Arithmétique : corrigés.

Le premier exercice de l'article d'Arithmétique est de montrer que cette définition est correcte :

Déf : Soit $n \in \mathbb{N} \setminus \{0,1\}$. Soient $a_1, \ldots, a_n \in \mathbb{N}$. Le plus grand commun diviseur de $a_1, \ldots, a_n$, noté $\mathrm{pgcd}(a_1, \ldots, a_n)$, est l'entier $d \in \mathbb{N}$ qui vérifie $d \mid a_1$, …, $d \mid a_n$ et si $c \mid a_1$, …, $c \mid a_n$ alors $c \mid d$.

Commençons par l'unicité :
Si d_1 et d_2 vérifient les propriétés de pgcd de $a_1, \ldots, a_n$ alors, comme $d_1 \mid a_1$, …, $d_1 \mid a_n$ on a $d_1 \mid d_2$ et comme $d_2 \mid a_1$, …, $d_2 \mid a_n$ on a $d_2 \mid d_1$.
Si $d_1 = 0$ alors comme $d_1 \mid d_2$ on a $d_2 = 0$. De même, si $d_2 = 0$ alors $d_1 = 0$.
Si $d_1 \neq 0$ et $d_2 \neq 0$ alors on a $d_1 \leq d_2$ et $d_1 \geq d_2$ (car $d_1 \mid d_2$ et $d_2 \mid d_1$) donc on a $d_1 = d_2$.
On a prouvé l'unicité du pgcd par disjonction de cas.

On va prouver l'existence du pgcd par récurrence sur n.
On a déjà prouvé l'existence pour $n = 2$.
Supposons que le pgcd de $n-1$ nombres existe.
On va vérifier que $\mathrm{pgcd}(\mathrm{pgcd}(a_1, \ldots, a_{n-1}), a_n)$ vérifie les conditions de la définition de $\mathrm{pgcd}(a_1, \ldots, a_n)$.
On remarque tout d'abord que c'est bien un entier naturel. $\mathrm{pgcd}(\mathrm{pgcd}(a_1, \ldots, a_{n-1}), a_n)$ divise a_n (cf. définition du pgcd). Soit $i \in \{1, \ldots, n-1\}$. $\mathrm{pgcd}(a_1, \ldots, a_{n-1})$ divise a_i et $\mathrm{pgcd}(\mathrm{pgcd}(a_1, \ldots, a_{n-1}), a_n)$ divise $\mathrm{pgcd}(a_1, \ldots, a_{n-1})$ donc $\mathrm{pgcd}(\mathrm{pgcd}(a_1, \ldots, a_{n-1}),$ divise a_i (si vous avez le moindre doute, explicitez ce que je viens d'écrire avec la définition de "diviser"). Soit $c \in \mathbb{N}$ tel que $c \mid a_1$, …, $c \mid a_n$. $c \mid a_1$, …, $c \mid a_{n-1}$ donc c divise $\mathrm{pgcd}(a_1, \ldots, a_{n-1})$ (cf. la définition du pgcd). De plus, c divise a_n, donc c divise $\mathrm{pgcd}(\mathrm{pgcd}(a_1, \ldots, a_{n-1}), a_n)$ (cf. la définition du pgcd).

Le deuxième exercice de l'article d'Arithmétique est de montrer que cette définition est correcte :

Déf : Soit $n \in \mathbb{N} \setminus \{0,1\}$. Soient $a_1, \ldots, a_n \in \mathbb{N}$. Le plus petit commun multiple de $a_1, \ldots, a_n$, noté $\mathrm{ppcm}(a_1, \ldots, a_n)$, est l'entier $m \in \mathbb{N}$ qui vérifie $a_1 \mid m$, …, $a_n \mid m$ et si $a_1 \mid c$, …, $a_n \mid c$ alors $m \mid c$.

Commençons par l'unicité :
Si m_1 et m_2 vérifient les propriétés de ppcm de $a_1, \ldots, a_n$ alors, comme $a_1 \mid m_1$,..., $a_n \mid m_1$ on a $m_2 \mid m_1$ et comme $a_1 \mid m_2$,..., $a_n \mid m_2$ on a $m_1 \mid m_2$.
Si $m_1 = 0$ alors comme $m_1 \mid m_2$ on a $m_2 = 0$. De même, si $m_2 = 0$ alors $m_1 = 0$.
Si $m_1 \neq 0$ et $m_2 \neq 0$ alors on a $m_1 \leq m_2$ et $m_1 \geq m_2$ (car $m_1 \mid m_2$ et $m_2 \mid m_1$) donc on a $m_1 = m_2$.
On a prouvé l'unicité du ppcm par disjonction de cas.

