Devoir surveillé 6

▸ Problème 1 : autour du grand théorème de Fermat

Au XVII$^{\text{ème}}$ siècle, Pierre de Fermat énonce un théorème qui en termes modernes (puisque Fermat l'a énoncé en latin) s'écrit :

Théorème : *Pour $n \geqslant 3$, l'équation $x^n + y^n = z^n$ ne possède pas de solutions $(x, y, z) \in (\mathbf{N}^*)^3$.*

Notons que la précision que x, y et z sont non nuls n'est pas superflue puisque pour tout $x \in \mathbf{N}$, $x^n + 0^n = x^n$.

Ce problème a fasciné des générations de mathématiciens durant trois siècles et demi ans avant d'être prouvé en 1995 par Andrew Wiles, aidé par son élève Richard Taylor.
S'il n'est pas question d'aborder la preuve de ce théorème ici (vous connaissez l'histoire, elle ne tient ni dans la marge ni sur votre copie), nous nous proposons d'étudier dans ce problème les solutions à $x^2 + y^2 = z^2$, et de prouver un analogue au théorème de Fermat dans le cas (bien plus facile) où les inconnues ne sont plus des entiers mais des polynômes à coefficients complexes.

La partie I est indépendante des parties II et III (qui traitent le cas des polynômes).

1. Justifier que si le théorème de Fermat est vrai pour $n = 4$ et pour n premier impair, alors il est vrai pour tout $n \geqslant 3$.

Partie I : le cas $n = 2$
Dans le cas $n = 2$, il existe des solutions non triviales à l'équation $x^2 + y^2 = z^2$, la plus célèbre d'entre elles étant probablement $3^2 + 4^2 = 5^2$.
On cherche dans cette partie à déterminer tous les triplets $(x, y, z) \in (\mathbf{N}^*)^3$ tels que $x^2 + y^2 = z^2$.
Un tel triplet est appelé **triplet pythagoricien**. On parlera de **triplet pythagoricien primitif** si de plus $x \wedge y \wedge z = 1$.

2. Soit (x, y, z) un triplet pythagoricien, et soit $d = x \wedge y \wedge z$. On pose alors $x' = \frac{x}{d}, y' = \frac{y}{d}$ et $z' = \frac{z}{d}$.
   Justifier que (x', y', z') est un triplet pythagoricien primitif, et que x', y', z' sont deux à deux premiers entre eux.
3. Soit (x, y, z) un triplet pythagoricien primitif.
   a. Prouver que x et y ne sont pas tous deux pairs.
      À l'aide de congruences modulo 4, justifier que x et y ne sont pas tous deux impairs.

   Dans la suite, quitte à échanger x et y, on suppose que x est pair et y est impair.

   b. Justifier qu'il existe $(u, v, w) \in (\mathbf{N}^*)^3$ tels que $x = 2u$, $z + y = 2v$ et $z - y = 2w$.
   c. Montrer que $v \wedge w = 1$.
   d. Prouver que vw est un carré, en déduire que v et w sont des carrés.
      On pose alors $v = n^2$ et $w = m^2$, avec $(m, n) \in (\mathbf{N}^*)^2$.
   e. Montrer que $n > m$ et que n et m sont premiers entre eux.
4. Montrer que (x, y, z) est un triplet pythagoricien primitif si et seulement si il existe deux entiers n et m premiers entre eux, de parités distinctes, avec $n > m > 0$ tels que

$$\begin{cases} x = 2nm \\ y = n^2 - m^2 \\ z = n^2 + m^2 \end{cases} \quad \textbf{ou} \quad \begin{cases} x = n^2 - m^2 \\ y = 2nm \\ z = n^2 + m^2 \end{cases}$$

En déduire tous les triplets pythagoriciens.

Partie II. L'inégalité de Mason

Si $P \in \mathbf{C}[X]$ est un polynôme non nul à coefficients complexes, on note :

- $R(P)$ l'ensemble des racines complexes de P, et $r(P)$ le cardinal de $R(P)$
- si $z \in \mathbf{C}$, $\mu_P(z)$ désigne la multiplicité de z comme racine de P, avec la convention que $\mu_P(z) = 0$ si z n'est pas racine de P.

5. Soient $A, B, C \in \mathbf{C}[X]$, non nuls, tels que $A = BC$. Déterminer des relations entre :
   a. $\deg(A)$, $\deg(B)$ et $\deg(C)$
   b. $R(A), R(B)$ et $R(C)$
   c. $r(A), r(B)$ et $r(C)$
   d. $\mu_A(z), \mu_B(z)$ et $\mu_C(z)$, pour $z \in \mathbf{C}$
   e. $r(A)$ et $\deg(A)$
   f. $\deg(A)$ et $\sum_{z \in R(A)} \mu_A(z)$

6. On suppose dans cette question que A, B et C sont trois polynômes à coefficients complexes tels que $A + B + C = 0$.
   On suppose de plus que A, B, C ne sont pas tous les trois constants, et qu'il n'existe pas de racine commune aux trois polynômes A, B et C, c'est-à-dire que $R(A) \cap R(B) \cap R(C) = \emptyset$.
   a. Montrer que $R(A), R(B)$ et $R(C)$ sont deux à deux disjoints.
   b. Dans la suite de la question 6, on note $P = AB' - BA'$.
      i. Montrer que P n'est pas nul.
      ii. Prouver que $P = BC' - CB' = CA' - AC'$.
      iii. En déduire que $\deg(P) \leqslant \deg(B) + \deg(C) - 1$ et $\deg(P) \leqslant \deg(A) + \deg(C) - 1$.
   c. Soit $z \in R(A)$. Démontrer que $\mu_P(z) \geqslant \mu_A(z) - 1$. En déduire des inégalités analogues pour B et C.
   d. En sommant les inégalités précédemment obtenues, prouver que :
   $$\deg(P) \geqslant \sum_{z \in R(A)} (\mu_A(z) - 1) + \sum_{z \in R(B)} (\mu_B(z) - 1) + \sum_{z \in R(C)} (\mu_C(z) - 1).$$
   e. En déduire que $\deg(P) \geqslant \deg(A) + \deg(B) + \deg(C) - (r(A) + r(B) + r(C))$.
   f. Prouver alors, à l'aide des inégalités de la question 6.b.iii *l'inégalité de Mason* :
   $$r(A) + r(B) + r(C) \geqslant 1 + \max(\deg(A), \deg(B), \deg(C)).$$

Partie III. Le théorème de Fermat pour les polynômes

7. Soit $n \in \mathbf{N}^*$, soit $D \in \mathbf{C}[X] \setminus \{0_{\mathbf{C}[X]}\}$, et soient $(\alpha, \beta) \in \mathbf{C}^* \times \mathbf{C}^*$ tels que $\alpha^n + \beta^n \neq 0$. Justifier qu'il existe $\gamma \in \mathbf{C}^*$ tel que $\gamma^n = \alpha^n + \beta^n$, et qu'alors $(\alpha D)^n + (\beta D)^n = (\gamma D)^n$.
   Ainsi, il existe toujours des solutions non nulles à l'équation de Fermat. On cherche dans la suite à prouver qu'il s'agit là des seules solutions.

8. Soit n un entier supérieur ou égal à 3. Soient U, V, W des polynômes à coefficients complexes, non nuls, et ne possédant pas de racine commune (c'est-à-dire tels que $R(U) \cap R(V) \cap R(W) = \emptyset$) tels que $U^n + V^n + W^n = 0$.
   À l'aide de l'inégalité de Mason, prouver que U, V et W sont constants.

9. Soit n un entier supérieur ou égal à 3. Soient $\widehat{U}, \widehat{V}$ et $\widehat{W}$ des polynômes complexes, non nuls, sans racine commune tels que $\widehat{U}^n + \widehat{V}^n = \widehat{W}^n$.
   Prouver que $\widehat{U}, \widehat{V}$ et $\widehat{W}$ sont constants.

