DEVOIR SURVEILLÉ N°5

Sujet donné le samedi 18 janvier 2025, 4h.

L'usage de la calculatrice n'est pas autorisé.

La notation tiendra particulièrement compte de la **qualité de la rédaction, la précision des raisonnements et l'énoncé des formules utilisés**. Les réponses aux questions seront numérotées et séparées par un trait horizontal. Les résultats essentiels devront être encadrés ou soulignés.

BON TRAVAIL

PROBLÈME - PETIT THÉORÈME DE FERMAT GÉNÉRALISÉ AU CALCUL MATRICIEL

Ce problème est composé de quatre parties indépendantes les unes des autres sauf mention du contraire.

Soit $n \in \mathbb{N}^*$. Pour $M \in \mathcal{M}_n(\mathbb{Z})$ et $(i, j) \in \llbracket 1, n \rrbracket^2$, on note $[M]_{i,j}$ le coefficient de M situé sur la i -ème ligne et la j -ème colonne.

L'objectif du problème est de démontrer et d'exploiter une généralisation du petit théorème de Fermat pour les matrices à coefficients entiers :

$$\forall p, \text{ nombre premier, } \forall A \in \mathcal{M}_n(\mathbb{Z}), \quad \text{Tr}(A^p) = \text{Tr}(A) [p]$$

I . Étude d'une suite récurrente linéaire via un calcul matriciel

On considère dans cette partie une matrice

$$A = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ -6 & 7 & 0 \end{pmatrix}$$

I.1. Montrer, à l'aide d'un algorithme de Gauss, que A est inversible et calculer A^{-1} .

I.2. Montrer que $A^3 = 7A - 6I_3$. On notera $\Pi = X^3 - 7X + 6$.

On admet que pour tout $n \in \mathbb{N}$, $\exists !(Q_n, R_n) \in (\mathbb{R}[X])^2$ tel que $X^n = Q_n \times \Pi + R_n$ avec $\deg R_n < 3$.

(a) Montrer qu'il existe $(a_n, b_n, c_n) \in \mathbb{R}^3$ tel que pour tout $x \in \mathbb{R}$,

$$x^n = Q_n(x) \times \Pi(x) + (a_n x^2 + b_n x + c_n)$$

(b) En exploitant les racines de Π , donner un système de trois équations à trois inconnues dont l'unique solution est le triplet (a_n, b_n, c_n) .

(c) Montrer que la matrice $\frac{1}{20} \begin{pmatrix} -5 & 4 & 1 \\ -5 & 8 & -3 \\ 30 & -12 & 2 \end{pmatrix}$ est l'inverse de la matrice associée au système de la question précédente.

En déduire, pour tout $n \in \mathbb{N}$, une expression de A^n en fonction A^2 , A et I_3 .

(d) L'égalité obtenue dans la question I.2(c) est-elle encore vraie pour $n = -1$?

I.3. On considère la suite récurrente (u_n) définie par :

$$u_0 = 3, u_1 = 0, u_2 = 14 \quad \text{et} \quad \forall n \in \mathbb{N}, u_{n+3} = 7u_{n+1} - 6u_n$$

(a) Donner les valeurs de u_n pour $n \in \llbracket 1, 7 \rrbracket$.

On vérifiera qu'on trouve $u_7 = 882$.

(b) Que pensez-vous de l'ensemble $\{n \in \llbracket 1, 7 \rrbracket \text{ tel que } n|u_n\}$?

(c) On note pour tout $n \in \mathbb{N}$, $U_n = \begin{pmatrix} u_n \\ u_{n+1} \\ u_{n+2} \end{pmatrix}$.

Pour tout entier $n \in \mathbb{N}$, exprimer U_{n+1} en fonction de A et de U_n .

(d) En déduire une expression explicite de U_n , en fonction de A et U_0 .

(e) En déduire une expression explicite de u_n en fonction de n , pour tout entier $n \in \mathbb{N}$.

(f) Démontrer que, pour tout p premier, $p|u_p$.

I.4. (a) En utilisant l'expression polynomiale s'annulant en A , montrer que la suite $(\text{Tr}(A^n))_{n \in \mathbb{N}}$ satisfait la même relation de récurrence que u .

(b) En déduire que, pour tout $n \in \mathbb{N}$, $u_n = \text{Tr}(A^n)$.

Ce résultat permettra dans la partie IV, de redémontrer, sans calcul ou presque, le résultat de la question I.3(f).

(c) Retrouver ainsi l'expression de u_n en fonction de a_n et c_n obtenue dans la question I.3(e) (dont cette question propose une deuxième preuve).

II . Formule d'inversion de Möbius

Pour $n \in \mathbb{N}^*$, on note $\mathcal{D}_n$ l'ensemble des nombres entiers naturels (donc > 0) divisant n et on écrit $\sum_{d|n} \dots = \sum_{d \in \mathcal{D}_n} \dots$ la somme sur

tous les nombres entiers naturels d divisant n .

Une fonction arithmétique est une fonction $f : \mathbb{N}^* \rightarrow \mathbb{C}$. L'ensemble des fonctions arithmétiques est noté $\mathbb{A}$.

On dit qu'une fonction arithmétique $f \in \mathbb{A}$ est multiplicative si

$$\begin{cases} f(1) \neq 0 \\ \forall (m, n) \in (\mathbb{N}^*)^2, m \wedge n = 1 \Rightarrow f(mn) = f(m)f(n) \end{cases}$$

On note $\mathbb{M}$ l'ensemble des fonctions arithmétiques multiplicatives.

$$\text{On note } \mathbf{1} : \begin{cases} \mathbb{N}^* \rightarrow \mathbb{C} \\ n \mapsto 1 \end{cases} \text{ et } \delta : \begin{cases} \mathbb{N}^* \rightarrow \mathbb{C} \\ n \mapsto \begin{cases} 1 & \text{si } n = 1 \\ 0 & \text{sinon} \end{cases} \end{cases} .$$

Si f et g sont deux fonctions arithmétiques, le produit de convolution de f et g est la fonction arithmétique $f * g$ définie par

$$\forall n \in \mathbb{N}^*, \quad (f * g)(n) = \sum_{d|n} f(d)g\left(\frac{n}{d}\right)$$

Par exemple $(f * g)(12) = \sum_{d|12} f(d)g\left(\frac{12}{d}\right) = f(1)g(12) + f(2)g(6) + f(3)g(4) + f(4)g(3) + f(6)g(2) + f(12)g(1)$.

On notera que l'on a : $\forall n \in \mathbb{N}^*, (f * g)(n) = \sum_{d|n} f(d)g\left(\frac{n}{d}\right) = \sum_{d_1 d_2 = n} f(d_1)g(d_2) = \sum_{d|n} f\left(\frac{n}{d}\right)g(d)$

II.1. Montrer que $\mathbf{1}$ et δ sont des fonctions arithmétiques multiplicatives.

II.2. **Structure de $\mathbb{A}$.**

- (a) Montrer que $(\mathbb{A}, +)$ est un groupe abélien.
- (b) Montrer que $*$ est une loi interne commutative sur $\mathbb{A}$. On admet que $*$ est également associative.
- (c) Montrer que δ est l'élément neutre pour $*$.
- (d) Conclure que $(\mathbb{A}, +, *)$ est un anneau commutatif. Est-ce un corps ?

II.3. **Stabilité de la propriété de multiplicativité et structure de $\mathbb{M}$.**

- (a) Soient m et n deux entiers naturels non nuls premiers entre eux.

Montrer que $\pi : \begin{cases} \mathcal{D}_m \times \mathcal{D}_n \rightarrow \mathcal{D}_{mn} \\ (d_1, d_2) \mapsto d_1 d_2 \end{cases}$ est bien définie (i.e. bien à valeurs dans $\mathcal{D}_{mn}$) et réalise une bijection de $\mathcal{D}_m \times \mathcal{D}_n$ sur $\mathcal{D}_{mn}$.

De plus, si $(d_1, d_2) \in \mathcal{D}_m \times \mathcal{D}_n$, calculer $d_1 \wedge d_2$.

- (b) En déduire que si f et g sont multiplicatives, alors $f * g$ est multiplicative.
- (c) i. Montrer que, si f est une fonction arithmétique multiplicative, alors $f(1) = 1$.
ii. Soient f et g deux fonctions arithmétiques multiplicatives telles que, pour tout nombre premier p , pour tout $k \in \mathbb{N}^*$, $f(p^k) = g(p^k)$. Montrer que $f = g$.
- (d) Soit f une fonction multiplicative.

Posons $g(1) = 1$ puis, pour tout nombre premier p , définissons la suite $(g(p^k))_{k \in \mathbb{N}}$ par récurrence en posant

$$\forall k \in \mathbb{N}^*, \quad g(p^k) = - \sum_{i=1}^k f(p^i)g(p^{k-i})$$

Nous venons de définir une fonction g sur la réunion de $\{1\}$ et des nombres premiers. On prolonge g aux entiers naturels non nuls en posant, pour n supérieur à 2 non premier,

$$g(n) = \prod_{i=1}^q g(p_i^{\alpha_i})$$

où $p_1, \dots, p_q$ sont les facteurs premiers deux à deux distincts de n et $(\alpha_1, \dots, \alpha_q) \in \mathbb{N}^{*q}$ sont leurs multiplicités respectives. Justifier que g est multiplicative puis, calculer pour tout nombre premier p et tout entier $k \in \mathbb{N}$, $(f * g)(p^k)$ afin d'en déduire $f * g$.

- (e) Que dire de $(\mathbb{M}, *)$?

II.4. **Fonction de Möbius.**

Soit μ la fonction arithmétique définie par :

$$\mu(n) = \begin{cases} 1 & \text{si } n = 1, \\ (-1)^r & \text{si } n \text{ est le produit de } r \text{ nombres premiers distincts,} \\ 0 & \text{sinon.} \end{cases}$$

- (a) Montrer que μ est multiplicative.

- (b) i. Soit $n \geq 2$ et $p_1, \dots, p_q$ les $q \in \mathbb{N}^*$ facteurs premiers de n deux à deux distincts. On note, pour tout $k \in \llbracket 0, q \rrbracket$, P_k l'ensemble des parties de $\llbracket 1, q \rrbracket$ comportant k éléments. Montrer que

$$\sum_{d|n} \mu(d) = 1 + \sum_{k=1}^q \sum_{I \in P_k} \mu \left(\prod_{i \in I} p_i \right) = 1 + \sum_{k=1}^q (-1)^k \binom{q}{k}$$

ii. En déduire que $\mu * \mathbf{1} = \delta$.

- (c) Soit $f \in \mathbb{A}$ et $F \in \mathbb{A}$ telle que, pour tout $n \in \mathbb{N}^*$, $F(n) = \sum_{d|n} f(d)$. Montrer que pour tout $n \in \mathbb{N}^*$,

$$f(n) = \sum_{d|n} \mu(d) F \left(\frac{n}{d} \right) = \sum_{d|n} \mu \left(\frac{n}{d} \right) F(d)$$

II.5. (★) On note $\mathbf{I} : \begin{array}{l} \mathbb{N}^* \rightarrow \mathbb{C} \\ n \mapsto n \end{array}$ et φ la fonction indicatrice d'Euler, définie par

$$\forall n \in \mathbb{N}^*, \quad \varphi(n) = \text{card}\{k \in \llbracket 1, n \rrbracket \mid k \wedge n = 1\}$$

Montrer que $\varphi = \mu * \mathbf{I}$ puis en déduire que $\forall n \in \mathbb{N}^*$, $n = \sum_{d|n} \varphi(d)$.

III . Mots circulaires

Dans cette partie, l'entier naturel m est fixé.

On considère un alphabet de m lettres : $\mathcal{A} = \{a_1, a_2, \dots, a_m\}$.

Un mot ℓ sur l'alphabet $\mathcal{A}$ est une suite de $\mathcal{A}^{\mathbb{N}}$: $\ell = (\ell_0, \ell_1, \ell_2, \dots)$ où, pour tout $i \in \mathbb{N}$, $\ell_i \in \mathcal{A}$ est la $(i+1)$ -ème lettre du mot ℓ .

Le mot ℓ est périodique s'il existe $p \in \mathbb{N}^*$ tel que $\forall i \in \mathbb{N}$, $\ell_{i+p} = \ell_i$. Un tel entier naturel non nul p est appelé **une** période de ℓ .

On note $\mathcal{L}(\mathcal{A})$ l'ensemble des mots périodiques sur l'alphabet $\mathcal{A}$: $\mathcal{L}(\mathcal{A}) = \{\ell \in \mathcal{A}^{\mathbb{N}} \mid \exists p \in \mathbb{N}^* : \forall i \in \mathbb{N}, \ell_{i+p} = \ell_i\}$.

Pour tout $n \in \mathbb{N}^*$, $\mathcal{L}_n(\mathcal{A})$ désigne l'ensemble des mots périodiques sur l'alphabet $\mathcal{A}$ dont n est une période

$$\mathcal{L}_n(\mathcal{A}) = \{\ell \in \mathcal{A}^{\mathbb{N}} \mid \forall i \in \mathbb{N}, \ell_{i+n} = \ell_i\}.$$

On note $c : \begin{array}{l} \mathcal{A}^{\mathbb{N}} \rightarrow \mathcal{A}^{\mathbb{N}} \\ \ell \mapsto \ell' \end{array}$ où pour tout $i \in \mathbb{N}$, $\ell'_i = \ell_{i+1}$.

On note $c^0 = \text{Id}_{\mathcal{A}^{\mathbb{N}}}$, pour tout $k \in \mathbb{N}^*$, $c^k = \underbrace{c \circ c \cdots \circ c}_k$ compositions.

III.1. Soit $\ell \in \mathcal{L}(\mathcal{A})$ un mot périodique fixé. Notons $\mathcal{P}(\ell)$ l'ensemble de ses périodes.

