Echanges

Réponse à un avis de recherche (n°51)

Jean BRETTE
Palais de la Découverte - Paris

Avis de recherche n°51 (Pierre Barnouin - Cabris)

...Demande l'aide des lecteurs au sujet de deux conjectures qu'il émet concernant les triplets d'entiers premiers entre eux mesurant les côtés d'un triangle dont un angle vaut 120° (qui sont donc solution de $x^2 + y^2 + xy = z^2$, comme (3, 5, 7) et (5, 16, 19).

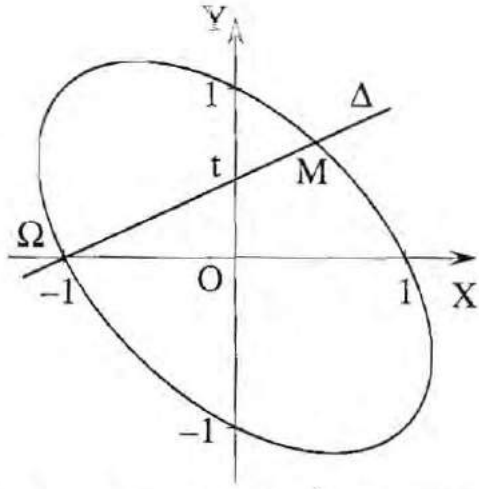
1) Tous les nombres impairs et tous les multiples de 8, et eux seulement, peuvent figurer dans ces triplets.

2) Le plus grand entier de chaque triplet est toujours congru à 1, 7, 13 ou 19 modulo 30.

1 - Des solutions rationnelles

Pour des équations de ce type, une méthode classique consiste à tout diviser par z^2, et à poser $X = x/z$ et $Y = y/z$. On est alors amené à chercher les points rationnels sur la conique (ici l'ellipse) d'équation :

$$X^2 + XY + Y^2 - 1 = 0 \qquad (1)$$



Il existe six points rationnels "évidents" sur cette ellipse : $(0, \pm 1)$, $(\pm 1, 0)$, $(-1, 1)$ et $(1, -1)$. Cherchons les autres.

Soit Ω le point $(-1, 0)$ et Δ une droite passant par Ω et un point $(0, t)$ de l'axe des Y. L'équation de cette droite est : $Y = t(1 + X)$ **(2)**

Elle coupe l'ellipse en Ω et en un point M dont les coordonnées s'obtiennent en substituant la valeur de Y de **(2)** dans **(1)**. On obtient :
$X^2(t^2 + t + 1) + X(2t^2 + t) + t^2 - 1 = 0$, dont le discriminant vaut $(t + 2)^2$.

Les coordonnées de M sont donc :

$$X = \frac{1 - t^2}{1 + t + t^2} \quad \text{et} \quad Y = \frac{t^2 + 2t}{1 + t + t^2} \qquad \textbf{(3)}$$

Ces formules, avec t rationnel, fournissent toutes les solutions rationnelles de **(1)**, sauf $(-1, 1)$.

En effet, si t est rationnel, alors X et Y aussi. Inversement, à chaque point rationnel M de l'ellipse, distinct de Ω et de $(-1, 1)$ correspond une unique valeur rationnelle de t, à savoir $t = Y/(1 + X)$, et $t = -2$ correspond au point Ω. On a donc une bijection entre les points rationnels de l'ellipse et les points rationnels de l'axe des y (...plus le point à l'infini qui correspond au point $(-1, 1)$.

Note 1 : En choisissant Ω et l'axe des Y plutôt que, par exemple, $(0, -1)$ et l'axe des X, on introduit une asymétrie dans le problème, que l'on retrouve bien sûr dans les formules **(3)**.

