Corrigé du DS n°8 de Maths

Exercice 1 — (Etude d'une suite récurrente).

Soit f la fonction définie sur $\mathbb{R}$ en posant :

$$\forall\, x \in \mathbb{R},\ f(x) = \ln\left(1 + x + \sqrt{1 + (1+x)^2}\right)$$

Et soit (u_n) la suite réelle définie en posant :

$$u_0 \in [0,2], \text{ et } \forall\, n \in \mathbb{N},\ u_{n+1} = f(u_n)$$

1/ Justifier que f est dérivable sur $\mathbb{R}$, et montrer que : $\forall\, x \in \mathbb{R},\ f'(x) = \dfrac{1}{\sqrt{1 + (1+x)^2}}$.

La fonction f est dérivable sur $\mathbb{R}$ selon les théorèmes généraux, et pour tout réel x on a :

$$f'(x) = \frac{1 + \dfrac{2(1+x)}{2\sqrt{1+(1+x)^2}}}{1 + x + \sqrt{1+(1+x)^2}} = \frac{\left(\dfrac{\sqrt{1+(1+x)^2} + (1+x)}{\sqrt{1+(1+x)^2}}\right)}{1 + x + \sqrt{1+(1+x)^2}} = \frac{1}{\sqrt{1+(1+x)^2}}$$

Conclusion. f est dérivable sur $\mathbb{R}$ et $\forall\, x \in \mathbb{R},\ f'(x) = \dfrac{1}{\sqrt{1 + (1+x)^2}}$

2/ Pour tout réel $x \in [0,2]$, on pose : $g(x) = f(x) - x$. Etablir que g réalise une bijection de $[0,2]$ vers un intervalle que l'on précisera.

La fonction g est dérivable sur $\mathbb{R}$ selon les théorèmes généraux, et pour tout réel x, on a :

$$g'(x) = \frac{1}{\sqrt{1 + (1+x)^2}} - 1$$

Il s'ensuit que : $\forall\, x \in \mathbb{R},\ g'(x) < 0$, puisqu'il est clair que : $\dfrac{1}{\sqrt{1 + (1+x)^2}} < 1$.

On en déduit que g est strictement décroissante sur $\mathbb{R}$.

Ainsi, la fonction g est continue sur $[0,2]$ (car dérivable sur $\mathbb{R}$), et strictement décroissante sur $[0,2]$: à ce titre, g réalise une bijection de $[0,2]$ vers $[g(2), g(0)]$.

De plus : $[g(2), g(0)] = \left[\ln\left(3 + \sqrt{10}\right) - 2;\ \ln\left(1 + \sqrt{2}\right)\right]$

Conclusion. La fonction g réalise une bijection de $[0,2]$ vers $\left[\ln\left(3 + \sqrt{10}\right) - 2;\ \ln\left(1 + \sqrt{2}\right)\right]$

3/ Etablir que l'équation $f(x) = x$ admet une unique solution dans $[0,2]$, que l'on notera ℓ.

On peut observer que* :

$$\ln\left(3+\sqrt{10}\right) - 2 \leqslant 0 \leqslant \ln\left(1+\sqrt{2}\right)$$

D'après la question précédente, 0 admet un unique antécédent ℓ par g dans $[0,2]$.

On conclut en observant que : $g(\ell) = 0 \iff f(\ell) = \ell$.

Conclusion. $\exists!\, \ell \in [0,2],\ g(\ell) = 0$

4/ Etablir que : $\forall\, n \in \mathbb{N},\ |u_{n+1} - \ell| \leqslant \dfrac{1}{\sqrt{2}}\,|u_n - \ell|$

Soit $n \in \mathbb{N}$. Si $u_n = l$, alors $u_{n+1} = f(u_n) = f(\ell) = \ell$; et l'inégalité est trivialement vraie (les deux termes sont nuls).

Sinon, la fonction f vérifie les hypothèses du théorème des accroissements finis sur $[u_n, \ell]$ ou sur $[\ell, u_n]$ (continue sur le fermé, dérivable sur l'ouvert). Par suite :

$$\exists\, c \in [u_n,\ell] \cup [\ell,u_n], \quad f(u_n) - f(\ell) = f'(c)\,(u_n - l)$$

On en déduit que :

$$u_{n+1} - \ell = f'(c)\,(u_n - l) \Longrightarrow |u_{n+1} - \ell| = |f'(c)| \times |u_n - l|$$

Par ailleurs, on déduit de la question 1 que f' est positive et décroissante sur $[0,2]$; elle admet donc un maximum en 0, égal à $1/\sqrt{2}$. En particulier : $|f'(c)| \leqslant \dfrac{1}{\sqrt{2}}$.

Conclusion. $\forall\, n \in \mathbb{N},\ |u_{n+1} - \ell| \leqslant \dfrac{1}{\sqrt{2}}\,|u_n - \ell|$

5/ Etablir que : $\forall\, n \in \mathbb{N},\ |u_n - \ell| \leqslant 2^{1-\frac{n}{2}}$

Par une récurrence immédiate, on déduit de la question précédente, on obtient : $\forall\, n \in \mathbb{N},\ |u_{n+1} - \ell| \leqslant 2^{-n/2}\,|u_0 - \ell|$.

Il suffit alors d'observer que u_0 et ℓ appartiennent à $[0,2]$ pour avoir : $|u_0 - \ell| \leqslant 2$.

Conclusion. D'après ce qui précède : $\forall\, n \in \mathbb{N},\ |u_n - \ell| \leqslant 2^{1-\frac{n}{2}}$

6/ Déduire de ce qui précède que (u_n) converge, et préciser sa limite.

D'après la question précédente : $\lim\limits_{n\longrightarrow+\infty} |u_n - \ell| = 0$.

Conclusion. On en déduit que la suite (u_n) est convergente, et que : $\lim\limits_{n\longrightarrow+\infty} u_n = \ell$

---

*. C'est au moins clair pour l'inégalité de droite ; pour celle de gauche, il "suffit" de voir que $3+\sqrt{10} \approx 5$ tandis que $\mathrm{e}^2 \approx 7$. J'imagine que vous ne vous satisferez pas de cette justification "bon marché". Si l'on veut être plus rigoureux, il faut utiliser le fait que $\mathrm{e}^2 \geqslant \sum\limits_{k=0}^{3} 2^k/k! \geqslant 6$, et vérifier que $3+\sqrt{10} \leqslant 6$, ce qui est plus humain. En tous les cas, l'inégalité de gauche pouvait être admise sans justification lors du devoir.

7/ Valeur approchée de ℓ, et majoration de l'erreur commise.

Dans les deux questions ci-dessous, on suppose que $u_0 = 0$.

L'objectif des 2 questions indépendantes ci-dessous est de déterminer une valeur approchée de ℓ, ainsi qu'une majoration de l'erreur commise. La première approche est numérique, et la seconde est théorique.

a/ Ecrire en langage Python une fonction `Vapp(epsilon)` qui reçoit comme paramètre un flottant `epsilon` strictement positif, et qui renvoie une valeur approchée de ℓ à `epsilon` près.

```
from math import *

def f(x):
    return log(1+x+sqrt(1+x**2)) # En Python, 'log' désigne le logarithme népérien

def Vapp(epsilon):
    u =0 # initialisation du terme de la suite
    n =0 # initialisation du rang
    while 2 ** (1 - (n / 2)) >=epsilon:
        u =f(u) # on remplace 'u(n)' par 'u(n+1)'
        n =n +1 # on incrémente le rang
    return u
```

b/ Soit p un entier naturel. Résoudre l'inéquation (d'inconnue $n \in \mathbb{N}$) : $2^{1-\frac{n}{2}} \leqslant 10^{-p}$

En déduire un entier n_0 tel que u_{n_0} est une valeur approchée à 10^{-p} près de ℓ.

