Polynôme annulateur & espace cyclique

Nous reprenons ici une grande partie du DS 7 de la saison 2020-2021.
A préparer pour vendredi 2 février (matin).

Notations :

— Dans toute cette partie, on note $\mathbb{K}$, un corps (qui est $\mathbb{R}$ en première partie).
Pour tout polynôme $\pi \in \mathbb{K}[X]$, on note (π) l'ensemble $\pi \cdot \mathbb{K}[X] = \{\pi \times Q, Q \in \mathbb{K}[X]\}$.

— n désigne un entier fixé dans tout le sujet et on fixe $M \in \mathcal{M}_n(\mathbb{R})$, une matrice carrée d'ordre n.

— On note $\mathbb{K}[M] = \{T(M), T \in \mathbb{K}[X]\}$, l'ensemble des polynômes en M.

Objectif :
On commence par se familiariser avec quelques notions ou sous-espaces à partir de trois exemples (partie I). Puis, on démontre quelques résultats sur l'arithmétique des polynômes : lien idéaux et division euclidienne (partie II). On exploite alors ces structures autour des polynômes en M, cela nous donne l'existence d'un polynôme minimal, annulateur de M (partie III). Enfin, en exploitant le lemme des noyaux, on optimise la majoration du degré du polynôme annulateur (partie IV).

A - Etude de cas particuliers

Dans cette partie, on se concentre sur trois matrices $A, C \in \mathcal{M}_3(\mathbb{R})$ et $B \in \mathcal{M}_4(\mathbb{R})$.
Dans les parties suivantes, elles pourront de nouveau être mobilisées.

$$A = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & -3 \\ 0 & 1 & 3 \end{pmatrix} \quad B = \frac{1}{2}\begin{pmatrix} 2 & 1 & -3 & 0 \\ 2 & -2 & -2 & -2 \\ 2 & 0 & -4 & -2 \\ -2 & 2 & 4 & 4 \end{pmatrix} \quad \text{et} \quad C = \begin{pmatrix} -2 & -1 & -10 \\ 2 & 1 & 8 \\ 1 & 1 & 3 \end{pmatrix}$$

1. Etude de A. On considère $X_1 = \begin{pmatrix} 1 \\ -2 \\ 1 \end{pmatrix}$ et $X_2 = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}$
   (a) Calculer AX_1 puis AX_2, A^2X_2 et A^3X_2.
   (b) On note $T_2 = X^3 - 3X^2 + 3X - 1$. Montrer que $T_2(A) \times X_2 = 0$ (colonne nulle)
   (c) Donner un polynôme de degré 1, $T_1 \in \mathbb{R}[X]$ tel que $T_1(A) \times X_1 = 0$ (colonne nulle)
   (d) Que valent $T_1 \wedge T_2$ (PGCD) et $T_1 \vee T_2$ (PPCM) ?
2. Etude de B.
   (a) La matrice B est-elle inversible ? Si oui, calculer B^{-1}.
   (b) Montrer que $B^4 = B^2$.
   (c) Pour tout $n \in \mathbb{N}, n \geqslant 4$, exprimer B^n. La formule reste-t-elle vraie pour $n = 3$?
3. Etude de C
   (a) Calculer C^2 et C^3.
   (b) On note $\pi = X^3 - 2X^2 - X + 2$. Montrer que $\pi(C) = 0$.
   (c) La matrice C est-elle inversible ? Si oui, calculer C^{-1}.
   (d) Pour tout $n \in \mathbb{N}$, exprimer C^n. La formule reste-t-elle vraie pour $n = -1$?
   (e) Montrer que pour tout $P \in \mathbb{R}_2[X]$ non nul, $P(C) \neq 0$.

B - Idéaux de $\mathbb{K}[X]$

Pour un anneau commutatif $(\mathcal{A}, +, \times)$, on dit que $\mathcal{I}(\subset \mathcal{A})$ est idéal de $\mathcal{A}$ si $(\mathcal{I}, +)$ est un sous-groupe de $(\mathcal{A}, +)$ et $\forall\ x \in \mathcal{I}\ \forall\ y \in \mathcal{A}$ et $x \times y \in \mathcal{I}$.
Ainsi, *pour démontrer que* $\mathcal{I}(\subset \mathcal{A})$ *est idéal de* $\mathcal{A}$, il suffit donc de montrer que :

— $\mathcal{I} \subset \mathcal{A}$
— $0_{\mathcal{A}} \in \mathcal{I}$ (élément neutre de l'addition)
— $\forall\ x_1, x_2 \in \mathcal{I}$, on a $x_1 - x_2 \in \mathcal{I}$
— $\forall\ x \in \mathcal{I}\ \forall\ y \in \mathcal{A}$, on a $x \times y \in \mathcal{I}$

1. Soit $\pi \in \mathbb{K}[X]$. Montrer que (π) est un idéal de $\mathbb{K}[X]$. (Définition de (π) en début d'énoncé)
2. Réciproquement, considérons un idéal $\mathcal{I}$ de $\mathbb{K}[X]$ non réduit à $\{0\}$.
   (a) Montrer que $\left\{ \deg P, P \in \mathcal{I} \setminus \{0\} \right\}$ admet un plus petit élément, noté r.
   (b) Soit $\pi \in \mathcal{I}$ tel que $\deg \pi = r$.
   Soit $S \in \mathcal{I}$, en exploitant la division euclidienne de S par π, montrer que $S \in (\pi)$.
   (c) En déduire que $\mathcal{I} = (\pi)$.

On dit que le polynôme π engendre l'idéal $\mathcal{I}$. Il n'y a qu'un seul polynôme unitaire qui engendre $\mathcal{I}$.

3. Structure de $\dfrac{\mathbb{K}[X]}{(\pi)}$ (défini plus loin). On fixe $\pi \in \mathbb{K}[X]$. On note $r = \deg \pi$
   Pour $M_1, M_2 \in \mathbb{K}[X]$, on note $M_1 \equiv M_2[\pi]$ si et seulement si $M_1 - M_2 \in (\pi)$
   (a) Montrer que $\equiv [\pi]$ est une relation d'équivalence sur $\mathbb{K}[X]$.

On note $\overline{M}$, la classe de M pour cette relation d'équivalence et $\dfrac{\mathbb{K}[X]}{(\pi)}$ l'ensemble de ces classes.

   (b) Soit $\varphi_\pi : \begin{array}{ccc} \mathbb{K}[X] & \to & \mathbb{K}_{r-1}[X] \\ Q & \mapsto & Q\%\pi \end{array}$ (reste de la division euclidienne de Q par π).
   Montrer que φ_π est surjective et que : $\varphi_\pi(M_1) = \varphi_\pi(M_2)$ ssi $M_1 \equiv M_2[\pi]$.

On en déduit que $\overline{\varphi_\pi} : \begin{array}{ccc} \dfrac{\mathbb{K}[X]}{(\pi)} & \longrightarrow & \mathbb{K}_{r-1}[X] \\ \overline{Q} & \longmapsto & Q\%\pi \end{array}$ est bien définie et est bijective.

