Sur les pas de Fermat

S. Darses, A. Devys, R. Dos Santos

Niveau : Terminale
Difficulté : ★★★
Durée : entre 3 et 4 heures
Rubrique(s) : Arithmétique, Trigonométrie

Cette atelier aborde l'arithmétique qui est une notion travaillée en classe de Terminale S, si vous avez choisi ou choisissez la spécialité mathématique. Mais nul besoin d'avoir vu les théorèmes de Terminale pour s'attaquer à cet atelier...

La petite histoire...
Résoudre une équation entre entiers, pas si simple ! les équations diophantiennes, comme on les appelle, ont donné et donnent encore beaucoup de fil à retordre aux mathématiciens. Déjà, Diophante d'Alexandrie (qui donna son nom aux fameuses équations) au III^e siècle rédigeait un livre sur le sujet.
Une équation diophantienne très célèbre est la suivante : trouver un triplet d'entiers naturels non nuls vérifiant pour n entier :

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

En réalité il n'existe pas de solution pour $n \geq 3$. Ce problème a occupé des mathématiciens pendant près de 350 ans. Au début du XVII^e siècle, Pierre de Fermat énonce en premier ce résultat en ajoutant dans la marge d'une traduction (du grec au latin) des *Arithmétiques* de Diophante :
« Au contraire, il est impossible de partager soit un cube en deux cubes, soit un bicarré en deux bicarrés, soit en général une puissance quelconque supérieure au carré en deux puissances de même degré : j'en ai découvert une démonstration véritablement merveilleuse que cette marge est trop étroite pour contenir ». Cependant personne n'a jamais vu cette démonstration dont parle Fermat.
Ce n'est qu'en 1994, après de nombreux mathématiciens célèbres tels Legendre, Dirichlet, Euler, Lamé, Cauchy..., qu'Andrew Wiles donne enfin une démonstration complète de ce résultat.
Reste un mystère, Fermat avait-il vraiment une démonstration ?

Monsieur et Madame
Ombrepremiersentredeuxettreize ont un fils...

Exercice 1 (Triplets pythagoriciens : méthode trigonométrique).

1. On appelle triplet pythagoricien tout triplet d'entiers naturels (a, b, c) vérifiant la relation de Pythagore $a^2 + b^2 = c^2$. Connaissez-vous un tel triplet ?

2. Soit $\left(O; \vec{i}, \vec{j}\right)$ un repère orthonormé du plan. Soient I,J et K les points de coordonnées respectives $(1, 0)$, $(0, 1)$ et $(-1, 0)$.
On note $\mathcal{C}$ le cercle de centre O et de rayon 1.
Montrer que (a, b, c) est un triplet pythagoricien avec a, b et c tous non nuls si, et seulement si, le point M de coordonnées $\left(\frac{a}{c}, \frac{b}{c}\right)$ appartient à l'arc de cercle IJ.

3. Soit M un point du cercle $\mathcal{C}$ de coordonnées (x, y) avec $x > 0$ et $y > 0$. On appelle H, le projeté orthogonal de M sur l'axe des abscisses. On note θ la mesure de l'angle $\widehat{IOM}$.

a. En se plaçant dans le triangle KHM, exprimer $\tan(\frac{\theta}{2})$ en fonction de x et y.

b. En déduire x et y en fonction de $\tan(\frac{\theta}{2})$.

Dans la suite de l'exercice, on note $t = \tan(\frac{\theta}{2})$ avec $\theta \in]0, \frac{\pi}{2}[$.

4. Montrer que si t est rationnel alors on peut trouver λ rationnel et c entier naturel non nul tel que $(\lambda x, \lambda y, c)$ soit un triplet pythagoricien.

5. Réciproquement, montrer que si (a, b, c) est un triplet pythagoricien avec a, b et c non tous nuls, alors il existe un réel θ tel que t soit rationnel.

6. Combien, du coup, y-a-t-il de triplets d'entiers (a, b, c) vérifiant $a^2+b^2 = c^2$?

Exercice 2 (Utile pour l'exercice 3).

Soient a et b deux entiers naturels.
On dit que d est un diviseur de a et b si d divise à la fois a et b. Le plus grand diviseur commun de a et b est noté PGCD(a, b). S'il vaut 1, on dit que les deux entiers sont premiers entre eux.

