NOUVELLES ANNALES DE MATHÉMATIQUES

S. RÉALIS

Scolies pour un théorème de Fermat

Nouvelles annales de mathématiques 3e série, tome 4 (1885), p. 367-372

<http://www.numdam.org/item?id=NAM_1885_3_4__367_1>

SCOLIES POUR UN THÉORÈME DE FERMAT;

Par M. S. RÉALIS,

Ingénieur à Turin.

Théorème. — *Si le nombre* p, *compris dans la forme linéaire* $4q+1$, *est premier, ou composé de facteurs premiers de cette forme,* p *est la somme de deux carrés.*

Dans la démonstration qu'il a donnée, le premier, de cet admirable théorème de Fermat (1), Euler a signalé

(1) *Voir* les *Nouveaux Commentaires de Pétersbourg,* t. IV, p. 3, et t. V, p. 3.

ce corollaire, que : *p étant comme il vient d'être dit, le nombre $q = \frac{p-1}{4}$ est la somme de deux nombres triangulaires* (dont l'un peut être nul).

En effet, dit Euler, le double de p est la somme de deux carrés impairs, et l'on peut poser

$$8q + 2 = (2a+1)^2 + (2b+1)^2,$$

ce qui donne

$$q = \frac{a^2+a}{2} + \frac{b^2+b}{2}.$$

A ces importantes propositions de Fermat et d'Euler on peut ajouter les remarques suivantes, qui leur servent de complément.

1° Un nombre donné $p = 4q + 1$ étant la somme de deux carrés x^2, y^2, on peut poser, en nombres entiers a, b, x, y,

$$a + b + 1 = x, \quad a - b = y,$$

et toutes les solutions entières de l'équation indéterminée

$$x^2 + y^2 = p$$

seront fournies par l'identité

$$(a+b+1)^2 + (a-b)^2 = 4\left(\frac{a^2+a}{2} + \frac{b^2+b}{2}\right) + 1,$$

c'est-à-dire

$$(a+b+1)^2 + (a-b)^2 = 2(a^2+a+b^2+b) + 1,$$

en attribuant à a et b des valeurs convenables (à savoir, des valeurs entières telles que le second membre de l'égalité se réduise à la valeur de p).

La détermination des deux carrés en lesquels se décompose p se trouve ainsi ramenée, d'une manière directe, à la détermination des deux nombres triangulaires en lesquels se décompose q.

Il est facile de voir que cela a lieu lors même que p

renfermerait des facteurs premiers de la forme $4q + 3$, pourvu que chaque facteur de cette espèce soit élevé à une puissance paire, et que p renferme au moins un facteur premier $4q + 1$ plus grand que l'unité. En ce cas, x et y ne seront plus premiers entre eux.

Pour $p = 45 = 3^2 . 5$, par exemple, on a, en prenant $a = 4$, $b = 1$,

$$6^2 + 3^2 = 4(10 + 1) + 1 = 45.$$

2° Si un nombre donné p, impair, ou double d'un impair, est décomposable en deux carrés premiers entre eux, en sorte que l'on ait

$$p = x^2 + y^2,$$

les racines x, y des carrés composants seront exprimées par le système de formules

$$x = p - \left(\frac{m^2 - m}{2} + \frac{n^2 - n}{2}\right),$$
$$y = p - \left(\frac{m^2 - m}{2} + \frac{n_2 + n}{2}\right),$$

m et n étant deux entiers convenablement déterminés.

Prenant, pour fixer les idées, les valeurs de x, y, m, n avec le signe positif, on énonce ce résultat avec plus de précision en disant que, dans les circonstances indiquées, *la racine $x > y$ est égale au nombre p, diminué de la somme de deux nombres triangulaires, et la racine y est égale au même nombre p, diminué de la somme de deux nombres triangulaires, dont l'un est égal au plus grand des triangulaires précédents, et l'autre est consécutif à l'autre triangulaire précédent.* A quoi il y a lieu d'ajouter que *les nombres m, n sont tous deux impairs, ou tous deux pairs, selon que p est lui-même impair, ou le double d'un impair.*

