

8 Pondichéry avril 2012

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 $ac \equiv bd \pmod{n}$.

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 :

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

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

1. Coder le mot ST.
2. On veut maintenant déterminer la procédure de décodage :
 1. Montrer que tout couple $(x_1; x_2)$ vérifiant les équations du système (S_1) , vérifie les équations du système :

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

2. 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

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

3. Montrer que tout couple $(x_1; x_2)$ vérifiant les équations du système (S_3) , vérifie les équations du système (S_1)
4. Décoder le mot YJ.

1. $23 \times (-9) - 26 \times (-8) = -207 + 208 = 1$: le couple $(-9 ; -8)$ est solution de l'équation (E).

2.
$$\begin{cases} 23x - 26y & = & 1 \\ 23 \times (-9) - 26 \times (-8) & = & 1 \end{cases} \implies \text{(par différence membre à membre)}$$
$$23(x + 9) - 26(y + 8) = 0 \iff 23(x + 9) = 26(y + 8) \quad (1)$$

Donc 23 divise $26(y+8)$ et comme il est premier avec 26; il divise $y+8$ (théorème de Gauss) : il existe donc un entier k tel que $y+8 = 23k \iff y = -8 + 23k$.

En remplaçant dans (1) $y+8$ par $23k$, on obtient :

$$23(x+9) = 26 \times 23k \iff x+9 = 26 \iff x = -9 + 26k.$$

Réciproquement les couples $(-9 + 26k; -8 + 23k)$ vérifient (E) car

$$23(-9 + 26k) - 26(-8 + 23k) = -207 + 23 \times 26k + 208 - 26 \times 23k = 1.$$

Les couples solutions de (E) sont donc de la forme : $(-9 + 26k; -8 + 23k)$, $k \in \mathbb{Z}$.

3. Il faut trouver un (ou des) couple(s) de premier terme a tel que $0 \leq a \leq 25$, donc vérifiant :

$$0 \leq -9 + 26k \leq 25 \iff 9 \leq 26k \leq 34. \text{ La solution } k = 1 \text{ est évidente ce qui donne } a = -9 + 26 = 17.$$

Donc comme $26b \equiv 0 \pmod{26}$, on a $23 \times 17 \equiv 1 \pmod{26}$.

Chiffrement de Hill

1. $\underbrace{\text{ST}}_{\text{mot en clair}} \xrightarrow{\text{étape 1}} (18, 19) \xrightarrow{\text{étape 2}} (21, 20) \xrightarrow{\text{étape 3}} \underbrace{\text{VU}}_{\text{mot codé}}$

2. a. $(S_1) \begin{cases} y_1 \equiv 11x_1 + 3x_2 \pmod{26} \\ y_2 \equiv 7x_1 + 4x_2 \pmod{26} \end{cases} \implies \begin{cases} -44x_1 - 12x_2 = -4y_1 \pmod{26} \\ 21x_1 + 12x_2 = 3y_2 \pmod{26} \end{cases} \Rightarrow (\text{par somme})$
 $-23x_1 = -4y_1 + 3y_2 \pmod{26}.$

De même :

$$(S_1) \begin{cases} y_1 \equiv 11x_1 + 3x_2 \pmod{26} \\ y_2 \equiv 7x_1 + 4x_2 \pmod{26} \end{cases} \implies \begin{cases} -77x_1 - 21x_2 = -7y_1 \pmod{26} \\ 77x_1 + 44x_2 = 11y_2 \pmod{26} \end{cases}$$

$\implies (\text{par somme}) 23x_2 = -7y_1 + 11y_2 \pmod{26}$ ou encore puisque $-7 \equiv 19 \pmod{26}$: $23x_2 = 19y_1 + 11y_2 \pmod{26}$.

Donc, 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. On a vu à la partie B que $23 \times 17 \equiv 1 \pmod{26}$ (23 a pour inverse 17 modulo 26), donc en multipliant chaque membre du système (S_2) par 17, on obtient

$$(S_2) \iff \begin{cases} 23x_1 \times 17 \equiv 4y_1 \times 17 + 23y_2 \times 17 \pmod{26} \\ 23x_2 \times 17 \equiv 19y_1 \times 17 + 11y_2 \times 17 \pmod{26} \end{cases} \implies \begin{cases} x_1 \equiv 68y_1 + 391y_2 \pmod{26} \\ x_2 \equiv 323y_1 + 187y_2 \pmod{26} \end{cases}$$

Or $68 \equiv 16 \pmod{26}$, $391 \equiv 1 \pmod{26}$, $323 \equiv 11 \pmod{26}$,

$187 \equiv 5 \pmod{26}$, donc finalement tout couple $(x_1; x_2)$ vérifiant les équations du système (S_2) , vérifie les équations du système

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

c. On calcule $11x_1 + 3x_2 = 11(16y_1 + y_2) + 3(11y_1 + 5y_2) = 176y_1 + 11y_2 + 33y_1 + 15y_2 = 209y_1 + 26y_2$.

Or $209 \equiv 1 \pmod{26}$ et $26 \equiv 0 \pmod{26}$, donc $11x_1 + 3x_2 \equiv 1y_1 + 0y_2 \pmod{26}$.

De même $7x_1 + 4x_2 = 7(16y_1 + y_2) + 4(11y_1 + 5y_2) = 112y_1 + 7y_2 + 44y_1 + 20y_2 = 156y_1 + 27y_2$.

Or $146 \equiv 0 \pmod{26}$ et $27 \equiv 1 \pmod{26}$, donc $7x_1 + 4x_2 \equiv 0y_1 + 1y_2 \pmod{26}$.

Conclusion : tout couple $(x_1 ; x_2)$ vérifiant les équations du système (S_3) , vérifie les équations du système (S_1) .

Finalement les systèmes (S_1) et (S_3) sont équivalents.

d. Pour YJ le couple $(y_1 ; y_2) = (24 ; 9)$. En appliquant les équations de (S_3) on obtient :

$$\begin{cases} x_1 & \equiv 16 \times 24 + 9 & (\text{mod } 26) \\ x_2 & \equiv 11 \times 24 + 5 \times 9 & (\text{mod } 26) \end{cases} \iff \begin{cases} x_1 & \equiv 393 & (\text{mod } 26) \\ x_2 & \equiv 309 & (\text{mod } 26) \end{cases}$$

Or $393 = 26 \times 15 + 3$, donc $393 \equiv 3 \pmod{26}$;

$309 = 26 \times 11 + 23$, donc $309 \equiv 23 \pmod{26}$.

On a donc $(x_1 ; x_2) = (3 ; 23)$ et en utilisant le tableau le mot décodé est donc **DX**.