DS 6
Analyse - Arithmétique
Correction

Simon Dauguet
simon.dauguet@gmail.com

Mercredi 29 Janvier 2025

On définie la fonction f par $f(x) = \frac{1}{1+x+x^2}$.

1. Préliminaires.

Soit $a \in \mathbb{R}$ et g définie sur $[a, +\infty[$ et dérivable sur $]a, +\infty[$. On suppose $g(a) = 0$ et $g(x) \xrightarrow[x\to+\infty]{} 0$.

1.(a) On pose, $\forall x \in [\arctan(a), \pi/2[$, $\varphi(x) = g(\tan(x))$.

On sait $\tan \in \mathcal{C}^\infty(]-\pi/2, \pi/2[, \mathbb{R})$. Or $\arctan : \mathbb{R} \to]-\pi/2, \pi/2[$. Donc $\arctan(a) \in]-\pi/2, \pi/2[$. Donc $\tan$ est en particulier $\mathcal{C}^\infty$ sur $[\arctan(a), \pi/2[$.

Par continuité de $\tan$ et par le TVI, on sait donc que $\tan([\arctan(a), \pi/2[)$ est intervalle. Comme $\tan$ est strictement croissante, par stricte monotonie, on sait que $\tan([\arctan(a), \pi/2[)$ est un intervalle de même type (donc semi ouvert) et la croissance nous donne en plus, grâce au théorème de la limite monotone, $\tan([\arctan(a), \pi/2[) = [\tan(\arctan(a)), \lim_{x\to\pi/2} \tan(x)[= [a, +\infty[$.

Donc $\tan \in \mathcal{C}^\infty([\arctan(a), \pi/2[, [a, +\infty[)$. Or $g \in \mathcal{D}^1([a, +\infty[, \mathbb{R})$, donc par composition, $\varphi \in \mathcal{D}^1([\arctan(a), \pi/2[)$.

En particulier, $\varphi \in \mathcal{C}^0([\arctan(a), \pi/2[, \mathbb{R})$. Mais, par composition dans les limites, $\varphi(x) = g(\tan(x)) \xrightarrow[x\to\pi/2]{} 0 = \varphi(\pi/2)$ car $g(x) \xrightarrow[x\to+\infty]{} 0$ par hypothèse. Donc φ est prolongeable par continuité en $\pi/2$ en posant $\varphi(\pi/2) = 0$.

On renomme alors

$$\begin{array}{rccc} & [\arctan(a), \pi/2] & \to & \mathbb{R} \\ \varphi : & x & \mapsto & \begin{cases} g(\tan(x)) & x \neq \pi/2 \\ 0 & x = \pi/2 \end{cases} \end{array}$$

Alors $\varphi \in \mathcal{C}^0([\arctan(a), \pi/2], \mathbb{R})$.

1.(b) D'après la question précédente, $\varphi \in \mathcal{C}^0([\arctan(a), \pi/2], \mathbb{R}) \cap \mathcal{D}^1(]\arctan(a), \pi/2[, \mathbb{R})$. Et

$$\varphi(a) = g(\tan(\arctan(a))) = g(a) = 0 = \varphi(\pi/2).$$

Donc, par le théorème de Rolle, $\exists c \in]\arctan(a), \pi/2[$ tel que $\varphi'(c) = 0$.

1.(c) Soit $c \in]\arctan(a), \pi/2[$ tel que $\varphi'(c) = 0$ (qui existe, d'après la question précédente). φ est dérivable sur $]\arctan(a), \pi/2[$ et $\forall x \in]\arctan(a), \pi/2[$, $\varphi'(x) = (1 + \tan(x)^2)g'(\tan(x))$. Donc $\varphi'(c) = 0 \iff (1 + \tan(c)^2)g'(\tan(c)) = 0 \iff g'(\tan(c)) = 0$ car $1 + \tan(c)^2 \neq 0$.

On pose alors $d = \tan(c)$. Donc $g'(d) = 0$. Et $c \in]\arctan(a), \pi/2[\implies d = \tan(c) \in]a, +\infty[$ par croissance de $\tan$.

2. Étude de f.

2.(a) Le discriminant du polynôme $1 + X + X^2$ est $\Delta = 1 - 4 = -3 < 0$. Donc le polynôme $1 + X + X^2$ n'a pas de racines réelles, *i.e.* $\forall x \in \mathbb{R}$, $1 + x + x^2 \neq 0$.

Donc f est l'inverse d'une fonction définie sur $\mathbb{R}$ qui ne s'annule pas, donc f est bien définie sur $\mathbb{R}$.

2.(b) Comme $x \mapsto 1+x+x^2 \in \mathcal{C}^\infty(\mathbb{R},\mathbb{R})$ en tant que fonction polynomiale et comme $\forall x \in \mathbb{R},\ 1+x+x^2 \neq 0$, on a donc $f \in \mathcal{C}^\infty(\mathbb{R},\mathbb{R})$.

