Corrigé du DS de Mathématiques n°9 — 18 mars 2023

Exercice 1 — (Matrices définies par blocs)

Partie A - Matrices de rotation

Pour tout réel θ, on définit la matrice $R(\theta) \in \mathrm{M}_2(\mathbb{R})$ en posant : $\quad R(\theta) = \begin{pmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{pmatrix}$

On a déjà établi en TD cette année que : $\quad \forall\, (\theta, \varphi) \in \mathbb{R}^2, \quad R(\theta)\, R(\varphi) = R(\theta + \varphi)$

1/ Etablir que : $\forall \theta \in \mathbb{R},\ R(\theta) \in \mathrm{GL}_2(\mathbb{R}) \quad$ et $\quad (R(\theta))^{-1} = R(-\theta)$

Soit θ un réel. D'après l'indication de l'énoncé : $R(\theta)\, R(-\theta) = R(0) = \mathrm{I}_2$, d'où la conclusion.

2/ Etablir que : $\forall \theta \in \mathbb{R},\ \forall n \in \mathbb{Z},\ (R(\theta))^n = R(n\theta)$

Soit $\theta \in \mathbb{R}$. Par une récurrence aisée sur n on établit que :

$$\forall n \in \mathbb{N},\ (R(\theta))^n = R(n\theta)$$

Soit à présent n entier négatif. Puisque la matrice $R(\theta)$ est inversible d'après la question 1, on écrit judicieusement :

$$(R(\theta))^n = \left((R(\theta))^{-1}\right)^{-n} = (R(-\theta))^{-n}$$

Comme $(-n) \in \mathbb{N}$, on en déduit que :

$$(R(\theta))^n = (R((-n) \times (-\theta))) = R(n\theta)$$

Conclusion. $\forall \theta \in \mathbb{R},\ \forall n \in \mathbb{Z},\ (R(\theta))^n = R(n\theta)$

3/ Soit m un entier naturel supérieur ou égal à 2, et soit N un entier naturel. Montrer que :

$$\left[\left(R\left(\frac{\pi}{m}\right)\right)^N = \mathrm{I}_2\right] \iff [N \equiv 0\,[2m]]$$

Soit m un entier naturel supérieur ou égal à 2, et soit N un entier naturel. On a, d'après la question précédente :

$$\left(R\left(\frac{\pi}{m}\right)\right)^N = R\left(\frac{N\pi}{m}\right)$$

Par suite :

$$\left[\left(R\left(\frac{\pi}{m}\right)\right)^N = \mathrm{I}_2\right] \iff \left[R\left(\frac{N\pi}{m}\right)\right] \iff \left[\cos\left(\frac{N\pi}{m}\right) = 1 \wedge \sin\left(\frac{N\pi}{m}\right) = 0\right]$$

$$\iff \left[\frac{N\pi}{m} \equiv 0\ [2\pi]\right] \iff \left[\frac{N}{m} \equiv 0\ [2]\right] \iff [N \equiv 0\ [2m]]$$

Conclusion. $\left[\left(R\left(\frac{\pi}{m}\right)\right)^N = \mathrm{I}_2\right] \iff [N \equiv 0\,[2m]]$

Partie B - Matrices par blocs

Dans cette partie, n désigne un entier supérieur ou égal à 2. Dans $\mathrm{M}_{2n}(\mathbb{R})$, on considère l'ensemble **E** des matrices s'écrivant :

$$\left(\begin{array}{c|c} A & 0_{\mathrm{M}_n(\mathbb{R})} \\ \hline 0_{\mathrm{M}_n(\mathbb{R})} & B \end{array}\right) \qquad \text{avec } A \text{ et } B \text{ dans } \mathrm{M}_n(\mathbb{R})$$

Formellement, une matrice $M = (m_{ij})$ de **E** est une matrice dans $\mathrm{M}_{2n}(\mathbb{R})$ dont les coefficients sont tels que :

$$\forall\ (i,j) \in [\![\ 1, 2n\ ]\!]^2,\ \begin{cases} [i > n \text{ et } j \leqslant n] \Longrightarrow m_{ij} = 0 \\ \\ [i \leqslant n \text{ et } j > n] \Longrightarrow m_{ij} = 0 \end{cases}$$

4/ Soient U et V deux matrices de **E**, notées :

$$U = \left(\begin{array}{c|c} A & 0_{\mathrm{M}_n(\mathbb{R})} \\ \hline 0_{\mathrm{M}_n(\mathbb{R})} & B \end{array}\right) \quad \text{et} \quad V = \left(\begin{array}{c|c} C & 0_{\mathrm{M}_n(\mathbb{R})} \\ \hline 0_{\mathrm{M}_n(\mathbb{R})} & D \end{array}\right) \quad \text{avec } A, B, C \text{ et } D \text{ dans } \mathrm{M}_n(\mathbb{R})$$

Etablir que $UV \in$ **E**.

Soient U et V comme dans l'énoncé. Notons $P = UV \in \mathrm{M}_{2n}(\mathbb{R})$.

