

Correction du devoir surveillé n°5

EXERCICE 1. — Une équation diophantienne

1. On remarque $9 \times 3 - 26 \times 1 = 1$ donc $(x_0; y_0) = (3; 1)$ est solution de (E) .
2. Soit $(x; y) \in \mathbb{Z}^2$ une solution de (E) . Alors, $9x - 26y = 1 = 9 \times 3 - 26 \times 1$ donc $9(x - 3) = 26(y - 1)$ [*]. En particulier, 26 divise $9(x - 3)$. Or, comme $9 \times 3 - 26 \times 1 = 1$, le théorème de Bézout assure que 9 et 26 sont premiers entre eux. Dès lors, d'après le théorème de Gauss, 26 divise $x - 3$ i.e. il existe un entier $k \in \mathbb{Z}$ tel que $x - 3 = 26k$ soit $x = 3 + 26k$. En substituant dans [*], on en déduit que $9 \times 26k = 26(y - 1)$ donc $9k = y - 1$ i.e. $y = 1 + 9k$. Ainsi, $(x; y)$ est de la forme $(3 + 26k; 1 + 9k)$.
Réciproquement, soit $k \in \mathbb{Z}$, $x = 3 + 26k$ et $y = 1 + 9k$. Alors,

$$9(3 + 26k) - 26(1 + 9k) = 9 \times 3 - 26 \times 1 + 9 \times 26k - 26 \times 9k = 1$$

donc $(x; y)$ est solution de (E) .

On conclut donc que l'ensemble des solutions de (E) est $\{(3 + 26k; 1 + 9k) \mid k \in \mathbb{Z}\}$.

3. Puisque $(x; y) \in \mathbb{Z}^2$ est solution de (E) , $9x - 26y = 1$ i.e. $9 \times x + (-y) \times 26 = 1$ donc d'après le théorème de Bézout, $\text{PGCD}(x, 26) = 1$.

EXERCICE 2. — Cryptage par la méthode de Hill

1. Méthode de cryptage

Les lettres « ES » se cryptent de la façon suivante :

$$\text{ES} \rightarrow C = \begin{pmatrix} 4 \\ 18 \end{pmatrix} \rightarrow AC = \begin{pmatrix} 108 \\ 82 \end{pmatrix} \rightarrow \begin{pmatrix} 4 \\ 4 \end{pmatrix} \rightarrow \text{EE}$$

Puisque « PION » se crypte en « LZWH », « PI » se crypte en « LZ » et « ON » en « WH ». On en déduit que le cryptage de « ESPION » donne « EELZWH ».

2. Méthode de décryptage

- a. Soit $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ une matrice carrée d'ordre 2 et $X = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$ et $Y = \begin{pmatrix} y_1 \\ y_2 \end{pmatrix}$ deux matrices colonnes de taille 2×1 . Supposons que $X \equiv Y$ [26]. Alors, par définition, $x_1 \equiv y_1$ [26] et $x_2 \equiv y_2$ [26].

Or, $MX = \begin{pmatrix} ax_1 + bx_2 \\ cx_1 + dx_2 \end{pmatrix}$ et $MY = \begin{pmatrix} ay_1 + by_2 \\ cy_1 + dy_2 \end{pmatrix}$. Puisque $x_1 \equiv y_1$ [26] et $x_2 \equiv y_2$ [26], par propriété des congruences, $ax_1 + bx_2 \equiv ay_1 + by_2$ [26] et $cx_1 + dx_2 \equiv cy_1 + dy_2$ [26] donc $MX \equiv MY$ [26].

- b. Le déterminant de A est $\det A = 9 \times 3 - 7 \times 4 = -1 \neq 0$ donc A est inversible et

$$A^{-1} = \frac{1}{-1} \begin{pmatrix} 3 & -4 \\ -7 & 9 \end{pmatrix} \text{ i.e. } A^{-1} = \begin{pmatrix} -3 & 4 \\ 7 & -9 \end{pmatrix}.$$

c. Considérons les deux lettres « XQ » et notons C_1 la matrice colonne correspondant aux deux lettres cryptées par « XQ ». Alors, par définition, $AC \equiv \begin{pmatrix} 23 \\ 16 \end{pmatrix}$ [26] et donc, d'après la question c., $A^{-1}AC \equiv A^{-1} \begin{pmatrix} 23 \\ 16 \end{pmatrix}$ [26] i.e $C \equiv \begin{pmatrix} -5 \\ 17 \end{pmatrix}$ [26] et ainsi $C \equiv \begin{pmatrix} 21 \\ 17 \end{pmatrix}$ [26] et donc « XQ » crypte les lettres « VR ». De même, les lettres « GY » correspondent à $C_2 = \begin{pmatrix} 6 \\ 24 \end{pmatrix}$, $A^{-1}C_2 = \begin{pmatrix} 78 \\ -174 \end{pmatrix} \equiv \begin{pmatrix} 0 \\ 8 \end{pmatrix}$ [26] donc « GY » crypte les lettres « AI ». Ainsi, le mot « XQGY » est le cryptage de « VRAI ».

EXERCICE 3

1. L'affirmation est fausse. Par exemple, 4 divise 12, 6 divise 12 mais $6 \times 4 = 24$ ne divise pas 12.
2. L'affirmation est vraie. En effet, soit a , b et c des entiers naturels tels que c divise a et b et tels que a et b sont premiers entre eux. Alors, comme c divise a et b , c divise $\text{PGCD}(a, b) = 1$. De plus, $c \geq 0$ donc $c = 1$.
3. L'affirmation est vraie. En effet, pour tout $n \in \mathbb{N}^*$, $0 \leq \text{PGCD}(n, 10) \leq 10$ donc, comme $n > 0$, $0 \leq u_n \leq \frac{10}{n}$. Or, $\lim_{n \rightarrow +\infty} \frac{10}{n} = 0$ donc, par le théorème d'encadrement, $\lim_{n \rightarrow +\infty} u_n = 0$ et ainsi, (u_n) est bien convergente.
4. L'affirmation est fausse. En effet, les seuls diviseurs positifs de 3 sont 1 et 3 donc, pour tout $n \in \mathbb{N}^*$, $\text{PGCD}(n, 3) \in \{1, 3\}$. Plus précisément, pour tout $n \in \mathbb{N}^*$, $\text{PGCD}(n, 3) = 3$ si 3 divise n et $\text{PGCD}(n, 3) = 1$ sinon. Or, pour tout $n \in \mathbb{N}^*$, $\text{PGCD}(n, 3)\text{PPCM}(n, 3) = 3n$ donc $v_n = \frac{3}{\text{PGCD}(3, n)}$ i.e. $v_n = 1$ si 3 divise n et $v_n = 3$ sinon. La suite (v_n) est donc périodique de période 3 et ses valeurs sur une période sont 3, 3 et 1 :

$$3, 3, 1, 3, 3, 1, 3, 3, 1, 3, 3, 1, 3, 3, 1, 3, 3, 1, \dots$$

Ainsi, (v_n) n'est pas convergente.