Triplets Pythagoriciens

S. Darses

Niveau : Approfondir la Terminale S

Difficulté : Moyenne, difficile sur la fin

Durée : 1h30 à 2h

Rubrique(s) : Arithmétique et trigonométrie

La petite histoire... Le but de ce problème est de trouver une méthode pour obtenir, si possible, tous les triplets pythagoriciens, c'est-à-dire tous les triangles rectangles dont la longueur des côtés est entière. Plus précisément, on cherche les triplets d'entiers naturels (a, b, c) vérifiant

$$a^2 + b^2 = c^2. \quad (*)$$

Pour cela, on va utiliser un peu de trigonométrie. Des formules de trigonométrie qu'on pourrait penser assez rébarbatives vont montrer toute leur beauté !
On passera ensuite à une preuve plus arithmétique de la caractérisation des triplets et pour finir à la preuve de la non-existence de solutions entières de l'équation

$$a^4 + b^4 = c^4.$$

Celle-ci est un cas particulier d'équations appelées diophantiennes. Elles sont très difficiles à résoudre en général. En 1994, Andrew Wiles, en s'appuyant sur un certain nombre de résultats très importants, donna une démonstration du grand théorème de Fermat :

Théorème :
Il n'existe pas de nombres entiers non nuls a, b et c tels que

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

dès lors que n est un entier strictement supérieur à 2.

La preuve du résultat de non-existence d'une solution a pris beaucoup de temps et a conduit à la naissance de nouvelles théorie en mathématiques. Pierre de Fermat énonce en premier ce résultat en ajoutant dans la marge :
“ ... J'ai trouvé une merveilleuse démonstration de cette proposition, mais la marge est trop étroite pour la contenir ”.
La communauté mathématique pense aujourd'hui qu'il n'avait pas en fait de preuve de ce résultat, vu les difficultés qu'il soulève. Vous démontrerez peut-être dans les années qui viennent ce résultat pour $n = 3$, $n = 5$ ... La suite pourrait vous amener à découvrir les courbes elliptiques et d'autres objets merveilleux...

Tous les entiers ici seront naturels (i.e. positifs) et nous utiliserons seulement comme notion d'arithmétique la notion de nombres premiers entre eux (rappel en exercice 2) et de PGCD (plus grand commun diviseur, rappel en exercice 3).

Exercice 1.

1) Connaissez-vous déjà un triplet pythagoricien ?

2) À quelle situation géométrique correspond le cas $b = 0$? et $c = 0$? On appellera ces cas des cas triviaux.

3) On se place désormais dans des cas non triviaux. Divisons donc l'équation $(*)$ par c^2 (qui est non nul). À quelle formules de trigonométrie bien connues vous fait penser la nouvelle équation ?

4) On rappelle les formules suivantes :

$$\begin{aligned} \cos\theta &= \frac{1-t^2}{1+t^2}, && (1) \\ \sin\theta &= \frac{2t}{1+t^2}, && (2) \end{aligned}$$

où $t = \tan(\theta/2)$.

a) Peut-on trouver θ tel que t soit rationnel, i.e. qu'il s'écrive $t = \frac{p}{q}$?

b) En déduire, avec la question 3), qu'on peut trouver plein de triplets pythagoriciens !

5) Avec les formules obtenues, donnez quelques exemples numériques de triplets pythagoriciens.

Indications et Commentaires : C'est l'occasion de revoir un peu de trigonométrie, notamment comment obtenir les formules (1) et (2).
L'exercice montre que l'on peut obtenir une infinité de solutions entières à l'équation

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

Une question vient alors : a-t-on trouvé TOUTES les solutions ? La réponse est oui !

Corrections.

1) On essaie $(3, 4, 5)$ et ça marche : $3^2 + 4^2 = 9 + 16 = 25 = 5^2$.

2) Le cas $b = 0$ correspond au cas où le triangle est aplati. Lorsque $c = 0$, cela veut dire que $a = b = 0$, donc cette fois-ci notre triangle est en fait juste un point.

3) En divisant par c^2 l'équation $(*)$, on obtient

$$\alpha^2 + \beta^2 = 1,$$

où $\alpha = a/c$ et $\beta = b/c$. Cette égalité nous fait penser à la formule

$$\cos^2\theta + \sin^2\theta = 1.$$

3.a) Oui, on peut trouver des t qui soient rationnels. On peut même tous les avoir ! Considérons un rationnel quelconque p/q. On pose $\theta = 2\text{Arctan}\,(p/q)$, où Arctan est la fonction réciproque de tan, c'est-à-dire $\tan(\text{Arctan}\,(x)) = x$. Alors on vérifie facilement que $t = p/q$.

