DS1

Exercice 1

Le but de cet exercice est d'envisager plusieurs décompositions arithmétiques du nombre 40.

Partie A

*Les questions **1.** et **2.** sont indépendantes.*

1. Soit $p \in \mathbb{N}$. On dit que p est un nombre premier si :

- $p \geqslant 2$,
- les seuls diviseurs positifs de p sont 1 et p.

Sans justification, donner deux nombres premiers x et y tels que : $40 = x + y$.

Démonstration.
On remarque : $23 + 17 = 40$.
De plus, 23 et 17 sont bien des nombres premiers.

Les réels $x = 23$ et $y = 17$ sont deux nombres premiers tels que : $40 = x + y$.

□

2. Le nombre 40 est une somme de deux carrés puisque : $40 = 2^2 + 6^2$. On veut savoir si 40 est aussi différence de deux carrés. Autrement dit, on s'intéresse à l'équation $x^2 - y^2 = 40$, où x et y désignent deux entiers naturels.

a) Démontrer que, pour tout $(x, y) \in \mathbb{N}^2$, les nombres $x - y$ et $x + y$ ont la même parité.

Démonstration.
Soit $(x, y) \in \mathbb{N}^*$. Deux cas se présentent :

- si $x - y$ est pair, alors : $x - y \equiv 0\ [2]$. On remarque :

$$x + y \ = \ (x - y) + 2\,y$$

De plus, comme $2 \equiv 0\ [2]$, alors : $2\,y \equiv 0\ [2]$. D'où :

$$x + y \equiv 0 + 0\ [2]$$

On en déduit que $x + y$ est pair.

- si $x - y$ est impair, alors : $x - y \equiv 1\ [2]$. On remarque :

$$x + y \ = \ (x - y) + 2\,y$$

De plus : $2\,y \equiv 0\ [2]$. D'où :

$$x + y \equiv 1 + 0\ [2]$$

On en déduit que $x + y$ est impair.

Pour tout $(x, y) \in \mathbb{N}^2$, les nombres $x - y$ et $x + y$ ont la même parité.

Commentaire

On pouvait également répondre à cette question en utilisant la disjonction de cas suivante :

- Si x pair et y pair
- Si x pair et y impair
- Si x impair et y pair
- Si x impair et y impair

Détaillons par exemple le dernier cas. Si x impair et y impair, alors :

$$x \equiv 1\ [2] \qquad \texttt{ET} \qquad y \equiv 1\ [2]$$

On en déduit :

$$x - y \equiv 0\ [2] \qquad \texttt{ET} \qquad x + y \equiv 2\ [2]$$

Or : $2 \equiv 0\ [2]$. D'où : $x + y \equiv 0\ [2]$.
Ainsi, $x - y$ et $x + y$ ont la même parité (ils sont tous les deux pairs).
□

b) En utilisant le fait que $40 = 2^3 \times 5$, déterminer toutes les solutions de l'équation $x^2 - y^2 = 40$, avec $(x, y) \in \mathbb{N}^2$.

Démonstration.
Soit $(x, y) \in \mathbb{N}^2$. On procède par analyse-synthèse.

- **Analyse**. Supposons : $x^2 - y^2 = 40$. Alors :

$$40 \ = \ x^2 - y^2 \ = \ (x - y)(x + y)$$

Or, d'après l'énoncé : $40 = 2^3 \times 5$.
Comme $y \geqslant 0$, alors $x - y \leqslant x + y$ et donc quatre cas se présentent :

× 1er cas : $\begin{cases} x - y = 1 \\ x + y = 40 \end{cases}$.
Ce système n'admet pas de solution puisque, d'après la question précédente, $x - y$ et $x + y$ n'ont pas la même parité.

