Partie A Restitution organisée de connaissance

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

Montrer que si $a \equiv b \pmod n$ et $c \equiv d \pmod n$ alors $a\,c \equiv b\,d \pmod n$.

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 $23\,a \equiv 1 \pmod{26}$.

Partie C Chiffrement de Hill

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

Étape1 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) $\begin{cases} y_1 \equiv 11\,x_1 + 3\,x_2 \pmod{26} \\ y_2 \equiv 7\,x_1 + 4\,x_2 \pmod{26} \end{cases}$ avec $0 \leq y_1 \leq 25$ 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 : $\underbrace{\text{TE}}_{\text{mot en clair}} \xrightarrow{\text{étape 1}} (19\,,4) \xrightarrow{\text{étape 2}} (13\,,19) \xrightarrow{\text{étape 3}} \underbrace{\text{NT}}_{\text{mot codé}}$

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

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

b. À l'aide de la partie B, montrer que tout couple $(x_1\,,x_2)$ vérifiant les équations du système (S_2), vérifie les équations du système

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

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.

CORRECTION

Partie A Restitution organisée de connaissance

si $a \equiv b \pmod n$, n divise $a - b$ donc il existe un entier relatif q tel que

$a - b = n\,q$ donc $a = b + n\,q$

si $c \equiv d \pmod n$, n divise $c - d$ donc il existe un entier relatif q' tel que $c - d = n\,q'$ donc $c = d + n\,q'$

$a\,c = (b + n\,p)\,(d + n\,q') = b\,d + n\,(b\,q' + d\,p + n\,p\,p')$ donc $a\,c - b\,d = n\,(b\,q' + d\,p + n\,p\,p')$

$(b\,q' + d\,p + n\,p\,p')$ est un entier relatif donc n divise $a\,c - b\,d$ donc $a\,c \equiv b\,d \pmod n$.

Partie B Inverse de 23 modulo 26

1. $23 \times (-9) = 207$ et $26 \times (-8) = 208$ donc $23 \times (-9) - 26 \times (-8) = 1$

Le couple $(-9\,;-8)$ est solution de l'équation (E).

2. $\begin{cases} 23\,x - 26\,y = 1 \\ 23 \times (-9) - 26 \times (-8) = 1 \end{cases}$ donc par différence membre à membre : $23\,(x + 9) - 26\,(y + 8) = 0$

$23\,(x + 9) = 26\,(y + 8)$, donc 23 divise $26\,(y + 8)$ or 23 et 26 sont premiers entre eux donc 23 divise $y + 8$

Il existe un entier relatif k tel que $y + 8 = 23\,k$ donc $y = 23\,k - 8$

En remplaçant dans $23\,(x + 9) = 26\,(y + 8)$, alors $x + 9 = 26\,k$ donc $x = 26\,k - 9$

Vérification si $x = 26\,k - 9$ et $y = 23\,k - 8$ alors $23\,x - 26\,y = 23\,(26\,k - 9) - 26\,(23\,k - 8) = 23 \times (-9) - 26 \times (-8) = 1$

Les solutions l'équation (E) sont les couples $(26\,k - 9\,;\,23\,k - 8)$ avec $k \in \mathbb{Z}$.

3. si $23\,a \equiv 1 \pmod{26}$ il existe un entier relatif b tel que $23\,a - 26\,b = 1$ donc $a = 26\,k - 9$

$0 \leq a \leq 25$ donc $k = 1$ et $a = 26 - 9 = 17$

Partie C **Chiffrement de Hill**

1. $\underbrace{\text{S T}}_{\text{mot en clair}} \xrightarrow{\text{étape 1}} (18, 19)$.

$\begin{cases} y_1 \equiv 11\times 18 + 3\times 19 \pmod{26} \\ y_2 \equiv 7\times 18 + 4\times 19 \pmod{26} \end{cases} \Leftrightarrow \begin{cases} y_1 \equiv 255 \pmod{26} \\ y_2 \equiv 202 \pmod{26} \end{cases}$ or 255 = 26 × 9 + 21 et 202 = 26 × 7 + 20 donc $y_1 = 21$ et $y_2 = 20$

$\underbrace{\text{S T}}_{\text{mot en clair}} \xrightarrow{\text{étape 1}} (18, 19) \xrightarrow{\text{étape 2}} (21, 20) \xrightarrow{\text{étape 3}} \underbrace{\text{V U}}_{\text{mot codé}}$

Le mot ST est codé par VU

2. *a.* (S_1) $\begin{cases} y_1 \equiv 11 x_1 + 3 x_2 \pmod{26} \\ y_2 \equiv 7 x_1 + 4 x_2 \pmod{26} \end{cases}$ donc $\begin{cases} 4 y_1 \equiv 44 x_1 + 12 x_2 \pmod{26} \\ 23 y_2 \equiv 141 x_1 + 112 x_2 \pmod{26} \end{cases}$ et $\begin{cases} 19 y_1 \equiv 209 x_1 + 57 x_2 \pmod{26} \\ 11 y_2 \equiv 77 x_1 + 44 x_2 \pmod{26} \end{cases}$.

or 209 = 26 ×+ 18 ; 57 = 26 × 2 + 5 ; 77 = 26 × 2 + 25 et 44 = 26 + 18 donc :

$\begin{cases} 4 y_1 \equiv 18 x_1 + 12 x_2 \pmod{26} \\ 23 y_2 \equiv 5 x_1 + 14 x_2 \pmod{26} \end{cases}$ et $\begin{cases} 19 y_1 \equiv x_1 + 5 x_2 \pmod{26} \\ 11 y_2 \equiv 25 x_1 + 18 x_2 \pmod{26} \end{cases}$.