Et $\forall x \in \mathbb{R},\ f'(x) = \frac{-1-2x}{(1+x+x^2)^2}$. Donc $\forall x \in \mathbb{R},\ (f'(x) \geq 0 \iff 1+2x \leq 0 \iff x \leq -1/2)$.

Et aussi, $\forall x \in \mathbb{R},\ f''(x) = -\frac{2(1+x+x^2)^2 - 2(1+2x)^2(1+x+x^2)}{(1+x+x^2)^4} = \frac{6x(1+x)}{(1+x+x^2)^3}$.

D'où le tableau de variations

x	$-\infty$		-1		$-\frac{1}{2}$		0		$+\infty$
$f''(x)$		$+$	0	$-$		$-$	0	$+$	
f'	0	↗	1	↘	0	↘	-1	↗	0
$f'(x)$		$+$		$+$	0	$-$		$-$	
f	0	↗		↗	$\frac{4}{3}$	↘		↘	0

2.(c) On considère la fonction g définie par $g(x) = f(x) - x$ pour tout $x \in \mathbb{R}$. Alors g est dérivable sur $\mathbb{R}$ en tant que combinaison linéaire d'applications dérivables et $\forall x \in \mathbb{R},\ g'(x) = f'(x) - 1$. D'après le tableau de variations précédente, $\forall x \in \mathbb{R},\ f'(x) \leq 1$. Donc $\forall x \in \mathbb{R},\ g'(x) \leq 0$. Donc g est décroissante sur $\mathbb{R}$.

En fait, on a même $\forall x \in \mathbb{R} \setminus \{-1\},\ f'(x) < 1$, donc $\forall x \neq -1,\ g'(x) < 0$. Donc g est strictement décroissante sur $\mathbb{R}$. Donc g est injective.

Par ailleurs, g est continue et $g(x) \xrightarrow[x\to-\infty]{} +\infty$ et $g(x) \xrightarrow[x\to+\infty]{} -\infty$ par linéarité de la limite. Donc $g(\mathbb{R}) = \mathbb{R}$. Donc $0 \in g(\mathbb{R})$, donc par définition, $\exists \alpha \in \mathbb{R}$, tel que $g(\alpha) = 0$.

Mais par injectivité de g, α est unique. Donc $\exists! \alpha \in \mathbb{R}$ tel que $g(\alpha) = 0$. Autrement dit, $\exists! \alpha \in \mathbb{R},\ f(\alpha) = \alpha$.

On notera que $g(1) = f(1) - 1 = 1/3 - 1 = -2/3 < 0$ et que $g(1/3) = f(1/3) - 1/3 = 9/13 - 1/3 = 14/39 > 0$. Donc, par décroissance de g, on en déduit $\alpha \in [1/3, 1]$.

2.(d) On sait que f' est continue sur $\mathbb{R}$. Donc en particulier sur $[1/3, 1]$. Par le théorème des bornes atteintes, f' est donc bornée et atteint ses bornes sur $[1/3, 1]$. Autrement dit, par le théorème des bornes atteintes, $\exists a \in [1/3, 1]$ tel que $\forall x \in [1/3, 1],\ |f'(x)| \leq |f'(a)|$. Et $f'(a) \neq 0$ car f' non constante.

Par ailleurs, d'après le tableau de variations précédents, f' est croissante sur $[1/3, 1]$ et $f'(1/3) = -135/169$ et $f'(1) = -1/3$. Donc $\forall x \in [1/3, 1],\ f'(x) \in [f'(1/3), f'(1)]$. Donc $\forall x \in [1/3, 1],\ |f'(x)| < 1$. Donc $\exists C \in]0, 1[$ (avec $C = |f'(a)|$) tel que $\forall x \in [1/3, 1],\ |f'(x)| \leq C$.

2.(e) On pose $u_0 = 1$ et $\forall n \in \mathbb{N},\ u_{n+1} = f(u_n)$.

Toujours d'après le tableau de variations précédent, f est décroissante sur $\mathbb{R}_+$, donc en particulier sur $[1/3, 1]$. Par continuité et décroissance, on a donc $f([1/3, 1]) \subset [f(1), f(1/3)] = [1/3, 9/13] \subset [1/3, 1]$. Donc l'intervalle $[1/3, 1]$ est intervalle stable par f.

Or $u_0 \in [1/3, 1]$. Donc la suite (u_n) est bien définie et $\forall n \in \mathbb{N},\ u_n \in [1/3, 1]$.

2.(f) D'après la question précédente, $\forall x \in [1/3, 1],\ |f'(x)| \leq C$. Or f est dérivable sur $[1/3, 1]$. Donc, par l'inégalité des accroissements finis, $\forall a, b \in [1/3, 1],\ |f(b) - f(a)| \leq C|b - a|$.