➤ Soit $(i,j) \in [\![\ 1, 2n\ ]\!]^2$, tel que $i \leqslant n$ et $j > n$. On a :

$$p_{ij} = \sum_{k=1}^{2n} u_{ik}v_{kj} = \sum_{k=1}^{n} u_{ik}\underbrace{v_{kj}}_{=0} + \sum_{k=n+1}^{2n} \underbrace{u_{ik}}_{=0}v_{kj} = 0$$

➤ Soit $(i,j) \in [\![\ 1, 2n\ ]\!]^2$, tel que $j \leqslant n$ et $i > n$. On a :

$$p_{ij} = \sum_{k=1}^{2n} u_{ik}v_{kj} = \sum_{k=1}^{n} \underbrace{u_{ik}}_{=0}v_{kj} + \sum_{k=n+1}^{2n} u_{ik}\underbrace{v_{kj}}_{=0} = 0$$

➤ En résumé, on a établi que : $\forall\ (i,j) \in [\![\ 1, 2n\ ]\!]^2,\ \begin{cases} [i > n \text{ et } j \leqslant n] \Longrightarrow p_{ij} = 0 \\ \\ [i \leqslant n \text{ et } j > n] \Longrightarrow p_{ij} = 0 \end{cases}$

Ce qui signifie que P appartient à **E**.

Conclusion. E est stable par produit.

Dans la suite de l'exercice, on pourra admettre que : $UV = \left(\begin{array}{c|c} AC & 0_{\mathrm{M}_n(\mathbb{R})} \\ \hline 0_{\mathrm{M}_n(\mathbb{R})} & BD \end{array}\right)$.

5/ Un cas particulier. On considère la matrice $W \in \mathrm{M}_4(\mathbb{R})$ ci-dessous :

$$W = \frac{1}{2}\begin{pmatrix} 1 & -\sqrt{3} & 0 & 0 \\ \sqrt{3} & 1 & 0 & 0 \\ 0 & 0 & \sqrt{2} & -\sqrt{2} \\ 0 & 0 & \sqrt{2} & \sqrt{2} \end{pmatrix}$$

a/ Etablir que W est inversible, et préciser son inverse.

D'après l'énoncé : $W = \left(\begin{array}{c|c} R\left(\frac{\pi}{3}\right) & 0_{\mathrm{M}_n(\mathbb{R})} \\ \hline 0_{\mathrm{M}_n(\mathbb{R})} & R\left(\frac{\pi}{4}\right) \end{array}\right)$

D'après l'indication précédente, et la question 1, on peut affirmer que la matrice W est inversible et que :

$$W^{-1} = \left(\begin{array}{c|c} R\left(-\frac{\pi}{3}\right) & 0_{\mathrm{M}_n(\mathbb{R})} \\ \hline 0_{\mathrm{M}_n(\mathbb{R})} & R\left(-\frac{\pi}{4}\right) \end{array}\right)$$

b/ Soit q un entier naturel. Montrer que : $\quad [W^q = \mathbf{I}_4] \iff [q \equiv 0 \ [24]]$

Soit $q \in \mathbb{N}$. D'après l'indication de l'énoncé sur le produit UV, et la question 2, on a :

$$W^q = \left(\begin{array}{c|c} R\left(\frac{q\pi}{3}\right) & 0_{\mathrm{M}_n(\mathbb{R})} \\ \hline 0_{\mathrm{M}_n(\mathbb{R})} & R\left(\frac{q\pi}{4}\right) \end{array}\right)$$

Par suite :

$$[W^q = \mathbf{I}_4] \iff \left[R\left(\frac{q\pi}{3}\right) = \mathrm{I}_2 \wedge R\left(\frac{q\pi}{4}\right) = \mathrm{I}_2\right]$$

Or, selon la question 3 :

$$\left[R\left(\frac{q\pi}{3}\right) = \mathrm{I}_2\right] \iff [q \equiv 0 \ [6]] \qquad \text{et} \qquad \left[R\left(\frac{q\pi}{4}\right) = \mathrm{I}_2\right] \iff [q \equiv 0 \ [8]]$$

On en déduit que : $[W^q = \mathbf{I}_4] \iff [6|q \text{ et } 8|q] \iff [(6 \vee 8)|q] \iff [24|q]$

Conclusion. $[W^q = \mathbf{I}_4] \iff [q \equiv 0 \ [24]]$

Exercice 2 — (Autour de la fonction arcsinus)

Partie A - Non-dérivabilité à gauche de 1 de la fonction arcsinus

1/ Etablir le développement limité à l'ordre 2 en $\frac{\pi}{2}$ de la fonction sinus.

On effectue un **retour à l'origine** en posant : $X = x - \frac{\pi}{2}$ (d'où : $x = X + \frac{\pi}{2}$).

On a : $\sin(x) = \sin\left(X + \frac{\pi}{2}\right) = \cos(X)$.

Or, selon le formulaire : $\cos(X) = 1 - \frac{X^2}{2} + o(X^2)$.

