Partie A

On considère l'algorithme suivant :

A et X sont des nombres entiers
Saisir un entier positif A
Affecter à X la valeur de A
Tant que X supérieur ou égal à 26
 | Affecter à X la valeur X - 26
Fin du tant que
Afficher X

1. Qu'affiche cet algorithme quand on saisit le nombre 3 ?
2. Qu'affiche cet algorithme quand on saisit le nombre 55 ?
3. Pour un nombre entier saisi quelconque, que représente le résultat fourni par cet algorithme ?

Partie B

On veut coder un bloc de deux lettres selon la procédure suivante (détaillée en quatre étapes) :

• **Étape 1** : chaque lettre du bloc est remplacée par un entier en utilisant le tableau ci-dessous :

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

On obtient une matrice colonne $\begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$ où x_1 correspond à la première lettre du mot et x_2 correspond à la deuxième lettre du mot.

• **Étape 2** : $\begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$ est transformé en $\begin{pmatrix} y_1 \\ y_2 \end{pmatrix}$ tel que $\begin{pmatrix} y_1 \\ y_2 \end{pmatrix} = \begin{pmatrix} 3 & 1 \\ 5 & 2 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$

La matrice $C = \begin{pmatrix} 3 & 1 \\ 5 & 2 \end{pmatrix}$ est appelée la matrice de codage.

• **Étape 3** : $\begin{pmatrix} y_1 \\ y_2 \end{pmatrix}$ est transformé en $\begin{pmatrix} z_1 \\ z_2 \end{pmatrix}$ tel que : $\begin{cases} z_1 \equiv y_1 (26) \text{ avec } 0 \leq z_1 \leq 25 \\ z_2 \equiv y_2 (26) \text{ avec } 0 \leq z_2 \leq 25 \end{cases}$

• **Étape 3** : $\begin{pmatrix} z_1 \\ z_2 \end{pmatrix}$ est transformé en un bloc de deux lettres en utilisant le tableau de correspondance donné dans l'étape 1.

Exemple :

$$RE \rightarrow \begin{pmatrix} 17 \\ 4 \end{pmatrix} \rightarrow \begin{pmatrix} 55 \\ 93 \end{pmatrix} \rightarrow \begin{pmatrix} 3 \\ 15 \end{pmatrix} \rightarrow DP$$

Le bloc RE est donc codé en DP

Justifier le passage de $\begin{pmatrix} 17 \\ 4 \end{pmatrix}$ à $\begin{pmatrix} 55 \\ 93 \end{pmatrix}$ puis à $\begin{pmatrix} 3 \\ 15 \end{pmatrix}$.

1. Soient x_1, x_2, x'_1, x'_2 quatre nombres entiers compris entre 0 et 25 tels que $\begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$ et $\begin{pmatrix} x'_1 \\ x'_2 \end{pmatrix}$ sont transformés lors du procédé

de codage en $\begin{pmatrix} z_1 \\ z_2 \end{pmatrix}$.

a. Montrer que $\begin{cases} 3x_1 + x_2 \equiv 3x'_1 + x'_2 \pmod{26} \\ 5x_1 + 2x_2 \equiv 5x'_1 + 2x'_2 \pmod{26} \end{cases}$.

b. En déduire que $x_1 \equiv x'_1 \pmod{26}$ et $x_2 \equiv x'_2 \pmod{26}$ puis que $x_1 = x'_1$ et $x_2 = x'_2$.

2. On souhaite trouver une méthode de décodage pour le bloc DP :

a. Vérifier que la matrice $C' = \begin{pmatrix} 2 & -1 \\ -5 & 3 \end{pmatrix}$ est la matrice inverse de C.

b. Calculer $\begin{pmatrix} y_1 \\ y_2 \end{pmatrix}$ tels que $\begin{pmatrix} y_1 \\ y_2 \end{pmatrix} = \begin{pmatrix} 2 & -1 \\ -5 & 3 \end{pmatrix} \begin{pmatrix} 3 \\ 15 \end{pmatrix}$.

c. Calculer $\begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$ tels que $\begin{cases} x_1 \equiv y_1 (26) \text{ avec } 0 \leq x_1 \leq 25 \\ x_2 \equiv y_2 (26) \text{ avec } 0 \leq x_2 \leq 25 \end{cases}$.

d. Quel procédé général de décodage peut-on conjecturer ?

3. Dans cette question nous allons généraliser ce procédé de décodage.

On considère un bloc de deux lettres et on appelle z_1 et z_2 les deux entiers compris entre 0 et 25 associés à ces lettres à l'étape 3. On cherche à trouver deux entiers x_1 et x_2 compris entre 0 et 25 qui donnent la matrice colonne $\begin{pmatrix} z_1 \\ z_2 \end{pmatrix}$ par les étapes 2 et 3 du procédé de codage.