- (a) Montrer qu'il existe un unique $p(\ell) \in \mathbb{N}^*$ tel que $\mathcal{P}(\ell) = p(\ell) \cdot \mathbb{N}^*$.
On dit que $p(\ell)$ est la **période primitive** de ℓ .
- (b) Montrer que, pour tout $p \in \mathbb{N}^*$, p est une période de ℓ si et seulement si $c^p(\ell) = \ell$.
- (c) Énoncer et démontrer une condition nécessaire et suffisante exprimée avec des puissances de c pour exprimer que $p(\ell)$ est la période primitive de ℓ .
- (d) Montrer que $c(\mathcal{L}(\mathcal{A})) \subset \mathcal{L}(\mathcal{A})$ puis que c restreinte à $\mathcal{L}(\mathcal{A})$ est injective.
- (e) En déduire que $p(c(\ell)) = \ell$.

III.2. Soit $p \in \mathbb{N}^*$. On note $\mathcal{P}_p$ l'ensemble des mots périodiques dont la période primitive est p : $\mathcal{P}_p = \{\ell \in \mathcal{L}(\mathcal{A}) \mid p(\ell) = p\}$.

- On note $\sim$ la relation binaire définie sur $\mathcal{P}_p$ par : $\ell \sim \ell'$ si et seulement si $\exists k \in \mathbb{N}$ tel que $c^k(\ell) = \ell'$.
- (a) Justifier que la relation binaire est bien définie puis montrer que $\sim$ est une relation d'équivalence.

Lorsque $(\ell, \ell') \in \mathcal{P}_p^2$ vérifient $\ell \sim \ell'$, on dit que les mots ℓ et ℓ' définissent le même mot circulaire.

On note $\bar{\ell}$ la classe d'équivalence de $\ell \in \mathcal{P}_p$ pour cette relation. Une classe d'équivalence représente donc un unique mot circulaire.

- (b) Soit $\ell \in \mathcal{P}_p$. Montrer que

$$\text{card}(\bar{\ell}) = p$$

On note $(\ell^i)_{i \in M_p}$ (l'indice est placé comme un exposant car ℓ^i représente une suite, mais ce n'est qu'une notation) un système de représentant des mots circulaires de période primitive p et $M(p)$ le cardinal de l'ensemble M_p qui indexe le système de représentants, c'est-à-dire le nombre de mots circulaires.

III.3. Soit $n \in \mathbb{N}^*$ fixé.

- (a) Montrer que $\mathcal{L}_n(\mathcal{A}) = \bigsqcup_{p|n} \mathcal{P}_p$.

(b) En déduire que

$$m^n = \sum_{p|n} pM(p)$$

III.4. **Inversion de Möbius.** On rappelle la formule trouvée dans la partie précédente :

$$\text{Si pour tout } n \in \mathbb{N}^*, F(n) = \sum_{d|n} f(d), \text{ alors pour tout } n \in \mathbb{N}^*, f(n) = \sum_{d|n} \mu\left(\frac{n}{d}\right) F(d).$$

(a) Montrer que $pM(p) = \sum_{q|p} \mu\left(\frac{p}{q}\right) m^q$.

(b) Montrer que si p est un nombre premier, $M(p) = \frac{m}{p}(m^{p-1} - 1)$.

En déduire le petit théorème de Fermat.

(c) Montrer que, pour tout $n \in \mathbb{N}^*$, le nombre total de mots circulaires de $\mathcal{L}_n(\mathcal{A})$ pour un alphabet $\mathcal{A}$ de m lettres est

$$S_n = \sum_{p|n} \frac{1}{p} \sum_{q|p} \mu\left(\frac{p}{q}\right) m^q$$

III.5. **Application au calcul de traces des puissances d'une somme de matrices.**

Soit n un entiers naturel non nul.

La trace d'une matrice $M \in \mathcal{M}_n(\mathbb{Z})$ est le réel noté $\text{Tr}(M)$ qui correspond à la somme des éléments diagonaux de M :

$$\text{Tr}(M) = \sum_{i=1}^n [M]_{i,i}$$

On admet dans cette question, le résultat qui fait l'objet de la question IV.1(a) :

$$\forall (M, N) \in \mathcal{M}_n(\mathbb{Z})^2, \text{Tr}(M + N) = \text{Tr}(M) + \text{Tr}(N) \quad \text{et} \quad \text{Tr}(MN) = \text{Tr}(NM).$$

On considère m matrices $(A_1, A_2, \dots, A_m) \in \mathcal{M}_n(\mathbb{Z})^m$ et l'on cherche à simplifier $\text{Tr}((A_1 + A_2 + \dots + A_m)^k)$ pour $k \in \mathbb{N}^*$.

(a) Montrer que $\text{Tr}((A_1 + A_2 + \dots + A_m)^k) = \sum_{\ell \in \mathcal{L}_k(\{1, 2, \dots, m\})} \text{Tr}(A_{\ell_0} A_{\ell_1} \dots A_{\ell_{k-1}})$

(b) En déduire que

$$\text{Tr}((A_1 + A_2 + \dots + A_m)^k) = \sum_{p|k} \left(\sum_{i \in M_p} p \text{Tr}((A_{\ell_0}^{i_0} A_{\ell_1}^{i_1} \dots A_{\ell_{p-1}}^{i_{p-1}})^{\frac{k}{p}}) \right) \quad (1)$$

IV . Généralisation du petit théorème de Fermat

Soit $n \in \mathbb{N}$. Les matrices considérées dans cette partie sont à coefficients dans l'anneau $\mathbb{Z}$.

Considérons également p un nombre premier.

IV.1. Soient $(B, C) \in \mathcal{M}_n(\mathbb{Z})^2$. Le but de cette question est d'établir la relation

$$\text{Tr}((B + C)^p) \equiv \text{Tr}(B^p) + \text{Tr}(C^p) \pmod{p} \quad (2)$$

(a) Montrer que, pour tout $(M, N) \in \mathcal{M}_n(\mathbb{Z})^2$, $\text{Tr}(M + N) = \text{Tr}(M) + \text{Tr}(N)$ et $\text{Tr}(MN) = \text{Tr}(NM)$.

(b) Établir par un calcul explicite les relations (5) pour $p = 2$ et $p = 3$.

(c) En reprenant la formule (4) démontrée en fin de partie précédente, prouver la relation (5) en toute généralité.

IV.2. **Petit théorème de Fermat matriciel.**

Soit $A \in \mathcal{M}_n(\mathbb{Z})$.

(a) Montrer, en raisonnant par analyse-synthèse, qu'il existe un unique couple $(B, C) \in \mathcal{M}_n(\mathbb{Z})^2$ tel que B est triangulaire inférieure, C est triangulaire supérieure à diagonale nulle et $A = B + C$.

On exprimera, pour tout $(i, j) \in \llbracket 1, n \rrbracket^2$, $[B]_{i,j}$ et $[C]_{i,j}$ en fonction de $[A]_{i,j}$.

(b) Calculer explicitement, par exemple par récurrence, pour tout $i \in \llbracket 1, n \rrbracket$, pour tout $k \in \mathbb{N}^*$, $[C^k]_{i,i}$ et $[B^k]_{i,i}$ en fonction de k et des coefficients de A .

(c) En exploitant la question IV.1 précédente, montrer que $\text{Tr}(A^p) = \text{Tr}(A) \pmod{p}$.

(d) **Application à une suite récurrente.** En reprenant le résultat de la question I.4(b), établir une nouvelle preuve du fait que, pour tout nombre premier $p : p|u_p$ (cette fois sans passer par le calcul explicite de u_n en fonction de n).

DEVOIR SURVEILLE 5 - Correction

PROBLÈME - PETIT THÉORÈME DE FERMAT GÉNÉRALISÉ AU CALCUL MATRICIEL

I . Étude d'une suite récurrente linéaire via un calcul matriciel

Lien avec une suite récurrente . . .

On considère dans cette partie une matrice

$$A = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ -6 & 7 & 0 \end{pmatrix}$$

I.1. Montrer, à l'aide d'un algorithme de Gauss, que A est inversible et calculer A^{-1} .

Par suites d'opérations élémentaires sur les lignes appliquées à la matrice par blocs ($A I_3$) :

$$\begin{pmatrix} 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 \\ -6 & 7 & 0 & 0 & 0 & 1 \end{pmatrix} \xrightarrow{\substack{L_1 \leftarrow -\frac{1}{6}L_3 \\ L_2 \leftarrow L_1 \\ L_3 \leftarrow L_2}} \begin{pmatrix} 1 & \frac{-7}{6} & 0 & 0 & 0 & \frac{-1}{6} \\ 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 \end{pmatrix} \xrightarrow{L_1 \leftarrow L_1 + \frac{7}{6}L_2} \begin{pmatrix} 1 & 0 & 0 & \frac{7}{6} & 0 & \frac{-1}{6} \\ 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 \end{pmatrix}$$

Par suite d'opérations élémentaires, on a transformé A en I_3 , donc A est inversible.

Par suite des mêmes opérations élémentaires, on transforme I_3 , en A^{-1} .

$$\text{Donc } A \text{ est inversible et } A^{-1} = \begin{pmatrix} \frac{7}{6} & 0 & \frac{-1}{6} \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} = \frac{1}{6} \begin{pmatrix} 7 & 0 & -1 \\ 6 & 0 & 0 \\ 0 & 6 & 0 \end{pmatrix}.$$

I.2. Montrer que $A^3 = 7A - 6I_3$. On notera $\Pi = X^3 - 7X + 6$

Les calculs donnent $A^2 = \begin{pmatrix} 0 & 0 & 1 \\ -6 & 7 & 0 \\ 0 & -6 & 7 \end{pmatrix}$ puis $A^3 = \begin{pmatrix} -6 & 7 & 0 \\ 0 & -6 & 7 \\ -42 & 49 & -6 \end{pmatrix}$.

Donc

$$A^3 - 7A + 6I_3 = \begin{pmatrix} -6 & 7 & 0 \\ 0 & -6 & 7 \\ -42 & 49 & -6 \end{pmatrix} - 7 \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ -6 & 7 & 0 \end{pmatrix} + 6 \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} -6+0+6 & 7-7 & 0 \\ 0 & -6-0+6 & 7-7 \\ -42+42 & 49-49 & -6+6 \end{pmatrix} = 0_{3 \times 3}$$

$$\text{On a donc bien } A^3 = 7A - 6I_3 \text{ ou encore } \Pi(A) = 0.$$

On admet que pour tout $n \in \mathbb{N}$, $\exists ! (Q_n, R_n) \in (\mathbb{R}[X])^2$ tel que $X^n = Q_n \times \Pi + R_n$ avec $\deg R_n < 3$.

(a) Montrer qu'il existe $(a_n, b_n, c_n) \in \mathbb{R}^3$ tel que pour tout $x \in \mathbb{R}$,

$$x^n = Q_n(x) \times \Pi(x) + (a_n x^2 + b_n x + c_n)$$

Puisque $\deg R_n < 3$, R_n est de la forme $aX^2 + bX + c$.

Tenant compte de la dépendance en n , on peut écrire :

$$\forall n \in \mathbb{N}, \quad \exists Q_n \in \mathbb{R}[X], (a_n, b_n, c_n) \in \mathbb{R}^3 \text{ tels que } X^n = Q_n \times \Pi + (a_n X^2 + b_n X + c_n)$$

Ce résultat calculatoire dans un anneau s'interprète

aussi bien dans l'anneau $\mathcal{M}_n(\mathbb{R})$ avec A à la place de X ;

que dans l'anneau (corps) $\mathbb{R}$ avec n'importe quel réel x à la place de X :

$$\forall n \in \mathbb{N}, \quad \exists Q_n \in \mathbb{R}[X], (a_n, b_n, c_n) \in \mathbb{R}^3 \text{ tels que } x^n = Q_n \times \Pi + (a_n x^2 + b_n x + c_n)$$

(b) En exploitant les racines de Π , donner un système de trois équations à trois inconnues dont l'unique solution est le triplet (a_n, b_n, c_n) .

1 est racine (évidente) de Π , on peut donc factoriser $\Pi(x)$ par $(x-1)$: $\Pi(x) = x^3 - 7x + 6 = (x-1)(x^2 + x - 6)$ 2 est racine (un peu moins évidente) de $x^2 + x - 6$, on peut donc factoriser $\Pi(x)$ par $(x-2)$: $\Pi(x) = (x-1)(x-2)(x+3)$ On a alors, puisque la relation est vraie en tout x , en prenant successivement $x \leftarrow 1$, $x \leftarrow 2$ et $x \leftarrow -3$:

$$\begin{cases} 1^n = Q_n(1) \times \Pi(1) + (a_n 1^2 + b_n 1 + c_n) \\ 2^n = Q_n(2) \times \Pi(2) + (a_n 2^2 + b_n 2 + c_n) \\ (-3)^n = Q_n(-3) \times \Pi(-3) + (a_n (-3)^2 + b_n (-3) + c_n) \end{cases}$$

Et comme $\Pi(1) = \Pi(2) = \Pi(-3) = 0$, on trouve que (a_n, b_n, c_n) est la solutions du système

$$\begin{cases} x & +y & +z & = & 1 \\ 4x & +2y & +z & = & 2^n \\ 9x & -3y & +z & = & (-3)^n \end{cases}$$

(c) Montrer que la matrice $\frac{1}{20} \begin{pmatrix} -5 & 4 & 1 \\ -5 & 8 & -3 \\ 30 & -12 & 2 \end{pmatrix}$ est l'inverse de la matrice associé au système de la question précédente.

En déduire, pour tout $n \in \mathbb{N}$, une expression de A^n en fonction A^2 , A et I_3 .

On note M_2 la matrice donnée dans la question et M_1 la matrice associé au système précédent.

C'est-à-dire : $M_1 = \begin{pmatrix} 1 & 1 & 1 \\ 4 & 2 & 1 \\ 9 & -3 & 1 \end{pmatrix}$.