Conclusion. Au voisinage de $\frac{\pi}{2}$, on a : $\sin(x) = 1 - \frac{\left(x - \frac{\pi}{2}\right)^2}{2} + o_{\frac{\pi}{2}}\left(\left(x - \frac{\pi}{2}\right)^2\right)$

2/ Etablir que :

$$\lim_{x \to 1^-} \frac{\arcsin(x) - \frac{\pi}{2}}{x - 1} = \lim_{u \to (\pi/2)^-} \frac{u - \frac{\pi}{2}}{\sin(u) - 1}$$

Soit x un réel de $[0, 1[$. Posons : $u = \arcsin(x)$.

On a : $\sin(u) = \sin(\arcsin(x)) = x$ puisque $\sin \circ \arcsin = \mathrm{id}_{[-1,1]}$.

En outre : $\lim\limits_{x \to 1^-} \arcsin(x) = \frac{\pi}{2}^-$.

Conclusion. D'après ce qui précède : $\lim\limits_{x \to 1^-} \frac{\arcsin(x) - \frac{\pi}{2}}{x - 1} = \lim\limits_{u \to (\pi/2)^-} \frac{u - \frac{\pi}{2}}{\sin(u) - 1}$

3/ A l'aide des deux questions précédentes, conclure.

D'après la question 1 :

$$\lim_{u \to (\pi/2)^-} \frac{u - \frac{\pi}{2}}{\sin(u) - 1} = \lim_{u \to (\pi/2)^-} \frac{u - \frac{\pi}{2}}{-\frac{\left(u - \frac{\pi}{2}\right)^2}{2} + o_{\frac{\pi}{2}}\left(\left(u - \frac{\pi}{2}\right)^2\right)} =$$

D'où :

$$\lim_{u \to (\pi/2)^-} \frac{u - \frac{\pi}{2}}{\sin(u) - 1} = \lim_{u \to (\pi/2)^-} \frac{1}{-\frac{\left(u - \frac{\pi}{2}\right)}{2} + o_{\frac{\pi}{2}}\left(\left(u - \frac{\pi}{2}\right)\right)}$$

Or :

$$\frac{1}{-\frac{\left(u - \frac{\pi}{2}\right)}{2} + o_{\frac{\pi}{2}}\left(\left(u - \frac{\pi}{2}\right)\right)} \sim_{\frac{\pi}{2}} \frac{2}{\frac{\pi}{2} - u}$$

On en déduit que :

$$\lim_{u\to(\pi/2)^-} \frac{u-\frac{\pi}{2}}{\sin(u)-1} = \lim_{u\to(\pi/2)^-} \frac{2}{\frac{\pi}{2}-u} = +\infty$$

D'après ce résultat et la question 2, on a : $\lim\limits_{x\to 1^-} \dfrac{\arcsin(x)-\frac{\pi}{2}}{x-1} = +\infty$

Conclusion. La fonction arcsinus n'est pas dérivable (à gauche) en 1.

Partie B - Un premier développement limité

Soit f la fonction définie sur $I =]-1,1[$ en posant :

$$\forall\, x \in I, \quad f(x) = (1+x)^\alpha \qquad \text{où } \alpha \text{ désigne un réel non nul.}$$

Le but de cette partie est de déterminer le développement limité à l'ordre n (n étant un entier arbitraire) en 0 de la fonction f.

4/ Justifier brièvement que f admet un développement limité à tout ordre n en 0 ; puis rappeler (sans justifications supplémentaires) le développement limité à l'ordre 3 en 0 de f.

Selon les théorèmes généraux, la fonction f est de classe $\mathscr{C}^\infty$ au voisinage de 0 : elle admet donc un DL à tout ordre en 0.

Par ailleurs, selon le cours, au voisinage de 0 :

$$f(x) = 1 + \alpha x + \frac{\alpha(\alpha-1)x^2}{2!} + \frac{\alpha(\alpha-1)(\alpha-2)x^3}{3!} + o(x^3)$$

5/ Justifier brièvement que pour tout réel $x \in I$, on a : $(1+x)f'(x) = \alpha f(x)$.

Pour tout réel $x \in I$, on a : $f'(x) = \alpha(1+x)^{\alpha-1}$. D'où : $\forall\, x \in I,\ (1+x)f'(x) = \alpha f(x)$

6/ En déduire à l'aide de la formule de Leibniz que pour tout entier naturel k on a :

$$f^{(k+1)}(0) = (\alpha - k) f^{(k)}(0)$$

Soit k un entier naturel. Selon les théorèmes généraux, les fonctions $x \mapsto (1+x)$ et f' sont de classe $\mathscr{C}^k$ sur I, et on peut donc utiliser la formule de Leibniz pour calculer la dérivée k-ème de $x \mapsto (1+x)f'(x)$.

Selon la question précédente, on a donc pour tout réel x dans I :

$$(1+x)f'^{(k)}(x) + \binom{k}{1} f'^{(k-1)}(x) = \alpha f^{(k)}(x) \iff (1+x)f^{(k+1)}(x) + kf^{(k)}(x) = \alpha f^{(k)}(x)$$

$$\iff (1+x)f^{(k+1)}(x) = (\alpha-k)f^{(k)}(x)$$

L'évaluation en $x = 0$ de cette relation permet de conclure.

