Lycée Bellevue – Toulouse **20 décembre 2024**
MPSI – Mathématiques

Corrigé du Devoir Surveillé n°4

Exercices. *(8 points)*

1. *(3 points)* Résolvons l'équation :

$$t(t+2)y' - 2(t+5)y = 12t^7. \qquad (E)$$

L'équation homogène associée à cette équation est :

$$t(t+2)y' - 2(t+5)y = 0. \qquad (H)$$

Comme $t(t+2)$ n'est pas nul sur $\mathbb{R}_+^*$ elle équivaut à :

$$y' - \frac{2(t+5)}{t(t+2)}y = 0.$$

Soit $a(t) = \frac{2(t+5)}{t(t+2)}$. Alors :

$$a(t) = \frac{5}{t} - \frac{3}{t+2}$$

On pose $A(t) = 5\ln|t| - 3\ln|t+2|$: A est une primitive de a.
De plus pour tout $t \in \mathbb{R}_+^*$: $\quad A(t) = 5\ln t - 3\ln(t+2)$.
Comme $\mathbb{R}_+^*$ est un intervalle alors les solutions de l'équation (H) sont les fonctions $y_0 : t \mapsto \lambda e^{A(t)}$ où λ est une constante réelle :

$$\forall t \in \mathbb{R}_+^* \qquad y_0(t) = \lambda \frac{t^5}{(t+2)^3} \qquad \text{avec} \quad \lambda \in \mathbb{R}.$$

Pour trouver une solution particulière on pose $y(t) = \lambda(t)\frac{t^5}{(t+2)^3}$ où λ est une fonction dérivable. Alors y est solution de l'équation de départ si et seulement si :

$$\lambda'(t) = 12t(t+2)^2$$

On écrit :

$$\lambda'(t) = 12(t+2)^3 - 24(t+2)^2$$

On choisit par exemple $\lambda(t) = 3(t+2)^4 - 8(t+2)^3 = (3t-2)(t+2)^3$.
On obtient pour solution particulière :

$$y_1 : t \mapsto (3t-2)t^5.$$

Les solutions de l'équation (E) sont les fonctions $y = y_0 + y_1$, *i.e.*, :

$$\forall t \in \mathbb{R}_+^* \qquad y(t) = \lambda \frac{t^5}{(t+2)^3} + (3t-2)t^5 \qquad \text{avec} \quad \lambda \in \mathbb{R}.$$

2. *(3 points)* Posons $y = \sqrt{t}$, *i.e.*, $t = y^2$.
La fonction $y \mapsto y^2$ est de classe $\mathcal{C}^1$, de dérivée $y \mapsto 2y$, ce qui donne $\frac{\mathrm{d}t}{\mathrm{d}y} = 2y$ donc $\mathrm{d}t = 2y\,\mathrm{d}y$.
Par changement de variable :

$$F(x) = \int_0^x \arctan\sqrt{t}\,\mathrm{d}t = \int_0^{\sqrt{x}} 2y\arctan y\,\mathrm{d}y.$$

Posons $u(y) = \arctan y$ et $v(y) = y^2$.
Les fonctions u et v sont de classe $\mathcal{C}^1$, avec $u'(y) = \frac{1}{1+y^2}$ et $v'(y) = 2y$.
Par intégration par parties :

$$F(x) = \Big[y^2\arctan y\Big]_0^{\sqrt{x}} - \int_0^{\sqrt{x}} \frac{y^2}{1+y^2}\,\mathrm{d}y.$$

On calcule :

$$\int_0^{\sqrt{x}} \frac{y^2}{1+y^2}\,\mathrm{d}y = \int_0^{\sqrt{x}} \left(1 - \frac{1}{1+y^2}\right)\mathrm{d}y = \Big[y - \arctan y\Big]_0^{\sqrt{x}} = \sqrt{x} - \arctan\sqrt{x}.$$

