Exercice 5 points

Candidats ayant suivi l'enseignement de spécialité.

Partie A 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 (E).

2) Résoudre alors l'équation (E).

3) En déduire un entier a tel que $0 \leqslant a \leqslant 25$ et $23a \equiv 1$ (mod. 26).

Partie B chiffrement de Hill

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

Étape 1 : Chaque lettre du mot est remplacé 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 pose $X = (x_1 \quad x_2)$ la matrice ligne où x_1 correspond à la première lettre du mot et x_2 correspond à la deuxième lettre du mot.

Étape 2 : La matrice $X = (x_1 \quad x_2)$ est transformée en la matrice $Y = (y_1 \quad y_2)$ telle que :

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

Étape 3 : La matrice $(y_1 \quad y_2)$ est transformée en un mot de deux lettres en utilisant le tableau de correspondance donné dans l'étape 1.

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

1) Démontrer que le mot ST est codé par VU.

2) a) Déterminer la matrice A telle que $Y \equiv XA$ (mod 26).

b) Justifier que la matrice A est inversible et déterminer la matrice inverse de A, notée A^{-1}.

3) On pose $B = 23\ A^{-1}$.

a) Montrer que $aAB \equiv I_2$ (mod 26) où a est l'entier défini dans la **partie A/** par :

$$0 \leqslant a \leqslant 25 \text{ et } 23a \equiv 1 \text{ (mod. 26)}$$

b) En déduire que $X \equiv aYB$ (mod 26)

c) Décoder le mot YJ.

Correction de l'exercice

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 (E).

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

(montrer le calcul … puisque le résultat est annoncé, il ne suffit pas de dire que c'est vrai ...)

(Ainsi, on prouve que 23 et 26 sont premiers entre eux)

2) Résoudre alors l'équation (E).

$\begin{cases} 23x - 26y = 1 \\ 23\times(-9) - 26\times(-8) = 1 \end{cases}$ par différence des deux lignes, (E) équivaut à $23(x + 9) - 26(y + 8) = 0$

on en déduit : $23(x + 9) = 26(y + 8)$. (E′).

On applique le théorème de Gauss :

Comme 23 et 26 sont premiers entre eux et que 23 divise le produit $26(y + 8)$, 23 divise $y + 8$.

Il existe un entier k tel que $y + 8 = 23k$.

On a alors en remplaçant dans (E′) : $23(x + 9) = 26\times23k$, soit : $x + 9 = 26k$.

On a montré : si $(x ; y)$ est solution de (E) alors $\begin{cases} x = -9 + 26k \\ y = -8 + 23k \end{cases}$, $k \in \mathbb{Z}$.

Réciproquement : Soit un couple $(-9 + 26k ; -8 + 23k)$, on a :

$23(-9 + 26k) - 26(-8 + 23k) = -207 + 23\times26k + 208 - 26\times23k = 1$

Conclusion : L'ensemble des solutions de (E) est l'ensemble des couples $(-9 + 26k ; -8 + 23k)$ où $k \in \mathbb{Z}$.

On peut aussi appliquer deux fois le théorème de Gauss :

Comme 23 et 26 sont premiers entre eux et que 23 divise le produit $26(y + 8)$, 23 divise $y + 8$.

Il existe un entier k tel que $y + 8 = 23k$.

Comme 23 et 26 sont premiers entre eux et que 26 divise le produit $23(x + 9)$, 26 divise $x + 9$.

Il existe un entier k' tel que $x + 9 = 26k'$.

On a alors : $23\times26k' = 26\times23k$, d'où, $k = k'$.

Il reste comme précédemment à vérifier que tous les couples de la forme $(-9 + 26k ; -8 + 23k)$ avec $k \in \mathbb{Z}$ sont solutions de (E).

3) En déduire un entier a tel que $0 \leqslant a \leqslant 25$ et $23a \equiv 1$ (mod. 26).

$23x - 26y = 1$ équivaut à $23x \equiv 1 \pmod{26}$

On veut donc : $0 \leqslant -9 + 26k \leqslant 25$, ce qui est vérifié lorsque $k = 1$.