Conclusion. $\forall\, k \in \mathbb{N},\ f^{(k+1)}(0) = (\alpha-k)f^{(k)}(0)$

7/ Montrer que : $\forall k \in \mathbb{N}^*,\ f^{(k)}(0) = \prod_{j=0}^{k-1}(\alpha - j)$

Posons pour tout entier naturel non nul k l'assertion P(k) : "$f^{(k)}(0) = \prod_{j=0}^{k-1}(\alpha - j)$"

Pour $k = 1$, on a : $f'(0) = \alpha$ et $\prod_{j=0}^{0}(\alpha - j) = \alpha$. Donc P$(1)$ est vraie.

Passons à l'hérédité. On suppose P(k) vraie pour un certain entier naturel non nul k. Alors, d'après la question précédente et l'hypothèse de récurrence on a :

$$f^{(k+1)}(0) = (\alpha - k)\prod_{j=0}^{k-1}(\alpha - j) \quad \text{d'où :} \quad f^{(k+1)}(0) = \prod_{j=0}^{k}(\alpha - j)$$

Ce qui signifie que $P(k+1)$ est vraie, et établit l'hérédité de la propriété.

Conclusion. $\forall k \in \mathbb{N}^*,\ f^{(k)}(0) = \prod_{j=0}^{k-1}(\alpha - j)$

Partie C - DL en 0 à tout ordre de $x \longmapsto 1/\sqrt{1+x}$, et de la fonction arcsinus

8/ A l'aide de la partie précédente, montrer que :

$$\forall x \in I,\ \forall n \in \mathbb{N}^*,\ \frac{1}{\sqrt{1+x}} = 1 + \sum_{k=1}^{n}\left[\frac{(-1)^k}{2^k \times (k!)}\prod_{i=0}^{k-1}(1+2i)\right]x^k + o\left(x^n\right)$$

Posons à présent pour tout réel x dans I : $g(x) = \dfrac{1}{\sqrt{1+x}} = (1+x)^{-1/2}$.

D'après la formule de Taylor-Young, on a :

$$\forall x \in I,\ \forall n \in \mathbb{N}^*,\ g(x) = 1 + \sum_{k=1}^{n}\frac{g^{(k)}(0)}{k!}x^k + o\left(x^n\right) \qquad (\spadesuit)$$

Par ailleurs, d'après la question 7 on a : $\forall k \in \mathbb{N}^*,\ g^{(k)}(0) = \prod_{i=0}^{k-1}\left(-\frac{1}{2} - i\right)$.

Or : $$\prod_{i=0}^{k-1}\left(-\frac{1}{2} - i\right) = \prod_{i=0}^{k-1}\left[-\left(\frac{1+2i}{2}\right)\right] = \frac{(-1)^k}{2^k}\prod_{i=0}^{k-1}(1+2i) \quad (\clubsuit)$$

Conclusion. D'après $(\spadesuit)$ et $(\clubsuit)$:

$$\forall x \in I,\ \forall n \in \mathbb{N}^*,\ \frac{1}{\sqrt{1+x}} = 1 + \sum_{k=1}^{n}\left[\frac{(-1)^k}{2^k \times (k!)}\prod_{i=0}^{k-1}(1+2i)\right]x^k + o\left(x^n\right)$$

9/ Etablir que : $\forall k \in \mathbb{N}^*, \quad \prod_{i=0}^{k-1}(1+2i) = \dfrac{(2k)!}{2^k \times (k!)}$

Notons pour tout entier naturel k l'assertion $\mathrm{P}(k)$: "$\prod_{i=0}^{k-1}(1+2i) = \dfrac{(2k)!}{2^k \times (k!)}$".

L'initialisation est immédiate.

Supposons que $\mathrm{P}(k)$ est vraie pour un entier naturel non nul k. Alors :

$$\prod_{i=0}^{k}(1+2i) = (1+2k)\prod_{i=0}^{k-1}(1+2i)$$

D'où, par hypothèse de récurrence :

$$\prod_{i=0}^{k}(1+2i) = \frac{(2k+1)\times[(2k)!]}{2^k \times (k!)} = \frac{(2k+2)(2k+1)\times[(2k)!]}{(2k+2)\times 2^k \times (k!)} = \frac{(2k+2)!}{2^{k+1}\times((k+1)!)}$$

Ce qui signifie que la propriété $\mathrm{P}(k+1)$ est vraie, et établit l'hérédité de la propriété.