Soient p et n deux entiers naturels. On a :

$$2^{1-\frac{n}{2}} \leqslant 10^{-p} \iff \left(1-\frac{n}{2}\right)\ln(2) \leqslant -p\ln(10) \iff 1-\frac{n}{2} \leqslant \frac{-p\ln(10)}{\ln(2)}$$

$$\frac{n}{2} \geqslant \frac{p\ln(10)}{\ln(2)} + 1 \iff n \geqslant \frac{2p\ln(10)}{\ln(2)} + 2 \iff n \geqslant \frac{2\left(p\ln(10)+\ln(2)\right)}{\ln(2)}$$

Puisque n est un entier naturel, et que le terme de droite de la dernière inégalité n'est pas entier, on en déduit finalement que :

$$2^{1-\frac{n}{2}} \leqslant 10^{-p} \iff n \geqslant \left\lfloor \frac{2\left(p\ln(10)+\ln(2)\right)}{\ln(2)} \right\rfloor + 1$$

Conclusion. Pour $n_0 = \left\lfloor \frac{2\left(p\ln(10)+\ln(2)\right)}{\ln(2)} \right\rfloor + 1$, u_{n_0} est une valeur approchée à 10^{-p} près de ℓ.

Problème 1 — Capacités numériques

Partie 1 - Questions préliminaires

Dans ce paragraphe, f désigne une fonction continue sur $[a,b]$ (avec $a<b$) et à valeurs réelles.

1/ Relation de Chasles généralisée. Démontrer par récurrence que :

$$\forall n\in\mathbb{N}^*,\ \forall (y_0,y_1,\dots,y_n)\in[a,b]^{n+1},\quad \sum_{k=0}^{n-1}\int_{y_k}^{y_{k+1}} f(x)\,\mathrm{d}x=\int_{y_0}^{y_n} f(x)\,\mathrm{d}x$$

Pour tout entier naturel non nul n, notons $P(n)$ l'assertion :

$$\forall (y_0,y_1,\dots,y_n)\in[a,b]^{n+1},\quad \sum_{k=0}^{n-1}\int_{y_k}^{y_{k+1}} f(x)\,\mathrm{d}x=\int_{y_0}^{y_n} f(x)\,\mathrm{d}x$$

Soient y_0 et y_1 dans $[a,b]$. On a : $\displaystyle\sum_{k=0}^{0}\int_{y_k}^{y_{k+1}} f(x)\,\mathrm{d}x=\int_{y_0}^{y_1} f(x)\,\mathrm{d}x$. D'où $P(1)$ est vraie.

Supposons à présent $P(n)$ vraie pour un certain $n\in\mathbb{N}^*$, et considérons $(y_0,y_1,\dots,y_{n+1})\in[a,b]^{n+2}$. On a :

$$\sum_{k=0}^{n}\int_{y_k}^{y_{k+1}} f(x)\,\mathrm{d}x=\sum_{k=0}^{n-1}\int_{y_k}^{y_{k+1}} f(x)\,\mathrm{d}x+\int_{y_n}^{y_{n+1}} f(x)\,\mathrm{d}x=\int_{y_0}^{y_n} f(x)\,\mathrm{d}x+\int_{y_n}^{y_{n+1}} f(x)\,\mathrm{d}x=\int_{y_0}^{y_{n+1}} f(x)\,\mathrm{d}x$$

D'où $P(n+1)$ est vraie. Récurrence établie.

Conclusion. $\forall (y_0,y_1,\dots,y_n)\in[a,b]^{n+1},\quad \displaystyle\sum_{k=0}^{n-1}\int_{y_k}^{y_{k+1}} f(x)\,\mathrm{d}x=\int_{y_0}^{y_n} f(x)\,\mathrm{d}x$

2/ Un lemme de majoration.

a/ Etablir que : $\displaystyle\int_a^b f(x)\,\mathrm{d}x\leqslant\int_a^b |f(x)|\,\mathrm{d}x$

Pour tout réel $x\in[a,b]$, on a : $f(x)\leqslant|f(x)|$.

L'inégalité de l'énoncé s'ensuit, par croissance de l'intégrale.

Conclusion. $\displaystyle\int_a^b f(x)\,\mathrm{d}x\leqslant\int_a^b |f(x)|\,\mathrm{d}x$

b/ En déduire soigneusement que : $\displaystyle\left|\int_a^b f(x)\,\mathrm{d}x\right|\leqslant\int_a^b |f(x)|\,\mathrm{d}x$

On distingue deux cas, suivant le signe de $\displaystyle\int_a^b f$.

Premier cas — Si $\displaystyle\int_a^b f\geqslant 0$. Le résultat provient directement de la question précédente :

$$0\leqslant\int_a^b f\leqslant\int_a^b |f|\qquad\text{d'où :}\qquad\left|\int_a^b f\right|\leqslant\int_a^b |f|$$

Second cas — Si $\displaystyle\int_a^b f < 0$**.** Par hypothèse et par linéarité de l'intégrale, on a alors : $\displaystyle\int_a^b (-f) > 0$.

D'après l'étude faite dans le cas précédent, on en déduit que : $\left|\displaystyle\int_a^b (-f)\right| \leqslant \int_a^b |-f|$.

D'où : $\left|\displaystyle\int_a^b f\right| \leqslant \int_a^b |f|$.

Conclusion. $\left|\displaystyle\int_a^b f(x)\,\mathrm{d}x\right| \leqslant \int_a^b |f(x)|\,\mathrm{d}x$

3/ Inégalité triangulaire généralisée.

On admet que : $\forall\,(x,y) \in \mathbb{R}^2,\ |x+y| \leqslant |x| + |y|$.

Démontrer par récurrence que :

$$\forall\, n \in \mathbb{N}^*,\ \forall\ (u_1,\ldots,u_n) \in \mathbb{R}^n,\ \left|\sum_{k=1}^{n} u_k\right| \leqslant \sum_{k=1}^{n} |u_k|$$

Pour tout entier naturel n non nul, notons $P(n)$: $\forall\ (u_1,\ldots,u_n) \in \mathbb{R}^n,\ \left|\displaystyle\sum_{k=1}^{n} u_k\right| \leqslant \sum_{k=1}^{n} |u_k|$

L'assertion $P(1)$ est vraie.

Supposons $P(n)$ vraie pour un certain $n \in \mathbb{N}^*$, et soit $(u_1,\ldots,u_{n+1}) \in \mathbb{R}^{n+1}$.

On a : $\left|\displaystyle\sum_{k=1}^{n+1} u_k\right| = \left|\sum_{k=1}^{n} u_k + u_{n+1}\right| \leqslant \left|\sum_{k=1}^{n} u_k\right| + |u_{n+1}| \leqslant \sum_{k=1}^{n} |u_k| + |u_{n+1}|$

Finalement : $\left|\displaystyle\sum_{k=1}^{n+1} u_k\right| \leqslant \sum_{k=1}^{n+1} |u_k|$. D'où $P(n+1)$ est vraie.

Récurrence établie.

