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

Les parties A et B peuvent être traitées de manière indépendante.

Partie A

Afin de crypter un message, on utilise un chiffrement affine.
Chaque lettre de l'alphabet est associée à un nombre entier comme 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

Soit x le nombre associé à la lettre à coder. On détermine le reste y de la division euclidienne de 7x+5 par 26, puis on en déduit la associée à y (c'est elle qui code la lettre d'origine).
Exemple :
M correspond à x=12.
$7\times12+5=89$ $89=3\times26+11$ $89\equiv11\ \ (26)$
11 correspond à la lettre L, donc la lettre M est codée par la lettre L.

1. Coder la lettre L.

2.a. Soit k un entier relatif. Montrer que si $k\equiv7x\ \ (26)$ alors $15k\equiv x\ \ (26)$.
b. Démontrer la réciproque de l'implication précédente.
c. En déduire que $y\equiv7x+5\ \ (26)$ équivaut à $x\equiv15y+3\ \ (26)$

3. A l'aide de la question précédente décoder la lettre E.

Partie B

On considère les suites (a_n) et (b_n) telles que a_0 et b_0 sont des entiers compris entre 0 et 25 inclus et pour tout entier naturel n, $a_{n+1}=7a_n+5$ et $b_{n+1}=15b_n+3$.
Montrer que pour tout entier naturel n, $a_n=\left(a_0+\frac{5}{6}\right)\times7^n-\frac{5}{6}$.
On admet pour la suite du problème que pour tout entier n, $b_n=\left(b_0+\frac{3}{14}\right)\times15^n-\frac{3}{14}$.

Partie C

Déchiffrer un message codé avec un chiffrement affine ne pose pas de difficulté (on peut tester les 312 couples de coefficients possibles). Afin d'augmenter cette difficulté de décryptage, on propose d'utiliser une clé qui indiquera pour chaque lettre le nombre de fois où l'on applique le chiffrement de la partie A.
Par exemple pour coder le mot MATH avec la clé 2-2-5-6, on applique 2 fois le chiffrement affine à la lettre M (cela donne E), 2 fois le chiffrement à la lettre A,5 fois le chiffrement à la lettre T et enfin 6 fois le chiffrement à la lettre H.
Dans cette partie, on utilisera la clé 2-2-5-6.
Décoder la lettre Q dans le mot IYYQ.

CORRECTION

Partie A

1. L correspond à x=11.
$7\times11+5=82$
On effectue la division euclidienne de 82 par 26 : $82=3\times26+4$
y=4 correspond à la lettre E.
L est codée par la lettre **E.**

2.a. Si $k\equiv7x\ (26)$ alors $15k\equiv15*7x\ (26)$ soit $15k\equiv105x\ (26)$
or $105=4\times26+1$ donc $105\equiv1\ (26)$
Conséquence
$15k\equiv x\ (26)$

b. Réciproquement
Si $15k\equiv x\ (26)$ alors $7*15k\equiv7x\ (26)$ soit $105k\equiv7x\ (26)$
Or $105\equiv1\ (26)$ donc $k\equiv7x\ (26)$

c. $y\equiv7x+5\ (26)\Leftrightarrow 15y\equiv15*7x+15*5\ (26)\Leftrightarrow 15y\equiv105x+75\ (26)$
($75=2\times26+23$ $75\equiv23\ (26)$ et $105\equiv1\ (26)$)
$\Leftrightarrow 15y\equiv x+23\ (26)\Leftrightarrow x\equiv15y-23\ (26)$
($-23=(-1)\times26+3$ $-23\equiv3\ (26)$)
$\Leftrightarrow x\equiv15y+3\ (26)$

3. F correspond à y=5
donc $x\equiv15*5+3\ (26)\Leftrightarrow x\equiv78\ (26)$
($78=3\times26+0$ et $78\equiv0\ (26)$)
$\Leftrightarrow x\equiv0\ (26)$
0 correspond à la lettre A
L est décodée par la lettre **A.**

Partie B

a_0 est un entier naturel compris entre 0 et 25 inclus et pour tout entier naturel n,
$a_{n+1}=7a_n+5$.

