

DEVOIR SURVEILLÉ N°07 : 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 $v_p(a^2) = v_p(bc)$ i.e. $2v_p(a) = v_p(b) + v_p(c)$. Puisque b et c sont premiers entre eux, l'une des deux valuations $v_p(b)$ ou $v_p(c)$ est nulle tandis que l'autre vaut $2v_p(a)$. Quoi qu'il en soit, les deux valuations $v_p(b)$ et $v_p(c)$ 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

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

Solution 2

1. Clairement $\mathbb{Z}[\sqrt{2}] \subset \mathbb{R}$.

$$1 = 1 + 0\sqrt{2} \in \mathbb{Z}[\sqrt{2}].$$

Soit $(x, y) \in \mathbb{Z}[\sqrt{2}]^2$. Il existe donc $(a, b, c, d) \in \mathbb{Z}^4$ tel que $x = a + b\sqrt{2}$ et $y = c + d\sqrt{2}$.

Alors $x - y = (a - c) + (b - d)\sqrt{2}$ et $(a - c, b - d) \in \mathbb{Z}^2$ donc $x - y \in \mathbb{Z}[\sqrt{2}]$.

Également, $xy = (ac + 2bd) + (ad + bc)\sqrt{2}$ et $(ac + 2bd, ad + bc) \in \mathbb{Z}^2$ donc $xy \in \mathbb{Z}[\sqrt{2}]$.

Ainsi $\mathbb{Z}[\sqrt{2}]$ est donc un sous-anneau de $(\mathbb{R}, +, \times)$.

2. a. Soit $x \in \mathbb{Z}[\sqrt{2}]$. L'existence d'un couple $(a, b) \in \mathbb{Z}^2$ tel que $x = a + b\sqrt{2}$ découle simplement de la définition de $\mathbb{Z}[\sqrt{2}]$. Soit maintenant $(c, d) \in \mathbb{Z}^2$ tel que

$$x = a + b\sqrt{2} = c + d\sqrt{2}$$

On a donc $(a - c) = (d - b)\sqrt{2}$. Si $d \neq b$, $\sqrt{2}$ serait rationnel. Ainsi $b = d$ et par suite $a = c$. D'où l'unicité du couple (a, b) .

- b. Soit $(x, y) \in \mathbb{Z}[\sqrt{2}]$. Il existe donc $(a, b, c, d) \in \mathbb{Z}^4$ tel que $x = a + b\sqrt{2}$ et $y = c + d\sqrt{2}$. Alors

$$\overline{x \cdot y} = \overline{(a + b\sqrt{2})(c + d\sqrt{2})} = \overline{ac + 2bd + (ad + bc)\sqrt{2}} = ac + 2bd - (ad + bc)\sqrt{2}$$

$$\overline{x} \cdot \overline{y} = \overline{a + b\sqrt{2}} \cdot \overline{c + d\sqrt{2}} = (a - b\sqrt{2})(c - d\sqrt{2}) = ac + 2bd - (ad + bc)\sqrt{2}$$

On a donc bien $\overline{x \cdot y} = \overline{x} \cdot \overline{y}$.

3. a. Soient $x \in \mathbb{Z}[\sqrt{2}]$ et $(a, b) \in \mathbb{Z}^2$ tel que $x = a + b\sqrt{2}$. Alors $N(x) = a^2 - 2b^2 \in \mathbb{Z}$.

- b. Soit $(x, y) \in \mathbb{Z}[\sqrt{2}]^2$. Alors, en utilisant la question précédente

$$N(xy) = xy \overline{xy} = xy \overline{x} \cdot \overline{y} = x \overline{x} y \overline{y} = N(x)N(y)$$

- c. Soit $x \in \mathbb{Z}[\sqrt{2}]$.

Supposons x inversible. Il existe donc $y \in \mathbb{Z}[\sqrt{2}]$ tel que $xy = 1$. Ainsi $N(xy) = N(1) = 1$. D'après la question précédente, $N(xy) = N(x)N(y)$ d'où $N(x)N(y) = 1$. Puisque $N(x)$ et $N(y)$ sont entiers, on a donc $N(x) = \pm 1$ i.e. $|N(x)| = 1$.

Réciproquement soit $x \in \mathbb{Z}[\sqrt{2}]$ tel que $|N(x)| = 1$. Si $N(x) = 1$, alors $x\overline{x} = 1$ donc x est inversible (d'inverse \overline{x}). Si $N(x) = -1$, alors $x(-\overline{x}) = 1$ donc x est inversible (d'inverse $-\overline{x}$).