Soient y'_1 et y'_2 tels que $\begin{pmatrix} y'_1 \\ y'_2 \end{pmatrix} = C' \begin{pmatrix} z_1 \\ z_2 \end{pmatrix}$ où $C' = \begin{pmatrix} 2 & -1 \\ -5 & 3 \end{pmatrix}$.

Soient x_1 et x_2 , les nombres entiers tels que $\begin{cases} x_1 \equiv y'_1 (26) \text{ avec } 0 \leq x_1 \leq 25 \\ x_2 \equiv y'_2 (26) \text{ avec } 0 \leq x_2 \leq 25 \end{cases}$

Montrer que $\begin{cases} 3x_1 + x_2 \equiv z_1 (26) \\ 5x_1 + 2x_2 \equiv z_2 (26) \end{cases}$.

Conclure.

4. Décoder QC.

CORRECTION

Partie A

1. $A = 3$ donc $X = A = 3$, $X < 26$ donc l'algorithme affiche 3

2. $A = 55$ donc $X = A = 55$, $X \geq 26$ donc X prend la valeur $55 - 26$ soit 29
 $29 > 26$ donc X prend la valeur $29 - 26$ soit 3 donc l'algorithme affiche 3

3. L'algorithme affiche le reste de la division de A par 26

Partie B

• **Étape 2 :** $\begin{pmatrix} 17 \\ 4 \end{pmatrix}$ est transformé en $\begin{pmatrix} y_1 \\ y_2 \end{pmatrix}$ tel que $\begin{pmatrix} y_1 \\ y_2 \end{pmatrix} = \begin{pmatrix} 3 & 1 \\ 5 & 2 \end{pmatrix} \begin{pmatrix} 17 \\ 4 \end{pmatrix}$.

$$\begin{pmatrix} y_1 \\ y_2 \end{pmatrix} = \begin{pmatrix} 3 & 1 \\ 5 & 2 \end{pmatrix} \begin{pmatrix} 17 \\ 4 \end{pmatrix} = \begin{pmatrix} 17 \times 3 + 4 \\ 17 \times 5 + 4 \times 2 \end{pmatrix} \text{ soit } \begin{pmatrix} y_1 \\ y_2 \end{pmatrix} = \begin{pmatrix} 55 \\ 93 \end{pmatrix}$$

• **Étape 3 :** $\begin{pmatrix} 55 \\ 93 \end{pmatrix}$ est transformé en $\begin{pmatrix} z_1 \\ z_2 \end{pmatrix}$ tel que : $\begin{cases} z_1 \equiv 55 (26) \text{ avec } 0 \leq z_1 \leq 25 \\ z_2 \equiv 93 (26) \text{ avec } 0 \leq z_2 \leq 25 \end{cases}$

$$55 = 26 \times 2 + 3 \text{ donc } 55 \equiv 3 (26) \text{ et } 93 = 26 \times 3 + 15 \text{ donc } 93 \equiv 15 (26)$$

$$0 \leq 3 \leq 25 \text{ et } 0 \leq 15 \leq 25 \text{ donc } \begin{pmatrix} 55 \\ 93 \end{pmatrix} \text{ est transformé en } \begin{pmatrix} 3 \\ 15 \end{pmatrix}.$$

1. a. Étape 2

$\begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$ est transformé en $\begin{pmatrix} y_1 \\ y_2 \end{pmatrix}$ tel que $\begin{pmatrix} y_1 \\ y_2 \end{pmatrix} = \begin{pmatrix} 3 & 1 \\ 5 & 2 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$ donc $\begin{cases} y_1 = 3x_1 + x_2 \\ y_2 = 5x_1 + 2x_2 \end{cases}$

de même $\begin{pmatrix} x'_1 \\ x'_2 \end{pmatrix}$ est transformé en $\begin{pmatrix} y'_1 \\ y'_2 \end{pmatrix}$ tel que $\begin{pmatrix} y'_1 \\ y'_2 \end{pmatrix} = \begin{pmatrix} 3 & 1 \\ 5 & 2 \end{pmatrix} \begin{pmatrix} x'_1 \\ x'_2 \end{pmatrix}$ donc $\begin{cases} y'_1 = 3x'_1 + x'_2 \\ y'_2 = 5x'_1 + 2x'_2 \end{cases}$

Étape 3

$\begin{pmatrix} y_1 \\ y_2 \end{pmatrix}$ est transformé en $\begin{pmatrix} z_1 \\ z_2 \end{pmatrix}$ tel que : $\begin{cases} z_1 \equiv y_1 (26) \text{ avec } 0 \leq z_1 \leq 25 \\ z_2 \equiv y_2 (26) \text{ avec } 0 \leq z_2 \leq 25 \end{cases}$

