Devoir Maison 8

un corrigé

Exercice 1 (suite implicite).

1. Soit $n \in \mathbb{N}^*$. La fonction f_n est deux fois dérivable sur $\mathbb{R}$ comme somme et inverse de fonctions qui le sont et pour tout $x \in \mathbb{R}$,

$$f_n'(x) = -\frac{\mathrm{e}^x}{(1+\mathrm{e}^x)^2} + n$$

puis :

$$\begin{aligned} f_n''(x) = -\frac{\mathrm{e}^x(1+\mathrm{e}^x)^2 - 2\,\mathrm{e}^x \times \mathrm{e}^x(1+\mathrm{e}^x)}{(1+\mathrm{e}^x)^4} &= -\frac{(1+\mathrm{e}^x)(\mathrm{e}^x + \mathrm{e}^{2x} - 2\mathrm{e}^{2x})}{(1+\mathrm{e}^x)^4} \\ &= \frac{\mathrm{e}^{2x} - \mathrm{e}^x}{(1+\mathrm{e}^x)^3} \\ &= \frac{\mathrm{e}^x}{(1+\mathrm{e}^x)^3}(\mathrm{e}^x - 1) \end{aligned}$$

Pour tout $x \in \mathbb{R}$, on a $\dfrac{\mathrm{e}^x}{(1+\mathrm{e}^x)^3} > 0$ (comme quotient de nombres strictement positifs) et :

$$\mathrm{e}^x - 1 > 0 \iff \mathrm{e}^x > 1 \iff x > 0$$

par stricte croissance de la fonction ln sur $\mathbb{R}_+^*$. On en déduit les tableaux de signes et de variations suivants (les limites de f_n' et f_n en $+\infty$ et $-\infty$ sont immédiates et $n - \frac{1}{4} > 0$ puisque $n \geqslant 1$ par hypothèse) :

x	$-\infty$		0		$+\infty$
$f_n''(x)$		$-$	0	$+$	
f_n'	n	$\searrow$	$n - \frac{1}{4} > 0$	$\nearrow$	n
$f_n'(x)$			$+$		
f_n	$-\infty$		$\nearrow$		$+\infty$

Concernant les limites de f_n sur $\mathbb{R}$, on a en effet $\lim\limits_{x \to -\infty} (1+\mathrm{e}^x) = 1$ et $\lim\limits_{x \to +\infty} (1+\mathrm{e}^x) = +\infty$ tandis que $\lim\limits_{x \to \pm\infty} nx = \pm\infty$, d'où les limites annoncées d'après les propriétés sur les quotients et sommes de limites.

Pour tout $x \in \mathbb{R}$, on a $f_n'(x) \geqslant n - \dfrac{1}{4} > 0$ donc :

$$\boxed{\text{la fonction } f_n \text{ est } \textit{strictement} \text{ croissante sur } \mathbb{R}}$$

2. Soit $n \in \mathbb{N}^*$. La fonction f_n est continue (car dérivable) et strictement croissante sur $\mathbb{R}$ (d'après la question 1.). D'après le théorème de la bijection, la fonction f_n réalise donc une bijection de $\mathbb{R}$ sur l'intervalle :

$$f_n(\mathbb{R}) = \left] \lim_{x \to -\infty} f_n(x), \lim_{x \to +\infty} f_n(x) \right[=]-\infty, +\infty[= \mathbb{R}$$

Comme $0 \in f_n(\mathbb{R})$, l'équation $f_n(x) = 0$ admet bien une unique solution dans $\mathbb{R}$. Ainsi :

$$\boxed{\text{pour tout } n \in \mathbb{N}^*, \text{ il existe un unique nombre réel } u_n \text{ tel que } f_n(u_n) = 0}$$

