DS2

Exercice 1 (Bac S 2019 (Asie))

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).

Démonstration.
On remarque :

$$\begin{aligned} & (-2)^3 + (-2\sqrt{3} + 2i)\,(-2i)^2 + (4 - 4i\sqrt{3})\,(-2i) + 8i \\ = \;& (-2)^3 i^3 + (-2\sqrt{3} + 2i)\,(-2)^2 i^2 - \cancel{8i} + 8i^2\sqrt{3} + \cancel{8i} \\ = \;& -8 \times (-i) - 4(-2\sqrt{3} + 2i) - 8\sqrt{3} \\ = \;& 8i + 8\sqrt{3} - 8i - 8\sqrt{3} \;=\; 0 \end{aligned}$$

Le nombre $-2i$ est donc solution de (E). □

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

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

Démonstration.
Soit $z \in \mathbb{C}$.

$$\begin{aligned} (z + 2i)\,(z^2 - 2\sqrt{3}\,z + 4) \;&=\; z^3 - 2\sqrt{3}\,z^2 + 4z + 2iz^2 - 4i\sqrt{3}\,z + 8i \\ &=\; z^3 + (-2\sqrt{3} + 2i)\,z^2 + (4 - 4i\sqrt{3})\,z + 8i \end{aligned}$$

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

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

Démonstration.
Soit $z \in \mathbb{C}$.

- Tout d'abord :

$$\begin{aligned} z \text{ solution de } (E) \;&\Leftrightarrow\; z^3 + (-2\sqrt{3} + 2i)\,z^2 + (4 - 4i\sqrt{3})\,z + 8i \\ &\Leftrightarrow\; (z + 2i)\left(z^2 - 2\sqrt{3}\,z + 4\right) \\ &\Leftrightarrow\; z + 2i = 0 \quad \texttt{OU} \quad z^2 - 2\sqrt{3}\,z + 4 = 0 \end{aligned}$$

- On note alors P le polynôme défini par : $P(X) = X^2 - 2\sqrt{3}\,X + 4$.
  On note Δ le discriminant de P. Alors :

$$\Delta \;=\; (-2\sqrt{3})^2 - 4 \times 1 \times 4 \;=\; 12 - 16 \;=\; -4$$

  On en déduit que P admet 2 racines complexes :
  × $z_1 = \dfrac{2\sqrt{3} + i\sqrt{-\Delta}}{2} = \dfrac{2\sqrt{3} + i\sqrt{4}}{2} = \dfrac{2\sqrt{3} + 2i}{2} = \dfrac{2(\sqrt{3}+1)}{2} = \sqrt{3} + i$
  × $z_2 = \dfrac{2\sqrt{3} - i\sqrt{-\Delta}}{2} = \dfrac{2\sqrt{3} - i\sqrt{4}}{2} = \dfrac{2\sqrt{3} - 2i}{2} = \dfrac{2(\sqrt{3}-1)}{2} = \sqrt{3} - i$
- On en conclut :

$$\begin{aligned} z \text{ solution de } (E) \quad &\Leftrightarrow \quad z + 2i = 0 \quad \texttt{OU} \quad z^2 - 2\sqrt{3}\,z + 4 = 0 \\ &\Leftrightarrow \quad z = -2i \quad \texttt{OU} \quad z = z_1 \quad \texttt{OU} \quad z = z_2 \\ &\Leftrightarrow \quad z = -2i \quad \texttt{OU} \quad z = \sqrt{3} + i \quad \texttt{OU} \quad z = \sqrt{3} - i \end{aligned}$$

Finalement, l'ensemble des solutions de (E) est : $\{-2i, \sqrt{3}+i, \sqrt{3}-i\}$. □

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 ?

Démonstration.
D'après l'énoncé :
- comme $z_A = -2i$, alors : $A = (\mathrm{Re}(z_A), \mathrm{Im}(z_A)) = (0, -2)$.
- comme $z_B = \sqrt{3} + i$, alors : $B = (\mathrm{Re}(z_B), \mathrm{Im}(z_B)) = (\sqrt{3}, 1)$.
- comme $z_C = \sqrt{3} - i$, alors : $C = (\mathrm{Re}(z_C), \mathrm{Im}(z_C)) = (\sqrt{3}, -1)$.

