Exercice 1 : équation fonctionnelle (20.5 points)

1. Soit $x \in \mathbb{R}$. Comme $g(x) \times g(x) = 1$, on déduit que $g(x) = 1$ ou $g(x) = -1$.

   On a donc obtenu que : $\forall x \in \mathbb{R} \quad \Big(g(x) = 1 \text{ ou } g(x) = -1\Big)$

   On cherche à montrer que : $\Big(\forall x \in \mathbb{R} \quad g(x) = 1\Big)$ ou $\Big(\forall x \in \mathbb{R} \quad g(x) = -1\Big)$

   Les deux propositions ne sont pas équivalentes. Par exemple, la fonction g définie par $g(x) = (-1)^{\lfloor x \rfloor}$ vérifie la première proposition mais pas la deuxième.

   La fonction g est continue et ne s'annule pas sur $\mathbb{R}$, par conséquent, elle est de signe constant.
   Ainsi, $\Big(\forall x \in \mathbb{R} \quad g(x) = 1\Big)$ ou $\Big(\forall x \in \mathbb{R} \quad g(x) = -1\Big)$

   $\boxed{\text{La fonction } g \text{ est constante}}$ **(1.5 pt)**

   Autre justification possible :
   Supposons par l'absurde que la fonction g ne soit pas constante.
   Alors il existe $a \in \mathbb{R}$ tel que $g(a) = -1$ et il existe $b \in \mathbb{R}$ tel que $g(b) = 1$.
   La fonction g étant continue sur $\mathbb{R}$ et comme elle change de signe, on déduit avec le théorème des valeurs intermédiaires qu'il existe $x \in \mathbb{R}$ tel que $g(x) = 0$.
   Ce qui est contradictoire avec $g(x) \times g(x) = 1$.

   $\boxed{\text{Ainsi, la fonction } g \text{ est constante}}$

   Autre justification possible :
   g est continue, donc $g(\mathbb{R})$ est un intervalle (l'image d'un intervalle par une fonction continue est un intervalle).
   $g(\mathbb{R})$ est un intervalle inclus dans $\{-1, 1\}$, par conséquent $g(\mathbb{R}) = \{1\}$ ou $g(\mathbb{R}) = \{-1\}$

   $\boxed{\text{Ainsi, } \Big(\forall x \in \mathbb{R} \quad g(x) = 1\Big) \text{ ou } \Big(\forall x \in \mathbb{R} \quad g(x) = -1\Big)}$

2. (a) D'après l'équation fonctionnelle, on a : $\Big(1 + f^2(0)\Big)f(0) = 2f(0)$.

   Ce qui donne : $f^3(0) - f(0) = 0$, c'est-à-dire $f(0)\Big(f(0) - 1\Big)\Big(f(0) + 1\Big) = 0$

   D'où $f(0) = 0$ ou $f(0) = 1$ ou $f(0) = -1$.

   $\boxed{\text{Ainsi, } f(0) \in \Big\{-1, 0, 1\Big\}}$ **(1.25 pt)**

   (b) Supposons que $f(0) = 1$.
   Soit $x \in \mathbb{R}$.
   On a d'après l'équation fonctionnelle : $\Big(1 + f(x)f(0)\Big) \times f(x) = f(x) + f(0)$, ce qui donne $f^2(x) = 1$.
   f étant de plus continue, on déduit avec le résultat préliminaire que f est constante.
   $\boxed{\text{On a montré que si } f(0) = 1, \text{ alors } f \text{ est constante}}$ **(1 pt)**