2 - Les solutions entières paramétriques de l'équation initiale

Comme on cherche les côtés d'un triangle, cela impose x, y et z positifs. Parmi les solutions de (**3**), on ne doit donc conserver que celles pour lesquelles X et Y sont simultanément positifs ou négatifs, c'est-à-dire les points rationnels du premier ou troisième cadran. Ces derniers étant symétriques des premiers par rapport à l'origine, on peut se limiter à X et Y positifs, ce qui correspond à $0 < t < 1$.

Soit donc $t = p/q$, avec $0 < p < q$ et pgcd$(p, q) = 1$. En substituant cette valeur de t dans (**3**), on obtient :

$$X = \frac{q^2 - p^2}{p^2 + pq + q^2} \quad \text{et} \quad Y = \frac{p^2 + 2pq}{p^2 + pq + q^2} \qquad (4)$$

d'où les solutions paramétriques du problème initial :

$$x = q^2 - p^2 \quad ; \quad y = p^2 + 2pq \quad \text{et} \quad z = p^2 + pq + q^2 \qquad (5)$$

Par exemple, les solutions mentionnées dans l'énoncé proviennent respectivement de $p = 1$; $q = 2$ et de $p = 2$; $q = 3$.

Note 2 : Le fait que p et q soient premiers entre eux n'implique pas que x, y, z le soient : par exemple, $p = 1$ et $q = 4$ conduisent aux valeurs 15, 9 et 21, qui sont toutes multiples de 3. Après division par 3, il leur corresppond la solution primitive (c'est-à-dire une solution où x, y et z sont premiers entre eux) : $(x', y', z') = (5, 3, 7)$. Il est donc intéressant de voir quels sont les diviseurs communs possibles. Il suffit d'ailleurs de regarder les diviseurs d communs à x et y puisque si d divise deux des termes, il divise aussi le troisième.

Si un nombre premier d divise $y = p(p + 2q)$, alors il divise p ou $p + 2q$. Il ne peut pas diviser p parce qu'il devrait diviser q pour diviser $x = q^2 - p^2$. Or, p et q sont premiers entre eux.

Supposons qu'il divise $p + 2q$. S'il divise aussi $q^2 - p^2$ alors il divise $(q + p)$ ou $(q - p)$. S'il divise $(p + q)$ alors il doit diviser la différence $(p + 2q) - (p + q) = q$. C'est impossible, car pour diviser $q^2 - p^2$, il devrait diviser p. Reste le cas où d divise $(p + 2q)$ et $(q - p)$. Dans ce cas, il doit diviser leur somme $3q$ et il ne peut pas diviser q pour les raisons vues ci-dessus.

Par conséquent, si x, y et z ont un diviseur commun, il est égal à 3. Dans ce cas, $(q - p)$ est un multiple de 3 et $p \equiv q \equiv 1$ ou $p \equiv q \equiv 2 \bmod 3$.

Les formules (**5**) donnent donc toutes les solutions primitives quand $(q - p)$ n'est pas multiple de 3. On les appellera solutions types S_1, notées (x, y, z).

Quand $(q-p)$ est un multiple de 3, les solutions primitives, dite de type S_3, sont données par :

$$x' = \frac{q^2 - p^2}{3} \quad , \quad y' = \frac{p^2 + 2pq}{3} \quad et \quad z' = \frac{p^2 + pq + q^2}{3} \qquad (5')$$

3 - Les multiples de 8

Tout d'abord, on vérifie aisément que z n'est jamais pair, ni *a fortiori* multiple de 8. Par conséquent, x ne sera multiple de 8 que si $q^2 - p^2$ l'est ; de même, y ne sera multiple de 8 que si $p^2 + 2pq$ l'est. (On n'a pas ici à se préoccuper de l'éventuelle division par 3 qui ne changerait de tooute façon rien à la divisibilité de x ou de y par 8 et on peut donc utiliser (**5**)).

3.1 x pair est-il nécessairement un multiple de 8 ?

