Devoir surveillé 5

▸ Exercice : sous-groupes et sous-anneaux de R.

Pour $\alpha \in \mathbf{R}$, on note $\alpha\mathbf{Z} = \{k\alpha,\ k \in \mathbf{Z}\}$.

1. Montrer que pour tout $\alpha \in \mathbf{R}$, $\alpha\mathbf{Z}$ est un sous-groupe de $(\mathbf{R}, +)$.
2. Dans cette question, on considère G un sous-groupe de $(\mathbf{R}, +)$, non réduit à $\{0\}$.
   a. Justifier que $G \cap \mathbf{R}_+^* \neq \emptyset$.
   b. On suppose dans cette question que $G \cap \mathbf{R}_+^*$ admet un plus petit élément α.
      i. Montrer que $\alpha\mathbf{Z} \subset G$.
      ii. Soit $g \in G$. Prouver que $g - \left\lfloor \frac{g}{\alpha} \right\rfloor \alpha \in G$. En déduire que $G = \alpha\mathbf{Z}$.
   c. On suppose à présent que $G \cap \mathbf{R}_+^*$ n'admet pas de plus petit élément, et on note $\alpha = \inf(G \cap \mathbf{R}_+^*)$.
      i. On suppose par l'absurde que $\alpha > 0$. Justifier qu'il existe deux éléments g et g' de G tels que $\alpha < g < g' < 2\alpha$.
      ii. En considérant $g' - g$, aboutir à une contradiction, de sorte que $\alpha = 0$.
      iii. Soient $x < y$ deux réels. Montrer que $\left]0, \frac{y-x}{2}\right[\cap G \neq \emptyset$.
      En déduire que $]x, y[\cap G \neq \emptyset$, puis que G est dense dans $\mathbf{R}$.
3. Montrer qu'un sous-anneau A de $(\mathbf{R}, +, \times)$ est dense dans $\mathbf{R}$ si et seulement si $A \cap]0, 1[\neq \emptyset$.

▸ Exercice : $SL_2(\mathbf{Z})$ est engendré par deux éléments

Dans cet exercice, on note $SL_2(\mathbf{Z})$ l'ensemble des matrices M de $\mathcal{M}_2(\mathbf{R})$, dont tous les coefficients sont entiers, et telles que $\det(M) = 1$.

On note $S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ et $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, dont il est clair qu'il s'agit de deux éléments de $SL_2(\mathbf{Z})$.

Pour $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbf{Z})$, on note $\mu(M) = |c|$.

On note également $\langle S, T \rangle$ l'ensemble des matrices $M \in SL_2(\mathbf{Z})$ telles qu'il existe $n \in \mathbf{N}^*$ et des entiers relatifs $a_1, \dots, a_n, b_1, \dots, b_n$ tels que $M = S^{a_1} T^{b_1} S^{a_2} T^{b_2} \cdots S^{a_n} T^{b_n}$.

1. Montrer que $SL_2(\mathbf{Z})$ est un sous-groupe de $(GL_2(\mathbf{R}), \times)$.
2. Pour tout $k \in \mathbf{Z}$, calculer T^k et S^k.
3. Montrer que si H est un sous-groupe de $SL_2(\mathbf{Z})$ tel que $S \in H$ et $T \in H$, alors $\langle S, T \rangle \subset H$.
4. Montrer que $\langle S, T \rangle$ est un sous-groupe de $SL_2(\mathbf{Z})$.
   Autrement dit, $\langle S, T \rangle$ est le plus petit (au sens de l'inclusion) sous-groupe de $SL_2(\mathbf{Z})$, qui contient à la fois S et T.
5. Montrer que si $M \in SL_2(\mathbf{Z})$ est telle que $\mu(M) = 0$, alors $M \in \langle S, T \rangle$.
6. Soit $M \in SL_2(\mathbf{Z})$ telle que $\mu(M) > 0$. Montrer, à l'aide d'une division euclidienne, qu'il existe $k \in \mathbf{Z}$ tel que $\mu(ST^k M) < \mu(M)$.
7. En déduire que $SL_2(\mathbf{Z}) = \langle S, T \rangle$.

▸ Exercice : calcul de la somme d'une série alternée

Pour $n \in \mathbf{N}^*$, on note $u_n = (-1)^n \dfrac{\ln(n)}{n}$ et $w_n = \displaystyle\sum_{k=1}^{n} \frac{1}{k} - \ln(n)$.

1. **a.** Prouver que pour tout $x \geqslant 1$, $\frac{1}{x+1} \leqslant \ln\left(1 + \frac{1}{x}\right) \leqslant \frac{1}{x}$.
   b. En déduire que $\forall n \in \mathbf{N}^*$, $0 \leqslant w_n \leqslant 1$.
   c. Montrer alors que la suite $(w_n)_{n\geqslant 1}$ est convergente.
   Dans toute la suite de l'exercice, on notera γ la limite de $(w_n)_{n\geqslant 1}$.
2. Étudier les variations de la fonction $\varphi : t \mapsto \dfrac{\ln t}{t}$ sur $]0, +\infty[$. Dresser le tableau de variations de la fonction φ en précisant les limites aux bornes de son ensemble de définition.
3. On note pour tout entier $n \geqslant 1$, $S_n = \displaystyle\sum_{k=1}^{n} u_k$.
   a. Montrer que les suites $(S_{2n})_{n\geqslant 2}$ et $(S_{2n+1})_{n\geqslant 2}$ sont adjacentes.
   b. Prouver alors que $(S_n)_{n\geqslant 1}$ converge.
4. On note pour tout entier $n \geqslant 1$, $v_n = \displaystyle\sum_{k=1}^{n} \frac{\ln k}{k} - \frac{\left[\ln(n)\right]^2}{2}$.
   a. Justifier que pour tout entier $n \geqslant 3$, on a : $\dfrac{\ln(n+1)}{n+1} \leqslant \displaystyle\int_n^{n+1} \frac{\ln(t)}{t}\, dt$.
   b. En déduire que la suite $(v_n)_{n\geqslant 3}$ est décroissante et convergente.
5. Montrer que pour tout entier $n \geqslant 1$,
$$S_{2n} = 2\sum_{k=1}^{n} \frac{\ln(2k)}{2k} - \sum_{k=1}^{2n} \frac{\ln(k)}{k}$$
   puis que :
$$S_{2n} = \ln(2)\sum_{k=1}^{n} \frac{1}{k} + v_n - v_{2n} - \frac{\left[\ln(2)\right]^2}{2} - \ln(2)\ln(n).$$
6. Démontrer alors que : $\displaystyle\lim_{n\to+\infty} S_n = \gamma \ln(2) - \frac{\left[\ln(2)\right]^2}{2}$.