Conclusion. $\forall k \in \mathbb{N}^*, \ \prod_{i=0}^{k-1}(1+2i) = \dfrac{(2k)!}{2^k \times (k!)}$

10/ En déduire que :

$$\forall x \in I, \ \forall n \in \mathbb{N}^*, \quad \frac{1}{\sqrt{1+x}} = 1 + \sum_{k=1}^{n}\left[\frac{(-1)^k}{2^{2k}}\binom{2k}{k}\right]x^k + o\left(x^n\right)$$

Soient $x \in I$ et $n \in \mathbb{N}^*$. D'après les questions 8 et 9 on a :

$$\frac{1}{\sqrt{1+x}} = 1 + \sum_{k=1}^{n}\left[\frac{(-1)^k}{2^k \times (k!)}\frac{(2k)!}{2^k \times (k!)}\right]x^k + o\left(x^n\right) = 1 + \sum_{k=1}^{n}\left[\frac{(-1)^k}{2^{2k}}\underbrace{\frac{(2k)!}{(k!)\times(k!)}}_{=\binom{2k}{k}}\right]x^k + o\left(x^n\right)$$

Conclusion. $\forall x \in I, \ \forall n \in \mathbb{N}^*, \ \dfrac{1}{\sqrt{1+x}} = 1 + \sum_{k=1}^{n}\left[\dfrac{(-1)^k}{2^{2k}}\binom{2k}{k}\right]x^k + o\left(x^n\right)$

11/ Dans cette question, n désigne encore un entier naturel non nul. Déterminer le développement limité à l'ordre $2n+2$ en 0 de la fonction arcsinus.

D'après ce qui précède :*

$$\forall x \in I, \ \forall n \in \mathbb{N}^*, \ \frac{1}{\sqrt{1-x}} = 1 + \sum_{k=1}^{n}\left[\frac{1}{2^{2k}}\binom{2k}{k}\right]x^k + o\left(x^n\right)$$

Par conséquent :†

$$\forall x \in I, \ \forall n \in \mathbb{N}^*, \ \frac{1}{\sqrt{1-x^2}} = 1 + \sum_{k=1}^{n}\left[\frac{1}{2^{2k}}\binom{2k}{k}\right]x^{2k} + o\left(x^{2n}\right)$$

∗. Et en observant que $x \in I \Longrightarrow (-x) \in I$

†. En observant que $x \in I \Longrightarrow x^2 \in I$

Puisque la fonction $x \longmapsto (1-x^2)^{-1/2}$ est paire, on peut affirmer que :

$$\forall\, x \in I,\ \forall\, n \in \mathbb{N}^*,\ \frac{1}{\sqrt{1-x^2}} = 1 + \sum_{k=1}^{n} \left[\frac{1}{2^{2k}} \binom{2k}{k} \right] x^{2k} + o\left(x^{2n+1}\right)$$

Enfin, puisque la fonction arcsinus est l'unique primitive de $x \longmapsto (1-x^2)^{-1/2}$ s'annulant en 0, on en déduit que :

$$\boxed{\forall\, x \in I,\ \forall\, n \in \mathbb{N}^*,\ \arcsin(x) = x + \sum_{k=1}^{n} \left[\frac{1}{2^{2k}\,(2k+1)} \binom{2k}{k} \right] x^{2k+1} + o\left(x^{2n+2}\right)}.$$

Exercice BLANC — 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 admettra dans cet exercice que $41 \in \mathscr{P}$.

1/ Sans calculer leur PGCD, justifier que les entiers 18 et 41 sont premiers entre eux.

41 est premier, et 41 ne divise pas 18. D'après le cours : 18 et 41 sont premiers entre eux.

2/ Résoudre dans $\mathbb{Z}^2$ l'équation : (E_1) $18x + 41y = 3$.

On peut commencer par déterminer un couple (u, v) de coefficients de Bezout pour les entiers 18 et 41, pour en déduire une solution particulière de (E_1).
L'algorithme d'Euclide donne :

$41 = 18 \times 2 + 5$

$18 = 5 \times 3 + 3$

$5 = 3 \times 1 + 2$

$3 = 2 \times 1 + 1$

On en déduit que $18 \wedge 41 = 1$.

En "remontant l'algorithme", on obtient successivement : $1 = 2\times 3 - 5 = 2\times 18 - 7\times 5 = 16\times 18 - 7\times 41$

Ainsi : $18 \times 16 - 41 \times 7 = 1$.

On en déduit que le couple $(48, -21)$ est solution de (E).

Des calculs de routine permettent de conclure.

Conclusion. L'ensemble des solutions de (E) est $\{(48 - 41k, -21 + 18k)\ /\ k \in \mathbb{Z}\}$

3/ Soit $n \in \mathbb{Z}$, tel que $n \notin 41\mathbb{Z}$. A l'aide du petit théorème de Fermat, établir que : $41 | n^{40} - 1$

Soit $n \in \mathbb{Z}$, tel que $n \notin 41\mathbb{Z}$. Puisque 41 est un nombre premier, le petit théorème de Fermat donne :

$$n^{41} \equiv n\,[41] \quad \text{d'où : } 41 | n^{41} - n \quad \text{soit encore : } 41 | n\,(n^{40} - 1)$$

Or $41 \wedge n = 1$ (puisque $41 \in \mathscr{P}$ et $n \notin 41\mathbb{Z}$). On en déduit grâce au théorème de Gauss que :

$$41 | n^{40} - 1$$

Conclusion. $\forall n \in \mathbb{Z}\backslash 41\mathbb{Z}, \quad 41|n^{40}-1$

4/ Etablir qu'il n'existe pas de triplet d'entiers (x,y,z) tel que : $x^{40}+y^{40}+z^{40} = 123\times 19^{2023}+8$.