Oui, puisque p et q sont premiers entre eux, ils ne sont pas tous les deux pairs et x ne peut donc être pair que si p et q sont impairs . Posons $p = 2p' + 1$ et $q = 2q' + 1$ et substituons-les dans (**5**). On obtient :

$$x = (q-p)(q+p) = 2(q'-p')2(q'+p'+1)$$

et on vérifie sans peine que l'expression $(q' - p')(q' + p' + 1)$ est paire quelles que soient les parités de p' et q'. Par conséquent, si x est pair, il est multiple de 8.

3.2 tout multiple positif de 8 peut-il être égal à x ?

Oui. Soit $x = 8m'$. Il suffit de prendre $p = 2m' - 1$ et $q = 2m' + 1$ pour vérifier que $x = q^2 - p^2 = 8m'$.

3.3 y pair est-il nécessairement un multiple de 8 ?

Oui, puisque l'équation initiale est symétrique en x et en y. On peut également le voir directement dans (**5**) : puisque p et q sont premiers entre eux, $y = p^2 + 2pq$ ne peut être pair que si p est pair et q est impair. Posons $p = 2p'$ et $q = 2q' + 1$ et substituons ces valeurs dans (**5**). Il vient :

$$y = p(p + 2q) = 2p'(2p' + 4q' + 2) = 4p'(p' + 2q' + 1)$$

et, là encore, on vérifie que l'expression $p'(p' + 2q' + 1)$ est paire quelles que soient les parités de p' et q'.

3.4 tout multiple positif de 8 peut-il être égal à y ?

Oui, à l'exception de 8. Soit $y = 8m'$, avec $m' > 1$. Il suffit de prendre $P = 2$ et $q = 2m' - 1$ pour vérifier que $y = p^2 + 2pq = 4 + 8m' - 4 = 8m'$.

4 - Les nombres impairs

On doit ici distinguer les solutions de type S_1 de celles de type S_3.

4.1 Dans une solution de type S_1, x peut-il prendre n'importe quelle valeur impaire ?

Oui, à l'exception de $x = 1$. Soit $x = 2k + 1$. Il suffit de prendre $p = k$ et $q = k + 1$. D'après la note 2, comme $(q - p) = 1$, les solutions données par (**5**) sont primitives.

4.2 Dans une solution de type S_3, x' peut-il prendre n'importe quelle valeur impaire ?

Non. Il existe une infinité de valeurs impossibles. La suite de ces valeurs est formée de progressions arithmétiques de longueurs et de raisons croissantes. Les premières sont $x' = 1$, puis 3, 9, 15, 21, 27, puis 45, 63, 81, 99, 117, 135, 153, 171, 189, 207, 225, 243, puis 297, 351, etc.

Montrons par exemple que x' ne peut pas prendre la valeur 15.

Si x était égal à 15, $q^2 - p^2$, dans (**5**) vaudrait $3 \times 15 = 45$. Le nombre 45 admet trois expressions de la forme $q^2 - p^2$: $23^2 - 22^2$; $9^2 - 6^2$ et $7^2 - 2^2$ mais dans la seconde p et q sont multiples de 3 et dans les autres $(q - p)$ n'est pas multiple de 3 et les solutions correspondantes sont de type S_1 : de fait, pour ces deux dernières, on obtient respectivement : $(x, y, z) = (45, 1496, 1519)$ et $(45, 32, 67)$.

Nous étudierons plus loin (point 6) cette curieuse suite de valeurs impossibles. En effet, elles ne contredisent pas la conjecture de Pierre BARNOUIN, car il existe toujours une solution de type S_3 où le nombre y', lui, peut prendre n'importe quelle valeur impmaire, à l'exclusion de 1. Montrons-le.

Supposons que $y' = 2k + 1$. Dans ce cas, $p(p + 2q) = 3y' = 6k + 3$ et il suffit de prendre $p = 1$; $q = 3k + 1$ pour obtenir cette valeur. On a bien $(q - p)$ multiple de 3 et p et q premiers entre eux.