On va prouver l'existence du ppcm par récurrence sur n.
On a déjà prouvé l'existence pour $n = 2$.
Supposons que le ppcm de $n - 1$ nombres existe.
On va vérifier que $\text{ppcm}(\text{ppcm}(a_1, \ldots, a_{n-1}), a_n)$ vérifie les conditions de la définition de $\text{ppcm}(a_1, \ldots, a_n)$.
On remarque tout d'abord que c'est bien un entier naturel. a_n divise $\text{ppcm}(\text{ppcm}(a_1, \ldots, a_{n-1}), a_n$
(cf. définition du ppcm). Soit $i \in \{1, \ldots, n-1\}$. a_i divise $\text{ppcm}(a_1, \ldots, a_{n-1})$
et $\text{ppcm}(a_1, \ldots, a_{n-1})$ divise $\text{ppcm}(\text{ppcm}(a_1, \ldots, a_{n-1}), a_n)$ donc a_i divise $\text{ppcm}(\text{ppcm}(a_1, \ldots, a_{n-}$
(si vous avez le moindre doute, explicitez ce que je viens d'écrire avec la définition de "diviser"). Soit $c \in \mathbb{N}$ tel que $a_1 \mid c$, ..., $a_n \mid c$. $a_1 \mid c$, ..., $a_{n-1} \mid c$ donc $\text{ppcm}(a_1, \ldots, a_{n-1})$ divise c (cf. la définition du pgcd). De plus, a_n divise c, donc $\text{ppcm}(\text{ppcm}(a_1, \ldots, a_{n-1}), a_n)$ divise c (cf. la définition du pgcd).

Le troisième exercice de l'article d'Arithmétique est de démontrer le lemme suivant :

Lemme : Soit p un nombre premier. Soit $n \in \mathbb{N}\backslash\{0\}$. Soient $a_1, \ldots, a_n \in \mathbb{N}$. Si $p \mid a_1 \times \cdots \times a_n$ alors $p \mid a_1$ ou ... ou $p \mid a_n$.

On fait un raisonnement par récurrence sur n.

Le cas $n = 1$ est évident (c'est $p \mid a_1$ implique $p \mid a_1$).

On démontre aussi le cas $n = 2$ parce qu'on va en avoir besoin dans la phase d'hérédité.
Commençons par remarquer que comme p est premier, pour tout $a \in \mathbb{N}$ $\text{pgcd}(p, a) = 1$ ou p (en effet les seuls diviseurs de p sont 1 et p).
Soient $a_1, a_2 \in \mathbb{N}$ tels que $p \mid a_1 \times a_2$.

Si p ne divise pas a_1 alors $\text{pgcd}(p, a_1) = 1$ (car ce ne peut pas être p puisque p ne divise pas a_1) donc, par le lemme de Gauss, p divise a_2.
Ainsi, p divise a_1 ou p divise a_2.

Supposons que pour tous nombres naturels $b_1, \ldots, b_{n-1}$ on a $p \mid b_1 \times \cdots \times b_{n-1}$ implique $p \mid b_1$ ou $\ldots$ ou $p \mid b_{n-1}$.
Soient $a_1, \ldots, a_n \in \mathbb{N}$ tels que $p \mid a_1 \times \cdots \times a_n$.
D'après la phase d'initialisation, si p ne divise pas a_n alors p divise $a_1 \times \cdots \times a_{n-1}$ donc, d'après l'hypothèse de récurrence, $p \mid a_1$ ou $\ldots$ ou $p \mid a_{n-1}$.
Ainsi, $p \mid a_1$ ou $\ldots$ ou $p \mid a_n$.

Exo : Résolution de l'équation de Pythagore $x^2+y^2 = z^2$ avec $x, y, z \in \mathbb{N}\backslash\{0\}$.

1) Soit $c \in \mathbb{N} \setminus \{0\}$. Montrer que (x, y, z) est un triplet pythagoricien si et seulement si (cx, cy, cz) est un triplet pythagoricien.

Si (x, y, z) est un triplet pythagoricien on a : $x^2+y^2 = z^2$ d'où $c^2 \times (x^2+y^2) = c^2 \times z^2$ d'où $c^2 \times x^2 + c^2 \times y^2 = c^2 \times z^2$ d'où $(cx)^2 + (cy)^2 = (cz)^2$.
Si (cx, cy, cz) est un triplet pythagoricien on a : $(cx)^2 + (cy)^2 = (cz)^2$ d'où $c^2 \times x^2 + c^2 \times y^2 = c^2 \times z^2$ d'où $c^2 \times (x^2 + y^2) = c^2 \times z^2$ d'où, en simplifiant par c^2, $x^2 + y^2 = z^2$.

2) Montrer, à l'aide de la question précédente, que les triplets pythagoriciens sont exactement les triplets de la forme (cx, cy, cz) avec (x, y, z) triplet pythagoricien de pgcd 1 et $c \in \mathbb{N} \setminus \{0\}$.

