DM6

Correction du devoir maison

Exercice 1

1. (a) Par hypothèse, y est deux fois dérivable sur $I =]-1,1[$. De plus, les fonctions cosinus et sinus sont deux fois dérivables sur $J =]0,\pi[$, et la fonction cosinus restreinte à $]0,\pi[$ est à valeurs dans $]-1,1[$. Par composition et produit, z est deux fois dérivable sur J. Et pour tout $t \in J$:

$$\begin{aligned} z'(t) &= \cos(t)\cdot y(\cos(t)) + \sin(t)(-\sin(t))y'(\cos(t)) \\ &\boxed{= \cos(t)\cdot y(\cos(t)) + (\cos^2(t)-1)y'(\cos(t))} \\ z''(t) &= -\sin(t)\cdot y(\cos(t)) - \cos(t)\sin(t)y'(\cos(t)) - 2\sin(t)\cos(t)y'(\cos(t)) \\ &\quad - (\cos^2(t)-1)\sin(t)y''(\cos(t)) \\ &\boxed{= -\sin(t)\cdot\Big(y(\cos(t)) + 3\cos(t)y'(\cos(t)) + (\cos^2(t)-1)y''(\cos(t))\Big)} \end{aligned}$$

   (b) y est solution de (E) sur I si y est deux fois dérivable sur I et

$$\forall x \in I, \quad (x^2-1)y''(x) + 3xy'(x) - 8y(x) = 2x.$$

Pour tout $x \in]-1,1[$, il existe un unique $t \in]0,\pi[$ tel que $x = \cos(t)$. En remplaçant dans (E), on obtient :

$$(\cos^2(t)-1)y''(\cos(t)) + 3\cos(t)y'(\cos(t)) - 8y(\cos(t)) = 2\cos(t).$$

Puisque $\sin(t) \neq 0$ pour $t \in]0,\pi[$, cette équation est équivalente à :

$$-\sin(t)(\cos^2(t)-1)y''(\cos(t)) - 3\sin(t)\cos(t)y'(\cos(t)) + 8\sin(t)y(\cos(t)) = -2\sin(t)\cos(t).$$

En posant $z : t \in J \mapsto \sin(t)\cdot y(\cos(t))$, on en déduit par la question précédente que z est deux fois dérivable sur J. L'égalité précédente est alors équivalente à :

$$z''(t) + 9\sin(t)y(\cos(t)) = z''(t) + 9z(t) = -2\sin(t)\cos(t) \qquad (E')$$

Ainsi :

$$\boxed{y \text{ solution de } (E) \text{ sur } I \quad \Leftrightarrow \quad z \text{ solution de } (E') \text{ sur } J.}$$

2. L'équation (E') est une équation différentielle linéaire du second ordre à coefficients constants. L'équation homogène associée est

$$z'' + 9z = 0. \qquad (E'_0)$$

L'équation caractéristique associée est $r^2 + 9 = 0$. Ces deux racines sont $r = 3i$ et $r' = -3i$. L'ensemble des solutions de (E'_0) est :

$$\{t \in J \mapsto A\cos(3t) + B\sin(3t),\ A, B \in \mathbb{R}\}.$$

On cherche une solution particulière de (E'). Pour tout $t \in J$:

$$z''(t) + 9z(t) = -2\sin(t)\cos(t) = -\sin(2t) = \frac{e^{-2it} - e^{2it}}{2i}$$

En utilisant le principe de superposition, on se ramène à déterminer des solutions particulières des deux équations suivantes :

$$z'' + 9z = \frac{e^{-2it}}{2i} \qquad (E'_1)$$

et

$$z'' + 9z = -\frac{e^{2it}}{2i} \qquad (E_2')$$

Pour (E_1'), $-2i$ n'est pas solution de l'équation caractéristique. On cherche donc une solution de (E_1') sous la forme $z : t \mapsto Ce^{-2it}$ avec $C \in \mathbb{C}$. En remplaçant dans (E_1'), on obtient :

$$-4Ce^{-2it} + 9Ce^{-2it} = \frac{e^{-2it}}{2i},$$

d'où $5C = \frac{1}{2i}$, et $C = -\dfrac{i}{10}$. Ainsi $z : t \mapsto -\dfrac{i}{10}e^{-2it}$ est solution de (E_1') sur J.

Une solution particulière de (E_2') se déduit alors de la solution précédente en considérant $t \mapsto \overline{-\dfrac{i}{10}e^{-2it}} = \dfrac{i}{10}e^{2it}$.