   (c) Soit $P(n)$: « $f\left(\dfrac{a}{2^n}\right) = 1$ »
   $P(0)$ est vraie par hypothèse.
   Supposons $P(n)$ vraie pour un entier $n \geq 0$.
   D'après l'équation fonctionnelle appliquée aux réels $\dfrac{a}{2^{n+1}}$ et $\dfrac{a}{2^{n+1}}$, on a :
   $$\left(1 + f^2\left(\frac{a}{2^{n+1}}\right)\right) \times f\left(\frac{a}{2^n}\right) = 2f\left(\frac{a}{2^{n+1}}\right)$$
   Comme par hypothèse de récurrence, $f\left(\dfrac{a}{2^n}\right) = 1$, on obtient : $1 + f^2\left(\dfrac{a}{2^{n+1}}\right) = 2f\left(\dfrac{a}{2^{n+1}}\right)$
   Ce qui donne : $1 + f^2\left(\dfrac{a}{2^{n+1}}\right) - 2f\left(\dfrac{a}{2^{n+1}}\right) = 0$
   c'est-à-dire : $\left(f\left(\dfrac{a}{2^{n+1}}\right) - 1\right)^2$ *on reconnaît l'identité remarquable* $x^2 - 2x + 1 = (x-1)^2$
   D'où $f\left(\dfrac{a}{2^{n+1}}\right) = 1$. $P(n+1)$ est vraie.

   $\boxed{\text{On a ainsi montré par récurrence que } \forall n \in \mathbb{N} \quad f\left(\dfrac{a}{2^n}\right) = 1}$ **(2 pts)**

$\dfrac{a}{2^n} \underset{n\to+\infty}{\longrightarrow} 0$ et f est continue, donc $f\left(\dfrac{a}{2^n}\right) \underset{n\to+\infty}{\longrightarrow} f(0)$

D'autre part, $f\left(\dfrac{a}{2^n}\right) = 1 \underset{n\to+\infty}{\longrightarrow} 1$

Par unicité de la limite, on déduit que $f(0) = 1$.

D'après la question b, $\boxed{f \text{ est constante}}$ **(1 pt)**

(d) S'il existe $a \in \mathbb{R}$ tel que $f(a) = -1$, la fonction $-f$ vérifie l'équation fonctionnelle, est continue et $-f(a) = 1$, donc d'après la question précédente, $-f$ est constante et ainsi f **est constante.** **(1.25 pt)**

3. (a) Soit $x \in \mathbb{R}$. On a : $\Big(1 + f(x)f(-x)\Big) \times f(0) = f(x) + f(-x)$.

Comme $f(0) = 0$, on obtient $f(x) + f(-x) = 0$, d'où $f(-x) = -f(x)$: $\boxed{f \text{ est impaire}}$ **(1 pt)**

(b) Supposons que par l'absurde que $f(x) \geq 1$.

$f(0) = 0$ et f est continue sur $\mathbb{R}$.

Donc d'après le théorème des valeurs intermédiaires, il existe $a \in \mathbb{R}$ tel que $f(a) = 1$.

D'après la question 2c, f est constante. **Contradiction.**

Par conséquent, $f(x) < 1$.

On montre de même que $f(x) > -11$.

$\boxed{\text{Ainsi, } \forall x \in \mathbb{R} \quad f(x) \in]-1, 1[}$ **(1.5 pt)**

(c) Soit $x \in \mathbb{R}$.

Soit $\mathcal{P}_n$: $\dfrac{1 + f(nx)}{1 - f(nx)} = \left(\dfrac{1 + f(x)}{1 - f(x)}\right)^n$

$\mathcal{P}_0$ est vraie.

Supposons $\mathcal{P}_n$ vraie pour un entier $n \geq 0$.

Comme $f((n+1)x) = \dfrac{f(nx) + f(x)}{1 + f(nx)f(x)}$ (équation fonctionnelle), on a :

$$\frac{1 + f((n+1)x)}{1 - f((n+1)x)} = \frac{1 + \frac{f(nx)+f(x)}{1+f(nx)f(x)}}{1 - \frac{f(nx)+f(x)}{1+f(nx)f(x)}} = \frac{1 + f(nx)f(x) + f(nx) + f(x)}{1 + f(nx)f(x) - f(nx) - f(x)}$$

$$= \frac{\Big(1 + f(nx)\Big)\Big(1 + f(x)\Big)}{\Big(1 - f(nx)\Big)\Big(1 - f(x)\Big)} = \left(\frac{1 + f(x)}{1 - f(x)}\right)^n \times \left(\frac{1 + f(x)}{1 - f(x)}\right) \text{ d'après } P(n)$$

