Master MEEF Maths **Capes Externe**
UE 2 **ORAL 2**
2014-2015

Dossier Alg 6	**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 compris entre 0 et 25 , selon le tableau suivant. 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 f 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 de $f(x)$ par 26 pour obtenir le codage voulu.
Pour que la fonction f 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. a. 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. Coder ALLO à l'aide de cette fonction.

b. Existe-t-il d'autres fonctions affines qui permettent de coder C en M et K en A ?

3. On appelle fonction de décodage de la fonction h , la fonction de chiffrement $k : x \mapsto ax + b$ telle que, pour tout entier x , $k[h(x)] \equiv x\ [26]$

a. Montrer que $5a \equiv 1\ [26]$ si et seulement si $a \equiv 21\ [26]$.

b. En déduire une fonction de décodage de h .

La réponse d'un élève à certaines questions

1. *J'ai utilisé le tableur pour calculer les images par f et g des entiers compris entre 0 et 25. J'ai pu constater que g est un code mais que f n'en est pas un.*

2. a *C a pour valeur 2 et h(2) =12 qui est bien la valeur de M. K a pour valeur 10 , h(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 k de la forme : $k(x) = 21x + b$. Elle doit permettre de transformer M en C et A en K. Je prends A : $k(0) = b = 10$. Je vérifie que c'est juste avec M : $k(12) = 21 \times 12 + 10 = 262$ et 262 est congru à 2 modulo 26.*

Le travail à exposer devant le jury

1) Analysez la production de cet élève en mettant en évidence ses réussites et les progrès qu'il doit réaliser.

2) Proposez une correction des questions **2.b** et **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. Vous prendrez soin de motiver vos choix.