

**Thème : arithmétique**

**L'exercice**

Pour coder un message à l'aide d'un chiffrement affine, on commence par remplacer chaque lettre de l'alphabet par un nombre entier de 0 à 25, selon le tableau ci-dessous. Les autres signes du texte sont ignorés.

A	B	C	D	E	F	G	H	I	J	K	...	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	...	23	24	25

Puis on utilise une fonction affine de chiffrement  $f(x) = ax + b$ , avec  $(a, b)$  un couple d'entiers compris entre 0 et 25.

Enfin, on prend le reste de la division par 26 de  $f(x)$  pour obtenir le codage voulu. Pour que  $f(x)$  soit une fonction de chiffrement, il faut que les transformations de deux lettres distinctes donnent deux lettres distinctes.

1. Les fonctions affines suivantes peuvent-elles être utilisées comme fonctions de chiffrement ?  
 $f : x \mapsto 13x + 3$                        $g : x \mapsto 3x + 7$
2. On souhaite choisir comme fonction affine de chiffrement une fonction qui permet de coder C en M et K en A. Montrer que la fonction  $h : x \mapsto 5x + 2$  convient et coder « ALLO » à l'aide de cette fonction.
3. On appelle fonction de décodage de la fonction  $h$ , la fonction de chiffrement  $k : x \mapsto ax + b$  telle que  $k[h(x)] \equiv x [26]$ , pour tout nombre entier  $x$ .
  - a) Montrer que  $5a \equiv 1 [26]$  si et seulement si  $a \equiv 21 [26]$
  - b) En déduire une fonction de décodage de la fonction  $h$ .

**La réponse d'un élève**

1. J'ai prolongé le tableau fourni dans une feuille de calcul tableur pour représenter les fonctions  $f$  et  $g$  et j'ai constaté que  $g$  était un code mais pas  $f$ .

2. C a pour valeur 2,  $f(2) = 12$  qui est bien la valeur de M. K a pour valeur 10,  $f(10) = 52$  qui est un multiple de 26, donc donne bien A. « ALLO » est codé « CFFU »

3. a)  $5 \times 21 = 105 = 4 \times 26 + 1$

b) je cherche la fonction  $l$  de la forme  $l(x) = 21x + b$  qui permet de transformer M en C et A en K, puisqu'il me reste une inconnue, je prends A car sa valeur vaut 0, et  $l(0) = b = 10$ . Je vérifie que ça marche aussi sur M :  $l(12) = 262$  qui est congru à 2 modulo 26.

**Le travail à exposer devant le jury**

- 1- Analysez la production de l'élève en mettant en évidence ses réussites et les progrès qu'il doit réaliser.
- 2- Proposez une correction de la question 3 telle que vous la présenteriez devant une classe de terminale S spécialité mathématiques.
- 3- Présentez deux ou trois exercices d'arithmétique au lycée, dont l'un au moins fait appel à des congruences.