EXERCICE 4 **5 points**

Candidats ayant choisi l'enseignement de spécialité

Le but de cet exercice est d'étudier, sur un exemple, une méthode de chiffrement publiée en 1929 par le mathématicien et cryptologue Lester Hill. Ce chiffrement repose sur la donnée d'une matrice A, connue uniquement de l'émetteur et du destinataire.

Dans tout l'exercice, on note A la matrice définie par : $A = \begin{pmatrix} 5 & 2 \\ 7 & 7 \end{pmatrix}$

Partie A – Chiffrement de Hill

Voici les différentes étapes de chiffrement pour un mot comportant un nombre pair de lettres :

<table>
<tr><td>Étape 1</td><td>On divise le mot en blocs de deux lettres consécutives puis, pour chaque bloc, on effectue chacune des étapes suivantes.</td></tr>
<tr><td>Étape 2</td><td>On associe aux deux lettres du bloc les deux entiers x_1 et x_2, tous deux compris entre 0 et 25, qui correspondent aux deux lettres dans le même ordre, dans le tableau suivant :
<table>
<tr><td>A</td><td>B</td><td>C</td><td>D</td><td>E</td><td>F</td><td>G</td><td>H</td><td>I</td><td>J</td><td>K</td><td>L</td><td>M</td></tr>
<tr><td>0</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>9</td><td>10</td><td>11</td><td>12</td></tr>
<tr><td>N</td><td>O</td><td>P</td><td>Q</td><td>R</td><td>S</td><td>T</td><td>U</td><td>V</td><td>W</td><td>X</td><td>Y</td><td>Z</td></tr>
<tr><td>13</td><td>14</td><td>15</td><td>16</td><td>17</td><td>18</td><td>19</td><td>20</td><td>21</td><td>22</td><td>23</td><td>24</td><td>25</td></tr>
</table></td></tr>
<tr><td>Étape 3</td><td>On transforme la matrice $X = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$ en la matrice $Y = \begin{pmatrix} y_1 \\ y_2 \end{pmatrix}$, vérifiant $Y = AX$.</td></tr>
<tr><td>Étape 4</td><td>On transforme la matrice $Y = \begin{pmatrix} y_1 \\ y_2 \end{pmatrix}$ 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 celui de la division euclidienne de y_2 par 26.</td></tr>
<tr><td>Étape 5</td><td>On associe aux entiers r_1 et r_2 les deux lettres correspondantes du tableau de l'étape 2. Le bloc chiffré est le bloc obtenu en juxtaposant ces deux lettres.</td></tr>
</table>

Question : utiliser la méthode de chiffrement exposée pour chiffrer le mot « HILL ».

Partie B - Quelques outils mathématiques nécessaires au déchiffrement

1. Soit a un entier relatif premier avec 26.
   Démontrer qu'il existe un entier relatif u tel que $u \times a \equiv 1$ modulo 26.
2. On considère l'algorithme suivant :

VARIABLES :	a, u, et r sont des nombres (a est naturel et premier avec 26)
TRAITEMENT :	Lire a
	u prend la valeur 0, et r prend la valeur 0
	Tant que $r \neq 1$
	u prend la valeur $u + 1$
	r prend la valeur du reste de la division euclidienne de $u \times a$ par 26
	Fin du Tant que
SORTIE :	Afficher u

On entre la valeur $a = 21$ dans cet algorithme.

a) Reproduire sur la copie et compléter le tableau suivant, jusqu'à l'arrêt de l'algorithme.

u	0	1	2	...
r	0	21	...	...

b. En déduire que $5 \times 21 \equiv 1$ modulo 26.

3. On rappelle que A est la matrice $A = \begin{pmatrix} 5 & 2 \\ 7 & 7 \end{pmatrix}$ et on note I la matrice : $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.

a. Calculer la matrice $12A - A^2$.
b. En déduire la matrice B telle que $B\,A = 21I$.
c. Démontrer que si $A\,X = Y$, alors $21X = B\,Y$.

Partie C - Déchiffrement

On veut déchiffrer le mot VLUP.

On note $X = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$ la matrice associée, selon le tableau de correspondance, à un bloc de deux lettres avant chiffrement, et $Y = \begin{pmatrix} y_1 \\ y_2 \end{pmatrix}$ la matrice définie par l'égalité : $Y = A\,X = \begin{pmatrix} 5 & 2 \\ 7 & 7 \end{pmatrix} X$

Si r_1 et r_2 sont les restes respectifs de y_1 et y_2 dans la division euclidienne par 26, le bloc de deux lettres après chiffrement est associé à la matrice $R = \begin{pmatrix} r_1 \\ r_2 \end{pmatrix}$.