Finalement, une solution particulière de (E') sur J est donnée par :

$$t \mapsto -\frac{i}{10}e^{-2it} + \frac{i}{10}e^{2it} = \frac{i}{10}(e^{2it} - e^{-2it}) = -\frac{1}{5}\sin(2t).$$

L'ensemble des solutions de (E') sur J est donc

$$\boxed{\left\{t \mapsto A\cos(3t) + B\sin(3t) - \frac{1}{5}\sin(2t),\ A, B \in \mathbb{R}\right\}.}$$

3. On obtient donc par ce qui précède que y est solution de (E) sur I si, et seulement si, il existe $A, B \in \mathbb{R}$ tel que pour tout $t \in J$,

$$\sin(t)y(\cos(t)) = A\cos(3t) + B\sin(3t) - \frac{1}{5}\sin(2t) \qquad (*)$$

Calculons :

$$\begin{aligned}
\cos(3t) &= \cos(2t)\cos(t) - \sin(2t)\sin(t) = \cos^3(t) - \sin^2(t)\cos(t) - 2\sin^2(t)\cos(t) \\
&= \cos(t)(\cos^2(t) - 3\sin^2(t)) = \cos(t)(4\cos^2(t) - 3) \\
\sin(3t) &= \sin(2t)\cos(t) + \cos(2t)\sin(t) = 2\sin(t)\cos^2(t) + \cos^2(t)\sin(t) - \sin^3(t) \\
&= \sin(t)(3\cos^2(t) - \sin^2(t)) = \sin(t)(4\cos^2(t) - 1) \\
\frac{1}{5}\sin(2t) &= \frac{2}{5}\cos(t)\sin(t)
\end{aligned}$$

D'où en remplaçant dans $(*)$, on obtient :

$$\sin(t)y(\cos(t)) = A\cos(t)(4\cos^2(t) - 3) + B\sin(t)(4\cos^2(t) - 1) - \frac{2}{5}\cos(t)\sin(t).$$

Puisque $\sin(t) \neq 0$ pour $t \in J$, on obtient :

$$\begin{aligned}
y(\cos(t)) &= A\frac{\cos(t)}{\sin(t)}(4\cos^2(t) - 3) + B(4\cos^2(t) - 1) - \frac{2}{5}\cos(t) \\
&= A\frac{\cos(t)}{\sqrt{1 - \cos^2(t)}}(4\cos^2(t) - 3) + B(4\cos^2(t) - 1) - \frac{2}{5}\cos(t)
\end{aligned}$$

car $\sin(t) > 0$ sur J. Alors en prenant $x = \cos(t)$, on obtient finalement :

$$y(x) = A\frac{x}{\sqrt{1 - x^2}}(4x^2 - 3) + B(4x^2 - 1) - \frac{2}{5}x.$$

Les solutions de l'équation (E) sont donc les fonctions de la forme :

$$\boxed{x \in I \mapsto A\frac{x}{\sqrt{1 - x^2}}(4x^2 - 3) + B(4x^2 - 1) - \frac{2}{5}x}$$

avec $A, B \in \mathbb{R}$.

Exercice 2 (Théorème des deux carrés)

1. (a) Soient $m, n \in \mathscr{E}$. Il existe $(a,b),(c,d) \in \mathbb{N}^2$ tels que $m = a^2+b^2$ et $n = c^2+d^2$. Posons $u = a+ib$ et $v = c+id$. Alors :

$$m \times n = |u|^2 \times |v|^2 = |u \times v|^2 = (ac-bd)^2 + (ad+cb)^2.$$

Donc $m \times n$ appartient à $\mathscr{E}$, et $\boxed{\mathscr{E} \text{ est stable par produit.}}$

(b) Soit $p \in \mathscr{E}$ impair. Par définition, il existe $(a,b) \in \mathbb{N}^2$ tel que $p = a^2+b^2$. Faisons une disjonction de cas selon la parité de a et b.

- Si a et b sont pairs, a^2+b^2 est pair, ce qui est impossible si p est impair.
- Si a et b sont impairs, a^2 et b^2 est impair, et a^2+b^2 est pair, ce qui est encore impossible si p est impair.
- S'il existe $k, \ell \in \mathbb{N}$ tel que $a = 2k$ et $b = 2\ell+1$, alors :

$$p = a^2+b^2 = 4k^2+4\ell^2+4\ell+1 \equiv 1\,[4].$$

Ainsi, $\boxed{\text{si } p \in \mathscr{E} \text{ est impair, alors } p \equiv 1\,[4].}$

2. (a) Le cardinal de $[\![0, \sqrt{n}]\!]^2$ est $(\lfloor\sqrt{n}\rfloor+1)^2$, et celui de $[\![0, n-1]\!]$ est n. Mais par définition de la partie entière d'un réel, $\sqrt{n} < \lfloor\sqrt{n}\rfloor+1$, et par stricte croissance de la fonction carrée sur $\mathbb{R}_+$, $n < (\lfloor\sqrt{n}\rfloor+1)^2$. Ainsi, le cardinal $[\![0, \sqrt{n}]\!]^2$ est strictement plus grand que celui de $[\![0, n-1]\!]$.