1. Soient deux entiers naturels a et b et $d = \text{PGCD}(a, b)$. Montrer qu'il existe deux entiers naturels a' et b', premiers entre eux tels que $a = da'$ et $b = db'$.

2. Montrer que si a, b et c sont des entiers naturels avec $c^2 = ab$ et a et b premiers entre eux alors a et b sont des carrés, c'est-à-dire qu'il existe deux entiers naturels a' et b' tels que $a = a'^2$ et $b = b'^2$.

Exercice 3 (Triplets pythagoriciens : méthode arithmétique).
Cherchons une preuve arithmétique du résultat de l'exercice 1 par analyse-synthèse. (On pourra se référer à la fiche de fondamentaux sur les différents types de raisonnements.)

1. Supposons qu'il existe trois entiers naturels a, b et c tels que $a^2 + b^2 = c^2$.

a. Montrer qu'on peut se ramener au cas où a, b, c sont premiers entre eux dans leur ensemble, c'est-à-dire que le plus grand diviseur commun de a, b et c est 1.
Montrer que si a, b et c sont trois entiers premiers entre eux et vérifient la relation $a^2 + b^2 = c^2$ alors ils sont premiers deux à deux.
Pour la suite on suppose que a, b et c sont premiers entre eux.

b. Montrer que pour tout entier naturel k, k et k^2 sont de même parité.

c. Montrer que nécessairement a ou b est pair.
Quitte à échanger les rôles de a et b, on suppose pour la suite que b est pair.

d. Montrer que a et c sont impairs.

2. Soit d un diviseur commun à $c - a$ et $c + a$. Montrer que d divise 2. En déduire que $\mathrm{PGCD}(c - a, c + a) = 2$.

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

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

4. Exprimer a, b et c en fonction de u et v.

5. Conclure.

Exercice 4 (Et pour $n = 4$?).
Cette fois cherchons à montrer qu'il n'existe pas de triplets d'entiers naturels (a, b, c) non nuls et premiers entre eux, tels que

$$a^4 + b^4 = c^2.$$

On va utiliser un raisonnement par l'absurde. On suppose qu'il existe un tel triplet.

1. Justifier que nécessairement a ou b est pair. Montrer que si b est pair alors a et c sont impairs.

2. En utilisant l'exercice 3, montrer qu'il existe u et v premiers entre eux avec u impair et v pair tels que :

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

3. Toujours en utilisant l'exercice 3, montrer qu'il existe des entiers naturels x, y_1, z et t avec z et t premiers entre eux, tels que

$$u = 2x^2, \quad v = y_1^2, \quad a = t^2 - z^2, \quad u = 2zt, \quad v = z^2 + t^2.$$

4. Montrer que z et t sont des carrés, c'est-à-dire qu'il existe z_1 et t_1 deux entiers tels que $z = z_1^2$ et $t = t_1^2$. En déduire, que $y_1^2 = z_1^4 + t_1^4$.

5. Montrer que $y_1 < c$. En déduire que si on réitère le procédé on aboutit à une absurdité et conclure.

6. Revenons au problème de Fermat pour $n = 4$, c'est-à-dire la résolution de l'équation $a^4 + b^4 = c^4$.

a. Montrer que l'on peut se ramener au cas où a, b et c sont premiers entre eux

b. Mais alors, existe-t-il un triplet d'entiers naturels non nuls tels que $a^4 + b^4 = c^4$?

Commentaires sur l'Exercice 4

Ce principe de démonstration s'appelle procédé de descente infinie. Même si elle apparaît dans les *Éléments* d'Euclide, c'est surtout Fermat qui formule cette méthode et la développe.

Indications

Indications sur l'Exercice 1

3.a. Penser au théorème de l'angle inscrit.

3.b. C'est un changement de variable assez courant avec le paramètre t qui est égal à $\tan(\frac{\theta}{2})$.

