Exercice 1 : Déchiffrer avec l'inverse modulaire de *a*

Pré requis : Règles d'opérations sur les congruences.

Objectifs : Utiliser les opérations sur les congruences. Utiliser l'inverse modulaire pour simplifier.

- On code les 26 lettres de l'alphabet en 26 entiers naturels x avec la table de codage suivante :

Lettre en clair	A	B	C	D	E	F	...	X	Y	Z
x	0	1	2	3	4	5	...	23	24	25

- On considère la fonction de chiffrement $f: x \mapsto y = f(x)$ définie sur $\{0; 1; 2; \dots; 24; 25\}$ où y est le reste de la division de $17x + 22$ par 26.

On remarque qu'on a alors la relation de congruence simplifiée : $y \equiv 17x + 22 \quad (26)$.

Lettre en clair	A	B	C	D	E	F	...	X	Y	Z
x	0	1	2	3	4	5	...	23	24	25
y	22	13	4	21	12	3		23	14	5

- Par lecture inverse de la table de codage, on déduit de y la lettre chiffrée :

Lettre en clair	A	B	C	D	E	F	...	X	Y	Z
x	0	1	2	3	4	5	...	23	24	25
y	22	13	4	21	12	3		23	14	5
Lettre chiffrée	W	N	E	V	M	D		X	O	F

1) Chiffrer le mot GRIS
2) On considère un entier[1] u tel que $17u \equiv 1 \quad (26)$.
   a) Démontrer que u est impair.
   b) Déterminer u.
3) En déduire l'expression d'une fonction de déchiffrement $g: y \mapsto x = g(y)$ de $\{0; 1; 2; \dots; 24; 25\}$ dans $\{0; 1; 2; \dots; 24; 25\}$ telle que : $\quad y = f(x) \iff x = g(y)$

> ***Méthode :***
> - On isole x dans $y \equiv 17x + 22 \quad (26)$ en multipliant les deux membres par u.
> - On utilise la propriété « Dans une relation de congruence, on peut remplacer un des nombres par un autre qui lui est congru »

4) Déchiffrer le mot SWZQ.

[1] Un tel entier *u* est **l'inverse modulaire** de 17 pour la multiplication modulo 26