4. a. Supposons $a \geq 0$ et $b \geq 0$. On ne peut avoir $(a, b) = (0, 0)$ car $0 \notin H$. Un des deux entiers naturels a et b est donc non nul. Ainsi $a \geq 1$ ou $b \geq 1$ et, dans les deux cas, $x \geq 1$.
- b. Supposons $a \leq 0$ et $b \leq 0$. On ne peut avoir $(a, b) = (0, 0)$ car $0 \notin H$. Un des deux entiers a et b est donc non nul. Ainsi $a \leq -1$ ou $b \leq -1$ et, dans les deux cas, $x \leq -1$.
- c. Supposons $ab \leq 0$. Alors $a(-b) \geq 0$. Les deux questions précédentes montrent que $|\overline{x}| \geq 1$. Puisque $|N(x)| = |x||\overline{x}| = 1$, $|x| \leq 1$.

5. a. Puisque $x > 1$, la question précédente montre qu'on ne peut avoir $a \leq 0$ et $b \leq 0$ ni $ab \leq 0$. C'est donc que nécessairement $a > 0$ et $b > 0$.

- b. $u \in H^+$ car $u > 1$ et $N(u) = -1$.

Soient $x \in H^+$ et $(a, b) \in \mathbb{Z}^2$ tel que $x = a + b\sqrt{2}$. D'après la question précédente, $a \geq 1$ et $b \geq 1$ donc $x \geq u$. Ainsi u est un minorant de H^+ .

u est donc le minimum de H^+ .

6. a. Il suffit de poser $n = \left\lfloor \frac{\ln x}{\ln u} \right\rfloor$. On a alors

$$n \leq \frac{\ln x}{\ln u} < n + 1$$

ou encore

$$n \ln(u) \leq \ln(x) < (n + 1) \ln u$$

car $\ln u > 0$. Puis par stricte croissance de l'exponentielle

$$u^n \leq x < u^{n+1}$$

b. Supposons $x \neq u^n$. Alors

$$u^n < x < u^{n+1}$$

puis

$$1 < \frac{x}{u^n} < u$$

car $u > 0$. Or H et $u \in H$ donc $u^n \in H$. On sait également que $x \in H$ donc $\frac{x}{u^n} \in H$ car H est un groupe. Or $\frac{x}{u^n} > 1$ donc $\frac{x}{u^n} \in H^+$. Or $\frac{x}{u^n} < u$, ce qui contredit la minimalité de u .
On a donc prouvé que $x = u^n$.

7. On sait que $u \in H$ donc $u^n \in H$ pour tout $n \in \mathbb{Z}$ car H est un groupe. Puisque $-1 \in H$, on a également $-u^n \in H$ pour tout $n \in \mathbb{Z}$. Ainsi

$$\{u^n, n \in \mathbb{Z}\} \cup \{-u^n, n \in \mathbb{Z}\} \subset H$$

Soit maintenant $x \in H$. On sait que $0 \notin H$ donc $x \neq 0$.

- Si $x > 1$, alors $x \in H^+$ et il existe donc $n \in \mathbb{Z}$ tel que $x = u^n$ d'après la question précédente.
- Si $x = 1$, alors $x = u^0$.
- Si $0 < x < 1$, alors $\frac{1}{x} \in H^+$ donc il existe $n \in \mathbb{Z}$ tel que $\frac{1}{x} = u^n$ i.e. $x = u^{-n}$.
- Si $x < 0$, alors $-x \in H$ et $-x > 0$, et les cas précédents montrent l'existence d'un $n \in \mathbb{Z}$ tel que $-x = u^n$ i.e. $x = -u^n$.

On a donc prouvé que

$$H \subset \{u^n, n \in \mathbb{Z}\} \cup \{-u^n, n \in \mathbb{Z}\}$$

Par double inclusion

$$H = \{u^n, n \in \mathbb{Z}\} \cup \{-u^n, n \in \mathbb{Z}\}$$

Solution 3

1. On trouve

$$\begin{array}{ll} d_0 = 123 & \varepsilon_0 = 0,456 \\ d_1 = 4 & \varepsilon_1 = 0,56 \\ d_2 = 5 & \varepsilon_2 = 0,6 \\ d_3 = 6 & \varepsilon_3 = 0 \end{array}$$

On montre alors par récurrence que $d_n = \varepsilon_n = 0$ pour tout $n \geq 4$. En effet, $d_4 = \lfloor 10\varepsilon_3 \rfloor = 0$ et $\varepsilon_4 = 10\varepsilon_3 - d_4 = 0$ puisque $\varepsilon_3 = 0$. Supposons que $d_n = 0$ pour un certain $n \geq 4$. Alors $d_{n+1} = \lfloor 10\varepsilon_n \rfloor = 0$ et $\varepsilon_{n+1} = 10\varepsilon_n - d_{n+1} = 0$. Par récurrence, $d_n = 0$ pour tout $n \geq 4$.