   (c) Montrer que les opérations $\overline{+}$ et $\overline{\times}$ définies sur $\dfrac{\mathbb{K}[X]}{(\pi)}$ par :
   $$\overline{M_1} \,\overline{+}\, \overline{M_2} = \overline{M_1 + M_2} \quad \text{et} \quad \overline{M_1} \,\overline{\times}\, \overline{M_2} = \overline{M_1 \times M_2}$$
   sont bien opérantes (*i.e. indépendantes de représentants choisis pour chaque classe*).

<u>On admet</u> qu'ainsi $\left(\dfrac{\mathbb{K}[X]}{(\pi)}, \overline{+}, \overline{\times}\right)$ est un anneau.

   (d) Montrer que $\left(\dfrac{\mathbb{K}[X]}{(\pi)}, \overline{+}, \overline{\times}\right)$ est un corps si et seulement si π est irréductible.

<u>On admet</u> également que $\bar{\cdot}$ est bien définie sur $\mathbb{K} \times \dfrac{\mathbb{K}[X]}{(\pi)}$ comme opération externe (avec $\mathbb{K}$ comme domaine).

   (e) Montrer que $\left(\dfrac{\mathbb{K}[X]}{(\pi)}, \overline{+}, \bar{\cdot}\right)$ est un $\mathbb{K}$-espace vectoriel de dimension r.
   On pourra montrer que $\left(\overline{1}, \overline{X}, \ldots \overline{X^{r-1}}\right)$ *en est une base.*

C. Polynôme annulateur et polynômes conducteurs

On considère dans cette partie les deux espaces vectoriels $\mathcal{M} = \mathcal{M}_n(\mathbb{K})$ et $E = \mathcal{M}_{n,1}(\mathbb{K})$.
On fixe $M \in \mathcal{M}$ une matrice, on note $\mathcal{I}_M = \{P \in \mathbb{K}[X] \mid P(M) = 0_{\mathcal{M}}\}$ et $\mathbb{K}[M] = \{T(M), T \in \mathbb{K}[X]\}$.
Puis, pour toute matrice colonne $X \in E$, on note également $\mathcal{I}_{M,X} = \{P \in \mathbb{K}[X] \mid P(M) \times X = 0_E\}$ ainsi que $\mathbb{K}[M]X = \{T(M) \times X, T \in \mathbb{K}[X]\}$. En partie I, nous avions obtenu $T_1 \in \mathcal{I}_{A,X_1}$ et $T_2 \in \mathcal{I}_{A,X_2}$.

1. Espaces de dimensions finis (à *passer en première lecture*).
   (a) Quelles sont les dimensions des espaces $\mathcal{M}$ et E ?
   (b) On note $C(M) := \text{vect}\{M^k, k \in \mathbb{N}\}$. Montrer que $C(M) = \mathbb{K}[M]$ et est un sous-espace vectoriel de dimension finie de $\mathcal{M}$.
   On note $r_M = \dim C(M)$.

<u>On admet</u> également que $\mathbb{K}[M]X = \{T(M) \times X, T \in \mathbb{K}[X]\}$ est un sous-espace vectoriel de E.

   (c) Montrer $(C(M), +, \times)$ est un sous-anneau commutatif de $(\mathcal{M}, +, \times)$.

2. Idéaux
   (a) Montrer que $\mathcal{I}_M$ et $\mathcal{I}_{M,X}$ sont des idéaux de $\mathbb{K}[X]$.
   Lequel est inclus dans l'autre.

On appelle polynôme minimal de M, noté π_M, le polynôme de $\mathbb{K}[X]$ unitaire tel que $(\pi_M) = \mathcal{I}_M$.
On appelle polynôme conducteur de M en X (ou minimal de(M, X)), noté $\pi_{M,X}$, le polynôme de $\mathbb{K}[X]$ unitaire tel que $(\pi_{M,X}) = \mathcal{I}_{M,X}$.

   (b) Montrer que la famille $\left(I_n, M, M^2, \dots M^{\deg \pi_M - 1}\right)$ est libre.
   (c) Montrer que $C(M) = \text{vect}\left(I_n, M, M^2, \dots M^{\deg \pi_M - 1}\right)$.
   On pourra exploiter une division euclidienne par π_M.
   (d) En déduire que $\deg \pi_M = r_M$ (défini en 1.(b)). Quelle majoration pour $\deg \pi_M$ obitent-on ?
   (e) Montrer que $\pi_{M,X} | \pi_M$ (divise)

D. Lemme des noyaux

Soit M une matrice de $\mathcal{M}$ et π_M son polynôme minimal.

On suppose que π_M se décompose en produit d'irréductibles : $\pi_M = \prod_{i=1}^{s} P_i^{\alpha_i}$

où pour tout $i \in \mathbb{N}_s$, P_i est unitaire irréductible dans l'anneau euclidien $\mathbb{K}[X]$ et $\alpha_i \in \mathbb{N}^*$.
On note, pour tout $i \in \mathbb{N}_s$, $K_i = \{X \in E \mid P_i^{\alpha_i}(M) \times X = 0\}$, c'est un sous espace vectoriel de E.

1. On commence par montrer le lemme des noyaux : $E = K_1 \oplus K_2 \cdots \oplus K_s$.
   Pour cela on note pour tout $i \in \mathbb{N}_s$, $Q_i = \prod_{j \in \mathbb{N}_s \setminus \{i\}} P_j^{\alpha_j}$. On a donc $P_i^{\alpha_i} Q_i = \pi_M$
   (a) En exploitant une relation de Bézout, montrer que
   $$\forall\ i \in \mathbb{N}_s, \exists\ U_i \in \mathbb{K}[X] \text{ tel que } I_n = \sum_{i=1}^{s} U_i(M) Q_i(M)$$
   (b) En déduire que pour tout $X \in E$, il existe $(N_i)_{i \in \mathbb{N}_s} \in K_1 \times K_2 \cdots \times K_s$ tel que : $X = \sum_{i=1}^{s} N_i$.
   (c) Qu'en déduit-on pour la somme $K_1 + K_2 + \cdots + K_s$?
   (d) On considère maintenant $(x_1, x_2, \cdots x_s) \in K_1 \times K_2 \cdots \times K_s$ tel que $\sum_{i=1}^{s} x_i = 0$.
   Montrer que pour tout $i \in \mathbb{N}_s$, $x_i = 0$.
   On pourra commencer par montrer que $Q_j(M) x_i = 0$ si $i \neq j$, puis également $j = i$ et exploiter la relation trouvée en 1.(a).
   (e) Qu'en déduit-on pour la somme $K_1 + K_2 + \cdots + K_s$?
2. <u>On admet</u> que *si une matrice $A \in \mathcal{M}$ n'est pas inversible,*
   alors il existe $X \in E$ tel que $AX = 0$ (colonne nulle) - résultat démontré en cours mardi.
   (a) Montrer que si $\pi_M = P_1 \times P_2$, avec $\deg P_1 > 0$, alors nécessairement $P_1(M)$ n'est pas inversible.
   (b) En exploitant le résultat admis ici, montrer que pour tout $i \in \mathbb{N}_s$, $K_i \neq \{0\}$.
   (c) (*) Supposons que pour tout $X \in E$ tel que $P_i^{\alpha_i}(M) \times X = 0$, on ait $P_i^{\alpha_i - 1}(M) \times X = 0$. Montrer qu'on a alors le résultat contradictoire $\frac{\pi_M}{P_i}(M) = 0$.
   En déduire l'existence de $X \in K_i$ tel que $P_i^{\alpha_i - 1}(M) \times X \neq 0$.