En particulier, $\forall n \in \mathbb{N},\ |u_{n+1} - \alpha| = |f(u_n) - f(\alpha)| \leq C|u_n - \alpha|$, car $\alpha \in [1/3, 1]$ d'après 2.(c).

On a évidemment, $|u_0 - \alpha| \leq C^0|u_0 - \alpha|$. Si $\exists n \in \mathbb{N}$ tel que $|u_n - \alpha| \leq C^n|u_0 - \alpha|$, alors $|u_{n+1} - \alpha| \leq C|u_n - \alpha| \leq C^{n+1}|u_0 - \alpha|$.

Donc, par principe de récurrence, on vient de montrer que $\forall n \in \mathbb{N},\ |u_n - \alpha| \leq C^n|u_0 - \alpha|$.

Mais $u_0 = 1$ et $\alpha \in [1/3, 1]$, donc $|u_0 - \alpha| = |1 - \alpha| \leq 2/3 \leq 1$. Donc finalement, $\forall n \in \mathbb{N},\ |u_n - \alpha| \leq C^n$.

Comme $C \in]0,1[$ d'après la question précédente, on a $C^n \xrightarrow[n\to+\infty]{} 0$ par convergence des suites géométriques. Donc, par un corollaire du théorème des gendarmes, $u_n \xrightarrow[n\to+\infty]{} \alpha$. Donc $(u_n)_{n\in\mathbb{N}}$ est une suite convergente vers α, le point fixe de f.

3. **Création d'une suite de polynômes.**

3.(a) f est de classe $\mathcal{C}^\infty$ en tant qu'inverse d'une fonction $\mathcal{C}^\infty$ qui ne s'annule pas sur $\mathbb{R}$.

On a déjà calculé $\forall x \in \mathbb{R},\ f'(x) = \frac{-1-2x}{(1+x+x^2)^2}$ et $f''(x) = \frac{6x(1+x)}{(1+x+x^2)^3}$. En posant donc $P_0(X) = 1$, $P_1(X) = -1-2X$ et $P_2(X) = 6X(1+X)$, on a donc $P_0, P_1, P_2 \in \mathbb{R}[X]$ et $\forall n \in \{0,1,2\},\ \forall x \in \mathbb{R},\ f^{(n)}(x) = \frac{\widetilde{P_n}(x)}{(1+x+x^2)^{n+1}}$.

On remarque également que $(1+X+X^2)P_0'(X) - (0+1)(2X+1)P_0(X) = -(1+2X) = P_1(X)$ et $(1+X+X^2)P_1'(X) - (1+1)(2X+1)P_1(X) = -2(1+X+X^2) + 2(2X+1)^2 = 6X^2+6X = 6X(X+1) = P_2(X)$.

Supposons maintenant que $\exists n \in \mathbb{N}$ tel que $\exists P_n \in \mathbb{R}[X]$ tel que $\forall x \in \mathbb{R},\ f^{(n)}(x) = \frac{\widetilde{P_n}(x)}{(1+x+x^2)^{n+1}}$. Alors :

$$\begin{aligned}\forall x \in \mathbb{R},\ f^{(n+1)}(x) &= \frac{\widetilde{P_n}'(x)(1+x+x^2)^{n+1} - (2x+1)(n+1)(1+x+x^2)^n\widetilde{P_n}(x)}{(1+x+x^2)^{2n+2}} \\ &= \frac{\widetilde{P_n}'(x)(1+x+x^2) - (n+1)(2x+1)\widetilde{P_n}(x)}{(1+x+x^2)^{n+2}}.\end{aligned}$$

On pose alors $P_{n+1}(X) = P_n'(X)(1+X+X^2) - (n+1)(2X+1)P_n(X)$. Alors $P_{n+1} \in \mathbb{R}[X]$ car $(\mathbb{R}[X],+,\times)$ est une anneau. Et de plus, $\forall x \in \mathbb{R},\ f^{(n+1)}(x) = \frac{\widetilde{P_{n+1}}(x)}{(1+x+x^2)^{n+2}}$.

Donc, par principe de récurrence, $\forall n \in \mathbb{N},\ \exists P_n \in \mathbb{R}[X]$ tq $\forall x \in \mathbb{R},\ f^{(n)}(x) = \frac{\widetilde{P_n}(x)}{(1+x+x^2)^{n+1}}$.

3.(b) La question précédente, montre que $\deg(P_n) = n$ et $\text{coeff dom}(P_n) = (-1)^n(n+1)!$ pour $n \in \{0,1,2\}$.

