DS2

Exercice 1

1. On considère dans l'ensemble dse nombres complexes l'équation (E) d'inconnue z :

$$z^3 + \left(-2\sqrt{3} + 2i\right) z^2 + \left(4 - 4i\sqrt{3}\right) z + 8i \;=\; 0 \qquad (E)$$

a) Montrer que le nombre $-2i$ est solution de l'équation (E).

b) Vérifier que, pour tout $z \in \mathbb{C}$, on a :

$$z^3 + \left(-2\sqrt{3} + 2i\right) z^2 + \left(4 - 4i\sqrt{3}\right) z + 8i \;=\; (z + 2i)\,\left(z^2 - 2\sqrt{3}\,z + 4\right)$$

c) Résoudre l'équation (E) dans $\mathbb{C}$.

Dans la suite, on se place dans le plan muni d'un repère orthonormé direct d'origine O.
On dit qu'un point M a pour affixe z s'il a pour coordonnées $(\mathrm{Re}\,(z)\,,\mathrm{Im}\,(z))$. Par exemple, le point d'affixe $2 - 3i$ a pour coordonnées $(2, -3)$.

2. On considère les points A, B et C d'affixes respectives $-2i$, $\sqrt{3} + i$ et $\sqrt{3} - i$.

a) Quelles sont les coordonnées des points A, B et C ?

b) On rappelle que la distance d'un point $M = (x_M, y_M)$ à un point $N = (x_N, y_N)$ s'obtient à l'aide de la formule suivante : $\sqrt{(x_N - x_M)^2 + (y_N - y_M)^2}$.
Calculer la distance des points A, B et C à l'originie O.
En déduire que A, B et C appartiennent à un même cercle de centre O dont on déterminera le rayon.

c) Placer ces points sur une figure que l'on complètera par la suite.

d) On note D le milieu du segment $[OB]$. Déterminer l'affixe z_L du point L tel que $AODL$ soit un parallélogramme.

3. On rappelle que, dans un repère orthonormé du plan, deux vecteurs de coordonnées respectives (x, y) et (x', y') sont orthogonaux si et seulement si $xx' + yy' = 0$.

a) Soit $\vec{u}$ et $\vec{v}$ deux vecteurs du plan de coordonnées respectives (x, y) et (x', y'). On note $z = x + iy$ et $z' = x' + iy'$.
Montrer que $\vec{u}$ et $\vec{v}$ sont orthogonaux si et seulement si $z\,\overline{z'}$ est un imaginaire pur.

b) À l'aide de la question ***3.a)***, démontrer que le triangle AOL est rectangle en L.

Exercice 2

1. Énoncer et démontrer la formule du binôme de Newton.

2. Soit $(x, y, z) \in \mathbb{R}^3$. On considère les 3 matrices suivantes.

$$A = \begin{pmatrix} 1 & 1 & 1 \\ 2 & 1 & 3 \\ 1 & 2 & 2 \end{pmatrix}, \quad X = \begin{pmatrix} x \\ y \\ z \end{pmatrix} \quad \text{et} \quad B = \begin{pmatrix} 2 \\ 1 \\ 2 \end{pmatrix}$$

a) Calculer le produit AX.

b) Démontrer l'équivalence suivante :

$$AX = B \quad \Leftrightarrow \quad \left\{ \begin{array}{rcrcrcl} x & + & y & + & z & = & 2 \\ 2x & + & y & + & 3z & = & 1 \\ x & + & 2y & + & 2z & = & 2 \end{array} \right.$$

c) Résoudre alors l'équation $AX = B$ d'inconnue $(x, y, z) \in \mathbb{R}^3$.