On vérifie :

$$M_1 \times M_2 = \frac{1}{20} \begin{pmatrix} 1 & 1 & 1 \\ 4 & 2 & 1 \\ 9 & -3 & 1 \end{pmatrix} \times \begin{pmatrix} -5 & 4 & 1 \\ -5 & 8 & -3 \\ 30 & -12 & 2 \end{pmatrix} = \frac{1}{20} \begin{pmatrix} 20 & 0 & 0 \\ 0 & 20 & 0 \\ 0 & 0 & 20 \end{pmatrix} = I_3$$

L'inversibilité à droite est suffisante : M_1 est inverse est inversible et $M_1^{-1} = M_2$.

On a l'équivalence :

$$M_1 \times \begin{pmatrix} a_n \\ b_n \\ c_n \end{pmatrix} = \begin{pmatrix} 1 \\ 2^n \\ (-3)^n \end{pmatrix} \iff \begin{pmatrix} a_n \\ b_n \\ c_n \end{pmatrix} = M_2 \times \begin{pmatrix} 1 \\ 2^n \\ (-3)^n \end{pmatrix}$$

Cela donne donc

Donc

$$\begin{cases} a_n & = & \frac{(-3)^n + 2^{n+2} - 5}{20} \\ b_n & = & \frac{(-3)^{n+1} + 2^{n+3} - 5}{20} \\ c_n & = & \frac{2(-3)^n - 3 \times 2^{n+2} + 30}{20} \end{cases}$$

Par ailleurs, nous avons vu en question 2.(a) que la relation polynomiale s'interprète également en la matrice A

$$A^n = Q_n(A) \times \Pi(A) + (a_n A^2 + b_n A + c_n I_3)$$

Or $\Pi(A) = 0$, donc $A^n = a_n A^2 + b_n A + c_n I_3$.

$$\forall n \in \mathbb{N}, \quad A^n = \frac{1}{20} [((-3)^n + 2^{n+2} - 5)A^2 + ((-3)^{n+1} + 2^{n+3} - 5)A + (2(-3)^n - 3 \times 2^{n+2} + 30)I_3]$$

(d) L'égalité obtenue dans la question I.2(c) est-elle encore vraie pour $n = -1$?

Pour $n = -1$, on a trouve

$$- 20a_{-1} = \frac{-1}{3} + 2 - 5 = \frac{-10}{3}, \text{ donc } a_{-1} = \frac{-1}{6}.$$

$$- 20b_{-1} = 1 + 4 - 5 = 0, \text{ donc } b_{-1} = 0.$$

$$- 20c_{-1} = \frac{-2}{3} - 6 + 30 = \frac{70}{3}, \text{ donc } c_{-1} = \frac{7}{6}.$$

Puis

$$\frac{-1}{6}A^2 + 0A + \frac{7}{6}I_3 = \begin{pmatrix} \frac{7}{6} & 0 & \frac{-1}{6} \\ 1 & \frac{-7}{6} + \frac{7}{6} & 0 \\ 0 & 1 & \frac{-7}{6} + \frac{7}{6} \end{pmatrix} = \begin{pmatrix} \frac{7}{6} & 0 & \frac{-1}{6} \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} = A^{-1}$$

Ainsi, la relation trouvée à la question précédente est également vraie pour $n = -1$.

On notera également que, puisque $A^3 - 7A + 6I_3 = 0$, on a : $(A^2 - 7I_3) \times A = A \times (A^2 - 7I_3) = -6I_3$, et donc $A^{-1} = \frac{1}{6}(7I_3 - A^2)$.

I.3. On considère la suite récurrente (u_n) définie par :

$$u_0 = 3, u_1 = 0, u_2 = 14 \quad \text{et } \forall n \in \mathbb{N}, u_{n+3} = 7u_{n+1} - 6u_n$$

- (a) Donner les valeurs de (u_n) pour $n \in \llbracket 1, 7 \rrbracket$.
On vérifiera qu'on trouve $u_7 = 882$.

On trouve successivement :

n	0	1	2	3	4	5	6	7
u_n	3	0	14	-18	98	210	794	882

- (b) Que pensez-vous de l'ensemble $\{n \in \llbracket 1, 7 \rrbracket \text{ tel que } n|u_n\}$?

1|0, 2|14, 3|-18, 4|98, 5|210, 6|794 et 7|882 (= 7 × 126).

Donc $\{n \in \llbracket 1, 7 \rrbracket \text{ tel que } n|u_n\} = \{1, 2, 3, 5, 7\}$, ce ne sont que des nombres premiers « comme par hasard ».

- (c) On note pour tout $n \in \mathbb{N}$, $U_n = \begin{pmatrix} u_n \\ u_{n+1} \\ u_{n+2} \end{pmatrix}$.

Pour tout entier $n \in \mathbb{N}$, exprimer U_{n+1} en fonction de A et de U_n .

Soit $n \in \mathbb{N}$,

$$A \times U_n = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ -6 & 7 & 0 \end{pmatrix} \times \begin{pmatrix} u_n \\ u_{n+1} \\ u_{n+2} \end{pmatrix} = \begin{pmatrix} u_{n+1} \\ u_{n+2} \\ -6u_n + 7u_{n+1} \end{pmatrix} = \begin{pmatrix} u_{n+1} \\ u_{n+2} \\ u_{n+3} \end{pmatrix} = U_{n+1}$$

$$\forall n \in \mathbb{N}, \quad U_{n+1} = A \times U_n$$

- (d) En déduire une expression explicite de U_n , en fonction de A et U_0 .

Notons, pour tout $n \in \mathbb{N}$, $\mathcal{P}_n$: « $U_n = A^n \times U_0$. »

— $A^0 = I_3$, et donc $\mathcal{P}_0$ est vraie.

— Soit $n \in \mathbb{N}$. Supposons que $\mathcal{P}_n$ est vraie. D'après la réponse précédente : $U_{n+1} = A \times U_n = A \times A^n \times U_0$, d'après $\mathcal{P}_n$.

Puis par associativité des produits matriciels : $U_{n+1} = A^{n+1}U_0$.

Ainsi $\mathcal{P}_{n+1}$ est vraie.

$$\forall n \in \mathbb{N}, \quad U_n = A^n \times U_0$$

- (e) En déduire une expression explicite de u_n en fonction de n , pour tout entier $n \in \mathbb{N}$.

On sait que $U_0 = \begin{pmatrix} u_0 \\ u_1 \\ u_2 \end{pmatrix} = \begin{pmatrix} 3 \\ 0 \\ 14 \end{pmatrix}$, donc

$$u_n = [U_n]_1 = [A^n \times U_0]_1 = 3[A^n]_{1,1} + 14[A^n]_{1,3}$$

Puis on reprend l'expression (horrible) de la question 2.(c) : $A^n = a_n A^2 + b_n A + c_n I_3$.

Et par linéarité de $[\cdot]_{i,j}$, on trouve

$$[A^n]_{1,1} = a_n [A^2]_{1,1} + b_n [A]_{1,1} + c_n [I_3]_{1,1} = 0 + 0 + c_n = c_n$$

$$[A^n]_{1,3} = a_n [A^2]_{1,3} + b_n [A]_{1,3} + c_n [I_3]_{1,3} = a_n + 0 + 0 = a_n$$

Donc

$$u_n = 14a_n + 3c_n = \frac{1}{20} [((-3)^n + 2^{n+2} - 5) \times 14 + (2(-3)^n - 3 \times 2^{n+2} + 30) \times 3]$$

$$u_n = \frac{1}{20} (20(-3)^n + 5 \times (2)^{n+2} + 20) = 1 + 2^n + (-3)^n$$

- (f) Démontrer que, pour tout p premier, $p|u_p$.

Soit p un nombre premier. $u_p = 1 + 2^p + (-3)^p$.

Le petit théorème de Fermat donne

$$u_p \equiv 1 + 2 + (-3) = 0 \quad [p]$$

Donc

$$\text{Pour tout } p \text{ premier, } p|u_p.$$

I.4. (a) En utilisant l'expression polynomiale s'annulant en A , montrer que la suite $(\text{Tr}(A^n))_{n \in \mathbb{N}}$ satisfait la même relation de récurrence que u .

(b) En déduire que, pour tout $n \in \mathbb{N}$, $u_n = \text{Tr}(A^n)$.

Ce résultat permettra dans la partie IV, de redémontrer, sans calcul ou presque, le résultat de la question I.3(f).

Pour tout $n \in \mathbb{N}$, en exploitant la linéarité de la trace (que l'on démontre plus loin...)

$$\text{Tr}(A^{n+3}) = \text{Tr}(A^n \times A^3) = \text{Tr}(A^n(7A - 6I_3)) = \text{Tr}(7A^{n+1} - 6A^n) = 7\text{Tr}(A^{n+1}) - 6\text{Tr}(A^n) = 7u_{n+1} - 6u_n$$

Donc la suite $(\text{Tr}(A^n))_{n \in \mathbb{N}}$ satisfait la même relation de récurrence que u .

Puis, pour conclure, on démontre le résultat par récurrence.

Posons, pour tout $n \in \mathbb{N}$ (dont 0!), $\mathcal{P}_n$: « $u_n = \text{Tr}(A^n)$ ».

— $u_0 = 3 = \text{Tr}(I_3) = \text{Tr}(A^0)$, donc $\mathcal{P}_0$ est vraie.

$u_1 = 0 = \text{Tr}(A^1)$, donc $\mathcal{P}_1$ est vraie.

$$u_2 = 14\text{Tr} \begin{pmatrix} 0 & 0 & 1 \\ -6 & 7 & 0 \\ 0 & -6 & 7 \end{pmatrix} = \text{Tr}(A^2), \text{ donc } \mathcal{P}_2 \text{ est vraie.}$$

— Soit $n \in \mathbb{N}$. Supposons que $\mathcal{P}_n$, $\mathcal{P}_{n+1}$ et $\mathcal{P}_{n+2}$ sont vraies.

En exploitant $\mathcal{P}_n$ et $\mathcal{P}_{n+1}$, d'après la relation démontrée précédemment :

$$\text{Tr}(A^{n+3}) = 7\text{Tr}(A^{n+1}) - 6\text{Tr}(A^n) = 7u_{n+1} - 6u_n$$

Or par définition de la suite (u_n) : $7u_{n+1} - 6u_n = u_{n+3}$. Donc $\mathcal{P}_{n+3}$ est vraie.

$$\forall n \in \mathbb{N}, \quad u_n = \text{Tr}(A^n)$$

(c) Retrouver ainsi l'expression de u_n en fonction de a_n et c_n obtenue dans la question I.3(e) (dont cette question propose une deuxième preuve).

On a vu que $A^n = a_n A^2 + b_n A + c_n I_3$.

Donc, en prenant la trace (toujours par linéarité) :

$$u_n = \text{Tr}(A^n) = a_n \text{Tr}(A^2) + b_n \text{Tr}(A) + c_n \text{Tr}(I_3) = 14a_n + 0b_n + 3c_n$$

C'est bien un calcul vu plus haut.

II . Formule d'inversion de Möbius

Pour $n \in \mathbb{N}^*$, on note $\mathcal{D}_n$ l'ensemble des nombres entiers naturels (donc > 0) divisant n et on écrit $\sum_{d|n} \dots = \sum_{d \in \mathcal{D}_n} \dots$ la somme sur

tous les nombres entiers naturels d divisant n .

Une fonction arithmétique est une fonction $f : \mathbb{N}^* \rightarrow \mathbb{C}$. L'ensemble des fonctions arithmétiques est noté $\mathbb{A}$.

On dit qu'une fonction arithmétique $f \in \mathbb{A}$ est multiplicative si

$$\begin{cases} f(1) \neq 0 \\ \forall (m, n) \in (\mathbb{N}^*)^2, m \wedge n = 1 \Rightarrow f(mn) = f(m)f(n) \end{cases}$$

On note $\mathbb{M}$ l'ensemble des fonctions arithmétiques multiplicatives.

$$\text{On note } \mathbf{1} : \begin{cases} \mathbb{N}^* & \rightarrow & \mathbb{C} \\ n & \mapsto & 1 \end{cases} \text{ et } \delta : \begin{cases} \mathbb{N}^* & \rightarrow & \mathbb{C} \\ n & \mapsto & \begin{cases} 1 & \text{si } n = 1 \\ 0 & \text{sinon} \end{cases} \end{cases} .$$

Si f et g sont deux fonctions arithmétiques, le produit de convolution de f et g est la fonction arithmétique $f * g$ définie par

$$\forall n \in \mathbb{N}^*, \quad (f * g)(n) = \sum_{d|n} f(d)g\left(\frac{n}{d}\right)$$

Par exemple $(f * g)(12) = \sum_{d|12} f(d)g\left(\frac{12}{d}\right) = f(1)g(12) + f(2)g(6) + f(3)g(4) + f(4)g(3) + f(6)g(2) + f(12)g(1)$.

On notera que l'on a : $\forall n \in \mathbb{N}^*, (f * g)(n) = \sum_{d|n} f(d)g\left(\frac{n}{d}\right) = \sum_{d_1 d_2 = n} f(d_1)g(d_2) = \sum_{d|n} f\left(\frac{n}{d}\right)g(d)$

II.1. Montrer que $\mathbf{1}$ et δ sont des fonctions arithmétiques multiplicatives.

★ $\mathbf{1}$ et δ sont des fonctions arithmétiques car définies de $\mathbb{N}^*$ dans $\mathbb{C}$.

★ $\mathbf{1}(1) = 1 \neq 0$ et $\delta(1) = 1 \neq 0$.

★ Soient $(m, n) \in \mathbb{N}^{*2}$ tels que $m \wedge n = 1$. D'une part

$$\mathbf{1}(mn) = 1 = 1 \times 1 = \mathbf{1}(m) \times \mathbf{1}(n)$$

et d'autre part,

— si $m = n = 1$, alors $\delta(mn) = \delta(1) = 1 = 1 \times 1 = \delta(m)\delta(n)$,

— sinon, $m \geq 2$ ou $n \geq 2$, donc $mn \neq 1$ d'où $\delta(mn) = 0$, et puisque l'un des deux entiers au moins est différent de 1, $\delta(m) \times \delta(n) = 0$ (car l'un des terme du produit est nul) donc $\delta(mn) = \delta(m)\delta(n)$.

Ainsi, $\mathbf{1}$ et δ sont des fonctions arithmétiques multiplicatives.