× 2ème cas : $\begin{cases} x - y = 2 \\ x + y = 20 \end{cases}$. Résolvons ce système.

$$\begin{cases} x - y = 2 \\ x + y = 20 \end{cases} \overset{L_2 \leftarrow L_2 - L_1}{\iff} \begin{cases} x - y = 2 \\ 2y = 18 \end{cases}$$

$$\overset{L_1 \leftarrow 2L_1 + L_2}{\iff} \begin{cases} 2x = 22 \\ 2y = 18 \end{cases}$$

$$\overset{\substack{L_1 \leftarrow \frac{1}{2} L_1 \\ L_2 \leftarrow \frac{1}{2} L_2}}{\iff} \begin{cases} x = 11 \\ y = 9 \end{cases}$$

× 3ème cas : $\begin{cases} x - y = 4 \\ x + y = 10 \end{cases}$. Résolvons ce système.

$$\begin{cases} x - y = 4 \\ x + y = 10 \end{cases} \overset{L_2 \leftarrow L_2 - L_1}{\iff} \begin{cases} x - y = 4 \\ 2y = 6 \end{cases}$$

$$\overset{L_1 \leftarrow 2L_1 + L_2}{\iff} \begin{cases} 2x = 14 \\ 2y = 6 \end{cases}$$

$$\overset{\substack{L_1 \leftarrow \frac{1}{2} L_1 \\ L_2 \leftarrow \frac{1}{2} L_2}}{\iff} \begin{cases} x = 7 \\ y = 3 \end{cases}$$

× $4^{\text{ème}}$ cas : $\begin{cases} x & - & y & = & 5 \\ x & + & y & = & 8 \end{cases}$.
Ce système n'admet pas de solution puisque, d'après la question précédente, $x-y$ et $x+y$ n'ont pas la même parité.

Finalement, les seules couples solutions possibles sont $(11,9)$ et $(7,3)$

- **Synthèse**. Vérifions que les deux couples trouvés sont bien solutions de l'équation : $x^2-y^2=40$.
  × On remarque :
  $$11^2-9^2 \;=\; 121-81 \;=\; 40$$
  Le couple $(11,9)$ est donc bien solution du problème posé.
  × On remarque :
  $$7^2-3^2 \;=\; 49-9 \;=\; 40$$
  Le couple $(7,3)$ est donc bien solution du problème posé.

Finalement, l'ensemble des solutions de l'équation $x^2-y^2=40$ dans $\mathbb{N}^2$ est $\{(11,9),(7,3)\}$. □

Partie B : sommes de cubes

*Les questions **3.** et **4.** sont indépendantes.*

Certains nombres entiers peuvent se décomposer en somme ou différence de cubes d'entiers naturels. Par exemple :
$$\begin{aligned} 13 &= 4^3+7^3+4^3-9^3-2^3 \\ 13 &= -1^3-1^3-1^3+2^3+2^3 \\ 13 &= 1^3+7^3+10^3-11^3 \end{aligned}$$

Dans tout ce qui suit, on écrira pour simplifier « sommes de cubes » à la place de « sommes ou différence de cubes d'entiers naturels ».
Les deux premiers exemples montrent que 13 peut se décomposer en somme de 5 cubes. Le troisième exemple montre que 13 peut se décomposer en somme de 4 cubes.

3. a) En utilisant l'égalité $13=1^3+7^3+10^3-11^3$, donner une décomposition de 40 en somme de 5 cubes.

Démonstration.

- Tout d'abord, d'après la question ***1.*** :
$$40 \;=\; 13+27$$
- Ensuite, d'après l'énoncé : $13=1^3+7^3+10^3-11^3$. On obtient alors :
$$\begin{aligned} 40 &= 1^3+7^3+10^3-11^3+27 \\ &= 1^3+7^3+10^3-11^3+3^3 \end{aligned}$$

Une décomposition de 40 en somme de 5 cubes est : $40=1^3+7^3+10^3-11^3+3^3$.

□

b) Démontrer, pour tout $n \in \mathbb{N}$:

$$6\,n \;=\; (n+1)^3 + (n-1)^3 - n^3 - n^3$$

Démonstration.
Soit $n \in \mathbb{N}$.

- D'une part :

$$\begin{aligned}(n+1)^3 &= (n+1)\,(n+1)^2\\ &= (n+1)\,(n^2+2n+1)\\ &= n^3+2n^2+n+n^2+2n+1\\ &= n^3+3n^2+3n+1\end{aligned}$$

- D'autre part :

$$\begin{aligned}(n-1)^3 &= (n-1)\,(n-1)^2\\ &= (n-1)\,(n^2-2n+1)\\ &= n^3-2n^2+n-n^2+2n-1\\ &= n^3-3n^2+3n-1\end{aligned}$$