Soit (s, t, u) un triplet pythagoricien. Posons $c = \text{pgcd}(s, t, u)$. Il existe $x, y, z \in \mathbb{N} \setminus \{0\}$ tels que $s = cx, t = cy, u = cz$. (cx, cy, cz) est un triplet pythagoricien donc, d'après la question précédente, (x, y, z) est un triplet pythagoricien, or $\text{pgcd}(x, y, z) = \frac{\text{pgcd}(s,t,u)}{c} = 1$, donc on a bien que les triplets pythagoriciens sont de la forme voulue.
Soit (x, y, z) un triplet pythagoricien de pgcd 1. Soit $c \in \mathbb{N} \setminus \{0\}$. D'après la question précédente, (cx, cy, cz) est un triplet pythagoricien.

3) Soit $m \in \mathbb{N} \setminus \{0\}$. Montrer que, dans la division euclidienne par 4, m^2 a pour reste 0 ou 1.

$m = 4q + r$ avec $r \in \{0, 1, 2, 3\}$. $m^2 = (4q + r)(4q + r) = 4(4q^2 + 2qr) + r^2$, donc si $r = 0$ alors le reste de m^2 est 0 (car $0^2 = 0$), si $r = 1$ alors le reste de m^2 est 1 (car $1^2 = 1$), si $r = 2$ alors $m^2 = 4(4q^2 + 4q + 1)$ (car $2^2 = 4$) donc le reste de m^2 est 0, si $r = 3$ alors $m^2 = 4(4q^2 + 6q + 2) + 1$ (car $3^2 = 9 = 4 \times 2 + 1$) donc le reste de m^2 est 1.

4) Soit (x, y, z) un triplet pythagoricien de pgcd 1. Déterminer le reste dans la division euclidienne de z^2 par 4 et en déduire que z est impair, puis que si x est pair alors y est impair et que si x est impair alors y est pair.

Si 4 divise x^2 et y^2 alors 4 divise $x^2+y^2 = z^2$, ce qui contredit $\mathrm{pgcd}(x^2, y^2, z^2) = 1$ (qui découle de $\mathrm{pgcd}(x, y, z) = 1$). Ainsi, 4 ne divise pas à la fois x^2 et y^2 (n'hésitez pas à réviser le raisonnement par l'absurde (cf. l'article 3)).
Le reste dans la division euclidienne de z^2 par 4 ne peut donc pas être 0 (car si $x^2 = 4q_1 + r_1$ et $y^2 = 4q_2 + r_2$ alors $z^2 = x^2 + y^2 = 4(q_1 + q_2) + r_1 + r_2$ or d'après la question précédente, $r_1, r_2 \in \{0, 1\}$ et on vient de montrer qu'on n'a pas à la fois $r_1 = 0$ et $r_2 = 0$) donc, d'après la question précédente, le reste dans la division euclidienne de z^2 par 4 est 1.
Il existe donc $q \in \mathbb{N}$ tel que $z^2 = 4q + 1 = 2 \times 2q + 1$ donc z^2 est impair (c'est-à-dire que z^2 n'est pas divisible par 2) donc z est impair (car si 2 divise z alors 2 divise $z^2 = z \times z$).
Si x^2 et y^2 sont pairs alors $z^2 = x^2 + y^2 = 2s_1 + 2s_2 = 2 \times (s_1 + s_2)$ est pair, ce qui contredit ce qui vient d'être démontré, donc on n'a pas à la fois x^2 et y^2 pairs.
Si x^2 et y^2 sont impairs alors $z^2 = x^2+y^2 = 2s_1+1+2s_2+1 = 2\times(s_1+s_2+1)$ est pair, ce qui contredit ce qui vient d'être démontré, donc on n'a pas à la fois x^2 et y^2 impairs.
Il suffit de remarquer que pour tout $m \in \mathbb{N}$ m^2 est pair si et seulement si m est pair pour conclure ; ce dernier fait se démontre comme suit : m^2 impair implique m pair se fait de la même manière que plus haut, et m^2 pair implique m pair découle du lemme démontré plus haut (le troisième exercice), du fait que 2 est premier et du fait que $m^2 = m \times m$.

5) Soit (x, y, z) un triplet pythagoricien de pgcd 1 avec x pair. Montrer que $\mathrm{pgcd}(\frac{z-y}{2}, \frac{z+y}{2}) = 1$. En déduire, puisque $(z - y)(z + y) = z^2 - y^2 = x^2$, que $\frac{z-y}{2}$ et $\frac{z+y}{2}$ sont des carrés d'entiers, puis une expression de x, y et z.