Ainsi, $\dfrac{1 + f((n+1)x)}{1 - f((n+1)x)} = \left(\dfrac{1 + f(x)}{1 - f(x)}\right)^{n+1}$: $P(n+1)$ est vraie.

$$\boxed{\forall x \in \mathbb{R} \quad \forall n \in \mathbb{N} \quad \frac{1 + f(nx)}{1 - f(nx)} = \left(\frac{1 + f(x)}{1 - f(x)}\right)^n}$$ **(2 pts)**

(d) Notons que $b > 0$ (car $f(1) \in]-1, 1[$).

Avec $x = 1$, la relation précédente donne $\dfrac{1 + f(n)}{1 - f(n)} = b^n$ puis $(b^n + 1)f(n) = b^n - 1$.

$\boxed{\text{Ainsi, } \forall n \in \mathbb{N} \quad f(n) = \dfrac{b^n - 1}{b^n + 1}}$ **(1 pt)**

(e) Soit $r \in \mathbb{Q}^+$. On pose $r = \dfrac{p}{q}$ avec $p \in \mathbb{N}$ et $q \in \mathbb{N}^*$.

On applique l'égalité de la question c à $n = q$ et $x = \dfrac{p}{q}$:

$$\frac{1 + f(q\frac{p}{q})}{1 - f(q\frac{p}{q})} = \left(\frac{1 + f(\frac{p}{q})}{1 - f(\frac{p}{q})}\right)^q \qquad \text{c'est-à-dire} \quad \frac{1 + f(p)}{1 - f(p)} = \left(\frac{1 + f(\frac{p}{q})}{1 - f(\frac{p}{q})}\right)^q$$

D'où $\dfrac{1 + f(\frac{p}{q})}{1 - f(\frac{p}{q})} = \left(\dfrac{1 + f(p)}{1 - f(p)}\right)^{1/q} = (b^p)^{1/q} = b^{p/q} = b^r$

On obtient alors : $1 + f(r) = b^r(1 - f(r))$, puis $(b^r + 1)f(r) = b^r - 1$

$\boxed{\text{On en déduit } \forall r \in \mathbb{Q}^+ \quad f(r) = \frac{b^r - 1}{b^r + 1}}$ **(2 pts)**

(f) Soit $r \in \mathbb{Q}^+$. On a : $b^r = e^{r\ln(b)}$.

En posant $k = \dfrac{\ln(b)}{2}$, on a : $b^r = e^{2kr}$, d'où $f(r) = \dfrac{b^r - 1}{b^r + 1} = \dfrac{e^{2kr}-1}{e^{2kr}+1} = \mathrm{th}(kr)$.

Les fonctions f et th étant impaires, cette dernière relation s'étend à $\mathbb{Q}$.

$\boxed{\text{Ainsi, pour } k = \dfrac{\ln(b)}{2}, \text{ on a } \forall r \in \mathbb{Q} \quad f(r) = \mathrm{th}(kr)}$ **(1.5 pt)**

Soit $x \in \mathbb{R}$.

$\mathbb{Q}$ est dense dans $\mathbb{R}$: il existe une suite $(r_n)_{n\geq 0}$ de rationnels qui converge vers x.

$$\left.\begin{array}{l} r_n \underset{n\to+\infty}{\longrightarrow} x \\ \\ f(t) \underset{t\to x}{\longrightarrow} f(x) \\ \text{(car } f \text{ est continue)} \end{array}\right\} \text{ donc } f(r_n) \underset{n\to+\infty}{\longrightarrow} f(x).$$

D'autre part, $f(r_n) = \mathrm{th}(kr_n) \underset{n\to+\infty}{\longrightarrow} \mathrm{th}(kx)$ par continuité de la fonction th.

Par unicité de la limite, $\boxed{\text{on déduit : } f(x) = \mathrm{th}(kx)}$ **(1.5 pt)**

4. Réciproquement, on vérifie aisément que pour $k \in \mathbb{R}$, la fonction $f : x \mapsto \mathrm{th}(kx)$ est continue et satisfait l'équation fonctionnelle, donc appartient à E.

