Nom : Prénom :	Devoir à la maison 6	Classe : Maths Expertes Pour le Mardi 23 Janvier

EXERCICE 1 :

Le chiffrement affine est une méthode simple de codage d'un message.
À chaque lettre de l'alphabet, on commence par associer son rang dans l'alphabet, diminué de 1, comme l'indique le tableau. On obtient un entier x entre 0 et 25.

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

Le codage affine nécessite deux clés a et b, qui sont des entiers naturels compris entre 0 et 25.
On calcule alors le reste de $ax + b$ dans la division euclidienne par 26.
On obtient un entier y tel que $y \equiv ax + b[26]$. (On choisit $y \in [\![0; 25]\!]$).
On cherche à quelle lettre correspond cet entier y. Cette lettre d'arrivée code alors la lettre de départ.

Partie A : Dans cette partie, on choisit les clés $a = 3$ et $b = 11$.
La fonction de codage est donc $y \equiv 3x + 11[26]$.

1. a. Montrer que G est codé par D. Comment est codé S ?
   b. Remplir, sans justification, 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
x	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
y																										
Codage																										

   c. Quel mot est codé par VBUTSB ?

2. On va maintenant chercher la fonction de décodage, c'est-à-dire l'expression de x en fonction de y.
   a. Chercher l'inverse de 3 modulo 26.
   (C'est-à-dire le nombre entier k tel que $0 \leqslant k \leqslant 25$ et $3k \equiv 1[26]$).
   b. En déduire la fonction de décodage.
   (C'est-à-dire déterminer a' et b' entier naturels tels que $x \equiv a'y + b'$ $[26]$).
   c. Vérifier votre fonction de décodage avec la lettre D.

Partie B : Dans cette partie, on ne connaît pas les clés de codage a et b.
On sait que E est codé par I et que V est codé par T.

1. Écrire les deux congruences vérifiées par a et b.
2. Déterminer a puis b, puis la fonction de codage. *(Aide : l'inverse de 17 modulo 26 est 23).*
3. Déterminer la fonction de décodage. *(Aide : l'inverse de 19 modulo 26 est 11).*

*(**Remarque :** Les amateurs de Python peuvent automatiser certaines étapes de l'exercice 2 avec des programmes. De plus un programme aurait pu aider à trouver "rapidement" les inverses modulo 26).*

EXERCICE 2 : On considère les matrices $A = \begin{pmatrix} 4 & -6 \\ 1 & -1 \end{pmatrix}$ et $P = \begin{pmatrix} 3 & 2 \\ 1 & 1 \end{pmatrix}$.

1. Montrer que la matrice P est inversible et déterminer sa matrice inverse.
2. Montrer que la matrice $P^{-1}AP$ est une matrice diagonale que l'on notera D et dont on donnera une expression.
3. Montrer que pour tout entier naturel n non nul, on a $D^n = \begin{pmatrix} 2^n & 0 \\ 0 & 1 \end{pmatrix}$.
4. Prouver, en utilisant $D = P^{-1}AP$, que $D^n = P^{-1}A^nP$ pour $n \in \mathbb{N}^*$.
5. Déduire de ce qui précède une expression de A^n en fonction de $n \in \mathbb{N}^*$.