- On obtient alors :

$$\begin{aligned}&(n+1)^3 + (n-1)^3 - n^3 - n^3\\ =\;& \cancel{n^3} + 3n^2 + 3n + 1 + \cancel{n^3} - 3n^2 + 3n - 1 - \cancel{n^3} - \cancel{n^3}\\ =\;& \cancel{3n^2} + 3n + \cancel{1} - \cancel{3n^2} + 3n - \cancel{1}\\ =\;& 6n\end{aligned}$$

$$\boxed{\forall n \in \mathbb{N},\ 6n = (n+1)^3 + (n-1)^3 - n^3 - n^3}$$

□

c) En déduire une décomposition de 48 en somme de 4 cubes, puis une décomposition de 40 en somme de 5 cubes, différente de celle donnée en ***3.a)***.

Démonstration.

- On cherche à utiliser la question précédente.
  Comme $48 = 6 \times 8$, on applique la question précédente à $n = 8$. On obtient :

$$\begin{aligned}48 &= 6 \times 8\\ &= (8+1)^3 + (8-1)^3 - 8^3 - 8^3\\ &= 9^3 + 7^3 - 8^3 - 8^3\end{aligned}$$

- On en déduit :

$$\begin{aligned}40 &= 48 - 8\\ &= 9^3 + 7^3 - 8^3 - 8^3 - 8\\ &= 9^3 + 7^3 - 8^3 - 8^3 - 2^3\end{aligned}$$

Une décomposition de 40 en somme de 5 cubes est donc : $40 = 9^3 + 7^3 - 8^3 - 8^3 - 2^3$.

□

4. Le nombre 40 est une somme de 4 cubes : $40 = 4^3 - 2^3 - 2^3 - 2^3$.
On veut savoir si 40 peut être décomposé en somme de 3 cubes.

a) Recopier et compléter en justifiant le tableau suivant :

Reste de la division euclidienne de n par 9	0	1	2	3	4	5	6	7	8
Reste de la division euclidienne de n^3 par 9					1				

Démonstration.

- Si $n \equiv 0$ [9], alors : $n^3 \equiv 0^3$ [9]. D'où :
$$n^3 \equiv 0 \text{ [9]}$$
- Si $n \equiv 1$ [9], alors : $n^3 \equiv 1^3$ [9]. D'où :
$$n^3 \equiv 1 \text{ [9]}$$
- Si $n \equiv 2$ [9], alors : $n^3 \equiv 2^3$ [9]. D'où :
$$n^3 \equiv 8 \text{ [9]}$$
- Si $n \equiv 3$ [9], alors : $n^3 \equiv 3^3$ [9]. 0r : $3^3 = 9 \times 3 \equiv 0$ [9]. D'où :
$$n^3 \equiv 0 \text{ [9]}$$
- Si $n \equiv 5$ [9], alors : $n^2 \equiv 5^2$ [9]. 0r : $5^2 = 25 \equiv 7$ [9]. D'où :
$$\begin{aligned} n^3 &\equiv 5 \times 7 \text{ [9]} \\ \text{donc} \quad n^3 &\equiv 35 \text{ [9]} \\ \text{d'où} \quad n^3 &\equiv 8 \text{ [9]} \qquad (\textit{car } 35 \equiv 8 \text{ [9]}) \end{aligned}$$
- Si $n \equiv 6$ [9], alors : $n^2 \equiv 6^2$ [9]. 0r : $6^2 = 36 \equiv 0$ [9]. D'où :
$$\begin{aligned} n^3 &\equiv 6 \times 0 \text{ [9]} \\ \text{donc} \quad n^3 &\equiv 0 \text{ [9]} \end{aligned}$$
- Si $n \equiv 7$ [9], alors : $n^2 \equiv 7^2$ [9]. 0r : $7^2 = 49 \equiv 4$ [9]. D'où :
$$\begin{aligned} n^3 &\equiv 7 \times 4 \text{ [9]} \\ \text{donc} \quad n^3 &\equiv 28 \text{ [9]} \\ \text{d'où} \quad n^3 &\equiv 1 \text{ [9]} \qquad (\textit{car } 285 \equiv 1 \text{ [9]}) \end{aligned}$$
- Si $n \equiv 8$ [9], alors : $n^2 \equiv 8^2$ [9]. 0r : $8^2 = 64 \equiv 1$ [9]. D'où :
$$\begin{aligned} n^3 &\equiv 8 \times 1 \text{ [9]} \\ \text{donc} \quad n^3 &\equiv 8 \text{ [9]} \end{aligned}$$

On obtient finalement le tableau suivant :

Reste de la division euclidienne de n par 9	0	1	2	3	4	5	6	7	8
Reste de la division euclidienne de n^3 par 9	0	1	8	0	1	8	0	1	8

Commentaire

On a ici détaillé la justification du remplissage de chaque case du tableau par soucis d'exhaustivité. Cependant, comme ici chaque cas se démontre de manière similaire, la démonstration rigoureuse de seulement 2 non triviaux d'entre eux suffit.

