

## Exercice 4 (5 points)

### Candidats ayant choisi l'enseignement de spécialité

#### Partie A : préliminaires

1. a) Soient  $n$  et  $N$  deux entiers naturels supérieurs ou égaux à 2, tels que :

$$n^2 \equiv N-1 \text{ modulo } N.$$

Montrer que :  $n \times n^3 \equiv 1 \text{ modulo } N$ .

- b) Dédurre de la question précédente un entier  $k_1$  tel que :  $5k_1 \equiv 1 \text{ modulo } 26$ .

On admettra que l'unique entier  $k$  tel que :  $0 \leq k \leq 25$  et  $5k \equiv 1 \text{ modulo } 26$  vaut 21.

2. On donne les matrices :  $A = \begin{pmatrix} 4 & 1 \\ 3 & 2 \end{pmatrix}$ ,  $B = \begin{pmatrix} 2 & -1 \\ -3 & 4 \end{pmatrix}$ ,  $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ ,  $X = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$  et  $Y = \begin{pmatrix} y_1 \\ y_2 \end{pmatrix}$ .

- a) Calculer la matrice  $6A - A^2$ .

b) En déduire que  $A$  est inversible et que sa matrice inverse, notée  $A^{-1}$ , peut s'écrire sous la forme  $A^{-1} = \alpha I + \beta A$ , où  $\alpha$  et  $\beta$  sont deux réels que l'on déterminera.

- c) Vérifier que :  $B = 5A^{-1}$ .

- d) Démontrer que si  $AX = Y$ , alors  $5X = BY$ .

#### Partie B : procédure de codage

Coder le mot « ET », en utilisant la procédure de codage décrite ci-dessous.

- Le mot à coder est remplacé par la matrice  $X = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$ , où  $x_1$  est l'entier représentant la première lettre du mot et  $x_2$  l'entier représentant la deuxième, selon le tableau de correspondance ci-dessous :

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

- La matrice  $X$  est transformée en la matrice  $Y = \begin{pmatrix} y_1 \\ y_2 \end{pmatrix}$  telle que :  $Y = AX$ .
- La matrice  $Y$  est transformée en la matrice  $R = \begin{pmatrix} r_1 \\ r_2 \end{pmatrix}$ , où  $r_1$  est le reste de la division euclidienne de  $y_1$  par 26 et  $r_2$  le reste de la division euclidienne de  $y_2$  par 26.
- Les entiers  $r_1$  et  $r_2$  donnent les lettres du mot codé, selon le tableau de correspondance ci-dessus.

**Exemple :** « OU » (mot à coder)  $\rightarrow X = \begin{pmatrix} 14 \\ 20 \end{pmatrix} \rightarrow Y = \begin{pmatrix} 76 \\ 82 \end{pmatrix} \rightarrow R = \begin{pmatrix} 24 \\ 4 \end{pmatrix} \rightarrow$  « YE » (mot codé).

**Partie C : procédure de décodage (on conserve les mêmes notations que pour le codage)**

Lors du codage, la matrice  $X$  a été transformée en la matrice  $Y = \begin{pmatrix} y_1 \\ y_2 \end{pmatrix}$  telle que :  $Y = AX$ .

1. Démontrer que : 
$$\begin{cases} 5x_1 = 2y_1 - y_2 \\ 5x_2 = -3y_1 + 4y_2 \end{cases}$$

2. En utilisant la question 1.b) de la **partie A**, établir que :

$$\begin{cases} x_1 \equiv 16y_1 + 5y_2 \\ x_2 \equiv 15y_1 + 6y_2 \end{cases} \text{ modulo } 26.$$

3. Décoder le mot « QP ».