Devoir à la maison n°09 : corrigé

Solution 1.

1. C'est du calcul.

2. **a.** Supposons que x et y admettent un diviseur premier commun p. Alors p divise x^2 et y^2. Puisque $z^2 = x^2+y^2$, p divise z^2. Puisque p est premier, p divise z. Ainsi p est un diviseur premier commun de x, y et z, ce qui est absurde puisque x, y et z sont premiers entre eux dans leur ensemble. Ainsi x et y ne possèdent pas de diviseur premier commun : ils sont premiers entre eux.
On prouve de même que x et z d'une part et y et z d'autre part sont premiers entre eux.

   b. Comme x et y sont premiers entre eux, ils ne peuvent pas être tous deux pairs.
Remarquons maintenant que le carré d'un entier pair est congru à 0 modulo 4 tandis que le carré d'un entier impair est congru à 1 modulo 4. Supposons x et y impairs. Alors $z^2 \equiv 2[4]$, ce qui est impossible puisque le carré d'un entier est congru à 0 ou 1 modulo 4.
Finalement x et y sont de parités distinctes. Dans ce cas, $z^2 \equiv 1[4]$, ce qui signifie que z est impair.

3. **a.** Notons δ le pgcd de $z-x$ et $z+x$. Tout d'abord, z et x étant impairs, $z-x$ et $z+x$ sont pairs donc 2 divise δ. De plus, $2x = (z+x)-(z-x)$ et $2z = (z+x)+(z-x)$ donc δ divise $2x$ et $2z$. Par conséquent, δ divise $2x \wedge 2z = 2(x \wedge z) = 2$. Finalement $\delta = 2$.

   b. Puisque le pgcd de $z-x$ et $z+x$ est 2, b et c sont premiers entre eux. De plus, $y^2 = z^2 - x^2 = (z-x)(z+x)$ i.e. $a^2 = bc$.
Puisque x, y, z sont strictement positifs, $a > 0$ et $b > 0$. Puisque $a^2 = bc$, on a également $c > 0$. On peut donc considérer les valuations p-adiques de a, b, c.
Soit alors p un nombre premier. Alors $\nu_p(a^2) = \nu_p(bc)$ i.e. $2\nu_p(a) = \nu_p(b) + \nu_p(c)$. Puisque b et c sont premiers entre eux, l'une des deux valuations $\nu_p(b)$ ou $\nu_p(c)$ est nulle tandis que l'autre vaut $2\nu_p(a)$. Quoi qu'il en soit, les deux valuations $\nu_p(b)$ et $\nu_p(c)$ sont paires. Ceci étant vrai pour tout nombre premier p, b et c sont des carrés d'entiers.

4. Soit (x, y, z) un triplet solution.

   - Si l'un des deux réels x et y est nul, on peut supposer que $y = 0$ quitte à permuter x et y. Alors $x^2 = z^2$. Si x et z sont de même signe, on a bien $x = d(u^2 - v^2)$, $y = 2duv$ et $z = d(u^2 + v^2)$ avec $d = x = z$, $u = 1$ et $v = 0$. Sinon, il suffit de poser $d = z = -x$, $u = 0$ et $v = 1$.
   - Si $z = 0$, alors $x = y = 0$ et on a bien $x = d(u^2 - v^2)$, $y = 2duv$ et $z = d(u^2 + v^2)$ avec $d = 0$ et u, v quelconques.

   On suppose donc maintenant que x, y, z sont non nuls et même strictement positifs. Notons d le pgcd de x, y et z. Alors $\left(\frac{x}{d}, \frac{y}{d}, \frac{z}{d}\right)$ est encore un triplet solution formé d'entiers naturels non nuls premiers entre eux dans leur ensemble. D'après ce qu'il précède, quitte à échanger x et y, il existe des entiers b et c tels que $\frac{z+x}{d} = 2b$ et $\frac{z-x}{d} = 2c$ avec b et c des carrés d'entiers naturels non nuls que l'on peut noter u et v. On a alors $z + x = 2du^2$ et $z - x = 2dv^2$ puis, par somme et différence, $z = d(u^2+v^2)$ et $x = d(u^2-v^2)$. Enfin, $y^2 = (z-x)(z+x) = 4d^2u^2v^2$ puis $y = 2duv$ puisque y, d, u, v sont positifs.
Enfin, si x, y, z sont non nuls mais pas forcément positifs, $(|x|, |y|, |z|)$ est encore solution de (E) de sorte que, quitte à permuter x et y, il existe $(d, u, v) \in (\mathbb{N}^*)^3$ tels que $|x| = d(u^2 - v^2)$, $|y| = 2duv$ et $|z| = d(u^2 + v^2)$. On a quand même (x, y, z) de la forme voulue quitte à

   - échanger u et v si $x < 0$, $y > 0$ et $z > 0$;
   - changer u en $-u$ si $x > 0$, $y < 0$ et $z > 0$;
   - changer d en $-d$, u en $-v$ et v en u si $x > 0$, $y > 0$ et $z < 0$;
   - changer u en $-v$ et v en u si $x < 0$, $y < 0$ et $z > 0$;
   - changer d en $-d$ et échanger u et v si $x > 0$, $y < 0$ et $z < 0$;
   - changer d en $-d$ et u en $-u$ si $x < 0$, $y > 0$ et $z < 0$;
   - changer d en $-d$ si $x < 0$, $y < 0$ et $z < 0$.

   La première question permet donc de conclure que l'ensemble des solutions de (E) est

$$\left\{(d(u^2 - v^2), 2duv, d(u^2 + v^2)),\ (d, u, v) \in \mathbb{Z}^3\right\} \cup \left\{(2duv, d(u^2 - v^2), d(u^2 + v^2)),\ (d, u, v) \in \mathbb{Z}^3\right\}$$

Solution 2.

1. Supposons que le système $(\mathscr{S})$ admette une solution x. Alors il existe $(k,l)\in\mathbb{Z}^2$ tel que $x=a+km$ et $y=b+ln$. On a donc $a+km=b+ln$ i.e. $a-b=ln-km$. Puisque $m\wedge n$ divise m et n, il divise $ln-km$ autrement dit $b-a$.
   Réciproquement, supposons que $a\equiv b[m\wedge n]$. Alors il existe k tel que $a-b=k\ m\wedge n$. Par ailleurs, d'après le théorème de Bézout, il existe $(u,v)\in\mathbb{Z}^2$ tel que $mu+nv=m\wedge n$. On en déduit que $kmu+knv=k\ m\wedge n=a-b$. Ainsi $a-kmu=b+knv$. En posant $x=a-kmu=b+knv$, on a alors bien $x\equiv a[m]$ et $x\equiv b[n]$.

2. Puisque x_0 est solution de $(\mathscr{S})$,

$$
\begin{aligned}
(\mathscr{S}) &\iff \begin{cases} x\equiv x_0[m] \\ y\equiv x_0[n] \end{cases} \\
&\iff \begin{cases} m|x-x_0 \\ d\mathrm{N}|x-x_0 \end{cases} \\
&\iff m\wedge n|x-x_0 \\
&\iff x\equiv x_0[m\wedge n]
\end{aligned}
$$

3. Dans ce cas, -6 est solution particulière de $(\mathscr{S})$. Puisque $8\vee 10=40$, l'ensemble des solutions de $(\mathscr{S})$ est $-6+40\mathbb{Z}$.