Dossier 2-13 *Sujet 2010 adapté*

Thème : Arithmétique

L'exercice

1) Déterminer deux entiers relatifs u et v tel que $7u - 13v = 1$ puis déterminer tous les couples (a, k) d'entiers relatifs tels que $14a - 26k = 4$.

2) On considère deux entiers naturels a et b. Pour tout entier n, on note $f(n)$ le reste de la division euclidienne de $an + b$ par 26. On décide de coder un message, en procédant comme suit : à chaque lettre de l'alphabet on associe un entier compris entre 0 et 25, selon le tableau suivant :

Lettre	A	B	C	D	E	F	G	H	I	J	K	L	M
Nombre	0	1	2	3	4	5	6	7	8	9	10	11	12

Lettre	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Nombre	13	14	15	16	17	18	19	20	21	22	23	24	25

Pour chaque lettre du message, on détermine l'entier n associé puis on calcule $f(n)$. La lettre est alors codée par la lettre associée à $f(n)$. On sait que la lettre F est codée par la lettre K et la lettre T est codée par la lettre O.

2.a) Montrer que les entiers a et b sont tels que : $\begin{cases} 5a + b & \equiv 10 \pmod{26} \\ 19a + b & \equiv 14 \pmod{26} \end{cases}$

2.b) En déduire qu'il existe un entier k tel que $14a - 26k = 4$.

2.c) Déterminer tous les couples d'entiers (a, b), avec $0 \leq a \leq 25$ et $0 \leq b \leq 25$, tels que

$$\begin{cases} 5a + b & \equiv 10 \pmod{26} \\ 19a + b & \equiv 14 \pmod{26} \end{cases}$$

2.d) On suppose que $a = 17$ et $b = 3$. Coder le message "GAUSS".

Un extrait des programmes officiels

Programme de terminale scientifique (enseignement de spécialité). BO n°4 du 30 août 2001

Contenus	Modalités de mise en oeuvre	Commentaires
Arithmétique		
Divisibilité dans $\mathbb{Z}$. Division euclidienne. Algorithme d'Euclide pour le calcul du PGCD. Congruences dans $\mathbb{Z}$. Entiers premiers entre eux.	On fera la synthèse des connaissances acquises dans ce domaine au Collège et en classe de Seconde. On étudiera quelques algorithmes simples et on les mettra en oeuvre sur calculatrice ou tableur : recherche d'un PGCD, décomposition d'un entier en facteurs premiers, reconnaissance de la primalité d'un entier.	On montrera l'efficacité du langage des congruences. On utilisera les notations : $a \equiv b \quad (n)$ ou $a \equiv b$ (modulo n) et on établira les compatibilité avec l'addition et la multiplication. Toute introduction de $\mathbb{Z}/n\mathbb{Z}$ est exclue.
Nombres premiers. Existence et unicité de la décomposition en produit de facteurs premiers. PPCM.	On démontrera que l'ensemble des nombres premiers est infini.	L'unicité de la décomposition en facteurs premiers pourra être admise.
Théorème de Bezout. Théorème de Gauss.	Sur des exemples simples, obtention et utilisation de critères de divisibilité. Exemples simples d'équations diophantiennes. Applications élémentaires au codage et à la cryptographie. Application : petit théorème de Fermat	L'arithmétique est un domaine avec lequel l'informatique interagit fortement ; on veillera à équilibrer l'usage de divers moyens de calculs : à la main, à l'aide d'un tableur ou d'une calculatrice.

Dossier 2-13 (suite)

Le travail à exposer devant le jury

1- Analyser les méthodes et les savoirs mis en jeu dans l'exercice.

2- Expliciter la place de cet exercice dans le cadre des programmes.

3- Présenter une solution des questions 1) et 2.c) de l'exercice.

4- Proposer un ou plusieurs exercices se rapportant au thème "Arithmétique".