Supposons que $\exists n \in \mathbb{N}^*,\ \deg(P_n) = n$. Alors $\deg(P_n) = n-1$ car $n \geq 1$. Et donc $\deg((1+X+X^2)P_n'(X)) = 2 + \deg(P_n') = \deg(P_n) + 1 = n+1$, par degré d'un produit. Et $\deg((2X+1)P_n(X)) = \deg(P_n)+1 = n+1$. Donc, par degré d'une somme, $\deg(P_{n+1}) \leq n+1$.

D'autres part, $\text{coeff dom}((1+X+X^2)P_n'(X)) = \text{coeff dom}(P_n') = \deg(P_n)\,\text{coeff dom}(P_n) = (-1)^n n(n+1)!$. Et $\text{coeff dom}((n+1)(2X+1)P_n(X)) = 2(n+1)\,\text{coeff dom}(P_n) = (-1)^n 2(n+1)(n+1)!$. Alors $\text{coeff dom}((1+X+X^2)P_n'(X)) - \text{coeff dom}((n+1)(2X+1)P_n(X)) = (-1)^n n(n+1)! - 2(n+1)(-1)^n(n+1)! = (-1)^n(n+1)!(n-2n-2) = (-1)^{n+1}(n+2)! \neq 0$.

On en déduit donc $\deg(P_{n+1}) = n+1$ et $\text{coeff dom}(P_{n+1}) = (-1)^{n+1}(n+2)!$.

Et finalement, par principe de récurrence, $\forall n \in \mathbb{N}^*,\ \deg(P_n) = n$ et $\text{coeff dom}(P_n) = (-1)^n(n+1)!$. Or c'est encore vrai pour $n = 0$, donc $\forall n \in \mathbb{N},\ \deg(P_n) = n$ et $\text{coeff dom}(P_n) = (-1)^n(n+1)!$.

3.(c) Soit $n \in \mathbb{N}$. Supposons $\exists P_n, Q_n \in \mathbb{R}[X]$ tel que $\forall x \in \mathbb{R},\ \frac{\widetilde{P_n}(x)}{(1+x+x^2)^{n+1}} = f^{(n)}(x) = \frac{\widetilde{Q_n}(x)}{(1+x+x^2)^{n+1}}$. Alors, $\forall x \in \mathbb{R},\ \widetilde{P_n}(x) = (1+x+x^2)f^{(n)}(x) = \widetilde{Q_n}(x)$. Et donc le polynôme $P_n - Q_n$ a une infinité de racines, et donc $P_n - Q_n = 0$ et donc $P_n = Q_n$.

D'où l'unicité de P_n.

4. **Des relations de récurrences vérifiées par $(P_n)_{n\in\mathbb{N}}$.**

4.(a) On pose $g(x) = 1+x+x^2$ pour tout $x \in \mathbb{R}$. Alors $g \in \mathcal{C}^\infty(\mathbb{R},\mathbb{R})$ car polynomiale. Donc $fg \in \mathcal{C}^\infty\mathbb{R}$. Et

$$\forall k \in \mathbb{N},\ \forall x \in \mathbb{R},\ g^{(k)}(x) = \begin{cases} 1+x+x^2 & k=0 \\ 1+2x & k=1 \\ 2 & k=2 \\ 0 & k \geq 3 \end{cases}$$

Par la formule de Leibniz, on a donc

$$\begin{aligned}\forall n \geq 2,\ (fg)^{(n)}(x) &= \sum_{k=0}^{n} \binom{n}{k} g^{(k)}(x) f^{(n-k)}(x) \\ &= g(x)f^{(n)}(x) + ng'(x)f^{(n-1)}(x) + \frac{n(n-1)}{2}g''(x)f^{(n-2)}(x)\end{aligned}$$

$$= (1+x+x^2)\frac{\widetilde{P_n}(x)}{(1+x+x^2)^{n+1}} + \frac{n(2x+1)\widetilde{P_{n-1}}(x)}{(1+x+x^2)^n} + \frac{n(n-1)\widetilde{P_{n-2}}(x)}{(1+x+x^2)^{n-1}}$$
$$= \frac{\widetilde{P_n}(x) + n(2x+1)\widetilde{P_{n-1}}(x) + n(n-1)(1+x+x^2)\widetilde{P_{n-2}}(x)}{(1+x+x^2)^n}.$$

Or $\forall x \in \mathbb{R}$, $g(x)f(x) = 1$, donc $\forall n \geq 1$, $\forall x \in \mathbb{R}$, $(gf)^{(n)}(x) = 0$.