On remarque tout d'abord que d'après la question précédente z et y sont

impairs (car x est pair) donc $z-y$ et $z+y$ sont pairs (et $z-y \geq 0$ car $z^2-y^2=x^2 \geq 0$ et z et y sont des entiers naturels) donc $\frac{z-y}{2}$ et $\frac{z+y}{2}$ sont bien des entiers naturels.
Si $\text{pgcd}(\frac{z-y}{2}, \frac{z+y}{2}) > 1$ alors il existe un nombre premier p qui divise $\frac{z-y}{2}$ et $\frac{z+y}{2}$ (il suffit de prendre p un facteur premier de $\text{pgcd}(\frac{z-y}{2}, \frac{z+y}{2})$).
Il existe donc $a, b \in \mathbb{N}$ tels que $\frac{z-y}{2} = ap$ et $\frac{z+y}{2} = bp$, c'est-à-dire :

$$z-y = 2ap, \ \ z+y = 2bp.$$

En additionnant ces deux égalités on a : $2z = 2p(a+b)$ c'est-à-dire :
$z = p(a+b)$. En soustrayant la première égalité à la deuxième on a :
$2y = 2p(b-a)$ c'est-à-dire $y = p(b-a)$.
Ainsi, p divise y et z donc divise $z^2-y^2 = x^2$ donc divise x (car p est premier), et x, y, z ont un facteur premier en commun, ce qui contredit $\text{pgcd}(x, y, z) = 1$.
Ainsi, $\text{pgcd}(\frac{z-y}{2}, \frac{z+y}{2}) = 1$.

$$\left(\frac{z-y}{2}\right)\left(\frac{z+y}{2}\right) = \frac{1}{4}(z-y)(z+y) = \frac{1}{4}x^2 = \left(\frac{x}{2}\right)^2$$

donc $\left(\frac{z-y}{2}\right)\left(\frac{z+y}{2}\right)$ est un carré d'entier (x est pair donc $\frac{x}{2}$ est un entier).
Or $\frac{z-y}{2}$ et $\frac{z+y}{2}$ sont premiers entre eux (on a montré plus haut que leur pgcd est 1) donc ce sont des carrés d'entiers.
En effet, $\left(\frac{z-y}{2}\right)\left(\frac{z+y}{2}\right)$ est un carré d'entier implique que pour tout nombre premier p la valuation p-adique de $\left(\frac{z-y}{2}\right)\left(\frac{z+y}{2}\right)$ est paire, or $0 = v_p(1) = v_p(\text{pgcd}(\frac{z-y}{2}, \frac{z+y}{2})) = \min(v_p(\frac{z-y}{2}), v_p(\frac{z+y}{2}))$ et $v_p(\left(\frac{z-y}{2}\right)\left(\frac{z+y}{2}\right)) = v_p(\frac{z-y}{2}) + v_p(\frac{z+y}{2})$ donc $v_p(\frac{z-y}{2})$ ou $v_p(\frac{z+y}{2})$ est égale à $v_p(\left(\frac{z-y}{2}\right)\left(\frac{z+y}{2}\right))$ qui est paire et l'autre est nulle donc paire. On a montré que pour tout p premier, $v_p(\frac{z-y}{2})$ et $v_p(\frac{z-y}{2})$ sont paires, donc $\frac{z-y}{2}$ et $\frac{z+y}{2}$ sont des carrés d'entiers
(car $p_1^{2k_1} \times \cdots \times p_r^{2k_r} = (p_1^{k_1})^2 \times \cdots \times (p_r^{k_r})^2 = (p_1^{k_1} \times \cdots \times p_r^{k_r})^2$).
Il existe donc des entiers naturels u et v tels que $\frac{z-y}{2} = u^2$ et $\frac{z+y}{2} = v^2$.
Ainsi $z-y = 2u^2$ et $z+y = 2v^2$ et on a, en sommant ces deux égalités et en soustrayant la première égalité à la deuxième égalité :
$2z = 2(u^2+v^2)$ et $2y = 2(v^2-u^2)$. En simplifiant par 2 on a :
$z = u^2+v^2$ et $y = v^2-u^2$.
De plus on a : $x^2 = z^2-y^2 = (u^2+v^2)^2 - (v^2-u^2)^2$ donc :

$$x^2 = u^4+v^4+2u^2v^2-v^4-u^4+2u^2v^2 = 4u^2v^2 = (2uv)^2$$

or x et $2uv$ sont positifs donc $x = 2uv$.

6) Donner tous les triplets pythagoriciens.

On a montré en répondant à la question précédente que si (x, y, z) est un triplet pythagoricien de pgcd 1 avec x pair alors il existe $u, v \in \mathbb{N}$ tels que $x = 2uv, y = v^2 - u^2, z = v^2 + u^2$.
Avec la question 4) on a que si (x, y, z) est un triplet pythagoricien de pgcd 1 avec x pair alors y est pair et, de même que précédemment, il existe $u, v \in \mathbb{N}$ tels que $y = 2uv, x = v^2 - u^2, z = v^2 + u^2$.
On remarque que dans les deux cas $v \geq u$ (car x et y sont positifs).
On remarque aussi que $u \neq 0$, $v \neq 0$ et $v \neq u$ (car $x \neq 0$ et $y \neq 0$).
Avec la question 2) on a que tous les triplets pythagoriciens sont de la forme (cx, cy, cz) avec (x, y, z) un triplet pythagoricien de pgcd 1 et $c \in \mathbb{N} \setminus \{0\}$ donc, avec ce qui précède, de la forme $(2cuv, c(v^2 - u^2), c(v^2 + u^2))$ ou $(c(v^2 - u^2), 2cuv, c(v^2 + u^2))$ avec $c, u, v \in \mathbb{N} \setminus \{0\}$ et $v > u$.
Il nous suffit maintenant de vérifier que si $c, u, v \in \mathbb{N} \setminus \{0\}$ vérifient $v > u$ alors $(2cuv, c(v^2 - u^2), c(v^2 + u^2))$ et $(c(v^2 - u^2), 2cuv, c(v^2 + u^2))$ sont des triplets pythagoriciens.

