Par l'absurde, supposons k_c non inversible modulo 26.

Alors k_c et 26 ne sont pas premiers entre eux

donc $\text{pgcd}(k_c, 26) > 1$.

On en déduit $\text{pgcd}(k_c, 26) \mid k_M$ et donc

$\text{pgcd}(k_c, 26)$ est un diviseur commun à k_c et k_M ce

qui contredit le fait que $\text{pgcd}(k_c, k_M) = 1$ par

définition de k_c et k_M.