Correction - DM 6

A rendre le 21/11/25

1. Soient a et b tels que $a^2 \mid b^2$. Notons $d = a \wedge b$ et a', b' premiers entre eux tels que $a = da'$ et $b = db'$. Alors $b^2 = d^2 b'^2$ est divisible par $a^2 = d^2 a'^2$, 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 $\boxed{a \mid b.}$

2. Puisque :
$$d = x \wedge y \wedge z = (dx') \wedge (dy') \wedge (dz') = d(x' \wedge y' \wedge z')$$
   par homogénéité, d'où $x' \wedge y' \wedge z' = 1$ puisque $d \neq 0$. De plus :
$$x'^2 + y'^2 = \frac{1}{d^2}(x^2 + y^2) = \frac{z^2}{d^2} = z'^2.$$
   Donc $\boxed{(x', y', z') \text{ est un triplet pythagoricien primitif.}}$

   Soit k un diviseur commun à x' et y'. Alors k^2 divise $x'^2 + y'^2 = z'^2$. Par la question 1, $k \mid z'$, 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 $k = \pm 1$. En particulier, $x' \wedge y' = 1$.

   Sur le même principe, un diviseur commun de x' et 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 $\boxed{x', y', z' \text{ sont deux à deux premiers entre eux.}}$

3. (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 $\boxed{\text{ne peuvent être tous deux multiples de 2.}}$

   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, $\boxed{x \text{ et } y \text{ sont de parités opposées.}}$

   (b) Puisque x est pair, il existe $u \in \mathbb{N}^*$ tel que $x = 2u$.

   Puisque $z^2 = x^2 + y^2 = y^2 + 4u^2$, z^2 est de même parité que y^2. Donc z et y sont de même parité, et $z + y$ et $z - y$ sont pairs. Il existe donc $v \in \mathbb{N}^*$ 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 $w \in \mathbb{N}^*$ tel que $z - y = 2w$.

   (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 la question 1, $d \mid x$.

   Ainsi, d divise $x \wedge y \wedge z = 1$, et donc $d = 1$. On a donc prouvé que $\boxed{v \wedge w = 1.}$

   (d) Puisque $4vw = y^2 - z^2 = x^2 = 4u^2$, alors $\boxed{vw = u^2 \text{ est un carré.}}$

   Pour tout nombre premier p :

   - d'une part, $v_p(v) + v_p(w) = v_p(vw) = v_p(u^2) = 2v_p(u)$;
   - d'autre part, v et w étant premiers entre eux, $v_p(v) = 0$ ou $v_p(w) = 0$.

Ainsi, soit $v_p(v) = 0$, et alors $v_p(w)$ est pair, soit $v_p(w) = 0$ et alors $v_p(v)$ est pair. Par conséquent, pour tout nombre premier p, $v_p(v)$ et $v_p(w)$ sont pairs, et il existe a_p, b_p entiers tels que $v_p(v) = 2a_p$ et $v_p(w) = 2b_p$. Et alors :

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

sont des carrés.

(e) Puisque $y \neq 0$, $z + y > z - y$, et donc $2n^2 > 2m^2$, d'où $n > m$.

Par ailleurs, tout diviseur commun à m et n est un diviseur commun à $v = n^2$ et $w = m^2$, et donc un diviseur de $v \wedge w = 1$. Donc $\boxed{m \wedge n = 1.}$

4. Nous venons de prouver que si (x, y, z) est primitif, alors il est bien de l'une des deux formes annoncées. En effet, dans le cas où, comme dans les questions précédentes, x est pair, on a montré l'existence de deux entiers $n > m > 0$ premiers entre eux tels que :

$$z + y = 2n^2 \text{ et } z - y = 2m^2, \text{ d'où } z = n^2 + m^2 \text{ et } y = n^2 - m^2.$$

D'où :

$$x^2 = z^2 - y^2 = (n^2 + m^2)^2 - (n^2 - m^2)^2 = 4n^2m^2$$

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 $y \wedge z = 1$.

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. Calculons pour cela :

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

Donc on est bien en présence d'un triplet pythagoricien.

Montrons que ce triplet est primitif. Notons pour cela $d = x \wedge y \wedge z$. Alors d est un diviseur commun de y et z, et donc de $2n^2 = z - y$ et $2m^2 = z + y$. Mais puisque $n \wedge m = 1$, $n^2 \wedge m^2 = 1$, et $2n^2 \wedge 2m^2 = 2$. Ainsi, $d = 1$ ou $d = 2$.

Reste à montrer que $d \neq 2$. Puisque m et n sont de parités distinctes, il en est de même de m^2 et n^2. Et donc $y = n^2 - m^2$ et $z = n^2 + m^2$ sont impairs, de sorte que $d \neq 2$.

Ainsi, $x \wedge y \wedge z = 1$, et $\boxed{(x, y, z) \text{ est un triplet pythagoricien primitif.}}$

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 $n > m > 0$ tels que :

$$\begin{cases} \frac{x}{d} = 2mn \\ \frac{y}{d} = n^2 - m^2 \\ \frac{z}{d} = n^2 + m^2 \end{cases} \text{ ou } \begin{cases} \frac{y}{d} = 2mn \\ \frac{x}{d} = n^2 - m^2 \\ \frac{z}{d} = n^2 + m^2 \end{cases}, \text{ soit encore } \begin{cases} x = 2mnd \\ y = d(n^2 - m^2) \\ z = d(n^2 + m^2) \end{cases} \text{ ou } \begin{cases} y = 2mnd \\ x = d(n^2 - m^2) \\ z = d(n^2 + m^2) \end{cases}$$

Et inversement, si $n > m > 0$ sont premiers entre eux, de parités distinctes, et $d \in \mathbb{N}^*$ alors

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

de sorte que $(2mnd, d(n^2 - m^2), d(n^2 + m^2))$ et $(d(n^2 - m^2), 2mnd, d(n^2 + m^2))$ sont des triplets pythagoriciens.

Finalement, les triplets pythagoriciens sont exactement les triplets de la forme

$$\boxed{(2mnd, d(n^2 - m^2), d(n^2 + m^2)) \quad \text{ou} \quad (d(n^2 - m^2), 2mnd, d(n^2 + m^2))}$$

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