CHIFFRE DE HILL

Niveau : terminale S spécialité. Séance sur table munie d'un poste informatique avec tableur, logiciel de calcul formel.
Lien avec le programme : congruence, matrice, théorème de Bézout, PGCD, problème de chiffrement.
Lien avec *Les maths au quotidien* : **Cryptographie**.

Le chiffrement que nous allons étudier a été publié par *Lester S. Hill* en 1929. C'est un chiffrement polygraphique, c'est-à-dire qu'on ne (dé)chiffre pas les lettres les unes après les autres, mais par paquets. On étudie ici la version bigraphique, c'est-à-dire que l'on groupe les lettres deux par deux, mais on peut envisager des paquets plus grands.

Pour coder un message selon ce procédé, on commence par grouper les lettres de ce message deux par deux, puis on remplace chaque lettre par un nombre, comme indiqué par le tableau suivant :

Lettre	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
Nombre	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 veut par exemple coder le message « J ADORE LES MATHS ».

On le décompose en JA-DO-RE-LE-SM-AT-HS puis on remplace par :
(9 ; 0)-(3 ; 14)-(17 ; 4)-(11 ; 4)-(18 ; 12)-(0 ; 19)-(7 ; 18).

Remarque : si le nombre de lettres du message avait été impair, on aurait ajouté une lettre arbitraire à la fin.

Ensuite chaque couple de nombres (x ; y) de la liste précédente est transformé en un nouveau couple (x' ; y') de nombres entiers compris entre 0 et 25, à l'aide d'une matrice $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ via la relation $A\begin{pmatrix} x \\ y \end{pmatrix} \equiv \begin{pmatrix} x' \\ y' \end{pmatrix}$ [26], ce qui signifie que $\begin{cases} ax + by \equiv x' \ [26] \\ cx + dy \equiv y' \ [26] \end{cases}$. La matrice A est appelé la clé du chiffrement.
Enfin ces deux nombres x' et y' sont transformés en lettres en utilisant le tableau de correspondance.

Le destinataire du message reçoit donc le message codé, et souhaite, à partir des couples de nombres (x' ; y'), retrouver les couples (x ; y) afin de retrouver le message en clair.

On va voir que toute matrice A ne convient pas pour avoir un « bon » chiffrement.

Déjà, pour disposer d'un « bon » chiffrement, on impose qu'à un couple codé (x' ; y') ne corresponde qu'un seul couple (x ; y) en clair, afin de déchiffrer le message sans ambiguïté. Cela signifie que le système précédent d'inconnue (x ; y) n'a qu'une solution. D'après le cours, il est par conséquent nécessaire que la matrice A soit inversible dans $\mathbb{R}$, c'est-à-dire que $ad - bc \neq 0$. On verra si cela constitue une condition suffisante…

I. Étude avec la clé $A = \begin{pmatrix} \mathbf{9} & \mathbf{5} \\ \mathbf{4} & \mathbf{7} \end{pmatrix}$

A. Chiffrement d'un message

1. Par la méthode décrite ci-dessus, coder les deux premières lettres du message « J ADORE LES MATHS »..

2. En utilisant un tableur, élaborer une feuille de calcul permettant le codage rapide de tout le message et donner alors ce message codé.

AIDE EXCEL

Obtenir le nombre correspondant à une lettre donnée du tableau ci-dessus	= CODE(lettre en majuscule) − 65
Obtenir la lettre correspondant à un nombre donné du tableau ci-dessus	= CAR(nombre + 65)
Reste de la division euclidienne de n par m	= MOD(n ; m)

B. Déchiffrement d'un message

1. Montrer que la matrice A est inversible et déterminer son inverse grâce à un logiciel de calcul formel. On écrit cette matrice inverse sous la forme $\frac{1}{43}B$ où B est une matrice à coefficients entiers ($43 = ad - bc = 9\times7 - 4\times5$).

2. Inverse de 43 modulo 26

On considère l'équation (E) : $43x - 26y = 1$, où x et y désignent deux entiers relatifs.

a. Montrer que l'équation (E) a des solutions.

b. En déduire qu'il existe un entier m tel que $0 \leqslant m \leqslant 25$ et $43m \equiv 1$ [26].
(pour les motivés, montrer que cet entier m est unique…utiliser le théorème de Gauss)

c. À l'aide du tableur, reproduire et compléter la feuille de travail ci-dessous : on entrera une formule dans la cellule B2 à étirer vers le bas.

	A	B
1	u	Reste de la division euclidienne de $43u$ par 26
2	1	
3	2	
4	3	
…	…	
24	23	
25	24	
26	25	

d. Donner un entier m tel que $0 \leqslant m \leqslant 25$ et $43m \equiv 1$ [26].

e. Montrer que la matrice mB est telle que $mB\begin{pmatrix}x'\\y'\end{pmatrix} \equiv \begin{pmatrix}x\\y\end{pmatrix}$ [26].

f. En déduire une matrice $A' = \begin{pmatrix}a' & b'\\c' & d'\end{pmatrix}$ avec a', b', c', d' quatre entiers compris entre 0 et 25, telle que $A'\begin{pmatrix}x'\\y'\end{pmatrix} \equiv \begin{pmatrix}x\\y\end{pmatrix}$ [26].

3. Déchiffrer le message (on a ajouté une lettre à la fin du message en clair) :
« BILUPYMDLHMQEQZLZLUESOBIOTXDUEJRUYXXHRMWKOFEHEFEMLXDSOBIWKWPQMGUW AOAOEGUBRKIMLXDSOBIWKPAGAHUHPMKSTPKKYKR »

II. Une condition suffisante pour obtenir « une bonne clé »

1. Dans le déchiffrement précédent, quelle condition particulière sur 43 et 26 permet de répondre à la question **2. a.** de la partie **I. B.** ?

2. Soit la clé $A = \begin{pmatrix}7 & 2\\4 & 3\end{pmatrix}$.
Montrer que $7\times3 - 4\times2$ n'est pas premier avec 26. Donner le PGCD de ces deux nombres.

3. Comparer les produits $A\begin{pmatrix}x\\y\end{pmatrix}$ et $A\begin{pmatrix}x+2\\y+6\end{pmatrix}$ modulo 26. Le procédé de chiffrement par la clé A est-il satisfaisant ?

4. Pour un chiffrement du type $A\begin{pmatrix}x\\y\end{pmatrix} \equiv \begin{pmatrix}x'\\y'\end{pmatrix}$ [26], avec $A = \begin{pmatrix}a & b\\c & d\end{pmatrix}$ où a, b, c, d sont quatre entiers, l'unicité de la correspondance dans le codage est une conséquence de l'inversibilité de la matrice A modulo 26.
Montrer que cette condition est vérifiée lorsque $ad - bc$ et 26 sont premiers entre eux.