TS spé

Devoir pour le mercredi 17 janvier 2018

Une personne a mis au point le procédé de cryptage suivant :

• À chaque lettre de l'alphabet, on associe un entier naturel n comme indiqué 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 choisit deux entiers naturels a et b compris* entre 0 et 25.

• Tout entier naturel n compris entre 0 et 25 est codé par le reste de la division euclidienne de $an+b$ par 26.

On suppose que la lettre E est codée par la lettre O et que la lettre A est codée par la lettre E.

1°) Déterminer tous les couples $(a\,;b)$ possibles.

2°) Étudier si le codage est envisageable pour chacun des couples obtenus.

* Dans tout le devoir, le mot « compris » est à prendre au sens large : a, b, n peuvent prendre les valeurs 0 et 25.

Corrigé du DM pour le 17-1-2018

1°) Déterminer tous les couples $(a\,;b)$ possibles.

On sait par hypothèse que la lettre E est codée par la lettre O et que la lettre A est codée par la lettre E.

On sait que le codage vérifie les deux conditions C_1 et C_2 suivantes :

C_1 : La lettre E est codée par la lettre O.

C_2 : La lettre A est codée par la lettre E.

Comme l'entier associé à la lettre A est 0 et que la lettre associée à E est 14, la condition C_2 permet de dire que le reste de la division euclidienne de $a\times 0+b=b$ par 26 est égal à 4.
Comme $0\leqslant b\leqslant 25$, on en déduit que $b=4$ car 4 est le seul entier naturel compris entre 0 et 25 dont le reste de la division euclidienne par 26 est égal à 4.

Comme l'entier associé à la lettre E est 4 et que la lettre associée à O est 14, la condition C_1 permet de dire que le reste de la division euclidienne de $a\times 4+4$ par 26 est égal à 14.

On cherche donc les entiers naturels compris entre 0 et 25 tels que le reste de la division euclidienne de $4a+4$ par 26 soit égale à 14.

On teste tous les entiers naturels de 0 à 25.

Pour gagner du temps, on peut utiliser la calculatrice en rentrant la « fonction » $\text{Y1}=\text{reste}(4\text{X}+4,\,26)$.
Compte tenu de la condition $0\leqslant a\leqslant 25$, on obtient deux valeurs possibles pour a : 9 et 22.

Autre façon : On « passe » en congruences modulo 26.

On a donc $4a+4\equiv 14$ (mod. 26).
Par conséquent, $4a\equiv 10$ (mod. 26).
On cherche les entiers naturels compris entre 0 et 25 tels que le reste de la division euclidienne de $4a$ par 26 soit égale à 10.

Il y a deux méthodes possibles.

1ère méthode :

On teste tous les entiers naturels de 0 à 25.

Pour gagner du temps, on peut utiliser la calculatrice en rentrant la « fonction » $\text{Y1}=\text{reste}(4\text{X},\,26)$.
Compte tenu de la condition $0\leqslant a\leqslant 25$, on obtient deux valeurs possibles pour a : 9 et 22.

2e méthode :

$4a \equiv 10 \pmod{26} \Leftrightarrow \exists k \in \mathbb{Z}$ tel que $4a = 10 + 26k$

$\Leftrightarrow \exists k \in \mathbb{Z}$ tel que $2a = 5 + 13k$

$\Leftrightarrow \exists k \in \mathbb{Z}$ tel que $a = \dfrac{5+13k}{2}$

On cherche les valeurs de k telles que $\dfrac{5+13k}{2}$ soit un entier naturel compris entre 0 et 25.

On obtient deux valeurs de k : 1 et 3.
Si $k = 1$, alors $a = 9$.
Si $k = 3$, alors $a = 22$.

Conclusion :

Il existe deux couples possibles : $(9\,;4)$ et $(22\,;4)$.

2°) Étudier si le codage est envisageable pour chacun des couples obtenus.

Dans chaque cas, on dresse une table de cryptage, facilement obtenue grâce à la calculatrice.
Pour chaque lettre, on note n l'entier naturel qui lui correspond et p le reste de la division euclidienne de $an+b$ par 26.

• Déterminons si le couple $(9\,;4)$ est envisageable pour le codage.

Lettre	A	B	C	D	E	F	G	H	I	J	K	L	M
n	0	1	2	3	4	5	6	7	8	9	10	11	12
p	4	13	22	5	14	23	6	15	24	7	16	25	8
Forme cryptée	E	N	W	F	O	X	G	P	Y	H	Q	Z	I

Lettre	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
n	13	14	15	16	17	18	19	20	21	22	23	24	25
p	17	0	9	18	1	10	19	2	11	20	3	12	21
Forme cryptée	R	A	J	S	B	K	T	C	L	U	D	M	V

L'application de codage est « injective » (deux lettres distinctes sont codées par deux lettres distinctes).

Le codage est donc envisageable avec le couple $(9\,;4)$.

On peut aussi observer que certaines lettres sont codées par la même lettre : on dit qu'elles sont invariantes.
C'est le cas des lettres G et T.

• Déterminons si le couple $(22\,;4)$ est envisageable pour le codage.

Lettre	A	B	C	D	E	F	G	H	I	J	K	L	M
n	0	1	2	3	4	5	6	7	8	9	10	11	12
p	4	0	22	18	14	10	6	2	24	20	16	12	8
Forme cryptée	E	A	W	S	D	K	G	B	Y	U	Q	M	I

Lettre	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
n	13	14	15	16	17	18	19	20	21	22	23	24	25
p	4	0	22	18	14	10	6	2	24	20	16	12	8
Forme cryptée	E	A	W	S	D	K	G	B	Y	U	Q	M	I

On observe une cyclicité d'ordre 13.
On observe qu'une lettre peut être codée par 2 lettres différentes.
Le codage n'est donc pas envisageable avec le couple $(22\,;4)$.