10. Soit n un entier naturel supérieur ou égal à 3, et soient A, B, C trois polynômes à coefficients complexes. Prouver que

$$A^n + B^n = C^n \Leftrightarrow \exists D \in \mathbf{C}[X] \setminus \{0_{\mathbf{C}[X]}\},\ \exists (\alpha, \beta, \gamma) \in (\mathbf{C}^*)^3,\ \begin{cases} \alpha^n + \beta^n = \gamma^n \\ A = \alpha D \\ B = \beta D \\ C = \gamma D \end{cases}$$

Ainsi, les seules solutions à l'équation de Fermat sont celles trouvées précédemment.

11. Pour $n = 2$, montrer qu'il existe des polynômes $U, V, W \in \mathbf{C}[X]$, non constants et sans racines communes (donc pas de la forme obtenue à la question précédente) tels que $U^2 + V^2 = W^2$.

▸ Problème 2 : 3-cycle implique chaos

Soit I un segment et soit $f : I \to I$.
Dans tout le problème, pour $n \in \mathbf{N}^*$, on note $f^n = \underbrace{f \circ f \circ \cdots \circ f}_{n \text{ fois}}$.

Pour $n \in \mathbf{N}^*$, un point $x_0 \in I$ est dit n-périodique si $f^n(x_0) = x_0$ et pour tout $k \in [\![1, n-1]\!]$, $f^k(x_0) \neq x_0$.
En particulier, un point 1-périodique est un point fixe de f.
Le but de ce problème est de prouver le résultat suivant, qui est un cas particulier d'un théorème prouvé par Sarkovskii en 1964.

> **Théorème :** *Soit I un segment de $\mathbf{R}$ et soit $f : I \to I$ une fonction continue. S'il existe un point 3-périodique, alors pour tout $n \in \mathbf{N}^*$, il existe un point n-périodique.*

Dans toute la suite, on considère une fonction $f : I \to I$, **continue**, où I est un **segment** de $\mathbf{R}$.

1. Prouver que f possède un point fixe.
2. Soit J un segment non vide inclus dans I, et soit K un segment inclus dans $f(J)$.
   On se propose de prouver qu'il existe un segment L inclus dans J tel que $K = f(L)$.
   a. Prouver le résultat si K est un singleton.
   b. On suppose à présent que $K = [\alpha, \beta]$, avec $\alpha < \beta$.
   Justifier l'existence de $(a, b) \in J^2$ tels que $f(a) = \alpha$ et $f(b) = \beta$.
   c. On suppose de plus dans la suite de la question 2 que $a < b$, le raisonnement étant identique dans le cas $a > b$. Justifier l'existence de $v = \min\{t \in [a, b] \mid f(t) = \beta\}$.
   d. Justifier l'existence de $u = \max\{t \in [a, v] \mid f(t) = \alpha\}$.
   Prouver alors l'existence d'un segment $L \subset J$ tel que $f(L) = K$.
3. Soit K un segment inclus dans I tel que $K \subset f(K)$. Prouver que f admet au moins un point fixe dans K.

Si I_1, I_2 sont deux segments inclus dans I, on note $I_1 \longrightarrow I_2$ si $I_2 \subset f(I_1)$.
Pour $I_1, I_2, \ldots, I_n$ segments inclus dans I, on note $I_1 \longrightarrow I_2 \longrightarrow I_3 \longrightarrow \ldots \longrightarrow I_n$ si pour tout $k \in [\![1, n-1]\!]$, $I_k \longrightarrow I_{k+1}$.
On notera en particulier que le résultat de la question 3 se reformule de la manière suivante : si K est un segment tel que $K \longrightarrow K$, alors f possède un point fixe dans K.

4. On suppose qu'il existe $n+1$ segments non vides $I_0, I_1, \ldots, I_n$ tels que $I_0 \longrightarrow I_1 \longrightarrow I_2 \longrightarrow \ldots \longrightarrow I_n$.
   a. Prouver qu'il existe $J_0, J_1, \ldots, J_{n-1}$ segments non vides de I tels que
      i) $\forall k \in [\![0, n-1]\!]$, $J_k \subset I_k$
      ii) $\forall k \in [\![0, n-2]\!]$, $f(J_k) = J_{k+1}$ et $f(J_{n-1}) = I_n$
   b. Montrer que pour $x_0 \in J_0$, et pour $k \in [\![0, n-1]\!]$, $f^k(x_0) \in J_k$.

5. Montrer, à l'aide des questions 3 et 4, que s'il existe des segments $I_0, I_1, I_2, \dots, I_{n-1}$ tels que $I_0 \longrightarrow I_1 \longrightarrow I_2 \longrightarrow \dots \longrightarrow I_{n-1} \longrightarrow I_0$, alors il existe $x \in I_0$ tel que $f^n(x) = x$ et $\forall k \in [\![0, n-1]\!]$, $f^k(x) \in I_k$.
6. On suppose qu'il existe un point 3-périodique x. On note alors $x_0 = \min\{x, f(x), f^2(x)\}$, $x_1 = f(x_0)$ et $x_2 = f(x_1)$.
   a. Justifier que x_0, x_1, x_2 sont deux à deux distincts, et tous les trois 3-périodiques.
   b. On suppose $x_1 < x_2$. On pose alors $I_0 = [x_0, x_1]$ et $I_1 = [x_1, x_2]$.
   Prouver que $I_1 \longrightarrow I_1$ et $I_0 \longrightarrow I_1 \longrightarrow I_0$.
   En déduire que f possède un point fixe et un point 2-périodique.
   c. On suppose que $x_2 < x_1$. On note alors $J = -I = \{-t, t \in I\}$, et g la fonction définie sur J par $g(x) = -f(-x)$.
   En appliquant la question 6.b à g, montrer que f possède un point fixe et un point 2-périodique.
7. On suppose toujours que f possède un point 3-périodique x.
   En cherchant une suite de la forme $I_0 \longrightarrow I_1 \longrightarrow I_1 \dots \longrightarrow I_1 \longrightarrow I_0$, montrer que pour tout $n \in \mathbf{N}^*$, f possède un point n-périodique.
8. Soit f la fonction définie sur $[0, 1]$ par $f(x) = \begin{cases} 2x & \text{si } x < \frac{1}{2} \\ 2(1-x) & \text{si } x \geqslant \frac{1}{2} \end{cases}$
   a. À l'aide de l'un des points $0, \frac{2}{3}, \frac{2}{5}, \frac{2}{7}$, montrer que f possède un point n-périodique pour tout $n \in \mathbf{N}^*$.
   b. **Question subsidiaire, à ne traiter que si vous avez traité tout le sujet.**
   Pour $n \in \mathbf{N}^*$, on note x_n le plus petit point n-périodique de f.
   Déterminer un équivalent de x_n, ainsi qu'une majoration du nombre de points n-périodiques de f.

Juste pour la culture, énonçons le résultat bien plus fort (et très surprenant) prouvé par Sarkovskii : il commence par définir une relation d'ordre totale $\prec$ sur $\mathbf{N}^*$ de la manière suivante :

$$3 \succ 5 \succ 7 \succ 9 \succ \dots \succ 2\times 3 \succ 2\times 5 \succ 2\times 7 \succ 2\times 9 \succ \dots$$
$$\dots \succ 2^n \times 3 \succ 2^n \times 5 \succ \dots \succ 2^{n+1} \times 3 \succ 2^{n+1} \times 5 \succ \dots 2^n \succ 2^{n-1} \succ \dots \succ 4 \succ 2 \succ 1.$$

Alors si $f : I \to I$ est une fonction continue sur un segment I, si f possède un point n-périodique, alors elle possède un point p-périodique pour tout $p \prec n$.
Le cas particulier que nous avons traité découle du fait que 3 est le plus grand élément de $\mathbf{N}^*$ pour $\prec$.