Supposons qu'il existe un triplet d'entiers (x,y,z) tel que : $x^{40}+y^{40}+z^{40} = 123\times 19^{2023}+8$.

Alors on aurait : $x^{40}+y^{40}+z^{40} \equiv 123\times 19^{2023}+8\ [41]$ soit : $x^{40}+y^{40}+z^{40} \equiv 123\times 19^{2023}+8\ [41]$.

Or d'après la question précédente, on a $x^{40}\equiv 1$ modulo 41 (si 41 ne divise pas x) ou $x^{40}\equiv 0$ modulo 41 (si 41 divise x)

On en déduit que $x^{40}+y^{40}+z^{40}$ peut être congru à 0, 1, 2 ou 3 modulo 41 ; mais pas à 8.

La congruence $x^{40}+y^{40}+z^{40}\equiv 8\ [41]$ n'est donc vérifiée pour aucun triplet d'entiers (x,y,z).

Conclusion. Il n'existe pas de triplet d'entiers (x,y,z) tel que : $x^{40}+y^{40}+z^{40} = 123\times 19^{2023}+8$.

5/ Un cas particulier du théorème de Dirichlet. La fin de cet exercice consiste à établir qu'il existe une infinité de nombre premiers congrus à 1 modulo 4 (comme 41).

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 : $N = 1+4\times\left(\prod_{k=1}^{m} p_k^2\right)$ soit : $N = 1+4\,(p_1\times\cdots\times p_m)^2$.

Soit p un diviseur premier de N.

a/ Justifier que $p\geqslant 3$.

p est premier impair, puisque 2 ne divise clairement pas N. **Conclusion.** $p\geqslant 3$

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

On a : $x^2+1 = N$. Puisque p est un diviseur de N, on a : $N\equiv 0\,[p]$. **Conclusion.** $x^2+1\equiv 0\ [p]$

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

Supposons que p divise x. Alors p divise x^2, et N. Donc p divise $N-x^2$, soit p divise 1 : absurde ! Donc p ne divise pas x.

Par un raisonnement analogue à celui de la question 3, on en déduit que : $x^{p-1}\equiv 1\ [p]$.

Conclusion. $x^{p-1}\equiv 1\ [p]$

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

L'entier p étant premier et distinct de 2, il est impair. Ainsi $p-1$ est pair, et le rationnel $\dfrac{p-1}{2}$ est donc un entier.

De plus : $x^p = (x^2)^{(p-1)/2}$. Or $x^2\equiv -1\ [p]$ d'après la question b.

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

e/ 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 c).

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

Exercice ORANGE — Groupes et arithmétique

Partie A - Sous-groupe engendré par un élément dans un groupe

Soient $(G, *)$ un groupe d'élément neutre e, et g un élément de G.

On note $g^2 = g*g$, $g^3 = g*g*g$. Plus généralement, pour tout entier naturel n, on note $g^n = \underbrace{g*g*\cdots*g}_{\text{avec } n \text{ g}}$

Cette notation peut être étendue aux entiers relatifs ; si n est un entier négatif, on pose : $g^n = (g^{-1})^{-n}$ pour se ramener à la définition précédente.

Enfin, on convient que $g^0 = \text{e}$, et que $g^1 = g$.

1/ On note : $\langle g \rangle = \left\{ g^k\ ,\ k \in \mathbb{Z} \right\}$. Montrer que $(\langle g \rangle\ , *)$ est un sous-groupe de $(G, *)$.

Par définition, $\langle g \rangle$ est une partie de G (SG1), contenant l'élément neutre de G (puisque $\text{e} = g^0$, SG2), stable pour la loi $*$ (SG3) et par passage à l'inverse (SG4).

Conclusion. $(\langle g \rangle\ , *)$ est un sous-groupe de $(G, *)$.

2/ On suppose dans cette question que g est **d'ordre fini**, càd qu'il existe un entier naturel N non nul tel que $g^N = \text{e}$ (et cet entier N est appelé l'**ordre de** g).

a/ Démontrer que : $\langle g \rangle = \left\{ g^k,\ k \in [\![\ 0, N-1\ ]\!] \right\}$

➤ On peut déjà observer que : $\left\{ g^k,\ k \in [\![\ 0, N-1\ ]\!] \right\} \subset \langle g \rangle$ (puisque $[\![\ 0, N-1\ ]\!] \subset \mathbb{Z}$, waouh !).

➤ Réciproquement, soit γ un élément de $\langle g \rangle$. Il existe un entier relatif k tel que $\gamma = g^k$.

Selon le théorème de la division euclidienne, il existe un unique couple (q, r) tel que :

$$k = Nq + r \qquad \text{et} \qquad r \in [\![\ 0, N-1\ ]\!]$$

Par suite :

$$\gamma = g^{Nq+r} = g^{Nq} * g^r = \left(g^N\right)^q * g^r = \text{e} * g^r = g^r$$

En résumé : $\gamma = g^r$ avec $r \in [\![\ 0, N-1\ ]\!]$. D'où : $\gamma \in \left\{ g^k,\ k \in [\![\ 0, N-1\ ]\!] \right\}$.