II.2. Structure de $\mathbb{A}$.

(a) Montrer que $(\mathbb{A}, +)$ est un groupe abélien.

Une fonction arithmétique est en fait une suite de complexes.

Nous avons vu dans le cours que l'ensemble des suites numériques à valeurs complexes est un groupe (et plus...) commutatif.
— $+$ est une loi de composition interne : $\forall (f, g) \in \mathbb{A}^2$ alors $f + g \in \mathbb{A}$ ce qui est immédiat par définition de la somme de deux suites.

— $+$ est une loi commutative : soient $(f, g) \in \mathbb{A}^2$,

$$\forall n \in \mathbb{N}^*, (f + g)(n) = \underbrace{f(n) + g(n) = g(n) + f(n)}_{\text{commutativité de } + \text{ dans } \mathbb{C}} = (g + f)(n)$$

donc $f + g = g + f$.

— $+$ est une loi associative : soient $(f, g, h) \in \mathbb{A}^2$,

$$\forall n \in \mathbb{N}^*, ((f + g) + h)(n) = \underbrace{(f + g)(n) + h(n) = f(n) + g(n) + h(n) = f(n) + (g + h)(n)}_{\text{associativité de } + \text{ dans } \mathbb{C}} = (f + (g + h))(n)$$

donc $(f + g) + h = f + (g + h)$.

— $+$ possède un élément neutre : posons $\mathbf{0} \left| \begin{array}{l} \mathbb{N}^* \rightarrow \mathbb{C} \\ n \mapsto 0 \end{array} \right.$, soit $f \in \mathbb{A}$,

$$\forall n \in \mathbb{N}^*, (\mathbf{0} + f)(n) = \mathbf{0}(n) + f(n) = f(n)$$

donc $\mathbf{0} + f = f$ et, par commutativité de $+$, $f + \mathbf{0} = \mathbf{0} + f = f$.

— Tout élément admet un symétrique (ici un opposé) : soit $f \in \mathbb{A}$, posons $g \left| \begin{array}{l} \mathbb{N}^* \rightarrow \mathbb{C} \\ n \mapsto -f(n) \end{array} \right.$,

$$\forall n \in \mathbb{N}^*, (f + g)(n) = f(n) + g(n) = f(n) - f(n) = 0 = \mathbf{0}(n)$$

donc $f + g = \mathbf{0}$ d'où, par commutativité de $+$, $g + f = f + g = \mathbf{0}$.

Ainsi $(\mathbb{A}, +)$ est un groupe abélien.

(b) Montrer que $*$ est une loi interne commutative sur $\mathbb{A}$. On admet que $*$ est également associative.

Soient $(f, g) \in \mathbb{A}^2$. Soit $n \in \mathbb{N}^*$. L'application $\psi \left| \begin{array}{l} \mathcal{D}_n \rightarrow \mathcal{D}_n \\ d \mapsto \frac{n}{d} \end{array} \right.$ vérifie $\psi \circ \psi = \text{Id}_{\mathcal{D}_n}$, c'est une involution donc une permutation de $\mathcal{D}_n$ (c'est une bijection de $\mathcal{D}_n$ dans $\mathcal{D}_n$) si bien que si h est une fonction définie sur $\mathcal{D}_n$, $\sum_{d|n} h(d) = \sum_{d|n} h\left(\frac{n}{d}\right)$ puisque ces deux sommes contiennent les mêmes termes, il ont simplement été permutés. On en déduit que

$$(f * g)(n) = \sum_{d|n} f(d)g\left(\frac{n}{d}\right) = \sum_{d|n} f\left(\frac{n}{d}\right)g\left(\frac{n}{\frac{n}{d}}\right) = \sum_{d|n} f\left(\frac{n}{d}\right)g(d) = \sum_{d|n} g(d)f\left(\frac{n}{d}\right) = (g * f)(n)$$

donc $f * g = g * f$.

Ainsi $*$ est une loi interne commutative sur $\mathbb{A}$.

(c) Montrer que δ est l'élément neutre pour $*$.

★ Soit $f \in \mathbb{A}$ fixée. Soit $n \in \mathbb{N}^*$ fixé.

$$(\delta * f)(n) = \sum_{d|n} \delta(d)f\left(\frac{n}{d}\right) = \underbrace{\delta(1)}_{=1} f(n) + \sum_{\substack{d|n \\ d \neq 1}} \underbrace{\delta(d)}_{=0} f\left(\frac{n}{d}\right) = f(n)$$

Par conséquent, $\delta * f = f$, or $*$ est commutative donc $f * \delta = \delta * f = f$ donc δ est un élément neutre pour la loi $*$.

* Nous savons que, pour une loi associative, il y a unicité de l'élément neutre sous réserve d'existence, or ici, * est associative donc δ est le élément neutre de la loi *.

Ainsi δ est l'élément neutre pour *.

(d) Conclure que $(\mathbb{A}, +, *)$ est un anneau commutatif. Est-ce un corps ?

- $(\mathbb{A}, +)$ est un groupe abélien.
- * est une loi de composition interne sur $\mathbb{A}$.
- * est une loi associative.
- * est une loi commutative.
- * admet un élément neutre qui est δ .
- * est distributive sur + : soient $(f, g, h) \in \mathbb{A}^3$, par distributivité de $\times$ sur + dans $\mathbb{C}$,

$$\forall n \in \mathbb{N}^*, ((f+g)*h)(n) = \sum_{d|n} (f(d)+g(d))h\left(\frac{n}{d}\right) = \sum_{d|n} f(d)h\left(\frac{n}{d}\right) + \sum_{d|n} g(d)h\left(\frac{n}{d}\right) = (f*h)(n) + (g*h)(n) = (f*h+g*h)(n)$$

donc $(f+g)*h = f*h + g*h$ d'ù la distributivité à droite de * sur +. La commutativité de * permet d'en déduire la distributivité à gauche de * sur +.

Ainsi $(\mathbb{A}, +, *)$ est un anneau commutatif.

Considérons la fonction σ $\left\{ \begin{array}{l} \mathbb{N}^* \rightarrow \mathbb{C} \\ n \mapsto \begin{cases} 1 & \text{si } n = 2 \\ 0 & \text{sinon} \end{cases} \end{array} \right.$

- $\sigma \neq \mathbf{0}$ car $\sigma(2) = 1$.
- Supposons que σ est inversible dans l'anneau $\mathbb{A}$, alors il existe $f \in \mathbb{A}$ telle que $\sigma * f = \delta$ donc

$$1 = \delta(1) = (\sigma * f)(1) = \sum_{d|1} \sigma(d)f\left(\frac{1}{d}\right) = \sigma(1)f(1) = 0$$

ce qui est une contradiction. Par conséquent, σ n'est pas inversible dans $\mathbb{A}$.

Ainsi $(\mathbb{A}, +, *)$ n'est pas un corps.

II.3. Stabilité de la propriété de multiplicativité et structure de $\mathbb{M}$.

(a) Soient m et n deux entiers naturels non nuls premiers entre eux.

Montrer que $\pi : \left\{ \begin{array}{l} \mathcal{D}_m \times \mathcal{D}_n \rightarrow \mathcal{D}_{mn} \\ (d_1, d_2) \mapsto d_1 d_2 \end{array} \right.$ est bien définie (i.e. bien à valeurs dans $\mathcal{D}_{mn}$) et réalise une bijection de $\mathcal{D}_m \times \mathcal{D}_n$ sur $\mathcal{D}_{mn}$.

De plus, si $(d_1, d_2) \in \mathcal{D}_m \times \mathcal{D}_n$, calculer $d_1 \wedge d_2$.

* Soient $(d_1, d_2) \in \mathcal{D}_m \times \mathcal{D}_n$.

Alors, $\left\{ \begin{array}{l} d_1 | m \\ d_2 | n \end{array} \right.$ donc il existe (d'_1, d'_2) tels que $\left\{ \begin{array}{l} d_1 d'_1 = m \\ d_2 d'_2 = n \end{array} \right.$ donc $d_1 d_2 d'_1 d'_2 = mn$ donc $d_1 d_2 | mn$ donc $d_1 d_2 \in \mathcal{D}_{mn}$ ce qui prouve que l'application π est bien définie.

* Soient $((d_1, d_2), (d'_1, d'_2)) \in (\mathcal{D}_m \times \mathcal{D}_n)^2$ fixés tels que $\pi(d_1, d_2) = \pi(d'_1, d'_2)$.

Alors $d_1 d_2 = d'_1 d'_2$.

Soit p un nombre premier fixé quelconque.

Les conditions $d_1 | m$ et $d'_1 | m$ imposent $\left\{ \begin{array}{l} 0 \leq \nu_p(d_1) \leq \nu_p(m) \\ 0 \leq \nu_p(d'_1) \leq \nu_p(m) \end{array} \right.$

— Si $\nu_p(m) = 0$, alors les encadrements ci-dessus imposent $\nu_p(d_1) = 0 = \nu_p(d'_1)$.

— Sinon, $\nu_p(m) > 0$, en prenant l'image de $d_1 d_2 = d'_1 d'_2$ par la valuation p -adique et en utilisant sa propriété de morphisme,

$$\nu_p(d_1) + \nu_p(d_2) = \nu_p(d'_1) + \nu_p(d'_2) \tag{3}$$

L'hypothèse $m \wedge n = 1$ implique $\nu_p(d_2) = \nu_p(d'_2) = 0$ (sinon p serait un facteur commun à m et d_2 ou d'_2 donc à m et n contredisant le fait que m et n sont premiers) donc l'égalité (3) devient

$$\nu_p(d_1) = \nu_p(d'_1)$$

Ainsi, d_1 et d'_1 ont les mêmes valuation p -adiques pour tout p premier, or ce sont des entiers naturels non nuls donc $d_1 = d'_1$.

En échangeant les rôles de d_1, d'_1, m avec ceux de d_2, d'_2 et n , on établit de même que $d_2 = d'_2$.

Ainsi, $(d_1, d_2) = (d'_1, d'_2)$ donc π est injective.

* Soit $d \in \mathcal{D}_{mn}$ fixé.

Notons $\mathcal{P}_m$ et $\mathcal{P}_n$ les ensembles de facteurs premiers apparaissant respectivement dans les décompositions en facteurs premiers de m et n de sorte que $m = \prod_{p \in \mathcal{P}_m} p^{\nu_p(m)}$ et $n = \prod_{p \in \mathcal{P}_n} p^{\nu_p(n)}$.

$d \in \mathcal{D}_{mn}$ donc $d|mn$ donc les facteurs premiers apparaissant dans la décomposition de d sont aussi des facteurs de m ou n si bien que $d = \prod_{p \in \mathcal{P}_m \cup \mathcal{P}_n} p^{\nu_p(d)}$. De plus, par hypothèse, m et n étant premiers entre eux, $\mathcal{P}_m \cap \mathcal{P}_n = \emptyset$ donc

$$d = \prod_{p \in \mathcal{P}_m \cup \mathcal{P}_n} p^{\nu_p(d)} = \left(\prod_{p \in \mathcal{P}_m} p^{\nu_p(d)} \right) \left(\prod_{p \in \mathcal{P}_n} p^{\nu_p(d)} \right)$$

Posons $d_1 = \prod_{p \in \mathcal{P}_m} p^{\nu_p(d)}$ et $d_2 = \prod_{p \in \mathcal{P}_n} p^{\nu_p(d)}$.

— La caractérisation de la divisibilité par les valuations p -adiques donne, pour tout $p \in \mathcal{P}_m \cup \mathcal{P}_n$, puisque $d|mn$,
 $\nu_p(d) \leq \nu_p(m) + \nu_p(n) = \begin{cases} \nu_p(m) & \text{si } p \in \mathcal{P}_m \text{ car alors } p \notin \mathcal{P}_n \text{ donc } \nu_p(n) = 0, \\ \nu_p(n) & \text{si } p \in \mathcal{P}_n \text{ car alors } p \notin \mathcal{P}_m \text{ donc } \nu_p(m) = 0. \end{cases}$

On en déduit que

$$\begin{aligned} \forall p \in \mathcal{P}_m, \nu_p(d_1) = \nu_p(d) \leq \nu_p(m) \text{ donc } d_1|m \text{ donc } d_1 \in \mathcal{D}_m \\ \forall p \in \mathcal{P}_n, \nu_p(d_2) = \nu_p(d) \leq \nu_p(n) \text{ donc } d_2|n \text{ donc } d_2 \in \mathcal{D}_n \end{aligned}$$

Par conséquent, $(d_1, d_2) \in \mathcal{D}_m \times \mathcal{D}_n$.

— Le calcul direct donne

$$\pi(d_1, d_2) = d_1 d_2 = \left(\prod_{p \in \mathcal{P}_m} p^{\nu_p(d)} \right) \left(\prod_{p \in \mathcal{P}_n} p^{\nu_p(d)} \right) = d$$

Ainsi, π est surjective.

Ainsi, π réalise une bijection de $\mathcal{D}_m \times \mathcal{D}_n$ sur $\mathcal{D}_{mn}$.

De plus, pour tout $(d_1, d_2) \in \mathcal{D}_m \times \mathcal{D}_n$, les facteurs premiers de d_1 appartiennent à $\mathcal{D}_m$ (car $d_1|m$) et ceux de d_2 appartiennent à $\mathcal{D}_n$ (car $d_2|n$), or $\mathcal{P}_m \cap \mathcal{P}_n = \emptyset$ donc $d_1 \wedge d_2 = \prod_{p \in \mathcal{D}_m \cup \mathcal{D}_n} p^{\min(\nu_p(d_1), \nu_p(d_2))} = \prod_{p \in \mathcal{D}_m \cup \mathcal{D}_n} p^0 = 1$.

Ainsi, pour tout $(d_1, d_2) \in \mathcal{D}_m \times \mathcal{D}_n$, $d_1 \wedge d_2 = 1$.

(b) En déduire que si f et g sont multiplicatives, alors $f * g$ est multiplicative.