Indications sur l'Exercice 2

2. On pourra utiliser la décomposition en facteurs premiers (et son unicité) en a et b.

Indications sur l'Exercice 3

5. Ne pas oublier la synthèse !

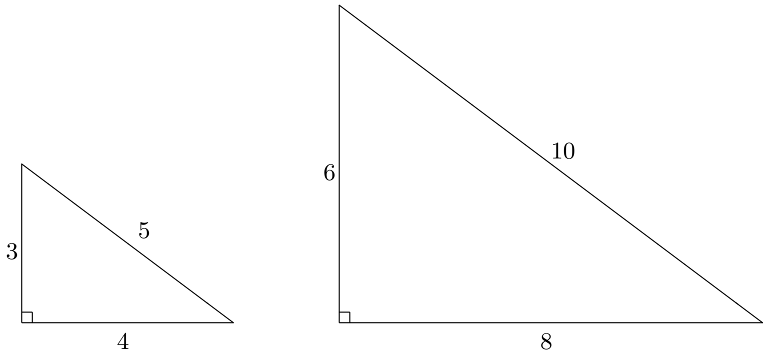
Indications sur l'Exercice 4

5. Cette question utilise une propriété de $\mathbb{N}$: il n'existe pas de suite strictement décroissante d'entiers. Voir la fiche des fondamentaux sur les entiers pour plus de détails.

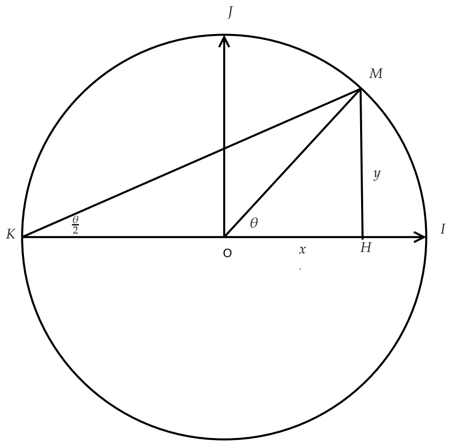
Corrections

Correction de l'Exercice 1

1. Par exemple $(3, 4, 5)$ et $(6, 8, 10)$.



2. Un petit dessin !



Puisque a, b et c sont tous non nuls, on peut diviser la relation $a^2 + b^2 = c^2$ par c^2. On obtient :

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

Les coordonnées du point $M\left(\frac{a}{c}, \frac{b}{c}\right)$ vérifient l'équation du cercle de centre O et de rayon 1 : $x^2 + y^2 = 1$. De plus $\frac{a}{c} > 0$ et $\frac{b}{c} > 0$ donc M appartient au quart de plan supérieur droit. Finalement, M appartient à l'arc IJ.

La réciproque est vraie : en effet si $M\left(\frac{a}{c}, \frac{b}{c}\right)$ appartient à l'arc IJ alors on peut choisir $a > 0$, $b > 0$ et $c > 0$. Ses coordonnées vérifient l'équation :

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

et en multipliant pas c^2, on obtient (a, b, c) vérifiant la relation de Pythagore.

3.a. D'après le théorème de l'angle inscrit, la mesure de l'angle $\widehat{HKM}$ est $\frac{\theta}{2}$. Le triangle HKM est rectangle en H donc $\tan\dfrac{\theta}{2} = \dfrac{HM}{KH} = \dfrac{y}{1+x}$.

3.b. De plus le triangle OMH est également rectangle en H, donc d'après le théorème de Pythagore, $x^2 + y^2 = 1$ soit en remplaçant à l'aide de la relation précédente :
$x^2 + t^2(1+x)^2 = 1$ avec $t = \tan\frac{\theta}{2}$. En réarrangeant, on obtient :

$$t^2 = \frac{1-x^2}{(1+x)^2} = \frac{(1+x)(1-x)}{(1+x)^2} = \frac{(1-x)}{(1+x)}.$$