□

b) On déduit du tableau précédent, pour tout $n \in \mathbb{N}$:

$$n^3 \equiv 0\ [9] \quad \texttt{OU} \quad n^3 \equiv 1\ [9] \quad \texttt{OU} \quad n^3 \equiv -1\ [9]$$

Prouver que 40 ne peut pas être décomposé en somme de 3 cubes.

Démonstration.
Raisonnons par l'absurde.
Supposons que 40 peut se décomposer en somme de 3 cubes.
Alors il existe $(n, p, q) \in \mathbb{Z}^3$ tel que :

$$40 \ = \ n^3 + p^3 + q^3$$

- Tout d'abord : $40 \equiv 4\ [9]$.
- Ensuite, comme précisé par l'énoncé, d'après le tableau précédent :

$$n^3 \equiv x\ [9] \quad \texttt{ET} \quad p^3 \equiv y\ [9] \quad \texttt{ET} \quad q^3 \equiv z\ [9]$$

où $(x, y, z) \in \{-1, 0, 1\}^3$. Alors :

× d'une part :

$$n^3 + p^3 + q^3 \equiv x + y + z\ [9]$$

× d'autre part :

$$-1 \leqslant x \leqslant 1 \quad \texttt{ET} \quad -1 \leqslant y \leqslant 1 \quad \texttt{ET} \quad -1 \leqslant z \leqslant 1$$

On en déduit : $-3 \leqslant x + y + z \leqslant 3$. En particulier : $x + y + z \neq 4$.

On en déduit :

$$n^3 + p^3 + q^3 \not\equiv 4\ [9]$$

Absurde !

L'entier 40 ne peut donc pas se décomposer en somme de 3 cubes.

□

Exercice 2

1. Soient $p \in \mathbb{N}^*$ et $(a, b, c, d) \in \mathbb{Z}^4$. Démontrer :

$$\left.\begin{array}{l} a \equiv b\ [p] \\ c \equiv d\ [p] \end{array}\right\} \quad \Rightarrow \quad a \times c \equiv b \times d\ [p]$$

Démonstration.
Supposons : $\left\{\begin{array}{l} a \equiv b\ [p] \\ c \equiv d\ [p] \end{array}\right.$. Alors :

× d'une part : $p \mid (a-b)$. Comme $c \in \mathbb{Z}$: $p \mid c\,(a-b)$. Donc : $p \mid (a\,c - b\,c)$.

× d'autre part : $p \mid (c-d)$. Comme $b \in \mathbb{Z}$: $p \mid b\,(c-d)$. Donc : $p \mid (b\,c - b\,d)$.

On en déduit : $p \mid \big((a\,c - \cancel{b\,c}) + (\cancel{b\,c} - b\,d)\big)$. D'où : $p \mid (a\,c - b\,d)$.
Finalement : $a\,c \equiv b\,d\ [p]$. □

2. a) Déterminer la forme algébrique du nombre complexe $\dfrac{3-5\,i}{i+1}$.

Démonstration.
On calcule :

$$\frac{3-5\,i}{i+1} = \frac{(3-5\,i)(1-i)}{(1+i)(1-i)} = \frac{3-3\,i-5\,i+5\,i^2}{1^2-i^2} = \frac{3-8\,i-5}{1-(-1)} = \frac{-2-8\,i}{2}$$

On en déduit que la forme algébrique de $\dfrac{3-5\,i}{i+1}$ est $-1-4\,i$. □

b) Résoudre dans $\mathbb{C}$ l'équation $(1+2\,i)\,z + 5\,i - 1 = 3 - 5\,i\,z$. On donnera le résultat sous forme algébrique.

Démonstration.