* $(f * g)(1) = \sum_{d|1} f(d)g\left(\frac{1}{d}\right) = f(1)g(1) \neq 0$ car $f(1) \neq 0$ et $g(1) \neq 0$ (puisque f et g sont multiplicatives).

* Soient $(m, n) \in \mathbb{N}^{*2}$ fixés tels que $m \wedge n = 1$. En utilisant la bijection π pour paramétrer les diviseurs de (m, n) par le produit cartésien $\mathcal{D}_m \times \mathcal{D}_n$, on obtient

$$(f * g)(mn) = \sum_{d \in \mathcal{D}_{mn}} f(d)g\left(\frac{mn}{d}\right) \stackrel{d = \pi(d_1, d_2)}{=} = \sum_{(d_1, d_2) \in \mathcal{D}_m \times \mathcal{D}_n} f(\pi(d_1, d_2))g\left(\frac{mn}{\pi(d_1, d_2)}\right) = \sum_{(d_1, d_2) \in \mathcal{D}_m \times \mathcal{D}_n} f(d_1 d_2)g\left(\frac{mn}{d_1 d_2}\right)$$

On nous avons établi dans la question précédente que, pour tout $(d_1, d_2) \in \mathcal{D}_m \times \mathcal{D}_n$, $d_1 \wedge d_2 = 1$ donc par multiplicativité de f ,

$$f(d_1 d_2) = f(d_1) f(d_2)$$

De même, $\frac{mn}{d_1 d_2} = \frac{m}{d_1} \times \frac{n}{d_2}$ avec $\left(\frac{m}{d_1}, \frac{n}{d_2}\right) \in \mathcal{D}_m \times \mathcal{D}_n$ si bien que le résultat de la question précédente s'applique pour $(d_1, d_2) \leftarrow \left(\frac{m}{d_1}, \frac{n}{d_2}\right)$ et permet d'affirmer que $\frac{m}{d_1} \wedge \frac{n}{d_2} = 1$ donc par multiplicativité de g ,

$$g\left(\frac{mn}{d_1 d_2}\right) = g\left(\frac{m}{d_1}\right) g\left(\frac{n}{d_2}\right)$$

En injectant dans le calcul de $(f * g)(mn)$,

$$\begin{aligned} (f * g)(mn) &= \sum_{(d_1, d_2) \in \mathcal{D}_m \times \mathcal{D}_n} f(d_1) f(d_2) g\left(\frac{m}{d_1}\right) g\left(\frac{n}{d_2}\right) = \sum_{d_1 \in \mathcal{D}_m} \left[f(d_1) g\left(\frac{m}{d_1}\right) \underbrace{\sum_{d_2 \in \mathcal{D}_n} f(d_2) g\left(\frac{n}{d_2}\right)}_{=(f * g)(n)} \right] \\ &= (f * g)(n) \underbrace{\sum_{d_1 \in \mathcal{D}_m} f(d_1) g\left(\frac{m}{d_1}\right)}_{=(f * g)(m)} \\ &= (f * g)(m) \times (f * g)(n) \end{aligned}$$

Ainsi, si f et g sont multiplicatives, alors $f * g$ est multiplicative.

- (c) i. Montrer que, si f est une fonction arithmétique multiplicative, alors $f(1) = 1$.

Appliquons la définition d'une fonction multiplicative pour $(m, n) \leftarrow (1, 1)$ ce qui est autorisé car $1 \wedge 1 = 1$ si bien que $f(1) = f(1 \times 1) = f(1) \times f(1) = f(1)^2$, or $f(1) \neq 0$ (par définition d'une fonction multiplicative) donc $1 = f(1)$.

Ainsi, si f est une fonction arithmétique multiplicative, alors $f(1) = 1$.

- ii. Soient f et g deux fonctions arithmétiques multiplicatives telles que, pour tout nombre premier p , pour tout $k \in \mathbb{N}^*$, $f(p^k) = g(p^k)$. Montrer que $f = g$.
-

Soit $n \in \mathbb{N}^*$ fixé.

★ Si $n = 1$, alors, f et g étant multiplicatives, le résultat de la question précédente donne $f(1) = 1$ et $g(1) = 1$ donc $f(1) = g(1)$.

★ Sinon, $n \geq 2$ donc n admet une décomposition en produits de facteurs premiers deux à deux distincts que l'on note

$$p_1, \dots, p_q \text{ avec leurs multiplicités respectives } (\alpha_1, \dots, \alpha_q) \in \mathbb{N}^{*q} : n = \prod_{i=1}^q p_i^{\alpha_i}.$$

$$p_1^{\alpha_1} \wedge \left(\prod_{i=2}^q p_i^{\alpha_i} \right) = 1 \text{ car ces deux nombres n'ont aucun facteur premier en commun d'où par multiplicativité de } f,$$

$$f(n) = f\left(p_1^{\alpha_1} \times \prod_{i=2}^q p_i^{\alpha_i}\right) = f(p_1^{\alpha_1}) \times f\left(\prod_{i=2}^q p_i^{\alpha_i}\right)$$

De même, $p_2^{\alpha_2} \wedge \left(\prod_{i=3}^q p_i^{\alpha_i}\right) = 1$ car ces deux nombres n'ont aucun facteur premier en commun d'où par multiplicativité de f ,

$$f\left(p_2^{\alpha_2} \times \prod_{i=3}^q p_i^{\alpha_i}\right) = f(p_2^{\alpha_2}) \times f\left(\prod_{i=3}^q p_i^{\alpha_i}\right)$$

En réitérant cet argument, on obtient

$$f(n) = f(p_1^{\alpha_1}) \times f\left(\prod_{i=2}^q p_i^{\alpha_i}\right) = f(p_1^{\alpha_1}) \times f(p_2^{\alpha_2}) \times f\left(\prod_{i=3}^q p_i^{\alpha_i}\right) = \dots = \prod_{i=1}^q f(p_i^{\alpha_i})$$

De plus, f et g coïncident sur les puissances des facteurs premiers donc pour tout $i \in \llbracket 1, q \rrbracket$, $f(p_i^{\alpha_i}) = g(p_i^{\alpha_i})$ d'où

$$f(n) = \prod_{i=1}^q f(p_i^{\alpha_i}) = \prod_{i=1}^q g(p_i^{\alpha_i}) = g(n) \text{ en utilisant la multiplicativité de } g \text{ comme celle de } f \text{ ci-dessus.}$$

Ainsi, si f et g coïncident sur les puissances des nombres premiers, alors $f = g$.

- (d) Soit f une fonction multiplicative.

Posons $g(1) = 1$ puis, pour tout nombre premier p , définissons la suite $(g(p^k))_{k \in \mathbb{N}}$ par récurrence en posant

$$\forall k \in \mathbb{N}^*, g(p^k) = - \sum_{i=1}^k f(p^i) g(p^{k-i})$$

Nous venons de définir une fonction g sur la réunion de $\{1\}$ et des nombres premiers. On prolonge g aux entiers naturels non nuls en posant, pour n supérieur à 2 non premier,

$$g(n) = \prod_{i=1}^q g(p_i^{\alpha_i})$$

où $p_1, \dots, p_q$ sont les facteurs premiers deux à deux distincts de n et $(\alpha_1, \dots, \alpha_q) \in \mathbb{N}^{*q}$ sont leurs multiplicités respectives. Justifier que g est multiplicative puis, calculer pour tout nombre premier p et tout entier $k \in \mathbb{N}$, $(f * g)(p^k)$ afin d'en déduire $f * g$.

- ★ Par définition, $g(1) = 1 \neq 0$.

★ Soient $(m, n) \in \mathbb{N}^{*2}$ tels que $m \wedge n = 1$.

Notons $\mathcal{P}_m$ et $\mathcal{P}_n$ les ensembles de facteurs premiers apparaissant respectivement dans les décompositions en facteurs premiers de m et n de sorte que $m = \prod_{p \in \mathcal{P}_m} p^{\nu_p(m)}$ et $n = \prod_{p \in \mathcal{P}_n} p^{\nu_p(n)}$.

Par définition de g , on a

$$g(m) = \prod_{p \in \mathcal{P}_m} g(p^{\nu_p(m)}) \quad \text{et} \quad g(n) = \prod_{p \in \mathcal{P}_n} g(p^{\nu_p(n)})$$

Par hypothèse, m et n étant premiers entre eux, $\mathcal{P}_m \cap \mathcal{P}_n = \emptyset$ donc la décomposition en facteurs premiers de mn est

$$mn = \left(\prod_{p \in \mathcal{P}_m} p^{\nu_p(m)} \right) \left(\prod_{p \in \mathcal{P}_n} p^{\nu_p(n)} \right)$$

car, pour tout $p \in \mathcal{P}_m \cup \mathcal{P}_n$, $\nu_p(mn) = \begin{cases} \nu_p(m) & \text{si } p \in \mathcal{P}_m, \\ \nu_p(n) & \text{si } p \in \mathcal{P}_n \end{cases}$ de sorte que, par définition de g ,

$$g(mn) = \left(\prod_{p \in \mathcal{P}_m} g(p^{\nu_p(m)}) \right) \left(\prod_{p \in \mathcal{P}_n} g(p^{\nu_p(n)}) \right) = g(m)g(n)$$

Ainsi g est une fonction multiplicative.

- Soit p un nombre premier fixé.
Soit $k \in \mathbb{N}^*$ fixé. $\mathcal{D}_k = \{1, p, \dots, p^k\} = \{p^i \mid i \in \llbracket 1, k \rrbracket\}$ si bien que

$$(f * g)(p^k) = \sum_{d|p^k} f(d)g\left(\frac{p^k}{d}\right) = \sum_{i=0}^k f(p^i)g\left(\frac{p^k}{p^i}\right) = \underbrace{\sum_{i=1}^k f(p^i)g(p^{k-i})}_{=-g(p^k) \text{ par définition de } g(p^k)} + \underbrace{f(1)g(p^k)}_{=1} = 0$$

Ainsi, pour tout p premier, $\forall k \in \mathbb{N}^*$, $(f * g)(p^k) = 0$.

- Nous venons d'établir que

$$\forall p \text{ premier}, \forall k \in \mathbb{N}^*, (f * g)(p^k) = 0 = \delta(p^k)$$

or $f * g$ est une fonction arithmétique multiplicative (d'après la question II.3(b) qui s'applique car f et g le sont) et δ est une fonction arithmétique multiplicative (d'après la question II.1) donc le résultat de la question II.3((c))ii permet de conclure que $f * g = \delta$.

Ainsi $f * g = \delta$.

(e) Que dire de $(\mathbb{M}, *)$?

- * * est une loi de composition interne sur $\mathbb{M}$ d'après la question II.3(b).
- * * est une loi commutative sur $\mathbb{M}$ car elle l'est sur $\mathbb{A}$ d'après la question II.2(b).
- * * est une loi associative sur $\mathbb{M}$ car elle l'est sur $\mathbb{A}$ (admis par l'énoncé dans la question II.2(b)).
- * * admet un élément neutre sur $\mathbb{A}$ qui est δ d'après la question II.2(c), or $\delta \in \mathbb{M}$ d'après la question II.1 donc δ est l'élément neutre de * sur $\mathbb{A}$.
- * Tout élément de $\mathbb{M}$ est symétrisable pour la loi * d'après la question II.3(d) où l'on a établi que, pour tout $f \in \mathbb{M}$, il existe $g \in \mathbb{M}$ telle que $f * g = g * f = \delta$ (en utilisant la commutativité de *).

Ainsi $(\mathbb{M}, *)$ est un groupe abélien.

II.4. Fonction de Möbius.

Soit μ la fonction arithmétique définie par :

$$\mu(n) = \begin{cases} 1 & \text{si } n = 1, \\ (-1)^r & \text{si } n \text{ est le produit de } r \text{ nombres premiers distincts,} \\ 0 & \text{sinon.} \end{cases}$$

(a) Montrer que μ est multiplicative.

— $\mu(1) = 1 \neq 0$.

— Soient $(m, n) \in \mathbb{N}^{*2}$ tels que $m \wedge n = 1$.

— Si $m = 1$, alors $mn = n$ donc $\mu(mn) = \mu(n) = \underbrace{1}_{=\mu(m)} \times \mu(n) = \mu(m)\mu(n)$.

— Si $n = 1$, alors $mn = m$ donc $\mu(mn) = \mu(m) = \mu(m) \times \underbrace{1}_{=\mu(n)} = \mu(m)\mu(n)$.

— Sinon, $m \geq 2$ et $n \geq 2$.

— Si m et n sont respectivement des produits de $r_m \in \mathbb{N}^*$ et $r_n \in \mathbb{N}^*$ nombres premiers deux à deux distincts, alors l'hypothèse $m \wedge n = 1$ garantit qu'ils n'ont aucun facteur premier commun donc mn est le produit de $r_m + r_n$ nombres premiers deux à deux distincts si bien que

$$\mu(mn) = (-1)^{r_m+r_n} = (-1)^{r_m} \times (-1)^{r_n} = \mu(m) \times \mu(n)$$

— Sinon, m ou n a au moins un facteur premier à une puissance ≥ 2 donc l'une des valeurs $\mu(m)$ ou $\mu(n)$ est nulle, et dans ce cas mn a aussi au moins un facteur premier avec une multiplicité ≥ 2 donc $\mu(mn) = 0 = \mu(m) \times \mu(n)$.

Ainsi, μ est une fonction arithmétique multiplicative.

- (b) i. Soit $n \geq 2$ et $p_1, \dots, p_q$ les $q \in \mathbb{N}^*$ facteurs premiers de n deux à deux distincts. On note, pour tout $k \in \llbracket 0, q \rrbracket$, P_k l'ensemble des parties de $\llbracket 1, q \rrbracket$ comportant k éléments. Montrer que

$$\sum_{d|n} \mu(d) = 1 + \sum_{k=1}^q \sum_{I \in P_k} \mu \left(\prod_{i \in I} p_i \right) = 1 + \sum_{k=1}^q (-1)^k \binom{q}{k}$$

Notons $(\alpha_1, \dots, \alpha_q) \in \mathbb{N}^{*q}$ les multiplicités respectives des facteurs premiers $p_1, \dots, p_q$ de $n : n = \prod_{i=1}^q p_i^{\alpha_i}$.