3. Soit $n \in \mathbb{N}^*$. Alors :

$$f_n\left(-\frac{1}{n}\right) = \frac{1}{1 + \mathrm{e}^{-\frac{1}{n}}} - 1$$

Or $\mathrm{e}^{-\frac{1}{n}} > 0$ puis $1 + \mathrm{e}^{-\frac{1}{n}} > 1$ et donc, comme la fonction inverse est strictement décroissante sur $\mathbb{R}_+^*$, on a $\dfrac{1}{1 + \mathrm{e}^{-\frac{1}{n}}} < 1$ ce qui implique que $f_n\left(-\dfrac{1}{n}\right) < 0$. Par ailleurs :

$$f_n(0) = \frac{1}{1 + \mathrm{e}^0} = \frac{1}{2} > 0$$

On en déduit donc que $f_n\left(-\dfrac{1}{n}\right) < f_n(u_n) < f_n(0)$ (puisque $f_n(u_n) = 0$ par définition de u_n). Or la fonction f_n est strictement croissante sur $\mathbb{R}$ et $-\dfrac{1}{n}, u_n, 0 \in \mathbb{R}$ donc on peut conclure que :

$$\boxed{-\frac{1}{n} < u_n < 0}$$

4. Soit $n \in \mathbb{N}^*$. Pour tout $x \in \mathbb{R}_-$, on a :

$$f_{n+1}(x) - f_n(x) = \frac{1}{1 + \mathrm{e}^x} + (n+1)x - \left(\frac{1}{1 + \mathrm{e}^x} + nx\right) = x \leqslant 0$$

puisque $x \in \mathbb{R}_-$. En évaluant cette inégalité en u_n on a, puisque $u_n \leqslant 0$ (d'après la question 3.) :

$$f_{n+1}(u_n) - f_n(u_n) \leqslant 0 \qquad \text{c'est-à-dire} \qquad f_{n+1}(u_n) \leqslant 0$$

car $f_n(u_n) = 0$ par définition de u_n. Or on a aussi $f_{n+1}(u_{n+1}) = 0$ (par définition de u_{n+1}) donc :

$$\boxed{f_{n+1}(u_n) \leqslant f_{n+1}(u_{n+1})}$$

On sait par ailleurs que la fonction f_{n+1} est strictement croissante sur $\mathbb{R}$ et $u_n, u_{n+1} \in \mathbb{R}$ donc on a l'inégalité $u_n \leqslant u_{n+1}$. Ainsi, la suite $(u_n)_{n \geqslant 1}$ est croissante. De plus, cette suite est majorée par 0 d'après la question 3. Le théorème de la limite monotone permet alors de conclure que :

$$\boxed{\text{la suite } (u_n)_{n \geqslant 1} \text{ est convergente}}$$

5. On sait que pour tout $n \in \mathbb{N}^*$,on a $-\dfrac{1}{n} \leqslant u_n \leqslant 0$. Or :

$$\lim_{n \to +\infty} -\frac{1}{n} = \lim_{n \to +\infty} 0 = 0$$

donc, d'après le théorème des gendarmes :

$$\boxed{\text{la suite } (u_n)_{n \geqslant 0} \text{ est convergente de limite } 0}$$

6. Soit $n \in \mathbb{N}^*$. On sait que $f_n(u_n) = 0$ donc :

$$\frac{1}{1 + \mathrm{e}^{u_n}} + nu_n = 0 \qquad \text{et donc} \qquad nu_n = -\frac{1}{1 + \mathrm{e}^{u_n}} \tag{1}$$

D'après la question 6., la suite $(u_n)_{n \geqslant 1}$ est convergente de limite 0 donc (par composition des limites et continuité de la fonction exponentielle en 0) :

$$\lim_{n \to +\infty} -\frac{1}{1 + \mathrm{e}^{u_n}} = -\frac{1}{2}$$

On déduit de (1) la limite demandée :

$$\boxed{nu_n \xrightarrow[n \to +\infty]{} -\frac{1}{2}}$$

Exercice 2 (nombres de Fermat).

