

EXERCICE 4 : corrigé

1) Soit x un entier relatif de E .

$$\begin{aligned} g(x) = x &\Rightarrow g(x) \equiv x \pmod{27} \Rightarrow 4x + 3 \equiv x \pmod{27} \Rightarrow 3x \equiv -3 \pmod{27} \\ &\Rightarrow \text{il existe un entier relatif } k \text{ tel que } 3x = -3 + 27k \\ &\Rightarrow \text{il existe un entier relatif } k \text{ tel que } x = -1 + 9k. \end{aligned}$$

Soient alors $k \in \mathbb{Z}$ puis $x = -1 + 9k$.

$$\begin{aligned} x \in E &\Leftrightarrow 0 \leq -1 + 9k \leq 26 \Leftrightarrow 1 \leq 9k \leq 27 \\ &\Leftrightarrow \frac{1}{9} \leq k \leq 3 \Leftrightarrow 1 \leq k \leq 3. \end{aligned}$$

$k = 1$ fournit $x = 8$, $k = 2$ fournit $x = 17$ et $k = 3$ fournit $x = 26$.

Réciproquement,

- si $x = 8$, alors $g(x) \equiv 4 \times 8 + 3 \pmod{27}$ puis $g(x) \equiv 35 \pmod{27}$ puis $g(x) \equiv 35 - 27 \pmod{27}$ puis $g(x) \equiv 8 \pmod{27}$ et enfin $g(x) = 8$.
- si $x = 17$, alors $g(x) \equiv 4 \times 17 + 3 \pmod{27}$ puis $g(x) \equiv 71 \pmod{27}$ puis $g(x) \equiv 71 - 54 \pmod{27}$ puis $g(x) \equiv 17 \pmod{27}$ et enfin $g(x) = 17$.
- si $x = 26$, alors $g(x) \equiv 4 \times 26 + 3 \pmod{27}$ puis $g(x) \equiv 4 \times (-1) + 3 \pmod{27}$ puis $g(x) \equiv -1 \pmod{27}$ puis $g(x) \equiv -1 + 27 \pmod{27}$ puis $g(x) \equiv 26 \pmod{27}$ et enfin $g(x) = 26$.

Les entiers x éléments de E tels que $g(x) = x$ sont 8, 17 et 26. On en déduit que les caractères invariants dans ce codage sont i, r et \star .

Les caractères invariants dans ce codage sont i, r et \star .

2) Soient x et y deux éléments de E .

$$\begin{aligned} y &\equiv 4x + 3 \pmod{27} \Rightarrow 7y \equiv 28x + 21 \pmod{27} \\ &\Rightarrow 7y \equiv x - 6 \pmod{27} \quad (\text{car } 28 = 1 + 27 \text{ et } 21 = -6 + 27) \\ &\Rightarrow x - 6 \equiv 7y \pmod{27} \Rightarrow x - 6 + 6 \equiv 7y + 6 \pmod{27} \\ &\Rightarrow x \equiv 7y + 6 \pmod{27}. \end{aligned}$$

Soient alors y_1 et y_2 deux éléments de E codant deux éléments x_1 et x_2 de E .

$$\begin{aligned} y_1 = y_2 &\Rightarrow 7y_1 = 7y_2 \Rightarrow 7y_1 + 6 = 7y_2 + 6 \\ &\Rightarrow 7y_1 + 6 \equiv 7y_2 + 6 \pmod{27} \Rightarrow x_1 \equiv x_2 \pmod{27} \\ &\Rightarrow x_1 = x_2 \quad (\text{car } 0 \leq x_1 \leq 26 \text{ et } 0 \leq x_2 \leq 26). \end{aligned}$$

Par contraposition, si $x_1 \neq x_2$, alors $y_1 \neq y_2$ ou encore deux éléments distincts de E sont codés par deux éléments distincts de E . Maintenant, deux éléments distincts de E sont associés à deux caractères distincts et deux caractères distincts sont associés à deux éléments distincts de E .

On a donc montré que deux caractères distincts sont codés par deux caractères distincts.

3) Un caractère d'un mot codé a pour rang un élément y de E . On calcule $7y + 6$ puis on calcule le reste x de la division euclidienne de $7y + 6$ par 27. x est le rang du caractère décodé.

4) • La lettre v a pour rang le nombre $y = 21$. $7y + 6 \equiv 7 \times (-6) + 6 \pmod{27}$ ou encore $7y + 6 \equiv -36 \pmod{27}$ ou encore $7y + 6 \equiv -36 + 2 \times 27 \pmod{27}$ ou enfin $7y + 6 \equiv 18 \pmod{27}$ avec $0 \leq 18 \leq 26$. 18 est le rang de la lettre s et donc

la lettre v code la lettre s.

• La lettre f est a pour rang le nombre $y = 5$. $7y + 6 \equiv 7 \times 5 + 6 \pmod{27}$ ou encore $7y + 6 \equiv 41 \pmod{27}$ ou encore $7y + 6 \equiv 41 - 27 \pmod{27}$ ou enfin $7y + 6 \equiv 14 \pmod{27}$ avec $0 \leq 14 \leq 26$. 14 est le rang de la lettre o et donc

la lettre f code la lettre o.

Finalement

le mot « vfv » code le mot « sos ».