Nouvelle Calédonie Mars 2016

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	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	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 lettre associée à y (*c*'est elle qui code la lettre d'origine).

• Exemple :

– M correspond à $x = 12$

– $7 \times 12 + 5 = 89$

– Or $89 \equiv 11 \quad [26]$ et 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 $k \equiv 7x \quad [26]$ alors $15k \equiv x \quad [26]$.

2. *b*. Démontrer la réciproque de l'implication précédente.

2. *c*. En déduire que $y \equiv 7x + 5 \quad [26]$ équivaut à $x \equiv 15y + 3 \quad [26]$.

3. À l'aide de la question précédente décoder la lettre F.

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,

$$a_{n+1} = 7a_n + 5 \text{ et } b_{n+1} = 15b_n + 3$$

Montrer que pour tout entier naturel n, $a_n = \left(a_0 + \frac{5}{6}\right) \times 7^n - \frac{5}{6}$

On admet pour la suite du problème que pour tout entier naturel n, $b_n = \left(b_0 + \frac{3}{14}\right) \times 15^n - \frac{3}{14}$

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 on lui applique le chiffrement affine 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 $x = 11$
   – $7 \times 11 + 5 = 82$
   – Or $82 \equiv 4 \quad [26]$ et 4 correspond à la lettre E donc la lettre L est codée par la lettre E.

2. *a*. Soit k un entier relatif. Montrer que si $k \equiv 7x \quad [26]$ alors $15k \equiv x \quad [26]$.

Si $k \equiv 7x \quad [26]$ alors $15k \equiv 15 \times 7x \quad [26]$, or $15 \times 7 = 105 = 26 \times 4 + 1$ donc $105 \equiv 1 \quad [26]$ donc $15k \equiv x \quad [26]$.

2. *b*. $15k \equiv x \quad [26]$ donc $15 \times 7k \equiv 7x \quad [26]$ or $15 \times 7 \equiv 1 \quad [26]$ donc $k \equiv 7x \quad [26]$

donc on *a* l'équivalence : $k \equiv 7x \quad [26] \Leftrightarrow 15k \equiv x \quad [26]$.

2. *c*. $y \equiv 7x + 5 \quad [26] \Leftrightarrow 7x \equiv y - 5 \quad [26] \Leftrightarrow x \equiv 15(y - 5) \quad [26] \Leftrightarrow x \equiv 15y - 75 \quad [26]$

$75 = 3 \times 26 - 3$donc $75 \equiv -3 \quad [26]$

$y \equiv 7x + 5 \quad [26] \Leftrightarrow x \equiv 15y - 75 \quad [26] \Leftrightarrow x \equiv 15y + 3 \quad [26]$

3. décoder F consiste à trouver x tel que $y \equiv 7x + 5 \quad [26]$

D'après l'équivalence précédente : $x \equiv 15y + 3 \quad [26]$

F correspond à $y = 5$, donc en remplaçant y par 5 : $x \equiv 78 \quad [26]$ or $78 = 3 \times 26$ donc $x \equiv 0 \quad [26]$

$0 \leq x \leq 25$ donc $x = 0$, F est décodé par A.

Partie B

Initialisation : si $n = 0$ alors $\left(a_0 + \frac{5}{6}\right) \times 7^0 - \frac{5}{6} = a_0$, la propriété est vérifiée pour $n = 0$

Hérédité : Montrons pour tout entier n que si $a_n = \left(a_0 + \frac{5}{6}\right) \times 7^n - \frac{5}{6}$ alors $a_{n+1} = \left(a_0 + \frac{5}{6}\right) \times 7^{n+1} - \frac{5}{6}$.

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

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

La propriété est héréditaire

Conclusion : La propriété est initialisée et héréditaire donc pour tout entier naturel n, $a_n = \left(a_0 + \frac{5}{6}\right) \times 7^n - \frac{5}{6}$.

Partie C

Q est en quatrième position dans IYYQ donc a été obtenu en appliquant « 6 » fois le chiffrement à une lettre inconnue, il faut décoder « 6 » fois de suite d'abord Q puis les différentes lettres obtenues.

Lettre codée	y	$15y + 3$	x	Lettre décodée
Q	16	243	9	J
J	9	138	8	I
I	8	123	19	T
T	19	288	2	C
C	2	33	7	H
H	7	108	4	E

Q est décodée en E

Pas demandé :

Lettre codée	y	$15y + 3$	x	Lettre décodée
I	8	123	19	T
T	19	288	2	C

Lettre codée	y	$15y + 3$	x	Lettre décodée
Y	24	363	25	Z
Z	25	378	14	O

Lettre codée	y	$15y + 3$	x	Lettre décodée
Y	24	363	25	Z
Z	25	378	14	O
O	14	213	5	F
F	5	78	0	A
A	0	3	3	D

IYYQ est donc décodé en CODE