Ainsi : $A = (0, -2)$, $B = (\sqrt{3}, 1)$ et $C = (\sqrt{3}, -1)$. □

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.

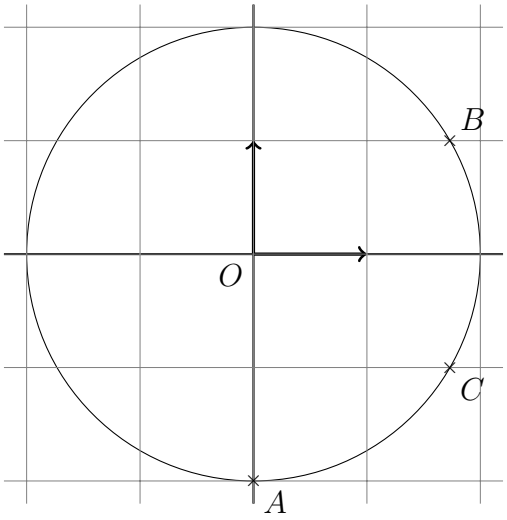
Démonstration.
D'après l'énoncé :
× $AO = \sqrt{(x_A - x_O)^2 + (y_A - y_O)^2} = \sqrt{(0-0)^2 + (2-0)^2} = \sqrt{4} = 2$
× $BO = \sqrt{(x_B - x_O)^2 + (y_B - y_O)^2} = \sqrt{(\sqrt{3}-0)^2 + (1-0)^2} = \sqrt{4} = 2$
× $CO = \sqrt{(x_C - x_O)^2 + (y_C - y_O)^2} = \sqrt{(\sqrt{3}-0)^2 + (-1-0)^2} = \sqrt{4} = 2$

On a donc : $AO = BO = CO = 2$.

On en déduit que les points 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.

Démonstration.



□

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

Démonstration.
Soit L un point du plan. On note : $L = (x_L, y_L)$

- Tout d'abord :

$$\begin{aligned} AODL \text{ parallélogramme} &\Leftrightarrow \overrightarrow{AL} = \overrightarrow{OD} \\ &\Leftrightarrow (x_L - x_A, y_L - y_A) = (x_D - x_O, y_D - y_O) \\ &\Leftrightarrow (x_L, y_L + 2) = (x_D, y_D) \end{aligned}$$

- Or, comme D est le milieu de $[OB]$:

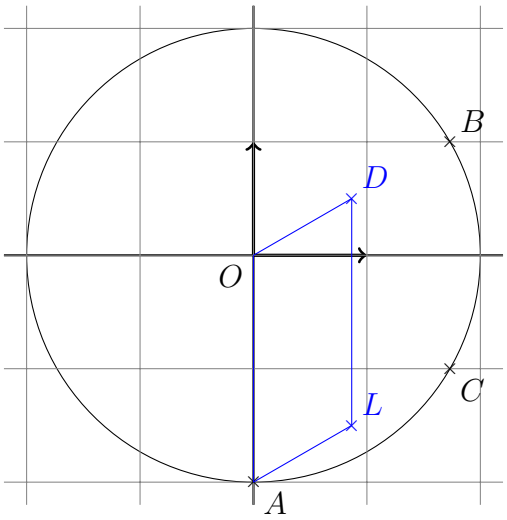
$$x_D = \frac{x_B - x_O}{2} = \frac{\sqrt{3}}{2} \quad \text{et} \quad y_D = \frac{y_B - y_O}{2} = \frac{1}{2}$$

- On en déduit :

$$\begin{aligned} AODL \text{ parallélogramme} &\Leftrightarrow (x_L, y_L + 2) = \left(\frac{\sqrt{3}}{2}, \frac{1}{2}\right) \\ &\Leftrightarrow \begin{cases} x_L &= \dfrac{\sqrt{3}}{2} \\ y_L + 2 &= \dfrac{1}{2} \end{cases} \\ &\Leftrightarrow \begin{cases} x_L &= \dfrac{\sqrt{3}}{2} \\ y_L &= -\dfrac{3}{2} \end{cases} \end{aligned}$$

L'affixe du point L tel que $AODL$ est un parallélogramme est : $z_L = \dfrac{\sqrt{3}}{2} - \dfrac{3}{2}\, i$.

On complète alors la figure :



□

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.

