

$$\textcircled{1} \textcircled{A} 11x - 26y = 1 \quad (E)$$

Recherchons une solution particulière de (E) à l'aide de l'algorithme d'Euclide.

$$26 = 11 \times 2 + 4$$

$$11 = 4 \times 2 + 3$$

$$4 = 3 + 1$$

$$\text{d'où } 1 = 4 - 3$$

$$\Leftrightarrow 1 = 4 - (11 - 4 \times 2)$$

$$\Leftrightarrow 1 = 4 \times 3 - 11$$

$$\Leftrightarrow 1 = (26 - 11 \times 2) \times 3 - 11$$

$$\Leftrightarrow 1 = 26 \times 3 - 7 \times 11$$

Donc  $-7 \times 11 + 3 \times 26 = 1 \Rightarrow (-7; -3)$  solution particulière de (E)

$$\text{D'autre part } (E) \Leftrightarrow 11x - 26y = 1$$

$$\text{Donc par différence, } 11(x+7) - 26(y+3) = 0$$

$$\Leftrightarrow 11(x+7) = 26(y+3) \quad (*)$$

11 et  $26 = 2 \times 13$  sont premiers entre eux

(\*) montre que  $\left. \begin{array}{l} 11 \mid 26(y+3) \\ 11 \cap 26 = 1 \end{array} \right\} \Rightarrow \text{d'après le théorème de Gauss}$

$$11 \mid y+3$$

Donc il existe  $k \in \mathbb{Z}$  tel que  $y = 11k - 3$

En reportant cette valeur de  $y$  dans (\*) on a  $11(x+7) = 26 \times 11k$

$$\Rightarrow x = 26k - 7$$

Vérifions que  $x = 26k - 7; y = 11k - 3; k \in \mathbb{Z}$  est bien solution de (E)

$$\begin{aligned} 11x - 26y &= 11 \times 26k - 11 \times 7 - 26 \times 11k + 26 \times 3 \\ &= -11 \times 7 + 26 \times 3 = 1 \end{aligned}$$

$$\text{d'où } S = \{(26k - 7, 11k - 3); k \in \mathbb{Z}\}$$

$$\textcircled{2} \text{ on veut } 0 \leq 26k - 7 \leq 25$$

$$\Leftrightarrow 7 \leq 26k \leq 32 \Leftrightarrow \frac{7}{26} \leq k \leq \frac{32}{26}$$

et  $\frac{7}{26} = 0, \dots; \frac{32}{26} = 1, \dots$  d'où la seule valeur entière de  $k$  est  $k = 1$

le couple  $(u, v)$  cherché est  $(19, 8)$

$$\text{Donc } 11 \times 19 - 26 \times 8 = 1$$

③ ①  $W$  est associée à 22

$$\begin{aligned} \text{et } 11x + 8 &\equiv 11(-4) + 8 \pmod{26} \\ &\equiv -36 \pmod{26} \\ &\equiv 16 \pmod{26} \end{aligned}$$

et 16 est associée à  $Q$  donc  $W$  est codé par  $Q$

② ①  $11x \equiv j \pmod{26} \rightarrow 11 \times 19 x \equiv 19j \pmod{26}$  (Compatibilité de la congruence avec le produit)

$$\rightarrow x \equiv 19j \pmod{26} \text{ car d'après ① } 11 \times 19 = 1 + 26 \times 8 \equiv 1 \pmod{26}$$

Réciproquement:

$$\begin{aligned} x \equiv 19j \pmod{26} &\Rightarrow 11x \equiv 11 \times 19j \pmod{26} \text{ (Compatibilité avec le produit)} \\ &\Rightarrow 11x \equiv j \pmod{26}. \end{aligned}$$

Finalement on a bien

$$11x \equiv j \pmod{26} \Leftrightarrow x \equiv 19j \pmod{26}$$

② Supposons qu'une lettre codée soit associée à  $y$ . Il faut résoudre  $11x + 8 \equiv y \pmod{26} \Leftrightarrow 11x \equiv y - 8 \pmod{26}$

③ Soit une lettre codée par  $W$  (associée à 22)

$$\text{c'est que } 11x + 8 \equiv 22 \pmod{26}$$

$$\Leftrightarrow 11x \equiv 14 \pmod{26}$$

$$\Leftrightarrow x \equiv 19 \times 14 \pmod{26}$$

$$\equiv (-7) \times (-12) \equiv 84 \equiv 3 \times 26 + 6 \pmod{26}$$

$$\equiv 6 \pmod{26} \text{ et } 6 \text{ associée à } G.$$

d'où la valeur de  $x$  est la lettre associée

d'où  $W$  se décode par  $G$ .

④ ① faisons la division de  $a$  par  $b$ :

$$\begin{array}{r} m^3 - 2m + 5 \\ m^3 + m^2 \\ \hline -m^2 - 2m + 5 \\ -m^2 - m \\ \hline -m + 5 \\ -m - 1 \\ \hline 6 \end{array}$$

$$\text{d'où } a = b(m^2 - m - 1) + 6$$

Donc d'après le th fondamental du PGCD

$$\text{on a } \text{PGCD}(a, b) = \text{PGCD}(b, 6)$$

$$\textcircled{2} \frac{a}{b} = m^2 - m - 1 + \frac{6}{b}$$

donc  $\frac{a}{b} \in \mathbb{Z} \Leftrightarrow \frac{6}{b} \in \mathbb{Z} \Leftrightarrow b$  diviseur de 6 d'où  $b \in \{-6, -3, -2, -1, 1, 2, 3, 6\}$

Donc  $m \in \{-7, -4, -3, -2, 0, 1, 2, 5\}$

$$\textcircled{2} \text{PGCD}(a, b) = 3 \Leftrightarrow \text{PGCD}(b, 6) = 3$$

$$\Leftrightarrow b \text{ multiple de } 3 \text{ sans être multiple de } 2$$

$$\Leftrightarrow b = 3k \text{ avec } k \text{ non multiple de } 2 \text{ (c'est-à-dire impair)}$$

$$\Leftrightarrow b = 3(2k' + 1)$$

$$\Leftrightarrow b = 6k' + 3 \Leftrightarrow b \equiv 3 \pmod{6} \Leftrightarrow m \equiv 2 \pmod{6}$$

Conclusion:  $\text{PGCD}(a, b) = 3 \Leftrightarrow b \equiv 3 \pmod{6}$