CORRECTION DU DEVOIR SURVEILLÉ 6

PROBLÈME : AUTOUR DU GRAND THÉORÈME DE FERMAT

1. Supposons le théorème de Fermat vrai pour les exposants premiers impairs et pour 4.
Soit $n \geqslant 3$. Supposons par l'absurde qu'il existe $(x,y,z) \in (\mathbf{N}^*)^3$ tels que $x^n + y^n = z^n$.
Alors soit n possède un facteur premier impair p, et donc il existe $k \in \mathbf{N}$ tel que $n = kp$.
Et alors $(x^k)^p + (y^k)^p = (z^k)^p$, ce qui est impossible puisque le théorème de Fermat est vrai pour p.
Soit n ne possède que 2 comme facteur premier, et étant supérieur à 3, il est divisible par 4 : il existe $k \in \mathbf{N}^*$ tel que $n = 4k$.
Et alors comme précédemment, $(x^k)^4 + (y^k)^4 = (z^k)^4$, ce qui est également absurde.
Donc si le théorème de Fermat est vrai pour les exposants premiers impairs et pour 4, alors il est vrai pour tout $n \geqslant 3$.

Partie I : le cas $n = 2$ (triplets pythagoriciens)

2. Il est évident que x', y' et z' sont premiers entre eux dans leur ensemble.
On a alors $x'^2 + y'^2 = \frac{1}{d^2}(x^2 + y^2) = \frac{z^2}{d^2} = z'^2$.
Donc $\boxed{(x', y', z') \text{ est un triplet pythagoricien primitif.}}$
Soit k un diviseur commun à x' et y'. Alors k^2 divise $x'^2 + y'^2 = z'^2$. Ce qui signifie que pour tout p premier, $2v_p(k) = v_p(k^2) \leqslant v_p(z'^2) = 2v_p(z')$.
Donc $v_p(k) \leqslant v_p(z')$, et ceci étant vrai pour tout premier p, k divise z'.
Et donc k divise x', y' et z', et donc vaut 1 car x', y', z' sont premiers entre eux dans leur ensemble.
Ainsi, $x' \wedge y' = 1$.

Sur le même principe, un diviseur commun de x' et de z' est un diviseur de y' à l'aide de la relation $y'^2 = z'^2 - x'^2$.

3.a. Nous venons de prouver que si (x,y,z) est un triplet pythagoricien primitif, alors x et y sont premiers entre eux, et donc ne peuvent être tous deux multiples de 2.
Si k est impair, alors $k \equiv 1\ [4]$ ou $k \equiv 3\ [4]$, et dans les deux cas, $k^2 \equiv 1\ [4]$.
Supposons par l'absurde que x et y sont impairs tous les deux. Alors $x^2 + y^2 \equiv 2\ [4]$.
Or, $x^2 + y^2 = z^2$, et modulo 4 un carré vaut 0 ou 1, d'où une contradiction.
Ainsi, $\boxed{x \text{ et } y \text{ sont de parités opposées.}}$

3.b. Puisque x est pair, il existe $u \in \mathbf{N}^*$ tel que $x = 2u$.
Par ailleurs, z^2 est de même parité que y^2, donc[1] z et y sont de même parité, et donc $z + y$ et $z - y$ sont pairs.
il existe donc $v \in \mathbf{N}^*$ tel que $z + y = 2v$.
Enfin, $z^2 = y^2 + x^2 > y^2$, donc $z > y$, de sorte que $z - y > 0$. Et donc il existe $w \in \mathbf{N}^*$ tel que $z - y = 2w$.

[1] Un entier et son carré sont toujours de même parité.

3.c. Soit d un diviseur commun à v et w. Alors $2d$ divise $2v + 2w = 2z$ et donc $d \mid z$.
Et de même, $2d \mid 2w - 2v = 2y$, et donc $d \mid y$.
Par ailleurs, $4d^2$ divise $2v \times 2w = z^2 - y^2 = x^2$.
Et donc en particulier, $d^2 \mid x^2$, de sorte que[2] $d \mid x$.
Ainsi, d divise $x \wedge y \wedge z = 1$, et donc $d = 1$. On a donc prouvé que $\boxed{v \wedge w = 1.}$

[2] Voir la preuve qui a été donnée question 2.

3.d. On a $4vw = y^2 - z^2 = x^2 = 4u^2$ et donc $vw = u^2$ $\boxed{\text{est un carré.}}$
Alors pour tout premier p, $v_p(vw) = v_p(u^2) = 2v_p(u)$.
Mais v et w étant premiers entre eux, $v_p(v) = 0$ ou $v_p(w) = 0$.
Et donc soit $v_p(v) = 0$, et alors $v_p(w)$ est pair, soit $v_p(w) = 0$ et alors $v_p(v)$ est pair.
Ainsi, pour tout premier p, $v_p(v)$ et $v_p(w)$ sont pairs, et donc il existe a_p, b_p entiers tels que $v_p(v) = 2a_p$ et $v_p(w) = 2b_p$.
Et alors

$$v = \left(\prod_{p\in\mathcal{P}} p^{a_p}\right)^2 \text{ et } w = \left(\prod_{p\in\mathcal{P}} p^{b_p}\right)^2$$

sont des carrés.

3.e. Puisque $y \neq 0$, $z+y > z-y$, et donc $2n^2 > 2m^2$, donc $n > m$.
Par ailleurs, tout diviseur commun à m et n est un diviseur commun à $v = n^2$ et $w = m^2$, et donc est un diviseur de $v \wedge w = 1$.
Donc $\boxed{m \wedge n = 1.}$

4. Nous venons de prouver que si (x,y,z) est primitif, alors il est bien de l'une des deux[3] formes annoncées.
Un seul point n'a alors pas été prouvé : c'est que m et n sont de parités distinctes. Mais si m et n étaient de même parité, alors m^2 et n^2 aussi, et donc y et z seraient tous deux pairs, contredisant le fait que $y \wedge z = 1$.

[3] La première si x est pair, la seconde sinon.

Inversement, reste à vérifier que pour $n > m$ premiers entre eux et de parités distinctes, $(x,y,z) = (2nm, n^2-m^2, n^2+m^2)$ est bien un triplet pythagoricien primitif. Mais

$$(2nm)^2 + (n^2-m^2)^2 = 4^2n^2m^2 + n^4 - 2n^2m^2 + m^4 = n^4 + 2n^2m^2 + m^4 = (n^2+m^2)^2.$$

Détails
Rappelons qu'un entier est premier avec un produit si et seulement si il est premier avec chacun des facteurs.
Donc $m \wedge n = 1 \Rightarrow m \wedge n^2 = 1$ puis $m^2 \wedge n^2 = 1$.

Donc on est bien en présence d'un triplet pythagoricien. Il est primitif puisque si $d = x \wedge y \wedge z$, alors d est un diviseur commun à y et z, et donc aussi un diviseur de $2n^2 = z-y$ et $2m^2 = z+y$.
Mais puisque $n \wedge m = 1$, $n^2 \wedge m^2 = 1$, et donc $2n^2 \wedge 2m^2 = 2$.
Donc $d = 1$ ou $d = 2$. Or on ne peut pas avoir $d = 2$, car m et n étant de parités distinctes, il en est de même de m^2 et n^2, et donc de y et z.
Ainsi, $x \wedge y \wedge z = 1$, et donc (x,y,z) est un triplet pythagorien primitif.

