ISM MP+, Mathématiques
Année 2024/2025

Corrigé de la séance 7 - MP+ - 28/03/25

Exercice 1 (***)

Étant donné un ensemble E et un groupe $(\mathrm{G}, \times)$ de neutre e, une *action* de G sur E est une application

$$\mathrm{G} \times \mathrm{E} \to \mathrm{E},\ (g, x) \mapsto g \cdot x$$

vérifiant $\forall x \in \mathrm{E} \quad e \cdot x = x$ et $\forall (g, g', x) \in \mathrm{G}^2 \times \mathrm{E} \quad g' \cdot (g \cdot x) = (g'g) \cdot x$

On dit que le groupe G *agit* ou *opère* sur l'ensemble E. Pour $x \in \mathrm{E}$, on définit *l'orbite* de x notée O_x par

$$\mathrm{O}_x = \{g \cdot x, g \in \mathrm{G}\}$$

le *stabilisateur* de x noté G_x par

$$\mathrm{G}_x = \{g \in \mathrm{G} \mid g \cdot x = x\}$$

et la relation binaire $\mathcal{R}$ pour $(x, y) \in \mathrm{E}^2$ par

$$x \mathcal{R} y \iff y \in \mathrm{O}_x$$

1. Vérifier que le groupe G agit sur lui-même par translation à gauche $\mathrm{G}^2 \to \mathrm{G}, (g, x) \mapsto gx$ et par conjugaison $\mathrm{G}^2 \to \mathrm{G}, (g, x) \mapsto gxg^{-1}$.
2. Établir que la relation $\mathcal{R}$ est une relation d'équivalence dont les classes d'équivalence sont les orbites.
3. Soit $x \in \mathrm{E}$. Établir que G_x est sous-groupe de G puis vérifier que la relation binaire $\mathcal{R}_x$ définie pour $(a, b) \in \mathrm{G}^2$ par

   $$a \mathcal{R}_x b \iff a \cdot x = b \cdot x$$

   est une relation d'équivalence.

   Dans ce qui suit, les ensembles E et G sont supposés finis.

4. En déduire $\forall x \in \mathrm{E} \quad \mathrm{Card\ G} = \mathrm{Card\ O}_x \times \mathrm{Card\ G}_x$
5. Conclure en montrant *l'équation aux classes*

   $$\mathrm{Card\ E} = \sum_{i=1}^{n} \frac{\mathrm{Card\ G}}{\mathrm{Card\ G}_{x_i}}$$

   où $x_1, \ldots, x_n$ sont des représentants des classes d'équivalence de $\mathcal{R}$.

Corrigé : 1. Considérons la translation à gauche $(g, x) \in \mathrm{G}^2 \mapsto gx$. On a clairement $ex = x$ pour $x \in \mathrm{G}$ et par associativité

$$\forall (g, g', x) \in \mathrm{G}^3 \quad g'(gx) = (g'g)x$$

Considérons ensuite la conjugaison $(g, x) \mapsto gxg^{-1}$. On a $exe^{-1} = x$ pour tout $x \in \mathrm{G}$ et par associativité

$$\forall (g, g', x) \in \mathrm{G}^3 \quad g'(gxg^{-1})g'^{-1} = (g'g)x(g'g)^{-1}$$

Le groupe G agit sur lui-même par translation à gauche et par conjugaison.

2. Soit $(x,y,z) \in \mathrm{E}^3$. On a $x = e \cdot x$ d'où $x \in \mathrm{O}_x$ ce qui signifie $x\mathcal{R}x$. Si $x\mathcal{R}y$, on dispose de $g \in \mathrm{G}$ tel que $y = g \cdot x$ ce qui implique $g^{-1} \cdot y = g^{-1} \cdot (g \cdot x) = x$ d'où $y\mathcal{R}x$. Si $x\mathcal{R}y$ et $y\mathcal{R}z$, on dispose de g et g' dans G tels que $y = g \cdot x$ et $z = g' \cdot y$. Il s'ensuit $z = g' \cdot (g \cdot x) = (g'g) \cdot x$ ce qui prouve $x\mathcal{R}z$. La relation binaire $\mathcal{R}$ est donc réflexive, symétrique, transitive. Par définition de $\mathcal{R}$, les ensembles O_x pour $x \in \mathrm{E}$ sont les classes associées et on conclut

La relation $\mathcal{R}$ est une relation d'équivalence donc les classes sont les orbites.

3. Soit $x \in \mathrm{E}$. On a $e \cdot x = x$ d'où $e \in \mathrm{G}_x$. Soit $(a,b) \in \mathrm{G}_x^2$. On $(ab) \cdot x = a \cdot (b \cdot x) = a \cdot x = x$ puis

$$a \cdot x = x \quad \Longrightarrow \quad a^{-1} \cdot (a \cdot x) = (a^{-1}a) \cdot x = x = a^{-1} \cdot x$$

Ainsi Pour $x \in \mathrm{E}$, l'ensemble G_x est un sous-groupe de G.

La relation $\mathcal{R}_x$ est clairement réflexive, symétrique et transitive et par conséquent

Pour $x \in \mathrm{E}$, la relation $\mathcal{R}_x$ est une relation d'équivalence.

