Exercice : L'anneau $\mathbb{Z}[j]$

1. (a) On sait que 1, j et j^2 sont les trois racines cubiques de l'unité. Or dès que $n \geq 2$, la somme des racines n-ièmes de l'unité vaut 0.

$$\boxed{1 + j + j^2 = 0}$$

On a :

$$j = e^{\frac{2i\pi}{3}} = \cos\left(\frac{2\pi}{3}\right) + i\sin\left(\frac{2\pi}{3}\right) = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$$

$$\boxed{j = -\frac{1}{2} + i\frac{\sqrt{3}}{2}}$$

(b) L'existence d'une telle écriture est donnée par la définition de $\mathbb{Z}[j]$, il reste à démontrer l'unicité. On suppose que :

$$z = a + bj = c + dj \text{ avec } (a, b, c, d) \in \mathbb{Z}^4$$

En utilisant l'écriture algébrique de j donnée dans la question précédente, il vient :

$$a - \frac{1}{2}b + \frac{\sqrt{3}}{2}ib = c - \frac{1}{2}d + \frac{\sqrt{3}}{2}id$$

On identifie les parties imaginaires pour obtenir : $b = d$ puis on identifie les parties réelles pour avoir $a = c$. Ce qui démontre l'unicité de l'écriture.

$$\boxed{\text{L'écriture d'un élément de } \mathbb{Z}[j] \text{ est unique}}$$

2. Nous allons démontrer que $(\mathbb{Z}[j], +, \times)$ est un anneau en démontrant plutôt que c'est un sous-anneau de $(\mathbb{C}, +, \times)$. Vérifions les différentes conditions requises.

- Déjà $\mathbb{Z}[j] \subset \mathbb{C}$.
- $0 \in \mathbb{Z}[j]$ car $0 = 0 + 0i$.
- Soient $z = a + bj$ et $z' = c + dj$ avec $(a, b, c, d) \in \mathbb{Z}^4$. On a :

$$z + z' = a + bj + c + dj = \underbrace{(a + c)}_{\in\mathbb{Z}} + \underbrace{(b + d)}_{\in\mathbb{Z}}j$$

donc $z + z' \in \mathbb{Z}[j]$.

- Soit $z = a + bj$ avec $(a, b) \in \mathbb{Z}^2$, on a :

$$-z = -(a + bj) = \underbrace{-a}_{\in\mathbb{Z}} + \underbrace{(-b)}_{\in\mathbb{Z}}j$$

donc $-z \in \mathbb{Z}[j]$.

- $1 = 1 + 0j \in \mathbb{Z}[j]$.
- Soient $z = a + bj$ et $z' = c + dj$ avec $(a, b, c, d) \in \mathbb{Z}^4$. En utilisant la relation $1 + j + j^2 = 0$, c'est-à-dire $j^2 = -j - 1$, on a :

$$z \times z' = (a + bj) \times (c + dj) = ac + (ad + bc)j + bdj^2 = ac + (ad + bc)j + bd(-1 - j) = \underbrace{ac - bd}_{\in\mathbb{Z}} + \underbrace{(ad + bc - bd)}_{\in\mathbb{Z}}j$$

donc $z \times z' \in \mathbb{Z}[j]$.

Enfin la mutiplication des nombres complexes est évidemment commutative, on en déduit que :

$$\boxed{(\mathbb{Z}[j], +, \times) \text{ est un anneau commutatif en tant que sous-anneau de } (\mathbb{C}, +, \times)}$$

3. (a) Soit $z = a + bj$ avec $(a, b) \in \mathbb{Z}^2$. On a :

$$N(z) = |z|^2 = z\bar{z} = (a + bj)(a + b\bar{j}) = a^2 + 2ab(j + \bar{j}) + b^2 j\bar{j} = a^2 - ab + b^2 \in \mathbb{Z}$$

car $j + \bar{j} = j + j^2 = -1$ et $j\bar{j} = j \times j^2 = j^3 = 1$. Or le module d'un nombre complexe est un nombre positif donc :

$$\boxed{N(z) \in \mathbb{N}}$$

(b) On procède par double implication.

($\Rightarrow$) On suppose que z est un inversible de $\mathbb{Z}[j]$, cela signifie qu'il existe $z' \in \mathbb{Z}[j]$ tel que $zz' = 1$. On note $z = a + bj$ et $z' = c + dj$ avec $(a, b, c, d) \in \mathbb{Z}^4$, on a :

$$N(zz') = |zz'|^2 = |z|^2|z'|^2 = N(z)N(z')$$

Ainsi $N(z)N(z') = N(zz') = N(1) = |1|^2 = 1$. Or $N(z)$ et $N(z')$ sont deux entiers naturels d'après la question précédente donc $N(z) = 1$.

($\Leftarrow$) Réciproquement, on suppose que $N(z) = 1$, on a :

$$N(z) = |z^2| = z\bar{z} = (a + bj)(a + b\bar{j}) = (a + bj)(a + bj^2) = (a + bj)(a - b - bj) = 1$$

Ainsi z est inversible et son inverse est $\underbrace{a - b}_{\in\mathbb{Z}} + \underbrace{(-b)}_{\in\mathbb{Z}} j$.

$$\boxed{z \text{ est inversible si et seulement si } N(z) = 1}$$

(c) D'après la question (b), chercher les inversibles de $\mathbb{Z}[j]$ revient à déterminer les éléments de module 1. Soit $z = a + bj$ avec $(a, b) \in \mathbb{Z}^2$. En utilisant le calcul de la question (a), on a :

$$N(z) = 1 \Leftrightarrow a^2 - ab + b^2 = 1 \Leftrightarrow a^2 - ab + b^2 - 1 = 0$$

On fixe $b \in \mathbb{Z}$, on obtient alors une équation de degré 2 en a. Le discriminant vaut $\Delta = b^2 - 4(b^2 - 1) = 4 - 3b^2$. Plusieurs cas sont à considérer :