Par la question 2, si (x,y,z) est un triplet pythagoricien, et si $d = x \wedge y \wedge z$, alors $\left(\frac{x}{d}, \frac{y}{d}, \frac{z}{d}\right)$ est un triplet pythagoricien primitif.
Donc il existe n, m premiers entre eux, de parités distinctes, avec $n > m$ tels que

$$\begin{cases} \frac{x}{d} = 2mn \\ \frac{y}{d} = n^2-m^2 \\ \frac{z}{d} = n^2+m^2 \end{cases} \Leftrightarrow \begin{cases} x = 2mnd \\ y = d(n^2-m^2) \\ z = d(m^2+n^2) \end{cases} \quad \textbf{ou} \quad \begin{cases} \frac{y}{d} = 2mn \\ \frac{x}{d} = n^2-m^2 \\ z = n^2+m^2 \end{cases} \Leftrightarrow \begin{cases} y = 2mnd \\ x = d(n^2-m^2) \\ z = d(m^2+n^2) \end{cases}$$

Et inversement, si $n > m$ sont premiers entre eux, de parités distinctes, et $d \in \mathbf{N}^*$ alors

$$(2mnd)^2 + \left(d\left(n^2-m^2\right)\right)^2 = d^2\left(n^4+4m^2n^2+m^4\right) = d^2\left(m^2+n^2\right)^2 = \left(d\left(n^2+m^2\right)\right)^2$$

de sorte que $\left(2mnd, d\left(n^2-m^2\right), d\left(n^2+m^2\right)\right)$ et $\left(d\left(n^2-m^2\right), 2mnd, d\left(n^2+m^2\right)\right)$ sont des triplets pythagoriciens.
Et donc les triplets pythagoriciens sont exactement les triplets de la forme

$$\left(2mnd, d\left(n^2-m^2\right), d\left(n^2+m^2\right)\right) \textbf{ ou } \left(d\left(n^2-m^2\right), 2mnd, d\left(n^2+m^2\right)\right)$$

avec $d \in \mathbf{N}^*$, $n > m$ premiers entre eux de parités distinctes.

Partie II : l'inégalité de Mason

5.a. C'est directement du cours : $\boxed{\deg(A) = \deg(B) + \deg(C).}$

5.b. Un complexe z est racine de A si et seulement si[4] il est racine de B ou de C.
Et donc $\boxed{R(A) = R(B) \cup R(C).}$

[4] C'est l'intégrité de $\mathbf{C}$: un produit de complexes est nul si et seulement si l'un des facteurs est nul.

5.c. Nous ne savons pas si $R(B)$ et $R(C)$ sont ou non disjoints[5], mais on a toujours $\boxed{r(A) \leqslant r(B) + r(C).}$

[5] Auquel cas l'inégalité qui suit est une égalité.

5.d. On a $B = (X-z)^{\mu_B(z)}B_1$ avec $B_1 \in \mathbf{C}[X]$ tel que $B_1(z) \neq 0$, et de même, $C = (X-z)^{\mu_C(z)}C_1$ avec $C_1(z) \neq 0$.
Donc $A = (X-z)^{\mu_B(z)+\mu_C(z)}B_1C_1$ avec $(B_1C_1)(z) \neq 0$, donc la multiplicité de z en tant que racine de A est égale à $\mu_B(z) + \mu_C(z)$, soit encore $\boxed{\mu_A(z) = \mu_B(z) + \mu_C(z).}$

5.e. Un polynôme non nul possède au plus autant de racines que son degré donc $\boxed{r(A) \leqslant \deg(A).}$

Détails
$r(A)$ désigne le nombre de racines **distinctes** de A, comptées sans multiplicité.

5.f. Tout polynôme à coefficient complexe est scindé sur $\mathbf{C}$, donc si $\alpha \neq 0$ désigne le coefficient dominant de A, on a

$$A = \alpha \prod_{z \in R(A)} (X-z)^{\mu_A(z)}.$$

Et donc par identification des degrés, $\boxed{\deg(A) = \sum_{z\in R(A)} \mu_A(z).}$

6.a. Supposons par l'absurde qu'il existe $z \in \mathbf{C}$ racine commune à A et B.
Alors $C(z) = -A(z) - B(z) = 0$, et donc $z \in R(A) \cap R(B) \cap R(C)$, ce qui n'est pas possible.
On prouve de même que $\boxed{R(B) \cap R(C) = R(A) \cap R(C) = \emptyset.}$

6.b.i. Supposons par l'absurde que $P = 0 \Leftrightarrow AB' = A'B$.
Si A n'est pas constant, par le théorème de d'Alembert-Gauss, il existe $z \in \mathbf{C}$ racine de A.
Et alors $\mu_{A'}(z) = \mu_A(z) - 1$.
Puisque par ailleurs, z n'est pas racine de B, $\mu_{A'B}(z) = \mu_{A'}(z) + \underbrace{\mu_B(z)}_{=0} = \mu_A(z) - 1$.
Mais la multiplicité de z comme racine de AB' est au moins égale à $\mu_A(z) > \mu_{A'B}(z)$, ce qui est absurde.

Et si A est constant, alors B ne l'est pas (faute de quoi $C = -A - B$ le serait également et donc A, B, C seraient tous trois constants), et on peut tenir le même raisonnement à l'aide d'une racine de B.
Donc $\boxed{P \text{ n'est pas le polynôme nul.}}$

> **Rappel**
> Si z est racine de P de multiplicité $m \geqslant 1$, alors z est racine de P' de multiplicité $m - 1$ (si $m = 0$, cela signifie que z n'est pas racine de P'.)

6.b.ii. Puisque $A = -B - C$, on a $A' = -B' - C'$, et donc

$$P = (-B - C)B' - B(-B' - C') = \boxed{BC' - CB'.}$$

On prouve de même que $\boxed{P = CA' - AC'.}$

> **Degré**
> Rappelons que le degré d'une somme est **inférieur ou égal** au plus haut degré des termes de la somme, et que si ces degrés sont distincts, alors c'est une égalité.

6.b.iii. On a $\deg P \leqslant \max(\deg(BC'), \deg(CB'))$.
Mais $\deg(BC') = \deg(B) + \deg(C') = \deg(B) + \deg(C) - 1$ et $\deg(CB') = \deg(C) + \deg(B) - 1$.
Donc $\boxed{\deg P \leqslant \deg B + \deg C - 1.}$
On prouve de même la seconde inégalité en utilisant $P = CA' - AC'$.

6.c. Nous avons déjà dit que $\mu_{A'}(z) = \mu_A(z) - 1$.
Et donc A étant divisible par $(X - z)^{\mu_A(z)}$, il est divisible par $(X - z)^{\mu_A(z)-1}$, et donc AB' est aussi divisible par $(X - z)^{\mu_A(z)-1}$.
De même, A' est divisible par $(X - z)^{\mu_{A'}(z)} = (X - z)^{\mu_A(z)-1}$, et donc $P = AB' - BA'$ est divisible par $(X - z)^{\mu_A(z)-1}$.
On en déduit donc que la multiplicité de z en tant que racine de P est au moins égale à $\mu_A(z) - 1$, c'est-à-dire que $\boxed{\mu_P(z) \geqslant \mu_A(z) - 1.}$
Et bien entendu, on a aussi $\mu_P(z) \geqslant \mu_B(z) - 1$ et $\mu_P(z) \geqslant \mu_C(z) - 1$.

6.d. Nous savons que $\deg(P) = \sum_{z\in R(P)} \mu_P(z)$.
Or la question précédente prouve que parmi les racines de P se trouvent les racines au moins doubles de A, les racines au moins doubles de B et les racines au moins doubles de C.
Notons donc $R_2(A) = \{z \in R(A) \mid \mu_A(z) \geqslant 2\}$ et de même, $R_2(B)$ et $R_2(C)$.
Alors $R_2(A) \cup R_2(B) \cup R_2(C) \subset R(P)$, et cette union est disjointe puisque A, B et C n'ont pas de racines en commun.
Donc il vient

$$\begin{aligned}
\deg(P) = \sum_{z\in R(P)} \mu_P(z) &\geqslant \sum_{z\in R_2(A)\cup R_2(B)\cup R_2(c)} \mu_P(z) \\
&= \sum_{z\in R_2(A)} \mu_P(z) + \sum_{z\in R_2(B)} \mu_P(z) + \sum_{z\in R_2(C)} \mu_P(z) \\
&\geqslant \sum_{z\in R_2(A)} (\mu_A(z) - 1) + \sum_{z\in R_2(B)} (\mu_B(z) - 1) + \sum_{z\in R_2(C)} (\mu_C(z) - 1) \\
&\boxed{\geqslant \sum_{z\in R(A)} (\mu_A(z) - 1) + \sum_{z\in R(B)} (\mu_B(z) - 1) + \sum_{z\in R(C)} (\mu_C(z) - 1).}
\end{aligned}$$

C'est une égalité car $R_2(A)$, $R_2(B)$ et $R_2(C)$ sont deux à deux disjoints.
C'est la question précédente.