3.b) Ainsi, en utilisant la formule trigo de la question 3), on obtient

$$\frac{\left(1-\frac{p^2}{q^2}\right)^2}{\left(1+\frac{p^2}{q^2}\right)^2} + \frac{\left(2\frac{p}{q}\right)^2}{\left(1+\frac{p^2}{q^2}\right)^2} = 1,$$

d'où

$$\left(1-\frac{p^2}{q^2}\right)^2 + \left(2\frac{p}{q}\right)^2 = \left(1+\frac{p^2}{q^2}\right)^2.$$

Finalement, en multipliant par q^4 on arrive à

$$\left(q^2-p^2\right)^2 + (2pq)^2 = \left(q^2+p^2\right)^2.$$

4) Pour s'amuser, prenons $p = 2$ et $q = 3$. On a :

$$\begin{aligned} q^2 - p^2 &= 5 \\ 2pq &= 12 \\ q^2 + p^2 &= 13. \end{aligned}$$

Vérification : $5^2 + 12^2 = 25 + 144 = 169 = 13^2$. Incroyable, non ?

$\square$

Exercice 2. On rappelle que des nombres sont premiers entre eux ssi leur seul diviseur entier commun est 1.
Montrer que si a, b et c sont des entiers avec a et b premiers entre eux et $c^2 = ab$, alors a et b sont des carrés, c'est à dire qu'il existe a' et b' entiers tels que $a = a'^2$ et $b = b'^2$.

Indications et Commentaires : Fondamentalement, c'est la décomposition en facteurs premiers (et son unicité) qui garantissent cette propriété. Commencer par faire cet exercice avec a et b premiers, puis a et b puissances d'un nombre premier, et enfin a et b chacun produit de deux nombres premiers.
On peut en fait généraliser la propriété précédente à $c^2 = c_1^2 c_2^2 \cdots c_n^2$ pour $n \in \mathbb{N}$ et $c_1, c_2, \cdots, c_n$ premiers entre eux.

Corrections. Les entiers a, b et c admettent une décomposition en facteurs premiers. Cela signifie qu'il existe k_a, k_b et k_c entiers, $2 \leqslant p_1 < p_2, \cdots < p_{k_a}$, $2 \leqslant q_1 < q_2 < \cdots < q_{k_b}$, $2 \leqslant r_1 \leqslant r_2 \leqslant \cdots \leqslant r_{k_c}$ des nombres premiers et $n_1, n_2, \cdots, n_k \geqslant 1$, $m_1, m_2, \cdots, m_k \geqslant 1$, $s_1, s_2, \cdots, s_k \geqslant 1$ entiers tels que

$$a = p_1^{n_1} p_2^{n_2} \cdots p_k^{n_k}, \qquad b = q_1^{m_1} q_2^{m_2} \cdots q_k^{m_{k_b}}, \qquad c = r_1^{s_1} r_2^{s_2} \cdots r_{k_c}^{s_{k_c}}.$$

De plus pour tous i, j, $p_i \neq q_j$ car a et b sont premiers entre eux. En effet, comme $n_i \geqslant 1$, p_i divise a et ne peut donc diviser b. Or pour tout j, q_j divise b car $m_j \geqslant 1$. Donc $p_i \neq q_j$. On obtient

$$c^2 = r_1^{2s_1} r_2^{2s_2} \cdots r_{k_c}^{2s_{k_c}} = ab = p_1^{n_1} p_2^{n_2} \cdots p_k^{n_k} \times q_1^{m_1} q_2^{m_2} \cdots q_k^{m_l}.$$

L'unicité de la décomposition en facteurs premiers de c^2 et le fait que $p_i \neq q_j$ impose que tous les n_i et les m_j soient pairs. Donc $n_i = 2n'_i$ et $m_j = 2m'_j$. Au final,

$$a = \left(p_1^{n'_1} p_2^{n'_2} \cdots p_k^{n'_k}\right)^2, \qquad b = \left(q_1^{m'_1} q_2^{m'_2} \cdots q_k^{m'_{k_b}}\right)^2,$$

ce qui prouve que a et b sont des carrés d'entiers :

$$a^2 = u^2 - v^2, \qquad b^2 = 2uv, \qquad c = u^2 + v^2.$$

$\square$

Exercice 3. Dans cet exercice, nous allons trouver par une méthode arithmétique tous les entiers a, b, c premiers entre eux tels que

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

Nous cherchons à montrer que les solutions sont de la forme

$$a = u^2 - v^2, \qquad b = 2uv, \qquad c = u^2 + v^2,$$

avec u et v entiers premiers entre eux. Supposons donc que $a^2 + b^2 = c^2$.