Conclusion. $\forall\, n \in \mathbb{N}^*,\ \forall\ (u_1,\ldots,u_n) \in \mathbb{R}^n,\ \left|\displaystyle\sum_{k=1}^{n} u_k\right| \leqslant \sum_{k=1}^{n} |u_k|$

Notations. A partir de maintenant, et jusqu'à la fin du problème.

- ➤ a et b sont deux réels, avec $a < b$; et n désigne un entier naturel non nul.
- ➤ On note $(x_0, x_1, \ldots, x_n)$ la subdivision régulière de $[a,b]$ de pas $h = \dfrac{b-a}{n}$, c'est à dire que :

$$\forall\, k \in [\![\, 0, n\,]\!],\ x_k = a + kh$$

Partie 2 - Méthode des rectangles à gauche

Tout au long de la partie 2, on suppose que f est de classe $\mathscr{C}^1$ sur $[a,b]$.
Dans cette partie, on approche f sur chacun des segments $[x_k, x_{k+1}]$ par la fonction constante égale $f(x_k)$.
On note $R_k(f)$ l'aire algébrique du rectangle construit sur le segment $[x_k, x_{k+1}]$, et de "hauteur" $f(x_k)$; et on note $R^n(f) = \sum_{k=0}^{n-1} R_k(f)$. La figure ci-dessous illustre cette construction.

Enfin, on note $I = \int_a^b f(x)\,\mathrm{d}x$.

4/ Justifier que :

$$I - R^n(f) = \sum_{k=0}^{n-1} \int_{x_k}^{x_{k+1}} (f(x) - f(x_k))\,\mathrm{d}x$$

D'après la question 1, et avec les notations de l'énoncé, on a :

$$I = \sum_{k=0}^{n-1} \int_{x_k}^{x_{k+1}} f(x)\,\mathrm{d}x \text{ et } R^n(f) = \int_{x_k}^{x_{k+1}} f(x_k)\,\mathrm{d}x$$

Conclusion. $I - R^n(f) = \sum_{k=0}^{n-1} \int_{x_k}^{x_{k+1}} (f(x) - f(x_k))\,\mathrm{d}x$

5/ Justifier qu'il existe un réel M_1 tel que :

$$\forall x \in [a,b],\ |f'(x)| \leqslant M_1$$

Par hypothèse, $f' \in \mathscr{C}^0([a,b],\mathbb{R})$. D'après le théorème des bornes atteintes, f' est bornée (et atteint ses bornes) sur $[a,b]$.

Conclusion. $\exists M_1 \in \mathbb{R},\ \forall x \in [a,b],\ |f'(x)| \leqslant M_1$

6/ Soit $k \in [\![0, n-1]\!]$. Démontrer que pour tout réel $x \in [x_k, x_{k+1}]$ on a :

$$|f(x) - f(x_k)| \leqslant M_1 (x - x_k)$$

L'inégalité est triviale si $x = x_k$.

Supposons à présent $x > x_k$. D'après l'énoncé, la fonction f est continue sur $[x_k, x]$, et f est dérivable sur $]x_k, x[$. D'après le théorème des accroissements finis :

$$\exists c \in]x_k, x[,\ f'(c) = \frac{f(x) - f(x_k)}{x - x_k}$$

En particulier :

$$|f(x) - f(x_k)| = |f'(c)| \times |x - x_k|$$

Il reste à observer que $(x - x_k) > 0$, et utiliser la question précédente pour conclure.

Conclusion. $\forall x \in [x_k, x_{k+1}],\ |f(x) - f(x_k)| \leqslant M_1 (x - x_k)$

7/ A l'aide de la question précédente, établir que :

$$\forall\, k \in [\![\, 0, n-1 \,]\!], \quad \left| \int_{x_k}^{x_{k+1}} (f(x) - f(x_k))\, \mathrm{d}x \right| \leqslant M_1 \frac{(b-a)^2}{2n^2}$$

Soit $k \in [\![\, 0, n-1 \,]\!]$. D'après q. 2, on a : $\left| \int_{x_k}^{x_{k+1}} (f(x) - f(x_k))\, \mathrm{d}x \right| \leqslant \int_{x_k}^{x_{k+1}} |f(x) - f(x_k)|\, \mathrm{d}x$ (♠)

D'après la question précédente, on a :

$$\int_{x_k}^{x_{k+1}} |f(x) - f(x_k)|\, \mathrm{d}x \leqslant M_1 \int_{x_k}^{x_{k+1}} x - x_k\, \mathrm{d}x = \frac{M_1}{2} \left[(x - x_k)^2\right]_{x_k}^{x_{k+1}} = \frac{M_1 h^2}{2}$$

Ainsi : $\int_{x_k}^{x_{k+1}} |f(x) - f(x_k)|\, \mathrm{d}x \leqslant M_1 \frac{(b-a)^2}{2n^2}$ (♣)

Conclusion. D'après (♠) et (♣) : $\forall\, k \in [\![\, 0, n-1 \,]\!], \quad \left| \int_{x_k}^{x_{k+1}} (f(x) - f(x_k))\, \mathrm{d}x \right| \leqslant M_1 \frac{(b-a)^2}{2n^2}$

8/ En déduire que :

$$|I - R^n(f)| \leqslant M_1 \frac{(b-a)^2}{2n}$$

D'après la question : $|I - R^n(f)| = \left| \sum_{k=0}^{n-1} \int_{x_k}^{x_{k+1}} (f(x) - f(x_k))\, \mathrm{d}x \right|$

D'après l'inégalité triangulaire (q. 3) : $|I - R^n(f)| \leqslant \sum_{k=0}^{n-1} \left| \int_{x_k}^{x_{k+1}} (f(x) - f(x_k))\, \mathrm{d}x \right|$

D'après la question 7 : $|I - R^n(f)| \leqslant \sum_{k=0}^{n-1} M_1 \frac{(b-a)^2}{2n^2}$

Or : $\sum_{k=0}^{n-1} M_1 \frac{(b-a)^2}{2n^2} = n \times M_1 \frac{(b-a)^2}{2n^2} = M_1 \frac{(b-a)^2}{2n}$

Conclusion. $|I - R^n(f)| \leqslant M_1 \frac{(b-a)^2}{2n}$

Remarque. *On en déduit que* $\lim_{n \to +\infty} R^n(f) = \int_a^b f$. *Ceci signifie que la méthode des rectangles à gauche converge (la somme des aires des rectangles tend vers l'intégrale de f), et que cette convergence est linéaire (dans le sens où l'on doit calculer 10^3 termes si l'on souhaite avoir une majoration de l'erreur de l'ordre de 10^{-3}). Le résultat eût été le même avec la méthode des rectangles à droite ; mais on verra dans la partie suivante que la convergence est plus rapide avec la méthode des rectangles médians.*

Partie 3 - Méthode des rectangles médians

Tout au long de la partie 3, on suppose que f est de classe $\mathscr{C}^2$ sur $[a,b]$.

Par ailleurs dans cette partie, on approche f sur chacun des segments $[x_k, x_{k+1}]$ par la fonction constante égale $f(m_k)$, où $m_k = \dfrac{x_k + x_{k+1}}{2}$ désigne le milieu du segment $[x_k, x_{k+1}]$.

On note $R_{n,k}(f)$ l'aire algébrique du rectangle construit sur le segment $[x_k, x_{k+1}]$, et de "hauteur" $f(m_k)$; et on note $R_n(f) = \displaystyle\sum_{k=0}^{n-1} R_{n,k}(f)$. Les figures ci-dessous illustrent cette construction.