1. Démontrer que : $\begin{cases} 21x_1 = 7y_1 - 2y_2 \\ 21x_2 = -7y_1 + 5y_2 \end{cases}$
2. En utilisant la question B .2., établir que : $\begin{cases} x_1 \equiv 9r_1 + 16r_2 \text{ modulo } 26 \\ x_2 \equiv 17r_1 + 25r_2 \text{ modulo } 26 \end{cases}$
3. Déchiffrer le mot VLUP, associé aux matrices $\begin{pmatrix} 21 \\ 11 \end{pmatrix}$ et $\begin{pmatrix} 20 \\ 15 \end{pmatrix}$.

CORRECTION

EXERCICE 4 **5 points**

Candidats ayant choisi l'enseignement de spécialité

Partie A – Chiffrement de Hill

Question : utiliser la méthode de chiffrement exposée pour chiffrer le mot « HILL ».

Étape 1 : Le mot « HILL » est décomposé en HI – LL.
Étape 2 : Au premier bloc HI on associe $x_1 = 7$ et $x_2 = 8$
Étape 3 : $X = \begin{pmatrix}7\\8\end{pmatrix}$ donc $Y = AX = \begin{pmatrix}5 & 2\\7 & 7\end{pmatrix}\begin{pmatrix}7\\8\end{pmatrix} = \begin{pmatrix}5\times 7+2\times 8\\7\times 7+7\times 8\end{pmatrix}$ ainsi $Y = \begin{pmatrix}51\\105\end{pmatrix}$
Étape 4 : $51 = 26\times 1+25$ donc $57 \equiv 25\ [26]$ et $105 = 26\times 4+1$ d'où $105 \equiv 1\ [26]$. Donc $R = \begin{pmatrix}25\\1\end{pmatrix}$
Étape 5 : $r_1 = 25$ correspond à la lettre Z et $r_2 = 1$ à la lettre B.
Ainsi HI est codé est ZB.

Étape 2 : Au second bloc LL on associe $x_1 = 11$ et $x_2 = 11$
Étape 3 : $X = \begin{pmatrix}11\\11\end{pmatrix}$ donc $Y = AX = \begin{pmatrix}5 & 2\\7 & 7\end{pmatrix}\begin{pmatrix}11\\11\end{pmatrix} = \begin{pmatrix}5\times 11+2\times 11\\7\times 11+7\times 11\end{pmatrix}$ ainsi $Y = \begin{pmatrix}77\\154\end{pmatrix}$
Étape 4 : $77 = 26\times 2+25$ donc $77 \equiv 25\ [26]$ et $154 = 26\times 5+24$ d'où $154 \equiv 24\ [26]$. Donc $R = \begin{pmatrix}25\\24\end{pmatrix}$
Étape 5 : $r_1 = 25$ correspond à la lettre Z et $r_2 = 24$ à la lettre Y.
Ainsi LL est codé est ZY.

Partie B - Quelques outils mathématiques nécessaires au déchiffrement

1. ***Soit a un entier relatif premier avec 26.***
   Démontrer qu'il existe un entier relatif u tel que $u \times a \equiv 1$ modulo 26.

D'après l'hypothèse, $\text{pgcd}(a, 26) = 1$ donc d'après le théorème de Bézout, il existe deux entiers u et v tels que $au + 26v = 1$ ce qui entraine $au + 26v \equiv 1\ [26]$ et donc $\boldsymbol{au \equiv 1\ [26]}$

---

2. On considère l'algorithme suivant :

VARIABLES :	$a, u,$ et r *sont des nombres (*a *est naturel et premier avec 26)*
TRAITEMENT :	*Lire* a
	u *prend la valeur 0, et* r *prend la valeur 0*
	Tant que $r \neq 1$
	u *prend la valeur* $u + 1$
	r *prend la valeur du reste de la division euclidienne de* $u \times a$ *par 26*
	Fin du Tant que
SORTIE :	*Afficher* u

On entre la valeur $a = 21$ *dans cet algorithme.*

2.a. Reproduire sur la copie et compléter le tableau suivant, jusqu'à l'arrêt de l'algorithme.

u	0	1	2	...
r	0	21	...	...

