Centres étrangers juin 2014

Partie A : préliminaires

1. *a.* Soient n et N deux entiers naturels 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 :

$$5\,k_1 \equiv 1 \text{ modulo } 26.$$

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

2. On donne les matrices :

$$A = \begin{pmatrix} 4 & 1 \\ 3 & 2 \end{pmatrix},\ B = \begin{pmatrix} 2 & -1 \\ -3 & 4 \end{pmatrix},\ I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},\ X = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \text{ et } Y = \begin{pmatrix} y_1 \\ y_2 \end{pmatrix}$$

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 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) $\rightarrow X = \begin{pmatrix} 14 \\ 20 \end{pmatrix}$

$$\rightarrow Y = \begin{pmatrix} 76 \\ 82 \end{pmatrix} \rightarrow R = \begin{pmatrix} 24 \\ 4 \end{pmatrix} \rightarrow \text{« YE » (mot codé).}$$

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 $\begin{cases} 5x_1 = 2y_1 - y_2 \\ 5x_1 = -3y_1 + 4y_2 \end{cases}$.

2. En utilisant la question **1. *b.*** de la **partie A**, établir que : $\begin{cases} x_1 \equiv 16y_1 + 5y_2 \\ x_1 \equiv 15y_1 + 6y_2 \end{cases}$ modulo 26

3. Décoder le mot « QP ».

CORRECTION

Partie A : préliminaires

1. *a.* N $\equiv 0$ modulo N donc si $n^2 \equiv$ N – 1 modulo N alors $n^2 \equiv -1$ modulo N donc $(n^2)^2 \equiv (-1)^2$ modulo N donc $n^4 \equiv 1$ modulo N soit : $n \times n^3 \equiv 1$ modulo N.

b. En posant $n = 5$ et N = 26, $n^2 = 25$ donc $n^2 \equiv$ N – 1 modulo N donc $n \times n^3 \equiv 1$ modulo N soit $5 \times 5^3 \equiv 1$ modulo 26
$k_1 = 5^3 = 125$

2. *a.* $A^2 = \begin{pmatrix} 19 & 6 \\ 18 & 7 \end{pmatrix}$ donc $6A - A^2 = \begin{pmatrix} 24 & 6 \\ 18 & 12 \end{pmatrix} - \begin{pmatrix} 19 & 6 \\ 18 & 7 \end{pmatrix} = \begin{pmatrix} 5 & 0 \\ 0 & 5 \end{pmatrix} = 5I.$

b. $6A - A^2 = 5I$ donc $\frac{6}{5}A - \frac{1}{5}A^2 = I$ soit $A\left(\frac{6}{5}I - \frac{1}{5}A\right) = I$

A est inversible et que sa matrice inverse, notée A^{-1}, est $A^{-1} = \frac{6}{5}I - \frac{1}{5}A$.

c. $A^{-1} = \frac{6}{5}I - \frac{1}{5}A = \begin{pmatrix} \frac{2}{5} & -\frac{1}{5} \\ -\frac{3}{5} & \frac{4}{5} \end{pmatrix} = \frac{1}{5}B$ donc $B = 5A^{-1}$.

d. Si $AX = Y$, alors $BAX = BY$ soit $5A^{-1}A = BY$ donc $5X = BY$.

Partie B : procédure de codage

« ET » (mot à coder) $\rightarrow X = \begin{pmatrix} 4 \\ 19 \end{pmatrix} \rightarrow Y = AX = \begin{pmatrix} 35 \\ 50 \end{pmatrix} \rightarrow R = \begin{pmatrix} 9 \\ 24 \end{pmatrix} \rightarrow$ « JY » (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 : $Y = AX$.

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 $Y = \begin{pmatrix} y_1 \\ y_2 \end{pmatrix}$.

1. $Y = AX \Leftrightarrow 5X = BY \Leftrightarrow 5\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} 2 & -1 \\ -3 & 4 \end{pmatrix} \times \begin{pmatrix} y_1 \\ y_2 \end{pmatrix} \Leftrightarrow \begin{cases} 5x_1 = 2y_1 - y_2 \\ 5x_1 = -3y_1 + 4y_2 \end{cases}$.

2. $21 \times 5 \equiv 1$ modulo 26 donc si $\begin{cases} 5x_1 = 2y_1 - y_2 \\ 5x_1 = -3y_1 + 4y_2 \end{cases}$ alors $\begin{cases} x_1 \equiv 21 \times 2y_1 - 21y_2 \\ x_1 \equiv -21 \times 3y_1 + 21 \times 4y_2 \end{cases}$ modulo 26

$21 \times 2 = 42 = 26 + 16$ donc $21 \times 2 \equiv 16$ modulo 26
$-21 = -26 + 5$ donc $-21 \equiv 5$ modulo 26
$-21 \equiv 5$ modulo 26 donc $-21 \times 3 \equiv 15$ modulo 26
$21 \times 4 = 84 = 26 \times 3 + 6$ donc $21 \times 4 \equiv 6$ modulo 26

si $\begin{cases} 5x_1 = 2y_1 - y_2 \\ 5x_1 = -3y_1 + 4y_2 \end{cases}$ alors $\begin{cases} x_1 \equiv 16y_1 + 5y_2 \\ x_1 \equiv 15y_1 + 6y_2 \end{cases}$ modulo 26

3. « QP » (mot à décoder) $\rightarrow Y = \begin{pmatrix} 16 \\ 15 \end{pmatrix} \rightarrow \begin{cases} x_1 \equiv 16y_1 + 5y_2 \\ x_1 \equiv 15y_1 + 6y_2 \end{cases}$ modulo 26 $\Leftrightarrow \begin{cases} x_1 \equiv 331 \\ x_1 \equiv 330 \end{cases}$ modulo 26 $\rightarrow R = \begin{pmatrix} 19 \\ 18 \end{pmatrix} \rightarrow$ « TS » (mot décodé)