Corrigé du devoir surveillé n°5

Exercice 1.

1. a. Écrivons les divisions successives :

$$\begin{aligned}47 &= 1 \times 43 + 4\\43 &= 10 \times 4 + 3\\4 &= 1 \times 3 + 1\end{aligned}$$

Ainsi, le dernier reste non nul est 1 donc 47 et 43 sont premiers entre eux.

b. On a successivement

$$\begin{aligned}1 &= 4 - 3\\&= 4 - (43 - 10 \times 4) = 4 - 43 + 10 \times 4 = 11 \times 4 - 43\\&= 11 \times (47 - 43) - 43 = 11 \times 47 - 11 \times 43 - 43 = 11 \times 47 - 12 \times 43\end{aligned}$$

Ainsi, $u = 11$ et $v = 12$ sont deux entiers naturels tels que $47u - 43v = 1$.

2. a. On a vu que 47 et 43 sont premiers entre eux donc leur P.G.C.D. est 1. Or, 1 divise 7 donc, par théorème, (E) possède des solutions.

b. On a vu que $47 \times 11 - 43 \times 12 = 1$ donc, en multipliant par 7, $47 \times 77 - 43 \times 84 = 7$. Ainsi, $(77\,;84)$ est une solution particulière de (E).

c. Soit $(u\,;v) \in \mathbb{Z}^2$ une solution de (E). Alors, $47u - 43v = 7 = 47 \times 77 - 43 \times 84$ donc $47(u - 77) = 43(v - 84)$. Ainsi, 43 divise $47(u - 77)$ et $\mathrm{PGCD}(47, 43) = 1$ donc, par le théorème de Gauss, 43 divise $u - 77$. Il existe donc un entier k tel que $u - 77 = 43k$ i.e. $u = 77 + 43k$. Or, $47(u - 77) = 43(v - 84)$ donc $47 \times 43k = 43(v - 84)$ i.e. $47k = v - 84$ soit encore $v = 84 + 47k$.

Ainsi, une solution de (E) est de la forme $(77 + 43k\,;84 + 47k)$ où $k \in \mathbb{Z}$.

Réciproquement, soit $k \in \mathbb{Z}$, $u = 77 + 43k$ et $v = 84 + 47k$. Alors,

$$47u - 43v = 47(77 + 43k) - 43(84 + 47k) = 47 \times 77 - 43 \times 84 + 47 \times 43k - 43 \times 47k = 7$$

donc $(u\,;v)$ est solution de (E).

On conclut que l'ensemble des solutions de (E) est $\{(77 + 43k\,;84 + 47k) \mid k \in \mathbb{Z}\}$.

3. Soit n un entier tel que $n \equiv 12\ [43]$ et $n \equiv 5\ [47]$. Alors, il existe des entiers p et q tels que $n = 12 + 43p$ et $n = 5 + 47q$. On a donc $12 + 43p = 5 + 47q$ i.e. $47q - 43p = 7$. Ainsi, $(q\,;p)$ est solution de (E) donc il existe $k \in \mathbb{Z}$ tel que $q = 77 + 43k$ et $p = 84 + 47k$. Il s'ensuit que $n = 12 + 43(84 + 47)k = 3624 + 2021k \equiv 3624\ [2021] \equiv 1603\ [2021]$.

Réciproquement, soit un entier n tel que $n \equiv 1603\ [2021]$. Alors, il existe un entier k tel que $n = 1603 + 2021k$. Dès lors, $n = 12 + 43 \times 37 + 47 \times 43k = 12 + 43(37 + 47k) \equiv 12\ [43]$ et $n = 5 + 47 \times 34 + 47 \times 43k = 5 + 47(34 + 43k) \equiv 5\ [47]$.

On conclut que l'ensemble des entiers n tels que $n \equiv 12\ [43]$ et $n \equiv 5\ [47]$ est l'ensemble des entiers $n \equiv 1603\ [2021]$ i.e. $\{1603 + 2021k \mid k \in \mathbb{Z}\}$.

Exercice 2.

1. Soit $n \in \mathbb{N}$. On remarque que

$$2u_n - u_{n+1} = 2(2^n - 1) - (2^{n+1} - 1) = 2^{n+1} - 1 - 2^{n+1} + 2 = 1$$

donc, par le théorème de Bézout, u_n et u_{n+1} sont premiers entre eux.