Puisque μ s'annule sur les entiers dont la décomposition en facteurs premiers fait apparaître des multiplicités ≥ 2 ,

$$\sum_{d|n} \mu(d) = \sum_{\substack{d|n \\ \forall i \in \llbracket 1, q \rrbracket, \nu_{p_i}(d) \in \{0, 1\}}} \mu(d)$$

Les diviseurs de d dont tous les facteurs premiers sont de multiplicité 0 ou 1 sont en bijection avec les parties de $\llbracket 1, q \rrbracket$:

$$\psi \left| \begin{array}{l} \{d \in \mathbb{N} \mid d|n \text{ et } \forall i \in \llbracket 1, q \rrbracket, \nu_{p_i}(d) \in \{0, 1\}\} \rightarrow \mathcal{P}(\llbracket 1, q \rrbracket) \quad (\text{notation pour les parties de } \llbracket 1, q \rrbracket) \\ d \mapsto \{i \in \llbracket 1, q \rrbracket \mid p_i | d\} \\ \prod_{i \in I} p_i \leftarrow I \end{array} \right.$$

si bien qu'en observant que $\psi(1) = \emptyset$,

$$\sum_{d|n} \mu(d) = \sum_{I \in \mathcal{P}(\llbracket 1, q \rrbracket)} \mu \left(\prod_{i \in I} p_i \right) = \underbrace{\mu(1)}_{\text{cas } I = \emptyset} + \sum_{\substack{I \in \mathcal{P}(\llbracket 1, q \rrbracket) \\ I \neq \emptyset}} \mu \left(\prod_{i \in I} p_i \right) = 1 + \sum_{\substack{I \in \mathcal{P}(\llbracket 1, q \rrbracket) \\ I \neq \emptyset}} \mu \left(\prod_{i \in I} p_i \right)$$

Utilisons qu'en regroupant les parties de $\llbracket 1, q \rrbracket$ selon la valeur de leur cardinal, on obtient la partition

$$\mathcal{P}(\llbracket 1, q \rrbracket) = \bigsqcup_{k=0}^q P_k = \{\emptyset\} \cup \left(\bigsqcup_{k=1}^q P_k \right)$$

d'où

$$\sum_{d|n} \mu(d) = 1 + \sum_{k=1}^q \sum_{I \in P_k} \underbrace{\mu \left(\prod_{i \in I} p_i \right)}_{=(-1)^k} = \sum_{k=0}^q (-1)^k |P_k| = \sum_{k=0}^q (-1)^k \binom{q}{k} \quad \text{car } \forall k \in \llbracket 1, q \rrbracket, |P_k| = \binom{q}{k}.$$

$$\text{Ainsi } \sum_{d|n} \mu(d) = 1 + \sum_{k=1}^q \sum_{I \in P_k} \mu \left(\prod_{i \in I} p_i \right) = 1 + \sum_{k=1}^q (-1)^k \binom{q}{k}$$

- ii. En déduire que $\mu * \mathbf{1} = \delta$.

★ Soient p un nombre premier et $k \in \mathbb{N}^*$ fixés. En utilisant que $\mathcal{D}_{p^k} = \{p^i \mid i \in \llbracket 0, k \rrbracket\}$,

$$(\mu * \mathbf{1})(p^k) = \sum_{d|p^k} \underbrace{\mu(p^i)}_{=0 \text{ si } i \geq 2} \underbrace{\mathbf{1} \left(\frac{p^k}{p^i} \right)}_{=1} = \mu(1) + \mu(p) = 1 + (-1)^1 = 0 = \delta(p^k) \quad \text{car } k \in \mathbb{N}^* \text{ donc } p^k \geq p \geq 2.$$

★ Nous venons de prouver que

$$\forall p \text{ premier}, \forall k \in \mathbb{N}^*, (\mu * \mathbf{1})(p^k) = \delta(p^k)$$

or $\mu * \mathbf{1}$ est une fonction arithmétique multiplicative (d'après la question II.3(b) qui s'applique car μ et $\mathbf{1}$ le sont d'après les questions II.4(a) et II.1) et δ est une fonction arithmétique multiplicative (d'après la question II.1) donc le résultat de la question II.3(c)ii permet de conclure que $\mu * \mathbf{1} = \delta$.

$$\text{Ainsi } \mu * \mathbf{1} = \delta.$$

- (c) Soit $f \in \mathbb{A}$ et $F \in \mathbb{A}$ telle que, pour tout $n \in \mathbb{N}^*$, $F(n) = \sum_{d|n} f(d)$. Montrer que pour tout $n \in \mathbb{N}^*$,

$$f(n) = \sum_{d|n} \mu(d) F \left(\frac{n}{d} \right) = \sum_{d|n} \mu \left(\frac{n}{d} \right) F(d)$$

Observons que la définition de F correspond à $\mathbf{1} * f$:

$$\forall n \in \mathbb{N}^*, (\mathbf{1} * f)(n) = \sum_{d|n} \underbrace{\mathbf{1} \left(\frac{n}{d} \right)}_{=1} f(d) = \sum_{d|n} f(d) = F(n)$$

donc en composant à gauche par μ l'égalité $F = \mathbf{1} * f$,

$$\mu * F = \mu * (\mathbf{1} * f) \underbrace{=}_{\substack{* \text{ associat.} \\ = \delta \text{ quest. II.4((b))ii}}} (\underbrace{\mu * \mathbf{1}}_{\substack{* \text{ neutre de } *}}) * f = \delta * f \underbrace{=}_{\substack{* \text{ neutre de } *}} f$$

si bien que

$$\forall n \in \mathbb{N}^*, f(n) = (\mu * F)(n) = \sum_{d|n} \mu(d) F\left(\frac{n}{d}\right)$$

$$\text{Ainsi pour tout } n \in \mathbb{N}^*, f(n) = \sum_{d|n} \mu(d) F\left(\frac{n}{d}\right) = \sum_{d|n} \mu\left(\frac{n}{d}\right) F(d).$$

II.5. (★) On note $\mathbf{I} : \begin{cases} \mathbb{N}^* & \rightarrow \mathbb{C} \\ n & \mapsto n \end{cases}$ et φ la fonction indicatrice d'Euler, définie par

$$\forall n \in \mathbb{N}^*, \varphi(n) = \text{card}\{k \in \llbracket 1, n \rrbracket \mid k \wedge n = 1\}$$

Montrer que $\varphi = \mu * \mathbf{I}$ puis en déduire que $\forall n \in \mathbb{N}^*, n = \sum_{d|n} \varphi(d)$.

• ★ Montrons que $\mathbf{I}$ est multiplicative.

— $\mathbf{I}(1) = 1 \neq 0$.

— Soient $(m, n) \in \mathbb{N}^{*2}$ fixés tels que $m \wedge n = 1$. Alors

$$\mathbf{I}(mn) = mn = \mathbf{I}(m) \times \mathbf{I}(n)$$

★ Montrons que φ est multiplicative.

— $\varphi(1) = |\{k \in \llbracket 1, 1 \rrbracket \mid k \wedge 1 = 1\}| = |\{1\}| = 1 \neq 0$.

— Soient $(m, n) \in \mathbb{N}^{*2}$ fixés tels que $m \wedge n = 1$.

Considérons l'application

$$\varphi(mn) = mn = \varphi(m) \times \varphi(n)$$

★ Soient p un nombre premier et $k \in \mathbb{N}^*$ fixés.

$\varphi(p^k)$ est le nombre d'entiers de $\llbracket 1, p^k \rrbracket$ qui sont premiers avec p^k .

★ Nous venons de prouver que

$$\forall p \text{ premier}, \forall k \in \mathbb{N}^*, (\mu * \mathbf{I})(p^k) = \varphi(p^k)$$

or $\mu * \mathbf{I}$ est une fonction arithmétique multiplicative (d'après la question II.3(b) qui s'applique car μ et $\mathbf{I}$ le sont) et φ est aussi une fonction arithmétique multiplicative donc le résultat de la question II.3((c))ii permet de conclure que $\mu * \mathbf{I} = \varphi$.

$$\text{Ainsi } \varphi = \mu * \mathbf{I}.$$

• Reprenons l'égalité ci-dessus et composons à gauche par $\mathbf{1}$:

$$\mathbf{1} * \varphi = \mathbf{1} * (\mu * \mathbf{I}) \underbrace{=}_{\substack{* \text{ associat.} \\ = \mu * \mathbf{1} * \text{ commut.} \\ = \delta \text{ quest. II.4((b))ii}}} (\underbrace{\mathbf{1} * \mu}_{\substack{* \text{ neutre de } *}}) * \mathbf{I} = \delta * \mathbf{I} \underbrace{=}_{\substack{* \text{ neutre de } *}} \mathbf{I}$$

donc, pour tout $n \in \mathbb{N}^*$,

$$n = \mathbf{I}(n) = (\mathbf{1} * \varphi)(n) = \sum_{d|n} \underbrace{\mathbf{1}\left(\frac{n}{d}\right)}_{=1} \varphi(d) = \sum_{d|n} \varphi(d)$$

$$\text{Ainsi } \forall n \in \mathbb{N}^*, n = \sum_{d|n} \varphi(d).$$

III . Mots circulaires

Dans cette partie, l'entier naturel m est fixé.

On considère un alphabet de m lettres : $\mathcal{A} = \{a_1, a_2, \dots, a_m\}$.

Un mot ℓ sur l'alphabet $\mathcal{A}$ est une suite de $\mathcal{A}^{\mathbb{N}}$: $\ell = (\ell_0, \ell_1, \ell_2, \dots)$ où, pour tout $i \in \mathbb{N}$, $\ell_i \in \mathcal{A}$ est la $(i+1)$ -ème lettre du mot ℓ .

Le mot ℓ est périodique s'il existe $p \in \mathbb{N}^*$ tel que $\forall i \in \mathbb{N}$, $\ell_{i+p} = \ell_i$. Un tel entier naturel non nul p est appelé une période de ℓ .

On note $\mathcal{L}(\mathcal{A})$ l'ensemble des mots périodiques sur l'alphabet $\mathcal{A}$: $\mathcal{L}(\mathcal{A}) = \{\ell \in \mathcal{A}^{\mathbb{N}} \mid \exists p \in \mathbb{N}^* : \forall i \in \mathbb{N}, \ell_{i+p} = \ell_i\}$.

Pour tout $n \in \mathbb{N}^*$, $\mathcal{L}_n(\mathcal{A})$ désigne l'ensemble des mots périodiques sur l'alphabet $\mathcal{A}$ dont n est une période

$$\mathcal{L}_n(\mathcal{A}) = \{\ell \in \mathcal{A}^{\mathbb{N}} \mid \forall i \in \mathbb{N}, \ell_{i+n} = \ell_i\}.$$

On note $c : \begin{array}{ccc} \mathcal{A}^{\mathbb{N}} & \longrightarrow & \mathcal{A}^{\mathbb{N}} \\ \ell & \longmapsto & \ell' \end{array}$ où pour tout $i \in \mathbb{N}$, $\ell'_i = \ell_{i+1}$.

On note $c^0 = \text{Id}_{\mathcal{A}^{\mathbb{N}}}$, pour tout $k \in \mathbb{N}^*$, $c^k = \underbrace{c \circ c \cdots \circ c}_k$.

III.1. Soit $\ell \in \mathcal{L}(\mathcal{A})$ un mot périodique fixé. Notons $\mathcal{P}(\ell)$ l'ensemble de ses périodes.

- (a) Montrer qu'il existe un unique $p(\ell) \in \mathbb{N}^*$ tel que $\mathcal{P}(\ell) = p(\ell) \cdot \mathbb{N}^*$.
On dit que $p(\ell)$ est la **période primitive** de ℓ .

ℓ est périodique, donc $\mathcal{P}(\ell)$ est une partie de $\mathbb{N}$ non vide. Elle admet un plus petit élément : p .

- Soit $k \in \mathbb{N}^*$, alors pour tout $i \in \mathbb{N}$, $\ell_i = \ell_{i+p}$ et donc $\ell_{i+kp} = \ell_{i+(k+1)p}$.
Donc la suite extraite $(\ell_{i+kp})_{k \in \mathbb{N}}$ est une suite constante. Et donc pour tout $k \in \mathbb{N}$, $kp \in \mathcal{P}(\ell)$.
Donc $p\mathbb{N}^* \subset \mathcal{P}(\ell)$.
- Réciproquement, soit t une autre période de ℓ . On peut faire la division euclidienne de t par $p (\neq 0)$.
Donc il existe un couple $(q, r) \in \mathbb{N}^* \times \mathbb{N}$ (car $t \in \mathbb{N}^*$) tel que $t = qp + r$ et $r \in \llbracket 0, p-1 \rrbracket$.
On a vu que qp est une période, ainsi que t , donc : $\forall i \in \mathbb{N}$, $\ell_{i+r} = \ell_{i+t-qp} = \ell_{i+t} = \ell_i$.
Donc si $r \neq 0$, $r \in \mathcal{P}(\ell)$ et également $r < p$. Cela est contradictoire. Donc $r = 0$.
Et finalement $t \in p\mathbb{N}^*$.

Par double inclusion,

il existe un unique $p(\ell) \in \mathbb{N}^*$ tel que $\mathcal{P}(\ell) = p(\ell) \cdot \mathbb{N}^*$.

- (b) Montrer que, pour tout $p \in \mathbb{N}^*$, p est une période de ℓ si et seulement si $c^p(\ell) = \ell$.

Soit $p \in \mathbb{N}^*$, notons $\ell' = c(\ell)$, pour tout $j \in \mathbb{N}$, la $j+1$ -ième lettre du mot $c(\ell)$ est la lettre $\ell'_j = \ell_{j+1}$.

Puis par récurrence immédiate, la $j+1$ -ième lettre du mot $\ell^{(k)} := c^k(\ell)$ est la lettre $\ell_j^{(k)} = \ell_{j+k}$.

