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

L'objet du problème est l'étude d'une méthode de cryptage dite « chiffrement de Hill », dans un cas particulier.
Cette méthode nécessite une matrice de la forme $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ dont les coefficients sont des nombres entiers choisis entre 0 et 25, et tels que ad – bc soit premier avec 26.
Cette matrice est connue seulement de l'émetteur et du destinateur.

Les deux parties de cet exercice sont indépendantes.

Partie A : quelques résultats

1. On considère l'équation (E) : $9d-26m=1$ où d et m désignent deux entiers relatifs.

a. Donner une solution simple de cette équation, de sorte que d et m soient des nombres entiers compris entre 0 et 3.

b. Démontrer que le couple $(d\,;m)$ est solution de l'équation (E) si et seulement si : $9(d=3)=25(m-1)$.

c. En déduire que les solutions de l'équation (E) sont les nombres entiers relatifs de la forme :
$\begin{cases} d=26k+3 \\ m=9k+1 \end{cases}$ $k\in\mathbb{Z}$

2.a. Soit n un nombre entier. Démontrer que si $n=26k-1$, avec k entier relatif, alors n et 26 sont premiers entre eux.

b. En déduire que les nombres $9d-28$, avec $d=26k+3$ et $k\in\mathbb{Z}$, sont premiers avec 26.

Partie B : cryptage et décryptage

On considère la matrice $A=\begin{pmatrix} 9 & 4 \\ 7 & 3 \end{pmatrix}$
On utilisera le tableau suivant pour la correspondance entre les lettres et les nombres.

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

Méthode de cryptage (pour un mot comportant un nmbre pair de lettres)	Exemple: avec le mot MATH	
1. On regroupe les lettres par paires	MA	TH
2. On remplace les lettres par les valeurs associées à l'aide du tableau précédent, et on place les couples de nombres obtenus dans les matrices colonne.	$C_1 = \begin{pmatrix} 12 \\ 0 \end{pmatrix}$	$C_2 = \begin{pmatrix} 19 \\ 7 \end{pmatrix}$
3. On multiplie les matrices colonne par la gauche par la matrice $A = \begin{pmatrix} 9 & 4 \\ 7 & 3 \end{pmatrix}$	$AC_1 = \begin{pmatrix} 108 \\ 84 \end{pmatrix}$	$AC_2 = \begin{pmatrix} 199 \\ 154 \end{pmatrix}$
4. On remplace chaque coefficientdes matrices colonne obtenues par leur reste dans la division euclienne par 26.	108=4x26+4 84=3x26+6 on obtient: $C_3 = \begin{pmatrix} 4 \\ 6 \end{pmatrix}$	199=7x26+17 154=5x26+24 on obtient: $C_4 = \begin{pmatrix} 17 \\ 24 \end{pmatrix}$
5. On utilise le tableau de correspondance entre lettres et nombres pour obtenir le mot crypté.	EG	RY

1. En cryptant par cette méthode le mot « PION », on obtient « LZWH ». En détaillant les étapes pour les lettres »ES », crypter le mot « ESPION ».

2. Méthode de décryptage

Notation : lorsqu'on manipule des matrices de nombres entiers relatifs, on peut utiliser la notation « $\equiv$ » pour parler de congruence coefficient par coefficient.
Par exemple, on peut écrire :
$\begin{pmatrix} 108 \\ 84 \end{pmatrix} \equiv \begin{pmatrix} 4 \\ 6 \end{pmatrix}$ modulo 26 car $108 \equiv 4$ modulo 26 et $84 \equiv 6$ modulo 26 .

Soient a, b, x, y, x' et y' des nombres entiers relatifs.
On sait que $x \equiv x'$ modulo26 et $y \equiv y'$ modulo 26 alors : $a\,x + b\,y \equiv a\,x' + b\,y'$ modulo 26
Ce résultat permet d'écrire que, si A est une matrice 2×2 et B et Csont deux matrices colonne 2×1 , alors :
$B \equiv C$ modulo26 implique $AB \equiv AC$ modulo 26 .

a. Etablir que la matrice A est inversible, et déterminer son inverse.
b. Décrypter le mot : XQGY.

