Devoir surveillé n°5

Durée : 1 heure
L'utilisation d'une calculatrice est autorisée

Exercice 1. — Une équation diophantienne (6 points)

On considère l'équation $(E) : 9x - 26y = 1$ d'inconnue $(x\,;y) \in \mathbb{Z}^2$.

1. Donner une solution simple $(x_0\,;y_0)$ de cette équation, de sorte que x_0 et y_0 soient des nombres entiers compris entre 0 et 3.
2. Résoudre l'équation (E) dans $\mathbb{Z}^2$.
3. On suppose que $(x\,;y) \in \mathbb{Z}^2$ est solution de (E). Déterminer $\text{PGCD}(x, 26)$.

Exercice 2. — Cryptage par la méthode de Hill (8 points)

1. **Méthode de cryptage**

   Étant donné un mot ayant un nombre pair de lettres, on le crypte de la manière suivante.

   a. On regroupe les lettres par paires.

   b. On remplace les lettres par les valeurs associées à l'aide du tableau suivant et on place les couples de nombres obtenus dans des matrices colonnes.

   c. On multiplie à gauche les matrices colonnes par la matrice $A = \begin{pmatrix} 9 & 4 \\ 7 & 3 \end{pmatrix}$.

   d. On remplace chaque coefficient des matrices colonnes obtenues par son reste dans la division euclidienne par 26.

   e. On utilise, à nouveau, le tableau ci-dessous pour obtenir le mot crypté.

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

Exemple. — On considère le mot « MATH ». On le sépare en « MA » et « TH ». On a ensuite

$$\text{MA} \to C_1 = \begin{pmatrix} 12 \\ 0 \end{pmatrix} \to AC_1 = \begin{pmatrix} 108 \\ 84 \end{pmatrix} \to \begin{pmatrix} 4 \\ 6 \end{pmatrix} \to \text{EG}$$

et

$$\text{TH} \to C_2 = \begin{pmatrix} 19 \\ 7 \end{pmatrix} \to AC_2 = \begin{pmatrix} 199 \\ 154 \end{pmatrix} \to \begin{pmatrix} 17 \\ 24 \end{pmatrix} \to \text{RY}$$

donc le mot crypté est « EGRY ».

En cryptant par cette méthode le mot « PION », on obtient « LZWH ». En détaillant les étapes pour les lettres « ES », crypter le mot « ESPION ».

2. Méthode de décryptage

Lorsqu'on manipule des matrices de nombres entiers relatifs, on peut utiliser la notation « $\equiv$ » pour parler de congruence coefficient par coefficient. Par exemple, on peut écrire $\begin{pmatrix}108\\84\end{pmatrix} \equiv \begin{pmatrix}4\\6\end{pmatrix}$ [26] car $108 \equiv 4$ [26] et $84 \equiv 6$ [26].

a. Montrer que, pour toute matrice carrée $M = \begin{pmatrix}a & b\\c & d\end{pmatrix}$ d'ordre 2 et pour toutes matrices colonnes $X = \begin{pmatrix}x_1\\x_2\end{pmatrix}$ et $Y = \begin{pmatrix}y_1\\y_2\end{pmatrix}$ de taille 2×1, si $X \equiv Y$ [26] alors $MX \equiv MY$ [26].

b. Établir que la matrice A est inversible puis déterminer son inverse.

c. En expliquant sa démarche, décrypter le mot « XQGY ».

Exercice 3 (6 points). — Pour chacune des affirmations suivantes, dire si elle est VRAIE ou FAUSSE en justifiant sa réponse.

1. Pour tous entiers relatifs distincts a, b et c, si a divise c et b divise c alors ab divise c.

2. Pour tous entiers naturels a, b et c, si c divise a et b et si a et b sont premiers entre eux alors $c = 1$.

3. La suite (u_n) définie, pour tout $n \in \mathbb{N}^*$, par $u_n = \dfrac{1}{n}\text{PGCD}(n, 10)$ est convergente.

4. (*bonus*) La suite (v_n) définie, pour tout $n \in \mathbb{N}^*$, par $v_n = \dfrac{1}{n}\text{PPCM}(n, 3)$ est convergente.