

Partie (A):

$$M = \begin{pmatrix} a & b \\ 5 & 3 \end{pmatrix}, \text{ où } a, b \in \mathbb{Z}$$

1) $\det M \neq 0$ - $N = \frac{1}{\det M} \begin{pmatrix} 3 & -b \\ -5 & a \end{pmatrix}$

Comme $\det M \neq 0$, alors M est inversible
et $M^{-1} = \frac{1}{\det M} \begin{pmatrix} 3 & -b \\ -5 & a \end{pmatrix}$

Donc N est l'inverse de M

on peut calculer:

$M \times M$ et $N \times M$ et

montrer que ces 2

produits valent l'identité

2) (E): $\det M = 3$

a) $\det M = 3a - 5b = 3$ (E)

$3 \times 6 - 5 \times 3 = 18 - 15 = 3$

Donc $(6; 3)$ est une solution de (E).

b) Si $(a; b)$ solution de (E):

$3a - 5b = 3$

et on a $3 \times 6 - 5 \times 3 = 3$

} d'où $3a - 5b = 3 \times 6 - 5 \times 3$
 $\Leftrightarrow 3(a - 6) = 5(b - 3)$

c) On a: $3 \mid 5(b - 3)$
et $\text{PGCD}(5; 3) = 1$

} D'après le théorème de Gauss,
 $3 \mid b - 3$

$\Leftrightarrow \exists k \in \mathbb{Z}, b - 3 = 3k$

$\Leftrightarrow \exists k \in \mathbb{Z}, b = 3k + 3$

De même:

$5 \mid 3(a - 6)$

et $\text{PGCD}(5; 3) = 1$

} D'après le théorème de Gauss,
 $5 \mid a - 6$

$\Leftrightarrow \exists k' \in \mathbb{Z}, a - 6 = 5k'$

$\Leftrightarrow \exists k' \in \mathbb{Z}, a = 5k' + 6$

(2)

Décomposément: $3 \times 5k' = 5 \times 3k$
 $\Rightarrow k' = k$

Donc l'ensemble des solutions de (E) est:

$$S = \{(5k+6; 3k+3), k \in \mathbb{Z}\}$$

Partie (B)

1) $Q = \begin{pmatrix} 6 & 3 \\ 5 & 3 \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ avec $(a; b) = (6; 3)$

Après la partie (A), Q est inversible et $Q^{-1} = \frac{1}{\det Q} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$

$$= \frac{1}{18-15} \begin{pmatrix} 3 & -3 \\ -5 & 6 \end{pmatrix}$$

$$= \frac{1}{3} \begin{pmatrix} 3 & -3 \\ -5 & 6 \end{pmatrix}$$

$$Q^{-1} = \begin{pmatrix} 1 & -1 \\ -\frac{5}{3} & 2 \end{pmatrix}$$

2) Mot: DO

On a: $X = \begin{pmatrix} 3 \\ 14 \end{pmatrix}$

$$Y = QX = \begin{pmatrix} 6 & 3 \\ 5 & 3 \end{pmatrix} \begin{pmatrix} 3 \\ 14 \end{pmatrix}$$

$$= \begin{pmatrix} 18 + 42 \\ 15 + 3 \times 14 \end{pmatrix} = \begin{pmatrix} 60 \\ 57 \end{pmatrix}$$

Or, $60 = 26 \times 2 + 8 = r_1$

et $57 = 26 \times 2 + 5 = r_2$

d'où $R = \begin{pmatrix} 8 \\ 5 \end{pmatrix} \begin{matrix} \rightarrow I \\ \rightarrow F \end{matrix}$

C'est-à-dire DO se code en $\boxed{IF}$

3) a) $Y = QX$

Dans la question 2), on a vu que Q est inversible.

$$\underline{3Q^{-1}Y} = \underline{3 \underbrace{Q^{-1}Q}_I X} = \underline{3X}$$

(3)

$$\text{donc } \begin{pmatrix} 3x_1 \\ 3x_2 \end{pmatrix} = 3 \times \begin{pmatrix} 1 & -1 \\ -\frac{5}{3} & 2 \end{pmatrix} \times \begin{pmatrix} y_1 \\ y_2 \end{pmatrix}$$

(d'après 1) partie (B))

$$= \begin{pmatrix} 3y_1 - 3y_2 \\ -5y_1 + 6y_2 \end{pmatrix}$$

En considérant les restes dans la division euclidienne par 26:

$$\begin{cases} 3x_1 \equiv 3y_1 - 3y_2 \pmod{26} \\ 3x_2 \equiv -5y_1 + 6y_2 \pmod{26} \end{cases}$$

b) $9 \times 3 = 27 \equiv 1 \pmod{26}$

On multiplie les égalités précédentes par 9:

$$\begin{cases} 9 \times 3x_1 \equiv 9 \times 3y_1 - 9 \times 3y_2 \pmod{26} \\ 9 \times 3x_2 \equiv 9 \times (-5)y_1 + 9 \times 6y_2 \pmod{26} \end{cases}$$

c) $\begin{cases} x_1 \equiv y_1 - y_2 \pmod{26} & (\text{car } 27 \equiv 1 \pmod{26}) \\ x_2 \equiv -45y_1 + 54y_2 \pmod{26} \end{cases}$

Or, $-45 \equiv 7 \pmod{26}$ (car $-52 \equiv 0 \pmod{26}$)
et $54 \equiv 2 \pmod{26}$ (car $52 \equiv 0 \pmod{26}$)

Par conséquent:

$$\begin{cases} x_1 \equiv y_1 - y_2 \pmod{26} \\ x_2 \equiv 7y_1 + 2y_2 \pmod{26} \end{cases}$$

c) $\begin{matrix} S \rightarrow 18 \\ G \rightarrow 6 \end{matrix} \quad \left. \vphantom{\begin{matrix} S \rightarrow 18 \\ G \rightarrow 6 \end{matrix}} \right\} \text{donc } \begin{aligned} x_1 &\equiv \overbrace{18 - 6}^{=12} \pmod{26} & (\rightarrow M) \\ x_2 &\equiv 7 \times 18 + 2 \times 6 \pmod{26} \\ &\equiv 126 + 12 \pmod{26} \\ &\equiv 138 \pmod{26} \\ &\equiv 8 \pmod{26} & (\downarrow I) \end{aligned}$

Donc SG se décode en MI