$\begin{pmatrix} y'_1 \\ y'_2 \end{pmatrix}$ est transformé en $\begin{pmatrix} z_1 \\ z_2 \end{pmatrix}$ tel que : $\begin{cases} z_1 \equiv y'_1 (26) \text{ avec } 0 \leq z_1 \leq 25 \\ z_2 \equiv y'_2 (26) \text{ avec } 0 \leq z_2 \leq 25 \end{cases}$

$$\text{donc } \begin{cases} y_1 \equiv y_1 (26) \\ y_2 \equiv y_2 (26) \end{cases} \text{ soit } \begin{cases} 3x_1 + x_2 \equiv 3x'_1 + x'_2 (26) \\ 5x_1 + 2x_2 \equiv 5x'_1 + 2x'_2 (26) \end{cases}$$

$$b. \begin{cases} 3x_1 + x_2 \equiv 3x'_1 + x'_2 (26) \\ 5x_1 + 2x_2 \equiv 5x'_1 + 2x'_2 (26) \end{cases} \text{ donc } \begin{cases} 5(3x_1 + x_2) \equiv 5(3x'_1 + x'_2) (26) \\ 3(5x_1 + 2x_2) \equiv 3(5x'_1 + 2x'_2) (26) \end{cases}$$

$$\text{soit } \begin{cases} -5(3x_1 + x_2) + 3(5x_1 + 2x_2) \equiv -5(3x'_1 + x'_2) + 3(5x'_1 + 2x'_2) (26) \\ 5x_1 + 2x_2 \equiv 5x'_1 + 2x'_2 (26) \end{cases} \text{ soit } \begin{cases} x_2 \equiv x'_2 (26) \\ 5x_1 + 2x_2 \equiv 5x'_1 + 2x'_2 (26) \end{cases}$$

$$\text{donc } \begin{cases} x_2 \equiv x'_2 & (26) \\ 5x_1 \equiv 5x'_1 & (26) \end{cases}$$

26 divise $x_2 - x'_2$ or $0 \leq x_2 \leq 25$ et $0 \leq x'_2 \leq 25$ donc $-25 \leq x_2 - x'_2 \leq 25$

Le seul multiple de 26 compris entre -25 et 25 est 0 donc $x_2 - x'_2 = 0$ donc $x_2 = x'_2$.

$5x_1 \equiv 5x'_1$ (26) donc $5 \times 5x_1 \equiv 5 \times 5x'_1$ (26) or $25 \equiv -1$ (26) donc $x_1 \equiv x'_1$ (26)

26 divise $x_1 - x'_1$ or $0 \leq x_1 \leq 25$ et $0 \leq x'_1 \leq 25$ donc $-25 \leq x_1 - x'_1 \leq 25$

Le seul multiple de 26 compris entre -25 et 25 est 0 donc $x_1 - x'_1 = 0$ donc $x_1 = x'_1$.

$$2. a. \quad C C' = \begin{pmatrix} 3 & 1 \\ 5 & 2 \end{pmatrix} \begin{pmatrix} 2 & -1 \\ -5 & 3 \end{pmatrix} = \begin{pmatrix} 3 \times 2 - 5 & -3 + 3 \\ 5 \times 2 - 2 \times 5 & -5 + 6 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

La matrice $C' \begin{pmatrix} 2 & -1 \\ -5 & 3 \end{pmatrix}$ est la matrice inverse de C .

$$b. \quad \begin{pmatrix} y_1 \\ y_2 \end{pmatrix} = \begin{pmatrix} 2 & -1 \\ -5 & 3 \end{pmatrix} \begin{pmatrix} 3 \\ 15 \end{pmatrix} = \begin{pmatrix} 2 \times 3 - 15 \\ -5 \times 3 + 3 \times 15 \end{pmatrix} \text{ donc } \begin{pmatrix} y_1 \\ y_2 \end{pmatrix} = \begin{pmatrix} -9 \\ 30 \end{pmatrix}$$

$$c. \quad \begin{cases} x_1 \equiv -9 & (26) \text{ avec } 0 \leq x_1 \leq 25 \\ x_2 \equiv 30 & (26) \text{ avec } 0 \leq x_2 \leq 25 \end{cases}$$

$-9 = 26 - 9$ soit $-9 \equiv 17$ (26) avec $0 \leq 17 \leq 25$

$$30 = 26 + 4 \text{ soit } 30 \equiv 4 \text{ (26) avec } 0 \leq 4 \leq 25 \text{ donc } \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} 17 \\ 4 \end{pmatrix}$$

d. On peut donc conjecturer le processus de décodage suivant :

• **Étape 1** : chaque lettre du bloc est remplacée par un entier en utilisant le tableau ci-dessous :

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

On obtient une matrice colonne $\begin{pmatrix} z_1 \\ z_2 \end{pmatrix}$ où z_1 correspond à la première lettre du mot et z_2 correspond à la deuxième lettre du mot.