Pour tout $i \in \mathbb{N}_s$, on considère un élément $X_i \in K_i$ tel que $P_i^{\alpha_i - 1}(M) \times X \neq 0$

3. On montre maintenant qu'il existe $X \in \mathcal{M}_{n,1}(\mathbb{K})$ tel que $\pi_M = \pi_{M,X}$
   (a) Montrer que le polynôme conducteur de M en X_i est $\pi_{M,X_i} = P_i^{\alpha_i}$
   (b) On rappelle que pour tout $i \in \mathbb{N}_s$, on note $\mathbb{K}[M]X_i = \{P(M) \times X_i, P \in \mathbb{K}[X]\}$.
   Montrer que $\mathbb{K}[M]X_i \subset K_i$.
   (c) En déduire qu'on a la somme directe : $\bigoplus_{h \in \mathbb{N}_s} \mathbb{K}[M]X_h$ (à *passer en première lecture*).
   (d) On note $X = \sum_{h \in H} X_h$. Montrer que $\pi_{M,X} = \bigvee_{h \in H} \pi_{M,X_h}$ (PPCM).

(e) Qu'en déduire concernant le degré de π_M ?

4. Pré-décomposition de Fröbenius.
   On fixe $i \in \mathbb{N}_s$ et on note $d_i = \deg P_i^{\alpha_i}$.
   (a) Montrer que $(X_i, MX_i, \dots M^{d_i-1}X_i)$ est une famille libre.
   (b) On note R_i, la matrice de $\mathcal{M}_{n,d_i}(\mathbb{K})$ tel que pour tout $j \in \mathbb{N}_{d_i}$, $C_j(R_i) = M^{j-1}X_i$.
   Evaluer (par produit en bloc de colonnes) la matrice $M \times R_i$.
   (c) Donner une matrice F_i « simple »de $\mathcal{M}_{d_i}(\mathbb{K})$ telle que $M \times R_i = R_i \times F_i$.

F_i s'appelle la matrice compagnon du polynôme $P_i^{\alpha_i}$.
En combinant bien toutes les matrices F_i, on obtient la décomposition de Fröbenius de M.

Remarques !

Quel lien entre les résultats trouvés ici et le théorème de Dirichlet ?

1. *On montre ici que si $a \wedge N \neq 1$, alors il y a au plus un nombre premier de la forme $a + kN$.*
   *On se place donc dans la situation $a \wedge N = 1$. On peut rendre nul les autres cas : règle **B**.*
2. *Comme on s'intéresse à l'ensemble $\mathcal{P}_{a,N} = \{p \in \mathcal{P} \mid p \equiv a[N]\}$, on ne différencie pas ces nombres.*
   *C'est pourquoi on vise $\chi(p_1) = \chi(p_2)$ si $p_1 \equiv p_2 (\equiv a)[N]$: règle **D**.*
3. *La « clé d'or »est une formule d'Euler, reprise par Riemann :*

$$\zeta(s) = \sum_{n=1}^{+\infty} \frac{1}{n^s} = \prod_{p \in \mathcal{P}} \frac{1}{1 - \frac{1}{p^s}}$$

   généralisée par Dirichlet en

$$L(s, \chi) = \sum_{n=1}^{+\infty} \frac{\chi(n)}{n^s} = \prod_{p \in \mathcal{P}} \frac{1}{1 - \frac{\chi(p)}{p^s}}$$

   *par la condition que χ soient complètement multiplicative : règle **C**.*
   Nous établirons cette égalité lors du DM sur les séries (chapitre 27).
4. *Cette formule permet de différencier les nombres premiers selon les valeurs de $\chi(p)$, caractéristiques des ensembles $\mathcal{P}_{a,N} = \{p \in \mathcal{P} \mid p \equiv a[N]\}$.*
   On exploite des propriétés algébriques pour inverser la relation de Dirichlet (avec la série L, dérivée logarithmiquement...).
5. *La convergence de la série $\displaystyle\sum_{n \geqslant 1} \frac{\chi(n)}{n}$, avec divergence de la série $\displaystyle\sum_{n \geqslant 1} \frac{|\chi(n)|}{n}$ donne pour condition nécessaire l'infinité des nombres premiers p dont chaque $\chi(p)$ a une même valeur ($\chi(a)$ par exemple).*
6. *Et mieux. En exploitant les méthodes d'analyse asymptotiques, La Vallée-Poussin, démontre mieux : la répartition des nombres premiers dans les classes d'équivalence $\mathcal{P}_{a,N}$ est uniforme (égale pour chaque classe ou encore : indépendante de a).*
   Ainsi, si on note $\Pi(a, N, x) = card\{p \in \mathcal{P} \mid p \leqslant x \,\&\, p \equiv a[N]\}$, on a

$$\Pi(a, N, x) \sim_{x \to \infty} \frac{x}{\varphi(N) \ln x}$$

7. *Une question résiste à notre niveau : comment construire la fonction χ ?*
   *Avec l'existence de a tel que $\chi(a) \notin \{0, 1\}$...(critère **E**). Une piste est donnée en question C.5.*

Problème - Caractères de Dirichlet

A - Indicatrice d'Euler

1. Pour tout entier N, $1 \in \mathcal{P}_N$, donc

$$\boxed{\forall\ N \in \mathbb{N}^*,\ \varphi(N) \geqslant 1}$$

$$\varphi(N) = 1 \iff \mathcal{P}_N = \{1\}$$

Or pour tout $N \geqslant 2$, $N-1 \in \mathcal{P}_N$, car $(N \wedge N-1)|N$ et $(N \wedge N-1)|N-1$ donc $(N \wedge N-1)|1$.
Ainsi, pour tout $N \geqslant 2$, $\varphi(N) = 1 \Longrightarrow N-1 = 1 \Longrightarrow N = 2$.
Réciproquement, comme $\varphi(2) = 1$ et $\varphi(1) = 1$;

$$\boxed{\text{les seuls entiers pour lesquels } \varphi(N) = 1 \text{ sont 1 et 2}}$$

2. Si p est un nombre premier, alors tous les entiers de 1 à $p-1$ sont premiers avec p ;
et ce n'est pas le cas de p.

$$\boxed{\varphi(p) = p-1}$$

Soit $n \in \mathbb{N}^*$. Soit $a \in [\![1, p^n]\!]$.
On note $\delta = a \wedge p^n$. Alors $\delta | p^n$, donc $\delta = p^m$ avec $m \in [\![0, n]\!]$.
Ainsi on a les équivalences :

$$a \notin \mathcal{P}_{p^n} \iff \delta \neq 1 \iff \exists\ m \in [\![1, n]\!] \text{ tel que } \delta = p^m \iff p|a$$

