

Pondichéry 2012. Enseignement de spécialité

EXERCICE 4 (5 points)

Partie A Restitution organisée de connaissances

Soit a, b, c et d des entiers relatifs et n un entier naturel non nul.
 Montrer que si $a \equiv b \pmod{n}$ et $c \equiv d \pmod{n}$ alors $ac \equiv bd \pmod{n}$.

Partie B Inverse de 23 modulo 26

On considère l'équation (E) : $23x - 26y = 1$, 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 $23a \equiv 1 \pmod{26}$.

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 (x_1, x_2) où x_1 correspond à la première lettre du mot et x_2 correspond à la deuxième lettre du mot.

Étape 2 (x_1, x_2) est transformé en (y_1, y_2) tel que :

$$(S_1) \begin{cases} y_1 \equiv 11x_1 + 3x_2 \pmod{26} \\ y_2 \equiv 7x_1 + 4x_2 \pmod{26} \end{cases} \text{ avec } 0 \leq y_1 \leq 25 \text{ et } 0 \leq y_2 \leq 25.$$

Étape 3 (y_1, y_2) est transformé en un mot de deux lettres en utilisant le tableau de correspondance donné dans l'étape 1.

Exemple : $\underbrace{\mathbf{TE}}_{\text{mot en clair}} \xrightarrow{\text{étape 1}} (19, 4) \xrightarrow{\text{étape 2}} (13, 19) \xrightarrow{\text{étape 3}} \underbrace{\mathbf{NT}}_{\text{mot codé}}$

1) Coder le mot **ST**.

2) On veut maintenant déterminer la procédure de décodage :

- a) Montrer que tout couple (x_1, x_2) vérifiant les équations du système (S_1) , vérifie les équations du système :

$$(S_2) \begin{cases} 23x_1 \equiv 4y_1 + 23y_2 \pmod{26} \\ 23x_2 \equiv 19y_1 + 11y_2 \pmod{26} \end{cases}$$

- b) À l'aide de la **partie B**, montrer que le couple (x_1, x_2) vérifiant les équations du système (S_2) , vérifie les équations du système :

$$(S_3) \begin{cases} x_1 \equiv 16y_1 + y_2 \pmod{26} \\ x_2 \equiv 11y_1 + 5y_2 \pmod{26} \end{cases}$$

- c) Montrer que tout couple (x_1, x_2) vérifiant les équations du système (S_3) , vérifie les équations du système (S_1) .
- d) Décoder le mot **YJ**.