4. Soit $x \in \mathrm{E}$. Pour $(a,b) \in \mathrm{G}^2$, on a

$$a\mathcal{R}_x b \iff a \cdot x = b \cdot x \iff x = (a^{-1}b) \cdot x \iff a^{-1}b \in \mathrm{G}_x \iff b \in a\mathrm{G}_x$$

On en déduit que les classes d'équivalence pour la relation $\mathcal{R}_x$ sont de la forme $a\mathrm{G}_x$ avec $a \in \mathrm{G}$. Elles sont en bijection avec G_x et donc de même cardinal. Enfin, le nombre de ces classes d'équivalence est le nombre de valeurs prises par $g \cdot x$ quand g parcourt G. Considérant $a_1, \ldots, a_p$ des représentants de ces classes, on a $\mathrm{G} = \bigsqcup_{i=1}^{p} a_i\mathrm{G}_x$ avec $p = \mathrm{Card}\ \mathrm{O}_x$ d'où

$$\boxed{\mathrm{Card}\ \mathrm{G} = \sum_{i=1}^{p} \mathrm{Card}\ a_i\mathrm{G}_x = p \times \mathrm{Card}\ \mathrm{G}_x = \mathrm{Card}\ \mathrm{O}_x \times \mathrm{Card}\ \mathrm{G}_x}$$

5. On a la partition $$\mathrm{E} = \bigsqcup_{i=1}^{n} \mathrm{O}_{x_i}$$

On conclut $$\boxed{\mathrm{Card}\ \mathrm{E} = \sum_{i=1}^{n} \mathrm{Card}\ \mathrm{O}_{x_i} = \sum_{i=1}^{n} \frac{\mathrm{Card}\ \mathrm{G}}{\mathrm{Card}\ \mathrm{G}_{x_i}}}$$

Exercice 2 (***)

On définit les *polynômes cyclotomiques* par

$$\forall n \in \mathbb{N}^* \qquad \Phi_n = \prod_{k \in [\![1\,;n]\!],\ k\wedge n=1} \left(\mathrm{X} - \mathrm{e}^{\frac{2\mathrm{i}k\pi}{n}}\right)$$

1. Montrer $\forall n \in \mathbb{N}^* \qquad \prod_{d|n} \Phi_d = \mathrm{X}^n - 1$

2. Montrer $\forall n \in \mathbb{N}^* \qquad \Phi_n \in \mathbb{Z}[\mathrm{X}]$

Corrigé : 1. On a la partition

$$[\![1\,;n]\!] = \bigsqcup_{d|n} \{k \in [\![1\,;n]\!] \mid k \wedge n = d\}$$

Soit $(a,b) \in \mathbb{Z}^2$ avec a ou b non nuls. On dispose de l'équivalence

$$a \wedge b = d \iff \exists !(a',b') \in \mathbb{Z}^2 \quad | \quad a = a'd \qquad b = b'd \quad \text{et} \quad a' \wedge b' = 1$$

Pour d diviseur de n, il vient

$$\prod_{k \in [\![1\,;n]\!],\ k\wedge n=d} \left(\mathrm{X} - \mathrm{e}^{\frac{2\mathrm{i}k\pi}{n}}\right) \underbrace{=}_{k=d\ell} \prod_{\ell \in [\![1\,;n/d]\!],\ \ell\wedge n/d=1} \left(\mathrm{X} - \mathrm{e}^{\frac{2\mathrm{i}d\ell\pi}{n}}\right) = \Phi_{n/d}$$

Enfin, si d parcourt l'ensemble des diviseurs de n, alors n/d également et on obtient

$$\prod_{d|n} \Phi_d = \prod_{d|n} \Phi_{n/d} = \prod_{d|n} \prod_{k \in [\![1\,;n]\!],\ k\wedge n=d} \left(\mathrm{X} - \mathrm{e}^{\frac{2\mathrm{i}k\pi}{n}}\right) = \prod_{k \in [\![1\,;n]\!]} \left(\mathrm{X} - \mathrm{e}^{\frac{2\mathrm{i}k\pi}{n}}\right)$$

On conclut

$$\boxed{\forall n \in \mathbb{N}^* \qquad \prod_{d|n} \Phi_d = \mathrm{X}^n - 1}$$

Remarque : En considérant les degrés dans cette égalité, on obtient

$$n = \sum_{d|n} \varphi(d)$$

2. Montrons le lemme suivant :

Lemme 1. *Soit* $\mathrm{B} \in \mathbb{Z}[\mathrm{X}]$ *non nul unitaire. Pour* $\mathrm{A} \in \mathbb{Z}[\mathrm{X}]$*, le quotient et reste de la division euclidienne de* A *par* B *dans* $\mathbb{R}[\mathrm{X}]$ *sont dans* $\mathbb{Z}[\mathrm{X}]$*.*

Preuve : On procède par récurrence sur $\deg \mathrm{A}$. L'initialisation pour $\deg \mathrm{A} = 0$ ne pose pas de problème en distinguant $\deg \mathrm{B} = 0$ et $\deg \mathrm{B} > 0$. On suppose le résultat vrai pour tout polynôme de degré $< n = \deg \mathrm{A}$. Si $\deg \mathrm{B} > n$, on a $\mathrm{Q} = 0$ et $\mathrm{R} = \mathrm{A}$ et le résultat suit. Si $\deg \mathrm{B} \leqslant n$, on note $\mathrm{A} = a\mathrm{X}^n + \mathrm{U}$ avec $a \in \mathbb{Z}$ et $\mathrm{U} \in \mathbb{Z}[\mathrm{X}]$. On pose $\mathrm{V} = \mathrm{A} - a\mathrm{X}^{n-d}\mathrm{B}$. On a $\mathrm{V} \in \mathbb{Z}[\mathrm{X}]$ et $\deg \mathrm{V} < n$ d'où $\mathrm{V} = \mathrm{BQ} + \mathrm{R}$ avec Q et R dans $\mathbb{Z}[\mathrm{X}]$ avec $\deg \mathrm{R} < \deg \mathrm{B}$ puis $\mathrm{A} = \mathrm{B}(\mathrm{Q} + a\mathrm{X}^{n-d}\mathrm{B}) + \mathrm{R}$ d'où l'hérédité.