> **Détails**
> Les termes que nous avons ajouté à la première somme correspondent aux racines simples de A, pour lesquel $\mu_A(z) - 1 = 0$.
> Et de même pour les autres sommes.

6.e. Il s'agit de noter que

$$\sum_{z\in R(A)} (\mu_A(z) - 1) = \sum_{z\in R(A)} \mu_A(z) - \sum_{z\in R(A)} 1$$

$$= \deg P - \underbrace{(1+1+\cdots+1)}_{\text{Card}(R(A)) \text{ fois}} = \deg P - \text{Card}(R(A)) = \deg(A) - r(A).$$

Et de même pour B et C. Donc l'inégalité de la question précédente s'écrit encore

$$\boxed{\deg P \geqslant \deg(A) + \deg(B) + \deg(C) - (r(A) + r(B) + r(C)).}$$

6.f. On a donc $r(A) + r(B) + r(C) \geqslant \deg(A) + \deg(B) + \deg(C) - \deg(P)$.
En utilisant l'inégalité de la question 6.b.iii, $\deg P \leqslant \deg(B) + \deg(C) - 1$,

$$r(A) + r(B) + r(C) \geqslant \deg(A) + \deg(B) + \deg(C) - \deg(B) - \deg(C) + 1 \geqslant \deg(A) + 1.$$

De même, à l'aide de $\deg(P) \leqslant \deg(A) + \deg(C) - 1$, il vient

$$r(A) + r(B) + r(C) \geqslant \deg(B) + 1.$$

Détails
Être plus grand que deux nombres, c'est être plus grand que le plus grand des deux.

Donc déjà $r(A) + r(B) + r(C) \geqslant \max(\deg(A), \deg(B)) + 1$.
Nous pourrions tirer une inégalité analogue à celles de la question 6.b.iii pour faire apparaître $\deg(C)$.
Mais notons plutôt que comme $C = -A - B$, alors $\deg C \leqslant \max(\deg(A), \deg(B))$, et donc $\max(\deg(C), \deg(A), \deg(B)) \leqslant \max(\deg(A), \deg(B))$.
On en déduit que $\boxed{r(A) + r(B) + r(C) \geqslant 1 + \max(\deg(A), \deg(B), \deg(C)).}$

Partie III. Le théorème de Fermat pour les polynômes

7. Puisque $\alpha^n + \beta^n \neq 0$, il possède des racines $n^{\text{èmes}}$ qui sont nécessairement non nulles. Et donc il existe bien $\gamma \in \mathbf{C}^*$ tel que $\gamma^n = \alpha^n + \beta^n$.
Et alors $(\alpha D)^n + (\beta D)^n = (\alpha^n + \beta^n) D^n = \gamma^n D^n = (\gamma D)^n$.

Détails
U^n et U possèdent les mêmes racines.

8. Puisque U, V et W n'ont pas racines communes, il en est de même de U^n, V^n et W^n.
Supposons que U, V, W ne sont pas tous les trois constants. Par l'inégalité de Mason, on a alors

$$r(U^n) + r(V^n) + r(W^n) \geqslant 1 + \max\left(\deg(U^n), \deg(V^n), \deg(W^n)\right).$$

Mais U^n et U ont les mêmes racines, et donc $r(U^n) = r(U)$.
En revanche, $\deg(U^n) = n \deg(U)$, et donc

$$r(U) + r(V) + r(W) \geqslant 1 + n \max(\deg(U), \deg(V), \deg(W)).$$

Par ailleurs, $r(U) \leqslant \deg(U)$ et de même pour V et W.
Donc $\deg(U) + \deg(V) + \deg(W) \geqslant r(U) + r(V) + r(W) > 3 \max(\deg(U), \deg(V), \deg(W))$.
Mais puisque $\deg(U) \leqslant \max(\deg(U), \deg(V), \deg(W))$, $\deg(V) \leqslant \max(\deg(U), \deg(V), \deg(W))$ et $\deg(W) \leqslant \max(\deg(U), \deg(V), \deg(W))$, on a aussi

$$\deg(U) + \deg(V) + \deg(W) \leqslant 3 \max(\deg(U), \deg(V), \deg(W))$$

ce qui est absurde.
Donc $\boxed{U, V \text{ et } W \text{ sont constants.}}$

9. Soit ζ une racine $n^{\text{ème}}$ de -1. Alors

$$\widehat{U}^n + \widehat{V}^n - \widehat{W}^n = 0 \Leftrightarrow \widehat{U}^n + \widehat{V}^n + \left(\zeta \widehat{W}\right)^n = 0.$$

Puisque les racines du polynôme $\zeta \widehat{W}$ sont exactement celles de $\widehat{W}$, il n'y a donc pas de racine commune à $\widehat{U}, \widehat{V}, \zeta \widehat{W}$, et donc le résultat de la question précédente s'applique, de sorte que $\widehat{U}, \widehat{V}$ et $\zeta \widehat{W}$ sont constants. Et en particulier, $\widehat{W}$ est également constant.

10. Le sens réciproque a déjà été prouvé à la question 7.
Supposons donc que A, B, C soient tels que $A^n + B^n = C^n$.
S'ils sont tous les trois constants, il suffit de prendre $D = 1$, et α, β, γ des racines $n^{\text{èmes}}$ de A, B, C (qui rappelons-le, sont des constantes complexes).
Supposons à présent que A, B, C ne sont pas tous les trois constants.
Notons alors $D = \prod_{z \in R(A) \cap R(B) \cap R(C)} (X - z)^{\min(\mu_A(z), \mu_B(z), \mu_C(z))}$ (avec bien entendu la convention que $D = 1$ si $R(A) \cap R(B) \cap R(C) = \emptyset$).

Intuition
L'idée est que D sera ce qu'on appelle le PGCD de A, B et C : c'est un diviseur des trois, et il n'y a pas de diviseur de degré plus grand puisque dans $\mathbf{C}[X]$, nous savons caractériser la divisibilité à l'aide des racines.

Alors D est un diviseur de A, puisque toutes les racines de D (qui sont les racines communes à A, B et C) sont des racines de A, avec une multiplicité inférieure ou égale à celle en tant que racine de A. Et de même D divise à la fois B et C.
Il existe donc des polynômes $A_1, B_1, C_1 \in \mathbf{C}[X]$ tels que $A = DA_1, B = DB_1$ et $C = DC_1$.

Alors A_1, B_1, C_1 n'ont pas de racine en commun. En effet, si z était une telle racine, ce serait un élément de $R(A) \cap R(B) \cap R(C)$, pour lequel $\mu_A(z) = \mu_D(z) + \mu_{A_1}(z) > \mu_D(z)$ et de même $\mu_B(z) > \mu_D(z)$ et $\mu_C(z) > \mu_D(z)$.
Donc $\min(\mu_A(z), \mu_B(z), \mu_C(z)) > \mu_D(z)$, ce qui est absurde puisqu'on a défini D de sorte que $\mu_D(z) = \min(\mu_A(z), \mu_B(z), \mu_C(z))$.

On a alors

$$A^n + B^n = C^n \Leftrightarrow (DA_1)^n + (DB_1)^n = (DC_1)^n$$

et par intégrité de $\mathbf{C}[X]$, $A_1^n + B_1^n = C_1^n$.
Par la question précédente, A_1, B_1 et C_1 sont donc constants, et comme précédemment, il existe $(\alpha, \beta, \gamma) \in (\mathbf{C}^*)^3$ tels que $A_1 = \alpha$, $B_1 = \beta$, $C_1 = \gamma$ et $\alpha^n + \beta^n = \gamma^n$.
Et donc on a bien prouvé l'existence de $D \in \mathbf{C}[X] \setminus \{0\}$ et de $\alpha, \beta, \gamma \in \mathbf{C}^*$ tels que

$$\alpha^n + \beta^n = \gamma^n,\ A = \alpha D,\ B = \beta D,\ C = \gamma D.$$

11. On peut s'inspirer du cas des triplets pythagoriciens d'entiers : prenons $N = X$ et $M = 1$, et posons $U = 2NM = 2X, V = N^2 - M^2 = X^2 - 1$ et $W = N^2 + M^2 = X^2 + 1$.
On a alors $U^2 + V^2 = 4X^2 + (X^2 - 1)^2 = X^4 + 2X^2 + 1 = (X^2 + 1)^2 = W^2$.
Et il est clair que U, V et W n'ont pas de racines communes.