- <u>Méthode 1</u> :
  Soit $z \in \mathbb{C}$.

$$\begin{aligned} & (1+2\,i)\,z + 5\,i - 1 = 3 - 5\,i\,z \\ \Leftrightarrow\ & (1+2\,i)\,z + 5\,i\,z = 4 - 5\,i \\ \Leftrightarrow\ & (1+7\,i)\,z = 4 - 5\,i \\ \Leftrightarrow\ & z = \frac{4-5\,i}{1+7\,i} \end{aligned}$$

Cherchons maintenant la forme algébrique de $\dfrac{4-5\,i}{1+7\,i}$:

$$\frac{4-5i}{1+7i} = \frac{(4-5i)(1-7i)}{(1+7i)(1-7i)} = \frac{4-28i-5i+35i^2}{1^2-(7i)^2} = \frac{4-33i-35}{1-49i^2} = \frac{-31-33i}{1-(-49)} = \frac{-31-33i}{50}$$

L'ensemble des solutions de l'équation est $\{-\frac{31}{50} - i\,\frac{33}{50}\}$.

- Méthode 2 :
  Soit $z \in \mathbb{C}$.
  Alors il existe $(x, y) \in \mathbb{R}^2$ tel que : $z = x + i\,y$.

$$
\begin{aligned}
& (1+2\,i)\,z + 5\,i - 1 = 3 - 5\,i\,z \\
\iff \quad & (1+2i)(x+iy) + 5i - 1 = 3 - 5i(x+iy) \\
\iff \quad & x + iy + 2ix + 2i^2y + 5i - 4 + 5ix + 5i^2y = 0 \\
\iff \quad & x + iy + 2ix - 2y + 5i - 4 + 5ix - 5y = 0 \\
\iff \quad & (x - 7y - 4) + i(y + 7x + 5) = 0 \\
\iff \quad & \begin{cases} x - 7y - 4 = 0 \\ y + 7x + 5 = 0 \end{cases} && \textit{(par unicité de la forme algébrique)} \\
\iff \quad & \begin{cases} x - 7y = 4 \\ 7x + y = -5 \end{cases} \\
\overset{L_2 \leftarrow L_2 - 7\,L_1}{\iff} \quad & \begin{cases} x - 7y = 4 \\ 50y = -33 \end{cases} \\
\overset{L_1 \leftarrow 50\,L_1 + 7\,L_2}{\iff} \quad & \begin{cases} 50x = -31 \\ 50y = -33 \end{cases} \\
\overset{\substack{L_1 \leftarrow \frac{1}{50}\,L_1 \\ L_2 \leftarrow \frac{1}{50}\,L_2}}{\iff} \quad & \begin{cases} x = -\frac{31}{50} \\ y = -\frac{33}{50} \end{cases}
\end{aligned}
$$

L'ensemble des solutions de l'équation est $\{-\frac{31}{50} - i\ \frac{33}{50}\}$.

□

Exercice 3

Partie A

Dans l'algorithme ci-contre, les variables a, b et c représentent des entiers naturels.

Algorithme

```
1  c ← 0
2  Tant que a ⩾ b, faire :
3      c ← c + 1
4      a ← a − b
5  Fin Tant que
```

1. On prend $a = 13$ et $b = 4$.
Donner les valeurs de a et c obtenues à la sortie de cet algorithme en indiquant les valeurs des variables à chaque étape.

Démonstration.
Détaillons les étapes de l'algorithme avec les valeurs $a = 13$ et $b = 4$.

1) On commence par initialiser la variable c à 0.

2) On entre ensuite dans une structure itérative (boucle `while`).

- On teste si $a \geqslant b$. À ce stage, la variable a contient 13 et la variable b contient 4. Ainsi, on a bien : $a \geqslant b$. On effectue alors les instructions suivantes :
  - × la variable c est incrémentée de 1. Elle contient donc maintenant la valeur $0 + 1 = 1$.
  - × la variable a est mise à jour et prend la valeur $a - b = 13 - 4 = 9$.