Finalement :

$$\forall x \in \mathbb{R}_+ \qquad F(x) = (x+1)\arctan\sqrt{x} - \sqrt{x}.$$

3. *(2 points)* Soit $n \in \mathbb{N}$ et $I_n = \displaystyle\int_{\frac{\pi}{6}}^{\frac{\pi}{3}} \frac{\mathrm{d}x}{1+\tan^n x}$.
Soit $t = \frac{\pi}{2} - x$, ce qui équivaut à $x = \frac{\pi}{2} - t$.
La fonction $t \mapsto \frac{\pi}{2} - t$ est de classe $\mathcal{C}^1$, de dérivée $t \mapsto -1$, donc $\mathrm{d}x = -\mathrm{d}t$.
Par changement de variable :

$$I_n = \int_{\frac{\pi}{6}}^{\frac{\pi}{3}} \frac{\mathrm{d}x}{1+\tan^n x} = \int_{\frac{\pi}{3}}^{\frac{\pi}{6}} \frac{-\mathrm{d}t}{1+\tan^n\left(\frac{\pi}{2}-t\right)}.$$

Comme $\tan\left(\frac{\pi}{2}-t\right) = \frac{1}{\tan t}$ alors :

$$I_n = \int_{\frac{\pi}{6}}^{\frac{\pi}{3}} \frac{\mathrm{d}t}{1+\tan^{-n} t} = \int_{\frac{\pi}{6}}^{\frac{\pi}{3}} \frac{\tan^n t}{1+\tan^n t}\,\mathrm{d}t$$

On remarque :

$$I_n = \int_{\frac{\pi}{6}}^{\frac{\pi}{3}} \left(1 - \frac{1}{1+\tan^n t}\right)\mathrm{d}t$$

Par linéarité :

$$I_n = \int_{\frac{\pi}{6}}^{\frac{\pi}{3}} 1\,\mathrm{d}t - \int_{\frac{\pi}{6}}^{\frac{\pi}{3}} \frac{1}{1+\tan^n t}\,\mathrm{d}t = \frac{\pi}{6} - I_n.$$

On en déduit $2I_n = \frac{\pi}{6}$ et finalement :

$$\forall n \in \mathbb{N} \qquad I_n = \frac{\pi}{12}$$

Problème 1. *(15 points)*

1. On suppose que f est une fonction de $\mathbb{R}$ dans $\mathbb{R}$ vérifiant :

$$\forall(x,y)\in\mathbb{R}^2 \qquad f(x)^2-f(y)^2=f(x+y)f(x-y). \tag{$\star$}$$

(a) *(1 point)* Pour $x=y=0$ la relation $(\star)$ montre que $0=f(0)^2$, donc $f(0)=0$.

(b) *(1 point)* La relation $(\star)$ est valable pour tout $(x,y)\in\mathbb{R}^2$. Comme f est deux fois dérivable alors elle est dérivable, donc tous les termes de l'équation $(\star)$ sont dérivables par composition, produit et somme.

En particulier en dérivant par rapport à x :

$$\forall(x,y)\in\mathbb{R}^2 \qquad 2f'(x)f(x)=f'(x+y)f(x-y)+f(x+y)f'(x-y).$$

Comme la fonction f est deux fois dérivable alors la fonction f' est dérivable, et par composition, produit et somme tous les termes de cette égalité sont dérivables par rapport à y. En dérivant par rapport à y elle donne :

$$\begin{aligned}\forall(x,y)\in\mathbb{R}^2 \qquad 0 &= f''(x+y)f(x-y)-f'(x+y)f'(x-y)\\ &\qquad +f'(x+y)f'(x-y)-f(x+y)f''(x-y)\\ \iff \qquad 0 &= f''(x+y)f(x-y)-f(x+y)f''(x-y).\end{aligned}$$

Finalement :

$$\forall(x,y)\in\mathbb{R}^2 \qquad f''(x+y)f(x-y)=f(x+y)f''(x-y).$$

(c) *(1 point)* La relation de la question précédente s'écrit :

$$\forall(u,v)\in\mathbb{R}^2 \qquad f''(u+v)f(u-v)=f(u+v)f''(u-v).$$

Soit $(x,y)\in\mathbb{R}^2$, puis $u=\frac{x+y}{2}$ et $v=\frac{x-y}{2}$. Alors $u+v=x$ et $u-v=y$ donc :

$$f''(x)f(y)=f(x)f''(y).$$

Ce résultat est valable pour tout $(x,y)\in\mathbb{R}^2$.

