Corrigé du devoir à la maison n°5

Partie A. – Étude d'un cas particulier

1. $u_2 = 7 \times 1 + 1 \times 0 = 7$, $u_3 = 7 \times 7 + 1 = 50$ et $u_4 = 7 \times 50 + 7 = 357$.

2. À l'aide de la calculatrice, on trouve $d_0 = d_1 = d_2 = d_3 = 1$.
On peut conjecturer que, pour tout $n \in \mathbb{N}$, $d_n = 1$ i.e. que u_n et u_{n+1} sont premiers entre eux.

3. Par définition, d_n divise u_n et u_{n+1} donc d_n divise $7u_{n+1} + u_n$ i.e. d_n divise u_{n+2}. Ainsi, d_n divise u_{n+1} et u_{n+2} donc d_n divise d_{n+1}.

4. Par définition, d_{n+1} divise u_{n+1} et u_{n+2} donc d_{n+1} divise $u_{n+2} - 7u_{n+1}$ i.e. d_{n+1} divise u_n. Ainsi, d_{n+1} divise u_{n+1} et u_n donc d_{n+1} divise d_n.

5. Soit $n \in \mathbb{N}$. On a montré que $d_n \mid d_{n+1}$ et $d_{n+1} \mid d_n$ donc, comme $d_n > 0$ et $d_{n+1} > 0$, $d_n = d_{n+1}$. Ainsi, la suite (d_n) est constante donc, comme $d_0 = 1$, pour tout $n \in \mathbb{N}$, $d_n = 1$. Ainsi, pour tout $n \in \mathbb{N}$, u_n et u_{n+1} sont premiers entre eux.

Partie B. – Cas général

On se place à présent dans le cas général i.e. on suppose que p et q sont des entiers strictement positifs quelconques.

Pour tout $n \in \mathbb{N}$, on pose $X_n = \begin{pmatrix} u_{n+1} \\ u_n \end{pmatrix}$.

1. Soit $n \in \mathbb{N}$. Alors,

$$X_{n+1} = \begin{pmatrix} u_{n+2} \\ u_{n+1} \end{pmatrix} = \begin{pmatrix} pu_{n+1} + qu_n \\ u_{n+1} \end{pmatrix} = \begin{pmatrix} p & q \\ 1 & 0 \end{pmatrix} \begin{pmatrix} u_{n+1} \\ u_n \end{pmatrix} = AX_n$$

en posant $A = \begin{pmatrix} p & q \\ 1 & 0 \end{pmatrix}$.

2. Soit $n \in \mathbb{N}^*$. Notons $A^n = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$. Alors, d'une part $X_n = A^n X_0$ donc

$$\begin{pmatrix} u_{n+1} \\ u_n \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} a \\ c \end{pmatrix}$$

donc $a = u_{n+1}$ et $c = u_n$. D'autre part, $X^{n+1} = A^n X_1$ donc

$$\begin{pmatrix} u_{n+2} \\ u_{n+1} \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} p \\ 1 \end{pmatrix} = \begin{pmatrix} ap + b \\ cp + d \end{pmatrix}$$

donc $b = u_{n+2} - ap = u_{n+2} - pu_{n+1} = qu_n$ et $d = u_{n+1} - cp = u_{n+1} - pu_n = qu_{n-1}$ (car $n \geqslant 1$).

Ainsi, on conclut que $A^n = \begin{pmatrix} u_{n+1} & qu_n \\ u_n & qu_{n-1} \end{pmatrix}$.