Démonstration.
On remarque :

$$\begin{aligned}
z\,\overline{z'} \in i\,\mathbb{R} &\Leftrightarrow z\,\overline{z'} = -\overline{z\,\overline{z'}} \\
&\Leftrightarrow z\,\overline{z'} = -\overline{z}\,z' \\
&\Leftrightarrow (x+iy)\,(x'-iy') = -(x-iy)\,(x'+iy') \\
&\Leftrightarrow x\,x' - \cancel{i\,x\,y'} + \cancel{i\,x'\,y} + y\,y' = -\left(x\,x' + \cancel{i\,x\,y'} - \cancel{i\,x'\,y} + y\,y'\right) \\
&\Leftrightarrow 2\,(x\,x' + y\,y') = 0 \\
&\Leftrightarrow x\,x' + y\,y' = 0 \\
&\Leftrightarrow \vec{u} \text{ et } \vec{v} \text{ orthogonaux}
\end{aligned}$$

Les vecteurs $\vec{u}$ et $\vec{v}$ sont donc orthogonaux si et seulement si : $z\,\overline{z'} \in i\,\mathbb{R}$.

□

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

Démonstration.

- On sait :

$$\begin{aligned}
AOL \text{ rectangle en } L &\Leftrightarrow \overrightarrow{AL} \text{ et } \overrightarrow{LO} \text{ orthogonaux} \\
&\Leftrightarrow z_{\overrightarrow{AL}}\,\overline{z_{\overrightarrow{LO}}} \in i\,\mathbb{R} \qquad \textit{(d'après ***3.a)***)}
\end{aligned}$$

- Calculons $z_{\overrightarrow{LO}}$:

$$\overrightarrow{LO} = (x_O - x_L, y_O - y_L) = \left(-\frac{\sqrt{3}}{2}, \frac{3}{2}\right)$$

D'où : $z_{\overrightarrow{OL}} = -\dfrac{\sqrt{3}}{2} + \dfrac{3}{2}\,i$.

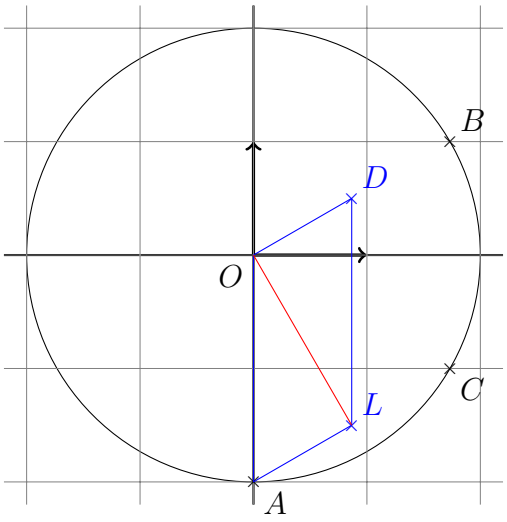
- On obtient :

$$\begin{aligned} z_{\overrightarrow{AL}}\,\overline{z_{\overrightarrow{LO}}} &= \left(\frac{\sqrt{3}}{2}+\frac{1}{2}\,i\right)\left(-\frac{\sqrt{3}}{2}-\frac{3}{2}\,i\right) \\ &= -\left(\frac{\sqrt{3}}{2}\right)^2-\frac{3\sqrt{3}}{4}\,i-\frac{\sqrt{3}}{4}\,i-\frac{3}{4}\,i^2 \\ &= -\frac{3}{4}-\frac{4\sqrt{3}}{4}\,i+\frac{3}{4} \;=\; -i\sqrt{3} \end{aligned}$$

On en déduit : $z_{\overrightarrow{AL}}\,\overline{z_{\overrightarrow{LO}}} = i\sqrt{3} \notin i\,\mathbb{R}$.

Ainsi, le triangle AOL est rectangle en L.

On complète alors la figure :



□

Exercice 2

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

Démonstration.
cf cours □

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.