(d) *(1 point)* Comme f n'est pas la fonction nulle alors il existe $y\in\mathbb{R}$ tel que $f(y)\neq 0$. Pour cette valeur de y la relation précédente devient :

$$\forall x\in\mathbb{R} \qquad f''(x)-\frac{f''(y)}{f(y)}f(x)=0.$$

En posant $\alpha=\frac{f''(y)}{f(y)}$ ceci montre que f est solution de l'équation :

$$y''-\alpha y=0. \tag{H}$$

(e) *(3 points)* L'équation caractéristique de l'équation différentielle ci-dessus est :

$$\lambda^2-\alpha=0. \tag{C}$$

Trois cas se présentent : $\alpha>0$, $\alpha<0$ et $\alpha=0$.

Cas $\alpha > 0$. Dans ce cas les racines de (C) sont $\lambda = \pm\sqrt{\alpha}$, donc les solutions réelles de l'équation (H) sont les fonctions :

$$y_0 : t \mapsto ae^{\sqrt{\alpha}t} + be^{-\sqrt{\alpha}t} \qquad \text{avec} \quad (a, b) \in \mathbb{R}^2.$$

Comme $f(0) = 0$ alors $a + b = 0$, donc :

$$\forall t \in \mathbb{R} \qquad f(t) = a\left(e^{\sqrt{\alpha}t} - e^{-\sqrt{\alpha}t}\right) = 2a\,\mathrm{sh}\left(\sqrt{\alpha}t\right).$$

En posant $A = \pm 2a$ on peut écrire ces solutions :

$$f(t) = A\,\mathrm{sh}(\beta t) \qquad \text{avec} \quad (A, \beta) \in \mathbb{R}^2.$$

Cas $\alpha < 0$. Dans ce cas les racines de (C) sont $\lambda = \pm i\sqrt{-\alpha}$, donc les solutions réelles de l'équation (H) sont les fonctions :

$$y_0 : t \mapsto a\cos\left(\sqrt{-\alpha}t\right) + b\sin\left(\sqrt{-\alpha}t\right) \qquad \text{avec} \quad (a, b) \in \mathbb{R}^2.$$

Comme $f(0) = 0$ alors $a = 0$, donc :

$$\forall t \in \mathbb{R} \qquad f(t) = b\sin\sqrt{-\alpha}t.$$

En posant $b = \pm A$ on peut écrire ces solutions :

$$f(t) = A\sin(\beta t) \qquad \text{avec} \quad (A, \beta) \in \mathbb{R}^2.$$

Cas $\alpha = 0$. Dans ce cas l'unique racine de (C) est $\lambda = 0$.
Les solutions réelles de l'équation (H) sont les fonctions :

$$y_0 : t \mapsto at + b \qquad \text{avec} \quad (a, b) \in \mathbb{R}^2.$$

Comme $f(0) = 0$ alors $b = 0$, donc :

$$\forall t \in \mathbb{R} \qquad f(t) = at \qquad \text{avec} \quad a \in \mathbb{R}.$$

2. *(2 points)* Dans les trois cas la fonction f est bien continue.
Cas 1. Supposons que :

$$\forall t \in \mathbb{R} \qquad f(t) = A\,\mathrm{sh}(\beta t) \qquad \text{avec} \quad (A, \beta) \in \mathbb{R}^2.$$

On calcule alors, pour tout $(x, y) \in \mathbb{R}$:

$$\begin{aligned} f(x)^2 - f(y)^2 &= A^2\left[\left(\frac{e^{\beta x} - e^{-\beta x}}{2}\right)^2 - \left(\frac{e^{\beta y} - e^{-\beta y}}{2}\right)^2\right] \\ &= \frac{A^2}{4}\left[\left(e^{2\beta x} - 2 + e^{-2\beta x}\right) - \left(e^{2\beta y} - 2 + e^{-2\beta y}\right)\right] \\ &= \frac{A^2}{4}\left(e^{2\beta x} + e^{-2\beta x} - e^{2\beta y} - e^{-2\beta y}\right) \end{aligned}$$

