## Exercice 4 Candidats ayant suivi l'enseignement de spécialité 5 points

*Les parties A et B sont indépendantes.*

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

. À chaque lettre de l'alphabet, on associe un entier 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 a et b compris entre 0 et 25.

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

Le tableau suivant donne les fréquences f en pourcentage des lettres utilisées dans un texte écrit en français.

| Lettre | A | B | C | D | E | F | G | H | I | J | K | L | M |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Fréquence | 9.42 | 1.02 | 2.64 | 3.38 | 15.87 | 0.94 | 1.04 | 0.77 | 8.41 | 0.89 | 0.00 | 5.33 | 3.23 |

| Lettre | N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Fréquence | 7.14 | 5.13 | 2.86 | 1.06 | 6.46 | 7.90 | 7.26 | 6.24 | 2.15 | 0.00 | 0.30 | 0.24 | 0.32 |

### Partie A

Un texte écrit en français et suffisamment long a été codé selon ce procédé. L'analyse fréquentielle du texte codé a montré qu'il contient 15,9 % de O et 9,4 % de E.

On souhaite déterminer les nombres a et b qui ont permis le codage

**1.** Quelles lettres ont été codées par les lettres O et E ?

**2.** Montrer que les entiers a et b sont des solutions du système :

$$\begin{cases} 4a+b\equiv 14\,(26) \\ b\equiv 4\,(26) \end{cases}$$

**3.** Déterminer tous les couples d'entiers (a;b) ayant pu permettre le codage de ce texte.

### Partie B

**1.** On choisit $a=22$ et $b=4$

**1.a.** Coder les lettres K et X

**1.b.** Ce codage est-il envisagable ?

**2.** On choisit $a=9$ et $b=4$

**2.a.** Montrer que que pour tous les entiers naturels m et n, on a :

$m\equiv 9n+4\ (26) \Leftrightarrow \quad n\equiv 3m+14\ (26)$

**2.b.** Décoder le mot AQ.

**CORRECTION**

**Partie A**

**1.** Dans le tableau donné 15,9 % correspond à la lettre E et 9,4 % correspond à la lettre A.
Conclusion
**La lettre E a été codée selon ce procédé par la lettre O.**
**La lettre A a été codée selon ce procédé par la lettre E.**

**2.** À la lettre E est associée le nombre 4 et à la lettre O est associée le nombre 14 donc :
$4a+b\equiv 14\ (26)$
À la lettre A est associée le nombre 0 et à la lettre E est associée le nombre 4 donc :
$0\times a+b\equiv 4\ (26)$ soit $b\equiv 4\ (26)$
Conséquence
Les entiers a et b sont solutions du système :
$$\begin{cases} 4a+b\equiv 14\ (26) \\ b\equiv 4\ (26) \end{cases}$$

**3.** Les nombres a et b sont des entiers compris entre 0 et 25 donc $b=4$.
Le coefficient de a : 4 n'est pas premier avec 26 donc pour résoudre $4a+4\equiv 14\ (26)$ soit $4a\equiv 10\ (26)$ il est préférable de déterminer les restes de la division euclidienne de 4a par 26 pour toutes les valeurs de a comprises entre 0 et 25.
On donne les résultats sous la forme d'un tableau.

| a | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 4a | 0 | 4 | 8 | 12 | 16 | 20 | 24 | 28 | 32 | 36 | 40 | 44 | 48 |
| Restes | 0 | 4 | 8 | 12 | 16 | 20 | 24 | 2 | 6 | 10 | 14 | 18 | 22 |

| a | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 4a | 52 | 56 | 60 | 64 | 68 | 72 | 76 | 80 | 84 | 88 | 92 | 96 | 100 |
| Restes | 0 | 4 | 8 | 12 | 16 | 20 | 24 | 2 | 6 | 10 | 14 | 18 | 22 |

**Il existe deux valeurs possibles de a : 9 et 22 donc il existe deux couples d'entiers (9;4) et (22;4) ayant pu permettre le codage de ce texte.**

**Partie B**

**1.** Pour $a=22$ et $b=4$

**1.a.** À la lettre K est associée le nombre 10 donc $22\times 10+4=224=8\times 26+16$
$22\times 10+4\equiv 16\ (26)$ au nombre 16 est associé la lettre Q.
**À la lettre K correspond dans le codage la lettre Q.**
À la lettre X est associée le nombre 23 donc $22\times 23+4=506+4=510=26\times 19+16$
$22\times 23+4\equiv 16\ (26)$ au nombre 16 est associé la lettre Q
**À la lettre X correspond dans le codage la lettre Q.**

**1.b.** Ce codage n'est pas envisageable, car à deux lettres distinctes ( K et X) correspond la même lettre codée.
( Il ne serait pas possible de décoder la lettre Q).

Remarque
*Peut-on trouver facilement deux lettres distinctes correspondant à la même lettre codée ?*
*Le pgcd de 22 et 26 est : 2. On a* $26=2\times 13$.
$22\times 0\equiv 0\ (26)$ *et* $22\times 13\equiv 0\ (26)$
On en déduit que les lettres A et N sont codées en la lettre E.

**2.** Pour $a=9$ et $b=4$

**2.a.** Si $m\equiv 9n+4\ (26)$ alors $3\times m\equiv 3\times(9n+4)\ (26)$ $\Leftrightarrow$ $3m\equiv(3\times 9)n+3\times 4\ (26)$
$\Leftrightarrow$ $3m\equiv 27n+12\ (26)\Leftrightarrow$ $3m\equiv n+12\ (26)$ $\Leftrightarrow$ $n\equiv 3m-12\ (26)\Leftrightarrow$ $n\equiv 3m+14\ (26)$
(car : 12+14=26)

. Si $n\equiv 3m+14\ (26)$ alors $9\times n\equiv 9\times(3m+14)\ (26)$ $\Leftrightarrow$ $9n\equiv 27m+126\ (26)$
$\Leftrightarrow$ $9n\equiv m+22\ (26)$ $\Leftrightarrow$ $m\equiv 9n-22\ (26)\Leftrightarrow$ $m\equiv 9n+4\ (26)$
( car : 4+22=26).

. <u>Conclusion</u>
$m\equiv 9n+4\ (26)$ $\Leftrightarrow$ $n\equiv 3m+14\ (26)$

**2.b.** À la lettre A correspond le nombre 0 donc $m=0$ .
$n\equiv 3\times 0+14\ (26)$
$n\equiv 14\ (26)$ et $0\leqslant n\leqslant 25$ donc n=14
On obtient la lettre O
À la lettre Q correspond le nombre 16 donc m=16.
$n\equiv 3\times 16+14\ (26)$
$n\equiv 48+14\ (26)$
$n\equiv 62\ (26)$
62=52+10 donc n=10
On obtient la lettre K
**Le décodage dumot AQ est le mot OK.**