

DEVOIR SURVEILLÉ N°07 : CORRIGÉ

Solution 1

- Supposons que a et b divisent c et que a et b sont premiers entre eux. D'après le théorème de Bézout, il existe $(u, v) \in \mathbb{Z}^2$ tel que $au + bv = 1$. Par conséquent, $acu + bcv = c$. Mais comme a et b divisent c , il existe $(k, l) \in \mathbb{Z}^2$ tel que $c = ka = lb$. On obtient alors $albu + bkav = c$ ou encore $ab(lu + kv) = c$, ce qui prouve que ab divise c .
- Soit d un diviseur commun de p et q . Comme p est premier, $d \in \{1, p\}$. De même, comme q est premier, $d \in \{1, q\}$. Ainsi $d \in \{1, p\} \cap \{1, q\}$. Mais comme $p \neq q$, $\{1, p\} \cap \{1, q\} = \{1\}$. Ainsi $d = 1$ i.e. $p \wedge q = 1$.
- Comme $e \wedge M = 1$, le théorème de Bézout montre qu'il existe $(u, v) \in \mathbb{Z}^2$ tel que $eu + Mv = 1$. On a donc $eu \equiv 1[M]$. Cependant, on ne sait pas si u est positif. On considère alors d le reste de la division euclidienne de u par M . Alors d est positif et $d \equiv u[n]$. Par conséquent, $ed \equiv eu \equiv 1[n]$.
- Par définition, e et d sont positifs donc $ed \geq 0$. Supposons que $ed = 0$. Alors $0 \equiv 1[M]$ et donc M divise 1 puis $M = 1$. Ceci signifierait que $p - 1 = q - 1 = 1$ puis que $p = q = 2$, ce qui contredit le fait que p et q sont distincts.
- Remarquons déjà qu'il existe $k \in \mathbb{Z}$ tel que $ed = 1 + kM$. Mais comme $ed \geq 1$ et $M \geq 1$, k est positif. Ceci est nécessaire pour la suite car un entier élevé à une puissance strictement négative n'est généralement pas un entier.
 - Dans ce cas, $x \equiv 0[p]$. Comme $ed \geq 1$, $x^{ed} \equiv 0[p]$. On a donc bien $x^{ed} \equiv x[p]$.
 - D'après le petit théorème de Fermat, $x^{p-1} \equiv 1[p]$. Par conséquent, $x^{(p-1)(q-1)} \equiv 1^{q-1}[p]$ i.e. $x^M \equiv 1[p]$. Comme $x^{ed} = x \cdot (x^M)^k$, $x^{ed} \equiv x[p]$.
- On a montré que $x^{ed} \equiv x[p]$ et on montre de la même manière que $x^{ed} \equiv x[q]$. Ainsi p et q divisent $x^{ed} - x$. Comme $p \wedge q = 1$, $N = pq$ divise également $x^{ed} - x$ d'après la question 1. Ainsi $x^{ed} \equiv x[N]$.

Solution 2

- 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 $(\mathbb{R}, +, \times)$.
- 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) .

- 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

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

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

- Soient $x \in \mathbb{Z}[\sqrt{2}]$ et $(a, b) \in \mathbb{Z}^2$ tel que $x = a + b\sqrt{2}$. Alors $N(x) = a^2 - 2b^2 \in \mathbb{Z}$.
 - 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 $x\bar{x} = 1$ donc x est inversible (d'inverse \bar{x}). Si $N(x) = -1$, alors $x(-\bar{x}) = 1$ donc x est inversible (d'inverse $-\bar{x}$).

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 $|\bar{x}| \geq 1$. Puisque $|N(x)| = |x||\bar{x}| = 1$, $|x| \leq 1$.
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 $b\varepsilon_{n+1}$ 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.