Donc $\mathcal{P}_{p^n} = [\![1, p^n]\!] \setminus (p\mathbb{Z}) = [\![1, p^n]\!] \setminus \{rp \mid 1 \leqslant r \leqslant p^{n-1}\}$.

$$\boxed{\forall\ n \in \mathbb{N}^*,\ \varphi(p^n) = \text{Card}(\mathcal{P}_{p^n}) = (p^n - 1 + 1) - (p^{n-1} - 1 + 1) = p^n - p^{n-1} = p^{n-1}(p-1)}$$

Piste de recherche...
Il s'agit donc de montrer une égalité entre fonctions définie comme cardinaux d'ensembles.
Dans cette situation, le plus courant est de montrer la bijectivité entre les deux ensembles.
Ici il s'agit du théorème dit « lemme des restes chinois ». Nous avons vu dans l'exercice 212.

$$P : \begin{array}{ccc} \mathcal{P}_{N_1N_2} & \longrightarrow & \mathcal{P}_{N_1} \times \mathcal{P}_{N_2} \\ a & \longmapsto & (a\%N_1, a\%N_2) \end{array}$$

mais faut-il s'assurer qu'elle est bien définie ; puis qu'elle est bien bijective.

(a) Soient N_1 et N_2 deux nombres premiers entre eux.
Soit $a \in \mathcal{P}_{N_1N_2}$. Donc $a \wedge N_1N_2 = 1$. Donc $\exists\ u, v \in \mathbb{Z}$ tel que $ua + vN_1N_2 = 1$
Soit $a_1 = a\%N_1$. Donc $a_1 \in [\![0, N_1 - 1]\!]$ et il existe $k_1 \in \mathbb{Z}$ tel que $a = k_1N_1 + a_1$, donc

$$1 = ua + vN_1N_2 = ua_1 + (uk_1 + vN_2)N_1 \qquad \Longrightarrow \qquad a_1 \wedge N_1 = 1$$

Ainsi $a_1 \in \mathcal{P}_{N_1}$.
Et de même si on note $a_2 = a\%N_2$, alors $a_2 \in [\![0, N_2 - 1]\!]$ et $a_2 \wedge N_2 = 1$, donc $a_2 \in \mathcal{P}_{N_2}$.

$$\boxed{\text{L'application } P : \begin{array}{ccc} \mathcal{P}_{N_1N_2} & \longrightarrow & \mathcal{P}_{N_1} \times \mathcal{P}_{N_2} \\ a & \longmapsto & (a\%N_1, a\%N_2) \end{array} \text{ est donc bien définie}}$$

(b) Soient $a, a' \in \mathcal{P}_{N_1N_2}$ tel que $P(a) = P(a')$.
Donc $a\%N_1 = a'\%N_1$, ainsi $N_1|(a - a')$. De même $N_2|(a - a')$.
Et comme $N_1 \wedge N_2 = 1$, d'après un lemme de Gauss $N_1N_2|(a - a')$.
Or $a, a' \in \mathcal{P}_{N_1N_2}$, donc $a - a' \in [\![2 - N_1N_2, N_1N_2 - 2]\!]$.
Le seul nombre divisible par N_1N_2 de cet intervalle est 0. Donc $a - a' = 0$.
Par conséquent $a = a'$ et P est injectif.

Piste de recherche...

Pour montrer la surjectivité, on considère a_1 et a_2 et on essaye de construire le nombre a tel que $P(a) = (a_1, a_2)$.
On se rend compte que $a = a_1 + k_1N_1 = a_2 + k_2N_2$, donc $a_1 - a_2 = k_2N_2 - k_1N_1$.
Cela nous fait penser à la décomposition de Bézout...

Soit $(a_1, a_2) \in \mathcal{P}_{N_1} \times \mathcal{P}_{N_2}$.
$N_1 \wedge N_2 = 1$. Il existe $u_1, u_2 \in \mathbb{Z}$ tel que $u_1N_1 + u_2N_2 = 1$.
Donc en multipliant par $a_1 - a_2$: $(a_1 - a_2)u_1N_1 + (a_1 - a_2)u_2N_2 = a_1 - a_2$.
Il existe $U_1(= (a_2 - a_1)u_1), U_2(= (a_1 - a_2)u_2) \in \mathbb{Z}$ tels que $U_1N_1 + a_1 = U_2N_2 + a_2$.
On note $A = U_1N_1 + a_1$, puis $a = A\%N_1N_2$.
Donc $a \in [\![0, N_1N_2 - 1]\!]$.
Puis si $\delta|a$ et $\delta|N_1N_2$, alors $\delta|A = a + KN_1N_2$.
Comme $N_1 \wedge N_2 = 1$, alors $\delta|N_1$ ou $\delta|N_2$.
Sans perte de généralité, supposons que $\delta|N_1$,
comme $\delta|A = U_1N_1 + a_1$, alors $\delta|N_1$ et $\delta|a_1$. Donc $\delta = 1$.
Donc $a \in \mathcal{P}_{N_1N_2}$.
Enfin, par construction, $a_1 \equiv A \equiv a[N_1]$ et $a_2 \equiv A \equiv a[N_2]$.
Donc il existe $a \in \mathcal{P}_{N_1N_2}$ tel que $P(a) = (a_1, a_2)$: P est surjective de $\mathcal{P}_{N_1N_2}$ sur $\mathcal{P}_{N_1}\mathcal{P}_{N_2}$.

L'application P est bijective

$\varphi(N_1) \times \varphi(N_2)$ est le cardinal du produit cartésien $\mathcal{P}_{N_1} \times \mathcal{P}_{N_2}$. Ainsi, il y a égalité des cardinaux :

$$\forall\ N_1, N_2 \in \mathbb{N},\ \text{tels que } N_1 \wedge N_2 = 1 \text{ alors } \varphi(N_1N_2) = \varphi(N_1)\varphi(N_2)$$

Remarques !

En fait l'application P est un morphisme bijectif de groupes,
du groupe des inversibles de $\frac{\mathbb{Z}}{N_1N_2\mathbb{Z}}$, i.e. $\left(\frac{\mathbb{Z}}{N_1N_2\mathbb{Z}}\right)^*$, de cardinal $\varphi(N_1N_2)$,
sur le groupe, produit cartésien, $\left(\frac{\mathbb{Z}}{N_1\mathbb{Z}}\right)^* \times \left(\frac{\mathbb{Z}}{N_2\mathbb{Z}}\right)^*$ de cardinal $\varphi(N_1)\varphi(N_2)$.

Remarques !