1. (a) On raisonne par l'absurde. Si a est impair, alors $a \equiv 1\,[2]$ donc $a^n \equiv 1\,[2]$ puis $a^n+1 \equiv 0\,[2]$. Ainsi, a^n+1 est un entier naturel pair et comme $a > 1$, on a $a^n + 1 > 2$. Or 2 est le seul nombre premier pair ; on obtient donc une absurdité. Finalement :

$$\boxed{a \text{ est pair}}$$

(b) Comme m est impair, on a $(-1)^m = -1$ et :

$$a^n + 1 = a^{km} - (-1)^m = (a^k)^m - (-1)^m = (a^k+1)\sum_{\ell=0}^{m-1} a^\ell (-1)^{m-1-\ell}$$

Or $\displaystyle\sum_{\ell=0}^{m-1} a^\ell(-1)^{m-1-\ell}$ est un entier (car est une somme d'entiers) donc, par définition de la divisibilité :

$$\boxed{a^k+1 \text{ divise } a^m+1}$$

Poursuivons le raisonnement : on sait que a^n+1 est un nombre premier et que a^k+1 divise a^n+1. Par conséquent, $a^k+1 \in \{1, a^n+1\}$. Or $a^k+1 > 1$ (car $a>1$) donc $a^k+1 = a^n+1$, ce qui implique que $a^k = a^n$ puis que $k = n$ (par injectivité de $x \longmapsto a^x$ sur $\mathbb{R}$).

(c) D'après la question précédente, le nombre n n'admet pas de diviseur impair (positif) différent de 1. En particulier, le seul nombre premier pouvant diviser n est 2. Or tout entier naturel supérieur ou égal à 2 est un produit de nombres premiers (d'après le théorème fondamental de l'arithmétique) donc on peut conclure que :

$$\boxed{\text{l'entier } n \text{ est une puissance de 2 } (\textit{i.e.} : \exists\,\ell \in \mathbb{N},\ n = 2^\ell)}$$

2. (a) Soit $n \in \mathbb{N}$. On a :

$$(F_n-1)^2+1 = \left(2^{2^n}\right)^2 + 1 = 2^{2^n\times 2}+1 = 2^{2^{n+1}}+1 = F_{n+1}$$

Ainsi :

$$\boxed{\forall n \in \mathbb{N}, \qquad F_{n+1} = (F_n-1)^2+1}$$

(b) On utilise un raisonnement par récurrence.

- ⋆ On a $F_1 = 2^2+1 = 5$ et :

$$\prod_{k=0}^{0} F_k = F_0 = 2^1+1 = 3 = F_1 - 2$$

donc l'égalité est vraie pour $n=1$.

- ⋆ Soit $n \in \mathbb{N}^*$. On suppose que $F_n - 2 = \displaystyle\prod_{k=0}^{n-1} F_k$. Montrons que $F_{n+1} - 2 = \displaystyle\prod_{k=0}^{n} F_k$. On utilise la question précédente :

$$\begin{aligned} F_{n+1}-2 = (F_n-1)^2 - 1 = F_n(F_n-2) &= F_n \times \prod_{k=0}^{n-1} F_k \qquad \text{(hypothèse de récurrence)} \\ &= \prod_{k=0}^{n} F_k \end{aligned}$$

donc l'égalité est vraie au rang n.

Par principe de récurrence simple, on peut conclure que :

$$\boxed{\forall n \in \mathbb{N}^*, \qquad F_n - 2 = \prod_{k=0}^{n-1} F_k}$$

(c) Soit $m, n \in \mathbb{N}$ tel que $m < n$. Par définition du PGCD, le nombre $F_m \wedge F_n$ divise F_m et F_n. Comme $m \in [\![0, n-1]\!]$, on a $F_m \in \{F_0, \dots, F_{n-1}\}$ donc $F_m \wedge F_n$ divise $\displaystyle\prod_{k=0}^{n-1} F_k$. Ainsi, $F_m \wedge F_n$ divise $F_n - \displaystyle\prod_{k=0}^{n-1} F_k$, c'est-à-dire $F_m \wedge F_n$ divise 2 (d'après la formule démontrée à la question précédente), c'est-à-dire $F_m \wedge F_n \in \{1, 2\}$. Or F_m et F_n sont des entiers impairs donc $F_m \wedge F_n$ est impair. Ainsi :