Considérons l'application $f : [\![0, \sqrt{n}]\!]^2 \to [\![0, n-1]\!]$ qui à tout couple $(x,y) \in [\![0, \sqrt{n}]\!]^2$ associe le reste de la division euclidienne de $ax+by$ par n. Si cette application était injective, $\mathrm{Im}(f)$ serait en bijection avec $[\![0, \sqrt{n}]\!]^2$, et $[\![0, n-1]\!]$ contiendrait un sous-ensemble de cardinal $(\lfloor\sqrt{n}\rfloor+1)^2$ qui est strictement plus grand que n, ce qui est impossible.

Ainsi, $\boxed{f \text{ n'est pas une application injective.}}$

(b) Puisque f n'est pas injective, il existe $(x_1,y_1),(x_2,y_2) \in [\![0, \sqrt{n}]\!]^2$ distincts tels que $f(x_1,y_1) = f(x_2,y_2)$, c'est-à-dire tels que ax_1+by_1 et ax_2+by_2 ont même reste dans la division euclidienne par n. Or, c'est le cas si et seulement si ils sont congrus modulo n, ce qui se récrit :

$$a(x_1-x_2)+b(y_1-y_2) \equiv 0\,[n].$$

Posons alors $u = x_1-x_2$ et $v = y_1-y_2$. Le couple (u,v) est non nul car (x_1,y_1) est distinct de (x_2,y_2), et tel que n divise $au+bv$. De plus, puisque $x_1, x_2 \in [\![0, \sqrt{n}]\!]$, $|u| = |x_1-x_2| \leq \sqrt{n}$. Mais comme u est un entier et pas $\sqrt{n}$ (car n n'est pas un carré parfait), il suit que $|u| < \sqrt{n}$. De même, $|v| < \sqrt{n}$.

D'où $\boxed{\text{l'existence de } (u,v) \in \mathbb{Z}^2 \text{ tel que } (u,v) \neq (0,0),\ |u| < \sqrt{n},\ |v| < \sqrt{n} \text{ et } n \text{ divise } au+bv.}$

(c) On a obtenu que n divise $au+bv$. Il divise donc également $(au+bv)(au-bv) = a^2u^2-b^2v^2$.

Puisque $a^2u^2-b^2v^2 = a^2(u^2+v^2)-(a^2+b^2)v^2$ et que n divise a^2+b^2, il suit que n divise $a^2(u^2+v^2)$. De même, on montre que n divise $b^2(u^2+v^2)$.

D'autre part, puisque a et b sont premiers entre eux, il en est de même de a^2 et b^2, d'où l'existence de $\alpha, \beta \in \mathbb{Z}$ tels que $\alpha a^2+\beta b^2 = 1$.

Finalement, n divise $\alpha a^2(u^2+v^2)+\beta b^2(u^2+v^2) = u^2+v^2$.

(d) D'après la question précédente, u^2+v^2 est un multiple de n, non nul car $(u,v) \neq (0,0)$, et strictement plus petit que $2n$ puisque $|u|, |v| < \sqrt{n}$. Or il n'y a qu'un seul multiple de n strictement compris entre 0 et $2n$: c'est n lui-même.

Par conséquent, $n = u^2+v^2$, et $\boxed{n \text{ appartient à } \mathscr{E}.}$

3. (a) Soit $x \in [\![1, p-1]\!]$.

Commençons par l'existence d'un tel entier y. Puisque $x \in [\![1, p-1]\!]$, x est premier avec p. Il existe donc $(u, v) \in \mathbb{Z}^2$ tel que $xu + pv = 1$, ce qui donne en passant aux congruences $xu \equiv 1\,[p]$. Mais rien ne dit que $u \in [\![1, p-1]\!]$. Effectuons pour cela la division euclidienne de u par p : il existe q, y des entiers tels que $u = qp + y$ avec $y \in [\![0, p-1]\!]$. D'où :

$$xy = xu + xqp \equiv xu \equiv 1\,[p].$$

Et $y \neq 0$ car $xy \not\equiv 0\,[p]$.