1) Montrer que a et b sont de parité différente et que c est impair.
On suppose désormais a impair et b pair.

2) Montrer que le PGCD de $c - a$ et $c + a$ est égal à 2. On rappelle que le pgcd de deux entiers est le plus grand entier qui les divise tous les deux.

3) En déduire qu'il existe deux entiers u et v tels que

$$c - a = 2u^2, \qquad \text{et} \qquad c + a = 2v^2.$$

4) Conclure en déterminant l'ensemble des triplets (a, b, c) premiers entre eux et solution de $a^2 + b^2 = c^2$.

Indications et Commentaires : 1) Montrer que la somme des carrés de deux nombres impairs est de la forme $4k + 1$.
3) Utiliser $(c - a)(c + a) = c^2 - a^2 = b^2$ et l'exercice précédent.
4) Il s'agit de prouver que, quitte à intervertir la place de a et b, si $a^2 + b^2 = c^2$ avec a, b, c premiers entre eux, alors il existe u et v premiers entre eux tels que

$$a = v^2 - u^2, \qquad b = 2uv, \qquad c = u^2 + v^2.$$

Corrections.

1) Si a et b sont impairs alors $a = 2k + 1, b = 2k' + 1$ et donc

$$a^2 + b^2 = (2k + 1)^2 + (2k' + 1)^2 = 4k^2 + 4k + 1 + 4k'^2 + 4k' + 1 = 4(k^2 + k + k'^2 + k') + 2 = c^2.$$

Donc c^2 est pair, d'où c est pair et $c = 2c'$. On en déduit que

$$4c'^2 = 4(k^2 + k + k'^2 + k') + 2, \qquad \text{i.e.} \qquad 2 = 4(c'^2 - (k^2 + k + k'^2 + k'))$$

et donc 4 divise 2, ce qui est faux.
Si a et b sont pairs, alors a^2 et b^2 sont pairs et $a^2 + b^2 = c^2$ est pair. Alors c^2 et donc c sont pairs. Ceci contredit le fait que a, b et c sont premiers entre eux.
Nous avons ainsi exclu les cas où a et b ont même parité : ils sont donc de parité différente. En remarquant ensuite que la parité d'un nombre est la même que celle de son carré et que la somme d'un nombre pair et d'un nombre impair est impair, on obtient que c est impair.

2) Si d divise $c - a$ et $c + a$, alors il divise leur somme et leur différence et donc d divise $2c$ et $2a$. Comme c et a sont premiers entre eux, d divise 2. Or c et a ont même parité (ils sont impairs tous les deux), ce qui fait que 2 est diviseur commun de $c - a$ et $c + a$. Donc le PGCD de $c - a$ et $c + a$ est précisément 2.

3) Comme $(c - a)(c + a) = c^2 - a^2 = b^2$, en posant

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

où x et y sont des entiers premiers entre eux, on obtient

$$xy = (b')^2.$$

L'exercice précédent assure que x et y sont des carrés et donc

$$c - a = 2u^2, \qquad c + a = 2v^2.$$

4) En ajoutant les deux égalités précédentes, on obtient :

$$c = u^2 + v^2.$$

En les retranchant, il vient :

$$a = v^2 - u^2.$$

Et en les multipliant :

$$b^2 = 4u^2v^2,$$

i.e. $b = 2uv$.

On a donc montré que les triplets (a, b, c) premiers entre eux et solution de $a^2 + b^2 = c^2$ sont nécessairement de la forme précédente.
Réciproquement, en les prenant de cette forme, on vérifie que $a^2 + b^2 = c^2$ car

$$a^2 = (v^2 - u^2)^2 = v^4 - 2u^2v^2 + u^4, \quad c^2 = (v^2 + u^2)^2 = v^4 + 2u^2v^2 + u^4.$$

□

Exercice 4. Le but de cette exercice est de démontrer qu'il n'y pas de triplet d'entiers non nuls solution de

$$a^4 + b^4 = c^4.$$

1) Montrer que s'il existe un triplet d'entiers non nuls a, b, c solution de l'équation précédente, alors il existe un triplet d'entiers premiers entre eux et solution de cette équation.