   En effet, pour $(x, y) \in \mathbb{R}^2$, $\mathrm{th}(kx + ky) = \dfrac{\mathrm{sh}(kx+ky)}{\mathrm{ch}(kx+ky)} = \dfrac{\mathrm{sh}(kx)\mathrm{ch}(ky) + \mathrm{ch}(kx)\mathrm{sh}(ky)}{\mathrm{ch}(kx)\mathrm{ch}(ky) + \mathrm{sh}(kx)\mathrm{sh}(ky)}$

   En divisant par $\mathrm{ch}(kx)\mathrm{ch}(ky)$, on obtient : $\mathrm{th}(kx+ky) = \dfrac{\mathrm{th}(kx) + \mathrm{th}(ky)}{1 + \mathrm{th}(kx)\mathrm{th}(ky)}$

   $\boxed{\text{Les éléments de } E \text{ sont donc les fonctions } x \mapsto \mathrm{th}(kx) \text{ (avec } k \in \mathbb{R}) \text{ et les fonctions constantes } x \mapsto 1 \text{ et } x \mapsto -1 \quad \textbf{(2 pts)}}$

Exercice 2 : algèbre (8.5 points)

1. $I \in \mathcal{H}$

   Soient $M = aI + bJ$ et $M' = a'I + b'J$ deux éléments de $\mathcal{H}$ (où a, b, a' et b' sont des réels).

   Alors $M - M' = (a - a')I + (b - b')J$, donc $M - M' \in \mathcal{H}$.

   Et $MM' = (aI + bJ)(a'I + b'J) = aa'I + (ab' + ba')J + bb'J^2$

   On vérifie que $J^2 = 0$, d'où $MM' = aa'I + (ab' + ba')J$, par conséquent, $MM' \in \mathcal{H}$.

   De plus, $M'M = a'aI + (a'b + b'a)J = MM'$.

   $\boxed{\text{Ainsi, } (\mathcal{H}, +, \times) \text{ est un sous-anneau commutatif de } (\mathcal{M}_2(\mathbb{R}), +, \times)}$ **(2 pts)**

2. Comme les matrices I et J commutent, on a d'après la formule du binôme :

   $M^n = \displaystyle\sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k I^{n-k} J^k$

   Or pour $k \geq 2$, $J^k = 0$.

   $\boxed{\text{Par conséquent, } M^n = a^nI + na^{n-1}bJ = \begin{pmatrix} a^n + na^{n-1}b & na^{n-1}b \\ -na^{n-1}b & a^n - na^{n-1}b \end{pmatrix}}$ **(2 pts)**

3. <u>**Analyse :**</u> supposons $M = \begin{pmatrix} a+b & b \\ -b & a-b \end{pmatrix}$ inversible.

   Alors il existe $N = \begin{pmatrix} a'+b' & b' \\ -b' & a'-b' \end{pmatrix}$ tel que $MN = I$.

   D'après la question 1, $MN = \begin{pmatrix} aa' + ab' + ba' & ab' + ba' \\ -(ab' + ba') & aa' - (ab' + ba') \end{pmatrix}$.

   On en déduit dans un premier temps que : $ab' + ba' = 0$ (*en identifiant le coefficient de position* $(1, 2)$ *des matrices* MN *et* I)

   D'où $MN = \begin{pmatrix} aa' & 0 \\ 0 & aa' \end{pmatrix}$.

   Par conséquent, $aa' = 1$.

   Nécessairement, $a \neq 0$.

   On a ainsi montré que si $M = \begin{pmatrix} a+b & b \\ -b & a-b \end{pmatrix}$ est inversible, alors $a \neq 0$.

Synthèse : supposons $M = \begin{pmatrix} a+b & b \\ -b & a-b \end{pmatrix}$ avec $a \neq 0$.

On pose $N = \frac{1}{a}I - \frac{b}{a^2}J$.