De cette égalité, on tire : $x = \dfrac{1-t^2}{1+t^2}$. Or $y = t(1+x) = \dfrac{2t}{1+t^2}$. On a donc finalement :

$$x = \frac{1-t^2}{1+t^2} \quad \text{et} \quad y = \frac{2t}{1+t^2}.$$

4. Soit $t = \frac{p}{q} \in \mathbb{Q}$, d'après ce qui précède le point de coordonnées

$$\left(x = \frac{1-t^2}{1+t^2}, y = \frac{2t}{1+t^2}\right)$$

appartient au cercle de centre O et de rayon 1, ses coordonnées vérifient son équation :

$$\begin{aligned}
\frac{\left(1-\left(\frac{p}{q}\right)^2\right)^2}{\left(1+\left(\frac{p}{q}\right)^2\right)^2} + \frac{4\left(\frac{p}{q}\right)^2}{\left(1+\left(\frac{p}{q}\right)^2\right)^2} &= 1 \\
\left(1-\left(\frac{p}{q}\right)^2\right)^2 + 4\left(\frac{p}{q}\right)^2 &= \left(1+\left(\frac{p}{q}\right)^2\right)^2 \quad \text{en multipliant par } \left(1+\left(\tfrac{p}{q}\right)^2\right)^2 \\
(q^2-p^2)^2 + (2pq)^2 &= (q^2+p^2)^2 \quad \text{en multipliant par } q^4
\end{aligned}$$

D'où le résultat avec $\lambda = q^4\left(1+\left(\frac{p}{q}\right)^2\right)^2 = (q^2+p^2)^2 = c$.

5. Récriproquement, si (a, b, c) est un triplet pythagoricien avec a, b et c non tous nuls, on a vu que $\left(\frac{a}{c}, \frac{b}{c}\right)$ appartient au cercle trigonométrique. Donc il existe $\theta \in [0, \frac{\pi}{2}]$ tel que $x = \cos\theta = \frac{a}{c}$ et $y = \sin\theta = \frac{b}{c}$. Le calcul précédent nous donne $t = \tan\frac{\theta}{2} = \frac{y}{1+x} = \frac{b}{c+a} \in \mathbb{Q}$.

6. On a vu à la question 4), qu'en posant $t = \frac{p}{q}$ avec $(p, q) \in \mathbb{Z} \times \mathbb{N}^*$

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

Tout triplet $(|q^2-p^2|, |2pq|, q^2+p^2)$ avec $(p, q) \in \mathbb{Z} \times \mathbb{N}^*$ est un triplet pythagoricien. Il y a donc une infinité de triplets! $\square$

Correction de l'Exercice 2

1. Puisque d est un diviseur de a, il existe un entier naturel a' tel que $a = da'$. De même, il existe un entier naturel b' tel que $b = db'$.

Soit d' un diviseur commun de a' et b', alors dd' est un diviseur commun de a et b. Or d est le plus grand diviseur commun de a et b, donc $dd' \leq d$, soit $d' \leq 1$. En tant que diviseur $d' \geq 1$ donc $d' = 1$. Le seul diviseur commun de a et b est donc 1, a et b sont premiers entre eux.
Une autre démonstration est possible en utilisant l'égalité de Bézout.

2. Les entiers a, b et c admettent chacun une décomposition en facteurs premiers. Cela signifie qu'il existe k_a, k_b et k_c entiers, $p_1 < p_2 < \cdots < p_{k_a}$, $q_1 < q_2 < \cdots < q_{k_b}$, $r_1 < r_2 < \cdots < r_{k_c}$ des nombres premiers et des entiers naturels non nuls $n_1, n_2, \ldots, n_{k_a}$, $m_1, m_2, \ldots, m_{k_b}$, $s_1, s_2, \ldots, s_{k_c}$ tels que

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

De plus pour tout i, j, $p_i \neq q_j$ car a et b sont premiers entre eux. En effet, si p_i divise à la fois a et b alors $\mathrm{PGCD}(a, b) \geq p_i$, ce qui contredit a et b premiers entre eux. Donc $p_i \neq q_j$.
On obtient

$$c^2 = r_1^{2s_1} r_2^{2s_2} \cdots r_{k_c}^{2s_{k_c}} = ab = p_1^{n_1} p_2^{n_2} \cdots p_{k_a}^{n_{k_a}} \times q_1^{m_1} q_2^{m_2} \cdots q_{k_b}^{m_{k_b}}.$$

L'unicité de la décomposition en facteurs premiers de c^2 et le fait que $p_i \neq q_j$ impose que $\forall i \in \{1, \ldots, k_a\}$ il existe $\ell \in \{1, \ldots, k_c\}$ tel que $n_i = 2s_\ell$ et $\forall j \in \{1, \ldots, k_b\}$, il existe $\ell' \in \{1, \ldots, k_c\}$ tel que $m_j = 2s_{\ell'}$. Ainsi, tous les n_i et les m_j sont pairs. Donc $n_i = 2n'_i$ et $m_j = 2m'_j$. Au final,

