# EXERCICE 3 ( 5 points )

**A chaque exercice prendre une nouvelle copie en mentionnant nom et classe**

**1 )** On considère l'équation (E) : $7u - 13v = 2$

**a)** Déterminer deux entiers relatifs $u$ et $v$ tels que $7u - 13v = 2$

**b)** ~~Déterminer tous les couples $(a; q)$ d'entiers relatifs tels que : $7u - 13v = 2$.~~

**c)** Déterminer tous les couples $(u; v)$ d'entiers relatifs tels que : $7u - 13v = 2$.

**2 )** On considère deux entiers naturels $a$ et $b$.

Pour tout entier $n$, on note $\phi(n)$ le reste de la division euclidienne de $a \times n + b$ par 26.

On décide de coder un message, en procédant comme suit :

- A chaque lettre de l'alphabet on associe un entier compris entre 0 et 25, selon le tableau suivant :

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

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

- Pour chaque lettre du message, on détermine l'entier $n$ associé puis on calcule $\phi(n)$.
- La lettre est alors codée par la lettre associée à $\phi(n)$.

On ne connaît pas les entiers $a$ et $b$, mais on sait que :

- La lettre F est codée par la lettre K ;
- La lettre T est codée par la lettre O.

**a)** Montrer que les entiers $a$ et $b$ sont tels que :

$$\begin{cases} 5a + b \equiv 10 \ \ [26] \\ 19a + b \equiv 14 \ \ [26] \end{cases}$$

**b)** En déduire qu'il existe un entier $q$ tel que $14a - 26q = 4$

**c)** Déterminer tous les couples d'entiers $(a; b)$, avec $0 \leq a \leq 25$ et $0 \leq b \leq 25$, tels que :

$$\begin{cases} 5a + b \equiv 10 \ \ [26] \\ 19a + b \equiv 14 \ \ [26] \end{cases}$$

**3 )** On suppose que $a = 17$ et $b = 3$.

**a)** Coder la lettre « G ».

**b)** Soit $n$ un entier naturel, montrer que $23\ \phi(n) + 9 - n$ est divisible par 26.

**c)** En déduire un procédé de décodage.

**d)** Décoder la lettre « Z ».

# Correction

**1 )**

**e)** On observe que :

$$7 \times 4 - 13 \times 2 = 28 - 26 = 2$$

Donc le couple d'entiers $\boxed{(u; v) = (4; 2)}$ est une solution particulière de (E)

**f)** Erreur d'énoncé, il fallait lire :

Déterminer tous les couples $(u; v)$ d'entiers relatifs tels que : $7u - 13v = 2$.

Soit $(u; v)$ un couple d'entiers relatifs tels que : $7u - 13v = 2$

On a donc : $\begin{cases} 7u - 13v = 2 \\ 7 \times 4 - 13 \times 2 = 2 \end{cases}$

En soustrayant membre à membre ces deux équation, on obtient donc :

$$7(u - 4) - 13(v - 2) = 0 \Leftrightarrow 7(u - 4) = 13(v - 2)$$

7 et 13 sont deux nombres premiers distincts, ils sont donc premiers entre eux.

7 divise le produit $13(v - 2)$ et 7 et 13 sont premiers entre eux, donc, d'après le théorème de Gauss, 7 divise $v - 2$

On a donc $v - 2 = 7k \Leftrightarrow v = 2 + 7k$ où $k \in \mathbb{Z}$

On reprend l'équation diophantienne (E) et d'après ce qui précède on a :

$$7u - 13v = 2 \Leftrightarrow \begin{cases} 7u - 13v = 2 \\ v = 2 + 7k \end{cases} \text{ où } k \in \mathbb{Z}$$

$$\Leftrightarrow \begin{cases} 7u = 13v + 2 \\ v = 2 + 7k \end{cases} \Leftrightarrow \begin{cases} 7u = 13(2 + 7k) + 2 \\ v = 2 + 7k \end{cases}$$

$$\Leftrightarrow \begin{cases} 7u = 26 + 13 \times 7k + 2 \\ v = 2 + 7k \end{cases} \Leftrightarrow \begin{cases} 7u = 13 \times 7k + 28 \\ v = 2 + 7k \end{cases}$$

$$\Leftrightarrow \begin{cases} u = \dfrac{13 \times 7k + 4 \times 7}{7} \\ v = 2 + 7k \end{cases} \Leftrightarrow \begin{cases} u = 4 + 13k \\ v = 2 + 7k \end{cases}$$