On a alors les équivalences :

- p est une période de $\ell \iff \forall i \in \mathbb{N}, \ell_{i+p} = \ell_i$
 $\iff \forall i \in \mathbb{N}$, la $i+1$ -ième lettre de $c^p(\ell)$ (qui vaut ℓ_{i+p}) est égale à ℓ_i
 $\iff \forall i \in \mathbb{N}$, la $i+1$ -ième lettre de $c^p(\ell)$ et celle de ℓ sont identiques.

Pour tout $p \in \mathbb{N}^*$, p est une période de ℓ si et seulement si $c^p(\ell) = \ell$.

- (c) Énoncer et démontrer une condition nécessaire et suffisante exprimée avec des puissances de c pour exprimer que $p(\ell)$ est la période primitive de ℓ .

Le nombre $p(\ell)$ est la période primitive de ℓ est équivalent à dire
que $p(\ell)$ est une période et il n'y en pas de plus petite.

$p(\ell)$ est la période primitive de ℓ si et seulement si $c^p(\ell) = \ell$ et $\forall k < p, c^k(\ell) \neq \ell$.

- (d) Montrer que $c(\mathcal{L}(\mathcal{A})) \subset \mathcal{L}(\mathcal{A})$ puis que c restreinte à $\mathcal{L}(\mathcal{A})$ est injective.

Soit $\ell \in \mathcal{L}(\mathcal{A})$. Il existe $p \in \mathbb{N}$ tel que ℓ est p -périodique. Par ailleurs, notons $\ell' = c(\ell)$

Pour tout $i \in \mathbb{N}$, $\ell'_{i+p} = \ell_{i+p+1} = \ell_{i+1+p} = \ell_{i+1}$ car ℓ est p -périodique.

Et donc $\ell'_{i+p} = \ell'_i$. Donc $c(\ell) = \ell' \in \mathcal{L}(\mathcal{A})$.

On notera que ℓ et $c(\ell)$ ont les mêmes périodes

$c(\mathcal{L}(\mathcal{A})) \subset \mathcal{L}(\mathcal{A})$

Soit $\ell^1, \ell^2 \in \mathcal{L}(\mathcal{A})$ tel que $c(\ell^1) = c(\ell^2)$.

Alors pour tout $i \in \mathbb{N}$, $(\ell^1)_{i+1} = (\ell^1)'_i = (\ell^2)'_i = (\ell^2)_{i+1}$.

Hormis la première lettre, il s'agit des mêmes mots. Ces deux mots sont périodiques.

Montrons qu'ils ont la même période.

Ensuite, on a donc $\ell^1_0 = \ell^1_p = \ell^2_p = \ell^2_0$ (puisque $p > 0$).

Ainsi $\ell^1 = \ell^2$.

c restreinte à $\mathcal{L}(\mathcal{A})$ est donc injective.

- (e) En déduire que $p(c(\ell)) = p(\ell)$.

III.2. Soit $p \in \mathbb{N}^*$. On note $\mathcal{P}_p$ l'ensemble des mots périodiques dont la période primitive est p : $\mathcal{P}_p = \{\ell \in \mathcal{L}(\mathcal{A}) \mid p(\ell) = p\}$.

On note $\sim$ la relation binaire définie sur $\mathcal{P}_p$ par : $\ell \sim \ell'$ si et seulement si $\exists k \in \mathbb{N}$ tel que $c^k(\ell) = \ell'$.

(a) Justifier que la relation binaire est bien définie puis montrer que $\sim$ est une relation d'équivalence.

- Pour $\ell \in \mathcal{P}_p$, $c^0(\ell) = \ell$, donc $\ell \sim \ell$. Et $\sim$ est reflexive.
- Soient $\ell, \ell' \in \mathcal{P}_p$ tels que $\ell \sim \ell'$.
 Donc il existe $k \in \mathbb{N}$ tel que $c^k(\ell) = \ell'$. Et donc (cf. 1.(b)), pour tout $i \in \mathbb{N}$, $\ell_{k+i} = \ell'_i$.
 p et ses multiples sont des périodes de ℓ (et ℓ'). Et, il existe $h \in \mathbb{N}^*$ tel que $hp > k$.
 Soit $j \in \mathbb{N}$, $\ell_j = \ell_{j+hp} = \ell_{k+(j+hp-k)}$ et donc en considérant $i = j + hp - k > 0$: $\ell_j = \ell'_{j+hp-k}$
 Ainsi, avec $k' = hp - k$, $\ell = c^{k'}(\ell')$. Ainsi $\ell' \sim \ell$
 Et $\sim$ est symétrique
- Soient $\ell, \ell', \ell'' \in \mathcal{P}_p$ tels que $\ell \sim \ell'$ et $\ell' \sim \ell''$.
 Alors il existe $k, k' \in \mathbb{N}$ tel que $c^k(\ell) = \ell'$ et $c^{k'}(\ell') = \ell''$.
 Donc $c^{k+k'}(\ell) = c^{k'}(c^k(\ell)) = c^{k'}(\ell') = \ell''$.
 Et comme $k + k' \in \mathbb{N}$, on a donc $\ell \sim \ell''$.
 Et $\sim$ est transitive.

$\sim$ est une relation d'équivalence définie sur $\mathcal{P}_p$.

Lorsque $(\ell, \ell') \in \mathcal{P}_p^2$ vérifient $\ell \sim \ell'$, on dit que les mots ℓ et ℓ' définissent le même mot circulaire.
 On note $\bar{\ell}$ la classe d'équivalence de $\ell \in \mathcal{P}_p$ pour cette relation. Une classe d'équivalence représente donc un unique mot circulaire.

(b) Soit $\ell \in \mathcal{P}_p$. Montrer que

$$\text{card}(\bar{\ell}) = p$$

Soit $\ell \in \mathcal{P}_p$.

Pour tout $k \in \llbracket 0, p-1 \rrbracket$, les mots $\ell^{(k)} := c^k(\ell)$ sont par construction en relation avec ℓ donc tous éléments de $\bar{\ell}$.

Par ailleurs on peut noter qu'ils sont tous distincts,

sinon, il existe $h_1, h_2 \in \llbracket 0, p-1 \rrbracket$ avec $h_1 < h_2$ (SPDG) tel que $c^{h_1}(\ell) = c^{h_2}(\ell)$.

Alors pour tout $i \in \mathbb{N}$, $\ell_{i+h_1} = \ell_i^{(h_1)} = \ell_i^{(h_2)} = \ell_{i+h_2}$.

Et donc pour $j \in \mathbb{N}$ et $\ell_j = \ell_{j+p} = \ell_{(j+p-h_1)+h_1} = \ell_{(j+p-h_1)+h_2} = \ell_{j+h_2-h_1+p} = \ell_{j+h_2-h_1}$ ($\ell \in \mathcal{P}_p$).

Et par conséquent ℓ est $h_2 - h_1 (< p)$ périodique,

ce qui est contradictoire avec le fait que p est la période primitive de ℓ .

Enfin, si $\ell' \in \bar{\ell}$, il existe $k \in \mathbb{N}$ tel que $c^k(\ell) = \ell'$.

Par p -périodicité, si $k = qp + r$ est la division euclidienne de k par p , on a

$c^r(\ell) = c^{k-qp}(\ell) = c^k(\ell) = \ell'$, donc $\ell' \in \{c^r(\ell), r \in \llbracket 0, p-1 \rrbracket\}$. On a énuméré l'ensemble $\bar{\ell}$,

$$\text{Card}(\bar{\ell}) = \text{Card}(\{c^r(\ell), r \in \llbracket 0, p-1 \rrbracket\}) = p$$

On note $(\ell^i)_{i \in M_p}$ (l'indice est placé comme un exposant car ℓ^i représente une suite, mais ce n'est qu'une notation) un système de représentant des mots circulaires de période primitive p et $M(p)$ le cardinal de l'ensemble M_p qui indexe le système de représentants, c'est-à-dire le nombre de mots circulaires.

III.3. Soit $n \in \mathbb{N}^*$ fixé.

(a) Montrer que $\mathcal{L}_n(\mathcal{A}) = \bigsqcup_{p|n} \mathcal{P}_p$.

Soit $\ell \in \mathcal{L}_n(\mathcal{A})$.

Alors ℓ est périodique. Notons $p(\ell)$ sa période primitive, donc les périodes de ℓ sont des éléments de $p(\ell) \cdot \mathbb{N}^*$.

Mais n est une période de ℓ , donc $p(\ell)|n$.

Ainsi, $\exists p \in \mathbb{N}$ tel que $p|n$ tel que $\ell \in \mathcal{P}_p$. C'est-à-dire : $\ell \in \bigcup_{p|n} \mathcal{P}_p$ et donc $\mathcal{L}_n(\mathcal{A}) \subset \bigcup_{p|n} \mathcal{P}_p$.

Par ailleurs, la réunion est bien disjointe, un mot ℓ ne peut avoir deux périodes primitives distinctes.

Enfin, si $\ell \in \bigcup_{p|n} \mathcal{P}_p$, alors il existe p , diviseur de n tel que $\ell \in \mathcal{P}_p$.

Donc ℓ est p -périodique et ℓ est alors hp périodique pour tout $h \in \mathbb{N}^*$, et en particulier n -périodique (puisque $p|n$).

Ainsi $\ell \in \mathcal{L}_n(\mathcal{A})$ et donc $\bigcup_{p|n} \mathcal{P}_p \subset \mathcal{L}_n(\mathcal{A})$

Par double inclusion

$$\mathcal{L}_n(\mathcal{A}) = \bigsqcup_{p|n} \mathcal{P}_p$$

(b) En déduire que

$$m^n = \sum_{p|n} pM(p)$$

Passons au calcul du cardinal. Puisque la réunion est disjointe :

$$\text{Card}\mathcal{L}_n(\mathcal{A}) = \text{Card}\left(\bigcup_{p|n} \mathcal{P}_p\right) = \sum_{p|n} \text{Card}(\mathcal{P}_p)$$

Par ailleurs, puisque $(\ell^i)_{i \in M_p}$ est un système de représentant des classes d'équivalence pour la relation $\sim$ définie sur $\mathcal{P}_p$:

$$\mathcal{P}_p = \bigcup_{i \in M_p} \bar{\ell}^i$$

En passant aux cardinaux :

$$\text{Card}(\mathcal{P}_p) = \sum_{i \in M_p} \text{Card}(\bar{\ell}^i) = \sum_{i \in M_p} p = p \sum_{i \in M_p} 1 = p \times \text{Card}(M_p)$$

Enfin, $\Phi : \mathcal{L}_n(\mathcal{A}) \rightarrow \mathcal{A}^n$, $\ell \mapsto (\ell_0, \ell_1, \dots, \ell_{n-1})$ est bijective, car la bijection réciproque et $\Psi : \mathcal{A}^n \rightarrow \mathcal{L}_n(\mathcal{A})$, $(a_0, a_1, \dots, a_{n-1}) \mapsto \ell$ tel que $\forall i \in \mathbb{N}$, $\ell_i = a_k$ si $k = i \% n$ est le reste de la division euclidienne de i par n . ℓ est bien n -périodique. Ainsi

$$\text{Card}\mathcal{L}_n(\mathcal{A}) = \text{Card}\mathcal{A}^n = m^n$$

Au final :

$$m^n = \sum_{p|n} pM(p)$$

III.4. **Inversion de Möbius.** On rappelle la formule trouvée dans la partie précédente :

Si pour tout $n \in \mathbb{N}^*$, $F(n) = \sum_{d|n} f(d)$, alors pour tout $n \in \mathbb{N}^*$, $f(n) = \sum_{d|n} \mu\left(\frac{n}{d}\right) F(d)$.

(a) Montrer que $pM(p) = \sum_{q|p} \mu\left(\frac{p}{q}\right) m^q$.

On applique la formule d'inversion pour $f(d) = dM(d)$ et $F(n) = m^n$ (variable : n).
Donc, on obtient :

$$\forall n \in \mathbb{N}^*, \quad nM(n) = \sum_{d|n} \mu\left(\frac{n}{d}\right) m^d$$

(b) Montrer que si p est un nombre premier, $M(p) = \frac{m}{p}(m^{p-1} - 1)$.

En déduire le petit théorème de Fermat.

On a donc, (en changeant les noms des variables libres) : $pM(p) = \sum_{q|p} \mu\left(\frac{p}{q}\right) m^q$.

Et donc si p est premier et n'admet que 1 et p comme diviseur :

$$pM(p) = \underbrace{\mu(p)m^1}_{q=1} + \underbrace{\mu(1)m^p}_{q=p} = m(\mu(p) + \mu(1)m^{p-1})$$

Or on a vu que $\mu(1) = 1$ et $\mu(p) = -1$, pour p un nombre premier.

En divisant par p :

$$M(p) = \frac{m}{p}(m^{p-1} - 1)$$

$M(p)$ étant un nombre entier (le nombre de mots circulants de taille p sur l'alphabet de m lettres), nécessairement p divise $m^p - m$.

Et donc $p|m^p - m$ ou encore $m^p \equiv m \pmod{p}$. C'est le petit théorème de Fermat.

(c) (pourrait être enlevée) Montrer que le nombre total de mots circulaires de période inférieure ou égale à n sur un alphabet de m lettres est

$$S_n = \sum_{p|n} \frac{1}{p} \sum_{q|p} \mu\left(\frac{p}{q}\right) m^q$$

On a vu que $pM(p) = \sum_{q|p} \mu\left(\frac{p}{q}\right) m^q$.

Le nombre de mots circulaires de périodes inférieure ou En synthèse, on a donc (en toute généralité) :

$$m^n =$$

III.5. Application au calcul de traces des puissances d'une somme de matrices.

Soit n un entiers naturel non nul.