On a : $MN = \left(aI + bJ\right)\left(\frac{1}{a}I - \frac{b}{a^2}J\right) = I + \left(-\frac{b}{a} + \frac{b}{a}\right)J = I$

Ce qui prouve que M est bien inversible.

Conclusion : les éléments inversibles de $\mathcal{H}$ sont les matrices $M = \begin{pmatrix} a+b & b \\ -b & a-b \end{pmatrix}$ avec $a \neq 0$

(2.75 pts)

4. Si $M = aI + bJ$ est un diviseur de zéro, alors il existe une matrice N non nulle de $\mathcal{H}$ telle que $MN = 0$.
   M n'est pas inversible (car sinon, en multipliant par M^{-1} à gauche la relation $MN = 0$, on obtiendrait $N = 0$)
   On en déduit que $a = 0$ (car d'après la question précédente, on a l'implication : M inversible $\Longrightarrow a \neq 0$)
   D'où $M = bJ$ avec $b \neq 0$.

   Réciproquement, si $M = bJ$ avec $b \neq 0$, alors $M^2 = b^2J^2 = 0$
   Donc M est un diviseur de zéro.

Conclusion : les diviseurs de zéro de l'anneau $\mathcal{H}$ sont les matrices $M = \begin{pmatrix} b & b \\ -b & -b \end{pmatrix}$ avec $b \neq 0$

(1.75 pt)

Exercice 3 : arithmétique (6 points)

1. Notons $d = (2n+1) \wedge (n^2)$ le pgcd de $2n+1$ et n^2.
   d divise $2n+1$ et n^2, donc d divise la combinaison linéaire $n \times (2n+1) - 2 \times n^2 = n$.
   Puis d divise la combinaison $(2n+1) - 2 \times n$.
   d est un diviseur positif de 1, donc $d = 1$.

Les entiers $2n+1$ et n^2 sont premiers entre eux

   1 pt

   Autre solution : $4 \times n^2 - (2n-1) \times (2n+1) = 1$.
   Il existe donc un couple $(u, v) \in \mathbb{Z}^2$ tel que $un^2 + v(2n+1) = 1$.
   D'après le théorème de Bézout, n^2 et $2n+1$ sont premiers entre eux.

2. (a) On a : $px = y^2 - x^2$, donc $px = (y-x)(y+x)$.
   p divise le produit $(y-x)(y+x)$.
   Et p est un nombre premier, donc est premier avec tous les nombres qu'il ne divise pas.
   Par conséquent, p divise au moins l'un des deux facteurs : $y - x$ ou $y + x$.
   Si p ne divise pas le premier facteur, alors il est premier avec lui, et donc divise l'autre facteur par le théorème de Gauss

p divise $y - x$ ou p divise $y + x$

   0.75 pt

   (b) Supposons que p divise $y - x$. Il existe donc $q \in \mathbb{Z}$ tel que $y - x = pq$.
   Comme $px \geq 0$, on a alors $y^2 = x^2 + px \geq x^2$, et donc $y \geq x$.
   On en déduit que $q \geq 0$.
   On reprend la relation : $(y-x)(y+x) = px$
   En remplaçant y par $x + pq$, on obtient : $pq(2x + pq) = px$.
   Ce qui donne après simplification par p (qui est non nul) : $2qx + pq^2 = x$
   Puis $pq^2 = x(1 - 2q)$.
   Comme pq^2 est positif, les entiers x et $1 - 2q$ ont le même signe. Par conséquent, $1 - 2q \geq 0$.
   q est un entier naturel vérifiant $q \leq \frac{1}{2}$, donc $q = 0$, puis $x = pq^2 = 0$ et enfin $y = x^2 + px = 0$.