On montre par récurrence que $\Phi_n \in \mathbb{Z}[\mathrm{X}]$ pour tout n entier non nul. Le résultat est vrai pour $n = 1$ avec $\Phi_1 = \mathrm{X} - 1$. On suppose le résultat vrai pour tout entier $< n$ avec $n \geqslant 2$ fixé. On a

$$\mathrm{X}^n - 1 = \prod_{d|n} \Phi_d = \Phi_n \prod_{d|n, d<n} \Phi_d$$

d'où $$\Phi_n = \frac{\mathrm{X}^n - 1}{\prod_{d|n, d<n} \Phi_d}$$

Il s'agit, par hypothèse de récurrence, d'un quotient d'un polynôme de $\mathbb{Z}[\mathrm{X}]$ par un polynôme unitaire non nul dans $\mathbb{Z}[\mathrm{X}]$. D'après le lemme, ce quotient est dans $\mathbb{Z}[\mathrm{X}]$ ce qui clôt la récurrence. On conclut

$$\boxed{\forall n \in \mathbb{N}^* \qquad \Phi_n \in \mathbb{Z}[\mathrm{X}]}$$

Exercice 3 (****)

La définition générale d'un corps est la suivante :

Définition 1. *On appelle* corps *un anneau* $(\mathbb{K}, +, \times)$ *non réduit à* $\{0\}$ *et tel que tous les éléments de* $\mathbb{K} \setminus \{0\}$ *sont inversibles.*

Notations : On note $\mathbb{K}^* = \mathbb{K} \setminus \{0\}$.

L'objectif de ce problème est d'établir le *théorème de Wedderburn* : tout corps fini est commutatif.

Soit $\mathbb{K}$ un corps fini. On définit son *centre* noté Z par

$$\mathrm{Z} = \{x \in \mathbb{K} \mid \forall y \in \mathbb{K} \qquad xy = yx\}$$

1. Montrer que le centre Z est un sous-corps commutatif de $\mathbb{K}$ de cardinal $q \geqslant 2$.
   En déduire qu'il existe n entier non nul tel que $\mathrm{Card}\ \mathbb{K} = q^n$.

   On suppose le corps $\mathbb{K}$ non commutatif.
2. En considérant que $\mathbb{K}^*$ opère sur lui-même par conjugaison, pour $x \in \mathbb{K}^*$, établir
$$\mathrm{Card}\ \mathrm{O}_x = \frac{\mathrm{Card}\ \mathbb{K}^*}{\mathrm{Card}\ {\mathbb{K}^*}_x}$$
3. Pour d entier non nul diviseur strict de n, montrer que $\Phi_n(q)$ divise $\dfrac{q^n - 1}{q^d - 1}$.
4. Établir
$$q^n - 1 = q - 1 + \sum \frac{q^n - 1}{q^d - 1}$$
   la somme portant sur un certain nombre de diviseurs stricts de n.
5. Conclure.

Corrigé : 1. L'ensemble $(\mathrm{Z}, +, \times)$ est un sous-anneau commutatif de $(\mathbb{K}, +, \times)$ et tout élément non nul de Z admet un inverse qui est aussi dans Z. L'ensemble Z n'est pas réduit à $\{0\}$ puisqu'il contient 1 et par conséquent

$$\boxed{\text{Le centre Z est un sous-corps commutatif de } \mathbb{K} \text{ de cardinal } q \geqslant 2.}$$

Le corps $\mathbb{K}$ est une extension du corps Z. C'est donc un Z-ev. L'ensemble $\mathbb{K}$ est une famille génératrice de $\mathbb{K}$ en tant que Z-ev et c'est une famille finie donc le corps $\mathbb{K}$ est un Z-ev de dimension finie. Les résultats établis pour les $\mathbb{R}$-ev ou $\mathbb{C}$-ev de dimension finie s'étendent à l'identique pour un Z-ev et il s'ensuit que le corps $\mathbb{K}$ est isomorphe à Z^n avec n entier non nul. Ainsi

$$\boxed{\text{Il existe } n \text{ entier non nul tel que } \mathrm{Card}\ \mathbb{K} = q^n.}$$

2. L'ensemble $(\mathbb{K}^*, \times)$ est un groupe. On le fait opérer sur lui-même par conjugaison. Pour $x \in \mathrm{E}$, on note O_x l'orbite de x et ${\mathbb{K}^*}_x$ le stabilisateur. On a

$$\mathrm{Card}\ \mathbb{K}^* = \mathrm{Card}\ \mathrm{O}_x \times \mathrm{Card}\ {\mathbb{K}^*}_x$$

Ainsi
$$\boxed{\forall x \in \mathbb{K}^* \qquad \mathrm{Card}\ \mathrm{O}_x = \frac{\mathrm{Card}\ \mathbb{K}^*}{\mathrm{Card}\ {\mathbb{K}^*}_x}}$$

