

Exercice 4

5 points

Candidats ayant suivi l'enseignement de spécialité

Deux matrices colonnes $\begin{pmatrix} x \\ y \end{pmatrix}$ et $\begin{pmatrix} x' \\ y' \end{pmatrix}$ à coefficients entiers sont dites congrues modulo 5 si et seulement

$$\text{si } \begin{cases} x \equiv x' [5] \\ y \equiv y' [5] \end{cases}.$$

Deux matrices carrées d'ordre 2 $\begin{pmatrix} a & c \\ b & d \end{pmatrix}$ et $\begin{pmatrix} a' & c' \\ b' & d' \end{pmatrix}$ à coefficients entiers sont dites congrues modulo

$$5 \text{ si et seulement si } \begin{cases} a \equiv a' [5] \\ b \equiv b' [5] \\ c \equiv c' [5] \\ d \equiv d' [5] \end{cases}.$$

Alice et Bob veulent s'échanger des messages en utilisant la procédure décrite ci-dessous.

- Ils choisissent une matrice M carrée d'ordre 2, à coefficients entiers.
- Leur message initial est écrit en lettres majuscules sans accent.
- Chaque lettre de ce message est remplacée par une matrice colonne $\begin{pmatrix} x \\ y \end{pmatrix}$ déduite du tableau ci-contre : x est le chiffre situé en haut de la colonne et y est le chiffre situé à la gauche de la ligne ; par exemple, la lettre T d'un message initial correspond à la matrice colonne $\begin{pmatrix} 4 \\ 3 \end{pmatrix}$.
- On calcule une nouvelle matrice $\begin{pmatrix} x' \\ y' \end{pmatrix}$ en multipliant $\begin{pmatrix} x \\ y \end{pmatrix}$ à gauche par la matrice M :

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = M \begin{pmatrix} x \\ y \end{pmatrix}.$$
- On calcule r' et t' les restes respectifs des divisions euclidiennes de x' et y' par 5.
- On utilise le tableau ci-contre pour obtenir la nouvelle lettre correspondant à la matrice colonne $\begin{pmatrix} r' \\ t' \end{pmatrix}$.

	0	1	2	3	4
0	A	B	C	D	E
1	F	G	H	I	J
2	K	L	M	N	O
3	P	Q	R	S	T
4	U	V	X	Y	Z

Remarque : la lettre W est remplacée par les deux lettres accolées V.

1. Bob et Alice choisissent la matrice $M = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}$.

- a. Montrer que la lettre « T » du message initial est codée par la lettre « U » puis coder le message « TE ».
- b. On pose $P = \begin{pmatrix} 3 & 1 \\ 4 & 2 \end{pmatrix}$. Montrer que les matrices PM et $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ sont congrues modulo 5.
- c. On considère A, A' deux matrices d'ordre 2 à coefficients entiers congrues modulo 5 et $Z = \begin{pmatrix} x \\ y \end{pmatrix}, Z' = \begin{pmatrix} x' \\ y' \end{pmatrix}$ deux matrices colonnes à coefficients entiers congrues modulo 5. Montrer alors que les matrices AZ et $A'Z'$ sont congrues modulo 5.

Dans ce qui suit on admet que si A, A' sont deux matrices carrées d'ordre 2 à coefficients entiers congrues modulo 5 et si B, B' sont deux matrices carrées d'ordre 2 à coefficients entiers congrues modulo 5 alors les matrices produit AB et $A'B'$ sont congrues modulo 5.

- d. On note $X = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$ et $Y = \begin{pmatrix} y_1 \\ y_2 \end{pmatrix}$ deux matrices colonnes à coefficients entiers. Dédurre des questions précédentes que si MX et Y sont congrues modulo 5 alors les matrices X et PY sont congrues modulo 5; ce qui permet de « décoder » une lettre chiffrée par la procédure utilisée par Alice et Bob avec la matrice M choisie.
 - e. Décoder alors la lettre « D ».
2. On souhaite déterminer si la matrice $R = \begin{pmatrix} 1 & 2 \\ 4 & 3 \end{pmatrix}$ peut être utilisée pour coder un message.
- a. On pose $S = \begin{pmatrix} 2 & 2 \\ 4 & 4 \end{pmatrix}$. Vérifier que la matrice RS et la matrice $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ sont congrues modulo 5.
 - b. On admet qu'un message codé par la matrice R peut être décodé s'il existe une matrice T telle que les matrices TR et I soient congrues modulo 5. Montrer que si c'est le cas alors les matrices TRS et S sont congrues modulo 5 (par la procédure expliquée en question 1. d. pour le codage avec la matrice M).
 - c. En déduire qu'un message codé par la matrice R ne peut être décodé.

Exercice 4

5 points

Candidats ayant suivi l'enseignement de spécialité

1. a.