$$\bullet \text{ Étape 2 : } \begin{pmatrix} z_1 \\ z_2 \end{pmatrix} \text{ est transformé en } \begin{pmatrix} y_1 \\ y_2 \end{pmatrix} \text{ tel que } \begin{pmatrix} y_1 \\ y_2 \end{pmatrix} = \begin{pmatrix} 2 & -1 \\ -5 & 3 \end{pmatrix} \begin{pmatrix} z_1 \\ z_2 \end{pmatrix}$$

$$\bullet \text{ Étape 3 : } \begin{pmatrix} y_1 \\ y_2 \end{pmatrix} \text{ est transformé en } \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \text{ tel que : } \begin{cases} x_1 \equiv y_1 (26) \text{ avec } 0 \leq x_1 \leq 25 \\ x_2 \equiv y_2 (26) \text{ avec } 0 \leq x_2 \leq 25 \end{cases}$$

$$\bullet \text{ Étape 4 : } \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \text{ est transformé en un bloc de deux lettres en utilisant le tableau de correspondance donné dans l'étape 1.}$$

$$3. \quad \text{Soient } y'_1 \text{ et } y'_2 \text{ tels que } \begin{pmatrix} y'_1 \\ y'_2 \end{pmatrix} = C' \begin{pmatrix} z_1 \\ z_2 \end{pmatrix} \text{ où } C' = \begin{pmatrix} 2 & -1 \\ -5 & 3 \end{pmatrix} \text{ donc } \begin{cases} y'_1 \equiv 2z_1 - z_2 \\ y'_2 \equiv -5z_1 + 3z_2 \end{cases}$$

$$\begin{pmatrix} y'_1 \\ y'_2 \end{pmatrix} = C' \begin{pmatrix} z_1 \\ z_2 \end{pmatrix} \text{ donc } C \begin{pmatrix} y'_1 \\ y'_2 \end{pmatrix} = C C' \begin{pmatrix} z_1 \\ z_2 \end{pmatrix} \text{ où } C \begin{pmatrix} y'_1 \\ y'_2 \end{pmatrix} = \begin{pmatrix} z_1 \\ z_2 \end{pmatrix}$$

$$C = \begin{pmatrix} 3 & 1 \\ 5 & 2 \end{pmatrix} \text{ donc } z_1 = 3y'_1 + y'_2 \text{ et } z_2 = 5y'_1 + 2y'_2.$$

$$\begin{cases} x_1 \equiv y'_1 (26) \text{ avec } 0 \leq x_1 \leq 25 \\ x_2 \equiv y'_2 (26) \text{ avec } 0 \leq x_2 \leq 25 \end{cases} \text{ donc } \begin{cases} 3x_1 + x_2 \equiv z_1 & (26) \\ 5x_1 + 2x_2 \equiv z_2 & (26) \end{cases}$$

donc z_1 est le nombre codé correspondant à x_1 et z_2 celui correspondant à x_2 .

$$\begin{cases} x_1 \equiv y'_1 (26) \text{ avec } 0 \leq x_1 \leq 25 \\ x_2 \equiv y'_2 (26) \text{ avec } 0 \leq x_2 \leq 25 \end{cases} \text{ donc } \begin{cases} x_1 \equiv 2z_1 - z_2 & (26) \text{ avec } 0 \leq x_1 \leq 25 \\ x_2 \equiv -5z_1 + 3z_2 & (26) \text{ avec } 0 \leq x_2 \leq 25 \end{cases}$$

4. • **Étape 1** : Q est remplacée par 16, R par 17

On obtient une matrice colonne $\begin{pmatrix} z_1 \\ z_2 \end{pmatrix} = \begin{pmatrix} 16 \\ 17 \end{pmatrix}$.

• **Étape 2 :** $C \begin{pmatrix} z_1 \\ z_2 \end{pmatrix} = \begin{pmatrix} 2 & -1 \\ -5 & 3 \end{pmatrix} \begin{pmatrix} 16 \\ 17 \end{pmatrix} = \begin{pmatrix} 2 \times 16 - 17 \\ -5 \times 16 + 3 \times 17 \end{pmatrix} = \begin{pmatrix} 15 \\ -29 \end{pmatrix}$

• **Étape 3 :**

$$0 \leq 15 \leq 26$$

$-29 = 26 \times 2 + 23$ donc $-29 \equiv 23 \pmod{26}$ donc $\begin{pmatrix} 15 \\ -29 \end{pmatrix}$ est remplacé par $\begin{pmatrix} 15 \\ 23 \end{pmatrix}$.

• **Étape 4 :**

Par lecture inverse du tableau :

15 est le nombre correspondant à P et 23 est le nombre correspondant à X donc QC est décodé en PX.