# Olympiades mathématiques de première 2017. Sujet académique de Amiens.

## I Exercice académique : langage codé.

Pour coder un message afin de le garder secret, on utilise la méthode de chiffrement suivante.

- On remplace chaque lettre du message par son rang indiqué dans 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 |

Les autres signes (virgules, espaces, points,...) sont supprimés.

- On calcule le reste $y$ de la division euclidienne de $7x + 5$ par 26.
- On remplace la lettre initiale $x$ par celle ayant pour rang $y$.

Cette technique de codage est appelée *chiffrement affine*.

1. Vérifier, qu'en effectuant la division euclidienne de 89 par 26, on obtient 3 comme quotient et que le reste est 11.
   En déduire que, par cette méthode, la lettre M est codée par la lettre L.

   $89 = 26 \times 3 + 11$.

   Pour la lettre M
   - M est associé à 12.
   - 12 est associé au reste de la division euclidienne de $7 \times 12 + 5 = 89$ par 26. D'après la division euclidienne précédente 12 est associé à 11.
   - La lettre associée à 11 est *L*.

   La lettre $M$ est codée par la lettre L.

2. Coder le mot MATHS.

| $x$ | position | $7x+5$ | reste | $y$ |
|---|---|---|---|---|
| M | 12 | 89 | 11 | L |
| A | 0 | 5 | 5 | F |
| T | 19 | 138 | 8 | I |
| H | 7 | 54 | 2 | C |
| S | 18 | 131 | 1 | B |

MATHS est codé en LFICB.

3. On admet la propriété suivante que l'on pourra utiliser lorsque nécessaire dans toute la suite de l'exercice :

> Soient $a$ et $b$ deux entiers relatifs et $c$ un entier naturel non nul.
>
> $a$ et $b$ ont le même reste dans la division euclidienne par $c$ si et seulement si $a-b$ est un multiple de $c$.

Montrer que, pour tout entier relatif $k$, si $a$ et $b$ ont le même reste dans la division euclidienne par $c$ alors les entiers $ka$ et $kb$ ont le même reste dans la division euclidienne par $c$.

Soit $k \in \mathbb{Z}$.
Supposons que $a$ et $b$ ont le même reste, $r$ (avec $0 \leqslant r < c$), dans la division euclidienne par $c$ et

démontrons que $ka$ et $kb$ ont même reste dans la division euclidienne par $c$.

Il existe des entiers $q_1$ et $q_2$ tels que :

$$a = q_1 \times c + r \quad \text{et} \quad b = q_2 \times c + r$$

En multipliant ces égalités par $k$ :

$$ak = q_1 \times k \times c + kr \quad \text{et} \quad bk = q_2 \times k \times c + kr$$

Nous en déduisons que le reste de la division euclidienne de $ak$ et $bk$ par $c$ est celui de la division euclidienne de $kr$ par $c$. Il s'agit bien du même.

$ka$ et $kb$ ont même reste dans la division euclidienne par $c$.

4. Soient $x$ et $y$ des entiers.

(a) Montrer que si $y$ et $7x$ ont le même reste dans la division euclidienne par 26 alors $15y$ et $x$ ont le même reste dans la division euclidienne par 26.

Supposons que $y$ et $7x$ ont le même reste, $r$ avec $0 \leqslant r \leqslant 25$, dans la division euclidienne par 26 et

démontrons que forcément $15y$ et $x$ ont le même reste dans la division euclidienne par 26.

Par hypothèse, il existe $q_1$ et $q_2$ des entiers tels que

$$y = q_1 \times 26 + r \quad \text{et} \quad 7x = q_2 \times 26 + r$$

Nous en déduisons

$$15 \times y = q_1 \times 15 \times 26 + 15 \times r \quad \text{et} \quad 15 \times 7x = q_2 \times 15 \times 26 \times +15 \times r$$

Autrement dit :

$$\begin{aligned}
&15y = (15q_1) \times 26 + 15r \quad \text{et} \quad 105x = (15q_2) \times 26 + 15r \\
&15y = (15q_1) \times 26 + 15r \quad \text{et} \quad (4 \times 26 + 1)x = (15q_2) \times 26 + 15r \\
&15y = (15q_1) \times 26 + 15r \quad \text{et} \quad (4x) \times 26 + x = (15q_2) \times 26 + 15r \\
&15y = (15q_1) \times 26 + 15r \quad \text{et} \quad x = (15q_2 - 4x) \times 26 + 15r
\end{aligned}$$

Par conséquent $15y$ et $x$ ont le même reste que $15r$ dans la division euclidienne par 26. Donc

| |
|---|
| $15y$ et $x$ ont le même reste dans la division euclidienne par 26. |

(b) Démontrer la réciproque de l'implication précédente.

Supposons que $x$ et $15y$ ont le même reste, $r$ avec $0 \leqslant r \leqslant 25$, dans la division euclidienne par 26 et

démontrons que forcément $y$ et $7x$ ont le même reste dans la division euclidienne par 26.

Par hypothèse, il existe $q_1$ et $q_2$ des entiers tels que

$$x = q_1 \times 26 + r \quad \text{et} \quad 15y = q_2 \times 26 + r$$

Nous en déduisons

$$7 \times x = (q_1 \times 7) \times 26 + 7 \times r \quad \text{et} \quad 7 \times 15y = (q_2 \times 7) \times 26 \times +7 \times r$$

Autrement dit :

$$\begin{aligned} 7x &= (q_1 \times 7) \times 26 + 7r \quad \text{et} \quad 7 \times 15y = (q_2 \times 7) \times 26 \times +7r \\ 7x &= (q_1 \times 7) \times 26 + 7r \quad \text{et} \quad 4y \times 26 + y = (q_2 \times 7) \times 26 \times +7r \\ 7x &= (q_1 \times 7) \times 26 + 7r \quad \text{et} \quad +y = (q_2 \times 7 - 4y) \times 26 \times +7r \end{aligned}$$

Par conséquent $7x$ et $y$ ont le même reste que $7r$ dans la division euclidienne par 26. Donc

$7x$ et  ont le même reste dans la division euclidienne par 26.

5. Déduire alors que : $y$ et $7x + 5$ ont même reste dans la division euclidienne par 26 équivaut à $x$ et $15y + 3$ ont même reste dans la division euclidienne par 26.

   Dans la question précédente nous avons démontré une implication et sa réciproque donc les deux propositions sont équivalentes.

6. À l'aide de la question précédente, décoder le mot ZERLGJFAHB.

| $y$ | position | $15y + 3$ | reste | $x$ |
|---|---|---|---|---|
| Z | 25 | 378 | 14 | O |
| E | 4 | 63 | 11 | L |
| R | 17 | 258 | 24 | Y |
| L | 11 | 168 | 12 | M |
| G | 6 | 93 | 15 | P |
| J | 9 | 138 | 8 | I |
| F | 5 | 78 | 0 | A |
| A | 0 | 3 | 3 | D |
| H | 7 | 108 | 4 | E |
| B | 1 | 18 | 18 | S |

ZERLGJFAHB se décode en OLYMPIADES.

*Déchiffrer un message codé par un chiffrement affine ne pose pas de difficulté. La cryptographie utilise des techniques bien plus complexes pour crypter des textes ou des données et en assurer l'inviolabilité.*