


On veut résoudre 
$$\begin{cases} x_c \alpha + \beta \equiv x_m \pmod{26} & (1) \\ y_c \alpha + \beta \equiv y_m \pmod{26} & (2) \end{cases}$$

De (1)-(2), on tire :

$$(x_c - y_c) \alpha \equiv x_m - y_m \pmod{26} (*)$$

  $x_c - y_c$  n'est pas toujours inversible modulo 26.

En notant  $d = \text{pgcd}(x_c - y_c, x_m - y_m)$ , (\*) équivaut à :

$$k_c \alpha \equiv k_m \pmod{26}$$

il suffit de diviser  
par  $d$  des 2 côtés

avec  $k_c, k_m \in \mathbb{Z}$  tels que  $x_c - y_c = d k_c$  et  $x_m - y_m = d k_m$ .

Rq : contrairement à  $x_c - y_c$ ,  $k_c$  est toujours inversible modulo 26 !

(savez-vous pourquoi ?)

On en déduit :  $\alpha \equiv k_c^{-1} k_m \pmod{26}$

et  $\beta \equiv x_m - x_c \alpha \pmod{26}$