Exemples :

$$p = 5;\quad \begin{cases} m = 3, \\ n = 1; \end{cases} \quad \begin{cases} x = 5 - (3 + 0) = 2, \\ y = 5 - (3 + 1) = 1; \end{cases}$$

$$p = 10;\quad \begin{cases} m = 4, \\ n = 2; \end{cases} \quad \begin{cases} x = 10 - (6 + 1) = 3, \\ y = 10 - (6 + 3) = 1; \end{cases}$$

$$p = 13;\quad \begin{cases} m = 5, \\ n = 1; \end{cases} \quad \begin{cases} x = 13 - (10 + 0) = 3, \\ y = 13 - (10 + 1) = 2; \end{cases}$$

$$p = 17;\quad \begin{cases} m = 5, \\ n = 3; \end{cases} \quad \begin{cases} x = 17 - (10 + 3) = 4, \\ y = 17 - (10 + 6) = 1; \end{cases}$$

$$p = 25;\quad \begin{cases} m = 7, \\ n = 1; \end{cases} \quad \begin{cases} x = 25 - (21 + 0) = 4, \\ y = 25 - (21 + 1) = 3; \end{cases}$$

$$p = 26;\quad \begin{cases} m = 6, \\ n = 4; \end{cases} \quad \begin{cases} x = 26 - (15 + 6) = 5, \\ y = 26 - (15 + 10) = 1; \end{cases}$$

....

3° Soit p un nombre impair résultant de l'addition de deux carrés x^2, y^2, premiers entre eux.

On aura, en ajoutant $2x^2$ à la valeur de p,

$$p + 2x^2 = 3x^2 + y^2,$$

où le second membre, en y supposant y premier avec 3, représente un nombre appartenant à la forme linéaire $6u + 1$. Cela résulte d'un autre théorème de Fermat, démontré par Euler. La supposition de y premier avec 3 n'a ici rien d'arbitraire, vu que, x et y n'ayant pas de facteur commun, l'un de ces nombres peut toujours être supposé premier avec un nombre premier donné.

Nous pouvons donc poser

$$p + 2x^2 = 6u + 1,$$

c'est-à-dire

$$x^2 = 3u - \tfrac{1}{2}(p - 1),$$

et nous conclurons de là ce corollaire, que : *selon que le nombre considéré p, diminué de l'unité, est ou n'est pas divisible par 3, l'un des carrés en lesquels se décompose p est ou n'est pas divisible par 9.*

L'utilité de cette proposition est évidente, lorsqu'on se propose de déterminer, par des essais successifs, les deux carrés dont la somme doit former le nombre considéré.

4° Il est visible que des remarques analogues à la précédente s'appliqueront utilement, en certains cas, à des nombres que l'on sait être décomposables en carrés selon des formes quadratiques autres que celle dont il vient d'être question.

Qu'il s'agisse, par exemple, de satisfaire à l'équation indéterminée

$$p = 2x^2 + y^2$$

par des valeurs de x et y premières entre elles, p étant un nombre donné, dont tous les facteurs premiers sont de la forme $8q + 1$. L'équation est toujours possible, comme on sait, et y sera nécessairement un nombre impair, x un nombre pair.

Pour assigner une condition qui assujettisse d'une manière plus spéciale la valeur de x, mettons la proposée sous la forme

$$p + x^2 = 3x^2 + y^2.$$

Nous en inférerons, en supposant y premier avec 3, l'existence d'une relation telle que

$$p + x^2 = 6u + 1,$$

c'est-à-dire

$$x^2 = 6u - (p - 1),$$

d'où nous conclurons sur-le-champ que x admettra ou n'admettra pas le diviseur 3, selon que $p - 1$ admet ou n'admet pas ce diviseur.

Nous avons supposé y premier avec 3; quand il en est autrement, x est nécessairement premier avec 3.

Soit pris, comme application,

$$p = 2689 = 8.336 + 1.$$

Le nombre $p - 1$ étant divisible par 3, et x devant être un multiple pair de 3, les valeurs de x à essayer, pour opérer la décomposition demandée, devront être prises dans la suite 6, 12, 18,...; d'après cela, on reconnaîtra aussitôt que la valeur $x = 12$, à laquelle correspond $y = 49$, satisfait à la question. On a, en effet,

$$2689 = 2.12^2 + 49^2.$$

Le nombre p ainsi décomposé étant premier, on est assuré qu'il n'y a pas d'autre solution.

Les nombres $p = 8q + 1$ que nous venons de considérer appartiennent, comme cas particuliers, à la classe des nombres $4q + 1$ dont il a été question plus haut; ils admettent par conséquent, en même temps que la représentation par la forme $2x^2 + y^2$, la représentation par la forme $x^2 + y^2$. C'est ainsi que, pour $p = 2689$, on a, outre l'égalité déjà écrite, l'égalité

$$2689 = 40^2 + 33^2,$$

à laquelle sont applicables les remarques exposées précédemment.