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

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

Correction de l'Exercice 3

1.a. Soit d le plus grand diviseur commun de a, b et c, alors il existe (a', b', c') tels que $a = da'$, $b = db'$ et $c = dc'$. L'égalité se réécrit $d^2a'^2 + d^2b'^2 = d^2c'^2$. En divisant le tout par d^2, j'obtiens $a'^2 + b'^2 = c'^2$, avec a', b' et c' n'ayant que 1 pour diviseur commun, soit ils sont premiers entre eux.
Maintenant supposons que a, b et c sont premiers entre eux (dans leur ensemble). Supposons par l'absurde que a et b ne sont pas premiers entre eux. Alors il existe p un nombre premier diviseur de a et b, donc p divise $a^2 + b^2 = c^2$. Donc p divise c^2. C'est-à-dire que nécessairement p apparait dans la décomposition de c^2 en produit de facteurs premiers, donc dans celle de c. Donc p divise également c. Dans ce cas, p est un diviseur premier commun à a, b et c ce qui est contraire à l'hypothèse a, b et c sont premiers entre eux (dans leur ensemble). a et b sont donc nécessairement premiers entre eux. On montre exactement de la même manière que b et c, puis a et c sont premiers entre eux. Les entiers a, b et c sont donc premiers entre eux deux à deux.
On suppose maintenant que a, b et c sont premiers entre eux.

1.b. Procédons par disjonction de cas.

- Si k est pair, il existe un entier p tel que $k = 2p$. Dans ce cas, $k^2 = 2 \times 2p^2$, donc k^2 est pair.
- Si k est impair, il existe un entier p tel que $k = 2p+1$. Dans ce cas $k^2 = 2 \times (2p^2 + 2p) + 1$ donc est impair.

Dans tous les cas, k et k^2 ont la même parité.
1.c. Par l'absurde, supposons que a et b sont impairs, alors il existe deux entiers k et ℓ tels que $a = 2k + 1$ et $b = 2\ell + 1$, et :

$$c^2 = a^2 + b^2 = (2k + 1)^2 + (2\ell + 1)^2 = 4(k^2 + \ell^2 + k + \ell) + 2 = 4K + 2, \quad \text{avec} \quad K \text{ un entier.}$$

De plus, en tant que somme de deux nombres impairs, c^2 est pair, donc d'après la question précédente c est pair. On en déduit que 2 divise c donc 4 divise c^2. Cela implique d'après le calcul précédent que 4 divise 2, ce qui est absurde. Donc a et b ne peuvent pas être tous les deux impairs, nécessairement l'un ou l'autre est pair. Quitte à échanger les rôles de a et b, on suppose pour la suite que b est pair.
1.d. Remarquons d'abord que si a est impair et b pair, alors c^2, donc c sont nécessairement impairs.
On procède donc par l'absurde en supposant a et b pairs. Alors 2 divise à la fois a^2 et b^2, donc 2 divise leur somme c^2. D'après la question précédente, 2 divise c et donc 2 est un diviseur commun de a, b et c, ce qui contredit notre hypothèse. a est donc impair et c aussi.

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'après la question 1.a), 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 $\mathrm{PGCD}(c - a, c + a) = 2$.

3. On a vu que $\mathrm{PGCD}(c-a, c+a) = 2$ donc d'après l'exercice 2, il existe x et y deux entiers naturels premiers entre eux tels que $c - a = 2x$ et $c + a = 2y$.
Par produit, j'obtiens $(c - a)(c + a) = c^2 - a^2 = 4xy$, soit $b^2 = 4xy$. D'après l'exercice 2, x et y sont des carrés, il existe u et v tels que $x = u^2$ et $y = v^2$. On a donc :

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

4. Par somme, on a $c = u^2 + v^2$ et par différence $a = v^2 - u^2$. En prenant la racine carrée, on obtient $b = 2uv$.

5. Pour la synthèse, on vérifie que pour tout couple d'entiers naturels (u, v) le triplet $a = |v^2 - u^2|$, $b = 2uv$ et $c = u^2 + v^2$ est solution de l'équation $a^2 + b^2 = c^2$ (on rajoute une valeur absolue pour être sûr d'avoir des entiers positifs). □