Ce qui prouve l'inclusion : $\left\{ g^k,\ k \in [\![\ 0, N-1\ ]\!] \right\} \supset \langle g \rangle$.

Conclusion. D'après la règle de double inclusion : $\left\{ g^k,\ k \in [\![\ 0, N-1\ ]\!] \right\} = \langle g \rangle$

b/ Démontrer avec soin que : $\text{Card}\,(\langle g\rangle) = N$

D'après la question précédente : $\text{Card}\,(\langle g\rangle) = \text{Card}\left(\left\{g^k,\ k \in [\![\, 0, N-1\,]\!]\right\}\right)$.

Ce qui assure que : $\text{Card}\,(\langle g\rangle) \leqslant N$.

Pour établir l'égalité, il s'agit de prouver que les éléments de $\left\{g^k,\ k \in [\![\, 0, N-1\,]\!]\right\}$ sont 2 à 2 distincts.

A cette fin, on raisonne par l'absurde en supposant qu'il existe deux entiers distincts k_1 et k_2 dans $[\![\, 0, N-1\,]\!]$ tels que : $g^{k_1} = g^{k_2}$.

SNALG, on peut supposer $k_1 > k_2$, et on en déduit que :

$$g^{k_1-k_2} = \text{e avec } 0 < k_1 - k_2 < N$$

On a ainsi prouvé l'existence d'un entier naturel m non nul ($m = k_1 - k_2$) tel que $g^m = \text{e}$, et tel que m est strictement plus petit que l'ordre de g (égal à N) : contradiction.

On en déduit que les éléments de $\left\{g^k,\ k \in [\![\, 0, N-1\,]\!]\right\}$ sont 2 à 2 distincts.

Conclusion. $\text{Card}\,(\langle g\rangle) = N$

Partie B - Ordre d'un élément dans un groupe fini

Tout au long de cette partie, $(G, *)$ désigne un groupe d'élément neutre e. On suppose en outre que G est fini, de cardinal $n \in \mathbb{N}^*$.

Soit $(H, *)$ un sous-groupe de G. Pour tout élément g de G, on note : $gH = \{g * h\,/\,h \in H\}$.

3/ Etablir que pour tout élément g de G, on a : $\text{Card}\,(gH) = \text{Card}\,(H)$.

Soit H un sous-groupe d'un groupe fini G. Observons que H est de cardinal fini, en tant que partie d'un ensemble fini.

Soit g un élément arbitraire de G.
Les applications $\varphi : H \longrightarrow gH$ et $\psi : gH \longrightarrow H$ sont clairement réciproques l'une de l'autre.
$h \longmapsto g * h$ $\quad$ $x \longmapsto g^{-1} * x$

En particulier φ et ψ sont bijectives ; H et gH sont donc équipotents. D'où : $\text{Card}(H) = \text{Card}(gH)$.

Conclusion. Pour tout élément g de G on a : $\text{Card}(H) = \text{Card}(gH)$

4/ Soient g et g' deux éléments de G. Montrer que les ensembles gH et $g'H$ sont soit égaux, soit disjoints.

Soient g et g' deux éléments de G. Supposons que gH et $g'H$ ne sont pas disjoints. Alors il existe deux éléments h et k dans H tels que : $g * h = g' * k$. En particulier : $g^{-1} * g' = h * k^{-1} \in H$.‡

Soit alors γ un élément quelconque de $g'H$. Il existe un élément h_0 de H tel que : $\gamma = g' * h_0$. On écrit alors judicieusement : $\gamma = g * g^{-1} * g' * h_0$. On en déduit que : $\gamma = g * \underbrace{h * k^{-1} * h_0}_{\in H}$. Par suite : $\gamma \in gH$.

On a ainsi établi que : $g'H \subset gH$.

‡. En effet, k est un élément de H. Puisque H est un sous-groupe, k^{-1} est un élément de H. Par ailleurs, h est un autre élément de H. En utilisant une nouvelle fois le fait que H est un sous-groupe, on en déduit que : $h * k^{-1} \in H$.

En réécrivant le même raisonnement en permutant g et g', ou en observant que g et g' jouent des rôles symétriques dans le raisonnement précédent, on obtient l'autre inclusion : $gH \subset g'H$. Finalement, lorsque gH et $g'H$ ne sont pas disjoints, ils sont égaux.

Conclusion. Pour tout couple (g, g') d'éléments de G, on a $[gH = g'H]$ ou $[gh \cap g'H = \emptyset]$

5/ En déduire que le cardinal de H divise celui de G.

Le groupe G est fini par hypothèse. On peut donc noter : $G = \{g_1, \ldots, g_n\}$ (avec $n = \text{Card}(G)$). On a alors :

$G = \bigcup_{i=1}^{n} \{g_i\}$ et donc $G = \bigcup_{i=1}^{n} g_i H$. La première égalité provient de l'observation puissante selon laquelle un ensemble fini est la réunion des singletons qui le composent ; la seconde découle de la première et du fait que pour tout entier i on a : $\{g_i\} \subset g_i H \subset G$.

