Baccalauréat Blanc

Mathématiques

Terminale S

Enseignement de spécialité

- Durée de l'épreuve : 4 heures
- Coefficient 9

Ce sujet comporte 4 exercices.

L'utilisation d'une calculatrice est autorisée.

Le candidat veillera à ce que lui soit remis le sujet correspondant à sa spécialité.

La qualité de la rédaction, la clarté et la précision des raisonnements entreront pour une part importante dans l'appréciation des copies.

Exercice 3 : 6 points

Candidats ayant suivi l'enseignement de spécialité

Partie A : ROC : Soient a, b, c, d des entiers relatifs et n un entier naturel non nul.

Prouver que si $a \equiv b \pmod{n}$ et $c \equiv d \pmod{n}$ alors $ac \equiv bd \pmod{n}$.

Supposons que $a \equiv b \pmod{n}$ et $c \equiv d \pmod{n}$, on a $a = b + kn$ et $c = d + k'n$ avec $k, k' dans \mathbb{Z}$
donc $ac = bd + knd + k'nb + kk'n^2$ ie $ac = bd + nq$ avec $q \in \mathbb{Z}$.
D'où $ac \equiv bd \pmod{n}$.

ROC facile car n'utilisant que la définition de la congruence, puis on multiplie et le tour est joué.

Partie B : Inverse de 23 modulo 26 : On considère l'équation (E) : $23x + 26y = 1$, où x, y sont deux entiers relatifs.

1. Vérifier que le couple $(-9\ ;\ 8)$ est une solution de (E).

Remplacer ! On nomme $(x_0\ ;y_0)$ cette solution.

2. Résoudre alors l'équation (E).

On a $23x + 26y = 1$ et $23x_0 + 26y_0 = 1$.

D'où en soustrayant ces deux égalités : $23(x - x_0) + 26(y - y_0) = 0$, soit $23(x - x_0) = 26(y_0 - y)$.(1)

Alors 26 divise $23(x - x_0)$.

Or 23 est premier avec 26 donc d'après le théorème de Gauss, 26 divise $(x - x_0)$.

D'où $x - x_0 = 26\ k$, avec $k \in \mathbb{Z}$. Soit $x = x_0 + 26k$.

En remplaçant dans (1), on obtient $23 \times 26k = 26(y_0 - y)$.

Donc $23k = y_0 - y$ et $y = y_0 - 23k$.

Les solutions sont donc les couples de la forme Soit $(-9 + 26k\ ;\ 8 - 23k)$, pour $k \in \mathbb{Z}$.

Question hyper classique, les équations diophantiennes sont à savoir résoudre parfaitement, sans hésitation.

3. En déduire un entier a tel que $0 \leq a \leq 25$ et $23\ a \equiv 1\ (mod\ 26)$.

Pour toute solution $(x\ ;y) de\ (E)$on a $23x + 26y = ie\ 23\ x \equiv 1\ (mod\ 26)$.

Pour $k = 1$, on obtient $x = -9 + 26 = 17$. Le nombre a cherché est $a = 17$.

Partie C : Chiffrement de Hill : On veut coder un mot de deux lettres suivant la procédure suivante :

Etape 1 : Chaque lettre du mot est remplacée par un entier en utilisant 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

On obtient un couple d'entiers $(x_1; x_2)$ où x_1 correspond à la première lettre du mot et x_2 à la deuxième.

Etape 2 : $(x_1; x_2)$ est transformé en $(y_1; y_2)$ tel que

$$(S_1) \begin{cases} y_1 \equiv 11x_1 + 3x_2 \pmod{26} \\ y_2 \equiv 7x_1 + 4x_2 \pmod{26} \end{cases} avec\ 0 \leq y_1 \leq 25\ et\ 0 \leq y_2 \leq 25$$

Etape 3 : $(y_1; y_2)$ est transformé en un mot de deux lettres en utilisant le tableau de l'étape 1.

Exemple : $TE \rightarrow (19\,;4) \rightarrow (13\,;19) \rightarrow NT$.

