que -1 est résidu quadratique des nombres de la première forme, et non-résidu de ceux de la seconde).

Soit alors p un nombre premier $4n + 1$.

Supposons le théorème reconnu exact pour tous les nombres premiers de cette même forme, inférieurs à p. Je dis qu'il est vrai pour p.

En effet, p divise une somme de deux carrés premiers entre eux $A^2 + B^2$. On peut supposer

$$A < \frac{p}{2}, \qquad B < \frac{p}{2},$$

sans quoi l'on remplacerait A et B par leurs résidus (mod p), de valeur absolue minimum. Posons

$$pm = A^2 + B^2.$$

On a

$$m = \frac{A^2 + B^2}{p} < \frac{p}{2}.$$

m divisant une somme de deux carrés premiers entre eux ne peut avoir comme facteurs premiers que 2 (1) et des nombres de la forme $4n+1$, naturellement tous plus petits que p. Soit p' un de ces derniers. Posons

$$m = m'p',$$

d'où

$$pm'p' = A^2 + B^2.$$

Le nombre premier p' est, par hypothèse, somme de deux carrés. Par conséquent, et par application du lemme du n° 1, pm' est somme de deux carrés premiers entre eux.

Si m' contient encore un ou plusieurs facteurs premiers $4n+1$, on continuera de même et l'on parviendra finalement à ce résultat que p ou $2p$ est une somme de deux carrés. Le second résultat entraîne le premier, en vertu de l'identité

$$\frac{\alpha^2+\beta^2}{2} = \left(\frac{\alpha+\beta}{2}\right)^2 + \left(\frac{\alpha-\beta}{2}\right)^2.$$

3. On sait que Fermat affirmait posséder la démonstration du théorème. Dans le seul passage où il ait donné quelque idée de ces méthodes, il dit procéder par récurrence.

La démonstration donnée ici présente ce caractère. En outre, elle repose sur des considérations très simples et ne fait aucun appel, patent ou déguisé, à des théories telles que celle des fractions continues. Il n'est donc pas impossible qu'elle se rapproche de la démonstration originale de Fermat.

---

(1) A la première puissance seulement, car 2^2 ne pourrait diviser A^2+B^2 sans que A et B fussent tous les deux pairs, ce qui n'est pas, puisque ces nombres sont premiers entre eux.