NOUVELLES ANNALES DE MATHÉMATIQUES

S. RÉALIS

Développements nouveaux sur quelques propositions de Fermat

Nouvelles annales de mathématiques 3e série, tome 5 (1886), p. 113-122

<http://www.numdam.org/item?id=NAM_1886_3_5__113_0>

DÉVELOPPEMENTS NOUVEAUX SUR QUELQUES PROPOSITIONS DE FERMAT;

PAR M. S. RÉALIS,
Ingénieur à Turin.

1. On sait, d'après un théorème de Fermat, démontré par Euler, que : *si le nombre p, compris dans la forme linéaire $8q+1$, est premier, ou composé de facteurs premiers de cette forme, p est la somme d'un carré et d'un double carré.* En d'autres termes, on sait que, p étant comme il vient d'être dit, on peut toujours satisfaire, par des valeurs entières de x et y, à l'équation indéterminée

$$(1) \qquad 2x^2 + y^2 = p.$$

Un corollaire, que nous allons d'abord ajouter à cette importante proposition, consiste en ce que : *un nombre donné $p = 8q+1$ étant la somme d'un carré et d'un double carré premiers entre eux, le nombre*

$$3q = \frac{3(p-1)}{8}$$

est la somme d'un nombre triangulaire et du double d'un nombre triangulaire.

Pour démontrer cette propriété, nous poserons d'abord l'identité

$$3(2x^2+y^2) = 2(x+y)^2 + (y-2x)^2,$$

où il y a lieu d'observer que, l'équation (1) étant vérifiée, x est nécessairement un nombre pair, et y un nombre impair. Nous pouvons donc poser une relation telle que

$$3(8q + 1) = 2(2a + 1)^2 + (2b + 1)^2,$$

où a et b sont entiers, et d'où résulte l'égalité

$$3q = 2 \cdot \frac{a^2 - a}{2} + \frac{b^2 - b}{2},$$

constituant la propriété énoncée.

On aura ainsi

$$p = \frac{8}{3}\left(a^2 - a + \frac{b^2 - b}{2}\right) - 1,$$

a et b étant tels que l'expression de q, et conséquemment celle de p, se réduisent à des nombres entiers.

Des relations

$$y + x = 2a + 1, \qquad y - 2x = 2b + 1,$$

subsistant entre les entiers a, b, x, y, on déduit

$$x = \tfrac{2}{3}(a - b), \qquad y = \tfrac{2}{3}(2a + b) + 1,$$

d'où, par identité,

$$2x^2 - y^2 = \frac{8}{3}\left(a^2 - a - \frac{b^2 - b}{2}\right) + 1.$$

On conclut de là que toutes les solutions entières de l'équation (1) sont renfermées dans la formule

$$(2)\quad \left\{ \begin{aligned} & 2\left(\frac{2a - 2b}{3}\right)^2 - \left(\frac{4a + 2b + 3}{3}\right)^2 \\ & = \frac{8}{3}\left(a^2 - a + \frac{b^2 + b}{2}\right) + 1, \end{aligned} \right.$$

où l'on attribuera à a et b des valeurs entières telles que son second membre se réduise à la valeur de p (ce qui est toujours possible, d'après ce qui précède). La recherche de a et b se trouvera d'ailleurs quelque peu facilitée par la considération que, x et y devant être entiers, les valeurs numériques de $a - b$ et de $2a + b$ doivent être divisibles par 3.

La détermination du carré et du double carré en lesquels se décompose p se trouve ainsi ramenée directement à celle du nombre triangulaire et du double triangulaire en lesquels se décompose le nombre plus petit $3q$.

On reconnait facilement que cela ne cessera pas d'avoir lieu si, parmi les facteurs premiers de p, il s'en trouve qui soient compris dans l'une quelconque des formes $8q - 1$, $8q \pm 3$, pourvu que chaque facteur de cette espèce soit affecté d'un exposant pair, et que p renferme au moins un facteur premier $8q + 1$ plus grand que l'unité. En ce cas, x et y ne seront plus premiers entre eux.

Pour $p = 3^2.17 = 153$, par exemple, on a, en faisant $a = 1$, $b = 10$ dans la formule (2),

$$2.6^2 + 9^2 = \tfrac{8}{3}(2.1 + 55) + 1 = 8.19 + 1 = 153,$$

Pour $p = 7^2.73 = 3577$, on a

$$2.42^2 + 7^2 = \tfrac{8}{3}(2.28 + 3403) + 1 = 8\ 447 + 1 = 3577.$$

ce qui correspond au cas de $a = -18$, $b = 45$, dans la formule (2).