- Si $|b| \geq 2$, l'équation n'a pas de solution réelle car le discriminant est négatif.
- Si $|b| = 1$ alors si $b = 1$ l'équation a pour solution $a = 0$ et $a = 1$ et si $b = -1$ l'équation a pour solution $a = -1$ et $a = 0$. Ce qui nous donne les inversibles : j, $-j$, $-1 - j$ et $1 + j$.
- Si $|b| = 0$, c'est-à-dire $b = 0$, on a : $a = 1$ et $a = -1$. Ce qui nous donne les inversibles 1 et -1.

$$\boxed{\mathbb{Z}[j]^\times = \{1, -1, j, -j, 1 + j, -1 - j\}}$$

Donnons les inverses :

$$1 \times 1 = 1$$
$$(-1) \times (-1) = 1$$
$$j \times (-1 - j) = j \times j^2 = j^3 = 1$$
$$-j \times (1 + j) = 1$$

(d) L'anneau $\mathbb{Z}[j]$ n'est pas un corps car tous les éléments non nuls ne sont pas inversibles comme nous l'avons vu dans la question précédente.

Exercice 2 : Triplets pythagoriciens

1. Soit $d \in \mathbb{N}^*$ un diviseur commun de x, y et z, il existe $(X, Y, Z) \in (\mathbb{N}^*)^3$ tels que $x = dX$, $y = dY$ et $z = dZ$. On a :
$$x^2 + y^2 = z^2 \Leftrightarrow (dX)^2 + (dY)^2 = (dZ)^2 \Leftrightarrow X^2 + Y^2 = Z^2$$
Il suffit de chercher les solutions sans diviseur commun, on obtiendra toutes les solutions en multipliant par un entier quelconque les trois coordonnées du triplet.

2. Soit $d \in \mathbb{N}^*$ un **nombre premier** tel que $d|x$ et $d|y$ alors $d|x^2 + y^2 = z^2$. Comme d divise z^2 alors d apparait dans la décomposition en facteurs premiers de z^2 donc il apparait dans la décomposition en facteurs premiers de z. En effet, les facteurs premiers de z et z^2 sont les mêmes, seules les valuations changent, ceci étant dû à l'unicité de la décomposition en facteurs premiers. Finalement d divise z. D'après l'hypothèse, un diviseur positif de x, y et z est égal à 1. On vient de démontrer que x et y n'ont pas de facteur premier en commun, d'après le cours cela implique qu'ils sont premiers entre eux.
On démontre de la même façon que $x \wedge z = y \wedge z = 1$.
$$\boxed{x \wedge y = x \wedge z = y \wedge z = 1}$$
Il est alors clair que x et y ne sont pas tous les deux pairs sinon ils auraient 2 comme facteur commun, ce qui est contradictoire avec le résultat précédent.

3. Par l'absurde, si x et y sont impairs alors il existe $(k, l) \in \mathbb{N}^2$ tels que $x = 2k + 1$ et $y = 2l + 1$. On a $x^2 = 4k^2 + 4k + 1$ et $y^2 = 4l^2 + 4l + 1$, ainsi $x^2 \equiv 1[4]$ et $y^2 \equiv 1[4]$ donc $z^2 \equiv 2[4]$. C'est absurde car on vérifie immédiatement avec une table de congruence qu'un carré est congru à 0 ou 1 modulo 4.
$$\boxed{x \text{ et } y \text{ sont de parités distinctes}}$$

4. L'entier naturel x est pair et y est impair donc x^2 est pair et y^2 est impair, ce qui implique que z^2 est impair et par suite z est impair. On en déduit que $z + y$ et $z - y$ sont impairs. D'autre part, étant donné que x, y et z sont non nuls, on a : $x \geq 1$, $z + y \geq 1$ et $z - y \geq 1$ car $z^2 = y^2 + x^2 \geq y^2 + 1$. Finalement :
$$\boxed{\exists (u, v, w) \in (\mathbb{N}^*)^3,\ x = 2u,\ z + y = 2v \text{ et } z - y = 2w}$$

5. Soit $d \in \mathbb{N}^*$ tel que $d|v$ et $d|w$ alors $d|v + w = z$ et $d|v - w = y$. Or $y \wedge z = 1$ donc $d = 1$.
$$\boxed{v \wedge w = 1}$$

6. On a $4vw = (z + y)(z - y) = z^2 - y^2 = x^2 = 4u^2$.
$$\boxed{vw = u^2}$$
On reprend l'égalité précédente en utilisant la décomposition en facteurs premiers :
$$vw = \Big(\prod_{p \in \mathcal{P}} p^{\nu_p(u)} \Big)^2$$
Soit $p \in \mathcal{P}$ un nombre premier qui apparait dans la décomposition précédente alors $p|vw$. Comme v et w sont premiers entre eux alors p divise v et p ne divise pas w ou p ne divise pas v et p divise w. Dans la décomposition précédente en regroupant les facteurs premiers selon qu'ils divisent v ou w, on obtient :
$$v = \Big(\prod_{p \in \mathcal{P},\ p|v} p^{\nu_p(u)} \Big)^2 \text{ et } w = \Big(\prod_{p \in \mathcal{P},\ p|w} p^{\nu_p(u)} \Big)^2$$
$$\boxed{\exists (n, m) \in \mathbb{N}^2,\ v = n^2 \text{ et } w = m^2}$$

7. On a $2v - 2w = 2y > 0$ donc $v > w$ d'où $n^2 > m^2$ et par suite :

$$\boxed{n > m}$$

Si $d \in \mathbb{N}^*$ avec $d|n$ et $d|m$ alors $d|n^2 = v$ et $d|m^2 = w$, or $v \wedge w = 1$ d'où $d = 1$.

$$\boxed{n \wedge m = 1}$$

On a vu que $vw = u^2$ donc $n^2m^2 = u^2$ donc $u = nm$ puisque l'on travaille avec des entiers naturels.

$$\boxed{u = nm}$$

8. On vient de démontrer que les conditions données dans cette question sont des conditions nécessaires, l'autre triplet étant obtenu en supposant x impair et y pair. En effet, $x = 2u = 2nm$, $y = v - w = n^2 - m^2$ et $z = w + v = n^2 + m^2$ et m et n sont bien de parités distinctes car y est impair.
Réciproquement, on a bien :

$$x^2 + y^2 = (2nm)^2 + (n^2 - m^2)^2 = 4n^2m^2 + n^4 - 2n^2m^2 + m^4 = (n^2 + m^2)^2 = z^2$$

et (x, y, z) est un triplet Pythagoricien car si d est un nombre premier tel que $d|x$, $d|y$ et $d|z$ alors $d|2n^2 = y + z$ et $d|2m^2 = z - y$. Or d n'est pas pair car y (ou x) est impair puisque n et m sont de parités distinctes. Ainsi $d|m^2$ et $d|n^2$ donc $d|m$ et $d|n$, comme m et n sont premiers entre eux cela implique que $d = 1$. On a bien un triplet Pythagoricien primitif.