On a montré que si p divise $y - x$, alors $x = 0$ et $y = 0$

   1.5 pt

   (c) On reprend la relation : $(y+x)(y-x) = px$
   En remplaçant y par $pk - x$, on obtient : $pk(pk - 2x) = px$.
   Ce qui donne après simplification par p (qui est non nul) : $pk^2 - 2kx = x$
   Puis $pk^2 = x(1 + 2k)$.
   $2k + 1$ divise le produit pk^2 et est premier avec k^2 d'après le résultat préliminaire,
   Le théorème de Gauss permet de déduire que $2k + 1$ divise p.
   D'où $2k + 1 = 1$ ou $2k + 1 = p$ (car p étant premier n'a que deux diviseurs positifs)
   Cas 1 : $2k + 1 = 1$
   On obtient alors $k = 0$, puis $x = pk^2 = 0$ et enfin $y = 0$

Cas 2 : $2k+1=p$

On obtient alors $k=\dfrac{p-1}{2}$ (qui est bien un entier car $p-1$ est pair)

Puis $x=k^2=\left(\dfrac{p-1}{2}\right)^2$ et $y=pk-x=\dfrac{p-1}{2}\left(p-\dfrac{p-1}{2}\right)=\dfrac{(p-1)(p+1)}{4}$ **2 pts**

3. Réciproquement, on vérifie que les couples $(0,0)$ et $\left(\left(\dfrac{p-1}{2}\right)^2, \dfrac{(p-1)(p+1)}{4}\right)$ sont solutions de l'équation.

   Supposons que $x=\left(\dfrac{p-1}{2}\right)^2$ et $y=\dfrac{(p-1)(p+1)}{4}$

   Comme p est impair, $\dfrac{p-1}{2}$ et $\dfrac{p+1}{2}$ sont bien des entiers, donc $x\in\mathbb{N}$ et $y\in\mathbb{N}$.

   $x^2+px=x(x+p)$ et $x+p=\left(\dfrac{p-1}{2}\right)^2+p=\dfrac{p^2-2p+1}{4}+p=\dfrac{p^2+2p+1}{4}=\left(\dfrac{p+1}{2}\right)^2$

   On a donc : $x^2+px=\left(\dfrac{p-1}{2}\right)^2\left(\dfrac{p+1}{2}\right)^2=y^2$

   $\boxed{\text{L'ensemble des solutions de l'équation est } \left\{(0,0), \left(\dfrac{(p-1)^2}{4}, \dfrac{(p-1)(p+1)}{4}\right)\right\}}$ **0.75 pt**

   Remarque : dans le cas où $p=2$, l'équation n'a qu'une seule solution, le couple $(0,0)$.

Exercice 4 : arithmétique (12.5 points)

1. Soit $n\in\mathcal{E}$.

   Supposons n pair.

   Alors 2 divise n, et n divise 2^n+1, donc 2 divise 2^n+1 (*par transitivité*).

   Comme $n\geq 1$, 2 divise 2^n.

   Par conséquent, 2 divise $(2^n+1)-2^n=1$. **Contradiction**.

   $\boxed{\text{Ainsi, tout élément de } \mathcal{E} \text{ est impair}}$ **(1.25 pt)**

2. Soit $P(k)$: « 3^k appartient à $\mathcal{E}$ »

   1 divise 2^1+1, donc $P(0)$ est vraie.

   3 divise 2^3+1, donc $P(1)$ est vraie.

   Supposons $P(k)$ vraie pour un entier $k\geq 1$.

   $2^{3^{k+1}}+1=2^{3^k\times 3}+1=(2^{3^k})^3+1=(2^{3^k}+1)(4^{3^k}-2^{3^k}+1)$

   D'après $P(k)$, $2^{3^k}+1$ est un multiple de 3^k.

   Il reste à montrer que $4^{3^k}-2^{3^k}+1$ est un multiple de 3.

   Or d'après $P(k)$, $2^{3^k}+1$ est un multiple de 3^k, donc est un multiple de 3.

   D'où : $2^{3^k}\equiv -1\ [3]$.

   Et $4^{3^k}\equiv 1\ [3]$.

   Par conséquent, $4^{3^k}-2^{3^k}+1\equiv 0\ [3]$.

   On peut ainsi déduire que $2^{3^{k+1}}+1$ est un multiple de 3^{k+1} : $P(k+1)$ est vraie.