En additionnant terme à terme $\begin{cases} 4 y_1 \equiv 18 x_1 + 12 x_2 \pmod{26} \\ 23 y_2 \equiv 5 x_1 + 14 x_2 \pmod{26} \end{cases}$ donc $4 y_1 + 23 y_2 = 23 x_1 + 26 x_2 \pmod{26}$

En additionnant terme à terme $\begin{cases} 19 y_1 \equiv x_1 + 5 x_2 \pmod{26} \\ 11 y_2 \equiv 25 x_1 + 18 x_2 \pmod{26} \end{cases}$ donc $19 y_1 + 11 y_2 = 26 x_1 + 23 x_2 \pmod{26}$

donc tout couple (x_1 , x_2) vérifiant les équations du système (S1), vérifie les équations du système $\begin{cases} 23 x_1 \equiv 4 y_1 + 23 y_2 \pmod{26} \\ 23 x_2 \equiv 19 y_1 + 11 y_2 \pmod{26} \end{cases}$

b. $\begin{cases} 23 x_1 \equiv 4 y_1 + 23 y_2 \pmod{26} \\ 23 x_2 \equiv 19 y_1 + 11 y_2 \pmod{26} \end{cases}$ or $23 \times 17 \equiv 1 \pmod{26}$, donc en multipliant par 17 : $\begin{cases} 23 x_1 \equiv 4 y_1 + 23 y_2 \pmod{26} \\ 23 x_2 \equiv 19 y_1 + 11 y_2 \pmod{26} \end{cases}$

donc $\begin{cases} 23\times 17\, x_1 \equiv 4\times 17\, y_1 + 23\times 17\, y_2 \pmod{26} \\ 23\times 17\, x_2 \equiv 19\times 17\, y_1 + 11\times 17 y_2 \pmod{26} \end{cases}$

n	4×17	23×17	19×17	11×17
reste de la division de n par 26	16	1	11	5
quotient de la division de n par 26	2	15	12	7

donc tout couple (x_1 , x_2) vérifiant les équations du système (S_2), vérifie les équations du système (S_3) $\begin{cases} x_1 \equiv 16 y_1 + y_2 \pmod{26} \\ x_2 \equiv 11 y_1 + 5 y_2 \pmod{26} \end{cases}$

c. $\begin{cases} 11 x_1 \equiv 16\times 11 y_1 + 11 y_2 \pmod{26} \\ 3 x_2 \equiv 11\times 3 y_1 + 5\times 3 y_2 \pmod{26} \end{cases}$

et $\begin{cases} 7 x_1 \equiv 16\times 7 y_1 + \times 7 y_2 \pmod{26} \\ 4 x_2 \equiv 11\times 4 y_1 + 5\times 4 y_2 \pmod{26} \end{cases}$.

n	16×11 = 176	11×3 = 33	16×7 = 112	11×4 = 44	5×4 = 20
reste de la division de n par 26	20	7	8	18	9
quotient de la division de n par 26	6	1	4	1	1

$\begin{cases} 11 x_1 \equiv 20 y_1 + 11 y_2 \pmod{26} \\ 3 x_2 \equiv 7 y_1 + 15 y_2 \pmod{26} \end{cases}$ et $\begin{cases} 7 x_1 \equiv 8 y_1 + \times 7 y_2 \pmod{26} \\ 4 x_2 \equiv 18 y_1 + 20 y_2 \pmod{26} \end{cases}$.

Par addition terme à terme :

$\begin{cases} 11 x_1 \equiv 20 y_1 + 11 y_2 \pmod{26} \\ 3 x_2 \equiv 7 y_1 + 15 y_2 \pmod{26} \end{cases}$ donc $11 x_1 + 3 x_2 \equiv 27 y_1 + 26 y_2 \pmod{26}$ soit $11 x_1 + 3 x_2 \equiv y_1 \pmod{26}$

$\begin{cases} 7x_1 \equiv 8y_1 + \times 7y_2 \pmod{26} \\ 4x_2 \equiv 18y_1 + 20y_2 \pmod{26} \end{cases}$ donc $7x_1 + 4x_2 \equiv 26y_1 + 27y_2 \pmod{26}$ soit $7x_1 + 4x_2 \equiv y_2 \pmod{26}$

Tout couple (x_1 , x_2) vérifiant les équations du système (S_3) $\begin{cases} x_1 \equiv 16y_1 + y_2 \pmod{26} \\ x_2 \equiv 11y_1 + 5y_2 \pmod{26} \end{cases}$, vérifie les équations du système (S_1).

d. $\underbrace{\text{Y J}}_{\text{mot en clair}} \xrightarrow{\text{étape 1}} (24, 9)$

$(y_1 ; y_2)$ donc $\begin{cases} x_1 \equiv 16 \times 24 + 9 \pmod{26} \\ x_2 \equiv 11 \times 24 + 5 \times 9 \pmod{26} \end{cases}$ or $16 \times 4 + 9 = 26 \times 15 + 3$ et $11 \times 24 + 5 \times 9 = 11 \times 26 + 23$ donc $\begin{cases} x_1 \equiv 3 \pmod{26} \\ x_2 \equiv 23 \pmod{26} \end{cases}$

$\underbrace{\text{Y J}}_{\text{mot codé}} \xrightarrow{\text{étape 1}} (24, 9) \xrightarrow{\text{étape 2}} (3, 23) \xrightarrow{\text{étape 3}} \underbrace{\text{D X}}_{\text{mot en clair}}$

Le mot en clair est DX