2. a. Soit $n \in \mathbb{N}$. Si $n = 0$, $\varepsilon_0 = x - \lfloor x \rfloor \in [0, 1[$ puisque $\lfloor x \rfloor \leq x < \lfloor x \rfloor + 1$. Sinon $\varepsilon_n = 10\varepsilon_{n-1} - \lfloor 10\varepsilon_{n-1} \rfloor \in [0, 1[$ car $\lfloor 10\varepsilon_{n-1} \rfloor \leq 10\varepsilon_{n-1} < \lfloor 10\varepsilon_{n-1} \rfloor + 1$.
- b. Soit $n \in \mathbb{N}^*$. Alors $\varepsilon_{n-1} \in [0, 1[$ d'après la question 2.a et donc $10\varepsilon_{n-1} \in [0, 10[$. On en déduit que $d_n = \lfloor 10\varepsilon_{n-1} \rfloor \in \llbracket 0, 9 \rrbracket$.
- c. Pour tout $n \in \mathbb{N}$,

$$\left(S_{n+1} + \frac{\varepsilon_{n+1}}{10^{n+1}}\right) - \left(S_n + \frac{\varepsilon_n}{10^n}\right) = S_{n+1} - S_n + \frac{\varepsilon_{n+1} - 10\varepsilon_n}{10^{n+1}} = \frac{d_{n+1}}{10^{n+1}} - \frac{\lfloor 10\varepsilon_n \rfloor}{10^{n+1}} = 0$$

La suite de terme général $S_n + \frac{\varepsilon_n}{10^n}$ est donc constante égale à son premier terme $S_0 + \frac{\varepsilon_0}{10^0} = d_0 + \varepsilon_0 = x$.

d. Puisque $\varepsilon_n \in [0, 1[$ pour tout $n \in \mathbb{N}$, on déduit de la question précédente que pour tout $n \in \mathbb{N}$

$$x - \frac{1}{10^n} < S_n \leq x$$

Puisque $\lim_{n \rightarrow +\infty} \frac{1}{10^n} = 0$, on obtient $\lim_{n \rightarrow +\infty} S_n = x$ d'après le théorème des gendarmes.

3. a. Soit $n \in \mathbb{N}$.

$$\begin{aligned} u_{n+1} &= 10^{N+T} S_{n+N+T+1} - 10^N S_{n+N+1} = 10^{N+T} \left(S_{n+N+T} + \frac{d_{n+N+T+1}}{10^{n+N+T+1}} \right) - 10^N \left(S_{n+N} + \frac{d_{n+N+1}}{10^{n+N+1}} \right) \\ &= u_n + \frac{d_{n+N+T+1} - d_{n+N+1}}{10^{n+1}} = u_n \end{aligned}$$

car (d_n) est T -périodique à partir du rang N . On en déduit que (u_n) est constante.

b. Comme (u_n) est constante, $u_n = u_0$ pour tout $n \in \mathbb{N}$.

$$u_0 = 10^{N+T}S_{N+T} - 10^N S_N = \sum_{k=0}^{N+T} d_k 10^{N+T-k} - \sum_{k=0}^N d_k 10^{N-k}$$

Pour $k \in \llbracket 0, N+T \rrbracket$, $10^{N+T-k} \in \mathbb{Z}$ et $d_k \in \mathbb{Z}$ donc $\sum_{k=0}^{N+T} d_k 10^{N+T-k} \in \mathbb{Z}$.

De même, pour $k \in \llbracket 0, N \rrbracket$, $10^{N-k} \in \mathbb{Z}$ et $d_k \in \mathbb{Z}$ donc $\sum_{k=0}^N d_k 10^{N-k} \in \mathbb{Z}$.

