Centres étrangers 2014. Enseignement de Spécialité

EXERCICE 4 (5 points) (candidats ayant suivi l'enseignement de spécialité)

Partie A : préliminaires

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

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

Montrer que : $n \times n^3 \equiv 1 \quad$ modulo N.

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

On admettra que l'unique entier k tel que : $0 \leqslant k \leqslant 25$ et $5k \equiv 1 \quad$ 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 deux réels que l'on déterminera.

c) Vérifier que : $B = 5A^{-1}$.

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

Partie B : procédure et 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 :

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

3) Décoder le mot « QP ».

 © Jean-Louis Rouget, 2014. Tous droits réservés.

Centres étrangers 2014. Enseignement de Spécialité

EXERCICE 4 (5 points) (candidats ayant suivi l'enseignement de spécialité)

Partie A : préliminaires

1) a) $n \times n^3 = n^4 = \left(n^2\right)^2$. Par hypothèse, $n^2 \equiv N-1$ modulo N ou encore $n^2 \equiv -1$ modulo N. Par suite, $\left(n^2\right)^2 \equiv (-1)^2$ modulo N ou encore

$$n \times n^3 \equiv 1 \quad \text{modulo } N.$$

b) On applique le résultat précédent à $n=5$ et $N=26$. On a $n^2 = 25$ avec $25 \equiv 26-1$ modulo 26.

D'après la question précédente, si on prend $k_1 = n^3$, alors $5k_1 = n \times n^3 \equiv 1$ modulo 26. L'entier $k_1 = 125$ convient.

2) a) $6A - A^2 = 6\begin{pmatrix} 4 & 1 \\ 3 & 2 \end{pmatrix} - \begin{pmatrix} 4 & 1 \\ 3 & 2 \end{pmatrix}\begin{pmatrix} 4 & 1 \\ 3 & 2 \end{pmatrix} = \begin{pmatrix} 24 & 6 \\ 18 & 12 \end{pmatrix} - \begin{pmatrix} 19 & 6 \\ 18 & 7 \end{pmatrix} = \begin{pmatrix} 5 & 0 \\ 0 & 5 \end{pmatrix} = 5I_2$.

b) Par suite, $A \times (6I - A) = (6I - A) \times A = 5I_2$ ou encore $A \times \frac{1}{5}(6I - A) = \frac{1}{5}(6I - A) \times A = I_2$. On en déduit que la matrice A est inversible et que

$$\boxed{A^{-1} = \frac{6}{5}I - \frac{1}{5}A.}$$

c) $5A^{-1} = 6I - A = 6\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} - \begin{pmatrix} 4 & 1 \\ 3 & 2 \end{pmatrix} = \begin{pmatrix} 2 & -1 \\ -3 & 4 \end{pmatrix} = B$.

d) $AX = Y \Rightarrow 5A^{-1}AX = 5A^{-1}Y \Rightarrow 5I_2X = BY \Rightarrow 5X = BY$.

Partie B : procédure et codage

• Le mot « ET » est remplacé par la matrice $X = \begin{pmatrix} 4 \\ 19 \end{pmatrix}$.

• La matrice X est transformée en la matrice

$$Y = AX = \begin{pmatrix} 4 & 1 \\ 3 & 2 \end{pmatrix}\begin{pmatrix} 4 \\ 19 \end{pmatrix} = \begin{pmatrix} 35 \\ 50 \end{pmatrix}.$$

• $35 = 1 \times 26 + 9$ avec $0 \leqslant 9 \leqslant 25$ et $50 = 1 \times 26 + 24$ avec $0 \leqslant 24 \leqslant 25$. Donc $r_1 = 9$ et $r_2 = 24$ ou encore $R = Y = \begin{pmatrix} 9 \\ 24 \end{pmatrix}$.

• Le vecteur colonne R est associé au mot « JY ».

$$\boxed{\text{Le mot « ET » est codé en le mot « JY ».}}$$

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

1) D'après la question 2)d) de la partie A, on a $5X = BY$ et donc

$$\begin{pmatrix} 5x_1 \\ 5x_2 \end{pmatrix} = 5X = BY = \begin{pmatrix} 2 & -1 \\ -3 & 4 \end{pmatrix}\begin{pmatrix} y_1 \\ y_2 \end{pmatrix} = \begin{pmatrix} 2y_1 - y_2 \\ -3y_1 + 4y_2 \end{pmatrix},$$

et donc $\begin{cases} 5x_1 = 2y_1 - y_2 \\ 5x_2 = -3y_1 + 4y_2 \end{cases}$.

2) On multiplie chacune des deux égalités précédentes par l'entier $k = 21$. Puisque $5k \equiv 1$ modulo 26 la question 1)b) de la partie A, on obtient

$$\begin{cases} x_1 \equiv 42y_1 - 21y_2 \\ x_2 \equiv -63y_1 + 84y_2 \end{cases} \quad \text{modulo } 26 \qquad (*).$$

D'autre part, $42 = 1 \times 26 + 16$ et donc $42 \equiv 16$ modulo 26. Ensuite, $-21 = (-1) \times 26 + 5$ et donc $-21 \equiv 5$ modulo 26. Ensuite, $-63 = (-3) \times 26 + 15$ et donc $-63 \equiv 15$ modulo 26. Enfin, $84 = 3 \times 26 + 6$ et donc $84 \equiv 6$ modulo 26. $(*)$ peut donc encore s'écrire

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

 © Jean-Louis Rouget, 2014. Tous droits réservés.

3) Le mot « QP » est associé au vecteur $Y = \begin{pmatrix} 16 \\ 15 \end{pmatrix}$. D'après la question précédente, modulo 26 $x_1 \equiv 16 \times 16 + 5 \times 15$ ou encore $x_1 \equiv 331$. Puisque $331 = 12 \times 26 + 19$, on a encore $x_1 \equiv 19$ modulo 26 et finalement $x_1 = 19$.

De même, $x_2 \equiv 15 \times 16 + 6 \times 15$ ou encore $x_2 \equiv 330$ puis $x_2 \equiv 18$ modulo 26 et finalement $x_2 = 18$.

Le vecteur $X = \begin{pmatrix} 19 \\ 18 \end{pmatrix}$ est associé au mot « TS » et donc

Le mot « QP » code le mot « TS ».

 © Jean-Louis Rouget, 2014. Tous droits réservés.