Avec la formule multiplicative et l'expression sur les puissances des nombres premiers, on montre que
si $n = \prod_{i=1}^{r} p_i^{n_i}$, alors

$$\varphi(n) = \prod_{i=1}^{r} p_i^{n_i}(1 - \frac{1}{p_i} = n\prod_{p|n}\left(1 - \frac{1}{p}\right)$$

4. Soit $N \in \mathbb{N}^*$. Soit $a \in \mathcal{P}_N$.
   (a) Soit $k \in \mathcal{P}_N$. Par définition $ka\%N \in [\![0, N]\!]$.
   Or $k \wedge N = 1$, $a \wedge N = 1$, donc d'après un lemme de Gauss (facteurs relativement premiers) :
   $ak \wedge N = 1$.

   Donc, pour tout $k \in \mathcal{P}_N$, $ka\%N \in \mathcal{P}_N$

   (b) On définit alors :

$$\psi_a : \mathcal{P}_N \to \mathcal{P}_N,\ k \mapsto ka\%N$$

Supposons que $\psi_a(k) = \psi_a(k')$, alors $N|(k - k')a$.
Donc, comme $N \wedge a = 1$, $N|k - k'$. Ainsi : $k - k' \in [\![2 - N, N - 2]\!] \cap (N \cdot \mathbb{Z}) = \{0\}$.
Ainsi $k = k'$ et donc ψ_a est injective.
Soit $h \in \mathcal{P}_N$. Comme $a \wedge N = 1$, alors d'après le théorème de Bézout,
il existe $u, v \in \mathbb{Z}$ tel que $ua + vN = 1$.
Donc en multipliant par h : $(hu)a + hvN = h$, et modulo N : $(hu)a \equiv h[n]$.
Enfin, en prenant $k = hu\%N$, on a donc $k \times a = h$;
et $u \wedge N = 1$, $h \wedge N = 1$, donc $hu \wedge N = 1$ et $k \wedge N = 1$.
Ainsi il existe $k \in \mathcal{P}_N$ tel que $a \times k = h$. Donc ψ_a est surjective.

ψ_a est bijective

Remarques !

Comme les ensembles de départ et d'arrivée de ψ_a sont finis, et qu'ils ont le même cardinal (ce sont les mêmes), on peut démontrer que

ψ_a est bijective si et seulement ψ_a est injective ou ψ_a est surjective.

On aurait donc pu réduire l'étude précédente.

Piste de recherche...

On applique exactement la même démonstration que pour le théorème de Fermat, mais avec moins de nombres (au lieu de prendre tous les nombres de 1 à $N-1$, on prend ceux de $\mathcal{P}_N$

Soit $a \in \mathcal{P}_N$:

$$\prod_{k\in\mathcal{P}_N} ka = a^{\text{card}(\mathcal{P}_N)} \prod_{k\in\mathcal{P}_N} k = a^{\varphi(N)} \prod_{k\in\mathcal{P}_N} k$$

Mais aussi :

$$\prod_{k\in\mathcal{P}_N} ka = \prod_{k\in\mathcal{P}_N} \psi_a(k) = \prod_{h\in\mathcal{P}_N} h$$

Comme $N \wedge h = 1$, pour tout $h \in \mathcal{P}_N$, alors (Gauss) : $N \wedge (\prod_{h\in\mathcal{P}_N} h) = 1$. Donc

$$a^{\varphi(N)} \prod_{k\in\mathcal{P}_N} k = \prod_{h\in\mathcal{P}_N} h \qquad \Longrightarrow a^{\varphi(N)} \equiv 1[N]$$

Si $A \in \mathbb{Z}$ et $A \wedge N = 1$, alors en prenant $a = A\%N$, on a $a \equiv A[N]$ donc $a \wedge N = 1$.

Puis, pour tout $k \in \mathbb{N}$, $A^k = (a+hN)^k = \sum_{i=0}^{k} \binom{k}{i} a^i (hN)^{k-i} \equiv a^k[N]$.

Et donc $A^{\varphi(N)} \equiv a^{\varphi(N)} \equiv 1[N]$.

$$\boxed{\forall\, a \in \mathbb{N}, \qquad a \wedge N = 1 \Longrightarrow a^{\varphi(N)} \equiv 1[N]}$$

Remarques !

On retrouve pour p premier, le petit théorème de Fermat :

$\varphi(p) = p-1$ et donc $a^{p-1} \equiv 1[p]$

B - Etude de arctan

On étudie ici la fonction arctan, de classe $\mathcal{C}^\infty$ sur $\mathbb{R}$ (résultat du cours).
On note également ici :

$$A : \mathbb{R} \to \mathbb{C},\ x \mapsto \frac{1}{1-ix}$$

1. A est une fraction rationnelle et son ensemble de définition est $\mathbb{R}$.

$$\boxed{\text{Donc } A \text{ est de classe } \mathcal{C}^\infty \text{ sur } \mathbb{R}.}$$

Posons, pour tout $k \in \mathbb{N}$, $\mathcal{P}_k$: « $\forall\, x \in \mathbb{R}$, $A^{(k)}(x) = \dfrac{k!i^k}{(1-ix)^{k+1}}$ ».

— Pour tout $x \in \mathbb{R}$, $A^{(0)}(x) = A(x) = \dfrac{1}{1-ix} = \dfrac{0!i^0}{(1-ix)^{0+1}}$, donc $\mathcal{P}_0$ est vraie.

— Soit $k \in \mathbb{N}$. On suppose que $\mathcal{P}_k$ est vraie.

Donc pour tout $x \in \mathbb{R}$, $A^{(k)}(x) = \dfrac{k!i^k}{(1-ix)^{k+1}}$. On applique l'algorithme de dérivation :

$$\forall\, x \in \mathbb{R}, \qquad A^{(k+1)}(x) = \frac{-k!i^k \times (k+1) \times (-i)}{(1-ix)^{k+1+1}} = \frac{(k+1)!i^{k+1}}{(1-ix)^{k+2}}$$

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

$$\boxed{\forall\ k \in \mathbb{N}, \forall\ x \in \mathbb{R},\ A^{(k)}(x) = \frac{k! i^k}{(1-ix)^{k+1}}}$$

2. Pour tout $x \in \mathbb{R}$, $\arctan'(x) = \dfrac{1}{1+x^2}$.
Puis $\mathrm{Re}(A(x)) = \dfrac{1}{2}(A(x) + \overline{A(x)}) = \dfrac{1}{2}\left(\dfrac{1}{1-ix} + \dfrac{1}{1+ix}\right) = \dfrac{1+ix+1-ix}{2(1+x^2)} = \dfrac{1}{1+x^2}$

$$\boxed{\text{Pour tout } x \in \mathbb{R},\ \arctan'(x) = \mathrm{Re}(A(x)).}$$

Puis par linéarité de la dérivation, pour tout $k \in \mathbb{N}$:

$$\arctan^{(k+1)} = (\arctan')^{(k)} = \left(\frac{1}{2}(A + \overline{A})\right)^{(k)} = \frac{1}{2}\left(A^{(k)} + \overline{A^{(k)}}\right) = \mathrm{Re}\left(A^{(k)}\right)$$

$$\boxed{\forall\ k \in \mathbb{N}, \quad \arctan^{(k+1)}(0) = \mathrm{Re}\left(\frac{k! i^k}{(1-0)^{k+1}}\right) = \begin{cases} 0 & \text{si } k = 2p+1 \\ (-1)^p (2p)! & \text{si } k = 2p \end{cases}}$$