Pour $p = 3^2.5^2.41 = 9225$, on a

$$2.60^2 + 45^2 = \tfrac{8}{3}(2.28 + 3403) + 1 = 8.1153 + 1 = 9225,$$

ce qui correspond au cas de $a = 8$, $b = 82$.

2. Un théorème de Fermat, démontré par Lagrange, établit que : *tout nombre premier, compris dans la forme* $8q + 3$, *est la somme d'un carré et d'un double carré.*

Ce théorème, d'après les principes connus, s'étend à tout nombre p de la forme $8q+3$, composé d'un nombre impair de facteurs premiers de cette forme, et d'un nombre quelconque de facteurs premiers $8q+1$.

D'après cela, l'équation indéterminée

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

où p est tel qu'il vient d'être dit, est toujours résoluble en nombres entiers impairs $x=2a+1$, $y=2b+1$, et peut être représentée par l'identité

$$2(2a+1)^2+(2b+1)^2=8\left(a^2+a+\frac{b^2+b}{2}\right)+3.$$

On voit que le nombre $q=\frac{p-3}{8}$ est ici la somme d'un triangulaire et d'un double triangulaire, et que toutes les solutions entières de l'équation considérée sont renfermées dans l'identité que nous venons d'écrire, moyennant des valeurs convenables des indéterminées a et b.

Nous ne devons pas omettre d'ajouter que la précédente décomposition de q en nombres triangulaires avait été signalée incidemment par Euler, qui l'énonce comme une condition nécessaire (mais non suffisante) pour que $8q+3$ soit un nombre premier ([1]).

3. Dans un précédent article, où il était question des nombres qui sont la somme de deux carrés, nous avons fait connaître une importante propriété de ces nombres, par laquelle la racine de chacun des carrés composants s'exprime par la différence entre le nombre considéré et un nombre qui est la somme de deux triangulaires ([2]).

([1]) Voir les *Nouveaux Commentaires de Petersbourg*, t. VII, p. 229.

([2]) Voir les *Nouvelles Annales de Mathématiques*, p. 369; 1883.

Nous allons signaler ici une propriété analogue, relative aux nombres p considérés dans les nos 1 et 2 qui précèdent.

Cette propriété consiste en ce que : *si un nombre p, impair, ou double d'un impair, est décomposable en un carré et un double carré, en sorte que l'on ait*

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

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

$$x = p - \frac{1}{3}\left[m(m+1) + \frac{2n(2n-1)}{2}\right],$$
$$y = p - \frac{2}{3}\left[\frac{m(m+1)}{2} + n(n+1)\right],$$

m et n étant deux entiers convenablement déterminés.

La vérification est facile, et nous laisserons au lecteur le soin de développer les calculs relatifs. Pour plus de simplicité, et puisque c'est le cas qu'il importe surtout de considérer, on peut admettre que x et y sont premiers entre eux; mais on reconnaîtra sans peine que cette restriction n'est pas nécessaire.

Exemples :

$$\begin{array}{lll}
p = 8.1 - 3 = 11; & \left\{\begin{array}{l} m = 4, \\ n = -2; \end{array}\right. & \left\{\begin{array}{l} x = 11 - \frac{1}{3}(20 + 10) = 1, \\ y = 11 - \frac{2}{3}(10 + 2) = 3; \end{array}\right. \\
p = 8.2 + 1 = 17; & \left\{\begin{array}{l} m = 6, \\ n = -1; \end{array}\right. & \left\{\begin{array}{l} x = 17 - \frac{1}{3}(42 + 3) = 2, \\ y = 17 - \frac{2}{3}(21 + 0) = 3; \end{array}\right. \\
p = 8.2 + 3 = 19; & \left\{\begin{array}{l} m = 6, \\ n = 2; \end{array}\right. & \left\{\begin{array}{l} x = 19 - \frac{1}{3}(42 + 6) = 3, \\ y = 19 - \frac{2}{3}(21 + 6) = 1. \end{array}\right. \\
p = 2.11 = 22; & \left\{\begin{array}{l} m = 7, \\ n = 1; \end{array}\right. & \left\{\begin{array}{l} x = 22 - \frac{1}{3}(56 + 1) = 3, \\ y = 22 - \frac{2}{3}(28 + 2) = 2, \end{array}\right. \\
p = 8.4 + 1 = 33; & \left\{\begin{array}{l} m = 8, \\ n = -3; \end{array}\right. & \left\{\begin{array}{l} x = 33 - \frac{1}{3}(72 + 21) = 2, \\ y = 33 - \frac{2}{3}(36 + 6) = 5; \end{array}\right.
\end{array}$$