On en déduit donc

$$\forall n \geq 2,\ \forall x \in \mathbb{R},\ \frac{\widetilde{P_n}(x) + n(2x+1)\widetilde{P_{n-1}}(x) + n(n-1)(1+x+x^2)\widetilde{P_{n-2}}(x)}{(1+x+x^2)^n}$$
$$\iff \forall n \geq 2,\ \forall x \in \mathbb{R},\ \widetilde{P_n}(x) + n(2x+1)\widetilde{P_{n-1}}(x) + n(n-1)(1+x+x^2)\widetilde{P_{n-2}}(x) = 0$$

Donc $\forall n \geq 2$, le polynôme $P_n(X) + n(2X+1)P_{n-1}(X) + n(n-1)(1+X+X^2)P_{n-2}(X)$ a une infinité de racines et donc on en déduit $\forall n \geq 2$, $P_n(X) + n(2X+1)P_{n-1}(X) + n(n-1)(1+X+X^2)P_{n-2}(X) = 0$.

4.(b) D'après la formule précédente, on a $\forall n \in \mathbb{N}^*$, $P_{n+1}+(n+1)(2X+1)P_n(X)+n(n+1)(1+X+X^2)P_{n-1}(X) = 0$.

Par définition de la suite $(P_n)_{n\in\mathbb{N}}$, on a également

$$\forall n \in \mathbb{N}^*,\ (1+X+X^2)P_n'(X) = P_{n+1}(X) + (n+1)(2X+1)P_n(X) = -n(n+1)(1+X+X^2)P_{n-1}(X).$$

Or $1+X+X^2 \neq 0$, donc on en déduit $\forall n \in \mathbb{N}^*$, $P_n'(X) = -n(n+1)P_{n-1}(X)$.

5. **Étude des racines réelles de P_n.**

5.(a) Soit $\beta \in \mathbb{R}$. Supposons $\exists n_0 \geq 2$ tel que β racine de P_n et P_{n-1}. D'après la question 4.(a), on a $P_{n_0}(X) + n_0(2X+1)P_{n_0-1} + n_0(n_0-1)(1+X+X^2)P_{n_0-2}(X) = 0$. Donc $0 = \widetilde{P_{n_0}}(\beta) + n_0(2\beta+1)\widetilde{P_{n_0-1}}(\beta) + n_0(n_0-1)(1+\beta+\beta^2)\widetilde{P_{n_0-2}}(\beta) = n_0(n_0-1)(1+\beta+\beta^2)\widetilde{P_{n_0-2}}(\beta) = 0$. Or $n_0(n_0-1)(1+\beta+\beta^2) \neq 0$, donc $\widetilde{P_{n_0-2}}(\beta) = 0$. Et donc β est une racine de P_{n_0-2}.

5.(b) Soit $n \in \mathbb{N}$. Supposons que P_n et P_{n+1} ont une racine en commun. Donc $\exists \beta \in \mathbb{R}$ tel que $\widetilde{P_n}(\beta) = 0 = \widetilde{P_{n-1}}(\beta)$. D'après la question précédente, on en déduit donc que β est aussi une racine de P_{n-1}. Donc β est une racine de P_n et P_{n-1}. Et par itération, β est une racine de P_{n+1}, P_n, P_{n-1}, $\ldots$, P_0. Or $P_0(X) = 1$. Donc P_0 n'a pas de racines et donc on a une contradiction.

5.(c) Soit $n \in \mathbb{N}^*$. D'après la question précédente, P_n et P_{n-1} n'ont pas de racines réelles en commun. Donc P_n et $n(n+1)P_{n-1}$ n'ont pas de racines réelles en communs. Donc P_n et P_n' n'ont pas de racines réelles en commun, d'après 4.(b). Et donc les racines réelles de P_n ne sont pas des racines de P_n'. (Autrement dit, les racines réelles de P_n sont simples.)

6. **Factorisation de P_n.**

6.(a) On a $P_1(X) = -1-2X$. Donc P_1 n'a qu'une seule racine sur $\mathbb{R}$ qui est $1/2$. Or $\forall x \in \mathbb{R}$, $f'(x) = \frac{\widetilde{P_1}(x)}{(1+x+x^2)^2}$. Donc f' ne s'annule qu'en $1/2$.

On a aussi $P_2(X) = 6X(X+1)$. Donc P_2 ne s'annule qu'en 0 et -1. Or $\forall x \in \mathbb{R}$, $f''(x) = \frac{\widetilde{P_2}(x)}{(1+x+x^2)^3}$. Donc f'' ne s'annule qu'en 0 et -1.

6.(b) Soit $n \in \mathbb{N}$ avec $n \geq 2$. On suppose que $f^{(n)}$ s'annule en $\alpha_1 < \cdots < \alpha_n$.

6.(b).i) On a montré plus haut que $\deg(P_n) = n$ et $\operatorname{coeff}\operatorname{dom}(P_n) = (-1)^n(n+1)!$.