Démonstration.
On calcule :

$$AX = \begin{pmatrix} 1 & 1 & 1 \\ 2 & 1 & 3 \\ 1 & 2 & 2 \end{pmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} x+y+z \\ 2x+y+3z \\ x+2y+2z \end{pmatrix}$$

$$\boxed{AX = \begin{pmatrix} x+y+z \\ 2x+y+3z \\ x+2y+2z \end{pmatrix}}$$

□

b) Démontrer l'équivalence suivante :

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

Démonstration.
On remarque :

$$AX = B \quad \Leftrightarrow \quad \begin{pmatrix} x+y+z \\ 2x+y+3z \\ x+2y+2z \end{pmatrix} = \begin{pmatrix} 2 \\ 1 \\ 2 \end{pmatrix} \qquad \textit{(d'après 2.a)}$$

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

$$\boxed{\text{Ainsi : } AX = B \Leftrightarrow \begin{cases} x + y + z = 2 \\ 2x + y + 3z = 1 \\ x + 2y + 2z = 2 \end{cases}.}$$

□

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

Démonstration.
Soit $(x, y, z) \in \mathbb{R}^3$.

$$AX = B \quad \Leftrightarrow \quad \begin{cases} x + y + z = 2 \\ 2x + y + 3z = 1 \\ x + 2y + 2z = 2 \end{cases} \qquad \textit{(d'après 2.b))}$$

$$\xLeftrightarrow[L_3 \leftarrow L_3 - L_1]{L_2 \leftarrow L_2 - 2L_1} \quad \begin{cases} x + y + z = 2 \\ -y + z = -3 \\ y + z = 0 \end{cases}$$

$$\xLeftrightarrow{L_3 \leftarrow L_3 + L_2} \quad \begin{cases} x + y + z = 2 \\ -y + z = -3 \\ 2z = -3 \end{cases}$$

$$\xLeftrightarrow[L_2 \leftarrow 2L_2 - L_3]{L_1 \leftarrow 2L_1 - L_3} \quad \begin{cases} 2x + 2y = 7 \\ -2y = -3 \\ z = 0 \end{cases}$$

$$\xLeftrightarrow{L_1 \leftarrow L_1 + L_2} \quad \begin{cases} 2x = 4 \\ -2y = -3 \\ 2z = -3 \end{cases}$$

$$\xLeftrightarrow[L_3 \leftarrow \frac{1}{2} L_3]{L_1 \leftarrow \frac{1}{2} L_1 \\ L_2 \leftarrow -\frac{1}{2} L_2} \quad \begin{cases} x = 2 \\ y = \frac{3}{2} \\ z = -\frac{3}{2} \end{cases}$$

L'ensemble $\mathcal{S}$ des solutions de l'équation $AX = B$ est donc $\mathcal{S} = \{(2, \frac{3}{2}, -\frac{3}{2})\}$.

□

Exercice 3 (Bac S 2018 (Pondichéry))

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.

Démonstration.

- D'après le tableau, la lettre « N » se chiffre par 13. On note alors : $x = 13$.
- D'après l'énoncé, on calcule ensuite y tel que :

$$y \equiv x\,(x + 13)\ [33] \qquad \text{et} \qquad 0 \leqslant y \leqslant 33$$

  × On remarque :

$$x\,(x + 13) \ = \ 13 \times 26 \ = \ 338$$

  Or : $338 = 33 \times 10 + 8$. D'où : $338 \equiv 8\ [33]$.

  × Ainsi, le nombre $y = 8$ vérifie :

$$y \equiv 338\ [33] \qquad \text{et} \qquad 0 \leqslant y \leqslant 33$$

La lettre « N » est donc codée par le nombre 8.

□

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

Démonstration.

- D'après le tableau, la lettre « O » se chiffre par : $x = 14$.
- On cherche ensuite y tel que :

$$y \equiv x\,(x + 13)\ [33] \qquad \text{et} \qquad 0 \leqslant y \leqslant 33$$

Ici : $x\,(x + 13) = 14 \times 27 = 378$. Or : $378 = 33 \times 11 + 15$. Donc : $378 \equiv 15\ [33]$.
De plus : $0 \leqslant 15 \leqslant 33$. D'où $y = 15$.

La lettre « O » est donc codée par le nombre 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.

Démonstration.
On propose la fonction suivante :

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

Détaillons les éléments de ce script.

- **Début de la fonction**
  On commence par préciser la structure de la fonction :
  - × cette fonction se nomme `Codage`,
  - × elle prend en entrée un paramètre `x`,
  - × elle admet pour variable de sortie la variable `y`.

```
1  def Codage(x) :
```

```
3      return y
```

- **Contenu de la fonction**
  La ligne 2 consiste à coder le nombre `x` à l'aide du chiffrement de RABIN. On cherche donc à obtenir le reste de la division euclidienne de $x(x+13)$ par 33.

```
2      y = (x * (x + 13)) % 33
```

□

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 :

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

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

Démonstration.