$$(2cuv)^2 + (c(u^2 - v^2))^2 = 4c^2u^2v^2 + c^2u^4 + c^2v^4 - 2c^2u^2v^2 = c^2u^4 + c^2v^4 + 2c^2u^2v^2 = (c(u^2 + v^2))^2$$

et $2cuv, c(v^2 - u^2), c(v^2 + u^2) \in \mathbb{N} \setminus \{0\}$ donc $(2cuv, c(v^2 - u^2), c(v^2 + u^2))$ et $(c(v^2 - u^2), 2cuv, c(v^2 + u^2))$ sont bien des triplets pythagoriciens.

<u>Exo</u> : Si $x, y, z \in \mathbb{Z} \setminus \{0\}$ vérifient $x^2 + y^2 = z^2$, en remplaçant x par $-x$ ou y par $-y$ ou z par $-z$ on a encore $x^2 + y^2 = z^2$ et $x, y, z \in \mathbb{Z} \setminus \{0\}$. En changeant les signes qu'il faut, on se ramène à $x, y, z \in \mathbb{N} \setminus \{0\}$, et l'exercice précédent nous donne donc tous les $x, y, z \in \mathbb{Z} \setminus \{0\}$ qui vérifient $x^2 + y^2 = z^2$ en changeant des signes (explicitez ces solutions).

Les $x, y, z \in \mathbb{Z} \setminus \{0\}$ tels que $x^2 + y^2 = z^2$ sont exactement les $(2cuv, c(v^2 - u^2), c(v^2 + u^2))$, $(-2cuv, c(v^2 - u^2), c(v^2 + u^2))$, $(2cuv, -c(v^2 - u^2), c(v^2 + u^2))$, $(2cuv, c(v^2 - u^2), -c(v^2 + u^2))$,$(2cuv, -c(v^2 - u^2), -c(v^2 + u^2))$, $(-2cuv, c(v^2 - u^2), -c(v^2 + u^2))$, $(-2cuv, -c(v^2 - u^2), c(v^2 + u^2))$,$(-2cuv, -c(v^2 - u^2), -c(v^2 + u^2))$ et $(c(v^2 - u^2), 2cuv, c(v^2 + u^2))$, $(c(v^2 - u^2), -2cuv, c(v^2 + u^2))$, $(-c(v^2 - u^2), 2cuv, c(v^2 + u^2))$, $(c(v^2 - u^2), 2cuv, -c(v^2 + u^2))$,$(-c(v^2 - u^2), 2cuv, -c(v^2 + u^2))$, $(c(v^2 - u^2), -2cuv, -c(v^2 + u^2))$, $(-c(v^2 - u^2), -2cuv, c(v^2 + u^2))$,$(-c(v^2 - u^2), -2cuv, -c(v^2 + u^2))$ avec $c, u, v \in \mathbb{N} \setminus \{0\}$ et $v > u$.

Exo : Pour prouver que pour tout $n \geq 3$ il n'existe pas $x, y, z \in \mathbb{Z} \setminus \{0\}$ tels que $x^n + y^n = z^n$ il suffit de le montrer pour $n = 3, n = 4$ et $n \geq 5$ premier.

Soit $n \geq 5$. Décomposons n en facteurs premiers : $n = p_1^{a_1} \times \cdots \times p_m^{a_m}$ où $p_1, \ldots, p_m$ sont des nombres premiers distincts et $a_1, \ldots, a_m \in \mathbb{N} \setminus \{0\}$.
Si n n'est pas une puissance de 2 : $m > 1$ ou $p_1 \neq 2$ (et dans le premier cas quitte à échanger p_1 et p_2 on peut supposer $p_1 \neq 2$), si $x^n + y^n = z^n$ avec $x, y, z \in \mathbb{Z} \setminus \{0\}$ alors $(x^{\frac{n}{p_1}})^{p_1} + (y^{\frac{n}{p_1}})^{p_1} = (z^{\frac{n}{p_1}})^{p_1}$ et $x^{\frac{n}{p_1}}, y^{\frac{n}{p_1}}, z^{\frac{n}{p_1}} \in \mathbb{Z} \setminus \{0\}$. Or $p_1 \neq 2$ donc $p_1 = 3$ ou $p_1 \geq 5$ premier : on est bien ramené aux cas voulus (si on a une solution pour n alors on a une solution pour p_1, donc si on a déjà montré qu'il n'y a pas de solution pour p_1 alors on a aussi qu'il n'y a pas de solution pour n).
Sinon, $n = 2^a$ avec $a \in \mathbb{N} \setminus \{0, 1\}$ (car $n \geq 5$) or $2^2 = 4$ donc 4 divise n : $n = 4q$. Si $x^n + y^n = z^n$ avec $x, y, z \in \mathbb{Z} \setminus \{0\}$ alors $(x^q)^4 + (y^q)^4 = (z^q)^4$ et $x^q, y^q, z^q \in \mathbb{Z} \setminus \{0\}$: on est bien ramené aux cas voulus (si on a une solution pour n alors on a une solution pour 4, donc si on a déjà montré qu'il n'y a pas de solution pour 4 alors on a aussi qu'il n'y a pas de solution pour n).