On veut démontrer en utilisant un raisonnement par récurrrence que pour tout entier naturel n,
on a : $a_n=\left(a_0+\frac{5}{6}\right)\times7^n-\frac{5}{6}$

Initialisation
Pour n=0 $\left(a_0+\frac{5}{6}\right)\times7^0-\frac{5}{6}=a_0+\frac{5}{6}-\frac{5}{6}=a_0$
La propriété est vérifiée pour n=0
Hérédité
Pour démontrer que la propriété est héréditaire pour tout entier naturel n, on suppose que
$a_n=\left(a_0+\frac{5}{6}\right)\times7^n-\frac{5}{6}$ et on doit démontrer que $a_{n+1}=\left(a_0+\frac{5}{6}\right)\times7^{n+1}-\frac{5}{6}$

$$a_{n+1}=7a_n+5=7\times\left[\left(a_0+\frac{5}{6}\right)\times7^n-\frac{5}{6}\right]+5=\left(a_0+\frac{5}{6}\right)\times7^n\times7-\frac{7\times5}{6}+5=\left(a_0+\frac{5}{6}\right)\times7^{n+1}-\frac{5}{6}$$

Conclusion
Le principe de récurrence nous permet d'affirmer que pour tout entier naturel n, on a :

$a_n=\left(a_0+\frac{5}{6}\right)\times 7^n-\frac{5}{6}$

On admet que pour tout entier natureln, on a : $b_n=\left(b_0+\frac{3}{14}\right)\times 15^n-\frac{3}{14}$

Partie C

Remarques

- On peut démontrer les résultats précédents en considérant la suite (u_n) (ou (v_n)) telle que pour tout entier naturel n, par : $u_n=a_n+\frac{5}{6}$ ($v_n=b_n+\frac{3}{14}$).
  On démontre facilement que (u_n) est une suite géométrique de raison 7 ((v_n) est une suite géométrique de raison 15).
  Mais les suites (u_n) et (v_n) ne sont pas des suites d'entiers naturels.
- (a_n) et (b_n) sont des suites d'entiers naturels.
  On peut facilement démontrer ce résultat par un raisonnement par récurrence.
  On peut aussi écrire pour tout entier naturel n :

$$a_n=a_0\times 7^n+\frac{5}{6}\times(7^n-1)=a_0\times 7^n+5\times\left(\frac{7^n-1}{6}\right)$$

$$b_n=b_0\times 15^n+\frac{3}{14}\times(15^n-1)=b_0\times 15^n+3\times\left(\frac{15^n-1}{14}\right)$$

On peut vérifier que :
Pour tout entier naturel n,
7^n-1 est divisible par 6
15^n-1 est divisible par 14
et pour tout entier naturel non nul

$$\frac{7^n-1}{6}=\frac{7^n-1}{7-1}=1+7+7^2+\ldots+7^{n-1}$$

$$\frac{15^n-1}{14}=\frac{15^n-1}{15-1}=1+15+15^2+\ldots+15^{n-1}$$

Première méthode
Pour décoder la lettre Q, on peut utiliser 6 fois l'algorithme de la partie A : $x\equiv 15y+3 \quad (26)$.

(1) Pour la lettre Q correspond y=16.
$x\equiv 15*16+3 \quad (26)$ $x\equiv 243 \quad (26)$
$243=26\times 9+9$ x=9 correspond à la lettre J.

(2) Pour la lettre J correspond y=9.
$x\equiv 15*9+3 \quad (26)$ $x\equiv 138 \quad (26)$
$138=26\times 5+8$ x=8 correspond à la lettre I.

(3) Pour la lettre I correspond y=8
$x\equiv 15*8+3 \quad (26)$ $x\equiv 123 \quad (26)$
$123=26\times 4+19$ x=19 correspond à la lettre T.

(4) Pour la lettre T correxpond y=19
$x\equiv 15*19+3 \quad (26)$ $x\equiv 288 \quad (26)$
$288=26\times 11+2$ x=2 correspond à la lettre C.

(5) Pour la lettre C correspond y=3
$x\equiv 15*2+3 \quad (26)$ $x\equiv 33 \quad (26)$
$33=26\times 1+7$ x=7 correspond la lettre H

(6) Pour la lettre H correspond y=7.
$x\equiv 15*7+3 \quad (26)$ $x\equiv 108 \quad (26)$
$108=26\times 4+4$ x=4 correspond à la lettre E.

Conclusion

La lettre Q est décodée en la lettre **E.**

Deuxième méthode

On peut utiliser la partie B, en calcullant le reste de la division euclidienne de b_6 par 26 (avec $b_0=16$ correspondant àla letre Q).

$$b_6=16\times15^6+3\times\left(\frac{15^6-1}{14}\right)$$

En utilisant la calculatrice

$15^6=11390625$

$\frac{15^6-1}{14}=813616$

$b_6=16\times11390625+3\times813616=184690848$

$b_6=26\times7103494+4$

$b_6\equiv4\ \ (26)$

x=4 correspond la lettre E.