$a = -9 + 26 = 17$ (En ce cas $b = -8 + 23 = 15$, et, $23\times17 - 26\times15 = \ldots = 1$)

Partie B ***chiffrement de Hill***

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

Étape 1 : Chaque lettre du mot est remplacé 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 pose $X = (x_1 \quad x_2)$ la matrice ligne où x_1 correspond à la première lettre du mot et x_2 correspond à la deuxième lettre du mot.

Étape 2 : La matrice $X = (x_1 \quad x_2)$ est transformée en la matrice $Y = (y_1 \quad y_2)$ telle que :

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

Étape 3 : La matrice $(y_1 \quad y_2)$ est transformée en un mot de deux lettres en utilisant le tableau de correspondance donné dans l'étape 1.

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

1) Le mot ST est codé par VU.

En effet : le couple (18 ; 19) code les lettres ST

$11 \times 18 + 3 \times 19 = 255$ et $255 = 26 \times 9 + 21$

et $7 \times 18 + 4 \times 19 = 202$ et $202 = 26 \times 7 + 20$

(Donner les divisions euclidiennes pour justifier puisque les résultats sont indiqués dans le texte)

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

2) a) Déterminer la matrice A telle que $Y \equiv XA \pmod{26}$.

Posons $A = \begin{pmatrix} 11 & 7 \\ 3 & 4 \end{pmatrix}$

$(x_1 \quad x_2)\begin{pmatrix} 11 & 7 \\ 3 & 4 \end{pmatrix} = (11x_1 + 3x_2 \quad 7x_1 + 4x_2) = (y_1 \quad y_2)$

b) Justifier que la matrice A est inversible et déterminer la matrice inverse de A, notée A^{-1}.

Le déterminant de A est : dét(A) = $11 \times 4 - 3 \times 7 = 23$

Comme le déterminant est différent de 0, la matrice A est inversible.

$A^{-1} = \frac{1}{23}\begin{pmatrix} 4 & -7 \\ -3 & 11 \end{pmatrix}$ (On peut vérifier : $\begin{pmatrix} 11 & 7 \\ 3 & 4 \end{pmatrix}\begin{pmatrix} 4 & -7 \\ -3 & 11 \end{pmatrix} =$

$\begin{pmatrix} 11\times4-7\times3 & -7\times11+7\times11 \\ 3\times4-4\times3 & -3\times7+4\times11 \end{pmatrix} = \begin{pmatrix} 23 & 0 \\ 0 & 23 \end{pmatrix}$, d'où, $A\,A^{-1} = \frac{1}{23}\begin{pmatrix} 23 & 0 \\ 0 & 23 \end{pmatrix} = I_2$.

3) On pose $B = 23\,A^{-1}$. (On a donc $B = \begin{pmatrix} 4 & -7 \\ -3 & 11 \end{pmatrix}$)

a) Montrer que $aAB \equiv I_2 \pmod{26}$ où a est l'entier déterminé dans la **partie A/**

$aAB = aA(23\,A^{-1}) = 23a\,A\,A^{-1}$

Or $23a \equiv 1 \pmod{26}$ et $A\,A^{-1} = I_2$.

Conclusion : $aAB \equiv I_2 \pmod{26}$

b) En déduire que $X \equiv aYB \pmod{26}$

On sait : $Y \equiv XA \pmod{26}$.

En multipliant à droite par B, on a : $YB \equiv XAB \pmod{26}$

puis en multipliant par l'entier a : $aYB \equiv aXAB \pmod{26}$

Or, $aXAB = X(aAB) = XI_2 = X$.

c) Décoder YJ.

$a = 17$ (partie A/3), $B = \begin{pmatrix} 4 & -7 \\ -3 & 11 \end{pmatrix}$ (partie B/3)

La matrice Y codant YJ est : $(24 \quad 9)$

On calcule donc : $17\times(24 \quad 9)\begin{pmatrix} 4 & -7 \\ -3 & 11 \end{pmatrix} = 17(24\times4 - 9\times3 \quad -24\times7 + 9\times11)$

$= (1173 \qquad -1173)$

$1173 = 26\times45 + 3$ et

$-1173 = 26\times(-46) + 23$

la matrice $X = (3 \quad 23)$

Le mot décodé est donc : DX.