Nouvelles annales de mathématiques

Ad. Guibert

Sur trois carrés, lorsqu'ils sont en progression arithmétique

Nouvelles annales de mathématiques 2^e série, tome 1 (1862), p. 213-219
<http://www.numdam.org/item?id=NAM_1862_2_1__213_1>

SUR TROIS CARRÉS, LORSQU'ILS SONT EN PROGRESSION ARITHMÉTIQUE;

PAR M. AD. GUIBERT.

Il y a une infinité de systèmes de trois carrés qui peuvent être en progression arithmétique; nous présentons, dans ce qui suit, quelques propriétés concernant ces nombres et les progressions auxquelles ils appartiennent.

I. — *Si trois carrés sont en progression arithmétique, leur différence est un multiple de* $2^3 \times 3$.

En divisant ces carrés par le plus grand commun diviseur de deux quelconques d'entre eux, on obtient trois carrés a^2, b^2, c^2 en progression arithmétique; l'égalité $a^2 + c^2 = 2b^2$ prouve qu'ils sont premiers entre eux, deux à deux, de la forme $8k + 1$, et aussi de la forme $3k' + 1$; leur différence $b^2 - a^2$ est donc divisible par $2^3 \times 3$.

Voici des exemples :

$$(127)^2,\ (145)^2,\ (161)^2,\quad b^2 - a^2 = 2^3 \times 3^2 \times 17,$$
$$(161)^2,\ (229)^2,\ (281)^2,\quad b^2 - a^2 = 2^3 \times 3 \times 5 \times 13 \times 17,$$
$$(271)^2,\ (409)^2,\ (511)^2,\quad b^2 - a^2 = 2^4 \times 3 \times 5 \times 17 \times 23.$$
$$(433)^2,\ (533)^2,\ (617)^2,\quad b^2 - a^2 = 2^3 \times 3 \times 5^2 \times 7 \times 23.$$

II. — *Les carrés* a^2, b^2, c^2, *premiers entre eux, étant en progression arithmétique, la raison sera divisible par* 5, *si le second carré n'est pas divisible par* 5; *et elle* *sera divisible par 7, si aucun des carrés extrêmes n'est un multiple de 7.*

En considérant les résidus quadratiques minima des modules 5 et 7, et l'égalité $a^2 + c^2 = 2b^2$, on voit que si l'un des nombres a, b, c est divisible par 5, ce doit être b; que si l'un d'eux est multiple de 7, ce ne peut être que a ou c.

Supposons b non multiple de 5, l'égalité précédente exige que les résidus quadratiques minima du module 5, relatifs aux carrés a^2, b^2, c^2, soient égaux; la raison est donc un multiple de 5.

De même, si aucun des nombres a, c n'est divisible par 7, l'égalité $a^2 + c^2 = 2b^2$ ne se vérifie que lorsque la raison est un multiple de 7.

Exemples :

$$1,\ (29)^2,\ (41)^3,\ b^2 - a^2 = 2^3 \times 3 \times 5 \times 7,$$
$$(23)^2,\ (37)^2,\ (47)^2,\ b^2 - a^2 = 2^3 \times 3 \times 5 \times 7,$$
$$(17)^2,\ (53)^2,\ (73)^2,\ b^2 - a^2 = 2^3 \times 3^2 \times 5 \times 7.$$

III. — *Lorsque trois nombres premiers, dont 7 ne fait point partie, ont leurs carrés en progression arithmétique, la raison est toujours un multiple de* $2^3 \times 3 \times 5 \times 7$.

Cette proposition découle de la précédente, en observant que $(7)^2$ n'étant point, par hypothèse, un des trois termes de la progression, $(5)^2$ n'est pas non plus un de ces termes; car les carrés 1, $(5)^2$, $(7)^2$ forment l'unique progression arithmétique entre les carrés de trois nombres premiers dont l'un est 5, et ces carrés sont exclus, d'après l'énoncé. La raison sera donc divisible par 5×7.

