EXERCICE 4 : **5 points**
Candidats ayant suivi l'enseignement de spécialité

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 $89 \equiv 11\ [26]$ 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 $k \equiv 7x\ [26]$ alors $15k \equiv x\ [26]$.
b. Démontrer la réciproque de l'implication précédente.
c. En déduire que $y \equiv 7x + 5\ [26]$ équivaut à $x \equiv 15y + 3\ [26]$.

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, $a_{n+1} = 7a_n + 5$ 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.

Ce document est mis à disposition sous licence Creative Commons
http://creativecommons.org/licenses/by-nc-sa/2.0/fr/

CORRECTION

EXERCICE 4 **5 points**

Candidats ayant suivi l'enseignement de spécialité

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 :

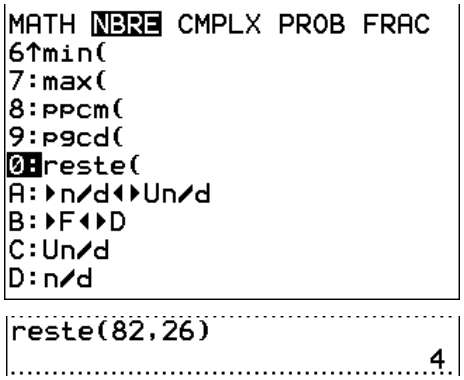
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

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).

1. Coder la lettre L.

L correspond à $x = 11$
$7 \times 11 + 5 = 82$
Or $82 \equiv 4\ [26]$ donc la lettre L est codée par la lettre E.

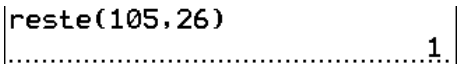
Remarque : Le reste de la division euclidienne de 82 par 26 peut être obtenu avec sa TI83 Premium en utilisant la fonction reste, accessible dans tests A math, onglet NBRE :



---

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

$k \equiv 7x\ [26]$ donc $15k \equiv 15 \times 7x\ [26]$ ainsi $15k \equiv 105x\ [26]$ or $105 \equiv 1\ [26]$ donc $\mathbf{15k \equiv x\ [26]}$



Ce document est mis à disposition sous licence Creative Commons
http://creativecommons.org/licenses/by-nc-sa/2.0/fr/

b. Démontrer la réciproque de l'implication précédente.

Si $15k \equiv x\ [26]$ alors $7 \times 15k \equiv 7x\ [26]$ donc $105k \equiv 7x\ [26]$ or $105 \equiv 1\ [26]$ d'où $\boldsymbol{k \equiv 7x\ [26]}$

---

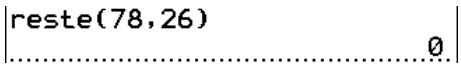
c. En déduire que $y \equiv 7x + 5\ [26]$ équivaut à $x \equiv 15y + 3\ [26]$.

$y \equiv 7x + 5\ [26] \Leftrightarrow y - 5 \equiv 7x\ [26]$
$\Leftrightarrow 15(y-5) \equiv x\ [26]$ d'après les questions 2.a et 2.b
$\Leftrightarrow 15y - 75 \equiv x\ [26] \Leftrightarrow \boldsymbol{15y + 3 \equiv x\ [26]}$ car $-75 \equiv 3\ [26]$

---

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

F correspond à $y = 5$
$15 \times 5 + 3 = 78$
Or $78 \equiv 0\ [26]$ donc la lettre **F est décodée par la lettre A.**



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

Montrons par récurrence sur $n \in \mathbb{N}$ que $a_n = \left(a_0 + \frac{5}{6}\right) \times 7^n - \frac{5}{6}$.

Initialisation : Montrons que la proposition est vraie au rang 0 :
$\left(a_0 + \frac{5}{6}\right) \times 7^0 - \frac{5}{6} = \left(a_0 + \frac{5}{6}\right) - \frac{5}{6} = a_0$. La proposition est donc vraie au rang 0.