   $\boxed{\text{On a ainsi montré que pour tout } k\in\mathbb{N}, \text{ le nombre } 3^k \text{ appartient à } \mathcal{E}}$ **(2 pts)**

3. (a) Comme n est impair, p est impair, et donc $p-1$ est pair.

   On peut écrire : $p-1=2q$ avec $q\in\mathbb{N}^*$.

   Comme p est le plus petit diviseur premier de n, alors n et $p-1$ n'ont pas de diviseur commun autre que 1 (*sinon n aurait un diviseur premier strictement plus petit que p*).

   n et $p-1$ sont donc premiers entre eux.

   n est alors premier avec le diviseur q de $p-1$.

   $\boxed{\text{On a ainsi : } (2n)\wedge(p-1)=(2n)\wedge(2q)=2\times(n\wedge q)=2}$ **(2 pts)**

   (b) p est un nombre premier, et 2 est premier avec p.

   Donc d'après le petit théorème de Fermat, $2^{p-1}\equiv 1\ [p]$

   $\boxed{\text{Ainsi, } p-1 \text{ appartient à } A}$ **(0.75 pt)**

   p divise n, et n divise 2^n+1, donc p divise 2^n+1.

   Par conséquent, $2^n\equiv -1\ [p]$

   D'où $(2^n)^2\equiv 1\ [p]$, ce qui donne : $2^{2n}\equiv 1\ [p]$

   $\boxed{\text{Ainsi, } 2n \text{ appartient à } A}$ **(0.75 pt)**

(c) A est une partie non vide de $\mathbb{N}$, $\boxed{\text{donc } A \text{ possède un plus petit élément } a}$ **(0.25 pt)**

(d) Supposons que k appartienne à A : $2^k \equiv 1 \; [p]$

Effectuons la division euclidienne de k par a : $k = aq + r$ avec $0 \leq r < a$.
On a alors : $2^k = (2^a)^q \times 2^r$.
Comme a est un élément de A, on a : $2^a \equiv 1 \; [p]$
Par hypothèse, $2^k \equiv 1 \; [p]$

$$(2^a)^q \times 2^r \equiv 1 \; [p]$$
$$2^r \equiv 1 \; [p]$$

Si r était non nul, alors r serait un élément de A, ce qui est exclu car $r < a$.
On en déduit que $r = 0$. Donc $k = aq$ est un multiple de a.

$\boxed{\text{On a montré que si } k \in A, \text{ alors } k \text{ est un multiple de } a}$ **(2 pts)**

(e) a divise tout élément de A, donc a divise les nombres $2n$ et $p-1$.
a divise donc leur PGCD : a divise 2 (en utilisant le résultat de la question a).
Comme $1 \notin A$, $\boxed{\text{on en déduit que } a = 2}$ **(0.75 pt)**

p divise $2^a - 1$, donc p divise 3.
$\boxed{\text{Par conséquent, } p = 3}$ **(0.25 pt)**

4. (a) Supposons que $n \in \mathcal{E}$ (ie n divise $2^n + 1$).
On peut écrire : $2^n + 1 = nq$ avec $q \in \mathbb{N}^*$.
Comme $2^n + 1$ est impair, q est impair.
Par conséquent, $(-1)^q = -1$.

D'où : $2^{2^n+1} + 1 = 2^{nq} + 1 = (2^n)^q - (-1)^q = \left(2^n + 1\right) \sum_{k=0}^{q-1} (-1)^k (2^n)^{q-1-k}$

On a ici utilisé l'identité remarquable $a^q - b^q = (a-b) \sum_{k=0}^{q-1} a^{q-k-1} b^k$

Ce qui prouve que $2^{2^n+1} + 1$ est un multiple de $2^n + 1$.
$\boxed{\text{On a montré que si } n \in \mathcal{E}, \text{ alors } 2^n + 1 \in \mathcal{E}}$ **(2 pts)**

(b) 9 appartient à $\mathcal{E}$, donc d'après ce qui précède, le nombre $2^9 + 1 = 513$ appartient à $\mathcal{E}$ (et ce n'est pas une puissance de 3). **(0.5 pt)**