3. Soit d un entier non nul diviseur strict de n. D'après les résultats sur les polynômes cyclotomiques, on a

$$\mathrm{X}^n - 1 = \prod_{m|n} \Phi_m = \prod_{m|n,\, m\nmid d} \Phi_m \times \prod_{m|d} \Phi_m = \prod_{m|n,\, m\nmid d} \Phi_m \times (\mathrm{X}^d - 1)$$

Par suite $$q^n - 1 = (q^d - 1) \prod_{m|n,\, m\nmid d} \Phi_m(q)$$

Comme les polynômes cyclotomiques sont dans $\mathbb{Z}[\mathrm{X}]$, on conclut

$$\boxed{\text{Pour } d \text{ entier non nul diviseur strict de } n, \text{ on a } \Phi_n(q) \text{ divise } \frac{q^n - 1}{q^d - 1}.}$$

Remarque : On a également établi $q^d - 1 | q^n - 1$.

4. On a $n > 1$ car $\mathbb{K} \neq \mathrm{Z}$ puisque le corps $\mathbb{K}$ est supposé non commutatif. Soit $x \in \mathbb{K}^*$. On vérifie sans difficulté que ${\mathbb{K}^*}_x \cup \{0\}$ est un corps contenant Z et c'est donc un Z-ev d'où l'existence de d entier non nul tel Card ${\mathbb{K}^*}_x \cup \{0\} = q^d$. Notant $n = dm + r$ avec m entier et $r \in [\![0\,;\, d-1]\!]$, on a

$$q^n - 1 = q^{dm+r} - 1 = q^r(q^{dm} - 1) + q^r - 1$$

Avec une factorisation de Bernoulli sur $q^{dm} - 1 = (q^d)^m - 1 = (q^d - 1)\ldots$, comme $q^d - 1 | q^n - 1$, alors on a $q^d - 1 | q^r - 1$ ce qui implique $r = 0$ et donc $d | n$. Enfin, on a

$$x \in \mathrm{Z} \iff \mathrm{O}_x = \{x\}$$

d'où Card $\mathrm{O}_x > 1$ pour $x \notin \mathrm{Z}$. D'après l'équation des classes, en séparant les classes triviales des autres, on obtient

$$\mathrm{Card}\ \mathbb{K}^* = \mathrm{Card}\ \mathrm{Z} \setminus \{0\} + \sum \frac{\mathrm{Card}\ \mathbb{K}^*}{\mathrm{Card}\ {\mathbb{K}^*}_x}$$

avec la somme portant sur certains éléments hors du centre. On conclut

$$\boxed{q^n - 1 = q - 1 + \sum \frac{q^n - 1}{q^d - 1}}$$

la somme portant sur un certain nombre de diviseurs stricts de n.

5. On suppose $n \geqslant 3$. Avec le résultat de la question 3, on en déduit $\Phi_n(q) | q - 1$. Or, notant $\zeta_1, \ldots, \zeta_r$ les racines primitives n-ièmes de l'unité, on a

$$\Phi_n(q) = \prod_{i=1}^{r} (q - \zeta_i)$$

et comme les ζ_i sont différentes de 1, il vient par inégalité triangulaire inverse (stricte ici)

$$|\Phi_n(q)| = \prod_{i=1}^{r} |q - \zeta_i| > \prod_{i=1}^{r} (|q| - |\zeta_i|) = (q-1)^r \geqslant q - 1$$

ce qui contredit $\Phi_n(q) | q - 1$. On n'a donc pas $n \geqslant 3$. Si $n = 2$, on trouve $\Phi_2(q) = q + 1$ diviseur de $q - 1$ ce qui est faux. Il en résulte que $n = 1$ et on conclut

$$\boxed{\text{Tout corps fini est commutatif.}}$$

Exercice 4 (**)

Pour n entier, on note $\tau(n)$ le nombre de diviseurs de n et $\sigma(n)$ la somme des diviseurs de n.

1. Établir l'égalité $\quad \forall n \in \mathbb{N} \quad \displaystyle\sum_{k=1}^{n} \tau(k) = \sum_{d=1}^{n} \left\lfloor \frac{n}{d} \right\rfloor$

2. En déduire $\quad \displaystyle\sum_{k=1}^{n} \tau(k) \underset{n\to+\infty}{\sim} n \ln n$

3. Établir l'égalité $\quad \forall n \in \mathbb{N} \quad \displaystyle\sum_{k=1}^{n} \sigma(k) = \sum_{j=1}^{n} \frac{1}{2} \left\lfloor \frac{n}{j} \right\rfloor \left(\left\lfloor \frac{n}{j} \right\rfloor + 1 \right)$

4. En déduire $\quad \displaystyle\sum_{k=1}^{n} \sigma(k) \underset{n\to+\infty}{\sim} \frac{\zeta(2)}{2} n^2 \quad$ où $\quad \zeta(2) = \sum_{n=1}^{+\infty} \frac{1}{n^2}$

Corrigé : 1. On a $\quad \displaystyle\sum_{k=1}^{n} \tau(k) = \sum_{k=1}^{n} \left(\sum_{d|k} 1 \right)$

Comme les sommes sont finies, on peut intervertir l'ordre de sommation. Le plus grand diviseur de n étant n lui-même, on obtient

$$\sum_{k=1}^{n} \tau(k) = \sum_{d=1}^{n} \left(\sum_{k \in [\![1\,;\, n]\!],\ d|k} 1 \right)$$