  (notons que la variable b n'est pas mise à jour)
- On teste si $a \geqslant b$. À ce stage, la variable a contient 9 et la variable b contient 4. Ainsi, on a bien : $a \geqslant b$. On effectue alors les instructions suivantes :
  - × la variable c est incrémentée de 1. Elle contient donc maintenant la valeur $1 + 1 = 2$.
  - × la variable a est mise à jour et prend la valeur $a - b = 9 - 4 = 5$.
- On teste si $a \geqslant b$. À ce stage, la variable a contient 5 et la variable b contient 4. Ainsi, on a bien : $a \geqslant b$. On effectue alors les instructions suivantes :
  - × la variable c est incrémentée de 1. Elle contient donc maintenant la valeur $2 + 1 = 3$.
  - × la variable a est mise à jour et prend la valeur $a - b = 5 - 4 = 1$.
- On teste si $a \geqslant b$. À ce stage, la variable a contient 1 et la variable b contient 4. Ainsi : $a \not\geqslant b$. On sort alors de la structure itérative.

À la sortie de cet algorithme, la variable a contient 1 et la variable c contient 3.

□

2. Que permet de calculer cet algorithme ?

Démonstration.
Détaillons les éléments du script proposé.

- **Début du script**
  On initialise la variable c à 0.

```
1  c ← 0
```

- **Structure itérative**
  Les lignes 2 à 5 consistent à déterminer le quotient q et le reste r de la division euclidienne de a. On notera $\mathtt{a}_{\mathtt{depart}}$ la valeur initiale de a (avant une quelconque mise à jour) par b. Pour cela, on doit augmenter la valeur de la variable c jusqu'à ce que la variable a vérifie : $\mathtt{a} < \mathtt{b}$. Autrement dit, on doit augmenter la valeur de la variable c tant que la variable a vérifie : $\mathtt{a} \geqslant \mathtt{b}$. Pour cela, on utilise une structure itérative (boucle while).

```
4        while a >= b:
```

  À chaque tour de boucle, on doit :

  1) incrémenter la variable c de 1.

```
5            c = c + 1
```

  2) mettre à jour la variable a.

```
6            a = a - b
```

  À l'issue de cette boucle, la variable a vérifie :

$$\begin{cases} 0 \leqslant \mathtt{a} < \mathtt{b} \\ \mathtt{a} = \mathtt{a}_{\mathtt{depart}} - \mathtt{c}\,\mathtt{b} \end{cases}$$

  Ainsi :

$$\begin{cases} 0 \leqslant \mathtt{a} < \mathtt{b} \\ \mathtt{a}_{\mathtt{depart}} = \mathtt{c}\,\mathtt{b} + \mathtt{a} \end{cases}$$

  On a donc bien déterminé le quotient c et le reste a de la division euclidienne de $\mathtt{a}_{\mathtt{depart}}$ par b.

□

3. Coder en **Python** cet algorithme.
On considèrera que les entiers a et b ont été au préalable rentrés par l'utilisateur.

Démonstration.
On propose le script suivant :

```
1  c = 0
2  while a >= b :
3      c = c + 1
4      a = a - b
```

□

Partie B

À chaque lettre de l'alphabet, on associe, grâce au tableau ci-dessous, un entier compris entre 0 et 25.

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 définit un procédé de codage de la façon suivante :

- **Étape 1** : à la lettre que l'on veut coder, on associe le nombre m correspondant dans le tableau.
- **Étape 2** : on calcule le reste de la division euclidienne de $9\,m + 5$ par 26 et on le note p.
- **Étape 3** : au nombre p, on associe la lettre correspondante dans le tableau.

4. Coder la lettre U en expliquant votre démarche.

Démonstration.

- **Étape 1**. À la lettre U, on associe le nombre $m = 20$, fourni par le tableau de l'énoncé.
- **Étape 2**. On obtient : $9m + 5 = 9 \times 20 + 5 = 185$. Or :

$$\begin{cases} 185 &= 26 \times 7 + 3 \\ 0 \leqslant 3 < 26 \end{cases}$$

  Donc $p = 3$ est le reste de la division euclidienne de $9m + 5$ par 26.
- **Étape 3**. Au nombre $p = 3$, d'après le tableau de l'énoncé, on associe la lettre D.

On code donc la lettre U avec la lettre D.

□

5. Écrire en **Python**, à l'aide de l'algorithme fourni par l'énoncé, une fonction `Codage` prenant en paramètre un entier `m` et renvoyant l'entier `p` défini par l'algorithme ci-dessus.
*On pourra utiliser la commande prédéfinie en **Python** pour obtenir le reste de la division euclidienne de a par b. Il s'agit de la commande* `a % b`*. Par exemple, la commande* `11 % 4` *renvoie* 3 *: le reste dans la division euclidienne de* 11 *par* 4.

