Exercice n°4 (spécialité) :
Partie A

D'une part :

$$\text{HI} \longrightarrow \begin{pmatrix} H \\ I \end{pmatrix} \longrightarrow \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} 7 \\ 8 \end{pmatrix} \longrightarrow \begin{pmatrix} y_1 \\ y_2 \end{pmatrix} = \begin{pmatrix} 5 & 2 \\ 7 & 7 \end{pmatrix} \begin{pmatrix} 7 \\ 8 \end{pmatrix} = \begin{pmatrix} 51 \\ 105 \end{pmatrix} \longrightarrow \begin{pmatrix} r_1 \\ r_2 \end{pmatrix} = \begin{pmatrix} 25 \\ 1 \end{pmatrix} \longrightarrow \begin{pmatrix} Z \\ B \end{pmatrix}$$

D'autre part :

$$\text{LL} \longrightarrow \begin{pmatrix} H \\ I \end{pmatrix} \longrightarrow \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} 11 \\ 11 \end{pmatrix} \longrightarrow \begin{pmatrix} y_1 \\ y_2 \end{pmatrix} = \begin{pmatrix} 5 & 2 \\ 7 & 7 \end{pmatrix} \begin{pmatrix} 11 \\ 11 \end{pmatrix} = \begin{pmatrix} 77 \\ 154 \end{pmatrix} \longrightarrow \begin{pmatrix} r_1 \\ r_2 \end{pmatrix} = \begin{pmatrix} 25 \\ 24 \end{pmatrix} \longrightarrow \begin{pmatrix} Z \\ Y \end{pmatrix}$$

Le mot HILL est chiffré par le mot **ZBZY**

Partie B

1. Puisque a et 26 sont premiers entre eux, alors, d'après le théorème de Bèzout, il existe deux entiers u et v tels que : $au + 26v = 1$ c'est-à-dire tel que : $au = 1 - 26v$.
   On obtient que : $a \times u \equiv 26$ modulo 26.
2. **a.**

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

   b. L'algorithme affiche 5, qui est donc le plus petit entier u tel que $a \times u \equiv 1 \mod 26$.
   Par suite : $5 \times 21 \equiv 1 \mod 26$.

3. **a.**
$$\begin{aligned} 12A - A^2 &= 12\begin{pmatrix} 5 & 2 \\ 7 & 7 \end{pmatrix} - \begin{pmatrix} 5 & 2 \\ 7 & 7 \end{pmatrix}\begin{pmatrix} 5 & 2 \\ 7 & 7 \end{pmatrix} \\ &= 12\begin{pmatrix} 5 & 2 \\ 7 & 7 \end{pmatrix} - \begin{pmatrix} 5\times5+2\times7 & 5\times2+2\times7 \\ 7\times5+7\times7 & 7\times2+7\times7 \end{pmatrix} \\ &= \begin{pmatrix} 60 & 24 \\ 84 & 84 \end{pmatrix} - \begin{pmatrix} 39 & 24 \\ 84 & 63 \end{pmatrix} \\ &= \begin{pmatrix} 21 & 0 \\ 0 & 21 \end{pmatrix} \\ &= 21 \times I \end{aligned}$$

   b. L'égalité $12A - A^2 = 21I$ s'écrit $(12I - A) \times A = 21I$.
   Par suite : $B = 12I - A$.

   c. Supposons :
$$A \times X = Y$$
   Multiplions chacun des deux membres de l'égalité (à gauche) par B :
$$B \times A \times X = B \times Y$$
   Puisque $BA = 21I$, l'égalité ci-dessus s'écrit :
$$21X = BY$$
   On a prouvé :
$$AX = Y \Longrightarrow 21X = BY$$

Partie C

1. Puisque, par hypothèse, Y=AX, on en déduit, d'après la partie précédente :

$$21X = BY$$

où B est la matrice $12I - A = \begin{pmatrix} 12 & 0 \\ 0 & 12 \end{pmatrix} - \begin{pmatrix} 5 & 2 \\ 7 & 7 \end{pmatrix} = \begin{pmatrix} 7 & -2 \\ -7 & 5 \end{pmatrix}$

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

• 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 en déduit :

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

2. Multiplions chacune des deux égalités ci-dessus par 5 :

$$\begin{cases} 105x_1 = 35y_1 - 10y_2 \\ 105x_2 = -35y_1 + 25y_2 \end{cases}$$

• Prouvons : $x_1 \equiv 9r_1 + 16r_2 \mod 26$:

Puisque $105 \equiv 1 \mod 26$, alors

$$105x_1 \equiv x_1 \mod 26 \ (a)$$

De $\begin{cases} 35 \equiv 9 \mod 26 \\ \text{et} \\ y_1 \equiv r_1 \mod 26 \end{cases}$, on déduit, par somme : $35y_1 \equiv 9r_1 \mod 26$ (1).

De $\begin{cases} -10 \equiv 16 \mod 26 \\ \text{et} \\ y_2 \equiv r_2 \mod 26 \end{cases}$, on déduit, par somme : $-10y_2 \equiv 16r_2 \mod 26$ (2).

En ajoutant membre à membre les congruences (1) et (2), on obtient

$$35y_1 - 10y_2 \equiv 9r_1 + 16r_2 \mod 26 \ (b)$$

De (a) et (b) on déduit :

$$x_1 \equiv 9r_1 + 16r_2 \mod 26$$

• Un raisonnement analogue montre que

$$x_2 \equiv 17r_1 + 25r_2 \mod 26$$

3.

$$VL \to \begin{pmatrix} r_1 \\ r_2 \end{pmatrix} = \begin{pmatrix} 21 \\ 11 \end{pmatrix} \to \begin{pmatrix} 9r_1 + 16r_2 \\ 17r_1 + 25r_2 \end{pmatrix} = \begin{pmatrix} 365 \\ 632 \end{pmatrix} \to \begin{pmatrix} 1 \\ 8 \end{pmatrix} \to BI$$

$$UP \to \begin{pmatrix} r_1 \\ r_2 \end{pmatrix} = \begin{pmatrix} 20 \\ 15 \end{pmatrix} \to \begin{pmatrix} 9r_1 + 16r_2 \\ 17r_1 + 25r_2 \end{pmatrix} = \begin{pmatrix} 420 \\ 715 \end{pmatrix} \to \begin{pmatrix} 4 \\ 13 \end{pmatrix} \to EN$$

VLUP code le mot **BIEN**