b) Pour l'existence de m : on teste et on trouve $41 \times 7 = 287$
$= 26 \times 11 + 1$

donc m existe car $41 \times 7 \equiv 1 \quad [26]$.

Pour l'unicité de m : supposons qu'il existe $m' \in [\![0 ; 25]\!]$
tq $41m' \equiv 1 \quad [26]$.

alors $41m - 41m' \equiv 0 \quad [26]$

$\iff 41(m - m') \equiv 0 \quad [26]$

Ainsi $26 \mid 41(m - m')$

or 41 est un nombre premier et $26 \nmid 41$

donc $26 \mid (m - m')$

Comme $0 \leqslant m \leqslant 25$ et $0 \leqslant m' \leqslant 25$ on a $-25 \leqslant m - m' \leqslant 25$

Nécessairement $m - m' = 0$ (seul nombre entre -25 et 25 divisible par 26)

$\iff m = m'$.

c) ~~$mB \times \begin{pmatrix} x' \\ y' \end{pmatrix} = 7 \times \begin{pmatrix} 8 & -3 \\ -5 & 7 \end{pmatrix} \times \begin{pmatrix} x' \\ y' \end{pmatrix} = 7 \begin{pmatrix} 8x' - 3y' \\ -5x' + 7y' \end{pmatrix}$~~ inutile.

On sait que $\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} 7 & 3 \\ 5 & 8 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = A \begin{pmatrix} x \\ y \end{pmatrix}$

donc $mB \begin{pmatrix} x' \\ y' \end{pmatrix} = mBA \begin{pmatrix} x \\ y \end{pmatrix}$

$\iff mB \begin{pmatrix} x' \\ y' \end{pmatrix} = m \times 41 A^{-1} A \begin{pmatrix} x \\ y \end{pmatrix}$

$\iff mB \begin{pmatrix} x' \\ y' \end{pmatrix} = 41m \begin{pmatrix} x \\ y \end{pmatrix}$

$$\Longrightarrow mB\begin{pmatrix}x'\\y'\end{pmatrix} \equiv \begin{pmatrix}x\\y\end{pmatrix} \quad [26] \quad \text{car } 41 \times m \equiv 1 \quad [26]$$

d) D'après ce qui précède on cherche $mB = \begin{pmatrix}56 & -21\\-35 & 49\end{pmatrix}$

ainsi $\begin{pmatrix}56 & -21\\-35 & 49\end{pmatrix}\begin{pmatrix}x'\\y'\end{pmatrix} \equiv \begin{pmatrix}x\\y\end{pmatrix} \quad [26]$

et donc $\begin{pmatrix}4 & 5\\17 & 23\end{pmatrix}\begin{pmatrix}x'\\y'\end{pmatrix} \equiv \begin{pmatrix}x\\y\end{pmatrix} \quad [26]$

e) Rentrer le nombre de lettres N.
$i \leftarrow 1$
Tant que $i \leqslant N$ Faire
| Rentrer x' la valeur de la $i^{ème}$ lettre
| $i \leftarrow i+1$
| Rentrer y' la valeur de la $i^{ème}$ lettre
| $i \leftarrow i+1$
| $x \leftarrow (4x' + 5y') \,\%\, 26$
| $y \leftarrow (17x' + 23y') \,\%\, 26$
| Afficher les lettres correspondants à x et y.
Fin Tant que.

X ⟶ 23 = x'
Z ⟶ 25 = y'

donc $\begin{cases} x \equiv 4 \times 23 + 5 \times 25 \quad [26] \\ y \equiv 17 \times 23 + 23 \times 25 \quad [26] \end{cases}$

ainsi $\begin{cases} x \equiv 9 \quad [26] \\ y \equiv 4 \quad [26] \end{cases}$

XZ codait donc JE

$E \longrightarrow 4 = x'$ $\quad$ donc $\quad \begin{cases} x \equiv 4 \times 4 + 5 \times 16 & [26] \\ y \equiv 17 \times 4 + 23 \times 16 & [26] \end{cases}$

$Q \longrightarrow 16 = y'$

$$\Longleftrightarrow \begin{cases} x \equiv 18 & [26] \\ y \equiv 20 & [26] \end{cases}$$

Ainsi EQ codait SU

$G \longrightarrow 6 = x'$ $\quad$ donc $\quad \begin{cases} x \equiv 4 \times 6 + 5 \times 2 & [26] \\ y \equiv 17 \times 6 + 23 \times 2 & [26] \end{cases}$.

$C \longrightarrow 2 = y'$

$$\Longleftrightarrow \begin{cases} x \equiv 8 & [26] \\ y \equiv 18 & [26] \end{cases}.$$

Ainsi GC codait IS

$X \longrightarrow 23 = x'$ $\quad$ donc $\quad \begin{cases} \dots \end{cases} \Longleftrightarrow \begin{cases} x \equiv 20 & [26] \\ y \equiv 13 & [26] \end{cases}$

$W \longrightarrow 22 = y'$

Ainsi XW codait UN

$C \longrightarrow 2 = x'$ $\quad$ donc $\quad \dots \quad \begin{cases} x \equiv 0 & [26] \\ y \equiv 18 & [26] \end{cases}$

$O \longrightarrow 14 = y'$

Ainsi CO codait AS.

On obtient JE.SUIS.UN.AS

3) 41 et 26 sont premiers entre eux,
c'est-à-dire que leur seul diviseur commun positif est 1

4) $A = \begin{pmatrix} 6 & 2 \\ 7 & 3 \end{pmatrix}$ $\det A = \dots = 4$.

Les diviseurs communs de 4 et 26 sont 1 et 2.

5) $\begin{pmatrix} 6 & 2 \\ 7 & 3 \end{pmatrix}\begin{pmatrix} x+13 \\ y+13 \end{pmatrix} = \begin{pmatrix} 6x+78+2y+26 \\ 7x+91+3y+39 \end{pmatrix}$

$\equiv \begin{pmatrix} 6x+2y \\ 7x+3y \end{pmatrix}$ [26].

$\equiv \begin{pmatrix} 6 & 2 \\ 7 & 3 \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix}$ [26].

ainsi A est codé comme N
B comme O, etc.

Le procédé n'est pas satisfaisant.