3. a. Soit $(k\,;m) \in \mathbb{N} \times \mathbb{N}^*$. Alors,

$$\begin{pmatrix} u_{m+k+1} \\ u_{m+k} \end{pmatrix} = X_{m+k} = A^{m+k} X_0 = A^m A^k X_0 = A^m X_k$$

donc, comme $m \geqslant 1$, d'après la question précédente,

$$\begin{pmatrix} u_{m+k+1} \\ u_{m+k} \end{pmatrix} = X_{m+k} = A^{m+k} X_0 = \begin{pmatrix} u_{m+1} & qu_m \\ u_m & qu_{m-1} \end{pmatrix} \begin{pmatrix} u_{k+1} \\ u_k \end{pmatrix} = \begin{pmatrix} u_{m+1}u_{k+1}qu_m u_k \\ u_m u_{k+1} + qu_{m-1}u_k \end{pmatrix}$$

En particulier, en identifiant les seconds coefficients, on obtient

$$u_{k+m} = u_m u_{k+1} + qu_{m-1}u_k.$$

b. Considérons, pour tout $n \in \mathbb{N}$, la proposition P_n : « u_m divise u_{nm} ».

Comme $u_0 = 0$ et que tout entier divise 0, la proposition P_0 est vraie.

Soit $k \in \mathbb{N}$. Supposons que P_k est vraie i.e. que u_n divise u_{km}. Alors, d'après la question précédente, puisque $m \geqslant 1$,

$$u_{(k+1)m} = u_{mk+m} = u_m u_{mk+1} + q u_{m-1} u_{mk}$$

mais u_m divise u_{km} et u_m donc il divise $u_m u_{mk+1} + q u_{m-1} u_{mk}$ i.e. u_m divise $u_{(k+1)m}$. Ainsi, P_{k+1} est vraie.

On a donc montré par récurrence que, pour tout $n \in \mathbb{N}$, u_m divise u_{nm}.

4. a. Soit d un diviseur positif commun à w et v. Alors, d divise w et w divise u donc d divise $\mathrm{PGCD}(u, v) = 1$ i.e., comme $d > 0$, $d = 1$. Ainsi, le seul diviseur positif commun à w et v est 1 donc w est premier avec u.

b. Par définition, δ divise a et b donc, comme a et b sont positifs, il existe des entiers naturels k et ℓ tels que $a = k\delta$ et $b = \ell\delta$. Comme $\delta > 0$, on déduit de la question **3.b.** que u_δ divise $u_{k\delta} = u_a$ et $u_{\ell\delta} = u_b$ donc u_δ divise $\mathrm{PGCD}(u_a, u_b)$ i.e. u_δ divise D.

c. Considérons, pour tout $n \in \mathbb{N}^*$, la proposition Q_n : « u_n est premier avec q ».

Comme $u_1 = 1$, Q_1 est vraie.

Soit $k \in \mathbb{N}^*$. Supposons que H_k est vraie i.e. que u_k est premier avec q. Notons $d = \mathrm{PGCD}(u_{k+1}, q)$. Alors, d divise u_{k+1} et d divise q donc d divise $u_{k+1} - q u_{k-1} = p u_k$. Or, d divise q et q est premier avec p donc, grâce à la question **4.a.**, d est premier avec p. Ainsi, par le théorème de Gauss, d divise u_k. Ainsi, d divise q et u_k donc d divise $\mathrm{PGCD}(q, u_k) = 1$ par hypothèse de récurrence. Ainsi, $d = 1$ donc u_{k+1} et q sont premiers entre eux donc Q_{k+1} est vraie.

On a donc montré par récurrence que, pour tout $n \in \mathbb{N}^*$, u_n et q sont premiers entre eux.

d. Considérons, pour tout $n \in \mathbb{N}$, la proposition H_n : « $d_n = 1$ ».

Comme $d_0 = \mathrm{PGCD}(u_0, u_1) = \mathrm{PGCD}(0, 1) = 1$ donc H_0 est vraie.