- On commence par remarquer :

$$(x+23)^2 \ = \ x^2 + 46x + 529$$

De plus :

× $46 \equiv 13 \ [33]$ (car $46 = 33 \times 1 + 13$)

× $529 \equiv 1 \ [33]$ (car $529 = 33 \times 16 + 1$)

- On en déduit :

$$\begin{aligned}(x+23)^2 \equiv 4\ [33] &\Leftrightarrow x^2+46x+529 \equiv 4\ [33]\\ &\Leftrightarrow x^2+13x+1 \equiv 4\ [33]\\ &\Leftrightarrow x^2+13x \equiv 3\ [33]\\ &\Leftrightarrow x\,(x+13) \equiv 3\ [33]\end{aligned}$$

$$\boxed{x\,(x+13) \equiv 3\ [33] \Leftrightarrow (x+23)^2 \equiv 4\ [33]}$$

□

5. 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.

Démonstration.
Supposons : $(x+23)^2 \equiv 4\ [33]$.
Alors il existe $k \in \mathbb{Z}$ tel que : $(x+23)^2 = 33k+4$. On en déduit :

- d'une part : $(x+23)^2 = 3\times 11k+4$.
  Ainsi, en posant $k_1 = 11k \in \mathbb{Z}$, on obtient : $(x+23)^2 = 3k_1+4$. D'où :

$$(x+23)^2 \equiv 4\ [3]$$

- d'autre part : $(x+23)^2 = 11\times 3k+4$.
  Ainsi, en posant $k_2 = 3k \in \mathbb{Z}$, on obtient : $(x+23)^2 = 11k_2+4$. D'où :

$$(x+23)^2 \equiv 4\ [11]$$

$$\boxed{\text{Finalement, si } (x+23)^2 \equiv 4\ [33], \text{ alors } \begin{cases}(x+23)^2 \equiv 4\ [3]\\ (x+23)^2 \equiv 4\ [11]\end{cases}.}$$

□

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

Démonstration.

- D'après la question précédente et ce qui est admis dans cette question, on a :

$$(x+23)^2 \equiv 4\ [33] \quad\Leftrightarrow\quad \begin{cases}(x+23)^2 \equiv 4\ [3]\\ (x+23)^2 \equiv 4\ [11]\end{cases}$$

- Or : $4 \equiv 1\ [3]$ (car $4 = 3\times 1+1$). D'où :

$$(x+23)^2 \equiv 4\ [3] \quad\Leftrightarrow\quad (x+23)^2 \equiv 1\ [3]$$

$$\boxed{\text{On en déduit : } (x+23)^2 \equiv 4\ [33] \Leftrightarrow \begin{cases}(x+23)^2 \equiv 1\ [3]\\ (x+23)^2 \equiv 4\ [11]\end{cases}}$$

□

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

Démonstration.
Soit $a \in [\![0, 2]\!]$. Trois cas se présentent.
- si $a = 0$, alors : $a^2 = 0$. D'où : $a^2 \equiv 0\ [3]$.
- si $a = 1$, alors : $a^2 = 1$. D'où : $a^2 \equiv 1\ [3]$.
- si $a = 2$, alors : $a^2 = 4$. 0r : $4 \equiv 1\ [3]$. D'où : $a^2 \equiv 1\ [3]$.

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 : $b^2 \equiv 4\ [11]$.

Démonstration.
Soit $b \in [\![0, 10]\!]$. Onze cas se présentent. On en détaille 2 et on les résume tous dans un tableau.
- si $b = 4$, alors : $b^2 = 16$. Or : $16 \equiv 5\ [11]$. D'où : $b^2 \equiv 5\ [11]$.
- si $b = 9$, alors : $b^2 = 81$. 0r : $81 \equiv 4\ [11]$. D'où : $b^2 \equiv 4\ [11]$.

On obtient finalement le tableau suivant :

$b \equiv \cdots\ [11]$	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

Les entiers $b \in [\![0, 10]\!]$ vérifiant $b^2 \equiv 4\ [11]$ sont les entiers 2 et 9.

