ESD 2014E –05 : Arithmétique

1. Le sujet

A. L'exercice proposé au candidat

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.

Lettre	A	B	C	D	E	F	G	H	…	…	X	Y	Z
Nombre	0	1	2	3	4	5	6	7	…	…	23	24	25

Puis on utilise une fonction affine de chiffrement $f(x)=a\,x+b$, 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 ?
$f : x \mapsto 13x+3$ $\qquad$ $g : x \mapsto 3x+7$

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 $k : x \mapsto a\,x+b$ telle que $k[h(x)]=x$ pour tout nombre entier *x*.
3.1. Montrer que $5a \equiv 1\ (26)$ si et seulement si $a \equiv 21\ (26)$
3.2. En déduire une fonction de décodage de la fonction *h*.

B. 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 »*

3.1. $5\times 21=105=4\times 26+1$

3.2. 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.*

C. 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.

2. Eléments de correction

Cet exercice a pour objectif une étude de quelques exemples de « chiffrement affine ». En cryptographie, le chiffrement affine consiste à construire une permutation des lettres de l'alphabet via une fonction affine $x \mapsto ax+b$ modulo 26. La donnée des deux paramètres *a* et *b* détermine la permutation choisie. Le code est très facile à casser, mais le chiffrement affine constitue un intéressant sujet d'étude en arithmétique. De nombreux manuels de terminale propose cette situation soit à titre de problème de synthèse, soit à titre de travaux dirigés.

Le jury a choisi de proposer aux candidats un mauvais énoncé, particulièrement bâclé à plus d'un titre, tant sur des points de détail :

- « Pour que $f(x)$ soit une fonction … » est incorrect : $f(x)$ est un nombre, « pour que la fonction *f* » ou « pour que la fonction $x \mapsto f(x)$ … » serait plus correct.

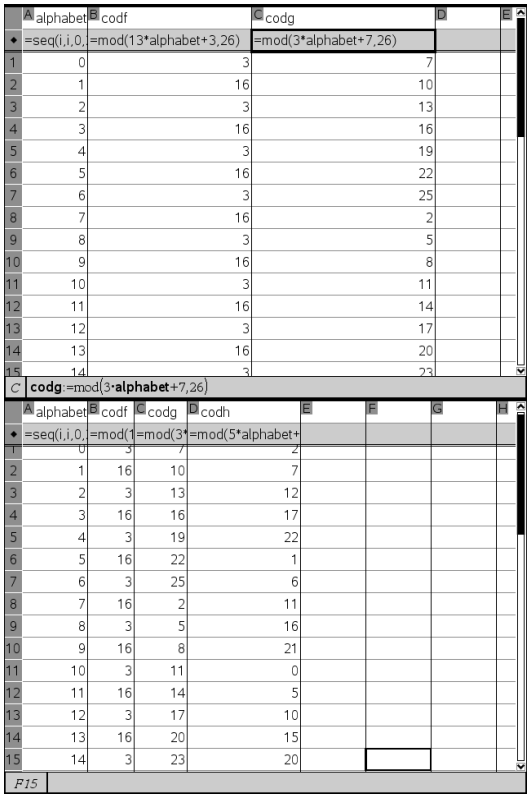
… que, plus préoccupant, sur des questions de fond :

- Stupidité de la question 2. Il s'agit de savoir si le décodage de deux lettres suffit pour casser le code en déterminant *a* et *b*. Mais alors pourquoi donner une réponse dans l'énoncé, ce qui détruit toute part de recherche ? De plus, l'énoncé ne se préoccupe pas de savoir si d'autres fonctions que celle proposée conviennent.
- La question 3.1 relève d'un simple constat et non d'une démonstration construite.
- La question 3.2 ne pose ni la question d'existence (qui n'est pas *a priori* évidente) ni celle de l'unicité éventuelle, qui pourtant aurait un sens puisque l'énoncé a défini (a, b) en tant que couple d'entiers compris entre 0 et 25.

Bref, un énoncé mal ficelé où la part d'initiative laissée aux élèves est très restreinte.
Sur le même thème, le lecteur trouvera sans peine dans les manuels des énoncés beaucoup mieux élaborés que celui-ci.

1.

Question 1.
Réussites
L'élève a su élaborer une expérimentation en utilisant un outil logiciel. Cette expérimentation résout la question posée puisqu'elle donne exhaustivement les images par les deux fonctions *f* et *g* des 26 lettres de l'alphabet.
Echecs.
Cet élève n'a pas justifié pour quelle raison il accepte *g* mais rejette *f* .



	A alphabet	B codf	C codg	D	E
◆	=seq(i,i,0,	=mod(13*alphabet+3,26)	=mod(3*alphabet+7,26)		
1	0	3	7		
2	1	16	10		
3	2	3	13		
4	3	16	16		
5	4	3	19		
6	5	16	22		
7	6	3	25		
8	7	16	2		
9	8	3	5		
10	9	16	8		
11	10	3	11		
12	11	16	14		
13	12	3	17		
14	13	16	20		
15	14	3	23		

C codg :=mod(3·alphabet+7,26)

	A alphabet	B codf	C codg	D codh	E	F	G	H
◆	=seq(i,i,0,	=mod(1	=mod(3*	=mod(5*alphabet+				
1	0	3	7	2				
2	1	16	10	7				
3	2	3	13	12				
4	3	16	16	17				
5	4	3	19	22				
6	5	16	22	1				
7	6	3	25	6				
8	7	16	2	11				
9	8	3	5	16				
10	9	16	8	21				
11	10	3	11	0				
12	11	16	14	5				
13	12	3	17	10				
14	13	16	20	15				
15	14	3	23	20				

F15

Question 2.
Réussites.
Cet élève a su traduire mathématiquement la situation proposée. Son codage du mot *ALLO* est correct.
Echecs.
Il n'a pas justifié pourquoi *f* est une fonction de chiffrement.