Pour le cas $n = 4$ on montre même qu'il n'y a pas de solution dans $\mathbb{Z} \setminus \{0\}$ à $x^4 + y^4 = z^2$ (ce qui implique le cas $n = 4$ en prenant z un carré d'entier). En effet, si on avait $x^4 + y^4 = c^4$ avec $x, y, c \in \mathbb{Z} \setminus \{0\}$ alors on aurait $x^4 + y^4 = (c^2)^2$ avec $x, y, c^2 \in \mathbb{Z} \setminus \{0\}$.

Il suffit de montrer qu'il n'y a pas de solution dans $\mathbb{N} \setminus \{0\}$ car les exposants (4,4 et 2) sont pairs (c'est-à-dire divisibles par 2 ; comme dans la remarque plus haut, on peut changer les signes de x, y, z pour avoir des entiers positifs).

Exo : Il n'y a pas de solution dans $\mathbb{N} \setminus \{0\}$ à $x^4 + y^4 = z^2$.

1) Se ramener à x, y, z de pgcd 1.

Indication : en notant d le pgcd de x, y, z, montrer que $\frac{x}{d}, \frac{y}{d}, \frac{z}{d^2}$ sont de pgcd 1.

Avant de parler du pgcd de $\frac{x}{d}, \frac{y}{d}, \frac{z}{d^2}$, il faut déjà vérifier que ce sont des nombres entiers, c'est-à-dire que d divise x et y et d^2 divise z. On sait que d divise x, y, z car d est le pgcd de x, y, z.

Soit p un nombre premier. $2v_p(z) = v_p(z^2) = v_p(x^4+y^4) \geq \min(v_p(x^4), v_p(y^4)) = \min(4v_p(x), 4v_p(y)) = 4\min(v_p(x), v_p(y))$ donc $v_p(z) \geq 2\min(v_p(x), v_p(y)) \geq 2\min(v_p(x), v_p(y), v_p(z)) = 2v_p(d) = v_p(d^2)$.
Ainsi d^2 divise z.

(Si vous avez eu du mal à suivre, relisez la partie de l'article d'Arithmétique qui traite des valuations p-adiques, et pour les inégalités remarquez que si p^k divise a et b alors p^k divise $a+b$ donc $v_p(a+b) \geq \min(v_p(a), v_p(b))$ et que le minimum d'un ensemble A plus grand (pour l'inclusion) qu'un ensemble B est plus petit que le minimum de B (en particulier pour tous a, b, c $\min(a, b) \geq \min(a, b, c)$))

On peut désormais remarquer que $\text{pgcd}(\frac{x}{d}, \frac{y}{d}, \frac{z}{d^2}) = \frac{1}{d}\text{pgcd}(x, y, \frac{z}{d})$ et qu'il suffit donc de montrer que $\text{pgcd}(x, y, \frac{z}{d}) = d$ pour montrer que

$$\text{pgcd}(\frac{x}{d}, \frac{y}{d}, \frac{z}{d^2}) = 1.$$

On va montrer que pour tout p premier $v_p(d) = v_p(\text{pgcd}(x, y, \frac{z}{d}))$.

Soit p un nombre premier.

On remarque tout d'abord que $v_p(z) \geq v_p(\frac{z}{d})$ (car $\frac{z}{d}$ divise z) donc $v_p(d) = \min(v_p(x), v_p(y), v_p(z)) \geq \min(v_p(x), v_p(y), v_p(\frac{z}{d})) = v_p(\text{pgcd}(x, y, \frac{z}{d}))$.

On remarque ensuite qu'on a montré plus haut que $v_p(z) \geq v_p(d^2)$, ce qui entraîne $v_p(\frac{z}{d}) \geq v_p(d)$ (car $v_p(\frac{z}{d}) = v_p(z) - v_p(d)$ et $v_p(d) = v_p(d^2) - v_p(d)$ (voir la proposition dans l'article Arithmétique qui stipule que pour tous a, b $v_p(ab) = v_p(a) + v_p(b)$)), d'où $v_p(d) \leq \min(v_p(x), v_p(y), v_p(\frac{z}{d})) = v_p(\text{pgcd}(x, y, \frac{z}{d}))$ (car on savait déjà $v_p(d) \leq v_p(x)$ et $v_p(d) \leq v_p(y)$).