La somme intérieure ci-dessus compte le nombre de multiples de d dans $[\![1\,;\, n]\!]$ qui sont

$$d, 2d, \ldots, \left\lfloor \frac{n}{d} \right\rfloor d$$

Par conséquent $\quad \boxed{\forall n \in \mathbb{N} \quad \displaystyle\sum_{k=1}^{n} \tau(k) = \sum_{d=1}^{n} \left\lfloor \frac{n}{d} \right\rfloor}$

2. Avec $x - 1 < \lfloor x \rfloor \leqslant x$ pour tout x réel, il vient pour n entier

$$\sum_{d=1}^{n} \left(\frac{n}{d} - 1 \right) \leqslant \sum_{k=1}^{n} \tau(k) \leqslant \sum_{d=1}^{n} \frac{n}{d} \iff n(\mathrm{H}_n - 1) \leqslant \sum_{k=1}^{n} \tau(k) \leqslant n\mathrm{H}_n \quad \text{avec} \quad \mathrm{H}_n = \sum_{d=1}^{n} \frac{1}{d}$$

La fonction $t \mapsto \dfrac{1}{t}$ est continue, décroissante de $]\,0\,;+\infty\,[$ dans $]\,0\,;+\infty\,[$. D'après le théorème de comparaison série/intégrale, la série $\displaystyle\sum_{k\geqslant 2} \left(\int_{k-1}^{k} \frac{\mathrm{d}t}{t} - \frac{1}{k} \right)$ converge d'où

$$\forall n \geqslant 2 \quad \sum_{k=2}^{n} \left(\int_{k-1}^{k} \frac{\mathrm{d}t}{t} - \frac{1}{k} \right) = \int_{1}^{n} \frac{\mathrm{d}t}{t} - \mathrm{H}_n + 1 \quad \Longrightarrow \quad \mathrm{H}_n \underset{n\to+\infty}{\sim} \ln n$$

On en déduit $\quad \boxed{\displaystyle\sum_{k=1}^{n} \tau(k) \underset{n\to+\infty}{\sim} n \ln n}$

3. Soit n entier. On a

$$\sum_{k=1}^{n} \sigma(k) = \sum_{k=1}^{n} \left(\sum_{(i,j) \in [\![1\,;\, n]\!]^2,\ ij=k} i \right) = \sum_{(i,j) \in [\![1\,;\, n]\!]^2,\ ij \leqslant n} i$$

En changeant l'ordre de sommation, on obtient

$$\sum_{(i,j)\in[\![1\,;n]\!]^2,\ ij\leqslant n} i = \sum_{j=1}^{n}\left(\sum_{i\in[\![1\,;n]\!],\ ij\leqslant n} i\right) = \sum_{j=1}^{n}\left(\sum_{i=1}^{\lfloor n/j\rfloor} i\right)$$

D'où
$$\boxed{\forall n\in\mathbb{N}\qquad \sum_{k=1}^{n}\sigma(k) = \sum_{j=1}^{n}\frac{1}{2}\left\lfloor\frac{n}{j}\right\rfloor\left(\left\lfloor\frac{n}{j}\right\rfloor+1\right)}$$

4. Avec l'encadrement utilisé à la question 2, on obtient pour n entier
$$\frac{1}{2}\sum_{j=1}^{n}\left(\frac{n}{j}-1\right)\frac{n}{j} \leqslant \sum_{k=1}^{n}\sigma(k) \leqslant \frac{1}{2}\sum_{j=1}^{n}\frac{n}{j}\left(\frac{n}{j}+1\right)$$

D'où
$$\frac{1}{2}\left(n^2\sum_{j=1}^{n}\frac{1}{j^2} - n\mathrm{H}_n\right) \leqslant \sum_{k=1}^{n}\sigma(k) \leqslant \frac{1}{2}\left(n^2\sum_{j=1}^{n}\frac{1}{j^2} + n\mathrm{H}_n\right)$$

On a
$$\sum_{j=1}^{n}\frac{1}{j^2} \xrightarrow[n\to\infty]{} \zeta(2) \quad\text{et}\quad n\mathrm{H}_n = n(\ln n + \mathrm{o}(1)) = \mathrm{o}(n^2)$$

Ainsi
$$\boxed{\sum_{k=1}^{n}\sigma(k) \underset{n\to+\infty}{\sim} \frac{\zeta(2)}{2}n^2}$$

Exercice 5 (****)

Soit $(G,+)$ un groupe abélien fini d'ordre pq avec p et q deux nombres premiers distincts. Montrer que G est cyclique.

Corrigé : Un élément de G non nul est d'ordre un diviseur de pq. Supposons que G possède un élément x d'ordre p et un élément y d'ordre q. On a $x+y \neq 0$ sinon $y=-x$ d'ordre p ce qui contredit y d'ordre q puis $p(x+y)=py \neq 0$ car $q \nmid p$ et $q(x+y)=qx \neq 0$ car $p \nmid q$. Ainsi, l'élément $x+y$ est d'ordre pq d'où $\langle x+y \rangle = G$. Supposons G non cyclique, autrement dit tous les éléments de G autre que 1 sont soit tous d'ordre p, soit tous d'ordre q. Supposons que ceux-ci soient d'ordre p. Soit z un élément d'ordre p de G. On définit la relation d'équivalence $x\mathcal{R}y$ par

$$\exists k \in \mathbb{Z} \quad | \quad y \in x + kz$$

À l'instar de la relation de congruence, l'opération $+$ est compatible avec la relation $\mathcal{R}$ et on définit l'opération $+$ sur les classes d'équivalence par $\bar{x}+\bar{y}=\overline{x+y}$ pour $(x,y) \in G^2$. Les classes pour $\mathcal{R}$ forment une partition de G et pour $x \in G$, la classe $\bar{x}=x+\langle z \rangle$ est en bijection avec $\langle z \rangle$ donc de cardinal p. Ainsi, il y a q classes d'équivalence et celles-ci forment un groupe G' pour la loi $+$. Un élément $\bar{x} \neq \bar{0}$ est donc d'ordre q. Or, on a $p\bar{x}=\overline{px}=\bar{0}$ ce qui prouve $q|p$ et qui est faux. On conclut

Un groupe abélien d'ordre pq avec p et q premiers distincts est cyclique.