La trace d'une matrice $M \in \mathcal{M}_n(\mathbb{Z})$ est le réel noté $\text{Tr}(M)$ qui correspond à la somme des éléments diagonaux de M :

$$\text{Tr}(M) = \sum_{i=1}^n [M]_{i,i}$$

On admet dans cette question, le résultat qui fait l'objet de la question IV.1(a) :

$$\forall (M, N) \in \mathcal{M}_n(\mathbb{Z})^2, \text{Tr}(M + N) = \text{Tr}(M) + \text{Tr}(N) \quad \text{et} \quad \text{Tr}(MN) = \text{Tr}(NM).$$

On considère m matrices $(A_1, A_2, \dots, A_m) \in \mathcal{M}_n(\mathbb{Z})^m$ et l'on cherche à simplifier $\text{Tr}((A_1 + A_2 + \dots + A_m)^k)$ pour $k \in \mathbb{N}^*$.

(a) Montrer que
$$\text{Tr}((A_1 + A_2 + \dots + A_m)^k) = \sum_{\ell \in \mathcal{L}_k(\{1, 2, \dots, m\})} \text{Tr}(A_{\ell_0} A_{\ell_1} \dots A_{\ell_{k-1}})$$

(b) En déduire que

$$\text{Tr}((A_1 + A_2 + \dots + A_m)^k) = \sum_{p|k} \left(\sum_{i \in \mathcal{M}_p} p \text{Tr}((A_{\ell_0^i} A_{\ell_1^i} \dots A_{\ell_{p-1}^i})^{\frac{k}{p}}) \right) \quad (4)$$

IV . Généralisation du petit théorème de Fermat

Soit $n \in \mathbb{N}$. Les matrices considérées dans cette partie sont définies dans l'anneau $\mathbb{Z}$.

Considérons également p un nombre premier.

IV.1. Soient $(B, C) \in \mathcal{M}_n(\mathbb{Z})^2$. Le but de cette question est d'établir la relation

$$\text{Tr}((B + C)^p) \equiv \text{Tr}(B^p) + \text{Tr}(C^p) \pmod{p} \quad (5)$$

(a) Montrer que, pour tout $(M, N) \in \mathcal{M}_n(\mathbb{Z})^2$, $\text{Tr}(M + N) = \text{Tr}(M) + \text{Tr}(N)$ et $\text{Tr}(MN) = \text{Tr}(NM)$.

Il s'agit d'une question de cours. On exploite la linéarité des applications $M \mapsto [M]_{i,j}$.

$$\text{Tr}(M + N) = \sum_{i=1}^n [M + N]_{i,i} = \sum_{i=1}^n ([M]_{i,i} + [N]_{i,i}) = \sum_{i=1}^n [M]_{i,i} + \sum_{i=1}^n [N]_{i,i} = \text{Tr}(M) + \text{Tr}(N)$$

Puis :

$$\begin{aligned} \text{Tr}(MN) &= \sum_{i=1}^n [MN]_{i,i} = \sum_{i=1}^n \left(\sum_{h=1}^n [M]_{i,h} [N]_{h,i} \right) = \sum_{i=1}^n \left(\sum_{h=1}^n [N]_{h,i} [M]_{i,h} \right) \\ &= \sum_{h=1}^n \left(\sum_{i=1}^n [N]_{h,i} [M]_{i,h} \right) = \sum_{h=1}^n [NM]_{h,h} = \text{Tr}(NM) \end{aligned}$$

On a bien : $\forall (M, N) \in \mathcal{M}_n(\mathbb{Z})^2, \text{Tr}(M + N) = \text{Tr}(M) + \text{Tr}(N)$ et $\text{Tr}(MN) = \text{Tr}(NM)$.

(b) Établir par un calcul explicite les relations (5) pour $p = 2$ et $p = 3$.

Soit $B, C \in \mathcal{M}_n(\mathbb{Z})$, on a donc :

$$\text{Tr}((B+C)^2) = \text{Tr}(B^2 + BC + CB + C^2) = \text{Tr}(B^2) + \text{Tr}(C^2) + \text{Tr}(BC) + \text{Tr}(CB) = \text{Tr}(B^2) + \text{Tr}(C^2) + 2\text{Tr}(BC) \equiv \text{Tr}B^2 + \text{Tr}C^2 \pmod{2}$$

Soit $B, C \in \mathcal{M}_n(\mathbb{Z})$, on a donc :

$$\begin{aligned} \text{Tr}((B + C)^3) &= \text{Tr}(B^3 + B^2C + BCB + CB^2 + BC^2 + CBC + C^2B + C^3) \\ &= \text{Tr}(B^3) + \text{Tr}(B^2C) + \text{Tr}(\underbrace{(BC)B}_{=\text{Tr}(B^2C)}) + \text{Tr}(\underbrace{CB^2}_{=\text{Tr}(B^2C)}) + \text{Tr}(BC^2) + \text{Tr}(\underbrace{C(BC)}_{=\text{Tr}(BC^2)}) + \text{Tr}(\underbrace{C^2B}_{=\text{Tr}(BC^2)}) + \text{Tr}(C^3) \\ &= \text{Tr}(B^3) + 3\text{Tr}(B^2C) + 3\text{Tr}(BC^2) + \text{Tr}(C^3) \equiv \text{Tr}(B^3) + \text{Tr}(C^3) \pmod{3} \end{aligned}$$

On trouve bien : $\forall B, C \in \mathcal{M}_n(\mathbb{Z}), \text{Tr}((B + C)^2) \equiv \text{Tr}(B^2) + \text{Tr}(C^2) \pmod{2}$ et $\text{Tr}((B + C)^3) \equiv \text{Tr}(B^3) + \text{Tr}(C^3) \pmod{3}$.

- (c) En reprenant la formule (4) démontrée en fin de partie précédente, prouver la relation (5) en toute généralité. p est un nombre premier, il n'admet comme diviseur que $d = p$ et $d = 1$. La formule (4) devient :

$$\begin{aligned} \text{Tr}((B+C)^p) &= \sum_{d|p} \left(\sum_{i \in M_d} d \text{Tr}((A_{\ell_0^i} A_{\ell_1^i} \cdots A_{\ell_{d-1}^i})^{\frac{p}{d}}) \right) \\ &= \underbrace{\sum_{i \in M_1} 1 \text{Tr}(A^p)}_{d=1} + \underbrace{\sum_{i \in M_p} p \text{Tr}(A_{\ell_0^i} \cdots A_{\ell_0^i}^p)}_{d=p} \\ &= \text{Tr}(B^p) + \text{Tr}(C^p) + p \sum_{i \in M_p} \text{Tr}(A_{\ell_0^i} \cdots A_{\ell_0^i}^p) \equiv \text{Tr}(B^p) + \text{Tr}(C^p) \quad [p] \end{aligned}$$

où l'on a exploité le fait que pour $d = 1$, les mots de période primitive égale à 1 sont les mots ultimes B^p et C^p .

$$\boxed{\forall B, C \in \mathcal{M}_n(\mathbb{Z}), \quad \text{Tr}(B+C)^p = \text{Tr}B^p + \text{Tr}C^p \quad [p]}$$

IV.2. Petit théorème de Fermat matriciel.

Soit $A \in \mathcal{M}_n(\mathbb{Z})$.

- (a) Montrer, en raisonnant par analyse-synthèse, qu'il existe un unique couple $(B, C) \in \mathcal{M}_n(\mathbb{Z})^2$ tel que B est triangulaire inférieure, C est triangulaire supérieure à diagonale nulle et $A = B + C$.
On exprimera, pour tout $(i, j) \in \llbracket 1, n \rrbracket^2$, $[B]_{i,j}$ et $[C]_{i,j}$ en fonction de $[A]_{i,j}$.

Analyse. Supposons que $A = B + C$, avec B triangulaire inférieure et C , triangulaire supérieure à diagonale nulle. Alors pour tout $(i, j) \in \mathbb{N}_n^2$:

— Si $i < j$, alors $[B]_{i,j} = 0$, puisque B est triangulaire inférieure, et donc

$$[A]_{i,j} = [B+C]_{i,j} = [B]_{i,j} + [C]_{i,j} = 0 + [C]_{i,j}$$

— Si $i \geq j$, alors $[C]_{i,j} = 0$, puisque C est triangulaire supérieure à diagonale nulle, et donc

$$[A]_{i,j} = [B+C]_{i,j} = [B]_{i,j} + [C]_{i,j} = [B]_{i,j} + 0$$

Synthèse. Soit B et C telles que

$$\forall i, j \in \mathbb{N}_n^2 : \quad \begin{cases} i < j \Rightarrow [B]_{i,j} = 0 \text{ et } [C]_{i,j} = [A]_{i,j} \\ i \geq j \Rightarrow [B]_{i,j} = [A]_{i,j} \text{ et } [C]_{i,j} = 0 \end{cases}$$

Alors $A = B + C$, B est triangulaire inférieure et C est triangulaire supérieure à diagonale nulle.

$$\boxed{\forall A \in \mathcal{M}_n(\mathbb{Z}), \exists !(B, C) \in \mathcal{M}_n(\mathbb{Z})^2 \text{ tel que } B \text{ est triangulaire inférieure, } C \text{ est triangulaire supérieure à diagonale nulle et } A = B + C.}$$

- (b) Calculer explicitement, par exemple par récurrence, pour tout $i \in \llbracket 1, n \rrbracket$, pour tout $k \in \mathbb{N}^*$, $[C^k]_{i,i}$ et $[B^k]_{i,i}$ en fonction de k et des coefficients de A .

Posons, pour tout $k \in \mathbb{N}^*$, $\mathcal{P}_k$:

« B^k est triangulaire inférieure avec pour tout $i \in \mathbb{N}_n$, $[B^k]_{i,i} = ([B]_{i,i})^k$,
 C^k est triangulaire supérieure à diagonale nulle ».

— $\mathcal{P}_1$ est immédiatement vraie.

— Soit $k \in \mathbb{N}^*$. Supposons que $\mathcal{P}_k$ est vraie.

Pour tout $i > j$:

$$[B^{k+1}]_{i,j} = \sum_{h=1}^n [B^k]_{i,h} [B]_{h,j} = \sum_{h=1}^j \underbrace{[B^k]_{i,h}}_{=0 \text{ car } i > j \geq h} [B]_{h,j} + \sum_{h=j+1}^n [B^k]_{i,h} \underbrace{[B]_{h,j}}_{=0 \text{ car } h > j} = 0$$

Donc B est triangulaire supérieure.

Avec le même calcul :

$$[B^{k+1}]_{i,i} = \sum_{h=1}^{i-1} \underbrace{[B^k]_{i,h} [B]_{h,i}}_{=0} + \underbrace{[B^k]_{i,i}}_{=([B]_{i,i})^k \text{ d'après } \mathcal{P}_k} [B]_{i,i} + \sum_{h=i+1}^n [B^k]_{i,h} \underbrace{[B]_{h,i}}_{=0} = ([B]_{i,i})^{k+1}$$

Pour tout $i \leq j$:

$$[C^{k+1}]_{i,j} = \sum_{h=1}^n [C^k]_{i,h} [C]_{h,j} = \sum_{h=1}^i [C^k]_{i,h} \underbrace{[C]_{h,j}}_{=0 \text{ car } j \geq i \geq h} + \sum_{h=i+1}^n \underbrace{[C^k]_{i,h}}_{=0 \text{ car } h > i} [C]_{h,j} = 0$$

Donc C est triangulaire inférieure à diagonale nulle.

Ainsi $\mathcal{P}_{k+1}$ est vraie.

Comme, pour tout $i \in \mathbb{N}_n$, $[B]_{i,i} = [A]_{i,i}$:

$$\boxed{\text{pour tout } i \in \llbracket 1, n \rrbracket, \text{ pour tout } k \in \mathbb{N}^*, [C^k]_{i,i} = 0 \text{ et } [B^k]_{i,i} = ([A]_{i,i})^k.}$$

(c) En exploitant la question IV.1 précédente, montrer que $\text{Tr}(A^p) = \text{Tr}(A) [p]$.

D'après la question 1. :

$$\text{Tr}(A^p) = \text{Tr}((B + C)^p) \equiv \text{Tr}(B^p) + \text{Tr}(C^p) [p]$$

Puis d'après 2.(b)

$$\text{Tr}(A^p) \equiv \sum_{i=1}^n [B^p]_{i,i} + \sum_{i=1}^n [C^p]_{i,i} = \sum_{i=1}^n ([A]_{i,i})^p + \sum_{i=1}^n 0 \equiv \sum_{i=1}^n [A]_{i,i} [p]$$

où l'on a utilisé pour finir le petit théorème de Fermat : $a^p \equiv a [p]$, pour tout entier relatif a .

$$\boxed{\text{Tr}(A^p) \equiv \text{Tr}(A) [p]}$$

(d) **Application à une suite récurrente.** En reprenant le résultat de la question I.4(b), établir une nouvelle preuve du fait que, pour tout nombre premier $p : p | u_p$ (cette fois sans passer par le calcul explicite de u_n en fonction de n).

On a vu que pour tout $n \in \mathbb{N}$, $u_n = \text{Tr}(A^n)$.

On a donc d'après la question précédente, pour p premier : $u_p = \text{Tr}(A^p) \equiv \text{Tr}(A) [p]$.

Or $\text{Tr}(A) = 0$, donc

$$\boxed{p | u_p}$$

IV.3. Application à une suite récurrente.

On rappelle que $A = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ -6 & 7 & 0 \end{pmatrix}$ et pour tout $n \in \mathbb{N}$, $u_n = \text{Tr}(A^n)$.

Montrer que l'on trouve bien pour tout nombre premier $p : p | u_p$.

On a donc pour tout nombre premier p :

$$\text{Tr}(A^p) \equiv \text{Tr}(A) = 0 [p]$$

$$\boxed{\text{Donc } p \text{ divise } \text{Tr}(A^p) = u_p.}$$

IV.4. Généralisation (cf bulletin vert du printemps 2024). On considère $A \in \mathcal{M}_n(\mathbb{Z})$

(a) Montrer que $\text{Tr}(A^{p^k}) \equiv \text{Tr}(A^{p^{k-1}}) [p^k]$

(b) Montrer que pour tout $n \in \mathbb{N}^*$, $\sum_{d|n} \text{Tr}(A^d) \mu\left(\frac{n}{d}\right) \equiv 0 [n]$

(c) Retour sur la suite ?