▸ Problème : Le grand théorème de Fermat pour $n = 4$

Au XVII[ème] siècle, Pierre de Fermat énonce un théorème qui en termes modernes (puisque Fermat l'a énoncé en latin) s'écrit :

> **Théorème :** *Pour $n \geqslant 3$, l'équation $x^n + y^n = z^n$ ne possède pas de solutions $(x, y, z) \in (\mathbf{N}^*)^3$.*

Notons que la précision que x, y et z sont non nuls n'est pas superflue puisque pour tout $x \in \mathbf{N}$, $x^n + 0^n = x^n$.

Ce problème a fasciné des générations de mathématiciens durant trois siècles et demi avant d'être prouvé en 1995 par Andrew Wiles, aidé par son élève Richard Taylor.
S'il n'est pas question d'aborder la preuve de ce théorème ici (vous connaissez l'histoire, elle ne tient ni dans la marge ni sur votre copie), nous nous proposons d'étudier dans ce problème les solutions à $x^2 + y^2 = z^2$, et de prouver le théorème de Fermat dans le cas $n = 4$.

1. Justifier que si le théorème de Fermat est vrai pour $n = 4$ et pour n premier impair, alors il est vrai pour tout $n \geqslant 3$.
2. **Un lemme utile** : soient a et b deux entiers non nuls. Montrer que si a^2 divise b^2, alors a divise b. *On pourra par exemple montrer que $a \wedge b = a$.*

Partie I : le cas $n = 2$

Dans le cas $n = 2$, il existe des solutions non triviales à l'équation $x^2 + y^2 = z^2$, la plus célèbre d'entre elles étant probablement $3^2 + 4^2 = 5^2$.
On cherche dans cette partie à déterminer tous les triplets $(x, y, z) \in (\mathbf{N}^*)^3$ tels que $x^2 + y^2 = z^2$.
Un tel triplet est appelé **triplet pythagoricien**. On parlera de **triplet pythagoricien primitif** si de plus $x \wedge y \wedge z = 1$.

3. Soit (x, y, z) un triplet pythagoricien, et soit $d = x \wedge y \wedge z$. On pose alors $x' = \frac{x}{d}, y' = \frac{y}{d}$ et $z' = \frac{z}{d}$.
   Justifier que (x', y', z') est un triplet pythagoricien primitif, et que x', y', z' sont deux à deux premiers entre eux.
4. Soit (x, y, z) un triplet pythagoricien primitif.
   a. Prouver que x et y ne sont pas tous deux pairs.
   À l'aide de congruences modulo 4, justifier que x et y ne sont pas tous deux impairs.

   Dans la suite, quitte à échanger x et y, on suppose que x est pair et y est impair.

   b. Justifier qu'il existe $(u, v, w) \in (\mathbf{N}^*)^3$ tels que $x = 2u$, $z + y = 2v$ et $z - y = 2w$.
   c. Montrer que $v \wedge w = 1$.
   d. Prouver que vw est un carré, en déduire que v et w sont des carrés.
   On pose alors $v = n^2$ et $w = m^2$, avec $(m, n) \in (\mathbf{N}^*)^2$.
   e. Montrer que $n > m$ et que n et m sont premiers entre eux.
5. Montrer que (x, y, z) est un triplet pythagoricien primitif si et seulement si il existe deux entiers n et m premiers entre eux, de parités distinctes, avec $n > m > 0$ tels que

$$\begin{cases} x = 2nm \\ y = n^2 - m^2 \\ z = n^2 + m^2 \end{cases} \quad \textbf{ou} \quad \begin{cases} x = n^2 - m^2 \\ y = 2nm \\ z = n^2 + m^2 \end{cases}$$

   En déduire tous les triplets pythagoriciens.

Partie II : le cas $n = 4$

Nous allons prouver dans cette partie que l'équation $x^4 + y^4 = z^2$ ne possède pas de solutions dans $(\mathbf{N}^*)^3$.
Pour cela on raisonne par l'absurde, en supposant qu'une telle solution existe, et on considère $(a, b, c) \in (\mathbf{N}^*)^3$ vérifiant $a^4 + b^4 = c^2$ et

$$c = \min\{k \in \mathbf{N}^* \mid \exists (p, q) \in (\mathbf{N}^*)^2, p^4 + q^4 = k^2\}.$$

Autrement dit, on suppose qu'on a un triplet (a, b, c) solution avec c minimal parmi les solutions.

6. Justifier que quitte à échanger a et b, il existe deux entiers m et n, premiers entre eux et de parités différentes, tels que $a^2 = 2mn$, $b^2 = n^2 - m^2$ et $c = n^2 + m^2$.
7. Calculer $m^2 + b^2$, et en déduire qu'il existe $p, q \in \mathbf{N}^*$, premiers entre eux, de parités différentes tels que $m = 2pq$, $b = p^2 - q^2$, $n = p^2 + q^2$.
8. En notant que $a^2 = 2mn = 4pqn$, prouver qu'il existe des entiers u, v, w tels que $p = u^2$, $q = v^2$ et $n = w^2$, et qu'alors $u^4 + v^4 = w^2$, avec $w < c$.
9. Conclure, et en déduire le théorème de Fermat pour $n = 4$.

CORRECTION DU DEVOIR SURVEILLÉ 5

▸ Exercice 1 : sous-groupes et sous-anneaux de R.

1. On a bien $0 = \alpha 0 \in \alpha\mathbf{Z}$.
Soient $x, y \in \alpha\mathbf{Z}$. Alors il existe deux entiers $n, p \in \mathbf{Z}$ tels que $x = \alpha n + \alpha p$, et donc $x + y = \alpha(n+p) \in \alpha\mathbf{Z}$.
Donc $\alpha\mathbf{Z}$ est stable par somme.
Enfin, si $x \in \alpha\mathbf{Z}$, alors il existe $n \in \mathbf{Z}$ tel que $x = \alpha n$, et donc $-x = \alpha(-n) \in \alpha\mathbf{Z}$.
Donc $\alpha\mathbf{Z}$ est stable par passage à l'inverse.
Et par conséquent, $\boxed{\alpha\mathbf{Z} \text{ est un sous-groupe de } (\mathbf{R}, +).}$

2.a. Puisque $G \neq \{0\}$, il existe $x \in G \cap \mathbf{R}^*$.
Si $x > 0$, alors $x \in G \cap \mathbf{R}_+^*$, qui est donc non vide.
Et si $x < 0$, alors $-x \in G$ (car G est un sous-groupe[1]) et $-x \in G \cap \mathbf{R}_+^*$.
Dans tous les cas, $G \cap \mathbf{R}_+^*$ est non vide.

[1] Et donc stable par inverse.

2.b.i. Une option est de faire une récurrence pour prouver que pour tout $k \in \mathbf{N}$, $k\alpha \in G$, puis de passer à l'inverse pour prouver que pour $k < 0$, $k\alpha \in G$.
Mais on peut simplement remarquer que $\alpha\mathbf{Z}$ est le sous-groupe de $(\mathbf{R}, +)$ engendré par α.
Puisqu'on sait que le sous-groupe engendré par un élément est toujours inclus dans le groupe de départ, $\alpha\mathbf{Z} \subset G$.