Donc $\exists a_0, \ldots, a_{n-1} \in \mathbb{R}$ tel que $P_n(X) = (-1)^n(n+1)!X^n + \sum_{k=0}^n a_k X^k$. Et donc

$$\forall x \in \mathbb{R}^*,\ f^{(n)}(x) = \frac{(-1)^n(n+1)!x^n + \sum_{k=0}^n a_k x^k}{(1+x+x^2)^{n+1}} = \frac{(-1)^n(n+1)! + \sum_{k=0}^n a_k x^{k-n}}{(x+1+1/x)^n(1+x+x^2)} \xrightarrow[x\to\pm\infty]{} 0.$$

6.(b).ii) On a donc $f^{(n)}(\alpha_n) = 0$ et $f^{(n)}(x) \xrightarrow[x\to+\infty]{} 0$, $f^{(n)}$ est continue sur $[\alpha_n, +\infty[$ et $f^{(n)}$ est dérivable sur $]\alpha_n, +\infty[$. Donc, d'après la question 1., $\exists \beta \in]\alpha_n, +\infty[$ tel que $f^{(n+1)}(\beta) = (f^{(n)})'(\beta) = 0$.

De la même manière, $f^{(n)}(x) \xrightarrow[x\to-\infty]{} 0$, $f^{(n)}(\alpha_1) = 0$, $f^{(n)} \in \mathcal{C}^0(]-\infty, \alpha_1], \mathbb{R}) \cap \mathcal{D}^1(]-\infty, \alpha_1[, \mathbb{R})$, donc, toujours par la question 1., $f^{(n+1)}(\gamma) = 0$ pour un certain $\gamma \in]-\infty, \alpha_1[$.

6.(b).iii) Soit $k \in \{1, \dots, n-1\}$. On a $f^{(n)} \in \mathcal{C}^0([\alpha_k, \alpha_{k+1}], \mathbb{R}) \cap \mathcal{D}^1(]\alpha_k, \alpha_{k+1}[, \mathbb{R})$ et $f^{(n)}(\alpha_k) = 0 = f^{(n)}(\alpha_{k+1})$. Donc par le théorème de Rolle, $\forall k \in \{1, \dots, n-1\}$, $\exists \beta_k \in]\alpha_k, \alpha_{k+1}[$ tel que $f^{(n+1)}(\beta_k) = 0$.

On vient donc de trouver $n-1$ zéros distincts pour la fonction $f^{(n+1)}$.

De plus, d'après la question précédente, $f^{(n+1)}$ s'annule aussi sur $]-\infty, \alpha_1[$ et sur $]\alpha_n, +\infty[$. Donc finalement, on vient de montrer que $f^{(n+1)}$ s'annule $n+1$ fois distinctes (on a $\beta_0 < \alpha_1 < \beta_1 < \alpha_2 < \cdots < \beta_{n-1} < \alpha_n < \beta_n$).

Problème 1 (Théorèmes de Wilson et Dickson) :
On notera $\mathcal{P}$ l'ensemble des nombres premiers.

1. **Généralités sur le PGCD.**

1.(a) Soit $a, b, c \in \mathbb{Z}$ tels que $a|b$ et $b \wedge c = 1$. Soit $d = a \wedge c$. Alors $d|a|b$ par transitivité de la divisibilité. Donc $d|b$ et $d|c$, par définition du pgcd. Donc $d|(b \wedge c)$ par caractérisation du pgcd. Donc $d|1$. Or $d \geq 0$ par positivité du pgcd. Donc $d = 1$, *i.e.* $a \wedge c = 1$.

1.(b) Soit $a, b, c \in \mathbb{N}^*$ tels que $a \wedge b = 1$.

Soit $d = a \wedge b$. Alors $d|a$ et $d|b|bc$. Donc, par caractérisation du pgcd, $d|(a \wedge (bc))$. Inversement, si $\delta = a \wedge (bc)$, alors $\delta|a$ par définition du pgcd et $\delta|bc$. Or $\delta|a$ et $a \wedge b = 1$. Donc, par la question précédente, $\delta \wedge b = 1$. Donc, par le lemme de Gauss, $\delta|c$. On a donc $\delta|a$ et $\delta|c$. Donc $\delta|(a \wedge c)$ par caractérisation du pgcd. Donc $d|\delta$ et $\delta|d$. Donc, par positivité, $d = a \wedge b = a \wedge (bc) = \delta$.

On a $(a \wedge c)|a|ab$ et bien sûr $(a \wedge c)|c$. Donc $(a \wedge c)|((ab) \wedge c)$ par caractérisation du pgcd. Par symétrie du problème en a et b, en reprenant le raisonnement précédent et en échangeant a et b, on a aussi $(b \wedge c)|((ab) \wedge c)$. Or $a \wedge b = 1$ et $(a \wedge c)|a$ et $(b \wedge c)|b$. Donc $(a \wedge c) \wedge (b \wedge c) = 1$. Donc $((a \wedge c)(b \wedge c))|((ab) \wedge c)$.

