VECTEURS DE LONGUEUR ENTIÈRE

Lucien Boisvert
Département de mathématiques
Cégep de Maisonneuve

On a souvent l'occasion, en géométrie vectorielle, d'utiliser dans $\mathbb{R}^3$ des vecteurs dont les composantes sont des entiers et dont la longueur est aussi un entier: par exemple les vecteurs:

$$(1, 2, 2); (2, 3, 6); (3, 4, 12); (4, 5, 20);...$$

On trouve facilement, pour les vecteurs précédents, la formule:

$$|(n, n+1, n^2+n)| = n^2+n+1$$

Mais il existe d'autres vecteurs de longueur entière dans $\mathbb{N}^3$ qui ne suivent pas cette formule: par exemple les vecteurs:

$$(2, 6, 9); (2, 5, 14); (8, 9, 12); (5, 12, 13).$$

Est-il possible de trouver une formule ou un algorithme simple permettant d'obtenir tous les vecteurs recherchés? Ce problème, dont la solution serait très utile en géométrie vectorielle, est, en fait, un problème qui concerne la théorie des nombres. On peut alors l'énoncer de la façon suivante:

Problème: résoudre dans $\mathbb{N}$ l'équation:

$$x^2 + y^2 + z^2 = u^2.$$

C'est une généralisation d'un problème classique en théorie des nombres résolu par les Grecs de l'Antiquité, à savoir celui de la construction des triangles pythagoriens, i.e. la recherche d'une formule donnant tous les triplets $(a, b, c) \in \mathbb{N}^3$ tels que $a^2 + b^2 = c^2$. On a déjà démontré en théorie des nombres que tous ces triplets ont la forme:

$$(r(m^2 \times - n^2), r(m^2+n^2), r(2mn)) \text{ où } m, n, r \in \mathbb{N}.$$

A) Avant de généraliser cette formule au cas de quadruplets $(a, b, c, d) \in \mathbb{N}^4$ tels que $a^2 + b^2 + c^2 = d^2$, il convient d'en donner une preuve dans $\mathbb{N}^3$ pour ensuite adapter cette preuve à $\mathbb{N}^4$.

Preuve: Soit $(x, y, z) \in \mathbb{N}^3$ tel que $x^2 + y^2 = z^2$.

1) On peut supposer que x est pair.

En effet, si x et y sont impairs, alors z est pair et $x^2 + y^2$ n'est pas divisible par 4 tandis que z^2 l'est; ce qui donne une contradiction.

2) Si $x = 2a$, $a \in \mathbb{N}$ alors:

$$y = \frac{a^2}{k} - k \text{ et } z = \frac{a^2}{k} + k$$

$$\text{où } k < a, k \in \mathbb{N} \text{ et } k \mid a^2.$$

Pour trouver ces formules, il faut considérer deux cas:

a) $y = 2c + 1$ et $z = 2d + 1$ sont impairs.

Alors, on a: $(2a)^2 + (2c+1)^2 = (2d+1)^2$.

Remplaçons $2d + 1$ par $(2c + 1) + 2k$ où $k \in \mathbb{N}$.

On obtient:

$$4a^2 + (2c+1)^2 = (2c+1)^2 + 4k(2c+1) + 4k^2 \text{ i.e.}$$
$$4a^2 = 4k(2c+1) + 4k^2$$
$$a^2 - k^2 = k(2c+1).$$

D'où, $2c + 1 = \frac{a^2}{k} - k = y$ où $k \mid a^2$.

Et comme $z = y + 2k$, alors: $z = \frac{a^2}{k} + k$.

b) $y = 2c$ et $z = 2d = 2c + 2k$ où $k \in \mathbb{N}$.

Alors, on a:

$$(2a)^2 + (2c)^2 = (2c+2k)^2$$
$$4a^2 + (2c)^2 = (2c)^2 + 2(2c)(2k) + 4k^2$$
$$4a^2 = 4k(2c) + 4k^2$$
$$a^2 - k^2 = k(2c) = ky.$$

Donc, $y = \frac{a^2}{k} - k$ et $z = \frac{a^2}{k} + k$.

De plus, pour avoir $y > 0$, il faut $k < a$.

3) Démontrons que toutes les solutions $\left(2a, \frac{a^2}{k} - k, \frac{a^2}{k} + k\right)$ sont de la forme

$r(2mn, m^2 - n^2, m^2 + n^2)$.