9/ Justifier que : $\quad I - R_n(f) = \displaystyle\sum_{k=0}^{n-1} \int_{x_k}^{x_{k+1}} [f(x) - f(m_k)]\,\mathrm{d}x$

Justification analogue à celle de la question 4.

10/ Estimation de l'erreur. Soient c et d deux réels quelconques de $[a,b]$, avec $c < d$.

a/ Soit A un nombre réel. On définit une fonction Φ sur $[c,d]$ en posant :

$$\forall\, x \in [c,d],\ \Phi(x) = f(d) - f(x) - (d-x)\,f'(x) - A\,\frac{(d-x)^2}{2}$$

Etablir qu'il existe une unique valeur de A, que l'on calculera†, tel que : $\Phi(c) = \Phi(d) = 0$.

Par définition, on a déjà $\Phi(d) = 0$.

Par ailleurs : $\Phi(c) = f(d) - f(c) - (d-c)\,f'(c) - A\,\dfrac{(d-c)^2}{2}$. D'où :

$$\Phi(c) = 0 \iff A\,\frac{(d-c)^2}{2} = f(d) - f(c) - (d-c)\,f'(c) \iff A = \frac{2}{(d-c)^2}\,(f(d) - f(c) - (d-c)\,f'(c))$$

Conclusion. $\exists!\, A \in \mathbb{R},\ \Phi(c) = \Phi(d) = 0 \quad$ avec $\quad A = \dfrac{2}{(d-c)^2}\,(f(d) - f(c) - (d-c)\,f'(c))$

b/ On suppose à présent que A est l'unique réel déterminé à la question précédente. Etablir que :

$$\exists\, \alpha \in\ ]c,d[\ ,\ A = f''(\alpha)$$

Par construction et selon les théorèmes généraux, la fonction Φ est continue sur $[c,d]$, dérivable sur $]c,d[$, et vérifie $\Phi(c) = \Phi(d) = 0$. D'après le théorème de Rolle :

$$\exists\, \alpha \in]c,d[,\ \Phi'(\alpha) = 0$$

Or : $\Phi'(\alpha) = 0 \iff -f'(\alpha) + f'(\alpha) - (d-\alpha)f''(\alpha) + A(d-\alpha) = 0 \iff A(d-\alpha) = (d-\alpha)f''(\alpha)$.

Puisque $d - \alpha \neq 0$, on en déduit que : $A = f''(\alpha)$.

Conclusion. $\exists\, \alpha \in\ ]c,d[\ ,\ A = f''(\alpha)$

†. On exprimera A en fonction de c, d, $f(c)$, $f(d)$ et $f'(c)$.

c/ En déduire que : $f(d) = f(c) + (d-c)\,f'(c) + \dfrac{(d-c)^2}{2}\,f''(\alpha)$

Par construction, $\Phi(d) = 0$. Par suite : $f(d) = f(c) + (d-c)\,f'(c) + A\,\dfrac{(d-c)^2}{2}$

Et d'après la question précédente : $A = f''(\alpha)$. La conclusion s'ensuit.

Conclusion. $\exists\,\alpha \in\ ]\,c,d\,[\ ,\ f(d) = f(c) + (d-c)\,f'(c) + \dfrac{(d-c)^2}{2}\,f''(\alpha)$

d/ Soit k un entier quelconque compris entre 0 et $(n-1)$. Etablir que :

$$\forall\, x \in [x_k, x_{k+1}]\,,\ |f(x) - f(m_k) - (x-m_k)\,f'(m_k)| \leqslant M_2\,\frac{(x-m_k)^2}{2}$$

où $M_2 = \max\limits_{x\in[a,b]} |f''(x)|$

Pour $x = m_k$, l'inégalité est immédiate.

Si $x \neq m_k$, on applique le résultat de la question précédente avec $c = m_k$ et $d = x$. On peut ainsi affirmer que :

$$\exists\,\alpha \in\ ]\,x_k, x_{k+1}\,[\ ,\ f(x) = f(m_k) + (x-m_k)\,f'(m_k) + \frac{(x-m_k)^2}{2}\,f''(\alpha)$$

En particulier : $|f(x) - f(m_k) - (x-m_k)\,f'(m_k)| = \left|\dfrac{(x-m_k)^2}{2}\,f''(\alpha)\right|$

D'où : $|f(x) - f(m_k) - (x-m_k)\,f'(m_k)| = \dfrac{(x-m_k)^2}{2}\,|f''(\alpha)|$

Il reste à observer que d'après l'énoncé $|f''(\alpha)| \leqslant M_2$ pour conclure.

Conclusion. $\forall\, x \in [x_k, x_{k+1}]\,,\ |f(x) - f(m_k) - (x-m_k)\,f'(m_k)| \leqslant M_2\,\dfrac{(x-m_k)^2}{2}$

avec $M_2 = \max\limits_{x\in[a,b]} |f''(x)|$

e/ En déduire que :

$$\forall\, k \in [\![\, 0, n-1\,]\!],\ |I_k - R_{n,k}(f)| \leqslant M_2\,\frac{(b-a)^3}{24n^3}$$

puis que : $|I - R_n(f)| \leqslant M_2\,\dfrac{(b-a)^3}{24n^2}$

Soit $k \in [\![\, 0, n-1\,]\!]$. Observons que :

$$\int_{x_k}^{x_{k+1}} f(x) - f(m_k) - (x-m_k)\,f'(m_k)\ \mathrm{d}x = \int_{x_k}^{x_{k+1}} f(x)\,\mathrm{d}x - \int_{x_k}^{x_{k+1}} f(m_k)\,\mathrm{d}x - \int_{x_k}^{x_{k+1}} (x-m_k)\,f'(m_k)\ \mathrm{d}x$$

Il s'ensuit que :

$$\int_{x_k}^{x_{k+1}} f(x) - f(m_k) - (x-m_k)\,f'(m_k)\ \mathrm{d}x = I_k - R_{n,k}(f) - \int_{x_k}^{x_{k+1}} (x-m_k)\,f'(m_k)\ \mathrm{d}x \quad (\spadesuit)$$

Or :

$$\int_{x_k}^{x_{k+1}} (x-m_k)\,f'(m_k)\,\mathrm{d}x = \frac{f'(m_k)}{2}\left[(x-m_k)^2\right]_{x_k}^{x_{k+1}} = \frac{f'(m_k)}{2}\left((x_{k+1}-m_k)^2-(x_k-m_k)^2\right)$$

D'où : $\displaystyle\int_{x_k}^{x_{k+1}} (x-m_k)\,f'(m_k)\,\mathrm{d}x = \frac{f'(m_k)}{2}\left(\left(\frac{h}{2}\right)^2-\left(-\frac{h}{2}\right)^2\right) = 0$

On en déduit avec (♠) que :

$$\int_{x_k}^{x_{k+1}} f(x)-f(m_k)-(x-m_k)\,f'(m_k)\,\mathrm{d}x = I_k - R_{n,k}(f)$$

Par suite :

$$|I_k - R_{n,k}(f)| = \left|\int_{x_k}^{x_{k+1}} f(x)-f(m_k)-(x-m_k)\,f'(m_k)\,\mathrm{d}x\right|$$