Exemple : on vient de voir qu'il n'existe pas de solution S_3 avec $x' = 15$, en voici une avec $y' = 15$: $3y' = 45 = 6k + 3$ donne $k = 7$ puis $p = 1$; $q = 22$ qui donnent dans (**5**) les numérateurs : 483, 45, 507 et après division par 3 : $(x', y', z') = (161, 15, 169)$.

Note 3 : Le fait que y' puisse prendre la valeur 15 et pas x' peut sembler paradoxal, dans la mesure où l'équation initiale est symétrique et x et en y. Cela provient du fait que l'échange de x et de y peut changer le type de la solution.

Voyons cela de plus près. Soit M un point de l'ellipse, de coordonnées (X, Y) et M' son symétrique par rapport à la première bissectrice, de coordonnées (Y, X). La valeur du paramètre t' associé à M' sera $t' = \dfrac{X}{1 + Y}$. En

remplaçant X et Y par leurs valeurs données par (3), on obtient : $t' = \dfrac{1-t}{1+2t}$,

et si t est rationnel, p/q, alors $t' = \dfrac{q-p}{q+2p} = \dfrac{p'}{q'}$.

On voit alors que si $q \equiv p \bmod 3$, alors p' et q' sont multiples de 3. Par exemple, $p = 1$; $q = 13$ (de type S_3) conduit aux valeurs $p' = 12$; $q' = 15$. Ces valeurs correspondent au même point M' que $p' = 4$; $q' = 5$ qui donne une solution de type S_1. On peut en conclure que y ne peut pas prendre toutes les valeurs impaires dans une solution de type S_1.

Exemple : La seule décomposition de 9 sous la forme $p(p + 2q)$ avec p premier à q est $p = 1$; $q = 4$. La solution (unique) correspondante est donc de type S_3 et la valeur $y = 9$ ne peut donc pas apparaître dans une solution de type S_1. (Pour ces valeurs de p et q, on a vu qu'on obtient $(x', y', z') = (15/3, 9/3, 21/3) = 5, 3, 7)$).

5 - Les congruences modulo 30 vérifiées par z.

Il y a là un phénomène de crible. On a $z = p^2 + pq + q^2$, qui est manifestement impair quand p et q sont premiers entre eux. Voyons de qui se passe modulo 3.

		q		
		0	1	2
p	0	0	1	1
	1	1	0	1
	2	1	1	0

z modulo 3

On constate que z est toujours congru à 1 modulo 3, sauf qi $p \equiv q \bmod 3$ auquel cas la solution sera du type S_3. Par conséquent, si une solution est de type S_1, la valeur de z correspondante est impaire et de la forme $3k + 1$. Modulo 30, cela ne laisse comme possibilités que 1, 7, 13, 19 et 25. Si on regarde maintenant z modulo 5, on constate que z n'est congru à 0 que si p et q le sont. Or p et q sont premiers entre eux, ce qui élimine 25.

Enfin, si la solution est de type S_3, $z' = (p^2 + pq + q^2)/3$ ne peut pas être un multiple de 3. Pour s'en assurer, on peut poser $p = 3k + a$, $q = 3k' + a$, avec $a = 1$ ou 2, et développer. On obtient z' de la forme $3K + a^2$, or a^2 est égale à 1 modulo 3. Par conséquent, z' est un nombre impair non multiple de 3. Par ailleurs, si 5 divisait z', il diviserait $p^2 + pq + q^2$ et on a vu que c'est

impossible. On est donc ramené au cas précédent et z' ne peut prendre que les valeurs 1, 7, 13, 19 modulo 30.

6 - La suite des valeurs impossibles pour x'

Montrons maintenant que dans une solution de type S_3, il existe une infinité de valeurs impaires que x' ne peut pas prendre.