Problème : Une équation fonctionnelle

Partie A : Généralités sur les fonctions de $\mathcal{E}$

1. Soit f une fonction constante de $\mathbb{R}$ dans $\mathbb{R}$, il existe $a \in \mathbb{R}$ tel que pour tout $x \in \mathbb{R}$, $f(x) = a$, on a :

$$f \in \mathcal{E} \Leftrightarrow \forall (x, y) \in \mathbb{R}^2,\ f(x) + f(y) = 2f\Big(\frac{x+y}{2}\Big)f\Big(\frac{x-y}{2}\Big) \Leftrightarrow 2a = 2a^2 \Leftrightarrow 2a(a-1) = 0 \Leftrightarrow a \in \{0, 1\}$$

$$\boxed{\mathcal{E} \text{ contient deux fonctions constantes, la fonction constante égale à 0 et la fonction constante égale à 1}}$$

2. La fonction constante égale à 1 appartient à $\mathcal{E}$ mais son opposé, la fonction constante égale à -1, ne vérifie clairement pas la relation $(\mathcal{R})$.

$$\boxed{\mathcal{E} \text{ n'est pas un sous-groupe additif de } \mathcal{F}(\mathbb{R}, \mathbb{R})}$$

3. Démontrons cela par double implication. Soit f une fonction de $\mathbb{R}$ dans $\mathbb{R}$.
($\Rightarrow$) On suppose que f vérifie (S) et on se donne $(x, y) \in \mathbb{R}^2$. En appliquant (S) avec $u = \dfrac{x+y}{2}$ et $v = \dfrac{x-y}{2}$, on a :

$$f(u+v) + f(u-v) = 2f(u)f(v) \Leftrightarrow f(x) + f(y) = 2f\Big(\frac{x+y}{2}\Big)f\Big(\frac{x-y}{2}\Big)$$

Ce qui démontre que f vérifie $(\mathcal{R})$.
($\Leftarrow$) Réciproquement, on suppose que f vérifie $(\mathcal{R})$ et on se donne $(u, v) \in \mathbb{R}^2$. En appliquant $(\mathcal{R})$ à $x = u + v$ et $y = u - v$, on a :

$$f(x) + f(y) = 2f\Big(\frac{x+y}{2}\Big)f\Big(\frac{x-y}{2}\Big) \Leftrightarrow f(u+v) + f(u-v) = 2f(u)f(v)$$

Ce qui démontre que f vérifie (S).

$$\boxed{f \text{ vérifie } (\mathcal{S}) \text{ si et seulement si } f \text{ vérifie } (\mathcal{R})}$$

4. (a) Soit $x \in \mathbb{R}$, appliquons $(\mathcal{R})$ au couple (x, x), cela donne :

$$2f(x) = 2f(x)f(0) \qquad (\bigstar)$$

Si $f(0) = 0$ alors pour tout $x \in \mathbb{R}$, $f(x) = 0$ d'après la relation ci-dessus. Ceci est exclu puisque, d'après l'hypothèse de l'énoncé, f n'est pas la fonction nulle. Ainsi :

$$\boxed{f(0) \neq 0}$$

On utilise ensuite $(\bigstar)$ avec $x = 0$, cela donne $2f(0) = 2f(0)^2$. Comme $f(0) \neq 0$ alors $f(0) = 1$.

$$\boxed{f(0) = 1}$$

(b) Soit $x \in \mathbb{R}$, on applique la relation $(\mathcal{S})$ au couple $(0, x)$, cela donne :

$$f(x) + f(-x) = 2f(0)f(x) \Leftrightarrow f(x) + f(-x) = 2f(x) \qquad \text{puisque } f(0) = 1$$

Ce qui démontre que pour tout $x \in \mathbb{R}$, $f(-x) = f(x)$.

$$\boxed{f \text{ est paire}}$$

(c) Soit $x \in \mathbb{R}$, on applique la relation $(\mathcal{R})$ au couple $(x, 0)$, cela donne :

$$f(x) + f(0) = 2f\Big(\frac{x}{2}\Big)^2 \Leftrightarrow f(x) = 2f\Big(\frac{x}{2}\Big)^2 - 1$$

Ce qui démontre que :

$$\boxed{\forall x \in \mathbb{R},\ f(x) \geq -1}$$

5. Soit λ un réel. Les fonctions $x \mapsto \mathrm{ch}(\lambda x)$ et $x \mapsto \cos(\lambda x)$ sont bien continues sur $\mathbb{R}$. D'après les relations rappelées en préambule et en utilisant la parité de ch et l'imparité de sh, on a :

$$\forall (x, y) \in \mathbb{R}^2,\ \mathrm{ch}(\lambda x + \lambda y) = \mathrm{ch}(\lambda x)\,\mathrm{ch}(\lambda y) + \mathrm{sh}(\lambda x)\,\mathrm{sh}(\lambda y)$$

$$\forall (x, y) \in \mathbb{R}^2,\ \mathrm{ch}(\lambda x - \lambda y) = \mathrm{ch}(\lambda x)\,\mathrm{ch}(\lambda y) - \mathrm{sh}(\lambda x)\,\mathrm{sh}(\lambda y)$$

En sommant ces relations on obtient :

$$\forall (x, y) \in \mathbb{R}^2,\ \mathrm{ch}(\lambda(x + y)) + \mathrm{ch}(\lambda(x - y)) = 2\,\mathrm{ch}(\lambda x)\,\mathrm{ch}(\lambda y)$$