Soit $k \in \mathbb{N}$. Supposons que H_k est vraie i.e. que $d_k = 1$. Comme d_{k+1} divise u_{k+1} et u_{k+2}, d_{k+1} divise $u_{k+2} - p u_{k+1} = q u_k$. Or, $k + 1 \geqslant 1$ donc, par la question **4.c.**, u_{k+1} est premier avec q. De plus, d_{k+1} divise u_{k+1} donc, par la question **4.a.**, d_{k+1} est premier avec q. Ainsi, comme d_{k+1} divise $q u_k$, on déduit du théorème de Gauss, que d_{k+1} divise u_k. Dès lors, d_{k+1} divise u_k et u_{k+1} donc d_{k+1} divise $d_k = 1$. Comme $d_{k+1} > 0$, on conclut que $d_{k+1} = 1$ i.e. H_{k+1} est vraie.

On a donc montré, que pour tout $n \in \mathbb{N}$, $d_n = 1$.

e. Comme $\delta = \mathrm{PGCD}(a, b)$, par théorème, il existe des entiers r et s tels que $ra + sb = \delta$. Si $r \leqslant 0$ et $s \leqslant 0$ alors, comme $a > 0$ et $b > 0$, $\delta = ra + sb \leqslant 0$ ce qui est absurde car $\delta \geqslant 1$. Si $r > 0$ et $s > 0$ alors, comme r est entier, $r \geqslant 1$ donc $\delta = ra + sb > ra \geqslant a$ ce qui est absurde car δ est un diviseur de a et $a > 0$. Ainsi, r et s sont de signes contraires.

f. Comme $ra - tb = \delta$, $ra = \delta + tb$ et, comme $\delta \geqslant 0$ et $tb \geqslant 0$, on a $A^{ra} = A^{\delta + tb} = A^\delta A^{tb}$. Ainsi, $X_{ra} = A^{ra} X_0 = A^\delta A^{tb} X_0 = A^\delta X_{tb}$. De plus, comme $\delta > 0$, d'après la question **2.**, $A^\delta = \begin{pmatrix} u_{\delta+1} & q u_\delta \\ u_\delta & q u_{\delta-1} \end{pmatrix}$ donc

$$\begin{pmatrix} u_{ra+1} \\ u_{ra} \end{pmatrix} = \begin{pmatrix} u_{\delta+1} & q u_\delta \\ u_\delta & q u_{\delta-1} \end{pmatrix} \begin{pmatrix} u_{tb+1} \\ u_{tb} \end{pmatrix} = \begin{pmatrix} u_{\delta+1} u_{tb+1} + q u_\delta u_{tb} \\ u_\delta u_{tb+1} + q u_{\delta-1} u_{tb} \end{pmatrix}.$$

En particulier, en identifiant les seconds coefficients,

$$u_{ra} = u_\delta u_{tb+1} + q u_{\delta-1} u_{tb}.$$

g. Par définition, D divise u_a et u_b donc, grâce à la question **3.b.**, comme $a > 0$ et $b > 0$, D divise u_{ra} et u_{tb}. Ainsi, d'après l'égalité de la question précédente, D divise $u_{ra} - qu_{\delta-1}u_{tb}$ i.e. D divise $u_\delta u_{tb+1}$. Or, D divise u_{tb} et, d'après la question **4.d.**, u_{tb} et u_{tb+1} sont premiers entre eux donc, d'après la question **4.a.**, D est premier avec u_{tb+1}. ainsi, par le théorème de Gauss, D divise u_δ.

Or, on a vu en question **4.b.** que u_δ divise D donc, comme ils sont tous les deux positifs, $D = u_\delta$.

5. Supposons que, pour tous entiers a et b strictement positifs, $\text{PGCD}(u_a, u_b) = u_{\text{PGCD}(a,b)}$. En particulier, pour $a = 2$ et $b = 3$, $\text{PGCD}(u_2, u_3) = u_{\text{PGCD}(2,3)} = u_1 = 1$. Ainsi, $u_2 = p$ et $u_3 = p^2 + q$ sont premiers entre eux. Notons d le P.G.C.D. de p et q. Alors, d divise p et q donc p divise u_2 et $u_3 = p \times p + q$ donc d divise $\text{PGCD}(u_2, u_3) = 1$ donc $p = 1$. Ainsi, p et q sont premiers entre eux.