1. Coder le mot ST.

$$ST \rightarrow (18\,;19) \rightarrow (255\,;202) \rightarrow (21;20) \rightarrow VU$$

2. On veut maintenant déterminer la procédure de décodage.

   a. Montrer que tout couple $(x_1; x_2)$ vérifiant les conditions du système (S_1), vérifie les équations du système :

$$(S_2) \begin{cases} 23\,x_1 \equiv 4\,y_1 + 23\,y_2 \pmod{26} \\ 23\,x_2 \equiv 19\,y_1 + 11\,y_2 \pmod{26} \end{cases}$$

Supposons que $(x_1; x_2)$ vérifie les conditions du système (S_1), on a : $\begin{cases} y_1 \equiv 11x_1 + 3x_2 \pmod{26} \\ y_2 \equiv 7x_1 + 4x_2 \pmod{26} \end{cases}$

Donc $4\,y_1 + 23\,y_2 \equiv 4\,(11x_1 + 3x_2) + 23\,(7x_1 + 4x_2) \equiv 205\,x_1 + 104\,x_2 \equiv 23\,x_1 + 6 \times 24\,x_2 \equiv 23\,x_1$

et $19\,y_1 + 11\,y_2 \equiv 19\,(11x_1 + 3x_2) + 11\,(7x_1 + 4x_2) \equiv 286\,x_1 + 101\,x_2 \equiv 11 \times 26\ x_1 + 23\,x_2 \equiv 23\,x_2$

Donc $(x_1; x_2)$ vérifie bien les équations du système (S_2).

   b. A l'aide de la partie B, montrer que tout couple $(x_1; x_2)$ vérifiant les conditions du système (S_2) , vérifie les équations du système :

$$(S_3) \begin{cases} x_1 \equiv 16\,y_1 + y_2 \pmod{26} \\ x_2 \equiv 11\,y_1 + 5\,y_2 \pmod{26} \end{cases}$$

Supposons que $(x_1; x_2)$ vérifiant les conditions du système (S_2), on a $\begin{cases} 23\,x_1 \equiv 4\,y_1 + 23\,y_2 \pmod{26} \\ 23\,x_2 \equiv 19\,y_1 + 11\,y_2 \pmod{26} \end{cases}$.

En multipliant chaque ligne par 17 (autorisé d'après la partie A) on obtient d'après la partie B :

$$\begin{array}{l} 23 \times 17\,x_1 \equiv 4 \times 17\,y_1 + 23 \times 17\,y_2 \pmod{26} \\ 23 \times 17\,x_2 \equiv 19 \times 17\,y_1 + 11 \times 17\,y_2 \pmod{26} \end{array}$$

Soit $\begin{array}{l} x_1 \equiv 68\,y_1 + 391\,y_2 \equiv 16y_1 + y_2 \pmod{26} \\ x_2 \equiv 323y_2 + 187\,y_2 \equiv 11\,y_1 + 5\,y_2 \pmod{26} \end{array}$.

Donc $(x_1; x_2)$ vérifie les équations du système (S_3) .

c. Montrer que tout couple $(x_1; x_2)$ vérifiant les conditions du système (S_3) vérifie les équations du système (S_1).

Soit un couple $(x_1; x_2)$ vérifiant les conditions du système (S_3).

On a $\begin{cases} x_1 \equiv 16\, y_1 + y_2 \quad (mod\ 26) \\ x_2 \equiv 11\, y_1 + 5\, y_2 \quad (mod\ 26) \end{cases}$.

Alors $\begin{cases} 11x_1 + 3x_2 \equiv 11\,(16\, y_1 + y_2) + 3\,(11\, y_1 + 5\, y_2) \equiv 209\, y_1 + 26\, y_2 \equiv y_1\ (mod\ 26) \\ 7\, x_1 + 4\, x_2 \equiv 7\,(16\, y_1 + y_2) + 4\,(11\, y_1 + 5\, y_2) \equiv 156 y_1 + 27\, y_2 \equiv y_2\ (mod\ 26) \end{cases}$

D'où $(x_1; x_2)$ vérifie les équations du système (S_1).

On a donc montré que les solutions de (S_1) sont aussi solutions de (S_2) et donc de (S_3). Mais comme les solutions de (S_3) sont aussi solutions de (S_1), ces trois systèmes sont en fait équivalents, c'est-à-dire qu'ils ont les mêmes solutions. On peut donc utiliser (S_3) pour décoder, car il nous donne x_1 et x_2 (codes de départ) en fonction de y_1 et y_2 (codes d'arrivée, des lettres après le codage).

d. Décoder le mot YJ.

En utilisant (S_3) on trouve :

$$(Y\,;\,J) \rightarrow \begin{cases} y_1 = 24 \\ y_2 = 9 \end{cases} \rightarrow \begin{cases} x_1 \equiv 16.24 + 9 \equiv 393 \equiv 3\ (mod\ 26) \\ x_2 \equiv 11.24 + 5.9 \equiv 309 \equiv 23\ (mod\ 26) \end{cases} \rightarrow (D\,;X)$$