Hérédité : Supposons que la propriété est vraie au rang $n \in \mathbb{N}$ fixé : $a_n = \left(a_0 + \frac{5}{6}\right) \times 7^n - \frac{5}{6}$ et montrons qu'elle est vraie au rang $n+1$:
On a $a_{n+1} = 7a_n + 5$ or d'après l'hypothèse de récurrence on a $a_n = \left(a_0 + \frac{5}{6}\right) \times 7^n - \frac{5}{6}$
Ainsi $a_{n+1} = 7\left(\left(a_0 + \frac{5}{6}\right) \times 7^n - \frac{5}{6}\right) + 5 = 7\left(a_0 + \frac{5}{6}\right) \times 7^n - \frac{35}{6} + 5 = \left(a_0 + \frac{5}{6}\right) \times 7^{n+1} - \frac{5}{6}$
La proposition est donc vraie au rang $n+1$.

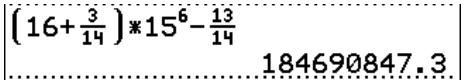
Conclusion : D'après le principe de récurrence, on a montré que $\forall n \in \mathbb{N}\ \boldsymbol{a_n = \left(a_0 + \frac{5}{6}\right) \times 7^n - \frac{5}{6}}$.

Ce document est mis à disposition sous licence Creative Commons
http://creativecommons.org/licenses/by-nc-sa/2.0/fr/

Partie C

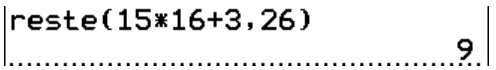
Déchiffrer un message codé avec un chiffrement affine ne pose pas de difficulté (on peut tester les 312 couples de coefficients possibles). Afin d'augmenter cette difficulté de décryptage, on propose d'utiliser une clé qui indiquera pour chaque lettre le nombre de fois où on lui applique le chiffrement 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.

Q correspond à $b_0 = 16$.
Calculons donc b_6 (la clé est 6 pour cette lettre) :
$b_6 = \left(16 + \frac{3}{14}\right) \times 15^6 - \frac{3}{14}$ ce calcul dépasse les capacités de la TI83 Premium :

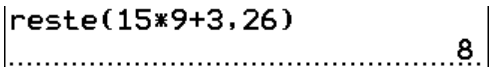


On obtient un nombre qui n'est pas entier, ce qui n'est pas possible, on va calculer b_6 en utilisant la formule de récurrence : $b_{n+1} = 15b_n + 3$:

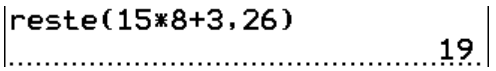
$b_1 \equiv 15b_0 + 3 \ [26]$ soit $b_1 \equiv 15 \times 16 + 3 \ [26]$
donc $b_1 \equiv 9 \ [26]$



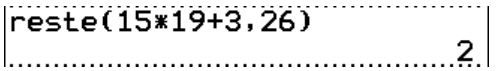
$b_2 \equiv 15b_1 + 3 \ [26]$ soit $b_2 \equiv 15 \times 9 + 3 \ [26]$
donc $b_2 \equiv 8 \ [26]$



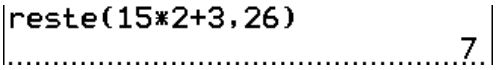
$b_3 \equiv 15b_2 + 3 \ [26]$ soit $b_3 \equiv 15 \times 8 + 3 \ [26]$
donc $b_3 \equiv 19 \ [26]$



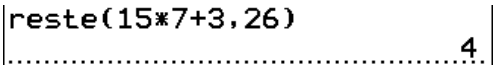
$b_4 \equiv 15b_3 + 3 \ [26]$ soit $b_4 \equiv 15 \times 19 + 3 \ [26]$
donc $b_4 \equiv 2 \ [26]$



$b_5 \equiv 15b_4 + 3 \ [26]$ soit $b_5 \equiv 15 \times 2 + 3 \ [26]$
donc $b_4 \equiv 7 \ [26]$



$b_6 \equiv 15b_4 + 3 \ [26]$ soit $b_6 \equiv 15 \times 7 + 3 \ [26]$
donc $b_6 \equiv 4 \ [26]$



Conclusion : La lettre **Q est décodée en E.**

Ce document est mis à disposition sous licence Creative Commons
http://creativecommons.org/licenses/by-nc-sa/2.0/fr/