Ce qui démontre que la fonction $x \mapsto \mathrm{ch}(\lambda x)$ vérifie $(\mathcal{S})$ et par suite elle appartient à $\mathcal{C}$.
De même pour la fonction $x \mapsto \cos(\lambda x)$ qui vérifie aussi $(\mathcal{S})$ puisque :

$$\forall (x, y) \in \mathbb{R}^2,\ \cos(\lambda(x + y)) + \cos(\lambda(x - y)) = 2\cos(\lambda x)\cos(\lambda y)$$

$$\boxed{x \mapsto \mathrm{ch}(\lambda x) \text{ et } x \mapsto \cos(\lambda x) \text{ appartiennent à } \mathcal{C}}$$

6. (a) On fixe $u \in \mathbb{R}$. Les fonctions $v \mapsto u + v$, $v \mapsto u - v$ et f sont dérivables deux fois sur $\mathbb{R}$; par composition, somme et produit, F est dérivable deux fois sur $\mathbb{R}$. Pour tout v réel, on a :

$$F'(v) = f'(u + v) - f'(u - v) - 2f(u)f'(v)$$

$$\boxed{F''(v) = f''(u + v) + f''(u - v) - 2f(u)f''(v)}$$

(b) Comme $f \in \mathcal{E}$, f vérifie $(\mathcal{S})$ ainsi F est la fonction nulle et F'' est également la fonction nulle. C'est-à-dire que pour tous $(u,v) \in \mathbb{R}^2$:

$$f''(u+v) + f''(u-v) = 2f(u)f''(v)$$

En particulier pour $v = 0$, cela donne pour tout $u \in \mathbb{R}$: $f''(u) = f''(0)f(u)$. On a le résultat voulu avec :

$$\boxed{k = f''(0)}$$

(c) Comme f appartient à $\mathcal{E}$, on a vu à la question 4.(a) que $f(0) = 1$ d'où la première condition. De plus, on sait que f est une fonction paire, ainsi f' est impaire et $f'(0) = 0$. Grâce à la question précédente, on en déduit que f est solution de :

$$\begin{cases} y'' = ky \\ y(0) = 1, \quad y'(0) = 0 \end{cases}$$

(d) Raisonnons selon le signe de k :

► Si $k = 0$, les solutions de l'équation différentielle précédente sont les fonctions définies sur $\mathbb{R}$ par $y : x \mapsto Ax + B$ où $(A,B) \in \mathbb{R}^2$. Les conditions initiales imposent $A = 0$ et $B = 1$. On trouve comme solution la fonction constante égale à 1. On remarque que l'on a bien $y''(0) = 0 = k$.

► Si $k > 0$. L'équation caractéristique s'écrit $x^2 - k = 0$ qui possède deux solutions réelles : $\sqrt{k}$ et $-\sqrt{k}$. Les solutions de l'équation différentielle précédente sont les fonctions définies sur $\mathbb{R}$ par $y : x \mapsto Ae^{\sqrt{k}x} + Be^{-\sqrt{k}x}$ où $(A,B) \in \mathbb{R}^2$. Tenons compte des conditions initiales :

$$\begin{cases} y(0) = 1 \\ y'(0) = 0 \end{cases} \Leftrightarrow \begin{cases} A + B = 1 \\ A\sqrt{k} - B\sqrt{k} = 0 \end{cases} \Leftrightarrow \begin{cases} B = 1 - A \\ A\sqrt{k} + (A-1)\sqrt{k} = 0 \end{cases} \Leftrightarrow \begin{cases} B = \dfrac{1}{2} \\ A = \dfrac{1}{2} \end{cases}$$

Ainsi les solutions de l'équation différentielle précédente sont les fonctions $y : x \mapsto \mathrm{ch}(\sqrt{k}x)$. On a bien $y''(0) = k$.

► Si $k < 0$. L'équation caractéristique s'écrit $x^2 - k = 0$ qui possède deux solutions complexes : $i\sqrt{-k}$ et $-i\sqrt{-k}$. Les solutions de l'équation différentielle précédente sont les fonctions définies sur $\mathbb{R}$ par $y : x \mapsto A\cos(\sqrt{-k}x) + B\sin(-\sqrt{-k}x)$ où $(A,B) \in \mathbb{R}^2$. Tenons compte des conditions initiales :

$$\begin{cases} y(0) = 1 \\ y'(0) = 0 \end{cases} \Leftrightarrow \begin{cases} A = 1 \\ -B\sqrt{-k} = 0 \end{cases} \Leftrightarrow \begin{cases} A = 1 \\ B = 0 \end{cases}$$

Ainsi les solutions de l'équation différentielle précédente sont les fonctions $y : x \mapsto \cos(\sqrt{-k}x)$. On a bien $y''(0) = k$.

Réciproquement les fonctions $x \mapsto \mathrm{ch}(\lambda x)$ et $x \mapsto \cos(\lambda x)$ appartiennent à $\mathcal{E}$ pour tout $\lambda \in \mathbb{R}$, d'après la question 5. Les fonctions dérivables deux fois et appartenant à $\mathcal{E}$ sont les fonctions définies sur $\mathbb{R}$ par :

$$\boxed{x \mapsto 0,\ x \mapsto \mathrm{ch}(\lambda x),\ x \mapsto \cos(\lambda x) \text{ où } \lambda \in \mathbb{R}}$$

On n'a pas oublié d'ajouter la fonction nulle qui est bien dérivable deux fois et qui appartient à $\mathcal{E}$.

La suite du problème va permettre de démontrer que les fonctions trouvées sont exactement les éléments de l'ensemble $\mathcal{C}$.