> **En effet**
> Ici la loi de groupe est notée additivement, donc ce qu'on notait usuellement x^n n'est rien d'autre que $nx = \underbrace{x + x + \cdots + x}_{n \text{ fois}}$.
> Et donc
> $\langle \alpha \rangle = \{k\alpha,\ k \in \mathbf{Z}\} = \alpha\mathbf{Z}$.

2.b.ii. Puisque $\left\lfloor \frac{g}{\alpha} \right\rfloor \alpha \in G$, $g - \left\lfloor \frac{g}{\alpha} \right\rfloor \alpha \in G$ par stabilité de G.
Or, par définition d'une partie entière, $\left\lfloor \frac{g}{\alpha} \right\rfloor \leqslant \frac{g}{\alpha} < \left\lfloor \frac{g}{\alpha} \right\rfloor + 1$, donc $\left\lfloor \frac{g}{\alpha} \right\rfloor \alpha \leqslant g < \left\lfloor \frac{g}{\alpha} \right\rfloor \alpha + \alpha$, et donc

$$0 \leqslant g - \left\lfloor \frac{g}{\alpha} \right\rfloor \alpha < \alpha.$$

Ainsi $g - \left\lfloor \frac{g}{\alpha} \right\rfloor \alpha$ est un élément de $G \cap \mathbf{R}_+$, strictement inférieur à α.
Et donc il ne peut être dans $\mathbf{R}_+^*$, car ceci contredirait la minimalité de α.
Donc $g - \left\lfloor \frac{g}{\alpha} \right\rfloor \alpha = 0 \Leftrightarrow g = \left\lfloor \frac{g}{\alpha} \right\rfloor \alpha \in \alpha\mathbf{Z}$.
Ainsi, $\boxed{G = \alpha\mathbf{Z}.}$

> **Détails**
> $\alpha \in G$ et $\left\lfloor \frac{g}{\alpha} \right\rfloor \in \mathbf{Z}$ donc $\left\lfloor \frac{g}{\alpha} \right\rfloor \alpha \in G$. Puis $g \in G$ donc $g - \left\lfloor \frac{g}{\alpha} \right\rfloor \alpha \in G$.

2.c.i. La caractérisation epsilonesque des bornes inférieures, avec $\varepsilon = \alpha$ prouve qu'il existe $g' \in G$ tel que $\alpha \leqslant g' < 2\alpha$.
Puisque par ailleurs, $G \cap \mathbf{R}_+^*$ n'a pas de minimum, $\alpha < g'$. Mais alors g' n'est pas un minorant de $G \cap \mathbf{R}_+^*$, donc il existe $g \in G$ tel que $\alpha \leqslant g < g'$. Et comme précédemment, $g \neq \alpha$, si bien que $\boxed{\alpha < g < g' < 2\alpha.}$

2.c.ii. On a donc $g' - g \in G$ car G est un sous-groupe, et $0 < g' - g < 2\alpha - \alpha = \alpha$.
Ceci contredit la définition de α, qui doit être un minorant de $G \cap \mathbf{R}_+^*$. Donc $\boxed{\alpha = 0.}$

2.d. Si $\left]0, \frac{y-x}{2}\right[\cap G$ était vide, cela signifierait que tout élément strictement positif de G est supérieur ou égal à $\frac{y-x}{2}$.
Donc que $G \cap \mathbf{R}_+^*$ est minoré par $\frac{y-x}{2} > 0$.
Par conséquent, sa borne inférieure[2] serait supérieure ou égale à $\frac{y-x}{2}$, et donc supérieure stricte à 0, ce qui n'est pas le cas par la question précédente.
Donc $\left]0, \frac{y-x}{2}\right[\cap G \neq \emptyset$.
Soit donc t un élément de cette intersection.
Alors $z = \underbrace{\left\lfloor \frac{x}{t} \right\rfloor}_{\in \mathbf{Z}} t + t$ est dans G car G est un sous-groupe.
Mais alors on a $x < z \leqslant x + t < y$, et donc $z \in]x, y[$.
Donc tout intervalle ouvert non vide de $\mathbf{R}$ contient un élément de G : $\boxed{G \text{ est dense dans } \mathbf{R}.}$

[2] Qui, rappelons-le, est le plus grand des minorants.

3. Soit A un sous-anneau de $\mathbf{R}$.
Si A est dense dans $\mathbf{R}$, alors tout intervalle ouvert non vide de $\mathbf{R}$ rencontre A, et en particulier, $A \cap]0,1[\neq \emptyset$.

Inversement, si A est un sous-anneau de $\mathbf{R}$ tel que $A \cap]0,1[\neq \emptyset$.
Alors en particulier, A est un sous-groupe de $(\mathbf{R},+)$, non réduit à $\{0\}$ puisqu'il contient 1.
Et donc soit il possède un plus petit élément strictement positif α, soit il est dense dans $\mathbf{R}$.
Supposons par l'absurde que $A \cap \mathbf{R}_+^*$ possède un plus petit élément α, qui est donc nécessairement dans $]0,1[$.
Considérons alors $q \in A \cap]0,1[$. Par stabilité de A par produit, pour tout $n \in \mathbf{N}$, $q^n \in A$.
Or, $q^n \underset{n\to+\infty}{\longrightarrow} 0$, et donc il existe $n_0 \in \mathbf{N}$ tel que $0 < q^{n_0} < \alpha$, ce qui est absurde.
Donc A est dense dans $\mathbf{R}$.
Par double implication, $\boxed{A \text{ est dense dans } \mathbf{R} \text{ si et seulement si } A \cap]0,1[\neq \emptyset.}$

▸ Exercice 2 : $SL_2(\mathbf{Z})$ est engendré par deux éléments

1. Commençons par noter que les matrices de $SL_2(\mathbf{Z})$ étant de déterminant $1 \neq 0$, elles sont toutes inversibles, et donc $SL_2(\mathbf{Z}) \subset GL_2(\mathbf{R})$.
Par ailleurs, $I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ est bien de déterminant 1.
Et si P, Q sont deux matrices de $SL_2(\mathbf{Z})$, alors il est clair que PQ est encore à coefficients entiers, et puisque $\det(PQ) = \det(P)\det(Q) = 1$, on a bien $PQ \in SL_2(\mathbf{Z})$.
Et pour $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbf{Z})$, on a $A^{-1} = \dfrac{1}{\det(A)} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} \in SL_2(\mathbf{Z})$.
Donc $\boxed{SL_2(\mathbf{Z}) \text{ est bien un sous-groupe de } (GL_2(\mathbf{R}), \times).}$

2. Une récurrence facile prouve que pour tout $k \in \mathbf{N}$, $T^k = \begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix}$.
Son inverse étant $\begin{pmatrix} 1 & -b \\ 0 & 1 \end{pmatrix}$, on a donc $T^{-k} = \begin{pmatrix} 1 & -k \\ 0 & 1 \end{pmatrix}$.
Et donc $\boxed{\text{pour tout } k \in \mathbf{Z},\ T^k = \begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix}.}$
Par ailleurs, $S^2 = -I_2$, et donc $S^3 = -S$ et $S^4 = I_2$.
Pour $k \in \mathbf{Z}$, si on note $k = 4q + r$ la division euclidienne de k par 4, avec $0 \leqslant r \leqslant 3$, on a donc $S^k = S^{4q+r} = (S^4)^q S^r = S^r$.
Et donc $\boxed{S^k = \begin{cases} I_2 & \text{si } k \equiv 0\ [4] \\ S & \text{si } k \equiv 1\ [4] \\ -I_2 & \text{si } k \equiv 2\ [4] \\ -S & \text{si } k \equiv 3\ [4] \end{cases}}$

> **Ordre fini**
> Pour le dire autrement, S est un élément d'ordre 4 du groupe $SL_2(\mathbf{Z})$.