Les solutions de l'équation (E) sont donc :

$$\boxed{S = \{(u; v) = (4 + 13k; 2 + 7k)/k \in \mathbb{Z}\}}$$

**4 )**

**a)**

- La lettre F est codée par la lettre K :

Pour la lettre F on a $n = 5$

Pour la lettre K on a donc $\phi(5) = 10$

Or $\phi(5)$ est le reste de la division euclidienne de $a \times 5 + b$ par 26.

On a donc $5a + b \equiv 10 \ \ [26]$

- La lettre T est codée par la lettre O.

Pour la lettre T on a $n = 19$

Pour la lettre O on a donc $\phi(19) = 14$

Or $\phi(19)$ est le reste de la division euclidienne de $a \times 19 + b$ par 26.

On a donc $19a + b \equiv 14 \ \ [26]$

On a donc bien :

$$\boxed{\begin{cases} 5a + b \equiv 10 \ \ [26] \\ 19a + b \equiv 14 \ \ [26] \end{cases}}$$

**b)** On vient de prouver que : $\begin{cases} 5a + b \equiv 10 \ \ [26] \\ 19a + b \equiv 14 \ \ [26] \end{cases}$

En soustrayant membre à membre ces deux équation, on obtient donc :

$$(19a + b) - (5a + b) = 14 - 10 \ \ [26] \Leftrightarrow 19a + b - 5a - b = 4 \ \ [26]$$

$$\Leftrightarrow 14a = 4 \ \ [26] \Leftrightarrow \text{Il existe un entier } q \text{ tel que } 14a = 4 + 26q$$

Ce qui prouve qu'il existe un entier $q$ tel que $14a - 26q = 4$

**c)** D'après la question précédente, on a :

$$\begin{cases} 5a + b \equiv 10 \ \ [26] \\ 19a + b \equiv 14 \ \ [26] \end{cases} \Rightarrow \text{Il existe un entier } q \text{ tel que } 14a - 26q = 4$$

Or on a :

$$14a - 26q = 4 \Leftrightarrow 7a - 13q = 2$$

$$\Leftrightarrow (a; q) \text{ est solution de l'équation (E)}$$

$$\Leftrightarrow \begin{cases} a = 4 + 13k \\ q = 2 + 7k \end{cases} \text{ où } k \in \mathbb{Z}$$

Or on veut avoir :

$$0 \leq a \leq 25 \Leftrightarrow 0 \leq 4 + 13k \leq 25$$

$$\Leftrightarrow -4 \leq 13k \leq 21 \Leftrightarrow -\frac{4}{13} \leq k \leq \frac{21}{13} \Leftrightarrow k = 0 \ ou \ k = 1$$

Car $k$ est un entier et que :

$$-\frac{13}{13} = -1 < -\frac{4}{13} < 0 = \frac{0}{13} \leq k \leq \frac{13}{13} = 1 < \frac{21}{13} < \frac{26}{13} = 2$$

Ainsi les seules valeurs possibles de $a$ sont :

$$\begin{cases} a = 4 + 13 \times 0 = 4 \\ ou \\ a = 4 + 13 \times 1 = 17 \end{cases}$$

On va maintenant calculer les valeurs possibles pour $b$ :

**1° cas :** $a = 4$

$$5a + b \equiv 10 \ [26] \Leftrightarrow 5 \times 4 + b \equiv 10 \ [26]$$

$$\Leftrightarrow b \equiv 10 - 20 \ [26] \equiv -10 \ [26] \equiv -10 + 26 \ [26] \equiv 16 \ [26]$$

Or on veut $0 \leq b \leq 25$, on obtient donc $b = 16$

Il faut encore justifier que la seconde équation $19a + b \equiv 14 \ [26]$ est vérifiée pour le couple $(a; b) = (4; 16)$

$$19a + b \equiv 19 \times 4 + 16 \ [26] \equiv 92 \ [26] \equiv 14 + 3 \times 26 \ [26] \equiv 14 \ [26]$$

Le couple $(a; b) = (4; 16)$ convient.