D'après la question 2 :

$$|I_k - R_{n,k}(f)| \leqslant \int_{x_k}^{x_{k+1}} |f(x)-f(m_k)-(x-m_k)\,f'(m_k)|\,\mathrm{d}x$$

D'après la question précédente :

$$|I_k - R_{n,k}(f)| \leqslant \int_{x_k}^{x_{k+1}} M_2\,\frac{(x-m_k)^2}{2}\,\mathrm{d}x$$

D'où :

$$|I_k - R_{n,k}(f)| \leqslant \frac{M_2}{6}\left[(x-m_k)^3\right]_{x_k}^{x_{k+1}}$$

D'où :

$$|I_k - R_{n,k}(f)| \leqslant \frac{M_2}{6}\left((x_{k+1}-m_k)^3-(x_k-m_k)^3\right) = \frac{M_2}{6}\left(\left(\frac{h}{2}\right)^3-\left(-\frac{h}{2}\right)^3\right) = \frac{M_2}{6}\times 2\frac{h^3}{8}$$

Finalement : $\forall\, k \in [\![\, 0, n-1\,]\!],\ |I_k - R_{n,k}(f)| \leqslant M_2\,\dfrac{(b-a)^3}{24n^3}$ (♣)

Par ailleurs, d'après la question 9 : $|I - R_n(f)| = \left|\displaystyle\sum_{k=0}^{n-1} I_k - R_{n,k}(f)\right|$

D'après l'inégalité triangulaire (q. 3) : $|I - R_n(f)| \leqslant \displaystyle\sum_{k=0}^{n-1} |I_k - R_{n,k}(f)|$

D'après (♣) : $|I - R_n(f)| \leqslant \displaystyle\sum_{k=0}^{n-1} M_2\frac{(b-a)^3}{24n^3}$

Or : $\displaystyle\sum_{k=0}^{n-1} M_2\frac{(b-a)^3}{24n^3} = n\times M_2\frac{(b-a)^3}{24n^3} = M_2\frac{(b-a)^3}{24n^2}$

Conclusion. $|I - R_n(f)| \leqslant M_2 \dfrac{(b-a)^3}{24n^2}$

Remarque. *On en déduit que* $\lim\limits_{n\longrightarrow+\infty} R_n(f) = \displaystyle\int_a^b f$. *Ceci signifie que la méthode des rectangles médians converge (la somme des aires des rectangles tend vers l'intégrale de f), et que cette convergence est quadratique (dans le sens où l'on doit calculer 10^3 termes si l'on souhaite avoir une majoration de l'erreur de l'ordre de 10^{-6}). Cette méthode est donc plus efficace ("plus rapide") en général que la méthode des rectangles à gauche ou à droite.*

Partie 4 - Programmation en Python

Ecrire en langage Python une fonction `RM(f,a,b,n,M2)` qui reçoit comme paramètres une fonction `f`, trois flottants `a, b` et `M2`, et un entier `n`, et qui retourne la valeur de $R_n(f)$ (valeur approchée de $I = \displaystyle\int_a^b f$) obtenue par la méthode des rectangles médians, ainsi qu'une majoration de l'erreur commise (càd un majorant de $|I - R_n(f)|$).
On pourra supposer que la fonction f a déjà été préalablement définie.

```
def MR(f,a,b,n,M2):
    h =(b-a)/n # Définition du pas

    x =a # Initialisation de x(k) à x(0) = a
    S =0 # Initialisation de la somme des rectangles

    for k in range(n):
        S +=h*f(x+(h/2)) # On rajoute à S l'aire du k-ème rectangle
        x +=h # On passe de x(k) à x(k+1)

    Maj_erreur =M2 *((b-a)**3) / (24*(n**2)) # Majorant de l'erreur
    return S, Maj_erreur
```

Problème 2A — Arithmétique

Notations. On rappelle que pour tout m entier relatif, $m\mathbb{Z}$ désigne l'ensemble des multiples de m.
Par ailleurs, on note $\mathscr{P}$ l'ensemble des nombres premiers. On admet dans ce problème que $53 \in \mathscr{P}$.

Partie 1 - Autour du nombre 53

1/ Etablir que les entiers 38 et 53 sont premiers entre eux.

53 est premier, et ne divise pas 38. **Conclusion**. $53 \wedge 38 = 1$

2/ Résoudre dans $\mathbb{Z}^2$ l'équation : (E_1) $38x + 53y = 6$.

Par la méthode décrite 200 fois en exercice on obtient :

$$(x, y) \text{ solution de } (E_1) \iff \exists\, k \in \mathbb{Z},\ (x, y) = (42 + 53k, -30 - 38k)$$

3/ Soit m un entier relatif. Montrer que :

$$[\,m \text{ est un inverse de 38 modulo 53}\,] \iff [\exists\, k \in \mathbb{Z},\ m = 60 + 53\,k]$$

Prouvons $\Longrightarrow$. Supposons que m est un inverse de 38 modulo 53.

Alors : $38m \equiv 1\,[53]$.

Par ailleurs, il résulte des calculs de la question précédente que : $38 \times 7 \equiv 1\,[53]$.

On en déduit que : $53\,|38(m-7)$. Or 53 et 38 sont premiers entre eux. D'où : $53\,|(m-7)$.

D'où : $m \equiv 7\,[53]$. D'où : $m \equiv 60\,[53]$. Donc : $\exists\, k \in \mathbb{Z},\ m = 60 + 53\,k$.

Ainsi : $[\,m$ est un inverse de 38 modulo $53\,] \Longrightarrow [\exists\, k \in \mathbb{Z},\ m = 60 + 53\,k]$

Réciproquement, supposons que : $\exists\, k \in \mathbb{Z},\ m = 60 + 53\,k$.

Alors : $m \equiv 60\,[53]$. D'où : $m \equiv 7\,[53]$. Or : $38 \times 7 \equiv 1\,[53]$. D'où : $38m \equiv 1\,[53]$.

Ainsi : $[\,m$ est un inverse de 38 modulo $53\,] \Longleftarrow [\exists\, k \in \mathbb{Z},\ m = 60 + 53\,k]$

Conclusion. $[\,m$ est un inverse de 38 modulo $53\,] \iff [\exists\, k \in \mathbb{Z},\ m = 60 + 53\,k]$

4/ Soit $n \in \mathbb{Z}$, tel que $n \notin 53\mathbb{Z}$. A l'aide du petit théorème de Fermat, établir que :

$$53 | n^{52} - 1$$

Soit $n \in \mathbb{Z}$. Puisque $53 \in \mathscr{P}$, le petit théorème de Fermat permet d'affirmer que : $n^{53} \equiv n\,[53]$.

D'où : $53\,|n\,(n^{52}n - 1)$. Or n et 53 sont premier entre eux, puisque $53 \in \mathscr{P}$ et ne divise pas n.

On en déduit que : $53\,|n^{52} - 1$

Conclusion. $\forall\, n \in \mathbb{Z}\backslash 53\mathbb{Z}$, $\quad 53\,|n^{52} - 1$

5/ Etablir qu'il n'existe pas de triplet d'entiers $(x, y, z) \in \mathbb{Z}^3$ tel que : $x^{520} + y^{520} + z^{520} = 20 + 53 \times 11^{2024}$.

Partie 2 - Une infinité de premiers $p \equiv 1\ [4]$

La fin de ce problème consiste à établir qu'il existe une infinité de nombre premiers congrus à 1 modulo 4 (comme 53).