D'autre part, toujours pour tout $(x, y) \in \mathbb{R}$:

$$\begin{aligned} f(x+y)f(x-y) &= A^2 \operatorname{sh}(\beta x + \beta y) \operatorname{sh}(\beta x - \beta y) \\ &= \frac{A^2}{4}\Big(e^{\beta x+\beta y} - e^{-\beta x-\beta y}\Big)\Big(e^{\beta x-\beta y} - e^{-\beta x+\beta y}\Big) \\ &= \frac{A^2}{4}\Big(e^{2\beta x} - e^{2\beta y} - e^{-2\beta y} + e^{-2\beta x}\Big). \end{aligned}$$

Ceci montre que :

$$\forall (x,y) \in \mathbb{R}^2 \qquad f(x)^2 - f(y)^2 = f(x+y)f(x-y).$$

La fonction f vérifie bien la relation $(\star)$.

Cas 2. Supposons que :

$$\forall t \in \mathbb{R} \qquad f(t) = A\sin(\beta t) \qquad \text{avec} \quad (A, \beta) \in \mathbb{R}^2.$$

La formule de transformation de produit en somme

$$\forall (x,y) \in \mathbb{R}^2 \qquad \sin x \sin y = \tfrac{1}{2}(\cos(x-y) - \cos(x+y))$$

montre que pour tout $(x, y) \in \mathbb{R}^2$:

$$\begin{aligned} f(x+y)f(x-y) &= A^2 \sin(\beta(x+y))\sin(\beta(x-y)) \\ &= \frac{A^2}{2}(\cos(2\beta y) - \cos(2\beta x)) \\ &= \frac{A^2}{2}\Big[\Big(1 - 2\sin^2(\beta y)\Big) - \Big(1 - 2\sin^2(x\beta)\Big)\Big] \\ &= A^2\Big(\sin^2(\beta x) - \sin^2(\beta y)\Big) \\ &= f(x)^2 - f(y)^2. \end{aligned}$$

La fonction f vérifie bien la relation $(\star)$.

Cas 3. Supposons que :

$$\forall t \in \mathbb{R} \qquad f(t) = at \qquad \text{avec} \quad a \in \mathbb{R}.$$

Alors :

$$\forall (x,y) \in \mathbb{R}^2 \qquad f(x+y)f(x-y) = a^2(x+y)(x-y) = a^2x^2 - a^2y^2 = f(x)^2 - f(y)^2.$$

La fonction f vérifie bien la relation $(\star)$.

Finalement, dans les trois cas les fonctions f obtenues sont solution du problème.

3. Soit f une fonction de $\mathbb{R}$ dans $\mathbb{R}$ continue non-nulle vérifiant :

$$\forall (x,y) \in \mathbb{R}^2 \qquad f(x)^2 - f(y)^2 = f(x+y)f(x-y). \qquad (\star)$$

(a) *(1 point)* Raisonnons par l'absurde en supposant :

$$\forall x \in \mathbb{R} \qquad \int_0^x f(t)\,\mathrm{d}t = 0.$$

La fonction f est continue, $\mathbb{R}$ est un intervalle, 0 est un élément de $\mathbb{R}$, donc d'après le théorème fondamental la fonction

$$\begin{aligned} F : \mathbb{R} &\longrightarrow \mathbb{R} \\ x &\longmapsto \int_0^x f(t)\,\mathrm{d}t \end{aligned}$$

est une primitive de f. Si cette fonction est nulle alors sa dérivée est nulle, donc f est nulle.

Ceci est supposé faux, donc l'hypothèse de départ est fausse et :

$$\exists x_0 \in \mathbb{R} \qquad \int_0^{x_0} f(t)\,\mathrm{d}t \neq 0.$$

(b) *(1 point)* La relation $(\star)$ s'écrit :

$$\forall (u,v) \in \mathbb{R}^2 \qquad f(u)^2 - f(v)^2 = f(u+v)f(u-v).$$

Soit $(x,y) \in \mathbb{R}^2$ et $u = \frac{x+y}{2}$, $v = \frac{x-y}{2}$. Alors $u+v = x$ et $u-v = y$, donc :

$$\forall (x,y) \in \mathbb{R}^2 \qquad f\left(\frac{x+y}{2}\right)^2 - f\left(\frac{x-y}{2}\right)^2 = f(x)f(y).$$

Ceci est le résultat attendu.