Commentaires *: il existe un analogue au théorème de* MASON *pour les entiers, c'est la* ***conjecture*** *abc, qui a été formulée dans les années* 80 *et n'est toujours pas prouvée à ce jour. Elle impliquerait alors le théorème de Fermat asymptotique, c'est-à-dire pour n suffisamment grand.*
Au début des années 2010*, un mathématicien japonais, Sinichi* MOCHIZUCKI *en a revendiqué une preuve, dans une série d'articles longs et difficiles (il y développe une théorie entièrement nouvelle). En* 2018*, Peter* SCHOLZE *(Médaille Fields) a trouvé une faille dans la preuve de* MOCHIZUKI*, ou du moins un point qui mérite d'être clarifié, et pense que la preuve est fausse, ce que* MOCHIZUKI *réfute. À l'heure actuelle, à l'exception de proches de* MOCHIZUKI*, la grande majorité de la communauté des mathématiciens compétents semble partager l'avis de* SCHOLZE*.*

PROBLÈME : 3-CYCLE IMPLIQUE CHAOS

1. C'est un grand classique : notons $I = [a, b]$, avec $a \leqslant b$.
Soit alors $g : x \mapsto f(x) - x$. Alors g est continue sur I, et vérifie $g(a) = f(a) - a \geqslant 0$ car $f(a) \in [a, b]$ et donc $f(a) \geqslant a$.
De même, $g(b) = f(b) - b \leqslant 0$ car $f(b) \leqslant b$.
Et donc par le théorème des valeurs intermédiaires[6], il existe $c \in [a, b]$ tel que $g(c) = 0$ soit encore $f(c) = c$. Donc $\boxed{f \text{ possède un point fixe.}}$

[6] Qui s'applique car g est continue et que $0 \in [g(b), g(a)]$.

2.a. Si K est un singleton $\{\alpha\}$, alors il existe $u \in I$ tel que $f(u) = \alpha$ et alors $f(\{u\}) = \{\alpha\} = K$.
Donc $\boxed{L = \{u\} \text{ convient.}}$

> **Rappel**
> Un singleton est un segment (dont les deux bornes sont égales).

2.b. Puisque K est inclus dans $f(J)$, $\alpha \in f(J)$ et $\beta \in f(J)$.
Donc α et β possèdent dans J des antécédents par f.

2.c. L'ensemble $E_\beta = \{t \in [a, b] \mid f(t) = \beta\}$ est une partie non vide de $\mathbf{R}$, puisqu'elle contient β, et est minorée par a.
Donc elle possède une borne inférieure v.
Cette borne inférieure v est nécessairement dans $[a, b]$ car par caractérisation séquentielle des bornes inférieures, il existe une suite (x_n) d'éléments de $E_\beta \subset [a, b]$ qui converge vers v. Et alors pour tout $n \in \mathbf{N}$, $a \leqslant x_n \leqslant b$, donc par passage à la limite $a \leqslant v \leqslant b$.
De plus, par caractérisation séquentielle de la continuité de f en v, $f(x_n) \underset{n\to+\infty}{\longrightarrow} f(v)$.
Mais pour tout $n \in \mathbf{N}$, $f(x_n) = \beta \underset{n\to+\infty}{\longrightarrow} \beta$, et donc par unicité de la limite, $f(v) = \beta$.

Ainsi, $v \in E_\beta$, et donc $\boxed{v \text{ est le plus petit élément de } E_\beta.}$

> **Rappel**
> La borne inférieure de A est le minimum de A si et seulement si elle est dans A.

2.d. De même, on prouve que $E_\alpha = \{t \in [a,v] \mid f(t) = \alpha\}$ est une partie non vide (elle contient a) et majorée (par v) de $\mathbf{R}$, donc elle possède une borne supérieure u.
Un raisonnement analogue à celui de la question précédente à base de caractérisations séquentielles prouve alors que $f(u) = \alpha$, de sorte que $u \in E_\alpha$, et donc u est le plus grand élément de E_α.

Nous allons prouver que $L = [u,v]$ convient.
Commençons par noter que $u < v$ puisque v est un majorant de E_α, et donc est supérieur ou égal au plus petit des majorants de E_α, qui est u. Donc $u \leqslant v$.
Et puisque u et v ont des images différentes par f, nécessairement ils sont distincts : $u < v$.

Nous savons, par le théorème des valeurs intermédiaires, que $f([u,v])$ est un intervalle[7] qui contient $f(u) = \alpha$ et $f(v) = \beta$.
Par définition d'un intervalle, il contient donc $[\alpha,\beta] = K$. Donc $K \subset f([u,v])$.
Supposons par l'absurde qu'il existe $t \in [u,v]$ tel que $f(t) \notin K$.
Par exemple supposons que $f(t) > \beta$ (le cas $f(t) < \alpha$ se traite de manière analogue).
Alors, on a $f(a) < \beta < f(t)$, donc par le théorème des valeurs intermédiaires, il existe $x \in]a,t[$ tel que $f(x) = \beta$.
Mais alors $x < v$ et $x \in E_\beta$, ce qui contredit le fait que $v = \min E_\beta$.
Donc f ne peut pas prendre sur $[u,v]$ de valeurs en dehors de K.
Et donc $f([u,v]) \subset K$, de sorte que par double inclusion, $f([u,v]) = K$, donc $L = [u,v]$ convient.

[7] Et même un segment si on utilise le théorème des bornes atteintes.

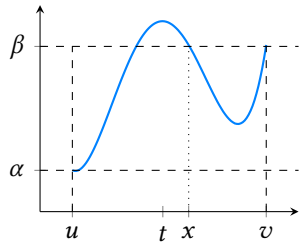


FIGURE 0.1– On prouve que le graphe de f sur $[u,v]$ ne peut pas sortir du carré en pointillés.

3. Notons $K = [a,b]$, avec $a \leqslant b$. Il s'agit de prouver que la fonction $g : x \mapsto f(x) - x$ s'annule sur K.
Elle est évidemment continue car f l'est.
Puisque $a \in K \subset f(K)$, il existe $u \in [a,b]$ tel que $f(u) = a$, et donc $g(u) = f(u) - u = a - u \leqslant 0$.
De même, $b \in f(K)$ et donc il existe $v \in [a,b]$ tel que $f(v) = b$, et alors $g(v) = f(v) - v = b - v \geqslant 0$.
Donc par le théorème des valeurs intermédiaires, il existe t compris entre u et v, et donc dans $K = [a,b]$ tel que $g(t) = 0 \Leftrightarrow f(t) = t$.
Donc $\boxed{f \text{ possède bien un point fixe dans } K.}$

4.a. Commençons par la fin : puisque $I_{n-1} \longrightarrow I_n$, $I_n \subset f(I_{n-1})$.
Par la question 2, il existe J_{n-1} segment inclus dans I_{n-1} tel que $f(J_{n-1}) = I_n$.
Mais alors $I_{n-2} \longrightarrow I_{n-1}$, ce qui signifie que $I_{n-1} \subset f(I_{n-2})$.
En particulier, puisque $J_{n-1} \subset I_{n-1}$, on a donc $J_{n-1} \subset f(I_{n-2})$.
Et donc par la question 2, il existe J_{n-2} segment inclus dans I_{n-2} tel que $f(J_{n-2}) = J_{n-1}$.
De proche en proche, on construit alors une suite de segments $J_0, J_1, \dots, J_{n-1}$ qui satisfont les conditions demandées.
Ils sont évidemment non vides puisque I_n est non vide, donc $J_{n-1} \neq \emptyset$, faute de quoi on aurait $f(\emptyset) \neq \emptyset$.
Et alors $J_{n-2} \neq \emptyset$ car $f(J_{n-2}) = J_{n-1} \neq \emptyset$, etc.

