DS 5 - Maths Expert.

CORRECTION

1 - a) La lettre T est associée à la matrice colonne $\begin{pmatrix} 4 \\ 3 \end{pmatrix}$

$$\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}\begin{pmatrix} 4 \\ 3 \end{pmatrix} = \begin{pmatrix} 10 \\ 24 \end{pmatrix}$$ avec $10 \equiv 0\ [5]$ et $0 \leq 0 < 5$

et $24 \equiv 4\ [5]$ et $0 \leq 4 < 5$

De plus, la matrice $\begin{pmatrix} 0 \\ 4 \end{pmatrix}$ est associée à la lettre U, donc T est codé par la lettre U.

De même. $\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}\begin{pmatrix} 4 \\ 0 \end{pmatrix} = \begin{pmatrix} 4 \\ 12 \end{pmatrix}$ avec $12 \equiv 2\ [5]$ et $0 \leq 2 < 5$

la lettre associée à la matrice $\begin{pmatrix} 4 \\ 2 \end{pmatrix}$ étant O, la lettre E sera codé par la lettre O.

$\boxed{\text{Donc "TE" sera codé par "UO"}}$

b) $$PM = \begin{pmatrix} 3 & 1 \\ 4 & 2 \end{pmatrix}\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} = \begin{pmatrix} 6 & 10 \\ 10 & 16 \end{pmatrix}$$

avec $6 \equiv 1\ [5]$ car $6 = 5 + 1$

et $16 \equiv 1\ [5]$ car $16 = 3 \times 5 + 1$

donc PM et I sont congrues modulo 5.

c) On pose $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ et $A' = \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix}$

$$AZ = \begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} ax + by \\ cx + dy \end{pmatrix}$$

$$AZ' = \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix}\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} a'x' + b'y' \\ c'x' + d'y' \end{pmatrix}$$

or A et A' sont congrues modulo 5, de même que Z et Z', donc

$$\begin{cases} \bullet\ a \equiv a' [5] \text{ et } x \equiv x' [5] \text{ d'où } ax \equiv a'x' [5] \\ \bullet\ b \equiv b' [5] \text{ et } y \equiv y' [5] \text{ d'où } by \equiv b'y' [5] \end{cases}$$

Donc $\boxed{ax + by \equiv a'x' + b'y' [5]}$

De même

$$\begin{cases} \bullet\ c \equiv c' [5] \text{ et } x \equiv x' [5] \text{ donc } cx \equiv c'x' [5] \\ \bullet\ d \equiv d' [5] \text{ et } y \equiv y' [5] \text{ donc } dy \equiv d'y' [5] \end{cases}$$

Donc $\boxed{cx + dy \equiv c'x' + d'y' [5]}$

$\boxed{\text{Donc } AZ \text{ congrue à } A'Z' \text{ modulo } 5.}$

2 - a) Supposons que MX est congrue à Y modulo 5

donc PMX est congrue à PY d'après 1-c

or PM est congrue à I, donc PMX est congrue à IX modulo 5, c'est à dire à X

Donc $\boxed{X \text{ est congrue à } PY \text{ modulo } 5.}$

b) La lettre D est associé à la matrice $\begin{pmatrix} 3 \\ 0 \end{pmatrix}$.

Supposons qu'il existe $\begin{pmatrix} x \\ y \end{pmatrix}$ tel que :

$$M\begin{pmatrix} x \\ y \end{pmatrix} \text{ est congrue à } \begin{pmatrix} 3 \\ 0 \end{pmatrix}$$

On a alors, d'après 2-a), $\begin{pmatrix} x \\ y \end{pmatrix}$ congrue à $P\begin{pmatrix} 3 \\ 0 \end{pmatrix}$

or $P\begin{pmatrix}3\\0\end{pmatrix} = \begin{pmatrix}3 & 1\\4 & 2\end{pmatrix}\begin{pmatrix}3\\0\end{pmatrix} = \begin{pmatrix}9\\12\end{pmatrix}$

or $9 \equiv 4\ [5]$ et $12 \equiv 2\ [5]$

donc $\begin{pmatrix}x\\y\end{pmatrix}$ est congrue à $\begin{pmatrix}4\\2\end{pmatrix}$ et dans ce cas, la lettre D est décodé par la lettre O

Réciproquement, $M\begin{pmatrix}4\\2\end{pmatrix} = \begin{pmatrix}1 & 2\\3 & 4\end{pmatrix}\begin{pmatrix}4\\2\end{pmatrix} = \begin{pmatrix}8\\20\end{pmatrix}$

avec $8 \equiv 3\ [5]$ et $20 \equiv 0\ [5]$
donc O est bien codé par la lettre D.

<u>Conclusion</u> :

$\boxed{\text{D est décodé par la lettre J}}$

③ - a) $RS = \begin{pmatrix}1 & 2\\4 & 3\end{pmatrix}\begin{pmatrix}2 & 2\\4 & 4\end{pmatrix} = \begin{pmatrix}10 & 10\\20 & 20\end{pmatrix}$

avec $10 \equiv 0\ [5]$ et $20 \equiv 0\ [5]$

donc RS est congrue à $\begin{pmatrix}0 & 0\\0 & 0\end{pmatrix}$ modulo 5.

b) Supposons que TR et I sont congrues modulo 5
donc, d'après ce que l'on admet dans la partie 2, on a
TRS et IS qui sont congrues modulo 5
donc $\boxed{\text{TRS et S sont congrues modulo 5.}}$

c) Supposons qu'un message codé à l'aide de la matrice $R = \begin{pmatrix}1 & 2\\4 & 3\end{pmatrix}$ puisse être décodé. Dans ce cas il existe une matrice T telle que TR et I sont congrues modulo 5, d'où, d'après 3-b, TRS et S sont congrue modulo 5

or, d'après 3-a, RS est congrue à $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ modulo 5,

donc TRS est congrue à $T \times \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$

or $T \times \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$

donc TRS est congrue à $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ modulo 5 et par conséquent S est congrue à $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ modulo 5

or $S = \begin{pmatrix} 2 & 2 \\ 4 & 4 \end{pmatrix}$ et 2 n'est pas congru à 0 modulo 5

d'où l'absurdité.

$\boxed{\text{Donc un message codé à l'aide de la matrice R ne peut pas être décodé}}$