Partie B : Etude de l'ensemble $\mathcal{C}$

1. (a) Soit $k \in \mathbb{N}^*$, on applique la relation $(\mathcal{S})$ au couple (ka, a) cela donne :

$$f(ka+a) + f(ka-a) = 2f(ka)f(a) \Leftrightarrow u_{k+1} + u_{k-1} = 2u_k u_1$$

$$\boxed{\forall k \in \mathbb{N}^*,\ u_{k+1} + u_{k-1} = 2u_1 u_k}$$

(b) On peut choisir $\alpha = \text{Arccos}(u_1)$ puisque $u_1 \in [-1, 1]$, ainsi $\cos(\alpha) = \cos(\text{Arccos}(u_1)) = u_1$.
Démontrons-le par récurrence double, pour $k \geq 0$ on considère l'hypothèse :

$$\mathcal{H}_k \ :\ u_k = \cos(k\alpha)$$

▶ Pour $k = 0$, on a $u_0 = f(0) = 1$ d'après la question 4.(a) de la partie A. Ce qui démontre que $u_0 = \cos(0 \times \alpha)$ et par suite $\mathcal{H}_0$ est vraie.
▶ Pour $k = 1$, on a $u_1 = \cos(\alpha)$ par définition de α, $\mathcal{H}_1$ est vraie.
▶ Fixons $k \in \mathbb{N}$, on suppose que $\mathcal{H}_k$ et $\mathcal{H}_{k+1}$ sont vraies. D'après la relation démontrée à la question 1.(a), on a :

$$u_{k+2} + u_k = 2u_1 u_{k+1} \Leftrightarrow u_{k+2} = 2\cos(\alpha)\cos((k+1)\alpha) - \cos(k\alpha)$$

Or pour tous $(b, c) \in \mathbb{R}^2$, on a : $\cos(b+c) + \cos(b-c) = 2\cos(b)\cos(c)$, si l'on applique cette formule avec $b = (k+1)\alpha$ et $c = \alpha$ cela donne :

$$\cos((k+2)\alpha) + \cos(k\alpha) = 2\cos((k+1)\alpha)\cos(\alpha) \Leftrightarrow \cos((k+2)\alpha) = 2\cos((k+1)\alpha)\cos(\alpha) - \cos(k\alpha)$$

Ce qui démontre que $u_{k+2} = \cos((k+2)\alpha)$ et par suite $\mathcal{H}_{k+2}$ est vraie. Ce qui achève la récurrence.

$$\boxed{\forall k \in \mathbb{N},\ u_k = \cos(k\alpha)}$$

(c) Si $u_1 \notin [-1, 1]$ alors $u_1 \in \mathbb{R} \setminus [-1, 1]$ mais d'après la question 4.(c) de la partie A, on a f qui est minorée par -1. Ainsi le cas où $u_1 = f(a) < -1$ est à exclure. On a : $u_1 > 1$.
D'après le cours, la fonction ch est strictement croissante de $]0, +\infty[$ dans $]1, +\infty[$ et continue, de plus $\lim\limits_{x \to 0} \text{ch}(x) = \text{ch}(0) = 1$ et $\lim\limits_{x \to +\infty} \text{ch}(x) = +\infty$. D'après le théorème de la bijection, ch induit une bijection de $]0, +\infty[$ dans $]1, +\infty[$. Comme nous l'avons vu $u_1 > 1$ donc u_1 admet un antécédent par ch : $\exists \beta \in \mathbb{R}_+^*$ tel que $u_1 = \text{ch}(\beta)$.
Démontrons-le par récurrence double, pour $k \geq 0$ on considère l'hypothèse :

$$\mathcal{H}_k \ :\ u_k = \text{ch}(k\beta)$$

▶ Pour $k = 0$, on a $u_0 = f(0) = 1$ d'après la question 4.(a) de la partie A. Ce qui démontre que $u_0 = \text{ch}(0 \times \beta)$ et par suite $\mathcal{H}_0$ est vraie.
▶ Pour $k = 1$, on a $u_1 = \text{ch}(\beta)$ par définition de β, $\mathcal{H}_1$ est vraie.
▶ Fixons $k \in \mathbb{N}$, on suppose que $\mathcal{H}_k$ et $\mathcal{H}_{k+1}$ sont vraies. D'après la relation démontrée à la question 1.(a), on a :

$$u_{k+2} + u_k = 2u_1 u_{k+1} \Leftrightarrow u_{k+2} = 2\,\text{ch}(\alpha)\,\text{ch}((k+1)\alpha) - \text{ch}(k\alpha)$$

Or pour tous $(b, c) \in \mathbb{R}^2$, on a : $\text{ch}(b+c) + \text{ch}(b-c) = 2\,\text{ch}(b)\,\text{ch}(c)$ comme nous l'avons démontré à la question 5. de la partie A. Si l'on applique cette formule avec $b = (k+1)\beta$ et $c = \beta$ cela donne :

$$\text{ch}((k+2)\beta) + \text{ch}(k\beta) = 2\,\text{ch}((k+1)\beta)\,\text{ch}(\beta) \Leftrightarrow \text{ch}((k+2)\beta) = 2\,\text{ch}((k+1)\beta)\,\text{ch}(\beta) - \text{ch}(k\beta)$$

Ce qui démontre que $u_{k+2} = \text{ch}((k+2)\beta)$ et par suite $\mathcal{H}_{k+2}$ est vraie. Ce qui achève la récurrence.

$$\boxed{\forall k \in \mathbb{N},\ u_k = \text{ch}(k\beta)}$$

2. (a) D'après la question 4.(a) de la partie A. On sait que $f(0) = 1$ et dans cette partie f est continue sur $\mathbb{R}$, en particulier elle est continue en 0, c'est-à-dire que :

$$\forall \varepsilon > 0,\ \exists b > 0,\ |x - 0| \leq b \Rightarrow |f(x) - f(0)| \leq \varepsilon$$