Raisonnons par l'absurde, et supposons qu'il existe seulement un nombre fini p_1, p_2,..., p_m de nombres premiers congrus à 1 modulo 4.

On pose : $\quad N = 1 + 4 \times \left(\prod_{k=1}^{m} p_k^2\right)$ soit : $N = 1 + 4\,(p_1 \times \cdots \times p_m)^2$. Soit p un diviseur premier de N.

6/ Justifier que $p \geqslant 3$.

2 ne divise clairement pas N, qui est manifestement impair ! Donc p est un premier différent de 2...

Conclusion. $p \geqslant 3$

7/ On note : $x = 2\prod_{k=1}^{m} p_k$. Calculer x^2+1 modulo p.

On a : $x^2+1 = N$ et $p|N$ selon l'énoncé. **Conclusion**. $x^2+1 \equiv 0\,[p]$

8/ Etablir que p ne divise pas x. En déduire que : $x^{p-1} \equiv 1\ [p]$.

Si p divisait x, alors il diviserait x^2, donc il diviserait $N - x^2 = 1$. C'est absurde.

Donc p ne divise pas x. Puisqu'il est premier, le corollaire du petit théorème de Fermat assure que : $x^{p-1} \equiv 1\ [p]$.

Conclusion. $x \in \mathbb{Z}\backslash p\mathbb{Z}$ et $x^{p-1} \equiv 1\ [p]$.

9/ Justifier que $\dfrac{p-1}{2}$ est un entier naturel, et établir que : $(-1)^{\frac{p-1}{2}} \equiv 1\ [p]$.

Puisque $p \in \mathscr{P}\backslash\{2\}$, p est impair. Il s'ensuit que $p-1$ est pair (et positif), d'où : $\dfrac{p-1}{2} \in \mathbb{N}$.

De plus : $x^{p-1} = \left(x^2\right)^{(p-1)/2}$. Or $x^2 \equiv -1\ [p]$ d'après la question 7, et $x^{p-1} \equiv 1\ [p]$ d'après la question précédente.

Conclusion. $(-1)^{\frac{p-1}{2}} \equiv 1\ [p]$

10/ En déduire que : $p \equiv 1\ [4]$. En exhibant une contradiction, conclure.

Puisque $(-1)^{(p-1)/2} \equiv 1\ [p]$ d'après la question précédente, et que 1 et -1 ne sont pas égaux modulo p (puisque $p \geqslant 3$), on peut affirmer que $\frac{p-1}{2}$ est pair. Il existe donc un entier k tel que $\frac{p-1}{2} = 2k$. On en déduit que $p = 4k+1$. Ainsi $p \equiv 1\ [4]$.

L'entier p étant un nombre premier congru à 1 modulo 4, c'est l'un des p_i. Par suite : $p|\prod_{k=1}^{m} p_k$. Donc $p|x$. Ce qui contredit le fait que p ne divise pas x (question 8).

Conclusion. Il existe une infinité de nombres premiers congrus à 1 modulo 4.

Problème 2B — Groupe des automorphismes de $\mathbb{U}_n$

Rappels et notations. Soit n un entier naturel $\geqslant 2$.

On note $(\mathbb{U}_n, \times)$ le groupe des racines n-èmes de l'unité.

On note $\boldsymbol{\omega_n}$ la première racine n-ème de l'unité non-triviale, c'est-à-dire :

$$\boldsymbol{\omega_n = \mathrm{e}^{2\mathrm{i}\pi/n}} \qquad \text{Ainsi :} \quad \boldsymbol{\mathbb{U}_n = \left\{\omega_n^k,\ k \in [\![\, 0, n-1 \,]\!]\right\}}$$

Un ***endomorphisme*** du groupe $(\mathbb{U}_n, \times)$ est un morphisme de groupes de $(\mathbb{U}_n, \times)$ dans $(\mathbb{U}_n, \times)$, c'est-à-dire une application $f : \mathbb{U}_n \longrightarrow \mathbb{U}_n$ telle que :

$$\forall\ (z_1, z_2) \in \mathbb{U}_n^2, \quad f(z_1 \times z_2) = f(z_1) \times f(z_2)$$

Un ***automorphisme*** du groupe $(\mathbb{U}_n, \times)$ est un endomorphisme du groupe $\mathbb{U}_n$ bijectif.

On note $\mathrm{End}(\mathbb{U}_n)$ l'ensemble des endomorphismes du groupe $\mathbb{U}_n$.

On note $\mathrm{Aut}(\mathbb{U}_n)$ l'ensemble des automorphismes du groupe $\mathbb{U}_n$. On peut observer que : $\mathrm{id}_{\mathbb{U}_n} \in \mathrm{Aut}(\mathbb{U}_n)$.

On admettra que $(\mathrm{Aut}(\mathbb{U}_n), \circ)$ est un groupe pour la composition des applications.

Partie 1 - Questions préliminaires

1/ Soit $f \in \mathrm{End}(\mathbb{U}_n)$. Justifier brièvement que : $f(1) = 1$

Puisque f est un morphisme de groupes, l'image de l'élément neutre par f est l'élément neutre.

Conclusion. $f \in \mathrm{End}(\mathbb{U}_n) \Longrightarrow f(1) = 1$

2/ Soit $f \in \mathrm{End}(\mathbb{U}_n)$, et soit $z \in \mathbb{U}_n$. Etablir que : $\forall\, m \in \mathbb{N},\ f\left(z^m\right) = f\left(z\right)^m$

Puisque f est compatible avec la multiplication, une récurrence immédiate fournit le résultat.

Conclusion. $\forall\, m \in \mathbb{N},\ f\left(z^m\right) = f\left(z\right)^m$

3/ Dans cette question, on prouve qu'un endomorphisme du groupe $\mathbb{U}_n$ est uniquement déterminé par l'image de ω_n. A cette fin, on considère deux éléments f et g de $\mathrm{End}(\mathbb{U}_n)$.

a/ Justifier brièvement que : $\mathrm{Im}(f) = \left\{\left(f\left(\omega_n\right)\right)^k,\ k \in [\![\, 0, n-1 \,]\!]\right\}$

Soit f dans $\mathrm{End}(\mathbb{U}_n)$.

On a :

$$\mathrm{Im}(f) = f\left(\mathbb{U}_n\right) = \left\{f\left(\omega_n^k\right),\ k \in [\![\, 0, n-1 \,]\!]\right\} = \left\{f\left(\omega_n\right)^k,\ k \in [\![\, 0, n-1 \,]\!]\right\}$$

Conclusion. $\mathrm{Im}(f) = \left\{\left(f\left(\omega_n\right)\right)^k,\ k \in [\![\, 0, n-1 \,]\!]\right\}$

b/ Etablir que :

$$[f(\omega_n) = g\left(\omega_n\right)] \Longleftrightarrow [\forall\, z \in \mathbb{U}_n, \quad f(z) = g(z)]$$

Soient f et g dans $\mathrm{End}(\mathbb{U}_n)$. Supposons que $f(\omega_n) = g\left(\omega_n\right)$.

Soit $z \in \mathbb{U}_n$: $\exists\, k \in [\![\, 0, n-1 \,]\!],\ z = \omega_n^k$.