□

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

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

Démonstration.
- Tout d'abord :

$$\begin{aligned} x\,(x+13) \equiv\ [33] &\Leftrightarrow (x+23)^2 \equiv 4\ [33] && \textit{(d'après 4.)} \\ &\Leftrightarrow \begin{cases} (x+23)^2 \equiv 1\ [3] \\ (x+23)^2 \equiv 4\ [11] \end{cases} && \textit{(d'après 5.b))} \end{aligned}$$

- Or :
  × d'après ***6.a)*** :

$$\begin{aligned} (x+23)^2 \equiv 1\ [3] &\Leftrightarrow x+23 \equiv 1\ [3] \quad \texttt{OU} \quad x+23 \equiv 2\ [3] \\ &\Leftrightarrow x \equiv -22\ [3] \quad \texttt{OU} \quad x \equiv -21\ [3] \\ &\Leftrightarrow x \equiv 2\ [3] \quad \texttt{OU} \quad x \equiv 0\ [3] && \textit{(car } -22 = 3 \times (-8) + 2 \equiv 2\ [3] \\ & && \textit{et } -21 = 3 \times 7 + 0 \equiv 0\ [3]\textit{)} \end{aligned}$$

× d'après ***6.b)*** :

$$\begin{aligned}(x+23)^2 \equiv 4\ [11] &\Leftrightarrow x+23 \equiv 2\ [11] \quad \text{OU} \quad x+23 \equiv 9\ [11]\\ &\Leftrightarrow x \equiv -21\ [11] \quad \text{OU} \quad x \equiv -14\ [11]\\ &\Leftrightarrow x \equiv 1\ [3] \quad \text{OU} \quad x \equiv 8\ [3]\end{aligned}$$

(car $-21 = 11 \times (-2) + 1 \equiv 1\ [11]$ *et* $-14 = 11 \times (-2) + 8 \equiv 8\ [11]$*)*

On obtient bien que $(x\,(x+13) \equiv 3\ [33]$ est équivalent à

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

□

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.

Démonstration.

- On remarque que l'entier 8 est solution du système $\begin{cases} x \equiv 2\ [3] \\ x \equiv 8\ [11] \end{cases}$ et vérifie : $0 \leqslant 8 < 33$.
- On remarque que l'entier 12 est solution du système $\begin{cases} x \equiv 0\ [3] \\ x \equiv 1\ [11] \end{cases}$ et vérifie : $0 \leqslant 12 < 33$.
- On remarque que l'entier 23 est solution du système $\begin{cases} x \equiv 2\ [3] \\ x \equiv 1\ [11] \end{cases}$ et vérifie : $0 \leqslant 23 < 33$.
- On remarque que l'entier 30 est solution du système $\begin{cases} x \equiv 0\ [3] \\ x \equiv 8\ [11] \end{cases}$ et vérifie : $0 \leqslant 30 < 33$.

□

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

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

Démonstration.
On propose le script suivant :

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

Détaillons les éléments de ce script.

- **Structure itérative**
  Les lignes 1 à 2 consistent à tester, pour chaque entier `x` compris entre 0 et 32, si cet entier vérifie la condition du chiffrement de RABIN : $\texttt{x}(\texttt{x}+13) \equiv 3\ [33]$. Pour cela on utilise une structure itérative (boucle *for*) :

```
1  for x in range(33) :
```

On teste ensuite pour cet entier `x` si le reste de la division euclidienne de $x(x+13)$ par 33 est égal à 3 :

```
2        if x * (x + 13) % 33 == 3 :
```

- **Fin du programme**
  Enfin, si l'entier `x` vérifie bien la relation du chiffrement de RABIN, on souhaite afficher cette valeur.

```
3            print(x)
```

□

9. 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 ?

Démonstration.

D'après la question ***7.b)***, le chiffre 3 peut être le chiffrement de 8, 12, 23 ou 30. Autrement dit, le chiffre 3 peut être le codage des lettres « I », « M » ou « X » (le nombre 30 ne correspond à aucune lettre car il n'est pas compris entre 0 et 25). Alice ne peut donc pas connaître la première lettre du message envoyé par Bob.
Le « chiffre de RABIN » n'est donc pas utilisable pour décoder un message lettre par lettre. □