3. (a) Soit $x \in]0,1]$. Considérons

$$\begin{aligned} h_N : t \ \mapsto\ & \arctan(x) - \sum_{k=0}^{N} \frac{\arctan^{(k)}(t)}{k!}(x-t)^k - R_N \frac{(x-t)^{N+1}}{(N+1)!} \\ & = \arctan(x) - \left(\arctan t + \frac{\arctan'(t)}{1}(x-t) + \ldots \frac{\arctan^{(n)}(t)}{n!}(x-t)^n\right) - R_N \frac{(x-t)^{N+1}}{(N+1)!} \end{aligned}$$

où R_N est choisi de manière à ce que $h_N(0) = 0$ i.e. $R_N = \dfrac{(N+1)!}{x^{N+1}}\left(\arctan(x) - \displaystyle\sum_{k=0}^{n} \frac{\arctan^{(k)}(0)}{k!} x^k\right)$.
Par ailleurs $h_N(x) = \arctan(x) - \arctan(x) = 0$.
Donc d'après le théorème de Rolle ($h_N(0) = h_N(x) = 0$), il existe $c \in]0, x[$ tel que $h'_N(c) = 0$.
Or, par télescopage

$$\begin{aligned} h'_N(t) = \ & -\left(\sum_{k=0}^{N} \frac{\arctan^{(k+1)}(t)}{k!}(x-t)^k - \frac{\arctan^{(k)}(t)}{(k-1)!}(x-t)^{k-1}\right) + \frac{R_N}{N!}(x-t)^N \\ & = -\frac{\arctan^{(N+1)}(t)}{N!}(x-t)^N + \frac{R_N}{N!}(x-t)^N \end{aligned}$$

Comme $h'_N(c) = 0$, on a donc $R_N = \arctan^{(N+1)}(c)$.
Enfin comme $h_N(0) = 0$, on a donc (en $t = 0$) :

$$\boxed{\forall\ x \in]0,1], \exists\ c_x \in]0, x[\text{ tel que } \arctan(x) = \sum_{k=0}^{N} \frac{\arctan^{(k)}(0)}{k!} x^k + \frac{\arctan^{N+1}(c_x)}{(N+1)!} x^{N+1}}$$

(b) En $x = 1$ et $N = 2p$, avec la formule de $\arctan^{(k)}(0)$ trouvée plus haut :
Il existe $c_1 \in]0, 1[$ tel que

$$\begin{aligned} \frac{\pi}{4} \ & = \arctan(0) + \sum_{k=0}^{p-1}\left(\frac{\arctan^{(2k+1)}(0)}{(2k+1)!} 1^{2k+1} + \frac{\arctan^{(2k+2)}(0)}{(2k+2)!} 1^{2k+2}\right) + \frac{\arctan^{2p+1}(c_1)}{(2p+1)!} 1^{2p+1} \\ & = \sum_{k=0}^{p} \frac{(-1)^k (2k)!}{(2k+1)!} + \frac{1}{(2p+1)!} \mathrm{Re}\left(A^{2p}(c_1)\right) \end{aligned}$$

$$\boxed{\exists\ c_1 \in]0,1[\text{ tel que } \frac{\pi}{4} = \sum_{k=0}^{p} \frac{(-1)^k}{2k+1} + \frac{1}{2p+1} \mathrm{Re}\left(\frac{i^{2p}}{(1-ic_1)^{2p}}\right)}$$

(c) Comme

$$\left|\mathrm{Re}\left(\frac{i^{2p}}{(1-ic_1)^{2p}}\right)\right| \leqslant \left|\frac{i^{2p}}{(1-ic_1)^{2p}}\right| = \left(\frac{|i|}{|1-ic_1|}\right)^{2p} = \left(\frac{1}{|1-ic_1|}\right)^{2p} \leqslant 1$$

car $|1-ic_1| = \sqrt{1+c_1^2} \geqslant 1$. Alors par théorème d'encadrement :

$$\boxed{\lim_{p\to\infty} \sum_{k=0}^{p} \frac{(-1)^k}{2k+1} = \frac{\pi}{4}}$$

C. Caractères. Cas particuliers : $N = 2$ et $N = 4$

1. Soit $N \in \mathbb{N}$. D'après la règle **C**, pour tout entier a, $\chi_N(a) = \chi_N(1 \times a) = \chi_N(1)\chi_N(a)$.
Or χ_N est non identiquement nul (règle **A**), donc il existe $a \in \mathbb{N}$, tel que $\chi_N(a) \neq 0$.

   Et nécessairement $\chi_N(1) = 1$, pour tout entier $N \in \mathbb{N}$.

2. Notons $\delta = a \wedge N$ et supposons que $\delta \neq 1$. Soit $p \in \{p \in \mathcal{P} \mid p \equiv a[N]\}$.
Alors $p = a + kN = \delta(a_1 + kN_1)$, donc $\delta | p$. Or p est premier donc $\delta = 1$ ou $\delta = p$.
Comme $\delta \neq 1$, on a donc $\delta = p$.

   Si $a \wedge N \neq 1$, $\{p \in \mathcal{P} \mid p \equiv a[N]\}$ contient 1 élément : $a \wedge N$ si $a \wedge N \in \mathcal{P}$ et 0 sinon

   Par contraposée :

   $\{p \in \mathcal{P} \mid p \equiv a[N]\} = +\infty \Longrightarrow a \wedge N = 1 \Longrightarrow \chi_N(a) \neq 0$ (Règle **B**).

3. On suppose $N = 2$. Par 2-parité :

$$\chi_2 : m \mapsto \begin{cases} 0 & \text{si } m \equiv 0[2] \\ 1 & \text{si } m \equiv 1[2] \end{cases}$$

4. (a) $\chi_4(9) = \big(\chi_4(3)\big)^2 = \chi_4(1 + 2 \times 4) = \chi_4(1) = 1$.

   $\chi_4(3)$ ne peut prendre que les valeurs 1 ou -1.