(c) *(2 points)* En intégrant pour y allant de 0 à x_0 l'égalité ci-dessus donne :

$$\forall x \in \mathbb{R} \qquad \int_{y=0}^{x_0} \left(f\left(\tfrac{x+y}{2}\right)^2 - f\left(\tfrac{x-y}{2}\right)^2 \right) \mathrm{d}y = \int_{y=0}^{x_0} f(x)f(y)\,\mathrm{d}y.$$

Par linéarité de l'intégrale :

$$\forall x \in \mathbb{R} \qquad \int_0^{x_0} f\left(\tfrac{x+y}{2}\right)^2 \mathrm{d}y - \int_0^{x_0} f\left(\tfrac{x-y}{2}\right)^2 \mathrm{d}y = f(x)\int_0^{x_0} f(y)\,\mathrm{d}y.$$

On applique le changement de variable $t = x+y$ dans la première intégrale.
La fonction $y \mapsto x+y$ est de classe $\mathcal{C}^1$ de dérivée $y \mapsto 1$, donc $\mathrm{d}t = \mathrm{d}y$ et :

$$\int_0^{x_0} f\left(\tfrac{x+y}{2}\right)^2 \mathrm{d}y = \int_x^{x+x_0} f\left(\tfrac{t}{2}\right)^2 \mathrm{d}t.$$

On applique le changement de variable $t = x-y$ dans la seconde intégrale.
La fonction $y \mapsto x-y$ est de classe $\mathcal{C}^1$ de dérivée $y \mapsto -1$, donc $\mathrm{d}t = -\mathrm{d}y$ et :

$$\int_0^{x_0} f\left(\tfrac{x-y}{2}\right)^2 \mathrm{d}y = -\int_x^{x-x_0} f\left(\tfrac{t}{2}\right)^2 \mathrm{d}t.$$

Comme on a défini $A = \displaystyle\int_0^{x_0} f(t)\,\mathrm{d}t$ alors :

$$\forall x \in \mathbb{R} \qquad \int_x^{x+x_0} f\left(\tfrac{t}{2}\right)^2 \mathrm{d}t + \int_x^{x-x_0} f\left(\tfrac{t}{2}\right)^2 \mathrm{d}t = Af(x).$$

Il s'agit du résultat attendu.

(d) *(2 points)* Comme A est non-nul alors :

$$\forall x \in \mathbb{R} \qquad f(x) = \frac{1}{A}\left(\int_x^{x+x_0} f\left(\frac{t}{2}\right)^2 \mathrm{d}t + \int_x^{x-x_0} f\left(\frac{t}{2}\right)^2 \mathrm{d}t\right).$$

La fonction $x \mapsto f\left(\frac{x}{2}\right)^2$ est continue car f est continue.
Elle admet donc une primitive que l'on note G. Ainsi :

$$\begin{aligned}\forall x \in \mathbb{R} \qquad f(x) &= \frac{1}{A}\left(\Big[G(t)\Big]_x^{x+x_0} + \Big[G(t)\Big]_x^{x-x_0}\right)\\ &= \frac{1}{A}(G(x+x_0) + G(x-x_0) - 2G(x)).\end{aligned}$$

Comme G est une primitive de la fonction $g : x \mapsto f\left(\frac{x}{2}\right)^2$ alors elle est dérivable de dérivée g. Par composition f est dérivable, de dérivée :

$$\forall x \in \mathbb{R} \qquad f'(x) = \frac{1}{A}(g(x+x_0) + g(x-x_0) - 2g(x))$$

Comme la fonction f est dérivable alors par composition et produit la fonction g est dérivable, puis par somme la fonction f' est dérivable, ce qui signifie que la fonction f est deux fois dérivable.

4. *(1 point)* Dans la question précédente il est démontré que si f est une solution du problème non-nulle alors elle est deux fois dérivable.