Soit x' un nombre impair, mis sous la forme $3^j(2k+1)$, où $2k+1$ n'est pas multiple de 3. On cherche sous quelles conditions le nombre $x = 3\times x' = 3^{j+1}(2k+1)$ peut s'écrire sous la forme $q^2 - p^2$ avec p et q premiers entre eux et $(q-p)$ multiple de 3. Posons $q = p + 3m$ et substituons cette valeur dans x. Il vient $x = q^2 - p^2 = 3m(3m+2p)$ et $x' = 3^j(2k+1) = m(3m+2p)$.

On ne peut avoir $m = 1$ car dans ce cas, $(3m+2p)$ serait divisible par 3 et p devrait être divisible par 3. Par ailleurs, $(3m+2p)$ ne peut diviser 3^j pour les mêmes raisons. Par conséquent, $(3m+2p)$ doit diviser $(2k+1)$. Soit $\alpha = \dfrac{2k+1}{3m-2p}$. On a donc $m = 3^j\alpha$. Dans ce cas, $(q-p) = 3m = 3^{j+1}\alpha$ et $(q+p) = (3m+2p) = \dfrac{2k+1}{\alpha}$, d'où l'on tire p et q et la décomposition (**6**) :

$$x = 3^{j+1}(2k+1) = q^2 - p^2, \text{ où } q = \frac{(2k+1) + 3^{j+1}\alpha^2}{2\alpha} \text{ et } p = \frac{(2k+1) - 3^{j+1}\alpha^2}{2\alpha}$$

Comme, par hypothèse, $(2k+1)$ n'est pas un multiple de 3, ces valeurs conduisent bien à une solution de type S_3, mais pour que cette décomposition soit acceptable, le nombre p doit être positif, ce qui impose : $k > \dfrac{3^{j+1}\alpha^2 - 1}{2}$, valeur elle-même supérieure à $\dfrac{3^{j+1}-1}{2}$, qui correspond à $\alpha = 1$.

Par conséquent, si $k \geqslant \dfrac{3^{j+1}-1}{2}$, x ne peut pas s'écrire sous la forme (**6**), et les $\dfrac{3^{j+1}-1}{2}$ valeurs correspondantes de x' sont impossibles.

La suite des $x' > 1$ impossibles est la réunion de toutes ces progressions

arithmétiques. Pour chaque progression P_j, le tableau ci-dessous donne seulement les nouvelles valeurs de x' imppossibles introduites par P_j. Par exemple,9 et 27 sont bien de la forme $18k + 9$ et appartiennent à P_2 ; ils ne sopnt pas mentionnés dans la ligne $j = 2$ car ils sont aussi de la forme $6k + 3$ et appartiennent donc déjà à P_1.

j	P_j	p	q	les k et les x' impossibles
0	$2k+1$	$k-1$	$k+2$	$k=0$: 1
1	$6k+3$	$k-4$	$k+5$	$0 \leqslant k \leqslant 4$: 3, 9, 15, 21, 27
2	$18k+9$	$k-13$	$k+14$	$2 \leqslant k \leqslant 14$: 45, 63,..., 243
3	$54k+27$	$k-40$	$k+41$	$5 \leqslant k \leqslant 40$: 297, ... , 2403
...	.....	.....	etc	....

7 - Les x impairs dans les solution S_1

On a vu en 4.1 que x pouvait prendre toutes les valeurs impaires en posant $p = k$; $q = k + 1$. Plus précisément :

$(p , q) \equiv (0, 1) \bmod 3$ donnent les impairs de la forme $6k + 1$

$(p , q) \equiv (1, 2) \bmod 3$ donnent les impairs de la forme $6k + 3$

$(p , q) \equiv (2, 0) \bmod 3$ donnent les impairs de la forme $6k + 5$.

On peut alors se demander quelles valeurs impaires peut prendre x avec les trois autres combinaisons de paramètres modulo 3 : $(p , q) \equiv (0,2)$; $(1,0)$ et $(2,1)$.