CORRECTION

Paetie A : quelques résultats

1.a. $9d-26m=1$
On remarque $9\times3-26\times1=1$ doncle couple (3;1) est slution de cette équation.

b. $9d-26m=1=9\times3-26\times1\Leftrightarrow9(d-3)=26(m-1)$

c. 9 divise $26(m-1)$ et 9 est premier avec 26, le théorème de GAUSS nous permet d'affirmer que 9 divise $(m-1)$ et il existe un entier relatif k tel que $m-1=9k$ soit $m=9k+1$.
Conséquence
$9(d-3)=26\times9k\Leftrightarrow d-3=26k\Leftrightarrow d=26k+3$.
Conclusion
L'ensemble des solutions de l'équation (E) est l'ensemble des couples $(d;m)$ tels que :
$\begin{cases}d=26k+3\\ m=9k+1\end{cases}$ $k\in\mathbb{Z}$

2.a. k est un entier relatif
$n=26k-1$ donc $26k-1\times n=1$
Il existe deux entiers relatifs a et b tels que $a\times26+b\times n=1$ ($a=k$ et $b=-1$), le théorème de Bezout nous permet d'affirmer que n et 26 sont premiers entre eux.

b. $9d-28=9(26k+3)-28=9\times26k-1=26\times(9k)-1=26K-1$ avec $K=9k$ entier relatif
donc $9d-28$ est premier avec 26.

Partie B : cryptage et décryptage

$$A=\begin{pmatrix}9&4\\7&3\end{pmatrix}$$

1. Pour crypter « ES » en utilisant le tableau, on obtient $C=\begin{pmatrix}4\\18\end{pmatrix}$

$$AC=\begin{pmatrix}9&4\\7&3\end{pmatrix}\begin{pmatrix}4\\18\end{pmatrix}=\begin{pmatrix}9\times4+4\times18\\7\times4+3\times18\end{pmatrix}=\begin{pmatrix}108\\82\end{pmatrix}$$
$108=4\times26+4$
$82=3\times26+4$
donc $\begin{pmatrix}108\\82\end{pmatrix}\equiv\begin{pmatrix}4\\18\end{pmatrix}$ modulo26
Par lecture du tableau on obtient : « EE ».
Conclusion
Le mot « ESPION » est crypté en le mot « EELZWH »

2.a. En utilisant la calculatrice on obtient l'inverse de la matrice A :
$A^{-1}=\begin{pmatrix}-3&4\\7&-9\end{pmatrix}$.
On peut vérifier :
$$AA^{-1}=\begin{pmatrix}9&4\\7&3\end{pmatrix}\begin{pmatrix}-3&4\\7&-9\end{pmatrix}=\begin{pmatrix}-3\times9+4\times7&4\times9-9\times4\\-3\times7+3\times7&7\times4-9\times3\end{pmatrix}=\begin{pmatrix}1&0\\0&1\end{pmatrix}$$
$$A^{-1}A=\begin{pmatrix}-3&4\\7&-9\end{pmatrix}\begin{pmatrix}9&4\\7&3\end{pmatrix}=\begin{pmatrix}-3\times9+4\times7&-3\times4+4\times3\\7\times9-9\times7&7\times4-9\times3\end{pmatrix}=\begin{pmatrix}1&0\\0&1\end{pmatrix}$$

b. $AC=C'\Leftrightarrow C=A^{-1}C'$
Le mot crypté est « XQGY ».
On sépare ce mot en deux blocs de deux lettres « XQ » et « GY ».

En utilisant le tableau pour « XQ » $C_1' = \begin{pmatrix} 23 \\ 16 \end{pmatrix}$.

$$C_1 = A^{-1}C_1' = \begin{pmatrix} -3 & 4 \\ 7 & -9 \end{pmatrix}\begin{pmatrix} 23 \\ 16 \end{pmatrix} = \begin{pmatrix} -3\times 23 + 4\times 16 \\ 7\times 23 - 9\times 16 \end{pmatrix} = \begin{pmatrix} -5 \\ 17 \end{pmatrix}$$

$-5 = -1\times 26 + 21$

$17 = 0\times 26 + 17$

donc $\begin{pmatrix} -5 \\ 17 \end{pmatrix} \equiv \begin{pmatrix} 21 \\ 17 \end{pmatrix}$ modulo26

Par lecture du tableau on obtient le mot : « VR ».

En utilisant le tableau pour « GY » $C_2' = \begin{pmatrix} 6 \\ 24 \end{pmatrix}$

$$C_2 = \begin{pmatrix} -3 & 4 \\ 7 & -9 \end{pmatrix}\begin{pmatrix} 6 \\ 24 \end{pmatrix} = \begin{pmatrix} -3\times 6 + 4\times 24 \\ 6\times 7 - 9\times 24 \end{pmatrix} = \begin{pmatrix} 78 \\ -124 \end{pmatrix}$$

$78 = 3\times 26 + 0$

$-174 = -7\times 26 + 8$

donc $\begin{pmatrix} 78 \\ -124 \end{pmatrix} \equiv \begin{pmatrix} 0 \\ 8 \end{pmatrix}$ modulo26

Par lecteur du tableau pour « AI »

Conclusion

Le mot « XQGY » est décrypé en le mot **« VRAI ».**