$$\mathbb{Z}_{26}^* = \{1; 3; 5; 7; 9; 11; 15; 17; 19; 21; 23; 25\}$$

Les nombres pairs ne sont pas inversibles mod 26.

$2k \notin \mathbb{Z}_{26}^*$ $\quad 1 \leq k \leq 12$ / $m \in \mathbb{Z}_{26}$

$2k \cdot m \equiv 1 \bmod 26$ $\quad 26 \mid (2km - 1)$

$(2km - 1) = \ell \cdot 26$ ce qui est impossible

impair $\quad$ pair

$\Rightarrow$ les nombres pairs sont exclus.

$13 \cdot m \equiv 1 \bmod 26$

13 n'est pas inversible mod 26.

$\Leftrightarrow \quad 13m - 1 = k \cdot 26$

$\Leftrightarrow \quad 13m - 1 = 2k \cdot 13$

$13m = 2k \cdot 13 + 1$ n'est pas multiple de 13

$3 \cdot 9 = 27 = 26 + 1 \equiv 1 \mod 26$

$\Rightarrow$ 3 et 9 sont dans $\mathbb{Z}_{26}^*$

$5 \cdot 21 = 105 = 104 + 1 = 4 \cdot 26 + 1 \equiv 1 \mod 26$

$\Rightarrow$ 5 et 21 $\in \mathbb{Z}_{26}^*$

$7 \cdot 15 = 105 \equiv 1 \mod 26$

$\Rightarrow$ 7 et 15 $\in \mathbb{Z}_{26}^*$

$11 \cdot 19 = 209 = 208 + 1 = 8 \cdot 26 + 1 \equiv 1 \mod 26$

$\Rightarrow$ 11 et 19 $\in \mathbb{Z}_{26}^*$

$17 \cdot 23 = 391 = 390 + 1 = 15 \cdot 26 + 1 \equiv 1 \mod 26$

$\Rightarrow$ 17 et 23 $\in \mathbb{Z}_{26}^*$

$25 \cdot 25 = 625 = 624 + 1 = 24 \cdot 26 + 1 \equiv 1 \mod 26$

$\Rightarrow$ 25 $\in \mathbb{Z}_{26}^*$