3. Soit H un sous-groupe de $SL_2(\mathbf{Z})$ qui contient S et T. Alors $\langle S \rangle = \{S^k,\ k \in \mathbf{Z}\} \subset H$, et de même, pour tout $k \in \mathbf{Z}$, $T^k \in H$.
Et donc pour $a_1, \dots, a_n, b_1, \dots, b_n \in \mathbf{Z}$, $S^{a_1}, \dots, S^{a_n}, T^{b_1}, \dots, T^{b_n}$ sont dans H, si bien que par stabilité de H par produit, $S^{a_1}T^{a_1}S^{a_2}T^{b_2} \cdots S^{a_n}T^{b_n} \in H$.
Ainsi, $\langle S, T \rangle \subset H$.

> **Rappel**
> Un sous-groupe qui contient g contient $\langle g \rangle$, et donc contient tous les g^k, pour $k \in \mathbf{Z}$.

4. On a $I_2 = S^0T^0 \in \langle S, T \rangle$.
Soient $M, N \in \langle S, T \rangle$. Alors il existe deux entiers naturels non nuls m et n et des entiers relatifs $a_1, \dots, a_n, b_1, \dots, b_n, c_1, \dots, c_m, d_1, \dots, d_m$ tels que

$$M = S^{a_1}T^{a_1} \cdots S^{a_n}T^{a_n} \text{ et } N = S^{c_1}T^{d_1} \cdots S^{c_m}T^{d_m}.$$

Et donc $MN = S^{a_1}T^{b_1} \cdots S^{a_n}T^{a_n}S^{c_1}T^{d_1} \cdots S^{c_m}T^{b_m} \in \langle S, T \rangle$.
Enfin, on a

$$M^{-1} = T^{-b_n}S^{-a_n}T^{-b_{n-1}}S^{-a_{n-1}} \cdots T^{-b_1}S^{-a_1} = S^0T^{-b_n}S^{-a_n}T^{-b_{n-1}}S^{-a_{n-1}} \cdots T^{-b_1}S^{-a_1}T^0 \in \langle S, T \rangle.$$

Ainsi, $\langle S, T \rangle$ est stable par produit et par inverse, et donc $\boxed{\text{est un sous-groupe de } SL_2(\mathbf{Z}).}$

5. Soient $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbf{Z})$. Alors $\mu(M) = 0 \Leftrightarrow c = 0$.
Puisque $\det(M) = 1$, on a $ad = 1$, donc $a = d = 1$ ou $a = d = -1$.
► Si $a = d = 1$, alors $M = \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} = T^b \in \langle S, T\rangle$.

► Et si $a = d = -1$, alors $S^2M = -M = \begin{pmatrix} 1 & -b \\ 0 & 1 \end{pmatrix} = T^{-b}$, si bien que $M = S^{-2}T^{-b} \in \langle S, T\rangle$.

6. Soit $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbf{Z})$.
Alors pour tout $k \in \mathbf{Z}$,

$$ST^kM = \begin{pmatrix} 0 & -1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 0 & -1 \\ 1 & k \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} -c & -d \\ a+kc & c+kd \end{pmatrix}.$$

Puisque $\mu(M) = |c| \neq 0$, on a soit $c > 0$, soit $c < 0$.

► Si $c > 0$, notons $a = qc + r$ la division euclidienne de a par c, avec $0 \leqslant r < c$.
Alors $ST^{-q}M = \begin{pmatrix} -c & -d \\ a-qc & c+dq \end{pmatrix} = \begin{pmatrix} -c & -d \\ r & c+dq \end{pmatrix}$, avec $\mu(ST^{-q}M) = r < \mu(M)$.

► Si $c < 0$, notons $a = q(-c) + r$ la division euclidienne de a par $-c$, avec $0 \leqslant r < -c$.
Alors $ST^qM = \begin{pmatrix} -c & -d \\ a+qc & c+qd \end{pmatrix} = \begin{pmatrix} c & d \\ r & c+qd \end{pmatrix}$, avec $\mu(ST^qM) = r < |c|$.

7. Puisqu'on a déjà $\langle S, T\rangle \subset SL_2(\mathbf{Z})$, prouvons l'inclusion réciproque.
Supposons par l'absurde qu'il existe $M \in SL_2(\mathbf{Z})$ telle que $M \notin \langle S, T\rangle$.
Alors il existe un entier $k_1 \in SL_2(\mathbf{Z})$ tel que $M_1 = ST^{k_1}M$ vérifie $\mu(M_1) < \mu(M)$.
Mais on ne peut alors pas avoir $M_1 \in \langle S, T\rangle$, faute de quoi on aurait $M = T^{-k_1}S^{-1}M_1 \in \langle S, T\rangle$.
Donc il existe $k_2 \in \mathbf{Z}$ tel que si on note $M_2 = ST^{k_2}M_1$, $\mu(M_2) < \mu(M_1)$. Et de même, $M_2 \notin \langle S, T\rangle$.
De proche en proche, on peut construire une suite $(M_k)_{k\geqslant 1}$ de matrices de $SL_2(\mathbf{Z})$, telles que pour tout $k \in \mathbf{N}^*$, $\mu(M_{k+1}) < \mu(M_k)$.
Donc $(\mu(M_k))_{k\geqslant 1}$ est une suite strictement décroissante d'entiers naturels, ce qui est absurde.

Alternative : un moyen convaincant de rédiger ceci est le suivant : supposons par l'absurde que $\langle S, T\rangle \neq SL_2(\mathbf{Z})$. Alors $\{\mu(M),\ M \in SL_2(\mathbf{Z}) \setminus \langle S, T\rangle\}$ est une partie non vide de $\mathbf{N}$.
Elle possède donc un plus petit élément c, et soit $M \in SL_2(\mathbf{Z}) \setminus \langle S, T\rangle$ telle que $\mu(M) = c$.
Alors par la question 5, $\mu(M) \neq 0$, et donc par la question 6, il existe $k \in \mathbf{Z}$ tel que $\mu(ST^kM) < c$.
Par définition de c, on a donc $ST^kM \in \langle S, T\rangle$. Et donc $M = T^{-k}S^{-1}(ST^kM) \in \langle S, T\rangle$, ce qui est absurde.
Et donc $\boxed{SL_2(\mathbf{Z}) = \langle S, T\rangle.}$

► Exercice : calcul de la somme d'une série alternée (d'après concours ECS 2016)

1.a. Notons f la fonction définie sur $[1, +\infty[$ par $f(x) = \ln\left(1 + \frac{1}{x}\right) - \frac{1}{x+1}$.
Alors f est dérivable, de dérivée égale à $f' : x \mapsto -\frac{1}{x(x+1)} + \frac{1}{(x+1)^2}$, de sorte que f' est négative sur $[1, +\infty[$, et donc f est décroissante sur ce même intervalle.
Lorsque $x \to +\infty$, $f(x) \underset{x\to+\infty}{\longrightarrow} \ln(1) = 0$.