   Dans la question 1 il est démontré que si f est une solution du problème non-nulle et deux fois dérivable alors elle est de la forme

   $$f : x \mapsto A\,\mathrm{sh}(\beta t) \qquad \text{ou} \qquad f : x \mapsto A\sin(\beta t) \qquad \text{ou} \qquad f : x \mapsto at$$

   avec A, β, a des réels.

   Dans la question 2 il est vérifié que ces fonctions sont bien solutions du problème.

   La fonction nulle est solution du problème, elle appartient aux trois familles de fonctions ci-dessus, obtenue pour $A = 0$ ou $a = 0$.

   Finalement les solutions du problème sont les trois familles de fonctions décrites ci-dessus.

Problème 2. *(15 points)*

1. *(2 points)* On remarque que :

$$F^{n+1} = 2^{p^{n+1}} - 1 = 2^{p^n \times p} - 1 = \left(2^{p^n}\right)^p - 1^p.$$

D'après la formule pour $a^n - b^n$, dite formule de Bernoulli :

$$F^{n+1} = \left(2^{p^n} - 1\right) \sum_{k=0}^{p-1} \left(2^{p^n}\right)^k = F_n \sum_{k=0}^{p-1} 2^{kp^n}.$$

Comme $\sum_{k=0}^{p-1} 2^{kp^n}$ est un entier alors F_n divise F_{n+1}, et son quotient est :

$$Q_n = \sum_{k=0}^{p-1} 2^{kp^n}.$$

2. *(1 point)* Soit d un diviseur de Q_n.
Alors d est un diviseur de $Q_n F_n = F_{n+1}$, et donc d divise $2^{p^{n+1}} - 1$.
Ceci donne $\quad 2^{p^{n+1}} - 1 \equiv 0 \ [d] \quad$ puis $\quad 2^{p^{n+1}} \equiv 1 \ [d]$.

3. *(2 points)* Pour tout $n \in \mathbb{N}$ on note $\mathcal{P}_n$ la propriété : $\quad F_n \equiv 1 \ [p]$.
On démontre par récurrence que cette propriété est vraie pour tout $n \in \mathbb{N}$.
<u>Initialisation.</u> Comme $F_0 = 2^1 - 1 = 1$ alors $F_0 \equiv 1 \ [p]$.
<u>Hérédité.</u> Supposons que pour un certain $n \in \mathbb{N}$ la propriété $\mathcal{P}_n$ est vraie : $\quad F_n \equiv 1 \ [p]$.
Alors $\quad 2^{p^n} - 1 \equiv 1 \ [p] \quad$ donc $\quad 2^{p^n} \equiv 2 \ [p]$.
La relation de congruence est compatible avec le produit donc : $\quad \left(2^{p^n}\right)^p \equiv 2^p \ [p]$.
Ceci donne : $\quad 2^{p^{n+1}} \equiv 2^p \ [p]$.
Comme p est un nombre premier alors d'après le petit théorème de Fermat :

$$\forall a \in \mathbb{Z} \qquad a^p \equiv a \ [p]\,.$$

En particulier pour $a = 2$ on obtient $2^p \equiv 2 \ [p]$ puis par transitivité : $\quad 2^{p^{n+1}} \equiv 2 \ [p]$.
Or $F_{n+1} = 2^{p^{n+1}} - 1$ donc : $\quad F_{n+1} \equiv 1 \ [p]$.
La propriété $\mathcal{P}_{n+1}$ est vraie.
L'hérédité est démontrée.
<u>Conclusion.</u> Par récurrence la propriété $\mathcal{P}_n$ est vraie pour tout $n \in \mathbb{N}$.

4. (a) *(1 point)* Soit d un diviseur de F_n. Alors $\quad F_n \equiv 0 \ [d] \quad$ donc : $\quad 2^{p^n} \equiv 1 \ [d]$.

D'après la question 1 : $\quad Q_n = \sum_{k=0}^{p-1} \left(2^{p^n}\right)^k$.

Comme $\quad 2^{p^n} \equiv 1 \ [d] \quad$ alors $\quad Q_n \equiv \sum_{k=0}^{p-1} 1^k = p \ [d] \quad$ et donc $\quad Q_n \equiv p \ [d]$.