On en déduit que $u_0 \in \mathbb{Z}$. En posant $p = u_0$, on a donc bien pour tout $n \in \mathbb{N}$

$$10^{N+T}S_{n+N+T} - 10^N S_{n+N} = p$$

c. Puisque (S_{n+N}) et (S_{n+N+T}) convergent toutes deux vers x (en tant que suites extraites de (S_n)), on obtient par unicité de la limite $10^{N+T}x - 10^N x = p$ et donc $x = \frac{p}{10^N(10^T-1)}$ puisque $10^T \geq 10 > 1$. Ceci prouve que x est rationnel.

4. On remarque que $10^6 x - 10^3 x = 123333$. Ainsi $x = \frac{123333}{999000} = \frac{41111}{333000}$.

5. a. La suite (r_n) est à valeurs dans l'ensemble fini $\llbracket 0, q-1 \rrbracket$. Elle ne peut donc être injective. Ainsi il existe des entiers N et M distincts tels que $r_N = r_M$.

b. Pour simplifier, supposons $N < M$ et posons $T = M - N$. On va montrer par récurrence que (r_n) est T -périodique à partir du rang N .

On a bien $r_{N+T} = r_N$.

Supposons que $r_{n+T} = r_n$ pour un certain entier $n \geq N$. On sait que r_{n+1} et r_{n+1+T} sont les restes respectifs des divisions euclidiennes de $10r_n$ et $10r_{n+T}$ par b . Mais puisque $10r_n = 10r_{n+T}$, on a $r_{n+1} = r_{n+1+T}$ par unicité du reste dans la division euclidienne.

Par récurrence, $r_{n+T} = r_n$ pour tout $n \geq N$. Ainsi (r_n) est T -périodique à partir du rang N .

c. Soit $n \geq N+1$. On sait que q_n et q_{n+T} sont les quotients respectifs de $10r_{n-1}$ et $10r_{n-1+T}$ par b . Puisque $n-1 \geq N$ et que (r_n) est T -périodique à partir du rang N , $r_{n-1} = r_{n-1+T}$ et donc $10r_{n-1} = 10r_{n-1+T}$. Par unicité du quotient dans la division euclidienne, $q_n = q_{n+T}$.

On a donc prouvé que (q_n) était T -périodique à partir du rang $N+1$.

d. Tout d'abord, $a = bq_0 + r_0$ avec $0 \leq r_0 < b$. On en déduit que

$$x - 1 = \frac{a}{b} - 1 < q_0 \leq \frac{a}{b} = x$$

et donc que $q_0 = \lfloor x \rfloor = d_0$. Par ailleurs,

$$r_0 = a - bq_0 = b\left(\frac{a}{b} - q_0\right) = b(x - \lfloor x \rfloor) = b\varepsilon_0$$

Supposons que $q_n = d_n$ et $r_n = b\varepsilon_n$ pour un certain $n \in \mathbb{N}$. Par définition,

$$10\varepsilon_n = d_{n+1} + \varepsilon_{n+1}$$

et donc

$$10b\varepsilon_n = bd_{n+1} + b\varepsilon_{n+1}$$

ou encore

$$10r_n = bd_{n+1} + b\varepsilon_{n+1}$$

On sait que $d_{n+1} \in \mathbb{Z}$ d'après la question 2.b. De plus, $b\varepsilon_{n+1} = 10r_n - bd_{n+1} \in \mathbb{Z}$. Enfin, $\varepsilon_{n+1} \in [0, 1[$ d'après la question 2.a donc $0 \leq b\varepsilon_{n+1} < b$. On en déduit que d_{n+1} et $q\varepsilon_{n+1}$ sont le quotient et le reste de la division euclidienne de $10r_n$ par b . Par unicité du quotient et du reste dans la division euclidienne, $q_{n+1} = d_{n+1}$ et $r_{n+1} = b\varepsilon_{n+1}$.

Par récurrence, $q_n = d_n$ et $r_n = b\varepsilon_n$ pour tout $n \in \mathbb{N}$.

6. On trouve successivement

$q_0 = 0$	$r_0 = 13$
$q_1 = 3$	$r_1 = 25$
$q_2 = 7$	$r_2 = 5$
$q_3 = 1$	$r_3 = 15$
$q_4 = 4$	$r_4 = 10$
$q_5 = 2$	$r_5 = 30$
$q_6 = 8$	$r_6 = 20$
$q_7 = 5$	$r_7 = 25$

On a $r_1 = r_7$ donc (r_n) est 6-périodique à partir du rang 1 d'après la question **5.b**. Toujours d'après la question **5.b**, (q_n) est 6-périodique à partir du rang 2. Mais puisque les suites (d_n) et (q_n) sont identiques, (d_n) est également 6-périodique à partir du rang 2.