2. **a.** Comme $u_m = 2^m - 1$, u_m divise $2^m - 1$ donc, par définition, $2^m \equiv 1\ [u_m]$. On en déduit que $(2^m)^q \equiv 1^q\ [u_m]$ i.e. $2^{qm} \equiv 1\ [u_m]$. Ainsi, u_m divise $2^{qm} - 1$ i.e. u_m divise u_{qm}.

   b. Par définition, $n = qm + r$ donc

$$\begin{aligned} u_{qm}(u_r + 1) + u_r &= (2^{qm} - 1)(2^r - 1 + 1) + 2^r - 1 = (2^{qm} - 1) \times 2^r + 2^r - 1 \\ &= 2^{qm+r} - 2^r + 2^r - 1 = 2^n - 1 \end{aligned}$$

   i.e. $u_{qm}(u_r + 1) + u_r = u_n$.

   c. Posons $d = \mathrm{PGCD}(u_n, u_m)$ et $d' = \mathrm{PGCD}(u_m, u_r)$. Par définition, d divise u_n et u_m donc, grâce à la question **2.a.**, d divise également u_{qm}. Il s'ensuit que d divise $u_n - u_{qm}(u_r + 1)$ i.e. d divise u_r. Dès lors, d divise u_m et u_r donc d divise d'.

   Inversement, d' divise u_m et u_r donc d' divise u_{qm} et u_r et ainsi d' divise également $u_{qm}(u_r + 1) + u_r = u_n$. Dès lors, d' divise u_n et u_m donc d' divise d.

   Comme $d > 0$ et $d' > 0$, on conclut que $d = d'$.

3. Écrivons les restes successifs dans l'algorithme d'Euclide appliqué à n et $m = r_0$: r_1, r_2, ..., r_k et $r_{k+1} = 0$. Alors, d'après la question précédente,

$$\mathrm{PGCD}(u_n, u_m) = \mathrm{PGCD}(u_{r_0}, u_{r_1}) = \mathrm{PGCD}(u_{r_1}, u_{r_2}) = \cdots = \mathrm{PGCD}(u_{r_k}, u_{r_{k+1}}).$$

   Or, $r_k = d$ et $r_{k+1} = 0$ donc $\mathrm{PGCD}(u_n, u_m) = \mathrm{PGCD}(u_d, 0) = u_d$.

4. Si n et m sont des entiers strictement positifs premiers entre eux alors, avec les notations précédentes, $d = 1$ donc $\mathrm{PGCD}(u_n, u_m) = u_d = u_1 = 2^1 - 1 = 1$ donc u_n et u_m sont premiers entre eux.

   Réciproquement, supposons que n et m sont des entiers strictement positifs tels que u_n et u_m sont premiers entre eux et posons $d = \mathrm{PGCD}(n, m)$. Alors, d'après la question précédente, $u_d = \mathrm{PGCD}(u_n, u_m) = 1$ donc $2^d - 1 = 1$ i.e. $2^d = 2$. Or, la suite (2^n) est strictement croissante et $2^1 = 2$ donc $d = 1$. Ainsi, n et m sont premiers entre eux et la réciproque est vraie.

Exercice 3. Soit $n \in \mathbb{N}$. Alors, d_n divise a_{n+1} et a_n donc d_n divise $a_{n+1} - a_n = 3$ car (a_n) est arithmétique de raison 3. Ainsi, $d_n = 1$ ou $d_n = 3$.

Supposons que $d_n = 3$. Alors, 3 divise $a_n = 3n + a_0$ donc, comme 3 divise $3n$, 3 divise $a_n - 3n = a_0$. Réciproquement, si $3 \mid a_0$ alors 3 divise $3n$ et a_0 donc 3 divise a_n et 3 divise $3(n+1)$ et a_0 donc 3 divise a_{n+1}. Dès lors, 3 divise d_n et donc $d_n = 3$.

On a donc montré que $d_n = 3$ si et seulement si a_0 est un multiple de 3.

On conclut donc que si a_0 est un multiple de 3 alors $d_n = 3$ et sinon $d_n = 1$.