Remarque : L'ensemble des classes d'équivalence pour la relation $\mathcal{R}$ est appelé *groupe quotient* de G par $H=\langle z \rangle$ et noté G/H.

Exercice 6 (****)

Soit $(\mathrm{G}, \times)$ un groupe abélien fini.

1. Montrer qu'il existe ℓ entier non nul minimal tel que $x^\ell = 1$ pour tout $x \in \mathrm{G}$.
2. Soit $x \in \mathrm{G}$ et $k \in \mathbb{Z}$. Établir
$$o(x^k) = \frac{o(x)}{o(x) \wedge k}$$
3. Soit $(x, y) \in \mathrm{G}^2$. Si $o(x) \wedge o(y) = 1$, déterminer $o(xy)$.
4. Établir $\qquad \exists g \in \mathrm{G} \quad | \quad o(g) = \ell$
5. Soit $\mathbb{K}$ un corps et G un sous-groupe fini de $\mathbb{K}^*$. Montrer que G est cyclique.

Corrigé : 1. L'ensemble $\left\{k \in \mathbb{N}^* \mid \forall x \in \mathrm{G} \quad x^k = 1\right\}$ est une partie de $\mathbb{N}$, non vide puisqu'elle contient Card G. Ainsi

$$\boxed{\text{Il existe } \ell \text{ entier non nul minimal tel que } x^\ell = 1 \text{ pour tout } x \in \mathrm{G}.}$$

2. Soit $k \in \mathbb{N}^*$, $d = o(x)$, $\delta = d \wedge k$ et on note $d = \delta d'$ et $k = \delta k'$ avec d', k' entiers relatifs premiers entre eux. On a
$$(x^k)^{d'} = x^{\delta k' d'} = (x^d)^{k'} = e \quad \Longrightarrow \quad o(x^k) | d'$$
Par ailleurs, pour ℓ entier tel que $x^{k\ell} = (x^k)^\ell = e$, il vient $d | k\ell$ autrement dit $\delta d' | \delta k' \ell$ d'où $d' | k'\ell$. D'après le théorème de Gauss, comme $d' \wedge k' = 1$, on obtient $d' | \ell$ donc en particulier $d' | o(x^k)$. Les entiers d' et $o(x^k)$ sont associés donc égaux et on conclut

$$\boxed{o(x^k) = \frac{o(x)}{o(x) \wedge k}}$$

3. Soit k entier tel que $(xy)^k = 1$. Par suite, on a $(xy)^{ko(x)} = y^{ko(x)} = 1$ d'où $o(y) | ko(x)$ et d'après le théorème de Gauss, il s'ensuit $o(y) | k$. Par symétrie des rôles, on a aussi $o(x) | k$ et comme $o(x) \wedge o(y) = 1$, on obtient $o(x)o(y) | k$. Comme on a clairement $(xy)^{o(x)o(y)} = 1$, on conclut

$$\boxed{o(x) \wedge o(y) = 1 \quad \Longrightarrow \quad o(xy) = o(x)o(y)}$$

4. On a $x^\ell = 1$ pour tout $x \in \mathrm{G}$. Par conséquent, pour tout $x \in \mathrm{G}$, l'ordre de x divise ℓ et l'entier ℓ est minimal pour cette propriété ce qui prouve que ℓ est le ppcm des ordres des éléments de G. Notant $\ell = \prod_{i=1}^{r} p_i^{\alpha_i}$ avec les p_i premiers deux à deux distincts et les α_i entiers non nuls, alors, pour tout $i \in [\![1 ; r]\!]$, il existe $x_i \in \mathrm{G}$ tel que $p_i^{\alpha_i} | o(x_i)$, d'où $o(x_i) = p_i^{\alpha_i} q_i$ avec $q_i \wedge p_i = 1$. Avec le résultat de la deuxième question, on obtient
$$o(x_i^{q_i}) = \frac{p_i^{\alpha_i} q_i}{(p_i^{\alpha_i} q_i) \wedge q_i} = p_i^{\alpha_i}$$
D'après le résultat de la question précédente, avec $g = \prod_{i=1}^{r} x_i^{q_i}$, il vient

$$\boxed{o(g) = o\left(\prod_{i=1}^{r} x_i^{q_i}\right) = \prod_{i=1}^{r} o(x_i^{q_i}) = \prod_{i=1}^{r} p_i^{\alpha_i} = \ell}$$

5. On a $\qquad \mathrm{G} \subset \left\{x \in \mathbb{K}^* \mid x^\ell = 1\right\}$

Or, d'après le résultat de l'exercice précédent, le polynôme $\mathrm{X}^\ell - 1$ admet au plus ℓ racines d'où Card $\mathrm{G} \leqslant \ell$. Mais d'après le résultat de la question précédente, il existe $g \in \mathrm{G}$ d'ordre ℓ, autrement dit $\langle g \rangle \subset \mathrm{G}$ avec Card $\langle g \rangle = \ell$. L'inclusion est donc une égalité et on conclut

Tout sous-groupe fini d'un corps (commutatif) est cyclique.