Alors : $f(z) = f\left(\omega_n^k\right) = f\left(\omega_n\right)^k = g\left(\omega_n\right)^k = g\left(\omega_n^k\right) = g(z)$

Conclusion. $[f(\omega_n) = g\left(\omega_n\right)] \Longleftrightarrow [\forall\, z \in \mathbb{U}_n, \quad f(z) = g(z)]$

Remarque. *Ceci signifie qu'un endomorphisme f du groupe $\mathbb{U}_n$ est uniquement déterminé par l'image de ω_n (la première racine n-ème de l'unité différente de 1). Il suffit de se donner $f(\omega_n)$ pour définir complètement f ; et deux morphismes de groupes prenant la même valeur en ω_n sont donc égaux.*

Partie 2 - Les cas $n = 4$ et $n = 5$

4/ Le groupe Aut$(\mathbb{U}_4)$.

Dans cette question, pour tout $k \in [\![\, 0, 3 \,]\!]$, on note f_k l'endomorphisme de $\mathbb{U}_4$ défini en posant $f_k(\mathrm{i}) = \mathrm{i}^k$.

a/ Etablir que $\mathrm{Im}(f_3) = \mathbb{U}_4$. En déduire que $f_3 \in \mathrm{Aut}(\mathbb{U}_4)$.

On a :

$$\mathrm{Im}(f_3) = f_3(\mathbb{U}_4) = \left\{1^3, \mathrm{i}^3, (-1)^3, (-\mathrm{i})^3\right\} = \{1, -\mathrm{i}, -1, \mathrm{i}\} = \mathbb{U}_4$$

On en déduit que $f_3 : \mathbb{U}_4 \longrightarrow \mathbb{U}_4$ est surjectif. Puisque l'ensemble de définition et l'ensemble d'arrivée de f_3 sont finis et de même cardinal, on en déduit que f_3 est bijective.

En résumé, f_3 est un endomorphisme de $\mathbb{U}_4$ bijectif.

Conclusion. $f_3 \in \mathrm{Aut}(\mathbb{U}_4)$ (f_3 est un automorphisme de $\mathbb{U}_4$).

b/ Etablir que $\mathrm{Im}(f_2) = \mathbb{U}_2$. En déduire que $f_2 \notin \mathrm{Aut}(\mathbb{U}_4)$.

On a :

$$\mathrm{Im}(f_2) = f_2(\mathbb{U}_4) = \left\{1^2, \mathrm{i}^2, (-1)^2, (-\mathrm{i})^2\right\} = \{1, -1\} = \mathbb{U}_2$$

On en déduit que $f_2 : \mathbb{U}_4 \longrightarrow \mathbb{U}_4$ n'est pas surjectif, donc n'est pas bijectif, donc n'est pas un automorphisme.

Conclusion. $\mathrm{Im}(f_2) = \mathbb{U}_2$ d'où $f_2 \notin \mathrm{Aut}(\mathbb{U}_4)$.

Remarque : on peut en déduire que le groupe $\mathrm{Aut}(\mathbb{U}_4)$ *est de cardinal* 2*, car il ne contient que* $f_1 = \mathrm{id}_{\mathbb{U}_4}$*, et* f_3.

5/ Le groupe Aut$(\mathbb{U}_5)$.

Dans cette question, on note $\omega_5 = \mathrm{e}^{2\mathrm{i}\pi/5}$, et pour tout $k \in [\![\, 0, 4 \,]\!]$, on note g_k l'endomorphisme de $\mathbb{U}_5$ défini en posant $g_k(\omega_5) = \omega_5^k$.

a/ Déterminer le noyau de g_0. En déduire que $g_0 \notin \mathrm{Aut}(\mathbb{U}_5)$.

Par définition : $\forall\, z \in \mathbb{U}_5,\ g_0(z) = z^0 = 1$. Il s'ensuit que $\ker g_0 = \mathbb{U}_5$.

Puisque $\ker g_0 \neq \{1\}$, l'endomorphisme g_0 n'est pas injectif, donc n'est pas bijectif.

Conclusion. $\ker g_0 = \mathbb{U}_5$ d'où $g_0 \notin \mathrm{Aut}(\mathbb{U}_5)$.

b/ Justifier que : $\quad g_2 \circ g_3 = \mathrm{id}_{\mathbb{U}_5} = g_3 \circ g_2$

On a :

$$(g_2 \circ g_3)(\omega_5) = g_2(\omega_5^3) = \omega_5^6 = \omega_5 \text{ (puisque } \omega_5^5 = 1)$$

De même :

$$(g_3 \circ g_2)(\omega_5) = g_3(\omega_5^2) = \omega_5^6 = \omega_5$$

Ainsi : $(g_3 \circ g_2)(\omega_5) = \mathrm{id}_{\mathbb{U}_5}(\omega_5) = (g_2 \circ g_3)(\omega_5)$

D'après la question 3-b : $g_2 \circ g_3 = \mathrm{id}_{\mathbb{U}_5} = g_3 \circ g_2$. **Conclusion**. $g_2 \circ g_3 = \mathrm{id}_{\mathbb{U}_5} = g_3 \circ g_2$

c/ Justifier que g_4 est une involution.

On a : $(g_4 \circ g_4)(\omega_5) = g_4(\omega_5^4) = \omega_5^{16} = \omega_5$ (puisque $\omega^{15} = 1$)

D'après la question 3-b : $g_4 \circ g_4 = \mathrm{id}_{\mathbb{U}_5}$. **Conclusion**. g_4 est une involution.

d/ En déduire que le groupe $\mathrm{Aut}(\mathbb{U}_5)$ est de cardinal 4, et qu'il est abélien.

D'après ce qui précède, g_2 et g_3 sont des automorphismes de $\mathbb{U}_5$ (et ils sont réciproques l'un de l'autre), de même que g_4 (qui est une involution). De plus $g_1 = \mathrm{id}_{\mathbb{U}_5}$ est naturellement une involution de $\mathbb{U}_5$.

Le dernier endomorphisme de $\mathbb{U}_5$ est g_0, qui n'est pas un endomorphisme (il est constant égal à 1 selon la question 5-a).

On en déduit que : $\mathrm{Aut}(\mathbb{U}_5) = \{g_1, g_2, g_3, g_4\}$. En particulier le groupe $\mathrm{Aut}(\mathbb{U}_5)$ est de cardinal 4, et il est donc abélien (puisque tout groupe de cardinal $\leqslant 5$ l'est).

Conclusion. Le groupe $\mathrm{Aut}(\mathbb{U}_5)$ est de cardinal 4, donc abélien.

Partie 3 - Arithmétique des automorphismes de $\mathbb{U}_n$

Dans cette partie, on note $\omega_n = \mathrm{e}^{2\mathrm{i}\pi/n}$ (où n désigne un entier naturel $\geqslant 2$).

Soit $\ell \in [\![\, 1, n-1 \,]\!]$. On note h_ℓ l'endomorphisme de $\mathbb{U}_n$ défini en posant : $h_\ell(\omega_n) = \omega_n^\ell$
On peut alors observer que : $\mathrm{Im}(h_\ell) = \left\{\omega_n^{k\ell},\ k \in [\![\, 0, n-1 \,]\!]\right\}$

6/ Soit N un entier naturel. Etablir que :

$$\left[\omega_n^N = 1\right] \iff [n \text{ divise } N]$$

Supposons que $\omega_n^N = 1$. Selon le théorème de la division euclidienne :

$$\exists (q, r) \in \mathbb{Z}^2,\ N = nq + r \text{ et } r \in [\![\, 0, n-1 \,]\!]$$

Ainsi : $\omega_n^N = \omega_n^{nq+r} = \underbrace{(\omega_n^n)^q}_{=1}\omega_n^r$.