Ecrivons cet algorithme à l'aide de notre TI83 Premium CE :
On a ajouté deux lignes : **Disp U,R**
Pause
afin d'afficher au fur et à mesure les valeurs de u et r.

```
PROGRAM:EXECICE4
:Prompt A
:0→U
:0→R
:While R≠1
:U+1→U
:reste(U*A,26)→R
:Disp U,R
:Pause
:End
:Disp U
```

On exécute l'algorithme et nous avons les valeurs de u et r qui s'affichent progressivement. On appuie sur précéd entrer pour mettre fin à la pause et passer aux valeurs suivantes.

```
prgmEXECICE4
A=?21
                1
               21
```

```
                1
               21
               16
                3
               11
                4
                6
                5
                1
                5
             Fait
```

u	0	1	2	3	4	5
r	0	21	16	11	6	1

2. b. En déduire que $\mathbf{5 \times 21 \equiv 1}$ ***modulo 26.***

L'algorithme précédent s'arrête lorsque $r = 1$ c'est-à-dire lorsque le reste de la division euclidienne de au par 26 vaut 1 $\Leftrightarrow au \equiv 1$ [26]. Lorsque $r = 1$ alors d'après le tableau $u = 5$.

On a donc $5 \times 21 \equiv 1$ [26]. Ce qu'on peut vérifier par le calcul :

$5 \times 21 = 105 = 26 \times 4 + 1 \Rightarrow \mathbf{5 \times 21 \equiv 1}$ **[26]**.

---

3. a. Calculer la matrice $\mathbf{12A - A^2}$.

$12A = \begin{pmatrix} 60 & 24 \\ 84 & 84 \end{pmatrix}$ et $A^2 = \begin{pmatrix} 5 & 2 \\ 7 & 7 \end{pmatrix} \times \begin{pmatrix} 5 & 2 \\ 7 & 7 \end{pmatrix} = \begin{pmatrix} 5 \times 5 + 2 \times 7 & 5 \times 2 + 2 \times 7 \\ 7 \times 5 + 7 \times 7 & 7 \times 2 + 7 \times 7 \end{pmatrix} = \begin{pmatrix} 39 & 24 \\ 84 & 63 \end{pmatrix}$

On en déduit que $12A - A^2 = \begin{pmatrix} 60 & 24 \\ 84 & 84 \end{pmatrix} - \begin{pmatrix} 39 & 24 \\ 84 & 63 \end{pmatrix} = \begin{pmatrix} 21 & 0 \\ 0 & 21 \end{pmatrix}$ donc $\mathbf{12A - A^2 = \begin{pmatrix} 21 & 0 \\ 0 & 21 \end{pmatrix}}$.

---

3. b. En déduire la matrice B ***telle que*** $\mathbf{B\,A = 21I}$.

On a vu dans la question 3.a. que $12A - A^2 = 21I \Leftrightarrow (12I - A)A = 21I$

Si on pose $B = 12I - A = \begin{pmatrix} 12 & 0 \\ 0 & 12 \end{pmatrix} - \begin{pmatrix} 5 & 2 \\ 7 & 7 \end{pmatrix}$ soit $\mathbf{B = \begin{pmatrix} 7 & -2 \\ -7 & 5 \end{pmatrix}}$ alors on a $\mathbf{B\,A = 12I}$

---

3. c. Démontrer que si $\mathbf{A\,X = Y}$***, alors*** $\mathbf{21X = B\,Y}$.

Si $A\,X = Y$ alors $BAX = BY$ donc $21IX = BY$ ce qui prouve que $\mathbf{21X = BY}$

Partie C - Déchiffrement

1. Démontrer que : $\begin{cases} \mathbf{21x_1 = 7y_1 - 2y_2} \\ \mathbf{21x_2 = -7y_1 + 5y_2} \end{cases}$

On a $Y = A\,X = \begin{pmatrix} 5 & 2 \\ 7 & 7 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} 5x_1 + 2x_2 \\ 7x_1 + 7x_2 \end{pmatrix}$. Et d'après 3.c. étant donné que $Y = A\,X$ alors $21X = BY$

On a d'une part : $21X = 21 \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} 21x_1 \\ 21x_2 \end{pmatrix}$

Et d'autre part $BY = \begin{pmatrix} 7 & -2 \\ -7 & 5 \end{pmatrix} \begin{pmatrix} y_1 \\ y_2 \end{pmatrix} = \begin{pmatrix} 7y_1 - 2y_2 \\ -7y_1 + 5y_2 \end{pmatrix}$

On a donc $\begin{cases} \mathbf{21x_1 = 7y_1 - 2y_2} \\ \mathbf{21x_2 = -7y_1 + 5y_2} \end{cases}$