Vérifions maintenant qu'un tel entier est unique. Soient pour cela $y_1, y_2 \in [\![1, p-1]\!]$ tels que $xy_1 \equiv 1\,[p]$ et $xy_2 \equiv 1\,[p]$. Alors :

$$y_1 \equiv y_1(xy_2) \equiv (y_1x)y_2 \equiv y_2[p]$$

et donc p divise $y_1 - y_2$. Or $y_1 - y_2$ est un entier compris entre $-p+1$ et $p-1$. Le seul multiple de p dans cet intervalle d'entiers étant 0, il suit que $y_1 = y_2$.

Ainsi, $\boxed{\text{pour tout } x \in [\![1, p-1]\!], \text{ il existe un unique } y \in [\![1, p-1]\!] \text{ tel que } xy \equiv 1[p].}$

✎ **Notation.**

> Pour tout $x \in [\![1, p-1]\!]$, on notera dans la suite $\text{inv}(x)$ l'unique élément $y \in [\![1, p-1]\!]$ tel que $xy \equiv 1[p]$.

(b) La réflexivité et la symétrie de $\sim$ sont immédiates. Soient à présent $x, y, z \in [\![1, p-1]\!]$ tels que $x \sim y$ et $y \sim z$. Si $x = y$ ou $y = z$, alors $x \sim z$ immédiatement. Sinon, on a $xy \equiv 1\,[p]$ et $yz \equiv 1[p]$. Mais par l'unicité établie à la question précédente, $x = \text{inv}(y) = z$, et donc $x \sim z$.

Ainsi, $\boxed{\sim \text{ est une relation d'équivalence sur } [\![1, p-1]\!].}$

(c) Soit $x \in [\![1, p-1]\!]$, et soit $z \in [\![1, p-1]\!]$. Alors $z \sim x$ si, et seulement si, $z = x$ ou $xz \equiv 1\,[p]$, soit encore $z = x$ ou $z = \text{inv}(x)$. Ainsi, $\text{cl}(x) = \{x, \text{inv}(x)\}$.

La classe de x est un singleton si, et seulement si, $x = \text{inv}(x)$. Or si $x = \text{inv}(x)$, alors :

$$x \times x \equiv x \times \text{inv}(x) \equiv 1\,[p]$$

de sorte que $p \mid x^2 - 1 = (x-1)(x+1)$. Puisque p est premier, on obtient $p \mid x-1$ ou $p \mid x+1$, et donc $x - 1 = 0$ ou $x + 1 = p$ puisque $1 \leq x \leq p-1$.

Réciproquement, si $x = 1$, on a bien $1 \times 1 \equiv 1\,[p]$, et donc $1 = \text{inv}(1)$, de sorte que $\text{cl}(1) = \{1\}$. Et si $x = p-1$, $x \times x \equiv (-1) \times (-1) \equiv 1\,[p]$.

Finalement, $\boxed{\text{cl}(x) \text{ est un singleton si, et seulement si, } x = 1 \text{ ou } x = p-1.}$

Dans le cas contraire, $\boxed{\text{cl}(x) = \{x, \text{inv}(x)\} \text{ est de cardinal 2.}}$

(d) Rappelons que :

- les classes d'équivalences forment une partition de $[\![1, p-1]\!]$;
- deux classes d'équivalence sont des singletons, la classe de 1 et la classe de $p-1$;
- toutes les autres classes d'équivalences sont de cardinal 2, de la forme $\text{cl}(x) = \{x, \text{inv}(x)\}$. Dans ce cas, le produit de ses éléments satisfait $x \times \text{inv}(x) \equiv 1\,[p]$.

Notons R un système de représentants de ces classes d'équivalence, qui contient donc 1 et $p-1$. Alors :

$$(p-1)! = 1 \times (p-1) \times \left(\prod_{x \in R \setminus \{1, p-1\}} x \times \text{inv}(x) \right) \equiv 1 \times (-1) \times \left(\prod_{x \in R \setminus \{1, p-1\}} 1 \right) \equiv -1\,[p].$$

D'où $\boxed{\text{le théorème de Wilson : } \quad (p-1)! \equiv -1\,[p].}$

Remarque. Le théorème de Wilson est encore valable lorsque $p = 2$, puisqu'alors $(p-1)! = 1$ et $-1 \equiv 1\,[2]$. De plus, la réciproque est vraie : si $p \geq 2$ satisfait $(p-1)! \equiv -1\,[p]$, alors il existe $k \in \mathbb{Z}$ tel que $kp - (p-1)! = 1$, et donc p est premier avec tous les entiers compris entre 2 et $p-1$. Il n'admet donc aucun diviseurs positifs autres que 1 et lui-même. Donc p est premier.