Correction de l'Exercice 4

1. On reprend le même raisonnement qu'à l'exercice 3.
Si a et b sont impairs, alors a^2 et b^2 sont impairs et il existe un entier K tel que $a^4 + b^4 = 4K + 2$. De plus a^4 et b^4 sont impairs, donc $c^2 = a^4 + b^4$ est pair, ce qui implique que c est pair. On a donc 2 qui divise c et 4 qui divise c^2. Ce qui contredit le calcul précédent. Nécessairement a ou b est pair. On suppose que b est pair, quitte à échanger les rôles de a et b.
Remarquons d'abord que si a est impair et b pair, alors c^2, donc c, sont nécessairement impairs.
On procède donc par l'absurde en supposant a et b pairs. Alors 2 divise à la fois a^4 et b^4, et 2 divise leur somme c^2, donc 2 divise c et donc 2 est un diviseur commun de a, b et c, ce qui est contredit notre hypothèse. a est donc impair et c aussi.

2. En posant $A = a^2$ et $B = b^2$ on se ramène aux questions 3 et 4 de l'exercice 3. On obtient, l'existence de u et v premiers entre eux tels que :

$$A = a^2 = v^2 - u^2, \quad B = b^2 = 2uv \quad \text{et} \quad c = u^2 + v^2.$$

Puisque u et v sont premiers entre eux, u, v et a sont également premiers entre eux. De plus ils sont liés par la relation $u^2 + a^2 = v^2$ et a est impair donc d'après la question 1.c) de l'exercice 3, on en déduit que u est pair et v impair.

3. Puisque $u^2 + a^2 = v^2$, d'après l'exercice 3, il existe deux entiers naturels z et t premiers entre eux tels que

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

Or $b^2 = 2uv$ avec $2u$ et v premiers entre eux, donc d'après l'exercice 2, $2u$ et v sont des carrés. Il existe r et y_1 des entiers naturels tels que $2u = r^2$ et $v = y_1^2$. r est donc pair, c'est-à-dire qu'il existe un entier naturel x tel que $r = 2x$, on a donc $u = 2x^2$.

4. On a donc $x^2 = zt$ avec z et t premiers entre eux. z et t sont donc des carrés et il existe z_1 et t_1 des entiers naturels tels que $z = z_1^2$ et $t = t_1^2$. v se réécrit $v = z_1^4 + t_1^4 = y_1^2$.

5. On a $c = u^2 + v^2 > v^2 = y_1^4 > y_1$, car y_1 et v sont supérieurs ou égaux à 1.
On a construit à partir de (a, b, c) triplet solution de $a^4 + b^4 = c^2$, un autre triplet solution (z_1, t_1, y_1) solution de la même équation avec $y_1 < c$. En appliquant ce résultat au triplet (z_1, t_1, y_1) on construit encore un nouveau triplet (z_2, t_2, y_2) avec $y_2 < y_1$. Ainsi de suite, on construit une suite $(y_n)_n$ d'entiers naturels strictement décroissante. Or il n'existe pas de telle suite. Nous aboutissons donc à une absurdité. Il n'existe pas de triplet d'entiers naturels non nuls (a, b, c) tel que $a^4 + b^4 = c^2$.

6.a. Soit d le plus grand diviseur commun de a, b et c, alors il existe (a', b', c') tels que $a = da'$, $b = db'$ et $c = dc'$. L'égalité se réécrit $d^4a'^4 + d^4b'^4 = d^4c'^4$. En divisant le tout par d^4, j'obtiens $a'^4 + b'^4 = c'^4$, avec a', b' et c' n'ayant que 1 pour diviseur commun, donc ils sont premiers entre eux (et même premiers entre eux deux à deux).

6.b. S'il existait un triplet (a, b, c) d'entiers naturels premiers entre eux, solution de $a^4 + b^4 = c^4$ alors le triplet (a, b, c^2) serait solution du problème précédent. Or on a vu qu'il n'en n'existait pas. Il n'existe donc pas de triplet (a, b, c) solution de $a^4 + b^4 = c^4$. □