4.b. Si $x_0 \in I_0$, alors $f(x_0) \in f(J_0) = J_1$, $f^2(x_0) = f(f(x_0)) \in f(J_1) = J_2$, et de proche en proche, pour tout $k \in [\![0, n-1]\!]$, $f^k(x_0) \in J_k$.

5. Par la question précédente, il existe $J_0, J_1, \dots, J_{n-1}$ des segments non vides tels que $f(J_{n-1}) = I_0$ et $\forall k \in [\![1, n-1]\!]$, $J_k \subset I_k$ et $f(J_k) = J_{k+1}$.
En particulier, $f(J_0) = J_1$, $f^2(J_0) = f(J_1) = J_2$, etc, $f^n(J_0) = f(J_{n-1}) = I_0$.
Et en particulier, $J_0 \subset I_0 = f^n(J_0)$.
Donc par la question 3, la fonction f^n, qui est continue, possède un point fixe x dans J_0 (et donc dans I_0).
Il existe donc bien $x \in I_0$ tel que $f^n(x) = x$.
De plus, par la question 4.b, pour tout $k \in [\![0, n-1]\!]$, $f^k(x) \in J_k \subset I_k$.

6.a. Puisque x est 3-périodique, $f^3(x) = x$, et $f(x) \neq x$ et $f^2(x) \neq x$.
Notons qu'on a aussi $f^2(x) \neq f(x)$ faut de quoi on aurait, en appliquant de nouveau f, $f^3(x) = f^2(x)$.
Et donc $f^4(x) = f(f^3(x)) = x$, $f^5(x) = f^2(f^3(x)) = f^2(x)$, $f^6(x) = x$ etc.

► **Si** $x_0 = x$, alors $x_1 = f(x)$ et $x_2 = f^2(x)$, de sorte que x_0, x_1, x_2 sont deux à deux distincts.
De plus, $f(x_2) = f^3(x) = x = x_0$. Donc $f^3(x_1) = f^4(x_0) = f(x_0) = x_1$ et $f^3(x_2) = f^2(x_0) = x_2$, de sorte que x_0, x_1 et x_2 sont 3-périodiques.
► **Si** $x_0 = f(x)$. Alors $x_1 = f^2(x)$ et $x_2 = f(f^2(x)) = f^3(x) = x$.

Donc une fois encore x_0, x_1, x_2 sont distincts, et $f(x_2) = f(x) = x_0$.
On prouve sur le même principe que x_0, x_1 et x_2 sont 3-périodiques.
► **Si** $x_0 = f^2(x)$, alors $x_1 = f^3(x) = x$ et $x_2 = f(x)$ donc x_0, x_1, x_2, sont deux à deux distincts.
Et $f(x_2) = f^2(x) = x_0$.

6.b. Puisque $f(x_1) = x_2$ et $f(x_2) = x_0$, d'après le théorème des valeurs intermédiaires, qui s'applique car f est continue, $f(I_1)$ est un intervalle, contenant x_0 et x_2, et donc contenant $[x_0, x_2]$.
Et donc en particulier, $I_1 \subset f(I_1)$, de sorte qu'on a bien $I_1 \longrightarrow I_1$.
Par la question 3, ceci implique $\boxed{\text{l'existence d'un point fixe à } f.}$

Sur le même principe, on a $f(x_0) = x_1$ et $f(x_1) = x_2$, donc $f(I_0)$ est un intervalle contenant $[x_1, x_2] = I_1$. Donc $I_0 \longrightarrow I_1$.
Et on a déjà prouvé précédemment que $[x_0, x_2] \subset f(I_1)$, et donc en particulier, $I_0 \subset f(I_1)$, $I_1 \longrightarrow I_0$.
On a donc bien $I_0 \longrightarrow I_1 \longrightarrow I_0$.
Par la question 4, ceci implique l'existence de $x \in I_0$ tel que $f^2(x) = x$ et $f(x) \in I_1$.
Ne concluons pas trop vite que x est un point 2-périodique, il faut encore s'assurer qu'il ne s'agit pas d'un point fixe de f, c'est-à-dire que $f(x) \neq x$.
Si tel était le cas, on aurait $x \in I_0$ et $x = f(x) \in I_1$. Donc $x \in I_0 \cap I_1 = \{x_1\}$.
Or x_1 n'est pas un point fixe de f puisque $f(x_1) = x_2 > x_1$.
Donc $f(x) \neq x$ et ainsi $\boxed{x \text{ est bien un point 2-périodique de } f.}$

6.c. Comme indiqué, posons $J = -I$, qui est encore un segment et $g : x \mapsto -f(-x)$.
Alors pour tout $x \in J$, $-x \in I$, et donc $f(-x) \in I$, de sorte que $g(x) \in J$. Donc on a bien $g : J \to J$, qui est évidemment continue.
Par ailleurs, pour tout $x \in J$ et tout $k \in \mathbf{N}$, $g^2(x) = -f(-(-f(-x))) = -f^2(-x)$. Puis $g^3(x) = g(g^2(x)) = -f(f^2(-x)) = -f^3(-x)$, et une récurrence facile prouve que pour tout $k \in \mathbf{N}$, $g^k(x) = -f^k(-x)$.
En particulier, $g^k(x) = x \Leftrightarrow -f^k(-x) = x \Leftrightarrow -x = f^k(-x)$.
Et donc $x \in J$ est un point k-périodique de g si et seulement si $-x$ est un point k-périodique de f.
En particulier, $-x_0$ est un point 3-périodique de g.
De plus, $x_1 = f(x_0) \Leftrightarrow -x_1 = -f(x_0) = g(-x_0)$.
Et de même, $-x_2 = g(-x_1)$ et donc $-x_0 = g(-x_2)$.
Donc $-x_1$ est un point 3-périodique de g, et puisqu'on avait $x_0 < x_2 < x_1$, on a $-x_1 < -x_2 < -x_0$. Autrement dit, nous sommes ramenés au cas de la question 6.a : g possède un point fixe et un point 2-périodique.
Et alors f possède également un point fixe[8] et un point 2-périodique.

[8] Qui est l'opposé du point fixe de g que nous venons d'obtenir.

7. Traitons de nouveau le cas où $x_1 < x_2$, le même raisonnement qu'en 6.b s'appliquant de nouveau.
Nous avons déjà prouvé que $I_0 \longrightarrow I_1$, $I_1 \longrightarrow I_1$ et que $I_1 \longrightarrow I_0$, donc évidemment, pour $n \in \mathbf{N}^*$, $I_0 \longrightarrow I_1 \longrightarrow I_1 \longrightarrow \ldots \longrightarrow I_1 \longrightarrow I_0$, où la suite comporte n flèches $\longrightarrow$.
On peut de nouveau appliquer la question 5 : il existe $x \in I_0$ tel que $f^n(x) = x$ et $\forall k \in [\![1, n-1]\!]$, $f^k(x) \in I_1$.
Donc x est de nouveau un bon candidat pour être un point n-périodique, il ne reste qu'à vérifier qu'on n'a pas $f^k(x) = x$ pour $k \in [\![1, n-1]\!]$.
Mais de nouveau, si tel était le cas, on aurait $x \in I_0$ et $x = f^k(x) \in I_1$, donc $x \in I_0 \cap I_1 = \{x_1\}$.
Or x_1 est 3-périodique, et ne peut donc être n-périodique si $n \neq 3$ (et si $n = 3$, la question n'a que peu d'intérêt).

Période
Notons que la période d'un point périodique x est unique, et peut s'écrire comme
$\min\{k \in \mathbf{N}^* \mid f^k(x) = x\}$.

