Corrigé du devoir surveillé n°5

Exercice 1.

1. Les divisions successives sont :

$$\begin{aligned} 39 &= 2 \times 16 + 7 \\ 16 &= 2 \times 7 + 2 \\ 7 &= 3 \times 2 + 1 \end{aligned}$$

donc 39 et 16 sont premiers entre eux.

2. On en déduit que

$$\begin{aligned} 1 &= 7 - 3 \times 2 \\ &= 7 - 3 \times (16 - 2 \times 7) \\ &= 7 \times 7 - 3 \times 16 \\ &= 7 \times (39 - 2 \times 16) - 3 \times 16 \\ &= 7 \times 39 - 17 \times 16 \end{aligned}$$

Ainsi $u = 7$ et $v = 17$ sont deux entiers tels que $39u - 16v = 1$.

3. Soit $(x\,;y) \in \mathbb{Z}^2$ une solution de l'équation diophantienne (E) : $39x - 16y = 1$. Alors, $39x - 16y = 39 \times 7 - 16 \times 17$ donc $39(x - 7) = 16(y - 17)$. Ainsi, 16 divise $39(x - 7)$ donc, comme 16 et 39 sont premiers entre eux, 16 divise $x - 7$. Il existe donc un entier k tel que $x - 7 = 16k$ i.e. $x = 7 + 16k$. En substituant $x - 7 = 16k$ dans $39(x - 7) = 16(y - 17)$, il vient $39 \times 16k = 16(y - 17)$ donc $y - 17 = 39k$ i.e. $y = 17 + 39k$. Ainsi, si $(x\,;y)$ est une solution de (E) alors il existe un entier k tel que $x = 7 + 16k$ et $y = 17 + 39k$.
Réciproquement, si $k \in \mathbb{Z}$ alors

$$39(7 + 16k) - 16(17 + 39k) = 39 \times 7 - 16 \times 17 + 39 \times 16k - 16 \times 39k = 1$$

donc $(7 + 16k\,;17 + 39k)$ est solution de (E).
On conclut que l'ensemble des solutions de (E) est $\{(7 + 16k\,;17 + 39k) \mid k \in \mathbb{Z}\}$.

4. Soit n un entier solution du système (S) $\begin{cases} n \equiv 6\ [39] \\ n \equiv 7\ [16] \end{cases}$. Alors, il existe des entiers p et q tels que $n = 6 + 39p = 7 + 16q$ donc $39p - 16q = 1$. Ainsi, d'après la question précédente, il existe $k \in \mathbb{Z}$ tel que $p = 7 + 16k$ donc $n = 6 + 39(7 + 16k) = 279 + 624k$. Réciproquement, comme 16 et 39 divisent 624, si $k \in \mathbb{Z}$ alors $279 + 624k \equiv 279\ [624] \equiv 279\ [16] \equiv 7\ [16]$ et $279 + 624k \equiv 279\ [624] \equiv 279\ [39] \equiv 6\ [39]$ donc $279 + 624k$ est solution de (S)
On conclut que l'ensemble des entiers solutions de (S) est $\{279 + 624k \mid k \in \mathbb{Z}\}$.

Exercice 2.
Partie A

1. $u_1 = 5 \times 0 + 1 = 1$, $u_2 = 5 \times 1 + 1 = 6$ et $u_3 = 5 \times 6 + 1 = 31$. Comme $-5u_2 + u_3 = 1$, d'après le théorème de Bézout, $\text{PGCD}(u_2, u_3) = 1$.
2. Soit $n \in \mathbb{N}$. Alors, par définition, $u_{n+1} = 5u_n + 1$ donc $u_{n+1} - 5u_n = 1$. Dès lors, d'après le théorème de Bézout, u_n et u_{n+1} sont premiers entre eux.
3. Soit la proposition P_n : « $4u_n = 5^n - 1$ » pour $n \in \mathbb{N}$.
   Comme $5^0 - 1 = 1 - 1 = 0 = 4u_0$, la proposition P_0 est vraie.
   Supposons que P_k soit vraie pour un certain $k \in \mathbb{N}$.
   Alors, $4u_{k+1} = 4(5u_k + 1) = 5(4u_k) + 4 = 5(5^k - 1) + 4 = 5 \times 5^k - 5 + 4 = 5^{k+1} - 1$ donc P_{k+1} est vraie.
   On a donc démontré par récurrence que, pour tout $n \in \mathbb{N}$, $u_n = 5^n - 1$.
4. Soit $n \in \mathbb{N}$. $\text{PGCD}(5^{n+1} - 1, 5^n - 1) = \text{PGCD}(4u_{n+1}, 4u_n) = 4\text{PGCD}(u_{n+1}, u_n)$. Or, d'après la question 2, $\text{PGCD}(u_{n+1}, u_n) = 1$ donc $\text{PGCD}(5^{n+1} - 1, 5^n - 1) = 4$.