$$p = 2.17 = 34; \quad \begin{cases} m = 9, \\ n = -1; \end{cases} \quad \begin{cases} x = 34 - \frac{1}{3}(90 + 3) = 3, \\ y = 34 - \frac{2}{3}(45 + 0) = 4; \end{cases}$$

$$p = 2.19 = 38; \quad \begin{cases} m = 7, \\ n = -5; \end{cases} \quad \begin{cases} x = 38 - \frac{1}{3}(56 + 55) = 1, \\ y = 38 - \frac{2}{3}(28 + 20) = 6; \end{cases}$$

. . . .

4. D'après un théorème de Fermat, démontré par Euler, on peut affirmer que : *si un nombre donné p, compris dans la forme linéaire $6q+1$, est premier, ou composé de facteurs premiers de cette forme, ce nombre est la somme d'un carré et d'un triple carré.*

Un corollaire qu'il y a lieu d'ajouter à cette proposition consiste en ce que : *p étant comme il vient d'être dit, le nombre $3q = \frac{p-1}{2}$ est la somme d'un triangulaire et d'un triple triangulaire.*

Soit, en effet, l'équation

$$(3) \qquad 3x^2 + y^2 = p,$$

subsistant, pour $p = 6q + 1$, en nombres entiers x, y, premiers entre eux; ces nombres seront nécessairement de différente parité, et y sera premier avec 3.

Posons l'identité

$$4(3x^2 + y^2) = 3(x + y)^2 + (3x - y)^2;$$

nous en conclurons aussitôt l'existence d'une relation telle que

$$4(6q + 1) = 3(2a + 1)^2 + (2b + 1)^2,$$

pour des valeurs entières de a et b, et nous obtiendrons

$$3q = 3\,\frac{a^2 + a}{2} + \frac{b^2 + b}{2},$$

ce qui démontre la propriété énoncée.

Il y a lieu de remarquer ici que le nombre triangulaire

$\frac{b^2+b}{2}$, qui entre dans l'expression de $3q$, doit être un multiple de 3; on a ainsi une condition propre à faciliter la décomposition de $3q$ en nombres triangulaires, et, par suite, la décomposition de p en carrés, selon l'équation (3). Cette condition, au reste, revient à ce que nous avons déjà remarqué, c'est-à-dire que y doit être premier avec 3.

Les égalités

$$x+y=2a+1, \qquad 3x-y=2b+1$$

donnent

$$x=\frac{a+b+1}{2}, \qquad y=\frac{3a-b+1}{2},$$

où a et b seront de différente parité (ce qui constitue une nouvelle condition propre à simplifier la recherche des nombres triangulaires en lesquels se décompose $3q$). Par ces expressions de x et y, l'équation (3) se trouve transformée en l'identité

$$3\left(\frac{a+b+1}{2}\right)^2+\left(\frac{3a-b-1}{2}\right)^2=6\left(\frac{a^2+a}{2}+\frac{1}{3}\cdot\frac{b^2+b}{2}\right)+1,$$

c'est-à-dire

$$(4)\qquad \left\{\begin{aligned} &3\left(\frac{a+b+1}{2}\right)^2+\left(\frac{3a-b+1}{2}\right)^2\\ &\quad=3(a^2+a)+b^2+b+1.\end{aligned}\right.$$

On voit par là que le nombre considéré $p=6q+1$ peut toujours être représenté par la forme indiquée par le second membre de cette identité, où l'on sait que a et b sont de différente parité, et que b^2+b est divisible par 3. Il en résulte que toutes les solutions entières de l'équation (3) rentreront dans l'identité (4), où l'on pourra toujours assigner à a et b des valeurs entières propres à identifier son second membre avec la valeur donnée de p.

Il est aisé de voir que ce qui précède continue d'avoir lieu lorsque p renferme des facteurs de la forme $6q - 1$, pourvu que chaque facteur premier de cette forme s'y trouve élevé à une puissance paire, et que p renferme au moins un facteur premier $6q + 1$ plus grand que l'unité. En ce cas, x^2 et y^2 auront pour diviseur commun un carré qui sera également diviseur de p.