De plus, en utilisant la relation de Bézout, $\exists u, v, n, m \in \mathbb{Z}$ tels que $au + cv = a \wedge c$ et $bn + cm = b \wedge c$. Donc

$$(a \wedge c)(b \wedge c) = (au + cv)(bn + cm) = abun + c(bvn + vcm + mau)$$

Or $(ab) \wedge c|ab$ et $(ab) \wedge c|c$, donc $(ab) \wedge c|(abun + c(bvn + vcm + mau))$, *i.e.* $(ab) \wedge c|(a \wedge c)(b \wedge c)$.

Puis, par positivité, on en déduit $(a \wedge c)(b \wedge c) = (ab) \wedge c$.

2. **Théorème de Wilson.**

Soit $p \in \mathbb{N}^*$.

2.(a) Supposons p non premier. Donc $\exists d \in \{2, \dots, p-1\}$ tel que $d|p$. Alors $d|(p-1)!$ car $(p-1)! = \prod_{k=1}^{p-1} k$.

Si $(p-1)! + 1 \equiv 0\ [p]$, alors par caractérisation de la divisibilité par les congruences (ou division euclidienne), $p|((p-1)! + 1)$. Et donc, par transitivité de la divisibilité, $d|((p-1)! + 1)$. Donc $d|(((p-1)! + 1) - (p-1)!) = 1$. Or $d \geq 2$. Donc ☠. Donc $p \nmid ((p-1)! + 1)$, *i.e.* $(p-1)! + 1 \not\equiv 0\ [p]$.

On suppose p premier.

2.(b) Si $p = 2$, alors $(p-1)! = 1! = 1$. Donc $(p-1)! \equiv 1 \equiv 2 - 1 \equiv -1\ [2]$.

Si $p = 2$, alors $(p-1)! = 2! = 2 = 3 - 1$. Donc $(p-1)! \equiv -1\ [3]$.

Supposons maintenant p premier et $p \geq 5$.

2.(c) Par définition de la primalité, $\forall k \in \{2 \dots, p-2\}$, $k \wedge p = 1$ car $p \nmid k$ et p premier. Donc, par le théorème de Bézout, $\forall k \in \{2, \dots, p-2\}$, $\exists u_k, v_k \in \mathbb{Z}$ tels que $pu_k + kv_k = 1$. Et donc, en passant aux congruences, $\forall k \in \{2, \dots, p-2\}$, $\exists v_k \in \mathbb{Z}$, $kv_k \equiv 1\ [p]$.

2.(d) Soit $k \in \{2, \dots, p-2\}$. Soit $v_k \in \mathbb{Z}$ tel que $kv_k \equiv 1\ [p]$ (cet entier v_k existe d'après la question précédente).

Par division euclidienne, $\exists q_k, \alpha_k \in \mathbb{Z}$ tels que $v_k = pq_k + \alpha_k$ et $0 \leq \alpha_k \leq p-1$. Donc $v_k \equiv \alpha_k\ [p]$. Alors

$$k\alpha_k \equiv kv_k \equiv 1\ [p]$$

De plus, si $\alpha_k = 0$, alors, $0 \equiv 1\ [p]$. Donc $p|1$. Or p premier. Donc ☠. Donc $\alpha \neq 1$. Donc $\alpha_k \in \{1, \dots, p-1\}$.

Enfin, si $\alpha_k = 1$, alors $k\alpha_k \equiv k \equiv 1\ [p]$. Donc $k-1$ est divisible par p. Or $k-1 \in \{1,\dots,p-3\}$ et il n'y a pas de multiple de p dans cet ensemble. Donc ☠. Donc $\alpha_k \neq 1$. De même, si $\alpha_k = p-1$, alors $1 \equiv k\alpha_k \equiv -k\ [p]$. Donc $p|(k+1)$ mais $k+1 \in \{3,\dots,p-1\}$ qui ne contient toujours pas de multiple de p. Donc $\alpha_k \neq p-1$.

Et donc $\alpha_k \in \{2,\dots,p-2\}$.

On vient donc de montrer que $\forall k \in \{2,\dots,p-2\}$, $\exists \alpha_k \in \{2,\dots,p-2\}$, $k\alpha_k \equiv 1\ [p]$.

2.(e) On va montrer l'unicité associée à l'existence de la question précédente. Soit $k \in \{2,\dots,p-2\}$. Supposons qu'il existe $\alpha_k, \beta_k \in \{2,\dots,p-2\}$ tels que $k\alpha_k \equiv k\beta_k \equiv 1\ [p]$.