Nous allons procéder par l'absurde et nous supposons qu'il existe un triplet d'entiers non nuls (a, b, c) premiers entre eux et solution de

$$a^4 + b^4 = c^2. \tag{3}$$

(Le c^2, et non c^4, n'est pas une erreur ! En fait on montre quelque chose de plus fort).

2) Montrer que a et b sont de parité différente et que c est impair. On suppose maintenant que a est impair et b est pair.

3) Montrer qu'il existe u et v premiers entre eux, avec u impair et v pair, tels que

$$a^2 = u^2 - v^2, \qquad b^2 = 2uv, \qquad c = u^2 + v^2.$$

4) Montrer alors qu'il existe des entiers x, y, z, t avec z et t premiers entre eux tels que

$$u = x^2, \quad v = 2y^2, \quad a^2 = z^2 - t^2, \quad v = 2zt, \quad \text{et} \quad u = z^2 + t^2.$$

5) Montrer enfin que z et t sont des carrés, i.e., $z = z_1^2$ et $t = t_1^2$. En déduire que

$$x^2 = z_1^4 + t_1^4.$$

6) Justifier que $x < c$ puis aboutir à une contradiction.

7) Conclure à la non-existence d'une solution entière non nulle à $a^4 + b^4 = c^4$.

Indications et Commentaires : 1) C'est la première question de l'exercice 1.
2) Utiliser le résultat de l'exercice 2 ainsi que sa première question.
3) Utiliser les deux exercices précédents.
5) Procédé de descente infinie, on peut répéter l'opération indéfiniment.

Corrections.

1) Si a, b, c est solution de $a^4 + b^4 = c^4$, on considère le PGCD (plus grand commun diviseur) de a, b, c et alors

$$a = da', \quad b = db', \quad c = dc', \quad \text{avec } a', b', c' \text{ premiers entre eux.}$$

De plus, en simplifiant l'équation par d^4, on a $a'^4 + b'^4 = c'^4$, ce qui répond à la question.

2) On applique le résultat de la question 1) de l'exercice 3 au triplet (a^2, b^2, c). On en déduit que a^2 et b^2 sont de parité différente, et donc a et b aussi. De plus, c est impair.

3) L'exercice 2 permet d'obtenir u et v premiers entre eux satisfaisant

$$a^2 = u^2 - v^2, \qquad b^2 = 2uv, \qquad c = u^2 + v^2.$$

De plus, a est impair. Or, $v^2 + a^2 = u^2$ et la question 1) de l'exercice 3 implique que u est impair et v et a sont de parité différente, donc v est pair.

4) En écrivant $a^2 + v^2 = u^2$, on déduit de la conclusion de l'exercice 3 (ou 1) qu'il existe z et t premiers entre eux tels que

$$a^2 = z^2 - t^2, \quad v = 2zt, \quad u = z^2 + t^2.$$

Comme $b^2 = 2uv$, on déduit de l'exercice 2 que u et $2v$ sont des carrés : $u = x^2$ et $2v = r^2$. Donc r est pair aussi, i.e. $r = 2y$. Ainsi, $2v = 4y^2$ et $v = 2y^2$.

5) En particulier, on obtient $y^2 = zt$. Comme z et t sont premiers entre eux, z et t sont nécessairement des carrés : $z = z_1^2$, $t = t_1^2$. Donc, en utilisant encore la question précédente, il vient :

$$x^2 = z_1^4 + t_1^4.$$

6) De l'égalité $c = u^2 + v^2$, on déduit que $c > u^2$. Donc

$$c > u = x^2 > x$$

car $u \geq 1$ et $x \geq 1$.

Finalement, on a trouvé un x strictement plus petit que c, qui s'écrit encore comme une somme d'entiers non nuls à la puissance 4. On peut alors réitérer le raisonnement et créer un nouvel entier strictement plus petit que x vérifiant cette propriété. Et ainsi de suite... On arrive donc en un nombre fini d'étapes à l'entier 1 qui devrait donc s'écrire encore comme une somme d'entiers non nuls à la puissance 4. Mais ceci est faux ! D'où une contradiction.

7) On en déduit donc que notre hypothèse de travail initiale, i.e. l'équation (3), est fausse, ce qui prouve le résultat voulu. $\square$