Question 3.1
Réussites.
L'élève a compris comment établir l'implication $a \equiv 21\ (26) \Rightarrow 5a \equiv 1\ (26)$ en revenant à la définition d'une congruence.
Echecs.
Ne rédige pas une démonstration construite de l'implication.
N'a pas démontré l'équivalence.

Question 3.2.
Réussites
L'élève propose une expression correcte de l : $l(x) = 21x + 10$, à l'aide d'une résolution artisanale qui exploite judicieusement les indications de l'énoncé.
Echecs
N'a pas justifié que $l(h(x)) = x$ pour tout entier x de $[0\ ;...\ ;\ 25]$

Ce travail montre que cet élève sait chercher (s'engager dans une démarche, prendre des initiatives) et, dans ce contexte au moins, modéliser.
En revanche, cet élève doit progresser dans le domaine du raisonnement (bâtir un raisonnement, savoir confirmer une conjecture) et de la communication de ses résultats (prendre conscience de la nécessité de justifier et de l'importance de la preuve).
Force est de reconnaître que le présent exercice ne va guère l'aider dans cette progression …

2. *Méthode 1*
(attendue par l'énoncé)
La question revient à étudier s'il existe une affine $k : x \mapsto a\,x + b$ telle que $5a\,x + 2a + b \equiv x\ (26)$ pour tout nombre entier x compris entre 0 et 25.
On établit d'abord que la congruence universelle : $5a\,x + 2a + b \equiv x\ (26)$ pour tout nombre entier x compris entre 0 et 25 est équivalente au système de deux congruences $\begin{cases} 5a \equiv 1\ (26) \\ 2a + b \equiv 0\ (26) \end{cases}$.
La recherche de a amène à la résolution d'une équation diophantienne : en effet, $5a \equiv 1\ (26)$ si et seulement si il existe un entier relatif c tel que : $5a + 26c = 1$
Le couple d'entiers relatifs $(-5\ ;\ 1)$ est une solution particulière de cette équation et, plus généralement, les couples solutions en sont les couples de la forme : $(a = -5 + 26u\ ;\ c = 1 - 5u)$ où u est un entier relatif. Un et un seul de ces couples est tel que $-5 + 26u$ est compris entre 0 et 25, obtenu lorsque $u = 1$. C'est le couple $(21\ ;\ -4)$. La question 3.1 telle qu'elle est proposée dans l'énoncé supprime cette partie de la résolution.
La recherche de b amène à déterminer s'il existe un entier compris entre 0 et 25 tel que : $42 + b \equiv 0\ (26)$. Les entiers b qui vérifient cette congruence sont ceux de la forme : $b = -42 + 26d$ où d est un entier relatif. Un et un seul d'entre eux est compris entre 0 et 25, obtenu lorsque $d = 2$, c'est $b = 10$
Il existe donc un et un seul couple d'entiers compris entre 0 et 25 qui vérifient le système $\begin{cases} 5a \equiv 1\ (26) \\ 2a + b \equiv 0\ (26) \end{cases}$, c'est le couple $(a = 21\ ;\ b = 10)$. Il existe donc une et une seule fonction de chiffrement permettant le décodage de h, c'est la fonction : $k : x \mapsto 21x + 10$

Méthode 2.
(basée sur la démarche de l'élève, mais en faisant abstraction de la question 3.1.)
Si $k : x \mapsto a\,x + b$ décode h, alors M est transformé en C et A en K.

C'est-à-dire que : $k(0)=b\equiv 10\ (26)$; $k(12)=12a+b\equiv 2\ (26)$. Les entiers a et b sont des solutions du système de congruences : $\begin{cases} b\equiv 10\ (26) \\ 12a\equiv -8\ (26) \end{cases}$ On retrouve la valeur de b de ci-dessus : $b=10$ mais la recherche de a amène à la résolution de : $12a+26c=-8$, équation équivalente à : $6a+13c=-4$

Cette équation a pour solutions les couples de la forme $(a=8+13u\ ;c=-1+6u)$ où u est un entier relatif.

Deux des couples sont tels que a est compris entre 0 et 25, obtenus pour $u=0$ et pour $u=1$.

Ou bien $a=8$, ou bien $a=13$. Deux fonctions affines sont « candidates », $x\mapsto 8x+10$ et $x\mapsto 21x+10$.

Les entiers 8 et 26 n'étant pas premiers entre eux, la première n'est pas une fonction de chiffrement (par exemple les deux lettres distinctes *A* et *N* donneraient la même lettre). D'ailleurs : $8(5x+2)+10=40x+26\equiv 14x\ (26)$ (et non congru à x comme attendu)

La deuxième en est une qui décode effectivement h : $21(5x+2)+10=105x+52\equiv x\ (26)$ pour tout entier x.

3. Voir REDCM pages 113 à 117.