On en déduit que f est positive sur $[1, +\infty[$, et donc que $\boxed{\text{pour tout } x \geqslant 1,\ \ln\left(1 + \frac{1}{x}\right) \geqslant \frac{1}{x+1}.}$

L'inégalité $\ln\left(1 + \frac{1}{x}\right) \leqslant \frac{1}{x}$ a quant à elle été prouvée en cours.

1.b. Soit $n \in \mathbf{N}^*$. Alors pour tout $k \in [\![1, n]\!]$, $\dfrac{1}{k+1} \leqslant \ln\left(1 + \dfrac{1}{k}\right) \leqslant \dfrac{1}{k}$.
Et donc en sommant ces relations,

$$\sum_{k=1}^{n} \frac{1}{k+1} \leqslant \sum_{k=1}^{n} \ln\left(1 + \frac{1}{k}\right) \leqslant \sum_{k=1}^{n} \frac{1}{k}.$$

Notons que $\ln\left(1+\frac{1}{k}\right) = \ln\left(\frac{k+1}{k}\right) = \ln(k+1)-\ln(k)$, si bien que la somme $\sum_{k=1}^{n} \ln\left(1+\frac{1}{k}\right)$ est télescopique :

$$\sum_{k=1}^{n} \ln\left(1+\frac{1}{k}\right) = \sum_{k=1}^{n} \left[\ln(k+1)-\ln(k)\right] = \ln(n+1)-\ln(1) = \ln(n+1).$$

Donc $\sum_{k=1}^{n} \frac{1}{k+1} \leqslant \ln(n+1) \leqslant \sum_{k=1}^{n} \frac{1}{k}$.
De la seconde inégalité, on déduit $w_n \geqslant \ln(n+1)-\ln(n) \geqslant 0$.
Et la première, en remplaçant n par $n-1$, nous donne

$$\sum_{k=1}^{n-1} \frac{1}{k+1} \leqslant \ln(n) \Leftrightarrow \sum_{k=2}^{n} \frac{1}{k} - \ln(n) \leqslant 0 \Leftrightarrow \boxed{w_n \leqslant 1.}$$

1.c. Pour $n \in \mathbf{N}^*$, on a

$$w_{n+1}-w_n = \sum_{k=1}^{n+1} \frac{1}{k} - \ln(n+1) - \sum_{k=1}^{n} \frac{1}{k} + \ln(n) = \frac{1}{n+1} - \ln\left(\frac{n+1}{n}\right) = \frac{1}{n+1} - \ln\left(1+\frac{1}{n}\right) \leqslant 0.$$

Donc (w_n) est décroissante, et étant minorée par 0, elle est donc convergente.

2. La fonction φ est dérivable sur $]0,+\infty[$, de dérivée égale à $\varphi' : t \mapsto \frac{1-\ln(t)}{t^2}$.
Et donc $\varphi'(t) \geqslant 0 \Leftrightarrow 1-\ln(t) \geqslant 0 \Leftrightarrow t \leqslant e$.
De plus, on a $\lim_{t\to 0^+} \varphi(t) = -\infty$ et par croissances comparées, $\lim_{t\to+\infty} \varphi(t) = 0$.
Le tableau de variations de φ est donc donné par

t	0		e		$+\infty$
$\varphi'(t)$	‖	$+$	0	$-$	
$\varphi(t)$	‖ $-\infty$	↗	e^{-1}	↘	0

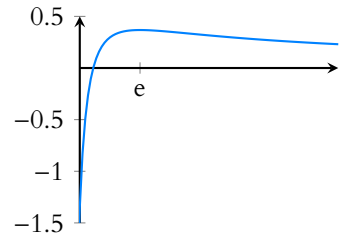

FIGURE 0.1– Représentation graphique

3.a. On a, pour $n \geqslant 2$,

$$S_{2n} - S_{2(n+1)} = S_{2n} - S_{2n+2} = \sum_{k=1}^{2n} \frac{(-1)^k \ln(k)}{k} - \sum_{k=1}^{2n+2} \frac{(-1)^k \ln(k)}{k}$$
$$= \frac{\ln(2n+1)}{2n+1} - \frac{\ln(2n+2)}{2n+2} = \varphi(2n+1) - \varphi(2n+2).$$

Danger !
$(S_{2n})_n$ n'est formée que des termes d'ordre pair de $(S_n)_n$, donc le terme suivant S_{2n} est bien $S_{2n+2} = S_{2(n+1)}$, et surtout pas S_{2n+1}.

Mais pour $n \geqslant 2$, on a $2n+1 \geqslant 3 > e$. La fonction φ étant décroissante sur $[e,+\infty[$, il vient $\varphi(2n+1) \geqslant \varphi(2n+2)$ et donc $S_{2n} - S_{2n+2} \geqslant 0$: $(S_{2n})_{n\geqslant 2}$ est décroissante.
De même,

$$S_{2n+1} - S_{2(n+1)+1} = \varphi(2n+3) - \varphi(2n+2) \leqslant 0$$

et donc $(S_{2n+1})_{n\geqslant 2}$ est croissante. Enfin,

$$S_{2n+1} - S_{2n} = \sum_{k=2}^{2n+1} u_k - \sum_{k=2}^{2n} u_k = u_{2n} = \frac{\ln(2n)}{2n} \xrightarrow[n\to+\infty]{} 0.$$

Ainsi, $\boxed{\text{les suites } (S_{2n})_{n\geqslant 2} \text{ et } (S_{2n+1})_{n\geqslant 2} \text{ sont adjacentes.}}$

3.b. Deux suites adjacentes sont convergentes et de même limite, donc les suites $(S_{2n})_{n\geqslant 2}$ et $(S_{2n+1})_{n\geqslant 2}$ convergent vers une même limite ℓ.
Or, il s'agit des suites extraites des termes d'ordre pair (resp. impair) de la suite $(S_n)_{n\geqslant 4}$.
Celle-ci est donc convergente, de limite ℓ.