IV. — *Si les trois nombres a, b, c, premiers entre eux, ont leurs carrés en progression arithmétique, chacun des nombres a, c est de l'une des formes* $8k + 1$, $8k + 7$, *b est de l'une des formes* $8k + 1$, $8k + 5$.

Par la résolution de l'équation indéterminée

$$a^2 + c^2 = 2b^2,$$

on trouve les valeurs générales des nombres positifs a, b, c; on parvient aux formules

$$\begin{aligned}
a &= p^2 - q^2 - 2pq \quad \text{pour} \quad p^2 > q^2 + 2pq,\\
a &= q^2 + 2pq - p^2, \quad \text{pour} \quad p^2 < q^2 + 2pq,\\
b &= p^2 + q^2,\\
c &= p^2 - q^2 + 2pq;
\end{aligned}$$

p et q sont deux entiers arbitraires premiers entre eux, l'un pair, l'autre impair; et comme nous supposons $a < b < c$ et que $b^2 - a^2 = 4pq(p^2 - q^2)$, p est plus grand que q; ces deux nombres peuvent toujours être pris positifs.

Or, quand $p^2 - q^2 - 2pq$ est positif,

$$a = p^2 - q^2 - 2pq = (p-q)^2 - 2q^2;$$

lorsque $p^2 - q^2 - 2pq$ est négatif,

$$a = q^2 + 2pq - p^2 = (p - 3q)^2 - 2(p - 2q)^2;$$

d'ailleurs

$$c = p^2 - q^2 + 2pq = (p+q)^2 - 2q^2;$$

a et c, de la forme $x^2 - 2y^2$, sont donc chacun de l'une des formes $8k + 1$, $8k + 7$, puisque y peut être pair ou impair.

Quant à $b = p^2 + q^2$, il est manifestement de l'une des formes $8k + 1$, $8k + 5$.

V. — *Il n'y a que deux progressions arithmétiques dont trois termes consécutifs sont des carrés, si la raison est égale à* $2^3 \times 3 \times 5 \times 7$.

Il suffit de considérer le cas où les trois carrés sont premiers entre eux.

La proposition se justifie par la résolution de l'équation

$$pq(p-q)(p+q)=2\times3\times5\times7,$$

où les facteurs $p, q, p-q, p+q$ du premier membre sont premiers entre eux deux à deux.

Lorsque q est pair, cette équation est résolue en prenant $q=2, p=5$; elle n'admet aucune autre solution : de là, les trois carrés en progression arithmétique

$$1,\ (29)^2,\ (41)^2.$$

q étant impair, l'équation n'est résolue que par $q=1$, $p=6$, ce qui donne les trois carrés

$$(23)^2,\ (37)^2,\ (47)^2.$$

Il est à remarquer que $1, (29)^2, (41)^2$ sont les carrés de trois nombres premiers, ainsi que $(23)^2, (37)^2, (47)^2$.

VI. — *Si l'on prolonge au delà du troisième carré la progression arithmétique dont les trois premiers termes, premiers entre eux, sont* a^2, b^2, c^2, *le* $n^{ième}$ *terme sera un carré,* 1° *quand on prendra* $q=1$, $2p=n-2$; 2° *lorsqu'on fera* $q=2$, $p=n-2$.

Le $n^{ième}$ terme est représenté généralement par

$$(p^2+q^2)^2+4(n-2)pq(p^2-q^2);$$

il est identiquement égal à

$$[p^2+2(n-2]qp-(2n^2-8n+7)q^2]^2$$
$$+4(n-1)(n-2)(n-3)[2p-(n-2)q]q^3;$$

sous cette forme, on voit qu'il se réduit à un carré, si $2p-(n-2)q=0$, ce qui donne, pour p et q, seulement les valeurs spécifiées dans l'énoncé.

