CRYPTOGRAPHIE – BAC S PONDICHÉRY 2016 (SPÉ)

PARTIE A

1) $NM = \dfrac{1}{\det(M)}\begin{pmatrix} 3 & -b \\ -5 & a \end{pmatrix}\begin{pmatrix} a & b \\ 5 & 3 \end{pmatrix} = \dfrac{1}{3a-5b}\begin{pmatrix} 3a-5b & 3b-3b \\ -5a+5a & -5b+3a \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I$, I étant la matrice unité de dimension 2 × 2. On en déduit que $N = M^{-1}$.

2)

2.a) L'équation (E) est équivalente à $3a-5b=3$. Il est évident que (a = 6 ; b = 3) est solution de (E).

2.b)

$3a-5b=3 \Leftrightarrow 3a-5b=3\times6-5\times3 \Leftrightarrow 3a-3\times6=5b-5\times3 \Leftrightarrow 3(a-6)=5(b-3)$

5 divise 3(a-6) et est premier avec 3 donc d'après le théorème de Gauss, 5 divise a-6 donc il existe un entier relatif k tel que a-6=5k puis en remplaçant a par 5k+6 :

$3(5k+6-6)=5(b-3)$

Donc b=3k+3

L'ensemble des solutions est S= {(a ;b) avec a = 6 + 5k ; b = 3 + 3k et $k \in$ **Z}**.

PARTIE B

1) $Q^{-1} = \dfrac{1}{3}\begin{pmatrix} 3 & -3 \\ -5 & 6 \end{pmatrix} = \begin{pmatrix} 1 & -1 \\ -\dfrac{5}{3} & 2 \end{pmatrix}$.

2) $\text{DO} \rightarrow X = \begin{pmatrix} 3 \\ 14 \end{pmatrix} \rightarrow Y = \begin{pmatrix} 6 & 3 \\ 5 & 3 \end{pmatrix}\begin{pmatrix} 3 \\ 14 \end{pmatrix} = \begin{pmatrix} 60 \\ 57 \end{pmatrix} \rightarrow R = \begin{pmatrix} 8 \\ 5 \end{pmatrix} \rightarrow \text{IF}$.

3)

3.a) $QX = Y \Rightarrow Q^{-1}QX = Q^{-1}Y \Rightarrow X = Q^{-1}Y \Rightarrow 3X = 3Q^{-1}Y$. Alors :

$3\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} 3x_1 \\ 3x_2 \end{pmatrix} = 3\begin{pmatrix} 1 & -1 \\ -\dfrac{5}{3} & 2 \end{pmatrix}\begin{pmatrix} y_1 \\ y_2 \end{pmatrix} = \begin{pmatrix} 3 & -3 \\ -5 & 6 \end{pmatrix}\begin{pmatrix} y_1 \\ y_2 \end{pmatrix} = \begin{pmatrix} 3y_1-3y_2 \\ -5y_1+6y_2 \end{pmatrix}$. On en tire :

$\begin{cases} 3x_1 = 3y_1 - 3y_2 \\ 3x_2 = -5y_1 + 6y_2 \end{cases} \Rightarrow \begin{cases} 3x_1 \equiv 3r_1 - 3r_2 \ [26] \\ 3x_2 \equiv -5r_1 + 6r_2 \ [26] \end{cases}$.

3.b) $\begin{cases} 27x_1 \equiv 27r_1 - 27r_2 \ [26] \\ 27x_2 \equiv -45r_1 + 54r_2 \ [26] \end{cases} \Rightarrow \begin{cases} x_1 \equiv r_1 - r_2 \ [26] \\ x_2 \equiv 7r_1 + 2r_2 \ [26] \end{cases}$

3.c) $\text{SG} \rightarrow R = \begin{pmatrix} 18 \\ 6 \end{pmatrix} \rightarrow \begin{cases} x_1 \equiv 12 \ [26] \\ x_2 \equiv 138 \ [26] \end{cases} \rightarrow X = \begin{pmatrix} 12 \\ 8 \end{pmatrix} \rightarrow \text{MI}$.