Exercice 4 — Candidats ayant suivi la spécialité — 5 points

Partie A : préliminaires

1 .a. Soient n et N deux entiers supérieurs ou égaux à 2, tels que :
$n^2 \equiv N-1$ modulo N
Montrer que : $n \times n^3 \equiv 1$ modulo N

b. Déduire de la question précédente un entier k_1 tel que $5k_1 \equiv 1$ modulo 26 .

On admettra que l'unique entier k tel que $0 \leqslant k \leqslant 25$ et $5k \equiv 1$ modulo 26 vaut 21.

2 . On donne les matrices : $A=\begin{pmatrix} 4 & 1 \\ 3 & 2 \end{pmatrix}$, $B=\begin{pmatrix} 2 & -1 \\ -3 & 4 \end{pmatrix}$, $X=\begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$ 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 α et β sont des 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 est 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 d 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 précédent.

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 :

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

3 . Décoder le mot **« QP ».**

Correction :

Partie A : préliminaires

1 .a. n et N sont des entiers naturels supérieurs ou égaux à 2 tels que : $n^2 \equiv N-1$ modulo N
on a $n \times n^3 = n^4 = (n^2)^2$
Donc, $n * n^3 \equiv (N-1)^2$ modulo N
$n * n^3 \equiv N^2 - 2N + 1$ modulo N
et $\boxed{n * n^3 \equiv 1}$ **modulo N**

b . Pour $n = 5$, $n^2 = 25 = 26 - 1$
Donc, $n^2 \equiv 26 - 1$ modulo 26
et $5 * 125 \equiv 1$ modulo 26

On peut choisir $k_1 = 125$
$125 = 4 \times 26 + 21$
L'unique entier k tel que $0 \leqslant k \leqslant 25$ et $5k \equiv 1$ modulo 26 est **21**.

2 .a. On peut utiliser la calculatrice pour effectuer le produit de deux matrices.

$A = \begin{pmatrix} 4 & 1 \\ 3 & 2 \end{pmatrix}$ $A^2 = \begin{pmatrix} 19 & 6 \\ 18 & 7 \end{pmatrix}$ $6A = \begin{pmatrix} 24 & 6 \\ 18 & 12 \end{pmatrix}$

$6A - A^2 = \begin{pmatrix} 5 & 0 \\ 0 & 5 \end{pmatrix} = 5.I$

b . $5.I = 6.A - A^2 = A(6.I - A) = (6.I - A)A$
$I = A\left(\frac{6}{5}I - \frac{1}{5}A\right) = \left(\frac{6}{5}I - \frac{1}{5}A\right)A$
Donc A est **une matrice inversible** et $\boxed{A^{-1} = \frac{6}{5}I - \frac{1}{5}A}$.

c. $A^{-1} = \begin{pmatrix} \frac{2}{5} & -\frac{1}{5} \\ -\frac{3}{5} & \frac{4}{5} \end{pmatrix}$ donc $5A^{-1} = \begin{pmatrix} 2 & -1 \\ -3 & 4 \end{pmatrix} = B$
$5A^{-1} = B$

d. $AX = Y \Leftrightarrow A^{-1}(AX) = A^{-1}Y \Leftrightarrow IX = A^{-1}Y \Leftrightarrow 5X = 5A^{-1}Y \Leftrightarrow \boxed{5X = BY}$

Partie B : procédure de codage

Pour « ET » $x_1 = 4$ et $x_2 = 19$ et $X = \begin{pmatrix} 4 \\ 19 \end{pmatrix}$
$Y = AX = \begin{pmatrix} 4 & 1 \\ 3 & 2 \end{pmatrix}\begin{pmatrix} 4 \\ 19 \end{pmatrix} = \begin{pmatrix} 16 + 19 \\ 12 + 38 \end{pmatrix} = \begin{pmatrix} 35 \\ 50 \end{pmatrix}$

$35=1\times26+9$ $\quad$ $50=1\times26+24$

donc $r_1=9$ et $r_2=24$ et R= $\begin{pmatrix}9\\24\end{pmatrix}$

Pour 9 on obtient la lettre J et pour 24 la lettre Y

« ET » → X = $\begin{pmatrix}4\\19\end{pmatrix}$ → Y = $\begin{pmatrix}35\\50\end{pmatrix}$ → R = $\begin{pmatrix}9\\24\end{pmatrix}$ → « JY »

Partie C : procédure de décodage

1 . Y = AX donc BY = BAX = 5X

Donc, $\begin{pmatrix}5x_1\\5x_2\end{pmatrix}=\begin{pmatrix}2&-1\\-3&4\end{pmatrix}\begin{pmatrix}y_1\\y_2\end{pmatrix}\Leftrightarrow\boxed{\begin{cases}5x_1=2y_1-y_2\\5x_2=-3y_1+4y_2\end{cases}}$

2 . On a $5x_1\equiv2y_1-y_2$ modulo 26

$21*5x_1\equiv21*2y_1-21y_2$ modulo 26

Or, $21*5\equiv1$ modulo 26 (partie A 1.b.)

et, $42\equiv16$ modulo 26 ($42=26\times1+16$)

$-21\equiv26-21$ modulo 26 soit $-21\equiv5$ modulo 26

On obtient $\boxed{x_1\equiv16y_1+5y_2}$ **modulo 26**

De même, $5x_2\equiv-3y-1+4y_2$ modulo 26

$21*5x_2\equiv-21*3y_1+21*4y_2$ modulo 26

Or, $-21\times3=-63=-3\times26+15$

$-21*3\equiv15$ modulo 26

$21\times4=84=3\times26+6$

$\boxed{21*4\equiv6}$ **modulo 26**

On obtient $\boxed{x_2\equiv15y_1+6y_2}$ **modulo 26**

3 . « QP » $y_1=16$ et $y_2=15$ et Y= $\begin{pmatrix}16\\15\end{pmatrix}$

$x_1\equiv16*16+5*5$ modulo 26

$x_1\equiv256+75$ modulo 26

$x_1\equiv331$ modulo 26

$331=26\times12+19$

$331\equiv19$ modulo 26 $\quad$ $0\leqslant19\leqslant25$

donc $\boxed{x_1=19}$

$x_2\equiv15*16+6*15$ modulo 26

$x_2\equiv240+90$ modulo 26

$x_2\equiv330$ modulo 26

$330=26\times12+18$

$x_2\equiv18$ modulo 26 $\quad$ $0\leqslant18\leqslant25$

donc $\boxed{x_2=18}$

et X= $\boxed{\begin{pmatrix}19\\18\end{pmatrix}}$

Pour 19 on obtient la lettre T et pour 18 on obtient la lettre S

« QP » → Y = $\begin{pmatrix}16\\15\end{pmatrix}$ → X = $\begin{pmatrix}19\\18\end{pmatrix}$ → TS .