Le chiffre affine

Exercice 1

À l'aide de la table de multiplication de $\mathbb{Z}_{26}$, répondre aux questions suivantes :

a) Peut-on trouver deux nombres a et b tels que

$$a \cdot b \equiv 0 \mod 26 \ ?$$

b) Donner la liste des nombres tels que

$$a \cdot b \equiv 0 \mod 26$$

c) Peut-on résoudre l'équation $3 \cdot z \equiv 1$ modulo 26 ?

d) Peut-on résoudre l'équation $14 \cdot z \equiv 1$ modulo 26 ?

e) Peut-on résoudre l'équation $13 \cdot z \equiv 1$ modulo 26 ?

f) Donner la liste des nombres inversibles modulo 26. C'est à dire la liste des a tels qu'il existe b avec

$$a \cdot b \equiv 1 \mod 26$$

g) Combien peut-on former de clefs pour le chiffrement affine ?

Les deux exercices suivants sont à faire à l'aide de code python.

Exercice 2

Chiffrer, à l'aide du décalage affine dont la clef est $(3, 13)$, le message suivant :

`PARFOISMAVIEOUVRAITLESYEUXDANSLOBSCURITE`

Donner la fonction de déchiffrement et retrouver le message à partir du chiffre.

Exercice 3

Établir la table de la fonction $f(z) = (2 \cdot z + 3) \mod 5$. Peut-on inverser cette fonction ? Justifier.

Exercice 4

Établir la table de la fonction $f(z) = (2 \cdot z + 3) \mod 4$. Peut-on inverser cette fonction ? Justifier.

Exercice 5

On a chiffré un message à l'aide du chiffrement affine avec $a = 15$ et $b = 7$. Le chiffre est donné ci-dessous :

`QHGJYXRRXGVAPPGQHRPAVLGXKXGP`

Déchiffrer ce message.

Exercice 6

À l'aide d'un ordinateur et en utilisant python, chiffrer les messages ci-dessous avec le chiffrement affine en utilisant la clef indiquée.

```
LAFOLLAANONIMACHERENDEANONIMIQUASIINVISIBILICOSICOSA (17, 24)
MAITRECORBEAUSURUNARBREPERCHETENAITENSONBECUNFROMAGE (15, 15)
ISURVIVEDANOTHERMEETINGTHATSHOUDHAVEBEENANEMAIL (3, 7)
IFYOUDONTKNOWTHATYOUDONTKNOWYOUTHINKYOUKNOW (5, 12)
QUOUSQUETANDEMABUTERECATILINAPATIENTIANOSTRA (11, 2)
UNCHAMPDEBLEPRENAITRACINESOUSLACOIFFEDEBECASSINE (7, 3)
VOMKLEINENMAULWURFDERWISSENWOLLTEWER (1, 1)
QUOILAMICECROCESTALAMODEPOURPRENDRESONCHAPEAU (19, 9)
TOBEORNOTTOBETHATISTHEQUESTIONWHETHERTISNOBLERINTHEMIND (21, 22)
ONVAALLERALHOTELSANSPAYERONVASINSCRIREALAFACSANSYALLER (23, 2)
```

Exercice 7

À l'aide d'un ordinateur et en utilisant python, déchiffrer les messages ci-dessous avec la clef de chiffrement affine indiquée.

```
SIKMLGCMOWOJKOWARGLGCKFWBKIJBJWTFJWA  avec la clef (17, 6)
WBEMCNMFVKFMQVPSVEMCNMFVKFMQEMCVPWFK  avec la clef (7, 18)
CTQPGODVALJADNATGUXNGQUTASYCSJGQYUFF  avec la clef (5, 6)
QTFRYBDMBMFZJYXJOIUBOXDVVBMXTYYCBXBO  avec la clef (7, 25)
OKENBOBADMZWHRANCAAHOZUHRMHKRWEDRMBA  avec la clef (23, 12)
VNBEUHXFUSHNJZJUJANUSUHKHUXWHEHANBEH  avec la clef (5, 13)
RKXWKJTKRRKXWRVGRMARVWSIWARMKTQVWRVW  avec la clef (17, 6)
IOSOYIOQTKXVQCKFOTQDQAKTWHWXKNKTWQXT  avec la clef (21, 10)
NGVWNNGGTWTEQGMBSFSTPSGTWTEQECOGIEET  avec la clef (3, 6)
ARLEEZZOBEZPATOZKERKJEMOBARLEKYRKWBY  avec la clef (9, 4)
```

Exercice 8

En utilisant le fichier liste_mots_francais.txt, écrire un programme qui casse le chiffre affine automatiquement pour un message d'origine écrit en français. Le programme retourne le message clair et la clef de chiffrement.