4.a. La fonction φ est décroissante sur $[3,+\infty[$, donc pour tout $t \in [n,n+1]$, $\varphi(t) \geqslant \varphi(n+1)$. Alors, par croissance de l'intégrale,

$$\int_n^{n+1} \varphi(t)\,dt \geqslant \int_n^{n+1} \varphi(n+1)\,dt \geqslant \varphi(n+1)$$

soit encore $\boxed{\dfrac{\ln(n+1)}{n+1} \leqslant \displaystyle\int_n^{n+1} \frac{\ln(t)}{t}\,dt.}$

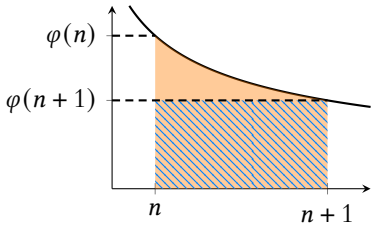

FIGURE 0.2– L'intégrale, qui est l'aire de la partie colorée est plus grande que l'aire de la partie hachurée, qui vaut $\varphi(n+1)$ (c'est l'aire d'un rectangle de largeur 1 et de hauteur $\varphi(n+1)$).

4.b. Pour $n \geqslant 3$, on a

$$\begin{aligned} v_{n+1}-v_n &= \sum_{k=1}^{n+1} \frac{\ln(k)}{k} - \frac{\left[\ln(n+1)\right]^2}{2} - \sum_{k=1}^{n} \frac{\ln(k)}{k} + \frac{\left[\ln(n)\right]^2}{2} \\ &= \frac{\ln(n+1)}{n+1} + \frac{\left[\ln(n)\right]^2 - \left[\ln(n+1)\right]^2}{2} \\ &= \frac{\ln(n+1)}{n+1} - \int_n^{n+1} \frac{\ln t}{t}\,dt \\ &\leqslant 0. \end{aligned}$$

Donc $\boxed{\text{la suite } (v_n)_{n\geqslant 3} \text{ est décroissante.}}$

Comme à la question 4.a, on prouve que pour tout entier $k \geqslant 3$, on a $\dfrac{\ln k}{k} \geqslant \displaystyle\int_k^{k+1} \frac{\ln t}{t}\,dt$.

Et alors, pour $n \geqslant 3$, on a

$$\begin{aligned} v_n &= \sum_{k=1}^{n} \frac{\ln k}{k} - \frac{\left[\ln(n)\right]^2}{2} \\ &= \frac{\ln 2}{2} + \sum_{k=3}^{n} \frac{\ln k}{k} - \frac{[\ln(n)]^2}{2} \\ &\geqslant \frac{\ln 2}{2} + \sum_{k=3}^{n} \int_k^{k+1} \frac{\ln t}{t}\,dt - \frac{[\ln(n)]^2}{2} \\ &\geqslant \frac{\ln 2}{2} + \int_3^{n+1} \frac{\ln t}{t}\,dt \\ &\geqslant \frac{\ln 2}{2} + \frac{[\ln(n+1)]^2}{2} - \frac{[\ln(3)]^2}{2} - \frac{[\ln(n)]^2}{2} \\ &\geqslant \frac{\ln 2}{2} - \frac{[\ln(3)]^2}{2}. \end{aligned}$$

Ainsi, la suite $(v_n)_{n\geqslant 3}$ est minorée, et par le théorème de la limite monotone, elle est donc $\boxed{\text{convergente.}}$

Primitive

On a

$$\frac{\ln t}{t} = \frac{1}{t}\ln t.$$

On reconnaît donc une fonction de la forme $u'u$, dont une primitive est alors donnée par $t \mapsto \dfrac{[\ln t]^2}{2}$.

5. Partons de l'expression proposée :

$$\begin{aligned} 2\sum_{k=1}^{n} \frac{\ln(2k)}{2k} - \sum_{k=1}^{2n} \frac{\ln(k)}{k} &= 2\sum_{k=1}^{n} \frac{\ln(2k)}{2k} - \sum_{k=1}^{n} \frac{\ln(2k)}{2k} - \sum_{k=0}^{n-1} \frac{\ln(2k+1)}{2k+1} \\ &= \sum_{k=1}^{n} \frac{\ln(2k)}{2k} - \sum_{k=0}^{n-1} \frac{\ln(2k+1)}{2k+1} \\ &= \sum_{k=1}^{2n} \frac{(-1)^k \ln(k)}{k} = \boxed{S_{2n}.} \end{aligned}$$

Détails

On a séparé la seconde somme en deux sommes, formées respectivement des k pairs et des k impairs.

On en déduit alors que

$$\begin{aligned} S_{2n} &= \sum_{k=1}^{n} \frac{\ln(2)+\ln(k)}{k} - \sum_{k=1}^{2n} \frac{\ln(k)}{k} \\ &= \ln(2)\sum_{k=1}^{n} \frac{1}{k} + \sum_{k=1}^{n} \frac{\ln(k)}{k} - \sum_{k=1}^{2n} \frac{\ln(k)}{k} \end{aligned}$$

$$= \ln(2)\sum_{k=1}^{n}\frac{1}{k} + v_n + \frac{\left[\ln(n)\right]^2}{2} - v_{2n} - \frac{\left[\ln(2n)\right]^2}{2}$$
$$= \ln(2)\sum_{k=1}^{n}\frac{1}{k} + v_n - v_{2n} + \frac{\ln(n)^2 - (\ln(2)+\ln(n))^2}{2}$$
$$= \ln(2)\sum_{k=1}^{n}\frac{1}{k} + v_n - v_{2n} + \frac{\ln(n)^2 - \ln(2)^2 + 2\ln(2)\ln(n) - \ln(n)^2}{2}$$
$$= \boxed{\ln(2)\sum_{k=1}^{n}\frac{1}{k} + v_n - v_{2n} + \ln(2)\ln(n) - \frac{\left[\ln 2\right]^2}{2}.}$$

6. De la dernière égalité, il vient

$$S_{2n} = \ln(2)\left(\sum_{k=1}^{n}\frac{1}{k} - \ln(n)\right) + v_n - v_{2n} - \frac{\left[\ln(2)\right]^2}{2}.$$

Mais si l'on note λ la limite de la suite (v_n), il vient alors, en passant à la limite[3] dans cette égalité

$$\lim_{n\to+\infty} S_{2n} = \ln(2)\gamma + \lambda - \lambda - \frac{\left[\ln(2)\right]^2}{2} = \boxed{\gamma\ln(2) - \frac{\left[\ln(2)\right]^2}{2}.}$$

[3] Tous les termes admettent une limite lorsque $n \to +\infty$, donc le passage à la limite est bien justifié.

▸ Problème : Le grand théorème de Fermat pour $n = 4$

1. Supposons le théorème de Fermat vrai pour les exposants premiers impairs et pour 4.
Soit $n \geqslant 3$. Supposons par l'absurde qu'il existe $(x, y, z) \in (\mathbf{N}^*)^3$ tels que $x^n + y^n = z^n$.
Alors soit n possède un facteur premier impair p, et donc il existe $k \in \mathbf{N}$ tel que $n = kp$.
Et alors $(x^k)^p + (y^k)^p = (z^k)^p$, ce qui est impossible puisque le théorème de Fermat est vrai pour p.
Soit n ne possède que 2 comme facteur premier, et étant supérieur à 3, il est divisible par 4 : il existe $k \in \mathbf{N}^*$ tel que $n = 4k$.
Et alors comme précédemment, $(x^k)^4 + (y^k)^4 = (z^k)^4$, ce qui est également absurde.
Donc si le théorème de Fermat est vrai pour les exposants premiers impairs et pour 4, alors il est vrai pour tout $n \geqslant 3$.