Voici le tableau des progressions dont il s'agit :

$q=1$;

$p=2$, 1, $(5)^2$, $(7)^2,\ldots$, le 6^e^ terme est $(11)^2$,

$p=4$, $(7)^2$, $(17)^2$; $(23)^2,\ldots$, le 10^e^ terme est $(47)^2$,

$p=6$, $(23)^2$, $(37)^2$, $(47)^2,\ldots$, le 14^e^ terme est $(107)^2$,

$p=8$, $(47)^2$, $(65)^2$, $(79)^2,\ldots$, le 18^e^ terme est $(191)^2$,

....

$q=2$;

$p=3$, $(7)^3$, $(13)^2$, $(17)^2,\ldots$, le 5^e^ terme est $(23)^2$,

$p=5$, 1, $(29)^2$, $(41)^2,\ldots$, le 7^e^ terme est $(71)^2$,

$p=7$, $(17)^2$, $(53)^2$, $(73)^2,\ldots$, le 9^e^ terme est $(143)^2$,

$p=9$, $(41)^2$, $(85)^2$, $(113)^2,\ldots$, le 11^e^ terme est $(239)^2$,

....

Lorsque $q=1$, le troisième terme de chaque progression est égal au premier terme de la progression suivante; quand $q=2$, il en est de même des progressions dont les rangs sont impairs et de celles où les rangs sont pairs.

Nous allons donner l'explication de ces particularités, en indiquant comment, pour une même valeur de q, arbitraire d'ailleurs, on peut former autant de séries que l'on voudra de progressions arithmétiques de trois carrés premiers entre eux, telles que dans chaque série le troisième terme d'une progression quelconque soit toujours égal au premier terme de la progression suivante :

L'expression de la condition dont il s'agit est

$$[(p+q)^2-2q^2]=[(p'-q)^2-2q^2]^2;$$

on en déduit

$$p'=p+2q.$$

D'après cela, on formera la première série résultant de la plus petite valeur de p, qui est $q+1$, en prenant les valeurs générales des carrés a^2, b^2, c^2, et y faisant successivement

$$p = q+1, \quad 3q+1, \quad 5q+1, \quad \text{etc.}$$

La seconde série dépendra du plus petit nombre s, premier avec q, mais plus grand que $q+1$; les valeurs successives de p seront

$$s, \quad s+2q, \quad s+3q, \quad \text{etc.}$$

Ainsi de suite.

Les termes signalés comme des carrés, au delà des troisièmes termes, dans les progressions relatives à $q=1$ et à $q=2$, donnent encore lieu à une remarque.

Dans toute progression arithmétique, si un terme est un carré u^2, on peut trouver une infinité de termes qui sont des carrés, il suffit de poser

$$u^2 + nr = (u + r\varphi)^2,$$

u^2 étant le premier terme, $n+1$ désigne le rang du terme qui doit être un carré, r la raison de la progression, φ un entier positif arbitraire ; il vient, en effet,

$$n = 2u\varphi + r\varphi^2.$$

Mais, et c'est l'observation que nous nous proposions de faire, si l'on voulait employer ce moyen pour obtenir les termes carrés dont on a parlé, placés au delà des troisièmes termes des progressions, φ devrait être fractionnaire et même pourrait être négatif ; c'est ce qu'il s'agit de justifier.

En partant du carré $(p^2+q^2)^2$, on prendra pour le n^{ieme} terme, dans chaque progression du tableau ci-dessus.

$$(p^2 + q^2)^2 + (n-2)r = (p^2 + q^2 + r\varphi)^2,$$

d'où

$$n - 2 = 2(p^2 + q^2)\varphi + r\varphi^2;$$

or, cette équation devient identique : 1° quand $q = 1$, $2p = n - 2$, φ étant égal, soit à $\frac{1}{2p}$, soit à $\frac{-p}{p^2 - 1}$; 2° lorsque $q = 2$, $p = n - 2$ et $\varphi = \frac{1}{4p}$, ou $\varphi = \frac{-p}{2(p^2 - 4)}$.