En prenant $\varepsilon = \dfrac{1}{2}$, il existe $b > 0$ tel que :

$$|x| \leq b \Rightarrow |f(x) - 1| \leq \frac{1}{2}$$

Ce qui est équivalent à dire que :

$$\forall x \in [-b, b],\ f(x) \in \left[\frac{1}{2}, \frac{3}{2}\right]$$

On a bien démontré que :

$$\boxed{\exists b > 0,\ \forall x \in [-b, b],\ f(x) > 0}$$

(b) D'après le théorème de caractérisation séquentielle de la limite, on a :

$$\begin{cases} \lim\limits_{n\to+\infty} \dfrac{b}{2^n} = 0 \\ f \text{ et continue en } 0 \end{cases} \Rightarrow \lim_{n\to+\infty} f\Big(\frac{b}{2^n}\Big) = f(0) = 1$$

$$\boxed{\lim_{n\to+\infty} v_n = 1}$$

(c) Soit $n \in \mathbb{N}$, il s'agit d'appliquer la propriété $(\mathcal{S})$ au couple $\Big(\dfrac{b}{2^{n+1}}, \dfrac{b}{2^{n+1}}\Big)$, cela donne :

$$f\Big(\underbrace{\frac{b}{2^{n+1}} + \frac{b}{2^{n+1}}}_{=\frac{b}{2^n}}\Big) + f(0) = 2f\Big(\frac{b}{2^{n+1}}\Big)^2$$

C'est-à-dire que pour tout $n \in \mathbb{N},\ v_n + 1 = 2v_{n+1}^2$. Or pour tout $n \in \mathbb{N}$, on a $\dfrac{b}{2^n} \in [-b, b]$ d'après la question 2.(a) cela implique que $v_n = f\Big(\dfrac{b}{2^n}\Big) > 0$. Ainsi la relation $v_n + 1 = 2v_{n+1}^2$ implique que :

$$\boxed{\forall n \in \mathbb{N},\ v_{n+1} = \sqrt{\frac{1 + v_n}{2}}}$$

(d) On choisit $\gamma = \text{Arccos}(v_0)$, comme $v_0 \in]0, 1]$, on a $\gamma \in \Big[0, \dfrac{\pi}{2}\Big[$. On a bien $\cos(\gamma) = v_0$.
Démontrons la propriété demandée par récurrence sur $n \in \mathbb{N}$, on pose :

$$\mathcal{H}_n \ :\ \ v_n = \cos\Big(\frac{\gamma}{2^n}\Big)$$

► Pour $n = 0$, on a $v_0 = \cos(\gamma)$ par définition de γ, $\mathcal{H}_0$ est vraie.
► On fixe $n \in \mathbb{N}$ et l'on suppose que $\mathcal{H}_n$ est vraie. On a :

$$v_{n+1} = \sqrt{\frac{v_n + 1}{2}} = \sqrt{\frac{\cos\Big(\frac{\gamma}{2^n}\Big) + 1}{2}} = \cos\Big(\frac{1}{2}\frac{\gamma}{2^n}\Big) = \cos\Big(\frac{\gamma}{2^{n+1}}\Big)$$

On a utilisé au passage la formule : $\cos^2(c) = \dfrac{1+\cos(2c)}{2}$ avec $c = \dfrac{\gamma}{2^{n+1}} \in \left[0, \dfrac{\pi}{2}\right[$, intervalle sur lequel la fonction cosinus est positive.
Ce qui achève la récurrence et démontre que :

$$\boxed{\forall n \in \mathbb{N},\ v_n = \cos\left(\frac{\gamma}{2^n}\right)}$$

(e) On suppose que $v_0 = f(b) > 1$. On justifie l'existence de $\delta > 0$ tel que $v_0 = \mathrm{ch}(\delta)$ avec exactement le même raisonnement qu'à la question 1.(c). Démontrons par récurrence sur $n \in \mathbb{N}$ la propriété suivante :

$$\mathcal{H}_n \ :\ \ v_n = \mathrm{ch}\left(\frac{\delta}{2^n}\right)$$

► Pour $n = 0$, on a $v_0 = \mathrm{ch}(\delta)$ par définition de δ, $\mathcal{H}_0$ est vraie.
► On fixe $n \in \mathbb{N}$ et l'on suppose que $\mathcal{H}_n$ est vraie. On a :

$$v_{n+1} = \sqrt{\frac{v_n+1}{2}} = \sqrt{\frac{\mathrm{ch}\left(\frac{\delta}{2^n}\right)+1}{2}} = \mathrm{ch}\left(\frac{1}{2}\frac{\delta}{2^n}\right) = \mathrm{ch}\left(\frac{\delta}{2^{n+1}}\right)$$

On a utilisé au passage la formule valable pour tout $c \in \mathbb{R}$: $\mathrm{ch}^2(c) = \dfrac{1+\mathrm{ch}(2c)}{2}$ avec $c = \dfrac{\delta}{2^{n+1}}$.

Cette formule de trigonométrie hyperbolique se démontre en revenant à la définition de la fonction ch*, pour tout* $c \in \mathbb{R},\ \mathrm{ch}(c) = \dfrac{1}{2}\left(e^c + e^{-c}\right)$.

Ce qui achève la récurrence et démontre que :

$$\boxed{\forall n \in \mathbb{N},\ v_n = \mathrm{ch}\left(\frac{\delta}{2^n}\right)}$$

(f) ► Si $f(b) \in]0,1]$, on a $f\left(\dfrac{b}{2^n}\right) = \cos\left(\dfrac{\gamma}{2^n}\right)$ d'après la question 2.(d). On pose $a = \dfrac{b}{2^n}$, on a $a > 0$ et $f(a) \in [-1,1]$ ce qui fait que l'on est dans le cadre de la question 1.(b). On sait alors que pour tout $k \in \mathbb{N}$, on a : $\underline{f(ka) = \cos(k\alpha)}$. En particulier avec $k = 1$ cela donne $f(a) = \cos(\alpha)$, c'est-à-dire $f\left(\dfrac{b}{2^n}\right) = \cos\left(\dfrac{\gamma}{2^n}\right) = \cos(\alpha)$. Or α et $\dfrac{\gamma}{2^n}$ sont deux éléments de $[0,\pi]$ et leurs cosinus sont égaux, d'où $\alpha = \dfrac{\gamma}{2^n}$.
L'expression soulignée devient :

$$\boxed{\forall (n,k) \in \mathbb{N}^2,\ f\left(k\frac{b}{2^n}\right) = \cos\left(k\frac{\gamma}{2^n}\right)}$$