8.a. Commençons par noter que la fonction f est bien continue sur $[0, 1]$. En effet, elle l'est sur $[0, \frac{1}{2}[$ car affine, et sur $]\frac{1}{2}, 1]$ pour les mêmes raisons.
De plus, $\lim\limits_{x \to \frac{1}{2}^-} f(x) = \lim\limits_{x \to \frac{1}{2}^-} 2x = 1$ et $\lim\limits_{x \to \frac{1}{2}^+} f(x) = \lim\limits_{x \to \frac{1}{2}^+} 2(1-x) = 1$. Puisque de plus $f\left(\frac{1}{2}\right) = 1$, f est bien continue en $\frac{1}{2}$.
Enfin, il est clair que f est à valeurs dans $[0, 1]$.
Donc f est bien une fonction continue de $[0, 1]$ dans lui-même.
Nous allons donc essayer de lui appliquer le théorème de Sarkovskii et de prouver l'existence d'un point 3-périodique afin de garantir l'existence d'un point n-périodique pour tout $n \in \mathbf{N}^*$.

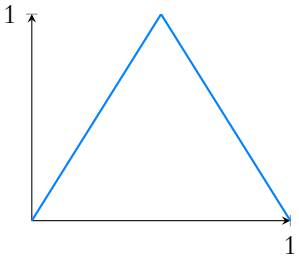
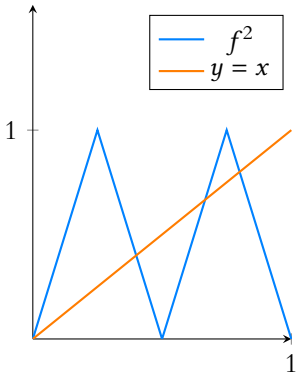


FIGURE 0.2– La fonction f.

On a $f^3(0) = 0$, mais puisque 0 est un point fixe de f, il ne s'agit pas d'un point 3-périodique.
On a $f\left(\frac{2}{3}\right) = \frac{2}{3}$, donc il s'agit d'un point fixe de f. Il vérifie bien $f^3(x) = x$, mais n'est pas 3-périodique, mais 1-périodique.
On a $f\left(\frac{2}{5}\right) = \frac{4}{5}$ et $f^2\left(\frac{2}{5}\right) = f\left(\frac{4}{5}\right) = \frac{2}{5}$. Donc $\frac{2}{5}$ est 2-périodique, et donc pas 3-périodique (de toutes façons, $f^3\left(\frac{2}{5}\right) \neq \frac{2}{5}$).
Enfin, $f\left(\frac{2}{7}\right) = \frac{4}{7}$, $f^2\left(\frac{2}{7}\right) = \frac{6}{7}$ et $f^3\left(\frac{2}{7}\right) = \frac{2}{7}$, donc nous avons là un point 3-périodique.
Et donc par le théorème de Sarkovskii, f possède des points n-périodiques pour tout $n \in \mathbf{N}^*$.

8.b. Essayons de nous représenter f^2 : soit $x \in [0,1]$.

- ▶si $x \in \left[0, \frac{1}{4}\right]$, alors $f(x) = 2x \in \left[0, \frac{1}{2}\right]$ et donc $f^2(x) = 4x$.
- ▶si $x \in \left[\frac{1}{4}, \frac{1}{2}\right]$, alors $f(x) = 2x \geqslant \frac{1}{2}$, et donc $f^2(x) = 2(1-2x) = 2-4x$.
- ▶si $x \in \left[\frac{1}{2}, \frac{3}{4}\right]$, alors $f(x) = 2-2x \in \left[\frac{1}{2}, 1\right]$ et donc $f^2(x) = 2(1-f(x)) = 4x-1$.
- ▶si $x \in \left[\frac{3}{4}, 1\right]$, $f(x) = 2-2x \in \left[0, \frac{1}{2}\right]$ et donc $f^2(x) = 4-4x$.



Il est alors facile de constater que l'équation $f^2(x) = x$ possède un unique solution dans $\left[0, \frac{1}{4}\right]$, qui est $x = 0$ (point fixe de f), une unique dans $\left[\frac{1}{4}, \frac{1}{2}\right]$, qui est $\frac{2}{5}$ (un point 2-périodique), une dans $\left[\frac{1}{2}, \frac{3}{4}\right]$ qui est $\frac{2}{3}$ (point fixe de f) et une dans $\left[\frac{3}{4}, 1\right]$, qui est $\frac{4}{5}$ (point 3-périodique).

Sur le même principe, on prouve que pour $n \in \mathbf{N}^*$, pour tout $x \in \left[0, \frac{1}{2^n}\right]$, $f(x) = 2x \in \left[0, \frac{1}{2}\right]$, donc $f^2(x) = 2^2x \in \left[0, \frac{1}{2}\right]$, etc, $f^n(x) = 2^nx$.
Donc sur $\left[0, \frac{1}{2^n}\right]$, $f^n(x) = x$ ne possède qu'une solution qui est 0, qui n'est pas n-périodique[9].
Sur $\left[\frac{1}{2^n}, \frac{1}{2^{n-1}}\right]$, on a $f(x) = 2x \in \left[\frac{1}{2^{n-1}}, \frac{1}{2^{n-2}}\right]$, $f^2(x) = 4x \in \left[\frac{1}{2^{n-2}}, \frac{1}{2^{n-3}}\right]$, etc $f^{n-1}(x) = 2^{n-1}x \in \left[\frac{1}{2}, 1\right]$.
Et donc $f^n(x) = 2-2^nx$.
Et alors l'équation $f^n(x) = x$ possède une unique solution dans $\left[\frac{1}{2^n}, \frac{1}{2^{n-1}}\right]$, qui est $\frac{2}{2^n+1}$.
C'est donc nécessairement la plus petite solution à $f^n(x) = x$.
Ça ne peut pas être un point k-périodique pour $k < n$, puisque la plus petite solution à $f^k(x) = x$ est $\frac{2}{2^k+1} > \frac{2}{2^n+1}$.
On en déduit que le plus petit point n-périodique de f est $x_n = \frac{2}{2^n+1}$.
Et donc $x_n \underset{n\to+\infty}{\sim} \frac{1}{2^{n-1}}$.

[9] Sauf si $n = 1$.

Il faut travailler un peu plus pour majorer le nombre de points n-périodiques de f, mais on montrerait comme on l'a fait pour $n = 2$ que f^n est affine sur chaque intervalle de la forme $\left[\frac{k}{2^n}, \frac{k+1}{2^n}\right]$, et que $f^n(x) = x$ possède une unique solution dans chacun de ces intervalles. Ce qui donne 2^n solutions à $f^n(x) = x$.
Par contre ces solutions ne sont pas toutes des points n-périodiques, puisque parmi elles se trouvent les deux points fixes de f (qui sont 0 et $\frac{2}{3}$), et éventuellement des points périodiques de plus petite période.
Donc une majoration du nombre de points périodiques est $2^n - 2$ (au moins pour $n > 2$), on peut sûrement faire mieux dans certains cas.

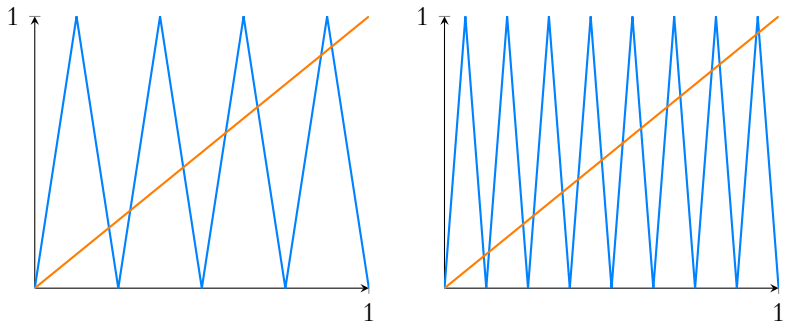


FIGURE 0.3 – Les graphes de f^3 et f^4. Les points n-périodiques sont parmi les points d'intersection du graphe de f^n et de la première bissectrice d'équation $y = x$.