C'est ainsi que, pour $p = 5^2.13 = 325$, on a

$$3.10^2 + 5^2 = 6\left(28 + \frac{78}{3}\right) + 1 = 3.56 + 156 + 1 = 325,$$

ce qui correspond à l'hypothèse de $a = 7$, $b = 12$, dans la formule (4).

On remarquera encore que la transformation de l'équation (3) en l'égalité (4) continue de subsister si, au lieu du nombre considéré p, on prend son triple, c'est-à-dire le nombre $3(6q + 1)$; cela tient à ce que le facteur 3, quoique non compris dans la forme linéaire $6q + 1$, n'en appartient pas moins à la forme quadratique $3x^2 + y^2$. En ce cas, le nombre $b^2 + b$ ne sera plus divisible par 3.

On a, par exemple, pour $p = 3.19 = 57$,

$$3.4^2 + 3^2 = 3.12 + 20 + 1 = 57,$$

ce qui répond aux valeurs $a = 3$, $b = 4$, dans la formule (4).

5. Il nous reste à signaler, à l'égard de l'équation (3), la propriété remarquable dont jouissent les racines x, y, de pouvoir s'exprimer très simplement par la différence entre p et une fonction linéaire déterminée de certains nombres triangulaires.

Cette propriété, analogue à celle que nous avons constatée plus haut à l'égard de l'équation (1), se rattache, de même que celle-ci, à un fait général sur lequel nous ne nous arrêterons pas en ce moment. Elle consiste en ce que : *si un nombre p, impair, ou quadruple d'un impair, est décomposable en un carré et un triple carré, en sorte que l'on ait*

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

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

$$x = p - \frac{1}{2}\left[\frac{m(m+1)}{2} + \frac{1}{3}\,\frac{3n(3n-1)}{2}\right],$$

$$y = p - \frac{1}{2}\left[\frac{m(m+1)}{2} + 3\,\frac{n(n+1)}{2}\right],$$

à l'aide de valeurs entières convenables attribuées à m et n.

La vérification ne présente pas de difficulté.

Exemples :

$$p = 4;\quad \begin{cases} m = 3, \\ n = 0; \end{cases} \quad \begin{cases} x = 4 - \frac{1}{2}(6 + 0) = 1, \\ y = 4 - \frac{1}{2}(6 + 0) = 1; \end{cases}$$

$$p = 7;\quad \begin{cases} m = 4, \\ n = -1; \end{cases} \quad \begin{cases} x = 7 - \frac{1}{2}(10 + \frac{6}{3}) = 1, \\ y = 7 - \frac{1}{2}(10 + 0) = 2; \end{cases}$$

$$p = 12;\quad \begin{cases} m = 5, \\ n = -2; \end{cases} \quad \begin{cases} x = 12 - \frac{1}{2}(15 + \frac{21}{3}) = 1, \\ y = 12 - \frac{1}{2}(15 + 3.1) = 3; \end{cases}$$

$$p = 13;\quad \begin{cases} m = 6, \\ n = 1; \end{cases} \quad \begin{cases} x = 13 - \frac{1}{2}(21 + \frac{3}{3}) = 2, \\ y = 13 - \frac{1}{2}(21 + 3.1) = 1; \end{cases}$$

$$p = 19;\quad \begin{cases} m = 6, \\ n = -3; \end{cases} \quad \begin{cases} x = 19 - \frac{1}{2}(21 + \frac{45}{3}) = 1, \\ y = 19 - \frac{1}{2}(21 + 3.3) = 4; \end{cases}$$

$$p = 21;\quad \begin{cases} m = 8, \\ n = -1; \end{cases} \quad \begin{cases} x = 21 - \frac{1}{2}(36 + \frac{6}{3}) = 2, \\ y = 21 - \frac{1}{2}(36 + 0) = 3; \end{cases}$$

$$p = 28;\quad \begin{cases} m = 7, \\ n = -4; \end{cases} \quad \begin{cases} x = 28 - \frac{1}{2}(28 + \frac{78}{3}) = 1, \\ y = 28 - \frac{1}{2}(28 + 3.6) = 5. \end{cases}$$

. . . .

Note. — Les propriétés qui viennent d'être considérées à l'égard des équations (1) et (3), et celles qui font l'objet de l'article cité au n° 3, pouvant trouver quelques applications utiles dans la théorie des nombres, nous pourrons y revenir en étendant la question.