Remarque : La définition officielle au programme de MP de corps suppose celui-ci commutatif. Il existe une définition plus générale qui ne requiert pas cette condition d'où le rappel ci-dessus du qualificatif *commutatif*.

Exercice 7 (****)

Soit $n \geqslant 3$ et a entier impair.

1. Montrer que $a^{2^{n-2}} \equiv 1\ [2^n]$
2. Le groupe $\mathrm{U}(\mathbb{Z}/2^n\mathbb{Z})$ est-il cyclique ?
3. Trouver le plus petit entier nul k tel que $3^k \equiv 1\ [2^n]$.
4. Montrer que $\mathrm{U}(\mathbb{Z}/2^n\mathbb{Z})$ est isomorphe au groupe produit $(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{n-2}\mathbb{Z}, +)$.

Corrigé : 1. On a

$$a^{2^{n-2}} - 1 = \left(a^{2^{n-3}} + 1\right)\left(a^{2^{n-3}} - 1\right) = \underbrace{\left(a^{2^{n-3}} + 1\right)\left(a^{2^{n-4}} + 1\right) \times \ldots \times \left(a^{2^1} + 1\right)}_{n-3 \text{ termes pairs}}(a^2 - 1)$$

D'où $2^{n-3} | a^{2^{n-2}} - 1$. Puis, comme a est impair, il existe k entier tel que $a = 2k + 1$ et $a^2 - 1 = (2k+1)^2 - 1 = 4k(k+1) \equiv 0\ [8]$. On conclut

$$\boxed{a^{2^{n-2}} \equiv 1\ [2^n]}$$

2. On a $\mathrm{Card}\ \mathrm{U}(\mathbb{Z}/2^n\mathbb{Z}) = \varphi(2^n) = 2^{n-1}(2-1) = 2^{n-1}$. Or, l'égalité $a^{2^{n-2}} \equiv 1\ [2^n]$ interdit la possibilité d'un générateur puisque l'ordre d'un élément de $\mathrm{U}(\mathbb{Z}/2^n\mathbb{Z})$ sera toujours inférieur ou égal à 2^{n-2}. On conclut

$$\boxed{\text{Le groupe } \mathrm{U}(\mathbb{Z}/2^n\mathbb{Z}) \text{ n'est pas cyclique.}}$$

3. Comme $3 \wedge 2^n = 1$, on a $\bar{3} \in \mathrm{U}(\mathbb{Z}/2^n\mathbb{Z})$. On a $3^{2n-2} \equiv 1\ [2^n]$ d'où $o(\bar{3}) | 2^{n-2}$. Notons $o(\bar{3}) = 2^p$ avec p entier. En s'inspirant de la démarche de la première question, on trouve

$$3^{2^p} - 1 = \left(3^{2^{p-1}} + 1\right)\left(3^{2^{p-2}} + 1\right) \ldots \left(3^{2^0} + 1\right)\left(3^{2^0} - 1\right)$$

Le produit comporte $p+1$ facteurs tous pairs avec en particulier $3^{2^0} + 1 = 4$ d'où 2^{p+2} divise $3^{2^p} - 1$. Par ailleurs, on observe que $3^2 \equiv 1\ [4]$ d'où $3^{2^k} \equiv 1\ [4]$ pour tout $k \geqslant 1$, autrement dit, pour tout $k \geqslant 1$, l'entier $3^{2^k} + 1$ n'est pas multiple de 4. Ainsi, on a $v_2(3^{2^p} - 1) = p + 2$. Or, on a $3^{2^p} \equiv 1\ [2^n]$ d'où $2^n | 3^{2^p} - 1$ d'où $n \leqslant p + 2$. On a donc établi $p \leqslant n - 2$ et $p \geqslant n - 2$ et par conséquent

$$\boxed{\text{Dans } \mathrm{U}(\mathbb{Z}/2^n\mathbb{Z}), \text{ on a } o(\bar{3}) = 2^{n-2}.}$$

4. On pose $\varphi : \begin{cases} \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{n-2}\mathbb{Z} \longrightarrow \mathrm{U}(\mathbb{Z}/2^n\mathbb{Z}) \\ \left(\widehat{k}, \dot{\ell}\right) \longmapsto \overline{(-1)^k 3^\ell} \end{cases}$

L'application φ est clairement un morphisme de groupes. Déterminer $\mathrm{Ker}\ \varphi$. Soit $(k, \ell) \in \mathbb{Z}^2$ tel que $\overline{(-1)^k 3^\ell} = \bar{1}$ c'est-à-dire $\overline{(-1)^k} = \overline{3^{-\ell}}$. Si $3^{-\ell} \equiv -1\ [2^n]$ avec $n \geqslant 3$, alors en particulier $3^{-\ell} \equiv -1\ [8]$ ce qui est faux puisque $3^{-\ell} \equiv 1\ [8]$ ou $\equiv 3\ [8]$. Par conséquent, on a $\widehat{k} = \widehat{0}$ puis $\bar{3}^{-\ell} = \bar{1}$ d'où $o(\bar{3}) = 2^{n-2} | \ell$ ce qui prouve $\dot{\ell} = \dot{0}$. Ainsi, le morphisme φ est injectif et on a égalité des cardinaux entre l'ensemble de départ et d'arrivée d'où

$$\boxed{\mathrm{U}(\mathbb{Z}/2^n\mathbb{Z}) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{n-2}\mathbb{Z}}$$

Exercice 8 (****)

Un nombre complexe est dit *algébrique* s'il est racine d'un polynôme à coefficients rationnels. Un nombre complexe qui n'est pas algébrique est dit *transcendant*.