D'après la question précédente, il peut exister parmi les $g_i H$ des ensembles égaux. Notons alors k le nombre de parties disjointes parmi ces $g_i H$. Quitte à renuméroter les g_i, on peut supposer qu'il s'agit des k premières parties, et on alors : $G = \bigcup_{i=1}^{k} g_i H$. Cette union étant disjointe, on a donc : $\text{Card}(G) = \sum_{i=1}^{k} \text{Card}\,(g_i H)$. Or d'après la question 1, on a : $\text{Card}(g_i H) = \text{Card}(H)$ (pour tout g_i).

On en déduit que : $\text{Card}(G) = \sum_{i=1}^{k} \text{Card}\,(H)$ d'où : $\text{Card}(G) = k\text{Card}\,(H)$. Finalement, le cardinal de G est multiple de celui de H.

Conclusion. Si G est un groupe fini, le cardinal de tout sous-groupe de G divise le cardinal de G.

6/ **Application.** Montrer que si G est fini de cardinal n, alors : $\forall\, g \in G,\ g^n = \text{e}$.

Soit g un élément d'un groupe fini G de cardinal n. Alors $\langle g \rangle$ (le sous-groupe engendré par g) est un sous-groupe de G. Notons N son cardinal. On a $g^N = \text{e}$, et N divise n d'après la question précédente. Il existe donc un entier d tel que $n = dN$. On en déduit que :

$$g^n = g^{dN} = \left(g^N\right)^d = \text{e}^d = \text{e}$$

Conclusion. Dans un groupe fini G de cardinal n, on a : $g^n = \text{e}$ pour tout élément g de G.

Partie C - Sous-groupes finis de $\mathbb{U}$

7/ Soit $(G, \times)$ un sous-groupe fini de $(\mathbb{U}, \times)$. Montrer qu'il existe un entier $n \in \mathbb{N}^*$ tel que $G = \mathbb{U}_n$.

Soit G un sous-groupe fini de $\mathbb{U}$. Notons n son cardinal. D'après la question précédente : $\forall\, g \in G,\ g^n = 1$. On en déduit que : $[g \in G] \Longrightarrow [g \in \mathbb{U}_n]$.

Par suite : $G \subset \mathbb{U}_n$. Puisqu'en outre G et $\mathbb{U}_n$ sont de même cardinal, on en déduit que $G = \mathbb{U}_n$.

Conclusion. Si G est un sous-groupe de $\mathbb{U}$ de cardinal n, alors $G = \mathbb{U}_n$.

8/ Soient m et n dans $\mathbb{N}^*$. Montrer que : $[\mathbb{U}_m \subset \mathbb{U}_n] \Longleftrightarrow [m \,|\, n]$.

Soient n et m deux entiers naturels. Supposons que : $\mathbb{U}_m \subset \mathbb{U}_n$. On a alors en particulier : $\text{e}^{2\text{i}\,k\pi/m} \in \mathbb{U}_n$.

D'où : $\left(\text{e}^{2\text{i}\,k\pi/m}\right)^n = 1 \Longrightarrow \text{e}^{2\text{i}\,nk\pi/m} = 1 \Longrightarrow \dfrac{n}{m} \in \mathbb{Z} \Longrightarrow m|n$.

Conclusion. $[\mathbb{U}_m \subset \mathbb{U}_n] \Longleftrightarrow [m \,|\, n]$

9/ Soient m et n dans $\mathbb{N}^*$. Montrer que : $\mathbb{U}_m \cap \mathbb{U}_n = \mathbb{U}_{m\wedge n}$.

Soient m et n deux entiers naturels non nuls.

Soit $g \in \mathbb{U}_m \cap \mathbb{U}_n$. D'après le théorème de Bezout, il existe deux entiers u et v tels que : $mu+nv = m\wedge n$. On en déduit que : $g^{m\wedge n} = g^{mu+nv} = g^{mu}g^{nv} = 1^u 1^v = 1$. D'où : $g \in \mathbb{U}_{m\wedge n}$. Ainsi : $\mathbb{U}_m \cap \mathbb{U}_n \subset \mathbb{U}_{m\wedge n}$.

Dans l'autre sens : il existe deux entiers k et p tels que $n = k\,(m \wedge n)$ et $m = p\,(m \wedge n)$. Considérons alors un élément g de $U_{m\wedge n}$. On a : $g^{m\wedge n} = 1$. A fortiori : $g^n = (g^{m\wedge n})^k = 1$ et $g^m = (g^{m\wedge n})^p = 1$. Il s'ensuit que $g \in \mathbb{U}_m \cap \mathbb{U}_n$. D'où : $\mathbb{U}_{m\wedge n} \subset \mathbb{U}_m \cap \mathbb{U}_n$.

Conclusion. $\mathbb{U}_m \cap \mathbb{U}_n = \mathbb{U}_{m\wedge n}$