Mais, auparavant examinons l'exemple suivant: trouvons, à l'aide des deux formules précédentes, toutes les solutions telles que $2a = 60 = 2rmn$.

Si $a = 30$, on a:

k	$\frac{900}{k} - k$	$\frac{900}{k} + k$
1	899	901
2	448	452
3	297	303
4	221	229
5	175	185
6	144	156
9	91	109
10	80	100
12	63	87
15	45	75
18	32	68
20	25	65
25	11	61
30	0	60

Et si $rmn = 30$, on a:

r	m	n	$r(m^2 - n^2)$	$r(m^2 + n^2)$
1	30	1	899	901
	15	2	221	229
	10	3	91	109
	6	5	11	61
2	15	1	448	452
	5	3	32	68
3	10	1	297	303
	5	2	63	87
5	6	1	175	185
	3	2	25	65
6	5	1	144	156
10	3	1	80	100
15	2	1	45	75
30	1	1	0	60

Les deux formules donnent les mêmes solutions qu'on peut regrouper de la façon suivante:

k	r
1, 4, 9, 25	1
2, 18	2
3, 12	3
5, 20	5
6	6
10	10
15	15
30	30

Où l'on voit que $k = rp^2$ où $r \mid a$ et $p \mid a$ et $rp \mid a$, $k \leqslant a$.

Or, dans la formule $\left(2a, \frac{a^2}{k} - k, \frac{a^2}{k} + k\right)$, il est permis de poser $k = rp^2$ où $r \mid a$, $p \mid a$, $rp^2 \mid a^2$ et $rp \mid a$.

On obtient alors:

$$\left(2a, \frac{a^2}{rp^2} - rp^2, \frac{a^2}{rp^2} + rp^2\right)$$
$$= r\left(\frac{2a}{r}, \frac{a^2}{r^2p^2} - p^2, \frac{a^2}{r^2p^2} + p^2\right)$$
$$= r\left(2\left(\frac{a}{rp}\right)(p), \left(\frac{a}{rp}\right)^2 - (p)^2, \left(\frac{a}{rp}\right)^2 + (p)^2\right)$$

Ce qui prouve que toute solution

$$\left(2a, \frac{a^2}{k} - k, \frac{a^2}{k} + k\right)$$

est bien de la forme $r(2mp, m^2 - p^2, m^2 + p^2)$.

B) Cherchons maintenant à résoudre dans $\mathbb{N}$ l'équation

$$x^2 + y^2 + z^2 = u^2.$$

1) On peut supposer que x et y sont pairs.

En effet, si deux des variables x, y, z sont impaires, disons x et y, alors z et u sont pairs ou bien z et u sont impairs et dans les deux cas $x^2 + y^2$ n'est pas divisible par 4 tandis que $u^2 - z^2$ l'est.

Et l'équation $x^2 + y^2 = u^2 - z^2$ devient alors impossible.

2) On peut démontrer que si $x = 2a$ et $y = 2b$ où $a, b \in \mathbb{N}$, alors:

$$z = \frac{a^2 + b^2}{k} - k \text{ et } u = \frac{a^2 + b^2}{k} + k \text{ où } k \mid (a^2 + b^2).$$

a) Si $z = 2c + 1$ et $u = (2c + 1) + 2k$, où $k \in \mathbb{N}$, sont impairs, alors:

$$(2a)^2 + (2b)^2 + (2c + 1)^2 = [(2c + 1) + 2k]^2$$
$$\rightarrow 2c + 1 = \frac{a^2 + b^2}{k} - k = z$$
$$\text{et } u = z + 2k = \frac{a^2 + b^2}{k} - k \text{ où } k \mid (a^2 + b^2).$$

b) Si $z = 2c$ et $u = 2c + 2k$, $k \in \mathbb{N}$, sont pairs, alors:

$$(2a)^2 + (2b)^2 + (2c)^2 = (2c + 2k)^2$$
$$\rightarrow 2c = \frac{a^2 + b^2}{k} - k = z$$
$$\text{et } u = z + 2k = \frac{a^2 + b^2}{k} + k.$$

3) Tout quadruplet:

$r(2mp, 2np, m^2 + n^2 - p^2, m^2 + n^2 + p^2)$
où $r, m, n, p \in \mathbb{N}$, est solution de l'équation. Car:

$$(2mp)^2 + (2np)^2 + (m^2 + n^2 - p^2) = (m^2 + n^2 + p^2)^2.$$

4) Est-il vrai que toute solution de la forme:

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

est de la forme:

$$r(2mp, 2np, m^2 + n^2 - p^2, m^2 + n^2 + p^2)?$$

Considérons l'exemple suivant:

Trouvons toutes les valeurs de z et de u telles que (6, 18, z, u) vérifie l'équation $6^2 + 18^2 + z^2 = u^2$.

a) Soit $2a = 6$ et $2b = 18$; d'où, $a^2 + b^2 = 90$.

k	$\frac{a^2 + b^2}{k} - k$	$\frac{a^2 + b^2}{k} + k$
1	89	91
2	43	47
3	27	33
5	13	23
6	9	21
9	1	19
10	−1	19
15	9	21
18	−13	23
30	−27	33
45	−43	47
90	−89	91

b) Soit $2rmp = 6$ et $2rnp = 18$.

r	m	n	p	$r(m^2 + n^2 - p^2)$	$r(m^2 + n^2 + p^2)$
1	3	9	1	89	91
	1	3	3	1	19
3	1	3	1	27	33

On voit donc que les solutions:

$(6, 18, 9, 21)$; $(6, 18, 13, 23)$ et $(6, 18, 43, 47)$

ne sont pas de la forme

$$r(2np, 2mp, m^2 + n^2 - p^2, m^2 + n^2 + p^2)$$

où $m, np, r \in \mathbb{N}$. Ceci vient du fait que pour diviser $a^2 + b^2$, il n'est pas nécessaire de diviser a et b.

Par contre, toute solution

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

si on la multiplie par k, prend la forme voulue

$$(2ak, 2bk, a^2 + b^2 - k^2, a^2 + b^2 + k^2)$$

où $r = 1$.

On peut donc affirmer que:

Théorème:

Toute solution de l'équation: $x^2 + y^2 + z^2 = u^2$ dans $\mathbb{N}$ a la forme: $\left(2a, 2b, \frac{a^2 + b^2}{k} - k, \frac{a^2 + b^2}{k} + k\right)$

où $a, b, k \in \mathbb{N}$ et $k \mid (a^2 + b^2)$; et cette forme est équivalente à $r(2np, 2mp, m^2 + n^2 - p^2, m^2 + n^2 + p^2)$

où $m, n, p \in \mathbb{N}$, $r \in \mathbb{N}$ ou $r = \frac{1}{s}$ et $s \in \mathbb{N}$.

C) Montrons, en terminant, comment ce théorème peut permettre de construire des vecteurs de longueur entière dans $\mathbb{N}^3$.

Exemple 1

Trouver toutes les valeurs de c telles que le vecteur $(4, 12, c)$ soit de longueur entière L.

Prenons $2a = 4$ et $2b = 12$, d'où; $a^2 + b^2 = 40$.

k	c	L
1	39	41
2	18	22
4	6	14
5	3	13
8	−3	13
10	−6	14
20	−18	22
40	−39	41

On a donc les vecteurs:

$(4, 12, 39)$; $(4, 12, 18)$; $(4, 12, 6)$; $(4, 12, 3)$.

Exemple 2

Trouver toutes les valeurs de c telles que $(3, 6, c)$ soit de longueur entière L.

Il suffit de déterminer c pour que le vecteur $(6, 12, 2c)$ soit de longueur entière 2L.

Prenons $2a = b$, $2b = 12$ et $a^2 + b^2 = 45$.

k	2c	2L
1	44	46
3	12	18
5	4	14
9	−4	14
15	−12	18
45	−44	46

On retient les vecteurs: $(6, 12, 44)$; $(6, 12, 12)$; $(6, 12, 4)$ et, en les divisant par 2, on a: $(3, 6, 22)$; $(3, 6, 6)$; $(3, 6, 2)$.

En résumé, on a les formules:

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

où $a, b, k, \frac{a^2 + b^2}{k} \in \mathbb{N}$ et

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

où $a, b, k, \frac{a^2 + b^2}{k} \in \mathbb{N}$ a pair, b impair.

Question

Que devient cette dernière formule si $a = n$, $b = n + 1$ et $k = 1$?