Partie A : Restitution organisée de connaissance

Soit *a*, *b*, *c*, *d* des entiers relatifs et *n* un entier naturel non nul.

Montrer que si $a \equiv b \left[\mathrm{mod}\, n \right]$ et $c \equiv d \left[\mathrm{mod}\, n \right]$ alors $ac \equiv bd \left[\mathrm{mod}\, n \right]$.

Partie B : Inverse de 23 modulo 26

On considère l'équation (E) : 23*x* – 26*y* = 1, où *x* et *y* désignent deux entiers relatifs.

1. Vérifier que le couple (–9 ; –8) est solution de l'équation (E).

2. Résoudre alors l'équation (E).

3. En déduire un entier *a* tel que $0 \leq a \leq 25$ et $23a \equiv 1 \left[\mathrm{mod}\, 26 \right]$.

Partie C : Chiffrement de Hill

On veut coder un mot de deux lettres selon la procédure suivante :

Étape 1 : Chaque lettre du mot est remplacée par un entier en utilisant le tableau ci-dessous :

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

On obtient un couple d'entiers $\left(x_1 ; x_2 \right)$ où x_1 correspond à la première lettre du mot et x_2 correspond à la deuxième lettre du mot.

Étape 2 : $\left(x_1 ; x_2 \right)$ est transformé en $\left(y_1 ; y_2 \right)$ tel que : $\left(\mathrm{S}_1 \right) \begin{cases} y_1 = 11x_1 + 3x_2 \left[\mathrm{mod}\, 26 \right] \\ y_2 = 7x_1 + 4x_2 \left[\mathrm{mod}\, 26 \right] \end{cases}$ avec $0 \leq y_1 \leq 25$ et $0 \leq y_2 \leq 25$.

Étape 3 : $\left(y_1 ; y_2 \right)$ est transformé en un mot de deux lettres en utilisant le tableau de correspondance donné dans l'étape 1.

Exemple : $\underset{\textit{mot en clair}}{\mathrm{TE}} \rightarrow (19 ; 4) \rightarrow (13 ; 19) \rightarrow \underset{\textit{mot codé}}{\mathrm{NT}}$.

1. Coder lemot ST.

2. On veut maintenant déterminer la procédure de décodage.

a. Montrer que tout couple $\left(x_1 ; x_2 \right)$ vérifiant les équations du système (S_1), vérifie les équations du système :

$$\left(\mathrm{S}_2 \right) \begin{cases} 23x_1 \equiv 4y_1 + 23y_2 \left[\mathrm{mod}\, 26 \right] \\ 23x_2 \equiv 19y_1 + 11y_2 \left[\mathrm{mod}\, 26 \right] \end{cases}.$$

b. À l'aide de la partie B, montrer que tout couple $\left(x_1 ; x_2 \right)$ vérifiant les équations du système (S_2), vérifie les équations du système (S_3) : $\left(\mathrm{S}_3 \right) \begin{cases} x_1 \equiv 16y_1 + y_2 \left[\mathrm{mod}\, 26 \right] \\ x_2 \equiv 11y_1 + 5y_2 \left[\mathrm{mod}\, 26 \right] \end{cases}$.

c. Montrer que tout couple $\left(x_1 ; x_2 \right)$ vérifiant les équations du système (S_3), vérifie les équations du système (S_1).

d. Décoder lemot YJ.