Solution :

la lettre « T » est remplacée par $\begin{pmatrix} 4 \\ 3 \end{pmatrix}$.

$$M \begin{pmatrix} 4 \\ 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} \times \begin{pmatrix} 4 \\ 3 \end{pmatrix} = \begin{pmatrix} 10 \\ 24 \end{pmatrix} \equiv \begin{pmatrix} 0 \\ 4 \end{pmatrix} [5].$$

On en déduit donc que la lettre « T » du message initial est codée par la lettre « U ».

la lettre « E » est remplacée par $\begin{pmatrix} 4 \\ 0 \end{pmatrix}$.

$$M \begin{pmatrix} 4 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} \times \begin{pmatrix} 4 \\ 0 \end{pmatrix} = \begin{pmatrix} 4 \\ 12 \end{pmatrix} \equiv \begin{pmatrix} 4 \\ 2 \end{pmatrix} [5].$$

On en déduit donc que la lettre « E » du message initial est codée par la lettre « O ».

Finalement, le message « TE » est codé par « UO ».

b.

Solution :

$$PM = \begin{pmatrix} 3 & 1 \\ 4 & 2 \end{pmatrix} \times \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} = \begin{pmatrix} 6 & 10 \\ 10 & 16 \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} [5]. \text{ On a donc bien } PM \equiv I [5].$$

c.

Solution :

$$\text{Posons } A = \begin{pmatrix} a & c \\ b & d \end{pmatrix} \text{ et } A' = \begin{pmatrix} a' & c' \\ b' & d' \end{pmatrix}$$

$$AZ = \begin{pmatrix} a & c \\ b & d \end{pmatrix} \times \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} ax + cy \\ bx + dy \end{pmatrix} \text{ et, de même } A'Z' = \begin{pmatrix} a'x' + c'y' \\ b'x' + d'y' \end{pmatrix}$$

$$\text{On sait que } \begin{cases} a \equiv a' [5] \\ b \equiv b' [5] \\ c \equiv c' [5] \\ d \equiv d' [5] \end{cases} \text{ et } \begin{cases} x \equiv x' [5] \\ y \equiv y' [5] \end{cases}$$

Les congruences étant compatibles avec la multiplication et l'addition,

$$\text{on en déduit que : } \begin{cases} ax + cy \equiv a'x' + c'y' [5] \\ bx + dy \equiv b'x' + d'y' [5] \end{cases}$$

Finalement, on a bien $AZ \equiv A'Z' [5]$.

d.

Solution :

$$MX \equiv Y [5] \implies PMX \equiv PY [5]$$

Or on a vu dans la question 1.c. que $PM \equiv I [5]$ avec I la matrice identité d'ordre 2. On en déduit que $PMX \equiv IX [5] \equiv X [5]$.
Finalement on a bien $MX \equiv Y [5] \implies X \equiv PY [5]$.

e.

Solution :

la lettre « D » est remplacée par $\begin{pmatrix} 3 \\ 0 \end{pmatrix}$.

$$P \begin{pmatrix} 3 \\ 0 \end{pmatrix} = \begin{pmatrix} 3 & 1 \\ 4 & 2 \end{pmatrix} \times \begin{pmatrix} 3 \\ 0 \end{pmatrix} = \begin{pmatrix} 9 \\ 12 \end{pmatrix} \equiv \begin{pmatrix} 4 \\ 2 \end{pmatrix} [5].$$

On en déduit donc que la lettre « D » du message codé est décodée par la lettre « O ».

2. a.

Solution :

$$RS = \begin{pmatrix} 1 & 2 \\ 4 & 3 \end{pmatrix} \times \begin{pmatrix} 2 & 2 \\ 4 & 4 \end{pmatrix} = \begin{pmatrix} 20 & 20 \\ 20 & 20 \end{pmatrix} \equiv \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} [5].$$

b.

Solution :

$S \equiv S [5]$, on en déduit alors que $TR \equiv I [5]$ entraîne $TRS \equiv IS [5] \equiv S [5]$ d'après le résultat admis avant la question 2. d.

c.

Solution :

Supposons qu'il existe une matrice T telle que les matrices TR et I soient congrues modulo 5.

$$\begin{cases} RS \equiv \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} [5] \\ T \equiv T [5] \end{cases} \implies TRS \equiv T \times \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} [5] \equiv \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} [5].$$

Or on a prouvé dans la question précédente que $TRS \equiv S [5]$.

Finalement s'il existe une matrice T telle que les matrices TR et I soient congrues modulo 5 alors $S \equiv \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} [5]$ ce qui est évidemment absurde.

On en déduit qu'il n'existe pas de matrice carrée d'ordre 2 à coefficients entiers telle que TR et I soient congrues modulo 5. Cela signifie que le codage à l'aide de la matrice R ne pourra pas être décodé.