Ainsi $v_p(d) = v_p(\text{pgcd}(x, y, \frac{z}{d}))$.

Ainsi $d = \text{pgcd}(x, y, \frac{z}{d})$ et $\text{pgcd}(\frac{x}{d}, \frac{y}{d}, \frac{z}{d^2}) = 1$.

2) Vérifier que si x, y, z est solution de $x^4 + y^4 = z^2$ et de pgcd 1 alors (x^2, y^2, z) est un triplet pythagoricien de pgcd 1 et en déduire qu'il existe $u, v \in \mathbb{N} \setminus \{0\}$ de pgcd 1 tels que $x^2 = 2uv, y^2 = v^2 - u^2$ et $z = v^2 + u^2$ (quitte à échanger x et y).

Indication : dans la preuve de l'exercice sur les triplets pythagoriciens, vous devriez avoir trouvé de tels u, v mais sans avoir prouvé qu'ils sont de pgcd 1 ; en revanche vous devriez avoir prouvé (avec les notations de l'exercice sur les triplets pythagoriciens) que $u^2 = \frac{z-y}{2}$, $v^2 = \frac{z+y}{2}$ et $\text{pgcd}(\frac{z-y}{2}, \frac{z+y}{2}) = 1$ (dans les notations ici il faut remplacer y par y^2), et vous devriez pouvoir en déduire que $\text{pgcd}(u, v) = 1$.

On remarque que $x^4 = (x^2)^2$ et $y^4 = (y^2)^2$ donc si $x^4 + y^4 = z^2$ alors (x^2, y^2, z) est un triplet pythagoricien. De plus si $\text{pgcd}(x, y, z) = 1$ alors $\text{pgcd}(x^2, y^2, z) = 1$ (car si un nombre premier p divise x^2, y^2, z alors il divise x, y, z (par le troisième lemme du II) ce qui contredit $\text{pgcd}(x, y, z) = 1$) donc si x, y, z est solution de $x^4 + y^4 = z^2$ et de pgcd 1 alors (x^2, y^2, z) est un triplet pythagoricien de pgcd 1.

Ainsi, d'après ce qu'on a montré dans l'exercice sur les triplets pythagoriciens, quitte à échanger x et y on a alors $u, v \in \mathbb{N} \setminus \{0\}$ tels que $x^2 = 2uv, y^2 = v^2 - u^2$, $z = v^2 + u^2$ et $\text{pgcd}(u^2, v^2) = 1$. On remarque que si un nombre premier p divise divise u et v alors il divise u^2 et v^2 ce qui contredit $\text{pgcd}(u^2, v^2) = 1$, donc $\text{pgcd}(u, v) = 1$.

3) Montrer que v est impair et que u est pair puis en déduire que v est un carré d'entier et que u est le produit de 2 et d'un carré d'entier.

D'après la question précédente, (x^2, y^2, z) est un triplet pythagoricien de pgcd 1 donc, d'après l'exercice sur les triplets pythagoriciens, z est impair. Or $z = v^2 + u^2$ donc v^2 et u^2 n'ont pas la même parité (c'est-à-dire que l'un des deux est impair et l'autre est pair).

Si u^2 est impair et v^2 pair alors 4 divise $y^2 + 1$ (car $y^2 = v^2 - u^2$) ce qui est impossible. Explications : on regarde les restes modulo 4 (c'est à dire qu'on considère $r_u, r_v, r_y \in \{0, 1, 2, 3\}$ tels que u^2 est égal à un multiple de 4 plus r_u, v^2 est égal à un multiple de 4 plus r_v et y^2 est égal à un multiple de 4 plus r_y (c'est comme regarder la parité d'un nombre mais par rapport à 4 au lieu de 2 (et du coup au lieu d'avoir deux possibilités, être pair ou être impair, on a quatre possibilités, être congru à 0 modulo 4 (c'est-à-dire être divisible par 4), être congru à 1 modulo 4 (c'est-à-dire que si on nous enlève 1 alors on est divisible par 4), être congru à 2 modulo 4 (c'est-à-dire que si on nous enlève 2 alors on est divisible par 4) ou être congru à 3 modulo 4 (c'est-à-dire que si on nous enlève 3 alors on est divisible par 4)) ; si vous avez des difficultés à comprendre ceci, lisez l'article 12 Arithmétique 2 sur les congruences)). On peut vérifier facilement qu'un carré est forcément congru à 0 ou 1 modulo 4 (faites une disjonction de cas selon le reste modulo 4 du nombre dont vous voulez considérer le carré), donc $r_u, r_v, r_y \in \{0, 1\}$; u^2 est impair donc ne peut pas être divisible par 4 (car 4 est divisible par 2) donc $r_u = 1$, et v^2 est pair donc ne peut pas être congru à 1 modulo 4 (car il s'écrirait $4q + 1$ pour un certain q, donc $2(2q) + 1$, donc serait impair), donc $r_v = 0$; or $r_y = r_v - r_u$ modulo 4 (car $y^2 = v^2 - u^2$) donc $r_y = -1 = 3$ modulo 4 (on a $3 = -1$ modulo 4 car $4 - 1 = 3$) ; or $r_y \in \{0, 1\}$ d'après ce qui précède, donc on a une contradiction. (Plus haut on avait écrit 4 divise $y^2 + 1$, c'est une reformulation de $r_y = -1 = 3$ modulo 4)

