Partie A Restitution organisée des connaissances

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 :

$$(E) : \quad 23x - 26y = 1$$

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 :

Etape 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.

Etape 2 $(x_1 ; x_2)$ est transformé en $(y_1 ; y_2)$ tel que :

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

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

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 :

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

b. A 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

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

c. 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**.

Analyse

Une jolie application de la congruence (chiffrement de Hill). Si la partie A est une question de cours classique (compatibilité de la relation de congruence avec la multiplication), la Partie B, via une équation diophantienne (également classique) permet d'inverser un entier modulo 26. Le codage/décodage conduit à des manipulations de systèmes modulo 26 (mise en équivalence des systèmes (S_1) et (S_3)) où on utilise quelques propriétés fondamentales de la congruence et le résultat de la partie B..

Résolution

Partie A Restitution organisée des connaissances

On a :

$$a \equiv b \pmod{n} \Leftrightarrow \exists k \in \mathbb{Z} / a = b + k n$$
$$c \equiv d \pmod{n} \Leftrightarrow \exists k' \in \mathbb{Z} / c = d + k' n$$

En multipliant membre à membre les deux égalités obtenues, il vient :

$$ac = (b + k n)(d + k' n) = bd + b k' n + d k n + k k' n^2 = bd + (b k' + d k + k k' n) n$$

Comme $b k' + d k + k k' n$ est un entier, il en découle immédiatement : $ac \equiv bd \pmod{n}$.

Partie B Inverse de 23 modulo 26

Question 1.

On a immédiatement : $23 \times (-9) - 26 \times (-8) = -207 + 208 = 1$.

Le couple $(-9\,;-8)$ est une solution de l'équation (E) : $23x - 26y = 1$.

Question 2.

D'après le résultat de la question précédente, l'équation (E) se récrit :

$$(E) : \quad 23x - 26y = 23 \times (-9) - 26 \times (-8)$$

Soit : $23(x+9) = 26(y+8)$. Comme 23 et 26 sont premiers entre eux (23 est premier et $26 = 2 \times 13$), le théorème de Gauss nous permet d'affirmer que 23 divise $y+8$, soit : $y + 8 = 23k$ ($k \in \mathbb{Z}$). On a alors : $23(x+9) = 26 \times 23k$ puis $x + 9 = 26k$.

Ainsi, si $(x\,;y)$ est un couple solution de l'équation (E), alors il est de la forme :

$$(x\,;y)=(-9+26k\,;-8+23k) \text{ où } k \text{ est un entier}$$

Réciproquement, on vérifie aisément que tout couple de cette forme est solution de l'équation (E).

Les solutions entières de l'équation (E) : $23x-26y=1$
sont les couples de la forme $(x\,;y)=(-9+26k\,;-8+23k)$ où k est un entier.

Question 3.

On a : $23a\equiv 1 \pmod{26} \Leftrightarrow \exists n\in\mathbb{Z} / 23a=1+26n \Leftrightarrow \exists k\in\mathbb{Z} / 23a-26n=1$.

Ainsi, le couple $(a\,;n)$ est de la forme $(-9+26k\,;-8+23k)$ où k est un entier.

On veut que a soit compris, au sens large, entre 0 et 25.
On cherche donc un entier k tel que : $0\leq -9+26k\leq 25$, soit $9\leq 26k\leq 34$.
Il vient immédiatement $k=1$ puis $a=-9+26\times 1=17$.

17 est l'unique entier a compris entre 0 et 25 tel que $23a\equiv 1 \pmod{26}$.

Partie C Chiffrement de Hill

Question 1.

Codage du mot ST.
Etape 1 : le couple d'entiers associés au mot ST est $(x_1\,;x_2)=(18,19)$.

Etape 2 : détermination du couple $(y_1\,;y_2)$.

On a : $11x_1+3x_2=11\times 18+3\times 19=255=9\times 26+21$. D'où : $11x_1+3x_2\equiv 21 \pmod{26}$.

Par ailleurs : $7x_1+4x_2=7\times 18+4\times 19=202=7\times 26+20$. D'où : $7x_1+4x_2\equiv 20 \pmod{26}$.

En définitive : $(y_1\,;y_2)=(21,20)$.

Etape 3 : par lecture directe dans le tableau, on obtient : **VU**.

En utilisant le chiffrement de Hill, le mot codé correspondant à ST est le mot VU.

Question 2.a.

Soit $(x_1\,;x_2)$ un couple d'entiers vérifiant le système (S_1). On a donc :

$$\begin{cases} 11x_1+3x_2\equiv y_1 \pmod{26} \\ 7x_1+4x_2\equiv y_2 \pmod{26} \end{cases}$$

Pour éliminer « x_2 », on multiplie la première ligne par 4 et on lui retranche 3 fois la seconde.
On obtient : $4(11x_1+3x_2)-3(7x_1+4x_2)\equiv 4y_1-3y_2 \pmod{26}$.
Soit : $23x_1\equiv 4y_1-3y_2 \pmod{26}$. D'où : $23x_1\equiv 4y_1-3y_2+26y_2 \pmod{26}$.
Finalement : $\underline{23x_1\equiv 4y_1+23y_2 \pmod{26}}$

Pour éliminer « x_1 », on multiplie la première ligne par 7 et on lui retranche 11 fois la seconde. On obtient : $7(11x_1+3x_2)-11(7x_1+4x_2)\equiv 7y_1-11y_2 \pmod{26}$.
Soit : $-23x_2\equiv 7y_1-11y_2 \pmod{26}$. D'où : $23x_2\equiv -7y_1+11y_2 \pmod{26}$.
Alors : $23x_2\equiv -7y_1+26y_1+11y_2 \pmod{26}$.
Finalement : $\underline{23x_2\equiv 19y_1+11y_2 \pmod{26}}$

Le couple $(x_1\,;x_2)$ vérifie bien le système :

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

Si le couple $(x_1\,;x_2)$ vérifie les équations du système (S_1)
alors il vérifie celles du système (S_2).