Démonstration.
On propose la fonction suivante :

```
1  def Codage(m) :
2      p = (9 * m + 5) % 26
3      return p
```

Détaillons les éléments de ce script.

- **Début de la fonction**
  On commence par préciser la structure de la fonction :
  - × cette fonction se nomme `Codage`,
  - × elle prend en entrée un paramètre `m`,
  - × elle admet pour variable de sortie la variable `p`.

```
1  def Codage(m) :
```

```
3      return p
```

- **Contenu de la fonction**
  La ligne 2 consiste à chiffrer le nombre `m` à l'aide du procédé défini à l'étape 2. On cherche donc à obtenir le reste de la division euclidienne de $9\texttt{m} + 5$ par 26.

```
2        p = (9 * m + 5) % 26
```

□

Partie C

6. Déterminer un inverse de 9 modulo 26.

Démonstration.
On remarque : $9 \times 3 = 27$. Or : $27 \equiv 1\ [26]$. D'où :

$$9 \times 3 \equiv 1\ [26]$$

L'entier 3 est donc un inverse de 9 modulo 26. □

7. Démontrer alors l'équivalence :

$$9\,m + 5 \equiv p\ [26] \quad \Leftrightarrow \quad m \equiv 3\,p - 15\ [26]$$

Démonstration.
On procède par double implication.

($\Rightarrow$) Supposons : $9m + 5 \equiv p\ [26]$.

$$\begin{array}{rrcll} & 9m + 5 & \equiv & p & [26] \\ \text{alors} & 3(9m + 5) & \equiv & 3p & [26] \\ \text{donc} & 3 \times 9m + 15 & \equiv & 3p & [26] \\ \text{d'où} & 3 \times 9m & \equiv & 3p - 15 & [26] \end{array}$$

Or, d'après la question précédente : $3 \times 9 \equiv 1\ [26]$. Donc : $3 \times 9m \equiv m\ [26]$.
D'où : $m \equiv 3 \times 9m\ [26]$.
Ainsi, par transitivité de la congruence :

$$m \equiv 3p - 15\ [26]$$

($\Leftarrow$) Supposons : $m \equiv 3p - 15\ [26]$. Alors :

$$\begin{array}{rcll} 9m & \equiv & 9(3p - 15) & [26] \\ & \equiv & 9 \times 3p - 135 & [26] \end{array}$$

Or, d'après la question précédente : $9 \times 3 \equiv 1\ [26]$. Donc : $9 \times 3p \equiv p\ [26]$.
De plus : $135 \equiv 5\ [26]$. En effet :

$$135 - 5 \ = \ 130 \ = \ 26 \times 5$$

D'où : $26 \mid (135 - 5)$.
Ainsi : $9 \times 3p - 135 \equiv p - 5\ [26]$.
On en déduit, par transitivité de la congruence : $9m \equiv p - 5\ [26]$. D'où :

$$9m + 5 \equiv p\ [26]$$

Finalement : $9\,m + 5 \equiv p\ [26] \quad \Leftrightarrow \quad m \equiv 3\,p - 15\ [26]$. □

8. Décoder alors la lettre B.

Démonstration.

- La lettre B est chiffrée par l'entier $p = 1$.
  D'après le procédé de codage, on cherche alors $m \in [\![0, 25]\!]$ tel que :

$$9m + 5 \equiv p \ [26]$$

- Or, d'après la question précédente :

$$\begin{array}{lrcll} & 9m+5 & \equiv & p & [26] \\ \Leftrightarrow & m & \equiv & 3p-15 & [26] \\ \Leftrightarrow & m & \equiv & 3\times 1-15 & [26] \quad \textit{(car ici } p=1\textit{)} \\ \Leftrightarrow & m & \equiv & -12 & [26] \\ \Leftrightarrow & m & \equiv & 14 & [26] \quad \textit{(car } -12 \equiv 14 \ [26]\textit{)} \\ \Leftrightarrow & m & = & 14 & \quad \textit{(car } m \in [\![0,25]\!]\textit{)} \end{array}$$

- On sait de plus que la lettre correspondant au chiffre 14 est la lettre O.

On en déduit que la lettre B est décodée en la lettre O.

□