2. Soient donc a et b tels que $a^2 \mid b^2$. Notons alors $d = a \wedge b$, et soient a', b' deux entiers premiers entre eux tels que $a = da'$ et $b = db'$.
Alors $b^2 = d^2b'^2$ est divisible par $a^2 = d^2a'^2$, si bien que $a'^2 \mid b'^2$.
Or a' et b' étant premiers entre eux, il en est de même de a'^2 et b'^2.
Et donc a'^2 est un diviseur commun de a'^2 et de b'^2, et donc divise leur pgcd qui vaut 1.
Ainsi, $a'^2 = 1$, si bien que $a' = 1$, et donc $d = a$, ce qui prouve que $a \mid b$.

> **Rappel**
> Un entier est premier avec un produit si et seulement si il est premier avec chacun de ses facteurs.

Alternative : on peut également utiliser des valuations p-adiques pour prouver ce résultat : pour tout premier p, on sait que $v_p(a^2) \leqslant v_p(b^2)$, soit encore $2v_p(a) \leqslant 2v_p(b)$, et donc $v_p(a) \leqslant v_p(b)$.
Et ceci étant vrai pour tout nombre premier, $a \mid b$.

Partie I : le cas $n = 2$ (triplets pythagoriciens)

3. Il est évident que x', y' et z' sont premiers entre eux dans leur ensemble.
On a alors $x'^2 + y'^2 = \frac{1}{d^2}(x^2 + y^2) = \frac{z^2}{d^2} = z'^2$.
Donc $\boxed{(x', y', z') \text{ est un triplet pythagoricien primitif.}}$

> **Attention**
> On n'a à ce stade pas complètement répondu à la question, puisque x', y' et z' pourraient encore ne pas être **deux à deux** premiers.

Soit k un diviseur commun à x' et y'. Alors k^2 divise $x'^2 + y'^2 = z'^2$. Par la question 2, on a donc $k \mid z'$, et donc k est un diviseur commun de x', y' et z'. Puisque ces entiers sont premiers entre eux dans leur ensemble, k divise 1, et donc $k = 1$. En particulier, $x' \wedge y' = 1$.

Sur le même principe, un diviseur commun de x' et de z' est un diviseur de y' à l'aide de la relation $y'^2 = z'^2 - x'^2$, et donc x' et z' sont premiers entre eux.
Donc x', y', z' sont deux à deux premiers entre eux.

4.a. Nous venons de prouver que si (x, y, z) est un triplet pythagoricien primitif, alors x et y sont premiers entre eux, et donc ne peuvent être tous deux multiples de 2.
Si k est un entier impair, alors $k \equiv 1\ [4]$ ou $k \equiv 3\ [4]$, et dans les deux cas, $k^2 \equiv 1\ [4]$.
Supposons par l'absurde que x et y sont impairs tous les deux. Alors $x^2 + y^2 \equiv 2\ [4]$.
Or, $x^2 + y^2 = z^2$, et modulo 4 un carré vaut 0 ou 1, d'où une contradiction.
Ainsi, $\boxed{x \text{ et } y \text{ sont de parités opposées.}}$

4.b. Puisque x est pair, il existe $u \in \mathbf{N}^*$ tel que $x = 2u$.
Donc z^2 est de même parité que y^2, donc[4] z et y sont de même parité, et donc $z+y$ et $z-y$ sont pairs.
Il existe donc $v \in \mathbf{N}^*$ tel que $z + y = 2v$.
Enfin, $z^2 = y^2 + x^2 > y^2$, donc $z > y$, de sorte que $z - y > 0$.
Et donc il existe $w \in \mathbf{N}^*$ tel que $z - y = 2w$.

[4] Un entier et son carré sont toujours de même parité.

4.c. Soit d un diviseur commun à v et w.
Alors $d \mid z + y$ et $d \mid z - y$, donc $d^2 \mid (z + y)(z - y) = z^2 - y^2 = x^2$. Par conséquent[5], $d \mid x$.
Ainsi, d divise $x \wedge y \wedge z = 1$, et donc $d = 1$. On a donc prouvé que $\boxed{v \wedge w = 1.}$

[5] C'est encore la question 2.

4.d. On a $4vw = y^2 - z^2 = x^2 = 4u^2$ et donc $vw = u^2$ $\boxed{\text{est un carré.}}$
Alors pour tout premier p, $v_p(vw) = v_p(u^2) = 2v_p(u)$.
Mais v et w étant premiers entre eux, $v_p(v) = 0$ ou $v_p(w) = 0$.
Et donc soit $v_p(v) = 0$, et alors $v_p(w)$ est pair, soit $v_p(w) = 0$ et alors $v_p(v)$ est pair.
Ainsi, pour tout premier p, $v_p(v)$ et $v_p(w)$ sont pairs, et donc il existe a_p, b_p entiers tels que $v_p(v) = 2a_p$ et $v_p(w) = 2b_p$.
Et alors

$$v = \left(\prod_{p\in\mathcal{P}} p^{a_p}\right)^2 \text{ et } w = \left(\prod_{p\in\mathcal{P}} p^{b_p}\right)^2$$

sont des carrés.

4.e. Puisque $y \neq 0$, $z + y > z - y$, et donc $2n^2 > 2m^2$, donc $n > m$.
Par ailleurs, tout diviseur commun à m et n est un diviseur commun à $v = n^2$ et $w = m^2$, et donc est un diviseur de $v \wedge w = 1$.
Donc $\boxed{m \wedge n = 1.}$

5. Nous venons de prouver que si (x, y, z) est primitif, alors il est bien de l'une des deux[6] formes annoncées.
En effet, dans le cas où, comme dans les questions précédentes, x est pair, alors
$x^2 = z^2 - y^2 = \left(n^2 + m^2\right)^2 - \left(n^2 - m^2\right)^2 = 4n^2m^2$ et donc $x = 2mn$.
Un seul point n'a alors pas été prouvé : c'est que m et n sont de parités distinctes. Mais si m et n étaient de même parité, alors m^2 et n^2 aussi, et donc y et z seraient tous deux pairs, contredisant le fait que $y \wedge z = 1$.

[6] La première si x est pair, la seconde sinon.