Question 2.b.

Soit $(x_1\,;x_2)$ un couple d'entiers vérifiant les équations du système (S_2). On a donc :

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

A la troisième question de la partie B, on a établi : $23\times 17\equiv 1 \pmod{26}$.
On a donc : $23\times 17\times x_1\equiv x_1 \pmod{26}$.
En multipliant alors chaque ligne du système (S_2) par 17, on obtient :

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

Soit :

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

Comme $17\times 4y_1 = 64y_1 = 2\times 26y_1 + 16y_1$, $17\times 19y_1 = 323y_1 = 12\times 26y_1 + 11y_1$ et $17\times 11y_2 = 187y_2 = 7\times 26y_2 + 5y_2$, on en tire le système :

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

On retrouve bien le système (S_3) de l'énoncé.

Si le couple $(x_1 ; x_2)$ vérifie les équations du système (S_2)
alors il vérifie celles du système (S_3).

Question 2.c.

Soit $(x_1 ; x_2)$ un couple d'entiers vérifiant les équations du système (S_3). On a donc :

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

On a alors :

$$\begin{aligned} 11x_1 + 3x_2 &\equiv 11\times(16y_1 + y_2) + 3\times(11y_1 + 5y_2) \pmod{26} \\ &\equiv (11\times 16 + 3\times 11)y_1 + (11 + 3\times 5)y_2 \pmod{26} \\ &\equiv 209y_1 + 26y_2 \pmod{26} \\ &\equiv 8\times 26y_1 + y_1 \pmod{26} \\ &\equiv y_1 \pmod{26} \end{aligned}$$

Et :

$$\begin{aligned} 7x_1 + 4x_2 &\equiv 7\times(16y_1 + y_2) + 4\times(11y_1 + 5y_2) \pmod{26} \\ &\equiv (7\times 16 + 4\times 11)y_1 + (7 + 4\times 5)y_2 \pmod{26} \\ &\equiv 156y_1 + 27y_2 \pmod{26} \\ &\equiv 6\times 26y_1 + 26y_2 + y_2 \pmod{26} \\ &\equiv y_2 \pmod{26} \end{aligned}$$

On en déduit ainsi que le couple $(x_1 ; x_2)$ vérifie les équations du système :

$$\begin{cases} 11x_1 + 3x_2 \equiv y_1 \pmod{26} \\ 7x_1 + 4x_2 \equiv y_2 \pmod{26} \end{cases}$$

qui n'est autre que le système (S_1).

Si le couple $(x_1 ; x_2)$ vérifie les équations du système (S_3)
alors il vérifie celles du système (S_1).

Question 2.d.

D'après les question 2.a. et 2.b., si un couple $(x_1 ; x_2)$ vérifie les équations du système (S_1) alors il vérifie celles du système (S_3). A la question 2.c. on a vu, réciproquement, que si un couple $(x_1 ; x_2)$ vérifie les équations du système (S_3) alors il vérifie celles du système (S_1). En d'autres termes, il y a équivalence entre les systèmes (S_1) et (S_3).

Le système (S_1) permet, connaissant le couple $(x_1 ; x_2)$ d'obtenir le couple $(y_1 ; y_2)$. C'est le codage.
Réciproquement, le système (S_3) permet, connaissant le couple $(y_1 ; y_2)$ d'obtenir le couple $(x_1 ; x_2)$. C'est le décodage.

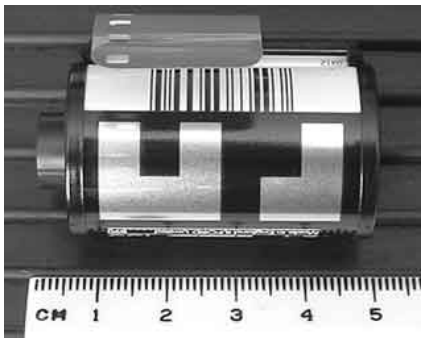
Au mot YJ correspond le couple $(y_1 ; y_2) = (24, 9)$.
En utilisant le système (S_3), on a alors :

- $16y_1 + y_2 = 16 \times 24 + 9 = 393 = 15 \times 26 + 3 \equiv 3 \pmod{26}$. D'où : $x_1 = 3$.
- $11y_1 + 5y_2 = 11 \times 24 + 5 \times 9 = 309 = 11 \times 26 + 23 \equiv 23 \pmod{26}$. D'où : $x_2 = 23$.

On a donc $(x_1 ; x_2) = (3, 23)$ et en tire immédiatement le mot décodé : DX.

Le mot en clair correspondant au mot codé YJ est le mot DX.

Remarque : le codage DX est le nom donné à un élégant codage des films photographiques 35mm argentiques au format 24×36. L'auteur(e) de ce sujet a peut-être utilisé ce type de film il y a de ça des années avant l'avènement des appareils numériques. Mais peut-être s'agit-il seulement d'un « simple » hasard …



Source du fichier correspondant à l'image : http://en.wikipedia.org/wiki/File:Dx135can.jpg.