   (b) On suppose maintenant $\chi_4(3) = -1$.
$\chi_4(2) = 0$, car $2 \wedge 4 = 2 \neq 1$. Donc par 4-parité :

$$\chi_4 : m \mapsto \begin{cases} 0 & \text{si } m \equiv 0[2] \\ 1 & \text{si } m \equiv 1[4] \\ -1 & \text{si } m \equiv 3[4] \end{cases}$$

   Donc, pour tout entier $s \in \mathbb{N}$, en notant $s = 4q_s + r_s$ (division euclidienne par 4)

$$\sum_{n=1}^{s} \frac{\chi(n)}{n} = \sum_{k=0}^{q_s-1} \left(\frac{\chi(1+4k)}{1+4k} + \frac{\chi(2+4k)}{2+4k} + \frac{\chi(3+4k)}{3+4k} + \frac{\chi(4+4k)}{4+4k}\right) + \sum_{h=1}^{r_s} \frac{\chi(4q_s+h)}{4q_s+h}$$

   (si $r_s = 0$, la dernière somme est nulle car vide.).
Ainsi, selon les valeurs de χ :

$$\sum_{n=1}^{s} \frac{\chi(n)}{n} = \sum_{k=0}^{q_s-1} \left(\frac{1}{1+4k} + \frac{-1}{3+4k}\right) + \sum_{h=1}^{r_s} \frac{\chi(4q_s+h)}{4q_s+h} = \sum_{j=0}^{2(q_s-1)} \frac{(-1)^j}{1+2j} + \sum_{h=1}^{r_s} \frac{\chi(4q_s+h)}{4q_s+h}$$

Comme, pour $s \to \infty$, $q_s \to \infty$:

$$\left|\sum_{h=1}^{r} \frac{\chi(4q_s+h)}{4q_s+h}\right| \leqslant \frac{2}{4q_s} \underset{s\to\infty}{\longrightarrow} 0$$

Donc, d'après la partie B. :

$$\boxed{\left(\sum_{n=1}^{s} \frac{\chi(n)}{n}\right)_n \text{ converge et } \lim_{s\to\infty} \sum_{n=1}^{s} \frac{\chi(n)}{n} = \frac{\pi}{4}}$$

5. (a) On suppose qu'il existe $a \in \mathcal{P}_N$ tel que $\{(a^k)\%N, k \in [\![1, \varphi(N)]\!]\} = \mathcal{P}_N$.
Il faut d'abord vérifier que χ_N^a est bien définie.
Si $t \in \mathbb{Z}$:
- ou bien $t \wedge N \neq 1$
- ou bien $t \wedge N = 1$ et dans ce cas, $t\%N \in \mathcal{P}_N$
  et donc il existe $k \in [\![1, \varphi(N)]\!]$ tel que $a^k\%N = t\%N$ i.e. $a^k \equiv t[N]$.

Les critères **A**, **B** et **D** sont évidents, par construction de χ_N^a.
Soient $b_1, b_2 \in \mathcal{P}_N$. Soit $k_1, k_2 \in [\![1, \varphi(N)]\!]$ tel que $b_1 = a^{k_1}\%N$ et $b_2 = a^{k_2}\%N$.
Alors $b_1 \times b_2 = a^{k_1+k_2}\%N$.
- Ou bien $k_1 + k_2 \leqslant \varphi(N)$
  et donc $\chi_N^a(b_1b_2) = \exp(2i\pi\frac{k_1+k_2}{\varphi(N)}) = \exp(2i\pi\frac{k_1}{\varphi(N)}) \times \exp(2i\pi\frac{k_2}{\varphi(N)}) = \chi(b_1) \times \chi(b_2)$
- Ou bien $k_1 + k_2 \geqslant \varphi(N)$
  et donc $\chi_N^a(b_1b_2) = \exp(2i\pi\frac{k_1+k_2-\varphi(N)}{\varphi(N)}) = \exp(2i\pi\frac{k_1+k_2}{\varphi(N)}) = \chi(b_1) \times \chi(b_2)$

Dans tous les cas, le critère **B** est également vérifié.

$$\boxed{\text{Donc } \chi_N^a : t \mapsto \begin{cases} 0 & \text{si } t \wedge N \neq 1 \\ \exp(2i\pi\frac{k_t}{\varphi(N)}) & \text{avec } t \equiv (a^{k_t})[N] \end{cases} \text{ est un caractère de Dirichlet.}}$$

(b) $\chi_N^a(a) = \exp(2i\pi\frac{1}{\varphi(N)}) \notin \{0, 1\}$.

$$\boxed{\text{Donc } \chi_N^a \text{ vérifie également le critère } \mathbf{E}.}$$

(c) $\varphi(6) = \varphi(2 \times 3) = 1 \times 2$. $\mathcal{P}_6 = \{1, 5\}$.

$$\boxed{\text{On peut (doit) considérer } \chi_6 : t \mapsto \begin{cases} -1 & \text{si } m \equiv 5[6] \\ 1 & \text{si } m \equiv 1[6] \\ 0 & \text{sinon} \end{cases}}$$

$\varphi(7) = 6$. $\mathcal{P}_7 = \{1, 2, 3, 4, 5, 6\}$.
On vérifie que $a = 2$ ne marche pas $2^3\%1[7]$.
Mais $a = 3$ fonctionne : $((3^k)\%7) = (3, 2, 6, 4, 5, 1)$.
On note $\alpha = e^{i\pi/3} (= -j^2)$, racine 6-ième primitive de l'unité

$$\boxed{\text{On peut considérer } \chi_7 : t \mapsto \begin{cases} 0 & \text{si } m \equiv 0[7] \\ 1 & \text{si } m \equiv 1[7] \\ \alpha^2 = j & \text{si } m \equiv 2[7] \\ \alpha = -j^2 & \text{si } m \equiv 3[7] \\ \alpha^4 = j^2 & \text{si } m \equiv 4[7] \\ \alpha^5 = -j & \text{si } m \equiv 5[7] \\ \alpha^3 = -1 & \text{si } m \equiv 6[6] \end{cases}}$$

D. Convergence de la série $\sum_{n\geqslant 1}\frac{\chi(n)}{n}$

1. Soit $a\in\mathcal{P}_N$. Par propriété multiplicative de χ, comme $a^{\varphi(N)}=1$:

$$1=\chi(1)=\chi\left(a^{\varphi(N)}\right)=[\chi(a)]^{\varphi(N)}$$

> Donc $\chi(a)$ est une racine $\varphi(N)$-ième de l'unité et ainsi $|\chi(a)|=1$

Remarques !
$\varphi(4)=\varphi(2^2)=2\times(2-1)=2$. Donc $\chi_4(3)$ est une racine deuxième (carrée) de l'unité.
On retrouve bien $\chi_4(3)=\pm 1$

2. Soit $a\in\mathcal{P}_N$ et $\overline{\psi_a}:[\![1,N-1]\!]\to[\![1,N-1]\!]$, $k\mapsto ak\%N$.
On reprend la même démonstration qu'en A.4.(b) (mais pour des ensembles plus larges).
$\overline{\psi_a}$ est bijective :
• elle est surjective, car $a\wedge N=1$, donc d'après l'identité de Bézout : $\exists\ K\in\mathbb{Z}$ tel que $Ka\equiv 1[N]$.
Pour tout $h\in[\![1,N-1]\!]$, avec $k=hK\%N$, alors $k\in[\![0,N-1]\!]$ et $ka\equiv hKA\equiv h1\equiv h[N]$.
Donc nécessairement $k\neq 0$ et $\overline{\psi_a}(k)=h$, donc ψ_a est surjective.
• pour des raisons de cardinaux : ψ_a est alors injective et bijective.
On a alors (changement d'indice $h=\psi_a(k)$) :

$$\sum_{k=1}^{N-1}\chi(ak)=\sum_{k=1}^{N-1}\chi(\overline{\psi_a}(k))=\sum_{h=1}^{N-1}\chi(h)$$

On suppose dorénavant qu'il existe $a\in\mathcal{P}_N$ vérifiant $\chi(a)\neq 1$.

