EXERCICE 4 Candidats ayant suivi l'enseignement de spécialité 5 points

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 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 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 lettre majuscule sans accent.

	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.

. Chaque lettre de ce message est remplacée par une matrice colonne $\begin{pmatrix} x \\ y \end{pmatrix}$ déduite du tableau ci-dessus : x est le chiffre situé en haut de la colonne et y est le chiffre situé à 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 : $\begin{pmatrix} x' \\ y' \end{pmatrix} = M \begin{pmatrix} x \\ y \end{pmatrix}$.

. On calcule r' et t' les restes respectifs des divisions euclidiennes de x' et y' par 5.

. On utilise le tableau ci-dessus pour obtenir la nouvelle lettre correspondant à la matrice colonne $\begin{pmatrix} r' \\ t' \end{pmatrix}$.

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

1.a. Montrer que la lettre « T » du message initial est codée par la lettre « U » puis coder le message « TE ».

1.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.

1.c. On considère A et A' deux matrices carrées 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 AZ' sont congrues modulo 5.

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

1.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 . Déduire des questions précédentes que si MX et Y sont 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.

1.e. Décoder 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.

2.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.

2.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).

2.c. En déduire qu'un message codé par la matrice R ne peut être décodé.

CORRECTION

Remarque : Dans cet exercice W est un mot de deux lettres.

1.a. À la lettre « T » correspond la matrice $\begin{pmatrix}4\\3\end{pmatrix}$.

$M\begin{pmatrix}4\\3\end{pmatrix}=\begin{pmatrix}1&2\\3&4\end{pmatrix}\begin{pmatrix}4\\3\end{pmatrix}=\begin{pmatrix}1\times4+2\times3\\3\times4+4\times3\end{pmatrix}=\begin{pmatrix}10\\24\end{pmatrix}$

$10=2\times5+0$ et $24=4\times5+4$

$M\begin{pmatrix}4\\3\end{pmatrix}\equiv\begin{pmatrix}0\\4\end{pmatrix}(5)$

À la matrice $\begin{pmatrix}0\\4\end{pmatrix}$ correspond la lettre « U ».

Conclusion

La lettre « T » est codée par la lettre « U ».

. À la lettre « E » correspond la matrice $\begin{pmatrix}4\\0\end{pmatrix}$.

$M\begin{pmatrix}4\\0\end{pmatrix}=\begin{pmatrix}1&2\\3&4\end{pmatrix}\begin{pmatrix}4\\0\end{pmatrix}=\begin{pmatrix}1\times4+2\times0\\3\times4+4\times0\end{pmatrix}=\begin{pmatrix}4\\12\end{pmatrix}$

$4=0\times5+4$ et $12=2\times5+2$

$M\begin{pmatrix}4\\0\end{pmatrix}\equiv\begin{pmatrix}4\\2\end{pmatrix}(5)$.

À la matrice $\begin{pmatrix}4\\2\end{pmatrix}$ correspond la lettre « O ».

Conclusion

Le message « TE » est codé en « UO ».

. Remarque : (résultat non demandé)

À la lettre « V » correspond la matrice $\begin{pmatrix}1\\4\end{pmatrix}$.

$M\begin{pmatrix}1\\4\end{pmatrix}=\begin{pmatrix}1&2\\3&4\end{pmatrix}\begin{pmatrix}1\\4\end{pmatrix}=\begin{pmatrix}9\\19\end{pmatrix}$

$9=1\times5+4$ et $19=3\times5+4$

$\begin{pmatrix}9\\19\end{pmatrix}\equiv\begin{pmatrix}4\\4\end{pmatrix}(5)$

À la matrice $\begin{pmatrix}4\\4\end{pmatrix}$ correspond la lettre « Z ».

Conclusion

Le message « W » est codé par le message « ZZ ».

1.b. $PM=\begin{pmatrix}3&1\\4&2\end{pmatrix}\begin{pmatrix}1&2\\3&4\end{pmatrix}=\begin{pmatrix}6&10\\10&16\end{pmatrix}$.