Inversement, reste à vérifier que pour $n > m$ premiers entre eux et de parités distinctes, $(x, y, z) = (2nm, n^2 - m^2, n^2 + m^2)$ est bien un triplet pythagoricien primitif. Mais

$$(2nm)^2 + (n^2 - m^2)^2 = 4^2n^2m^2 + n^4 - 2n^2m^2 + m^4 = n^4 + 2n^2m^2 + m^4 = (n^2 + m^2)^2.$$

Donc on est bien en présence d'un triplet pythagoricien. Il est primitif puisque si $d = x\wedge y\wedge z$, alors d est un diviseur commun à y et z, et donc aussi un diviseur de $2n^2 = z-y$ et $2m^2 = z+y$.
Mais puisque $n \wedge m = 1$, $n^2 \wedge m^2 = 1$, et donc $2n^2 \wedge 2m^2 = 2$.
Donc $d = 1$ ou $d = 2$. Or on ne peut pas avoir $d = 2$, car m et n étant de parités distinctes, il en est de même de m^2 et n^2, et donc de y et z.
Ainsi, $x \wedge y \wedge z = 1$, et donc (x, y, z) est un triplet pythagorien primitif.

Détails
Rappelons qu'un entier est premier avec un produit si et seulement si il est premier avec chacun des facteurs. Donc $m\wedge n = 1 \Rightarrow m\wedge n^2 = 1$ puis $m^2 \wedge n^2 = 1$.

Par la question 2, si (x, y, z) est un triplet pythagoricien, et si $d = x \wedge y \wedge z$, alors $\left(\frac{x}{d}, \frac{y}{d}, \frac{z}{d}\right)$ est un triplet pythagoricien primitif.
Donc il existe n, m premiers entre eux, de parités distinctes, avec $n > m$ tels que

$$\begin{cases} \frac{x}{d} = 2mn \\ \frac{y}{d} = n^2 - m^2 \\ \frac{z}{d} = n^2 + m^2 \end{cases} \Leftrightarrow \begin{cases} x = 2mnd \\ y = d(n^2 - m^2) \\ z = d(m^2 + n^2) \end{cases} \quad \textbf{ou} \quad \begin{cases} \frac{y}{d} = 2mn \\ \frac{x}{d} = n^2 - m^2 \\ z = n^2 + m^2 \end{cases} \Leftrightarrow \begin{cases} y = 2mnd \\ x = d(n^2 - m^2) \\ z = d(m^2 + n^2) \end{cases}$$

Et inversement, si $n > m$ sont premiers entre eux, de parités distinctes, et $d \in \mathbf{N}^*$ alors

$$(2mnd)^2 + \left(d\left(n^2-m^2\right)\right)^2 = d^2\left(n^4+4m^2n^2+m^4\right) = d^2\left(m^2+n^2\right)^2 = \left(d\left(n^2+m^2\right)\right)^2$$

de sorte que $\left(2mnd, d\left(n^2-m^2\right), d\left(n^2+m^2\right)\right)$ et $\left(d\left(n^2-m^2\right), 2mnd, d\left(n^2+m^2\right)\right)$ sont des triplets pythagoriciens.
Et donc les triplets pythagoriciens sont exactement les triplets de la forme

$$\left(2mnd, d\left(n^2-m^2\right), d\left(n^2+m^2\right)\right) \textbf{ ou } \left(d\left(n^2-m^2\right), 2mnd, d\left(n^2+m^2\right)\right)$$

avec $d \in \mathbf{N}^*$, $n > m$ premiers entre eux de parités distinctes.

Partie II : le cas $n = 4$

6. Commençons par noter que c n'est pas égal à 1 puisque $a^2 + b^2 \geqslant 2$.
Puisqu'il est clair que (a^2, b^2, c) est un triplet pythagoricien[7], montrons qu'il est primitif.
Si d est un diviseur commun de a et de b, alors d^4 divise $a^4 + b^4$, et donc $d^4 \mid c^2$.
Donc par la question 2, $d^2 \mid c$, si bien que $\left(\frac{a}{d}, \frac{b}{d}, \frac{c}{d^2}\right)$ est encore une solution de l'équation $x^4 + y^4 = z^2$.
Et puisque $\frac{c}{d^2} \leqslant c$, par minimalité de c, $c = \frac{c^2}{d^2}$, et donc $d = 1$.
Ainsi, a et b sont déjà premiers entre eux, donc a, b et c sont premiers entre eux dans leur ensemble, si bien que (a^2, b^2, c) est un triplet pythagoricien primitif.
Et donc par la partie I, a^2 et b^2 sont de parités opposées.
Quitte à les échanger, on peut supposer que c'est a^2 qui est pair, et donc a est pair.
Et la caractérisation des triplets pythagoriciens primitifs de la partie I nous assure alors de l'existence de trois réels m, n, p, avec $m \wedge n = 1$, m et n de parités contraires, tels que $a^2 = 2mn$, $b^2 = n^2 - m^2$ et $c^2 = n^2 + m^2$.

[7] Car $a^4 + b^4 = c^2$.

Rappel
Si on dispose de n entiers avec deux d'entre eux premiers, alors ces n entiers sont premiers entre eux dans leur ensemble.

7. On a alors $m^2 + b^2 = n^2$. Donc donc (m, b, n) est encore un triplet pythagoricien. Il est primitif puisqu'on sait déjà m et n premiers entre eux.
Donc par conséquent, il existe p, q premiers entre eux, de parités différentes, tels que $m = 2pq$, $b = p^2 - q^2$ et $n = p^2 + q^2$. .

Parités
a^2 et b^2 étant de parités opposées, et a^2 étant pair, b^2 est impair, et donc b aussi. Et donc des deux nombres m et b celui qui est pair doit être m.

8. Comme indiqué, on a bien $x^2 = 4pqn$. Puisque $m = 2pq$ est premier avec n, pq est premier avec n.
Donc par le même raisonnement qu'en 4.d, pq et n sont des carrés parfaits. Et p et q étant premiers entre eux, p et q sont aussi des carrés parfaits.
D'où l'existence de u, v, w tels que $p = u^2$, $q = v^2$ et $n = w^2$.
Puisque $n^2 = c - m^2 < c$, on a $w \leqslant w^2 < c$.
Et enfin, $u^4 + v^4 = p^2 + q^2 = n = w^2$. Donc (u, v, w) est encore solution de $x^4 + y^4 = z^2$.

9. La solution (u, v, w) que nous venons de construire vérifie $w < c$, ce qui contredit la minimalité de c. Et donc notre hypothèse de départ, à savoir l'existence de solutions non triviales est absurde, donc l'équation $x^4 + y^4 = z^2$ n'a pas de solutions dans $(\mathbf{N}^*)^3$.

Par conséquent, il n'existe pas non plus de triplets $(x, y, z) \in (\mathbf{N}^*)^3$ tels que $x^4 + y^4 = z^4$.

Commentaire historique *: l'idée globale dans ce qui précède est que si on a une solution (a, b, c), on peut en produire une autre, (a', b', c'), avec $c' < c$.*
Le procédé pourrait donc être itéré une infinité de fois, produisant une suite strictement décroissante d'entiers positifs, ce qui n'est pas possible. C'est ce que Fermat avait nommé le ***principe de descente infinie.***