(b) *(1 point)* Soit $d = Q_n \wedge F_n$.
Alors d divise F_n donc d'après la question précédente : $Q_n \equiv p\ [d]$.
Aussi d divise Q_n donc : $Q_n \equiv 0\ [d]$.
Par transitivité : $p \equiv 0\ [d]$, donc d divise p.
Comme p est premier alors : $d = 1$ ou $d = p$.
Si $d = p$ alors d'après la question (3) : $F_n \equiv 1\ [d]$.
Or $F_n \equiv 0\ [d]$ car d divise F_n, ce qui donne $0 \equiv 1\ [d]$, puis $d = 1$.
C'est impossible si $d = p$ car p est un nombre premier.
Donc par l'absurde $d = 1$, ce qui signifie que Q_n et F_n sont premiers entre eux.

(c) *(1 point)* Soit m et n deux entiers naturels distincts.
Quitte à les inverser on peut supposer $m < n$.
Soit $d = Q_m \wedge Q_n$. Alors d divise Q_m donc d divise $Q_m F_m = F_{m+1}$,
Comme m et n sont des entiers et $m < n$ alors $m + 1 \leqslant n$.
D'après la question (1), pour tout $k \in \mathbb{N}$: F_k divise F_{k+1}.
Donc par transitivité F_{m+1} divise F_n.
De plus d divise F_{m+1} donc d divise F_n, encore par transitivité.
Or $d = Q_m \wedge Q_n$ donc d divise Q_n.
Ainsi d divise F_n et Q_n, lesquels sont premiers entre eux d'après la question précédente, donc $d = 1$.
Ceci montre que Q_m et Q_n sont premiers entre eux.

5. (a) *(1 point)* Soit $k \in \mathbb{N}^*$.
Comme $b > 0$ alors la division euclidienne de a^k par b est définie :
Il existe un unique couple (q_k, r_k) d'entiers tel que :

$$a^k = q_k b + r_k \qquad \text{et} \qquad 0 \leqslant r_k < b.$$

Les entiers $r_1, \ldots, r_{b+1}$ sont $b+1$ entiers de l'ensemble $\{0, \ldots b-1\}$, lequel contient b éléments. Donc deux d'entre eux au moins sont égaux, ce qui signifie qu'il existe i et j distincts dans $\{1, \ldots, b+1\}$ tels que $r_i = r_j$.
Quitte à les inverser on peut supposer $i < j$.

(b) *(1 point)* Comme $r_i = r_j$ alors $a^i - q_i b = a^j - q_j b$ et donc : $a^i \equiv a^j\ [b]$.
Ceci donne $a^j - a^i \equiv 0\ [b]$, puis $a^i(a^{j-i} - 1) \equiv 0\ [b]$.
Ainsi b divise $a^i(a^{j-i} - 1)$. Comme b est premier avec a alors d'après le lemme de Gauss b divise $a^{j-i} - 1$, et donc $a^{j-i} \equiv 1\ [b]$.
Comme de plus $j - i \in \mathbb{N}^*$ alors $j - i \in E$.
L'ensemble E est une partie de $\mathbb{N}^*$ non-vide car elle contient $j - i$, donc elle admet un plus petit élément.

(c) *(2 points)* Soit $n \in e\mathbb{N}^*$, *i.e.,* $n = ek$ où $k \in \mathbb{N}^*$.

Comme $e \in E$ alors : $a^e \equiv 1 \ [b]$.

Donc $a^n = a^{ek} = (a^e)^k \equiv 1^k \equiv 1 \ [b]$, ce qui montre que $n \in E$.

Ainsi $e\mathbb{N}^* \subseteq E$.

Soit maintenant $n \in E$.

Comme $e \in E$ alors e est strictement positif, donc la division euclidienne de n par e est définie, *i.e.,* il existe $(q, r) \in \mathbb{N}^2$ tels que $n = qe + r$ avec $0 \leqslant r < e$.

Comme $n \in E$ alors : $a^n \equiv 1 \ [b]$.

Or : $a^n = a^{qe+r} = (a^e)^q a^r$.