$6=1\times5+1$ et $10=2\times5+0$ et $16=3\times5+1$

$\begin{pmatrix}6&10\\10&16\end{pmatrix}\equiv\begin{pmatrix}1&0\\0&1\end{pmatrix}(5)$

$PM\equiv I(5)$

1.c. $A=\begin{pmatrix}a&c\\b&d\end{pmatrix}$ $A'=\begin{pmatrix}a'&c'\\b'&d'\end{pmatrix}$ $Z=\begin{pmatrix}x\\y\end{pmatrix}$ $Z'=\begin{pmatrix}x'\\y'\end{pmatrix}$ $AZ=\begin{pmatrix}ax+cy\\bx+dy\end{pmatrix}$ $A'Z'=\begin{pmatrix}a'x'+c'y'\\b'x'+d'y'\end{pmatrix}$

$A\equiv A'(5)\Leftrightarrow\begin{cases}a\equiv a'(5)\\b\equiv b'(5)\\c\equiv c'(5)\\d\equiv d'(5)\end{cases}$ $Z\equiv Z'(5)\Leftrightarrow\begin{cases}x\equiv x'(5)\\y\equiv y'(5)\end{cases}$

En utilisant les propriétés sur les congruences somme et produit), on obtient :
$ax+cy\equiv a'x'+c'y'(5)$ et $bx+dy\equiv b'x'+d'y'(5)$
donc $AZ\equiv A'Z'(5)$

A, A', B et B' sont 4 matrices carrées d'ordre 2 à coefficients entiers, on admet que si :
$\begin{cases} A\equiv A'(5) \\ B\equiv B'(5) \end{cases}$ alors $AB\equiv A'B'(5)$

1.d. $X=\begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$ $Y=\begin{pmatrix} y_1 \\ y_2 \end{pmatrix}$
On utilise le résultat de la question **1.c.** avec A=A'=P ($P\equiv P(5)$) et Z=MX et Z'=Y ($Z\equiv Z'(5)$)
On obtient :
$P(MX)\equiv PY(5)$
Or P(MX)=(PM)X et $PM\equiv I(5)$ donc $(PM)X\equiv IX(5)$
IX=X donc $(PM)X\equiv X(5)$
Conséquences :
$X\equiv PY(5)$
Connaissant la lettre codée, on détermine sa matrice correspondante Y, puis on calcule PY et on détermine la matrice X congrue à PY puis la lettre initiale correspondante à X.

1.e. Pour la lettre codée « D » correspond la matrice $Y=\begin{pmatrix} 3 \\ 0 \end{pmatrix}$

$PY=\begin{pmatrix} 3 & 1 \\ 4 & 2 \end{pmatrix}\begin{pmatrix} 3 \\ 0 \end{pmatrix}=\begin{pmatrix} 9 \\ 12 \end{pmatrix}$
$9=1\times5+4$ et $12=2\times5+2$
$\begin{pmatrix} 9 \\ 2 \end{pmatrix} \equiv \begin{pmatrix} 4 \\ 2 \end{pmatrix}$ (5)

La lettre correspondante à la matrice $\begin{pmatrix} 4 \\ 2 \end{pmatrix}$ est la lettre « J ».

Conclusion :
La lettre décodée de la lettre « D » est la lettre «J ».

2.a. $R=\begin{pmatrix} 1 & 2 \\ 4 & 3 \end{pmatrix}$ $S=\begin{pmatrix} 2 & 2 \\ 4 & 4 \end{pmatrix}$ $RS=\begin{pmatrix} 2+8 & 2+8 \\ 8+12 & 8+12 \end{pmatrix}=\begin{pmatrix} 10 & 10 \\ 20 & 20 \end{pmatrix}$
$10=2\times5+0$ $20=4\times5+0$
$RS \equiv \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ (5)

2.b. A=TR A'=I $A\equiv A'(5)$
B=B'=S $B\equiv B'(5)$
donc $AB\equiv A'B'(5)$ et $TRS\equiv IS(5)$
or IS=S donc $TRS\equiv S(5)$

2.c. Un message codé par la matrice R peut être décodé s'il existe une matrice T telle que $TR\equiv I(5)$.
Si on suppose qu'il existe une matrice T telle que $TR\equiv I(5)$ alors $TRS\equiv S(5)$.
Or TRS=T(RS)=T $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}=\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ on doit donc avoir S $\equiv \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ (5)
Ce résultat est absurde donc l'hypothèse proposée est fausse.
Conclusion
Il n'existe pas de matrice T telle que $TR\equiv I(5)$ et un message codé par la matrice R ne peut pas être décodé.
Remarque
On peut remarquer que les lettres « A »' « L », « X », « I » et « T » sont codées par la même lettre « A » avec la matrice R (donc on ne peut pas décoder la lettre « A »).