Devoir maison numéro 2

Partie A

1. Inventer une matrice $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ carrée d'ordre 2 vérifiant les conditions suivantes :
   - les coefficients a, b, c et d sont entiers, compris entre 1 et 25 inclus ;
   - $\Delta = ad - bc$ n'est pas congru à 1 modulo 26 ;
   - Δ n'est pas pair, ni n'est un multiple de 13.
2. Vérifier que la matrice M n'est pas inversible dans $\mathbb{Z}$: c'est-à-dire que si son inverse existe, les coefficients de cet inverse ne sont pas entiers.

   Envoyer cette matrice par courrier électronique à votre professeur de mathématiques expertes.
   Continuer l'exercice en attendant sa réponse, qui sera à utiliser en fin de devoir.
3. Jusqu'à la fin du devoir, la matrice M est celle trouvée ci-dessus, et toutes les notations de cette question sont conservées.

   a) Préparer une feuille de calcul de tableur sur le modèle ci-contre, avec un bon nombre de lignes. Ces lignes doivent être remplies par copier-glisser de la ligne 2. Écrire les formules de la ligne 2 sur la copie, ou envoyer le fichier au professeur.

k	$k \times \Delta$	$k \times 26$
1	...	26
2	...	52

   b) Rechercher à l'aide de ce tableau deux entiers relatifs u et v tels que : $\Delta \times u - 26 \times v = 1$. Ces deux nombres sont désormais fixés jusqu'à la fin de l'exercice.

   c) Soit $N = u \times \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$.

   On généralise l'écriture des congruences entre entiers aux matrices à coefficients entiers.
   Autrement dit, si $A = (a_{i,j})$ et $B = (b_{i,j})$ sont deux matrices de mêmes dimensions à coefficients entiers, on écrit $A \equiv B$ [26] quand, pour tous i et j, on a : $a_{i,j} \equiv b_{i,j}$ [26].

   Calculer $M \times N$ et $N \times M$, et préciser à quelle matrice connue sont congrus les résultats modulo 26.

Partie B — Chiffrement de Hill

On veut coder un bloc de deux lettres selon la procédure suivante (détaillée en quatre étapes) :

- **Étape 1** : chaque lettre du bloc 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 une matrice colonne $\begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$ où x_1 et x_2 correspondent à la première et à la deuxième lettres du mot.

- **Étape 2** : $\begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$ est transformé en $\begin{pmatrix} y_1 \\ y_2 \end{pmatrix}$ tel que : $\begin{pmatrix} y_1 \\ y_2 \end{pmatrix} = M \times \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$

La matrice M, appelée **matrice de codage**, est celle inventée en A.1.

- **Étape 3** : $\begin{pmatrix} y_1 \\ y_2 \end{pmatrix}$ est transformé en $\begin{pmatrix} z_1 \\ z_2 \end{pmatrix}$ tel que : $\begin{cases} z_1 \equiv y_1\,[26] & \text{avec } 0 \leqslant z_1 \leqslant 25 \\ z_2 \equiv y_2\,[26] & \text{avec } 0 \leqslant z_2 \leqslant 25 \end{cases}$
- **Étape 4** : $\begin{pmatrix} z_1 \\ z_2 \end{pmatrix}$ est transformé en un bloc de deux lettres en utilisant le tableau donné dans l'étape 1.

1. Coder selon cette méthode le mot de six lettres : FERMAT, que l'on séparera en 3 groupes de 2 lettres : FE-RM-AT.
   Question de culture générale : qui était Pierre de Fermat ? La réponse n'a pas à être écrite dans ce devoir.
2. Soit $\begin{pmatrix} z_1 \\ z_2 \end{pmatrix}$ le résultat numérique du codage d'un message $\begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$.

   Écrire une relation de congruence liant $\begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$, $\begin{pmatrix} z_1 \\ z_2 \end{pmatrix}$ et M.

   On se propose de réaliser le calcul : $N \times \begin{pmatrix} z_1 \\ z_2 \end{pmatrix}$. À quoi peut-il servir ? Argumenter la réponse.
3. Votre professeur vous a répondu... Décoder le message qu'il vous a envoyé.

Le valet de chambre entrait. Je ne lui disais pas que j'avais sonné plusieurs fois, car je me rendais compte que je n'avais fait jusque là que le rêve que je sonnais. J'étais effrayé pourtant de penser que ce rêve avait eu la netteté de la connaissance. La connaissance aurait-elle, réciproquement, l'irréalité du rêve ?

Marcel Proust, Sodome et Gomorrhe.