Comme $e \in E$ alors $a^e \equiv 1 \ [b]$ et donc : $a^n \equiv 1^q a^r = a^r \ [b]$.

Ceci montre que $a^r \equiv 1 \ [b]$.

Si $r > 0$ alors $r \in E$. Mais $r < e$ et e est le plus petit élément de E, donc ceci est impossible. Ainsi $r = 0$, puis $n = qe$, donc $n \in e\mathbb{N}^*$.

On a démontré que $E \subseteq e\mathbb{N}^*$.

Par double inclusion $E = e\mathbb{N}^*$.

6. (a) *(1 point)* Tout d'abord 2 et d sont premiers entre eux.

En effet, d divise Q_n qui divise $F_{n+1} = 2^{p^{n+1}} - 1$, lequel est impair car $p^{n+1} \geqslant 1$, donc d est impair et ainsi 2 est premier avec d.

On peut donc définir l'ordre de 2 modulo d, que l'on note e.

Comme d divise Q_n alors d'après la question (2) : $2^{p^{n+1}} \equiv 1 \ [d]$.

Ceci montre que $p^{n+1} \in \left\{ k \in \mathbb{N}^* \mid 2^k \equiv 1 \ [d] \right\} = e\mathbb{N}^*$.

En conséquence e divise p^{n+1}.

Comme p est premier alors e est de la forme $e = p^k$ avec $k \in \{0, \ldots, n+1\}$.

Si $k < n+1$ alors $k \leqslant n$, donc e divise p^n, et ainsi : $2^{p^n} \equiv 1 \ [d]$.

Alors d diviserait $2^{p^n} - 1 = F_n$. Mais d divise Q_n, alors que Q_n et F_n sont premiers entre eux, c'est absurde.

Donc $k = n+1$, et ainsi $e = p^{n+1}$, *i.e.,* l'ordre de 2 modulo d est p^{n+1}.

(b) *(1 point)* Comme d est premier alors d'après le petit théorème de Fermat : $2^d \equiv 2 \ [d]$.

Ceci montre que d divise $2^d - 2 = 2(2^{d-1} - 1)$.

Nous avons justifié dans la question précédente que Q_n est impair pour tout $n \in \mathbb{N}$, donc Q_{n-1} est impair pour $n \in \mathbb{N}^*$.

Comme d est un diviseur de Q_{n-1} alors d est impair, et ainsi d ne divise par 2.

Or d divise $2(2^{d-1} - 1)$ donc d'après le lemme d'Euclide d divise $2^{d-1} - 1$, ce qui montre que : $2^{d-1} \equiv 1 \ [d]$.

Ainsi $d - 1 \in \left\{ k \in \mathbb{N}^* \mid 2^k \equiv 1 \ [d] \right\} = e\mathbb{N}^*$ avec $e = p^{n+1}$.

Donc $d - 1$ est un multiple de p^{n+1}, et ainsi : $d \equiv 1 \ [p^n]$.

(c) *(1 point)* L'expression de Q_n obtenue dans la question (1) montre que pour tout $n \in \mathbb{N} : \quad Q_n > 1$.

Donc chaque Q_n admet un diviseur premier d_n.

D'après la question (4c) les Q_n sont premiers entre eux deux-à-deux, donc les d_n sont des nombres premiers distincts.

Soit $n \in \mathbb{N}^*$. Supposons qu'il n'existe qu'un nombre fini N de nombres premiers tels que $d \equiv 1 \ [p^n]$.

Alors d_{n-1}, d_n, d_{n+1}, $\ldots$, d_{n+N-1} sont $N+1$ nombres premiers distincts.

D'après la question précédente :

$$\forall k = n-1 \ldots, n+N-1 \qquad d_k \equiv 1 \ \left[p^{k+1}\right].$$

Si $k \geqslant n-1$ alors p^n divise p^{k+1}, donc $d_k \equiv 1 \ [p^n]$.

On a donc obtenu $N+1$ nombre premiers distincts d tels que $d \equiv 1 \ [p^n]$, ce qui contredit la définition de N.

En conséquence il existe une infinité de nombres premiers congrus à 1 modulo p^n.