3. Pour $h=0$: notons

$$S_0=\sum_{k=0}^{N-1}\chi(k)=\sum_{k=1}^{N-1}\chi(k)$$

Alors d'après la question précédente :

$$S_0=\sum_{k=1}^{N-1}\chi(ak)=\chi(a)\sum_{k=1}^{N-1}\chi(k)=\chi(a)S_0$$

Or $\chi(a)\neq 1$, donc nécessairement : $S_0=0$.
Faisons les deux changements de variables : $u=k-hN$, par N-périodicité (règle **D.**) :

$$S_h=\sum_{k=hN}^{(h+1)N-1}\chi(k)=\sum_{u=0}^{N-1}\chi(u+hN)=\sum_{u=0}^{N-1}\chi(u)=S_0=0$$

> Pour tout entier h, $\sum_{k=hN}^{(h+1)N-1}\chi(k)=0$.

4. Soit $m>0$, On considère $m=pN+r$ avec $r=m\%N$, la division euclidienne de m par N.

$$\begin{aligned}\left|\sum_{k=1}^{m}\chi(k)\right| &= \left|\sum_{k=0}^{m}\chi(k)\right|=\left|\sum_{i=0}^{p}\left(\sum_{h=iN}^{(i+1)N-1}\chi(h)\right)+\sum_{h=pN}^{pN+r}\chi(h)\right|=\left|0+\sum_{h=pN}^{pN+r}\chi(h)\right|\\ &=\left|\sum_{h=0}^{r}\chi(h+pN)\right|=\left|\sum_{h\in\mathcal{P}_N,h\leqslant r}\chi(h)\right|=\left|\sum_{h\in\mathcal{P}_N,h\leqslant r}1\right|\leqslant \mathrm{card}(\mathcal{P}_N)=\varphi(N)\end{aligned}$$

$$\left|\sum_{k=1}^{m}\chi(k)\right|\leqslant\varphi(N)$$

5. (a) On dit que $\mathbb{R}$ est complet :

Si (u_n) est une suite réelle : (u_n) converge si et seulement si (u_n) vérifie le critère de Cauchy

(b) Si (u_n) est à valeurs complexes,
Supposons que (u_n) vérifie le critère de Cauchy.
$\left|\big(\mathrm{Re}(u)\big)_q - \big(\mathrm{Re}(u)\big)_p\right| = |\mathrm{Re}(u_q - u_p)| \leqslant |u_q - u_p|$ et $\left|\big(\mathrm{Im}(u)\big)_q - \big(\mathrm{Im}(u)\big)_p\right| \leqslant |u_q - u_p|$,
alors $(\mathrm{Re}(u))_n$ et $(\mathrm{Im}(u))_n$ vérifient le critère de Cauchy (réelle),
et ainsi elles sont convergentes, donc (u_n) est convergente.
Réciproquement, si (u_n) est convergente,
$(\mathrm{Re}(u))_n$ et $(\mathrm{Im}(u))_n$ sont convergentes donc vérifient le critère de Cauchy (réelle),
puis comme $|u_q - u_p| \leqslant \left|\big(\mathrm{Re}(u)\big)_q - \big(\mathrm{Re}(u)\big)_p\right| + \left|\big(\mathrm{Im}(u)\big)_q - \big(\mathrm{Im}(u)\big)_p\right|$,
alors (u_n) vérifie le critère de Cauchy.

Si (u_n) est une suite complexe : (u_n) converge si et seulement si (u_n) vérifie le critère de Cauchy

Donc $\mathbb{C}$ est également complet.

(c) On remarque que pour $k \geqslant 1$, $\chi(k) = S_k - S_{k-1}$,
puis on fait une transformation d'Abel (sorte d'intégration par parties, pour les sommes).
Soient $n \in \mathbb{N}^*$ et $q > p \geqslant n$:

$$\sum_{k=p}^{q} \frac{\chi(k)}{k} = \sum_{k=p}^{q} \frac{S_k - S_{k-1}}{k} = \sum_{k=p}^{q} \frac{S_k}{k} - \sum_{k=p}^{q} \frac{S_{k-1}}{k} = \sum_{k=p}^{q} \frac{S_k}{k} - \sum_{k=p-1}^{q-1} \frac{S_k}{k+1}$$

$$\boxed{\sum_{k=p}^{q} \frac{\chi(k)}{k} = \sum_{k=p}^{q-1} S_k \left(\frac{1}{k} - \frac{1}{k+1}\right) + \frac{S_q}{q} - \frac{S_{p-1}}{p}}$$

(d) Ainsi pour $q > p \geqslant n$,

$$\begin{aligned}\left|\sum_{k=p}^{q} \frac{\chi(k)}{k}\right| &= \left|\sum_{k=p}^{q-1} S_k \left(\frac{1}{k} - \frac{1}{k+1}\right) + \frac{S_q}{q} - \frac{S_{p-1}}{p}\right| \\ &\leqslant \sum_{k=p}^{q-1} \left|S_k \left(\frac{1}{k} - \frac{1}{k+1}\right)\right| + \frac{|S_q|}{q} + \frac{|S_{p-1}|}{p} \leqslant \varphi(N) \left(\sum_{k=p}^{q-1} \left|\left(\frac{1}{k} - \frac{1}{k+1}\right)\right| + \frac{1}{q} + \frac{1}{p}\right)\end{aligned}$$

Or $\dfrac{1}{k} - \dfrac{1}{k+1} \geqslant 0$, donc $\left|\left(\dfrac{1}{k} - \dfrac{1}{k+1}\right)\right| = \dfrac{1}{k} - \dfrac{1}{k+1}$ et donc

$$\left|\sum_{k=p}^{q} \frac{\chi(k)}{k}\right| \leqslant \varphi(N) \left(\sum_{k=p}^{q-1} \left(\frac{1}{k} - \frac{1}{k+1}\right) + \frac{1}{q} + \frac{1}{p}\right) = \frac{2\varphi(N)}{p} \leqslant \frac{2\varphi(N)}{n}$$

Or $\lim\limits_{n\to\infty} \dfrac{2}{n}\varphi(N) = 0$,

donc pour tout $\epsilon > 0$, il existe $n \in \mathbb{N}^*$ tel que $\forall\ q > p \geqslant m$, $\left|\sum\limits_{k=p}^{q} \dfrac{\chi(k)}{k}\right| \leqslant \epsilon$.

Donc la suite $(T_n)_{n\in\mathbb{N}}$ vérifie le critère de Cauchy.

(e) Elle est donc convergente dans $\mathbb{C}$:

la suite $\left(\sum\limits_{k=1}^{n} \dfrac{\chi(k)}{k}\right)_{n\geqslant 1}$ est convergente