DS2 /90

Exercice 1 /33

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).

- **2 pts**

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

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

- **1 pt : soit** $z \in \mathbb{C}$
- **1 pt : calcul**

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

- **1 pt : quantification de** z
- **1 pt :** z **solution de** $(E) \Leftrightarrow z + 2i = 0$ `OU` $z^2 - 2\sqrt{3}\, z + 4 = 0$
- **1 pt : introduction rigoureuse de** Δ
- **1 pt :** $\Delta = -4$
- **1 pt :** $z_1 = \sqrt{3} + i$ **et** $z_2 = \sqrt{3} - i$
- **1 pt :** $\mathcal{S} = \{-2i, \sqrt{3} + i, \sqrt{3} - i\}$
- -1 **si l'élève ne raisonne pas par équivalence**

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 ?

- **1 pt :** $A = (0, -2)$
- **1 pt :** $B = (\sqrt{3}, 1)$
- **1 pt :** $C = (\sqrt{3}, -1)$

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.

- **1 pt :** $AO = 2$
- **1 pt :** $BO = CO = 2$
- **1 pt :** A, B **et** C **appartiennent au cercle de centre** O **et de rayon** 2

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

- **3 pts : placement de** A, B **et** C
- **1 pt : tracé du cercle de centre** O **et de rayon** 2

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

- **1 pt :** $D = \left(\frac{\sqrt{3}}{,}2\frac{1}{2}\right)$
- **1 pt :** $AODL$ **parallélogramme** $\Leftrightarrow \overrightarrow{AL} = \overrightarrow{OD}$
- **1 pt :** $\overrightarrow{AL} = \overrightarrow{OD} \Leftrightarrow (x_L, y_L + 2) = (x_D, y_D)$
- **1 pt :** $D = \left(\frac{\sqrt{3}}{,}2 - \frac{3}{2}\right)$
- **1 pt :** $z_L = \frac{\sqrt{3}}{-}2\frac{3}{2}\,i$
- **3 pts : compléter la figure avec** D**,** L **et le parallélogramme** $AODL$

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.

- **1 pt :** $z\,\overline{z'} \in i\,\mathbb{R} \Leftrightarrow z\,\overline{z'} = -\overline{z\,\overline{z'}}$
- **1 pt : reste**

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

- **1 pt :** AOL **rectangle en** $L \Leftrightarrow \overrightarrow{AL}$ **et** $\overrightarrow{LO}$ **orthogonaux**
- **1 pt :** $\overrightarrow{AL}$ **et** $\overrightarrow{LO}$ **orthogonaux** $\Leftrightarrow z_{\overrightarrow{AL}}\,\overline{z_{\overrightarrow{LO}}} \in i\,\mathbb{R}$
- **1 pt :** $z_{\overrightarrow{OL}} = -\frac{\sqrt{3}}{2} + \frac{3}{2}\,i$
- **1 pt :** $z_{\overrightarrow{AL}}\,\overline{z_{\overrightarrow{LO}}} = i\,\sqrt{3} \notin i\,\mathbb{R}$

Exercice 2 /15

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

- **1 pt : énoncer la formule**
- **1 pt :** $\mathcal{P}(n)$ **posée convenablement**
- **1 pt : initialisation**
- **1 pt : hérédité démarrée rigoureusement**
- **1 pt : distributivité**
- **1 pt : décalage d'indice**
- **1 pt : isolation des termes « en trop »**
- **1 pt : triangle de Pascal**
- **1 pt : reste du calcul**

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.

- **1 pt :** $AX = \begin{pmatrix} x+y+z \\ 2x+y+3z \\ x+2y+2z \end{pmatrix}$

b) Démontrer l'équivalence suivante :

$$AX = B \quad \Leftrightarrow \quad \begin{cases} x + y + z = 2 \\ 2x + y + 3z = 1 \\ x + 2y + 2z = 2 \end{cases}$$

- **1 pt : utilisation de *2.a)***
- **1 pt : reste**

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

- **3 pts :** $\mathcal{S} = \{(2, \frac{3}{2}, -\frac{3}{2})\}$
  0 **si présence de substitution**

Exercice 3 /42

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.