Exercice 3

À toute lettre de l'alphabet, on associe un nombre entier x compris entre 0 et 25 comme indiqué dans 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

Le « chiffre de RABIN » est un dispositif de cryptage asymétrique inventé en 1979 par l'informaticien Michael Rabin.
Alice veut communiquer de manière sécurisée en utilisant ce cryptosystème. Elle choisit deux nombres premiers distincts p et q. Ce couple de nombres est sa clé privée qu'elle garde secrète. Elle calcule ensuite $n = p \times q$ et elle choisit un nombre entier naturel B tel que $0 \leqslant B \leqslant n - 1$.
Si Bob veut envoyer un message secret à Alice, il le code lettre par lettre.
Le codage d'une lettre représentée par le nombre entier x est le nombre y tel que :

$$y \equiv x(x + B)\ [n] \quad \text{avec} \quad 0 \leqslant y \leqslant n$$

Dans tout l'exercice, on prend $p = 3$, $q = 11$ donc $n = p \times q = 33$ et $B = 13$.

Partie A : Cryptage

Bob veut envoyer le mot « NO » à Alice.

1. Montrer que Bob code la lettre « N » avec le nombre 8.

2. Déterminer le nombre qui code la lettre « O ».

3. Écrire en **Python** une fonction `Codage` prenant en paramètre un entier `x` entre 0 et 25 (`x` est le nombre correspondant à la lettre à coder) et renvoyant l'entier `y` correspondant au codage de `x` par chiffrement de RABIN.
*On pourra utiliser la commande prédéfinie en **Python** pour obtenir le reste de la division euclidienne de a par b. Il s'agit de la commande* `a % b`. *Par exemple, la commande* `11 % 4` *renvoie* 3 *: le reste dans la division euclidienne de* 11 *par* 4.

Partie B : Décryptage

Alice a reçu un message crypté qui commence par le nombre 3.
Pour décoder ce premier nombre, elle doit déterminer le nombre entier x tel que :

$$x(x+13) \equiv 3\ [33] \quad \text{avec} \quad 0 \leqslant x < 26$$

3. Démontrer : $x(x+13) \equiv 3\ [33] \ \Leftrightarrow\ (x+23)^2 \equiv 4\ [33]$.

4. a) Montrer que si $(x+23)^2 \equiv 4\ [33]$, alors le système d'équations $\begin{cases} (x+23)^2 & \equiv & 4 & [3] \\ (x+23)^2 & \equiv & 4 & [11] \end{cases}$ est vérifié.

b) On admet que, réciproquement, si $\begin{cases} (x+23)^2 & \equiv & 4 & [3] \\ (x+23)^2 & \equiv & 4 & [11] \end{cases}$, alors $(x+23)^2 \equiv 4\ [33]$.

En déduire : $x(x+13) \equiv 3\ [33] \ \Leftrightarrow\ \begin{cases} (x+23)^2 & \equiv & 1 & [3] \\ (x+23)^2 & \equiv & 4 & [11] \end{cases}$

5. a) Déterminer les entiers $a \in [\![0,2]\!]$ tels que : $a^2 \equiv 1\ [3]$.

b) Déterminer les entiers $b \in [\![0,10]\!]$ tels que : $b^2 \equiv 4\ [11]$.

6. a) En déduire que $x(x+13) \equiv 3\ [33]$ équivaut aux quatre systèmes suivants :

$$\begin{cases} x & \equiv & 2 & [3] \\ x & \equiv & 8 & [11] \end{cases} \quad \text{ou} \quad \begin{cases} x & \equiv & 0 & [3] \\ x & \equiv & 1 & [11] \end{cases} \quad \text{ou} \quad \begin{cases} x & \equiv & 2 & [3] \\ x & \equiv & 1 & [11] \end{cases} \quad \text{ou} \quad \begin{cases} x & \equiv & 0 & [3] \\ x & \equiv & 8 & [11] \end{cases}$$

b) On admet que chacun des systèmes admet une unique solution entière x telle que $0 \leqslant x < 33$.
Déterminer, sans justification, chacune de ces solutions.

7. Compléter l'algorithme **Python** suivant pour qu'il affiche les quatre solutions trouvées dans la question précédente.

```
for ..... in range(.....) :
    if ..... % ..... == ..... :
        print(.....)
```

8. Alice peut-elle connaître la première lettre du message envoyé par Bob ?
Le « chiffre de RABIN » est-il utilisable pour décoder un message lettre par lettre ?