$$\boxed{F_m \wedge F_n = 1}$$

3. (a) On sait que p divise F_n, c'est-à-dire p divise $2^{2^n}+1$. Autrement dit, $2^{2^n} \equiv -1\,[p]$ et donc, en élément au carré :

$$\left(2^{2^n}\right)^2 \equiv 1\,[p] \qquad \text{c'est-à-dire} \qquad 2^{2^{n+1}} \equiv 1\,[p]$$

Par ailleurs, on a bien $2^{n+1} \in \mathbb{N}^*$ donc :

$$\boxed{2^{n+1} \in A}$$

(b) L'ensemble A est une partie de $\mathbb{N}$ (par définition) qui est non vide (elle contient 2^{n+1}) donc :

$$\boxed{A \text{ admet un minimum (noté } m)}$$

(c) On sait que m est un entier naturel non nul (en effet, m appartient à A donc en particulier à $\mathbb{N}^*$). D'après le théorème de la division euclidienne, il existe $q \in \mathbb{Z}$ et $r \in [\![0, m-1]\!]$ tels que $2^{n+1} = qm+r$. Comme $2^{n+1} \in \mathbb{N}$ et $m \in \mathbb{N}$, on a $q \in \mathbb{N}$. De plus :

$$2^{2^{n+1}} = (2^m)^q \times 2^r$$

On sait que $2^{2^{n+1}} \equiv 1\,[p]$ (question 3.(a)) et $2^m \equiv 1\,[p]$ (par définition de m) donc l'égalité précédente implique que $2^r \equiv 1\,[p]$. Si $r \neq 0$, alors r est un élément de A strictement plus petit que m. Ceci contredit le caractère minimal de m donc $r = 0$. Finalement, $2^{n+1} = qm$, ce qui signifie que :

$$\boxed{m \text{ divise } 2^{n+1}}$$

(d) D'après la question 3.(c), l'entier m est une puissance de 2. Il existe donc un entier $\ell \in [\![0, n+1]\!]$ tel que $m = 2^\ell$, et il s'agit de montrer que $\ell = n+1$. Raisonnons par l'absurde en supposant que $\ell \leqslant n$. Par définition de m, on a $2^{2^\ell} \equiv 1\,[p]$, ce qui nous donne, en élevant à la puissance $2^{n-\ell}$, la congruence $2^{2^n} \equiv 1\,[p]$. Comme p divise F_n par hypothèse, on a aussi $2^{2^n} \equiv -1\,[p]$. Ainsi, $2 \equiv 0\,[p]$, ce qui signifie que 2 divise p. Or p est un nombre premier donc $p = 2$. Ceci n'est pas possible car on sait que F_n est un entier impair. Finalement :

$$\boxed{m = 2^{n+1}}$$

(e) Tout d'abord $p-1 \in \mathbb{N}^*$ (car $p \geqslant 2$). On sait que p est un nombre premier impair (car F_n est impair et p divise F_n) donc p ne divise pas 2. Ainsi, d'après le petit théorème de Fermat,

$$\boxed{2^{p-1} \equiv 1\,[p], \text{ ce qui signifie que } p-1 \text{ est un élément de } A}$$

(f) D'après le théorème de la division euclidienne, il existe $q \in \mathbb{N}$ et $r \in [\![0, m-1]\!]$ tels que $p-1 = mq+r$. Or $2^{p-1} \equiv 1\,[p]$ et $2^m \equiv 1\,[p]$ et $2^{p-1} = (2^m)^q \times 2^r$ donc $2^r \equiv 1\,[p]$. Comme $r < m$, la minimalité de m entraîne que $r = 0$. On en déduit donc que m divise $p-1$, c'est-à-dire $p - 1 \equiv 0\,[m]$, soit encore :

$$\boxed{p \equiv 1\,[2^{n+1}]}$$