---

2. En utilisant la question B .2., établir que : $\begin{cases} x_1 \equiv 9r_1 + 16r_2 \ \ modulo\ 26 \\ x_2 \equiv 17r_1 + 25r_2 \ \ modulo\ 26 \end{cases}$

On sait que $\begin{cases} 21x_1 = 7y_1 - 2y_2 \\ 21x_2 = -7y_1 + 5y_2 \end{cases}$ ce qui entraine $\begin{cases} 21x_1 \equiv 7y_1 - 2y_2 \ \text{ modulo } 26 \\ 21x_2 \equiv -7y_1 + 5y_2 \ \text{ modulo } 26 \end{cases}$

d'où $\begin{cases} 5 \times 21x_1 \equiv 35y_1 - 10y_2 \ \text{ modulo } 26 \\ 5 \times 21x_2 \equiv -35y_1 + 25y_2 \ \text{ modulo } 26 \end{cases}$ or on sait que $5 \times 21 \equiv 1 \ [26]$ ce qui nous donne bien

$$\begin{cases} x_1 \equiv 9y_1 + 16y_2 \ \ \textbf{modulo 26} \\ x_2 \equiv 17y_1 + 25y_2 \ \ \textbf{modulo 26} \end{cases}$$

---

3. Déchiffrer le mot VLUP, associé aux matrices $\begin{pmatrix} 21 \\ 11 \end{pmatrix}$ *et* $\begin{pmatrix} 20 \\ 15 \end{pmatrix}$.

D'après la question 2. on a : $\begin{cases} x_1 \equiv 9r_1 + 16r_2 \ \ modulo\ 26 \\ x_2 \equiv 17r_1 + 25r_2 \ \ modulo\ 26 \end{cases} \Leftrightarrow \begin{cases} x_1 \equiv 9 \times 21 + 16 \times 11 \ \ modulo\ 26 \\ x_2 \equiv 17 \times 21 + 25 \times 11 \ \ modulo\ 26 \end{cases}$

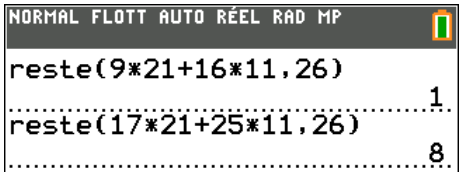
$$\Leftrightarrow \begin{cases} x_1 \equiv 365 \ \ modulo\ 26 \\ x_2 \equiv 632 \ \ modulo\ 26 \end{cases} \Leftrightarrow \begin{cases} x_1 \equiv 1 \ \ modulo\ 26 \\ x_2 \equiv 8 \ \ modulo\ 26 \end{cases}$$

VL est décodé en BI

Vérifions nos calculs à l'aide de notre TI83 Premium CE :
Pour calculer modulo 26 il suffit de trouver le reste de la division euclidienne par 26.

On appuie sur tests A [math] et dans l'onglet **NBRE** on choisit **reste** :

Ce qui nous donne bien $\begin{cases} x_1 \equiv 1 \ \ \textbf{modulo 26} \\ x_2 \equiv 8 \ \ \textbf{modulo 26} \end{cases}$

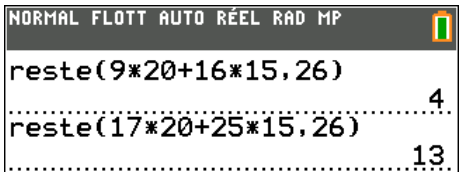


De la même façon, on a : $\begin{cases} x_1 \equiv 9r_1 + 16r_2 \ \ modulo\ 26 \\ x_2 \equiv 17r_1 + 25r_2 \ \ modulo\ 26 \end{cases} \Leftrightarrow \begin{cases} x_1 \equiv 9 \times 20 + 16 \times 15 \ \ modulo\ 26 \\ x_2 \equiv 17 \times 20 + 25 \times 15 \ \ modulo\ 26 \end{cases}$

$$\Leftrightarrow \begin{cases} x_1 \equiv 420 \ \ modulo\ 26 \\ x_2 \equiv 715 \ \ modulo\ 26 \end{cases} \Leftrightarrow \begin{cases} x_1 \equiv 4 \ \ modulo\ 26 \\ x_2 \equiv 13 \ \ modulo\ 26 \end{cases}$$

Vérifions nos calculs à l'aide de notre TI83 Premium CE :

Ce qui nous donne bien $\begin{cases} x_1 \equiv 4 \ \ \textbf{modulo 26} \\ x_2 \equiv 13 \ \ \textbf{modulo 26} \end{cases}$



UP est décodé en EN. Conclusion : VLUP est décodé en BIEN.