7.1 Si $(p,q) \equiv (0,2) \bmod 3$, les impairs concernés sont de la forme $x = 6k+1$, mais apparaissent-ils tous ?

Non.Soiot $x = (q + p)(q - p)$. Posons $\alpha = (q + p)$ et $\beta = (q - p)$. On doit donc avoir $2q = \alpha + \beta$ et $2p = \alpha - \beta$. Pour être représentable, il est donc nécessaire que x admette une décomposition en produit de deux facteurs α et β avec $\alpha \equiv \beta \equiv 2 \bmod 3$, ce qui élimine de nombreux impairs.

En particulier, x ne peut pas être premier, car alors son unique décomposition en facteurs est $\alpha = x$, $\beta = 1$, différent de 2 modulo 3. De même, x ne peut être le carré d'un nombre premier α, car ses seules décompositions en facteurs sont alors $\alpha.\alpha$ et $\alpha^2.1$, qui conduisent respectivement à $p = \alpha - \alpha = 0$ et à $\beta = 1$. Le plus petit nombre impair représentable ainsi est : $55 = 5 \times 11 = 8^2 - 3^2$.

7.2 Si $(p,q) \equiv (1,0) \bmod 3$, les impairs concernés sont de la forme $x = 6k + 5$

Des arguments similaires montrent que, là aussi, une infinité d'impairs ne

peuvent être atteints. En particulier, x ne peut être ni premier ni le carré d'un nombre premier et le plus petit impair représentable ainsi est : $35 = 5 \times 7 = 6^2 - 1^2$.

7.3 Si $(p,q) \equiv (2,1)$ mod 3, les impairs concernés sont de la forme $x = 6k + 3$

Posons $p = 3p' + 2$; $q = 3q' + 1$. On obtient $x = (q + p)(q - p) = 3(q' + p' + 1)(3q' - p' - 1)$, et p' et q' doivent donc être congrus modulo 2 (avec $q' > p'$). Le plus petit impair représentable est : $45 = 5 \times 9 = 7^2 - 2^2$.

7.4 Les première valeurs atteintes

$(p,q) \equiv (0,2)$ $x = 6k + 1$	$(p,q) \equiv (1,0)$ $x = 6k + 5$	$(p,q) \equiv (2,1)$ $x = 6k + 3$
	$35 = 5 \times 7 = 6^2 - 1^2$	$45 = 5 \times 9 = 7^2 - 2^2$
$55 = 5 \times 11 = 8^2 - 3^2$	$65 = 5 \times 13 = 9^2 - 4^2$	
$85 = 5 \times 17 = 11^2 - 6^2$	$95 = 5 \times 19 = 12^2 - 7^2$	$105 = 5 \times 21 = 13^2 - 8^2$
$115 = 5 \times 23 = 14^2 - 9^2$		$135 = 5 \times 27 = 16^2 - 11^2$
	$143 = 5 \times 13 = 12^2 - 1^2$	
$145 = 5 \times 29 = 17^2 - 12^2$	$155 = 5 \times 31 = 18^2 - 13^2$	$165 = 5 \times 33 = 19^2 - 14^2$ (et $165 = 11 \times 15 = 13^2 - 2^2$)
	$185 = 5 \times 37 = 21^2 - 16^2$	
$187 = 11 \times 17 = 14^2 - 3^2$		
$205 = 5 \times 41 = 23^2 - 18^2$	$209 = 11 \times 19 = 15^2 - 4^2$	
	$215 = 5 \times 43 = 24^2 - 19^2$	$231 = 11 \times 21 = 16^2 - 5^2$

On voit qu'il existe relativement peu de valeurs impaires possibles pour x représenté sous l'une ou l'autre de ces trois formes et que leur distribution, qui dépend de la nature des facteurs premiers de x, est très irrégulière. Finalement, ce qui est surprenant n'est donc pas le fait qu'il y ait des valeurs impossibles pour x' dans des solutions de type S_3, c'est qu'elles forment une suite aussi simple.