**2° cas :** $a = 17$

$$5a + b \equiv 10 \ [26] \Leftrightarrow 5 \times 17 + b \equiv 10 \ [26]$$

$$\Leftrightarrow b \equiv 10 - 85 \ [26] \equiv -75 \ [26] \equiv -75 + 3 \times 26 \ [26] \equiv 3 \ [26]$$

Or on veut $0 \leq b \leq 25$, on obtient donc $b = 3$

Il faut encore justifier que la seconde équation $19a + b \equiv 14 \ [26]$ est vérifiée pour le couple $(a; b) = (17; 3)$

$$19a + b \equiv 19 \times 17 + 3 \ [26] \equiv 326 \ [26] \equiv 14 + 12 \times 26 \ [26] \equiv 14 \ [26]$$

Le couple $(a; b) = (17; 3)$ convient.

Ainsi la solution du système posé est :

$$\boxed{S = \{(4; 16); (17; 3)\}}$$

**5 )** On suppose que $a = 17$ et $b = 3$.

**Remarque :** On est rassuré c'est une des deux solutions trouvées précédemment …

**a)** Coder la lettre « G ».

Pour la lettre G on a $n = 6$

On calcule $\phi(6)$ reste de la division euclidienne de $17 \times 6 + 3$ par 26 :

$$17 \times 6 + 3 = 105 = 4 \times 26 + 1$$

Ainsi $\phi(6) = 1$

La lettre codée est donc B

La lettre G est codée en B

**b)** On a, d'après le principe de codage :

$$17n + 3 \equiv \phi(n) \ \ [26]$$

$$\Rightarrow 23(17n + 3) \equiv 23\phi(n) \ \ [26]$$

$$\Leftrightarrow 391n + 69 \equiv 23\phi(n) \ \ [26]$$

Or on a :

$$391 = 15 \times 26 + 1 \equiv 1 \ \ [26]$$

Et :

$$69 = 2 \times 26 + 17 \equiv 17 \ \ [26]$$

On a donc :

$$\left.\begin{array}{l} 391n + 69 \equiv 23\phi(n) \ \ [26] \\ 391 = 15 \times 26 + 1 \equiv 1 \ \ [26] \\ 69 = 2 \times 26 + 17 \equiv 17 \ \ [26] \end{array}\right\} \Rightarrow 1 \times n + 17 \equiv 23\phi(n) \ \ [26]$$

$$n + 17 \equiv 23\phi(n) \ \ [26] \Leftrightarrow 23\phi(n) - n - 17 \equiv 0 \ \ [26]$$

$$\Leftrightarrow 23\phi(n) - n - 17 + 26 \equiv 0 \ \ [26] \Leftrightarrow 23\phi(n) - n + 9 \equiv 0 \ \ [26]$$

Ce qui prouve finalement que $23\phi(n) - n + 9$ est divisible par 26

**c)** On a :

$$23\phi(n) - n + 9 \equiv 0 \ \ [26] \Leftrightarrow 23\phi(n) + 9 \equiv n \ \ [26]$$

On peut décoder un message, en procédant comme suit :

- Pour chaque lettre du message codé, on détermine l'entier $p$ associé dans le tableau de l'énoncé.
- Puis on calcule $\varphi(p)$ le reste de la division euclidienne de $23p + 9$ par 26.
- La lettre est alors décodée par la lettre associée à $\varphi(p)$.

**d)**

Pour la lettre Z on a $p = 25$

On calcule $\varphi(25)$ reste de la division euclidienne de $23 \times 25 + 9$ par 26 :

$$23 \times 25 + 9 = 584 = 22 \times 26 + 12$$

Ainsi $\varphi(25) = 12$

La lettre décodée est donc M

La lettre Z est décodée en M

**Complément :** Si on le temps, on peut vérifier que la lettre M se code bien en Z :

Pour la lettre M on a $n = 12$

On calcule $\phi(12)$ reste de la division euclidienne de $17 \times 12 + 3$ par 26 :

$$17 \times 12 + 3 = 207 = 7 \times 26 + 25$$

Ainsi $\phi(12) = 25$

La lettre codée est donc bien Z