► Si $f(b) > 1$, on a : $f\left(\dfrac{b}{2^n}\right) = \mathrm{ch}\left(\dfrac{\delta}{2^n}\right)$ d'après la question 2.(e). On pose $a = \dfrac{b}{2^n}$, on a $a > 0$ et $f(a) > 1$ ce qui fait que l'on est dans le cadre de la question 1.(c). On sait alors que pour tout $k \in \mathbb{N}$, on a : $\underline{f(ka) = \mathrm{ch}(k\beta)}$. En particulier avec $k = 1$ cela donne $f(a) = \mathrm{ch}(\beta)$, c'est-à-dire $f\left(\dfrac{b}{2^n}\right) = \mathrm{ch}\left(\dfrac{\delta}{2^n}\right) = \mathrm{ch}(\beta)$. Or β et $\dfrac{\delta}{2^n}$ sont strictement positifs et leur cosinus hyperbolique sont égaux, d'où $\beta = \dfrac{\delta}{2^n}$.
L'expression soulignée devient :

$$\boxed{\forall (n,k) \in \mathbb{N}^2,\ f\left(k\frac{b}{2^n}\right) = \mathrm{ch}\left(k\frac{\delta}{2^n}\right)}$$

(g) i. Pour tout $x \geq 0$ et $n \in \mathbb{N}$, on a l'encadrement usuel sur la fonction partie entière :

$$2^n \frac{x}{b} - 1 < \left\lfloor 2^n \frac{x}{b} \right\rfloor \leq 2^n \frac{x}{b}$$

On multiplie cet encadrement par $\dfrac{b}{2^n}$ qui est strictement positif pour obtenir :

$$x - \frac{b}{2^n} < \frac{b}{2^n} \left\lfloor 2^n \frac{x}{b} \right\rfloor \leq x$$

D'après le théorème d'encadrement, il apparaît que :

$$\boxed{\lim_{n\to+\infty} \frac{b}{2^n} p_n = x}$$

ii. D'après le résultat de la question précédente et par continuité de f en $x \in \mathbb{R}_+$, on a :

$$\boxed{\lim_{n\to+\infty} f\Big(\frac{b}{2^n} p_n\Big) = f(x)}$$

iii. Comme dans tout le problème, il y a deux cas à distinguer :

► Si $f(b) \in]0,1]$, on peut appliquer la question 2.(f) avec $k = p_n$ qui est bien un entier. Cela nous donne que pour tout $n \in \mathbb{N}$, $\underline{f\Big(\frac{b}{2^n} p_n\Big) = \cos\Big(p_n \frac{\gamma}{2^n}\Big)}$. Or $\lim\limits_{n\to+\infty} p_n \frac{\gamma}{2^n} = x\frac{\gamma}{b}$. En passant à la limite dans la relation soulignée grâce à la continuité des fonctions mises en jeu et à la question précédente, on obtient :

$$f(x) = \cos\Big(x\frac{\gamma}{b}\Big)$$

► Si $f(b) > 1$, on peut appliquer la question 2.(f) avec $k = p_n$ qui est bien un entier. Cela nous donne que pour tout $n \in \mathbb{N}$, $\underline{f\Big(\frac{b}{2^n} p_n\Big) = \mathrm{ch}\Big(p_n \frac{\delta}{2^n}\Big)}$. Or $\lim\limits_{n\to+\infty} p_n \frac{\delta}{2^n} = x\frac{\delta}{b}$. En passant à la limite dans la relation soulignée grâce à la continuité des fonctions mises en jeu et à la question précédente, on obtient :

$$f(x) = \mathrm{ch}\Big(x\frac{\delta}{b}\Big)$$

3. Les fonctions appartenant à $\mathcal{C}$ sont paires d'après la question 4.(b) de la partie A, ainsi les relations trouvées précédemment valables sur $\mathbb{R}_+$ le sont aussi sur $\mathbb{R}$. Ce qui démontre que si f est une fonction non nulle appartenant à $\mathcal{C}$ alors :

$$f : \begin{array}{ccc} \mathbb{R} & \to & \mathbb{R} \\ x & \mapsto & \cos(\lambda x) \end{array} \quad \text{ou} \quad f : \begin{array}{ccc} \mathbb{R} & \to & \mathbb{R} \\ x & \mapsto & \mathrm{ch}(\lambda x) \end{array} \quad \text{avec } \lambda \in \mathbb{R}$$

Ceci en posant $\lambda = \dfrac{\gamma}{b}$ ou $\lambda = \dfrac{\delta}{b}$ selon que $f(b) \in]0,1]$ ou $f(b) > 1$.

Réciproquement de telles fonctions appartiennent à $\mathcal{C}$ d'après la question 5. de la partie A.

En résumé, en tenant compte de la fonction nulle qui appartient bien sûr à $\mathcal{C}$, l'ensemble $\mathcal{C}$ est composé des fonctions définies sur $\mathbb{R}$ par :

$$\boxed{x \mapsto 0,\ x \mapsto \cos(\lambda x),\ x \mapsto \mathrm{ch}(\lambda x) \text{ où } \lambda \in \mathbb{R}}$$

Exercice 3 : Arithmétique de la suite de Fibonacci

1. Soit $n \in \mathbb{N}$, l'identité de Cassini démontrée dans le DS2 s'écrit : $F_{n+1}^2 - F_n F_{n+2} = (-1)^n$. Soit $p \in \mathbb{Z}$, un diviseur commun de F_{n+1} et F_n alors p divise toute combinaison de F_{n+1} et F_n. En particulier p divise $F_{n+1}^2 - F_n F_{n+2} = (-1)^n$. Ce qui démontre que les seuls diviseurs communs de F_{n+1} et F_n sont -1 et 1.

$$\boxed{\forall n \in \mathbb{N},\ F_{n+1} \text{ et } F_n \text{ sont premiers entre eux}}$$

2. ▶ Démontrons par récurrence double sur $p \in \mathbb{N}$:

$$\mathcal{H}_p\ :\ \forall n \in \mathbb{N}^*,\ F_{n+p} = F_{n-1}F_p + F_n F_{p+1}$$

• **Initialisation.** Pour $p = 0$, on a $F_0 = 0$ et $F_1 = 1$ ainsi la formule annoncée se résume à : $\forall n \in \mathbb{N}^*,\ F_n = F_n$. Pour $p = 1$, on a : $F_1 = 1$ et $F_2 = 1$ ainsi la formule annoncée devient : $\forall n \in \mathbb{N}^*,\ F_{n+1} = F_{n-1} + F_n$. Ce qui est vrai par définition de la suite de Fibonacci.