Alors $k(\alpha_k - \beta_k) \equiv 0\ [p]$. Donc $p|k(\alpha_k - \beta_k)$. Or $p \wedge k = 1$ car $k \in \{2,\dots,p-2\}$ et p premier. Donc, par lemme de Gauss, $p|(\alpha_k - \beta_k)$. Or $\alpha_k, \beta_k \in \{2,\dots,p-2\}$. Donc $\alpha_k - \beta_k \in \{4-p,\dots,p-4\}$. Donc $|\alpha_k - \beta_k| \in \{0,\dots,p-4\}$. Et $p\mathbb{Z} \cap \{4-p,\dots,p-4\} = \{0\}$. Donc $\alpha_k - \beta_k = 0$. Donc $\alpha_k = \beta_k$.

D'où l'unicité. Autrement dit, $\forall k \in \{2,\dots,p-2\}$, $\exists! \alpha_k \in \{2,\dots,p-2\}$ tel que $k\alpha_k \equiv 1\ [p]$.

2.(f) Notons que dans la question précédente, on a $\alpha_k \neq k$. En effet : soit $k \in \{1,\dots,p-1\}$. Supposons $k^2 \equiv 1\ [p]$. Donc $p|(k^2-1)$ c'est-à-dire $p|(k-1)(k+1)$. Or p est premier donc $p|(k-1)$ ou $p|(k+1)$. Mais $k-1 \in \{0,\dots,p-2\}$ et $k+1 \in \{2,\dots,p\}$. Donc $k=1$ ou $k=p-1$. Et la réciproque est évidente : si $k \in \{1,p-1\}$, alors $k \equiv \pm 1\ [p]$ et donc $k^2 \equiv 1\ [p]$.

Donc si $k \in \{1,\dots,p-1\}$, $k^2 \equiv 1\ [p] \iff k \in \{1,p-1\}$.

Donc $\forall k \in \{2,\dots,p-2\}$, $\exists! \alpha_k \in \{2,\dots,p-2\}$ tel que $k\alpha_k \equiv 1\ [p]$ et $\alpha_k \neq k$.

Par conséquent, tous les entiers de $\{2,\dots,p-2\}$ peuvent être regroupés par pair de la forme (k,α_k) dont le produit est congru à 1 modulo p. Et donc,

$$\prod_{k=2}^{p-2} k \equiv 1\ [2]$$

en regroupant ces entiers par pairs. On notera d'ailleurs qu'il y a $p-2-2+1 = p-3$ entiers entre 2 et $p-2$, et $p-3$ est pair car p est un nombre premier différent de 2 (donc p est impair).

On vient donc de montrer que $(p-2)! \equiv 1\ [p]$.

2.(g) On obtient donc immédiatement $(p-1)! \equiv p-1 \equiv -1\ [p]$ à partir de la question précédente. Et donc $p|((p-1)!+1)$.

3. **Théorème de Disckson.**

Soit $n \in \mathbb{N}$ avec $n \geq 2$. Supposons qu'il existe $m \in \{1,\dots,n-1\}$ tel que $(m-1)!(n-m)! \equiv (-1)^m\ [n]$.

3.(a) Par hypothèse $(m-1)!(n-m)! \equiv (-1)^m\ [n]$. Donc, par définition des congruences, $\exists u \in \mathbb{Z}$ tel que $(m-1)!(n-m)! = (-1)^m + nu$. Et donc aussi $(-1)^m(m-1)!(n-m)! - (-1)^m un = 1$. D'où, par théorème de Bézout, $(n-m)! \wedge n = 1$.

Donc si $k \in \{1,\dots,n-m\}$, alors $k|(n-m)!$. Or $n \wedge (n-m)! = 1$. Donc $n \wedge k = 1$.

3.(b) Soit $k \in \{n-m+1,\dots,n-1\}$. Alors $n-k \in \{1,\dots,m-1\}$. Or d'après le théorème de Bézout avec la relation $(m-1)!(n-m)! \equiv (-1)^m\ [n]$, on en déduit $(m-1)! \wedge n = 1$. Et $(n-k)|(m-1)!$. Donc $(n-k) \wedge n = 1$.

D'après le théorème de Bézout, $\exists u, v \in \mathbb{Z}$ tels que $(n-k)u + nv = 1$. donc $n(u+v) - uk = 1$. Et donc, de nouveau par le théorème de Bézout, $(n-k) \wedge k = 1$.

3.(c) On vient de montrer que si $\exists m \in \{1,\dots,n-1\}$ tel que $(m-1)!(n-m)! \equiv (-1)^m\ [n]$, alors $\forall k \in \{1,\dots,n-1\}$, $n \wedge k = 1$. Donc n n'a pas de diviseurs non trivial. Et donc n est premier.

Réciproquement, si n est premier, d'après le théorème de Wilson, $(n-1)! \equiv -1\ [n]$. Donc $(1-1)!(n-1)! \equiv (-1)^1\ [n]$. Et donc $\exists m \in \{1,\dots,n-1\}$ tel que $(m-1)!(n-m)! \equiv (-1)^m\ [n]$ en prenant $m=1$.