Ainsi v^2 est impair et u^2 est pair donc v est impair et u est pair (si 2 divisait v alors il diviserait v^2 et pour u on utilise le troisième lemme du II).

Or $x^2 = 2uv$ et $\text{pgcd}(u, v) = 1$ (voir la question précédente) donc v est un carré d'entier et u est le produit de 2 et d'un carré d'entier. En effet, si $x = p_1^{n_1} \dots p_r^{n_r}$, avec $p_1 < \cdots < p_r$ est la décomposition en facteurs premiers de x on a $x^2 = p_1^{2n_1} \dots p_r^{2n_r}$ donc $2uv = p_1^{2n_1} \dots p_r^{2n_r}$ donc $p_1 = 2$ et, comme il est à la puissance $2n_1$, on retrouve 2 dans u (car v est impair), et si on écrit $u = 2w$ on a $wv = 2^{2n_1 - 2} p_2^{2n_2} \dots p_r^{2n_r}$ or w et v sont premiers entre eux (car u et v le sont) donc $v_2(w) = 2n_1 - 2, v_2(v) = 0$ ou $v_2(w) = 0, v_2(v) = 2n_1 - 2$, et $v_{p_2}(w) = 2n_2, v_{p_2}(v) = 0$ ou $v_{p_2}(w) = 0, v_{p_2}(v) = 2n_2$, et ... et $v_{p_r}(w) = 2n_r, v_{p_r}(v) = 0$ ou $v_{p_r}(w) = 0, v_{p_r}(v) = 2n_r$, et pour tout p premier n'appartenant pas à $\{2, p_2, \dots, p_r\}$ $v_p(w) = 0, v_p(v) = 0$, donc w et v sont des carrés d'entier (car $2^{2n_1 - 2} = (2^{n_1 - 1})^2$, $p_i^{2n_i} = (p_i^{n_i})^2$ et un produit de carrés d'entiers est un carré d'entier).

4) Vérifier que (u, y, v) est un triplet pythagoricien de pgcd 1 et, en utilisant les questions précédentes, en déduire qu'il existe $x', y', z' \in \mathbb{N} \setminus \{0\}$ de pgcd 1 tels que $x'^4 + y'^4 = z'^2$ et $z' < z$.

D'après 2) u et v sont premiers entre eux et $u^2 + y^2 = v^2$ donc (u, y, v) est un triplet pythagoricien de pgcd 1. Il existe donc $a, b \in \mathbb{N} \setminus \{0\}$ de pgcd 1 tels que $u = 2ab, y = b^2 - a^2$ et $v = b^2 + a^2$ (car y est impair).
De plus, comme u est le produit de 2 et d'un carré d'entier (cf. 3)), il existe $d, e \in \mathbb{N} \setminus \{0\}$ tels que $a = d^2$ et $b = d^2$ (par le même raisonnement qu'à la fin de la question précédente). Et d et e sont premiers entre eux car a et b le sont.

On a $e^4 + d^4 = b^2 + a^2 = v = t^2$ pour un certain $t \in \mathbb{N} \setminus \{0\}$ (cf. 3)) et (e, d, t) de pgcd 1 (car e et d le sont), et $t < z$ (car $t \leq v$ et $v < z$ (car $z = v^2 + u^2$ et $u^2 > 0$)).

5) Utiliser le fait que toute partie non vide de $\mathbb{N}$ admet un plus petit élément pour conclure.

Posons $A = \{z \in \mathbb{N}\setminus\{0\},$ il existe $x, y \in \mathbb{N}\setminus\{0\}, x^4+y^4 = z^2$ et $\mathrm{pgcd}(x, y, z) = 1\}$.

Si A est non vide, alors il admet un plus petit élément z. Mais d'après 4) on peut trouver $z' \in A$ tel que $z' < z$, ce qui contredit le fait que z est le plus petit élément de A. L'ensemble A est donc vide.

D'après 1), il n'y a donc pas de $x, y, z \in \mathbb{N} \setminus \{0\}$ tels que $x^4 + y^4 = z^2$.

Clémentine Lemarié–Rieusset