• **Hérédité.** On suppose $\mathcal{H}_p$ et $\mathcal{H}_{p+1}$ vraies pour un entier naturel p fixé. Soit $n \in \mathbb{N}^*$, on a :

$$\begin{array}{rcll} F_{n+p+2} & = & F_{n+p+1} + F_{n+p} & \text{par définition de la suite de Fibonacci} \\ & = & (F_{n-1}F_{p+1} + F_n F_{p+2}) + (F_{n-1}F_p + F_n F_{p+1}) & \text{en utilisant } \mathcal{H}_{p+1} \text{ et } \mathcal{H}_p \\ & = & F_{n-1}(F_{p+1} + F_p) + F_n(F_{p+2} + F_{p+1}) & \\ & = & F_{n-1}F_{p+2} + F_n F_{p+3} & \end{array}$$

Nous avons démontré $\mathcal{H}_{p+2}$ et cela termine la récurrence.

$$\boxed{\forall (n,p) \in \mathbb{N}^* \times \mathbb{N},\ F_{n+p} = F_{n-1}F_p + F_n F_{p+1}}$$

▶ Soit $n \in \mathbb{N}^*$ et $p \in \mathbb{N}$, nous allons démontrer que les couples (F_p, F_n) et (F_{n+p}, F_n) ont les mêmes diviseurs communs ainsi ils auront bien le même pgcd.
• Soit $d \in \mathbb{Z}$, si $d|F_p$ et $d|F_n$ alors $d|(F_{n-1}F_p + F_n F_{p+1}) = F_{n+p}$ (d'après la question précédente). Ce qui démontre que $d|F_n$ et $d|F_{n+p}$.
• Soit $d \in \mathbb{Z}$, si $d|F_{n+p}$ et $d|F_n$ alors $d|(F_{n+p} - F_n F_{p+1}) = F_{n-1}F_p$. Or F_n et F_{n-1} sont premiers entre eux d'après la question 1., par hypothèse $d|F_n$ donc d est premier avec F_{n-1}. D'après le théorème de Gauss : $d|F_{n-1}F_p$ et d premier avec F_{n-1} implique $d|F_p$. Finalement $d|F_n$ et $d|F_p$.

$$\boxed{\forall (n,p) \in \mathbb{N}^* \times \mathbb{N},\ \text{pgcd}(F_{n+p}, F_n) = \text{pgcd}(F_n, F_p)}$$

▶ Démontrons par récurrence sur $q \in \mathbb{N}$:

$$\mathcal{H}_q\ :\ \text{pgcd}(F_{qn+p}, F_n) = \text{pgcd}(F_p, F_n)$$

• **Initialisation.** Pour $q = 0$, la formule est évidente.

• **Hérédité.** On fixe $q \in \mathbb{N}$, on suppose que $\mathcal{H}_q$ est vraie :

$$\text{pgcd}(F_{(q+1)n+p}, F_n) = \underbrace{\text{pgcd}(F_{qn+p+n}, F_n) = \text{pgcd}(F_{qn+p}, F_n)}_{\text{question précédente}} = \text{pgcd}(F_p, F_n)$$

Ce qui démontre que $\mathcal{H}_{q+1}$ est vraie et achève la récurrence.

$$\boxed{\forall (n,p) \in \mathbb{N}^* \times \mathbb{N},\ \forall q \in \mathbb{N},\ \text{pgcd}(F_{qn+p}, F_n) = \text{pgcd}(F_p, F_n)}$$

▶ Soient m et n deux entiers naturels. Suivons les notations de l'algorithme d'Euclide et posons : $r_0 = m$, $r_1 = n$ et r_i le reste de la division euclidienne de r_{i-2} par r_{i-1}. On sait que cet algorithme se termine dans le sens où il existe un plus petit entier naturel $N \in \mathbb{N}$ tel que $r_N = 0$ et que $\text{pgcd}(m, n) = r_{N-1}$.
Démontrons par récurrence sur $i \in [\![0, N-1]\!]$:

$$\mathcal{H}_i \ : \ \text{pgcd}(F_{r_0}, F_{r_1}) = \text{pgcd}(F_{r_i}, F_{r_{i+1}})$$

• **Initialisation.** Pour $i = 0$, la formule est évidente.

• **Hérédité.** On fixe $i \in [\![0, N-2]\!]$ et on suppose que $\mathcal{H}_i$ est vraie. Effectuons la division euclidienne de r_i par r_{i+1}, on a :

$$\exists q \in \mathbb{N}, \ r_i = q r_{i+1} + r_{i+2}$$

Ainsi :

$$\text{pgcd}(F_{r_0}, F_{r_1}) = \text{pgcd}(F_{r_i}, F_{r_{i+1}}) = \underbrace{\text{pgcd}(F_{qr_{i+1}+r_{i+2}}, F_{r_{i+1}}) = \text{pgcd}(F_{r_{i+2}}, F_{r_{i+1}})}_{\text{question précédente}}$$

Ce qui démontre que $\mathcal{H}_{i+1}$ est vraie et termine la récurrence.
En particulier, $\mathcal{H}_N$ est vérifiée donc :

$$\text{pgcd}(F_m, F_n) = \text{pgcd}(F_{r_0}, F_{r_1}) = \text{pgcd}(F_{r_{N-1}}, F_{r_N}) = \text{pgcd}(F_{r_{N-1}}, F_0) = \text{pgcd}(F_{r_{N-1}}, 0) = F_{r_{N-1}} = F_{\text{pgcd}(m,n)}$$

$$\boxed{\forall (m, n) \in \mathbb{N}^2, \ \text{pgcd}(F_m, F_n) = F_{\text{pgcd}(m,n)}}$$