Partie B

1. **a.** Étant donné que $a^{n+1} = a^n \times a$,

$$(a^{n+1} - 1) \times 1 + (a^n - 1) \times (-a) = a^{n+1} - 1 - a^{n+1} + a = a - 1$$

   donc le couple $(u\,;v) = (1\,;-a)$ convient.

   b. Soit $k \in \mathbb{N}$. Comme $a = 1 + (a-1)$, $a \equiv 1\ [a-1]$ donc $a^k \equiv 1^k\ [a-1]$ i.e. $a^k \equiv 1\ [a-1]$ et donc $a^k - 1 \equiv 0\ [a-1]$. Par conséquent, pour tout $k \in \mathbb{N}$, $a - 1$ divise $a^k - 1$.

   c. Soit $n \in \mathbb{N}$. On déduit de la question précédente que $a - 1$ divise $a^n - 1$ et $a^{n+1} - 1$ et alors, par théorème, la question 1.a. assure que $\text{PGCD}(a^{n+1} - 1, a^n - 1) = a - 1$.

2. **a.** Par définition, d divise $a^m - 1$ donc $a^m - 1 \equiv 0\ [d]$ et ainsi $a^m \equiv 1\ [d]$. On justifie de même que $a^n \equiv 1\ [d]$.

   b. Comme m et n sont premiers entre eux, le théorème de Bézout assure l'existence de deux entiers u et v tels que $mu + nv = 1$.
   Si $m = 0$ alors $nv = 1$ donc, comme $n \geqslant 0$, $v \geqslant 0$. Ainsi, en posant $s = 0$ et $t = v$, on a bien deux entiers naturels tels que $nt = 1 + ms$.
   De même, si $n = 0$ alors $mu = 1$ et on peut poser $s = u$ et $t = 0$ et alors $ms = 1 + nt$.
   Supposons à présent que $m \geqslant 1$ et $n \geqslant 1$. Si $u > 0$ et $v > 0$ alors $u \geqslant 1$ et $v \geqslant 1$ donc $mu + nv \geqslant m + n \geqslant 2$ ce qui est absurde puisque $nu + nv = 1$. De même, si $u < 0$ et $v < 0$ alors $mu + nv \leqslant -m - n < 0$. Ainsi, u et v sont de signe contraire. Si $u \geqslant 0$ et $v \leqslant 0$, on pose $s = u$ et $t = -v$ ce qui donne $ms = 1 + nt$ et si $u \leqslant 0$ et $v \geqslant 0$, on pose $s = -u$ et $t = v$ ce qui donne $nt = 1 + ms$.
   Ainsi, dans tous les cas, il existe des entiers naturels t et s tels que $ms = 1 + nt$ ou $nt = 1 + ms$.

   c. Supposons qu'il existe deux entiers naturels t et s tels que $ms = 1 + nt$. Alors, $a^{ms} = a^{1+nt}$ Or, $a^{ms} = (a^m)^s \equiv 1^s\ [d] \equiv 1\ [d]$ et $a^{1+nt} = a \times (a^n)^t \equiv a \times 1^t\ [d] \equiv a\ [d]$.

On en déduit donc que $a \equiv 1$ $[d]$. Le raisonnement est analogue si $nt = 1 + ms$. Ainsi, dans tous les cas, $a - 1 \equiv 0$ $[d]$ donc d divise $a - 1$. Or, d'après la question 1.b, $a - 1$ divise $a^n - 1$ et $a^m - 1$ donc $a - 1$ divise d. Comme $d > 0$ et $a - 1 > 0$, on conclut que $d = a - 1$.

Exercice 3. Supposons que $\sqrt{n}$ est rationnel. Alors, il existe deux entiers naturels a et b premiers entre eux tels que $\sqrt{n} = \frac{a}{b}$ donc $\frac{n}{1} = \frac{a^2}{b^2}$. Or, n et 1 sont premiers entre eux tout comme a^2 et b^2 donc les deux fractions $\frac{n}{1}$ et $\frac{a^2}{b^2}$ sont irréductibles. Par unicité de la forme irréductible, on en déduit que $n = a^2$ (et $b^2 = 1$) donc $\sqrt{n} = a$ est un entier.