(e) Remarquons tout d'abord que :

$$\begin{aligned}\prod_{k=1}^{m} k(p-k) &= \left(\prod_{k=1}^{m} k\right) \times \left(\prod_{k=1}^{m} (p-k)\right) \\ &= 1 \times \cdots \times \left(\frac{p-1}{2}\right) \times \left(\frac{p+1}{2}\right) \times \cdots \times (p-1) \\ &= (p-1)! \equiv -1\,[p].\end{aligned}$$

D'autre part :

$$\begin{aligned}\prod_{k=1}^{m} k(p-k) &= \left(\prod_{k=1}^{m} k\right) \times \left(\prod_{k=1}^{m} (p-k)\right) \\ &\equiv m! \times \left(\prod_{k=1}^{m} (-k)\right)\,[p] \\ &\equiv (-1)^m m! \times \left(\prod_{k=1}^{m} k\right)\,[p] \\ &\equiv (-1)^m (m!)^2\,[p]\end{aligned}$$

Et donc :

$$\boxed{(m!)^2 \equiv (-1)^{m+1}\,[p].}$$

(f) Si $p \equiv 1\,[4]$, alors $m = \frac{p-1}{2}$ est un entier pair, et donc $(m!)^2 \equiv (-1)^{m+1} \equiv -1\,[p]$. Par conséquent, p divise $(m!)^2 + 1$.

On se retrouve alors dans la situation de la question 2 : $m!$ et 1 sont premiers entre eux, et p n'est pas un carré parfait puisque p est premier. Par la question 2.(d), $\boxed{p \text{ appartient à } \mathscr{E}.}$

4. Soit $n \in \mathbb{N}^*$. Procédons par double implication.

⇐ Supposons que $v_p(n)$ est pair pour tout $p \in \mathbb{P}$ congru à 3 modulo 4. Pour tout $p \in \mathbb{P}$:

- si $p \equiv 3\,[4]$, $p^{v_p(n)}$ est un carré puisque $v_p(n)$ est pair, et donc appartient à $\mathscr{E}$ (prendre $a = p^{v_p(n)/2}$ et $b = 0$ par exemple) ;
- si $p \equiv 1\,[4]$, alors $p \in \mathscr{E}$ par la question 3.(f), et donc $p^{v_p(n)}$ aussi car $\mathscr{E}$ est stable par produit ;
- si $p = 2$, alors $p = 1^2 + 1^2 \in \mathscr{E}$, et donc $2^{v_2(n)} \in \mathscr{E}$ toujours parce que $\mathscr{E}$ est stable par produit.

Par stabilité de $\mathscr{E}$ par produit, $n = \prod_{p \in \mathbb{P}} p^{v_p(n)}$ appartient à $\mathscr{E}$.

⇒ Supposons que $n \in \mathbb{N}^*$ appartient à $\mathscr{E}$.

Si n est un carré parfait, ses valuations p-adiques sont paires pour tout $p \in \mathbb{P}$, donc en particulier pour tout $p \in \mathbb{P}$ congru à 3 modulo 4.

Supposons à présent que n ne soit pas un carré parfait. Il existe $a, b \in \mathbb{N}^*$ tels que $n = a^2 + b^2$. Notons alors $d = a \wedge b$ et $a', b' \in \mathbb{N}$ premiers entre eux tels que $a = da'$ et $b = db'$. Alors :

$$n = a^2 + b^2 = d^2(a'^2 + b'^2).$$

Puisque d^2 est un carré parfait, ses valuations p-adiques sont toutes paires. On est donc ramené à étudier les valuations p-adiques de $a'^2 + b'^2$.

Soit $p \in \mathbb{P}$ un diviseur de $a'^2 + b'^2$. On est dans le cadre d'application de la question 2 : a' et b' sont premiers entre eux, et p n'est pas un carré parfait car p est premier. Par conséquent, p appartient à $\mathscr{E}$ par la question 2.(d), et $p \equiv 1\,[4]$ par la question 1.(b).

On peut à présent conclure : si p est un nombre premier congru à 3 modulo 4, alors $p \nmid (a'^2 + b'^2)$ (puisque $p \not\equiv 1\,[4]$), et donc $v_p(a'^2 + b'^2) = 0$. Ainsi :

$$v_p(n) = v_p(d^2) + v_p(a'^2 + b'^2) = 2v_p(d) \in 2\mathbb{N}.$$

On en déduit le *théorème des deux carrés* :

Un entier $n \in \mathbb{N}^*$ est la somme de deux carrés parfaits si, et seulement si, $v_p(n)$ est pair pour tout $p \in \mathbb{P}$ congru à 3 modulo 4.