Or par hypothèse $\omega_n^N = 1$, d'où : $\omega_n^r = 1$. D'où : $r = 0$. Il s'ensuit que $n|N$.

Ainsi : $\left[\omega_n^N = 1\right] \Longrightarrow [n \text{ divise } N]$

Réciproque immédiate.

Conclusion. $\left[\omega_n^N = 1\right] \iff [n \text{ divise } N]$

7/ Etablir que :

$$[n \wedge \ell = 1] \Longrightarrow \left[\text{Card}\left\{\omega_n^{k\ell},\ k \in [\![\, 0, n-1 \,]\!]\right\} = n\right]$$

Supposons que $n \wedge \ell = 1$.

Par l'absurde, supposons que $\text{Card}\left\{\omega_n^{k\ell},\ k \in [\![\, 0, n-1 \,]\!]\right\} < n$.

Il existe alors deux entiers $k < m$ dans $[\![\, 0, n-1 \,]\!]$ tels que $\omega_n^{k\ell} = \omega_n^{m\ell}$.

Par conséquent : $\omega_n^{(m-k)\ell} = 1$. D'après la question précédente, on en déduit que : $n|(m-k)$. Or ceci est absurde puisque $m-k$ est compris entre 1 et $n-1$.

Il s'ensuit que : $\text{Card}\left\{\omega_n^{k\ell},\ k \in [\![\, 0, n-1 \,]\!]\right\} = n$.

Conclusion. $[n \wedge \ell = 1] \Longrightarrow \left[\text{Card}\left\{\omega_n^{k\ell},\ k \in [\![\, 0, n-1 \,]\!]\right\} = n\right]$

8/ Etablir que :

$$[n \wedge \ell = 1] \Longleftrightarrow [h_\ell \in \text{Aut}(\mathbb{U}_n)]$$

Supposons que $n \wedge \ell = 1$. D'après la question précédente :

$$\text{Card}\left(h_\ell\left(\mathbb{U}_n\right)\right) = \text{Card}\left\{\omega_n^{k\ell},\ k \in [\![\, 0, n-1 \,]\!]\right\} = n$$

Il s'ensuit que $h_\ell\left(\mathbb{U}_n\right)$ est une partie de cardinal n de $\mathbb{U}_n$. Donc : $h_\ell\left(\mathbb{U}_n\right) = \mathbb{U}_n$.

Ceci signifie que h_ℓ est surjectif ; puisque son ensemble de départ et d'arrivée sont finis et de même cardinal, l'endomorphisme h_ℓ est bijectif.

Ainsi : $[n \wedge \ell = 1] \Longrightarrow [h_\ell \in \text{Aut}(\mathbb{U}_n)]$

Réciproquement, supposons que $h_\ell \in \text{Aut}(\mathbb{U}_n)$.

Par l'absurde, supposons que $n \wedge \ell \neq 1$. Alors il existe trois entiers d, n' et ℓ' dans $[\![\, 2, n-1 \,]\!]$ tels que :

$$n = dn' \quad \text{et} \quad \ell = d\ell'$$

On observe alors judicieusement que :

$$h_\ell\left(\omega_n^{n'}\right) = \omega_n^{n'\ell} = \omega_n^{n'd\ell'} = \omega_n^{n\ell'} = \left(\omega_n^n\right)^{\ell'} = 1$$

On en déduit que : $\omega_n^{n'} \in \ker h_\ell$. Or $\omega_n^{n'} \neq 1$ (puisque $n' \in [\![\, 2, n-1 \,]\!]$).

Par suite : $\ker h_\ell \neq \{1\}$. Donc h_ℓ n'est pas injectif, donc n'est pas un automorphisme de $\mathbb{U}_n$, ce qui contredit l'hypothèse initiale.

Ainsi : $[n \wedge \ell = 1] \Longleftarrow [h_\ell \in \text{Aut}(\mathbb{U}_n)]$

Conclusion. $[n \wedge \ell = 1] \Longleftrightarrow [h_\ell \in \text{Aut}(\mathbb{U}_n)]$

9/ Soit p un nombre premier. Etablir que : $\text{Card}\left(\text{Aut}\left(\mathbb{U}_p\right)\right) = p-1$

D'après la question précédente, il existe autant d'automrphismes de $\mathbb{U}_p$ que d'entiers de $[\![\, 1, p-1 \,]\!]$ premiers avec p. Or, puisque p est premier, tous les entiers de $[\![\, 1, p-1 \,]\!]$ sont premiers avec p.

Conclusion. $\text{Card}\left(\text{Aut}\left(\mathbb{U}_p\right)\right) = p-1$ (et $\text{Aut}(\mathbb{U}_p) = \{h_\ell,\ \ell \in [\![\, 1, p-1 \,]\!]\}$)

10/ Soient p un nombre premier, et $\alpha \in \mathbb{N}^*$. Etablir que : $\quad \text{Card}\left(\text{Aut}\left(\mathbb{U}_{p^\alpha}\right)\right) = p^\alpha - p^{\alpha-1}$

D'après la question 8, il existe autant d'automorphismes de $\mathbb{U}_{p^\alpha}$ que d'entiers de $[\![\, 1, p^\alpha - 1 \,]\!]$ premiers avec p.

Pour déterminer le nombre d'entiers de $[\![\, 1, p^\alpha - 1 \,]\!]$ premiers avec p, on peut déterminer le nombre d'entiers de $[\![\, 1, p^\alpha - 1 \,]\!]$ qui ne sont pas premiers avec p.

Soit m un entier de $[\![\, 1, p^\alpha - 1 \,]\!]$ non premier avec p. Alors $(p \in \mathscr{P})$ p divise m. Autrement écrit :

$$m \wedge p \neq 1 \iff p|m$$

Il suffit donc de compter le nombre de multiples de p compris entre 1 et $p^\alpha - 1$. Pour des raisons qu'il serait superfétatoire de détailler, il en existe exactement $p^{\alpha-1} - 1$.

Par conséquent, il existe exactement $(p^{\alpha-1} - 1)$ entiers dans $[\![\, 1, p^\alpha - 1 \,]\!]$ non premiers avec p.

Donc il existe exactement

$$p^\alpha - 1 - (p^{\alpha-1} - 1) = p^\alpha - p^{\alpha-1}$$

entiers dans $[\![\, 1, p^\alpha - 1 \,]\!]$ premiers avec p.

Conclusion. $\text{Card}\left(\text{Aut}\left(\mathbb{U}_{p^\alpha}\right)\right) = p^\alpha - p^{\alpha-1}$ (et : $\text{Aut}\left(\mathbb{U}_{p^\alpha}\right) = \{h_\ell,\ \ell \in [\![\, 1, p^\alpha - 1 \,]\!] \setminus p\mathbb{Z}\}$)

Remarque. *Par exemple :* $\text{Aut}\left(\mathbb{U}_9\right) = \text{Aut}\left(\mathbb{U}_{3^2}\right) = \{h_1, h_2, h_4, h_5, h_7, h_8\}$

et $\text{Aut}\left(\mathbb{U}_{25}\right) = \{h_1, h_2, h_3, h_4, h_6, h_7, h_8, h_9, h_{11}, h_{12}, h_{13}, h_{14}, h_{16}, h_{17}, h_{18}, h_{19}, h_{21}, h_{22}, h_{23}, h_{24}\}$