- **1 pt : N est codée par** 13
- **1 pt :** $338 \equiv 8 \ [33]$
- **1 pt : on a bien** $0 \leqslant 8 \leqslant 33$
- **1 pt : N est codée par** 8

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

- **1 pt : O est codée par** 14
- **1 pt :** $378 \equiv 15$ [33]
- **1 pt : on a bien** $0 \leqslant 15 \leqslant 33$
- **1 pt : O est codée par** 15

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.

- **3 pts**

```
1  def Codage(x) :
2      y = (x * (x + 13)) % 33
3      return y
```

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].

- **1 pt :** $(x+23)^2 = x^2 + 46x + 529$
- **1 pt :** $46 \equiv 13$ [33]
- **1 pt :** $529 \equiv 1$ [33]
- **1 pt :** $(x+23)^2 \equiv 4$ [33] $\equiv$ $x(x+13) \equiv 3$ [33]
  0 si pas de raisonnement par équivalence

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.

- **1 pt : structure de démonstration d'une implication**
- **1 pt :** $(x+23)^2 \equiv 4$ [33] **donc il existe** $k \in \mathbb{Z}$ **tel que** $(x+23)^2 = 33k + 4$
- **1 pt :** $(x+23)^2 = 3k_1 + 4$ **où** $k_1 = 11k \in \mathbb{Z}$**, donc** $(x+23)^2 \equiv 4$ [3]
- **1 pt :** $(x+23)^2 = 11k_2 + 4$ **où** $k_2 = 3k \in \mathbb{Z}$ **donc** $(x+23)^2 \equiv 4$ [11]

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] $\Leftrightarrow$ $\begin{cases} (x+23)^2 \equiv 1 \ [3] \\ (x+23)^2 \equiv 4 \ [11] \end{cases}$

- **1 pt : avec qst précédente et ce qui est admis dans la question :** $(x+23)^2 \equiv 4$ [33] $\Leftrightarrow$ $\begin{cases} (x+23)^2 \equiv 4 \ [3] \\ (x+23)^2 \equiv 4 \ [11] \end{cases}$
- **1 pt :** $4 \equiv 1$ [3] **d'où la conclusion**

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

- **2 pts : Les entiers $a \in [\![0, 2]\!]$ vérifiant $a^2 \equiv 1\ [3]$ sont les entiers 1 et 2**

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

- **2 pts : détaillez précisément 2 cas non triviaux**
- **1 pt : tableau récapitulatif**

$b \equiv \cdots\ [11]$	0	1	2	3	4	5	6	7	8	9	10
$b^2 \equiv \cdots\cdots\ [11]$	0	1	4	9	5	3	3	5	9	4	1

- **1 pt : Les entiers $b \in [\![0, 10]\!]$ vérifiant $b^2 \equiv 4\ [11]$ sont les entiers 2 et 9**

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

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

- **1 pt : d'après *4.* et *5.b)* :** $x\,(x + 13) \equiv\ [33] \Leftrightarrow \begin{cases} (x + 23)^2 \equiv 1\ [3] \\ (x + 23)^2 \equiv 4\ [11] \end{cases}$
- **2 pts : d'après *6.a)* :** $(x + 23)^2 \equiv 1\ [3] \Leftrightarrow x \equiv 2\ [3]$ `OU` $x \equiv 0\ [3]$
- **2 pts : d'après *6.b)* :** $(x + 23)^2 \equiv 4\ [11] \Leftrightarrow x \equiv 1\ [3]$ `OU` $x \equiv 8\ [3]$

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.

- **4 pts : les solutions sont, dans l'ordre, 8, 12, 23 et 30 (1 pt par solution)**

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

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

- **4 pts**

```
for x in range(33) :
    if x * (x + 13) % 33 == 3 :
        print(x)
```

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 ?

- **2 pts (dont 1 pt pour dire que 30 n'est pas solution)**