1. Montrer que l'ensemble $\mathscr{A}$ des nombres algébriques est dénombrable.
2. Soit x un rationnel. Montrer qu'il existe $c > 0$ tel que, pour tout $(p, q) \in \mathbb{Z} \times \mathbb{N}^*$ avec $x \neq \dfrac{p}{q}$, on a
$$\left| x - \frac{p}{q} \right| \geqslant \frac{c}{q}$$
3. Soit x un réel irrationnel algébrique. Montrer qu'il existe $(a, b) \in (\mathbb{R}_+^*)^2$ tel que, pour tout $(p, q) \in \mathbb{Z} \times \mathbb{N}^*$, on a
$$\left| x - \frac{p}{q} \right| \geqslant \frac{a}{q^b}$$
4. Montrer que $\displaystyle\sum_{n=0}^{+\infty} 10^{-n!}$ n'est pas algébrique.

Corrigé : 1. L'ensemble des polynômes à coefficients rationnels $\mathbb{Q}[\mathrm{X}]$ peut s'écrire $\displaystyle\bigcup_{n\in\mathbb{N}} \mathbb{Q}_n[\mathrm{X}]$. Or, pour n entier, l'ensemble $\mathbb{Q}_n[\mathrm{X}]$ est en bijection avec $\mathbb{Q}^{n+1}$ qui est dénombrable comme produit fini d'ensembles dénombrables. Ainsi, l'ensemble $\displaystyle\bigcup_{n\in\mathbb{N}} \mathbb{Q}_n[\mathrm{X}]$ est une union dénombrable d'ensemble dénombrable ce qui prouve que $\mathbb{Q}[\mathrm{X}]$ est dénombrable. Pour $\mathrm{P} \neq 0$, l'ensemble $\mathrm{P}^{-1}(\{0\})$ est un ensemble fini. Or, on a

$$\mathscr{A} = \bigcup_{\mathrm{P}\in\mathbb{Q}[\mathrm{X}]\setminus\{0\}} \mathrm{P}^{-1}(\{0\})$$

Ainsi, l'ensemble des nombres algébriques est une union dénombrable d'ensemble fini donc est au plus dénombrable. L'ensemble $\mathscr{A}$ est clairement infini puisqu'il contient $\mathbb{Q}$ par exemple et on conclut

$$\boxed{\text{L'ensemble des nombres algébriques est dénombrable.}}$$

2. Notons $x = \dfrac{p'}{q'}$ avec $(p', q') \in \mathbb{Z} \times \mathbb{N}^*$. Il vient

$$\left| x - \frac{p}{q} \right| = \frac{|p'q - pq'|}{qq'} \quad \text{et} \quad |p'q - pq'| \in \mathbb{N}^*$$

Notant $c = \dfrac{1}{q'} > 0$, on obtient

$$\boxed{\exists c > 0 \quad | \quad \forall (p, q) \in \mathbb{Z} \times \mathbb{N}^* \qquad x \neq \frac{p}{q} \quad \Longrightarrow \quad \left| x - \frac{p}{q} \right| \geqslant \frac{c}{q}}$$

3. Soit $\mathrm{P} \in \mathbb{Q}[\mathrm{X}]$ irréductible de degré $d \geqslant 2$ tel que $\mathrm{P}(x) = 0$ (si $d = 1$, alors x serait rationnel ce qui est exclu). Soit $(p, q) \in \mathbb{Z} \times \mathbb{N}^*$. D'après le théorème des accroissements finis, il existe y entre x et $\dfrac{p}{q}$ tel que

$$\mathrm{P}\left(\frac{p}{q}\right) = \mathrm{P}\left(\frac{p}{q}\right) - \mathrm{P}(x) = \mathrm{P}'(y)\left(\frac{p}{q} - x\right)$$

Il existe $A \in \mathbb{N}^*$ tel que $AP \in \mathbb{Z}[X]$ et par suite $P\left(\frac{p}{q}\right) Aq^d$ est un entier relatif non nul sans quoi on aurait $P\left(\frac{p}{q}\right) = 0$ ce qui contredirait l'irréductibilité de P. Par suite, on a

$$|P'(y)| \left|x - \frac{p}{q}\right| \geqslant \frac{1}{Aq^d}$$

Puis par continuité sur un compact, il existe $K > 0$ tel que

$$\forall t \in [\, x-1\,;x+1\,] \qquad |P'(t)| \leqslant K$$

d'où
$$\left|\frac{p}{q} - x\right| \leqslant 1 \quad \Longrightarrow \quad \left|x - \frac{p}{q}\right| \geqslant \frac{1}{KAq^d}$$

Avec $a = \text{Inf}\,(1, \frac{1}{KA})$, on conclut

$$\boxed{\exists a > 0 \quad \exists d \in \mathbb{N} \setminus \{0,1\} \quad | \quad \forall (p,q) \in \mathbb{Z} \times \mathbb{N}^* \qquad \left|x - \frac{p}{q}\right| \geqslant \frac{a}{q^d}}$$

4. Notons $\alpha = \sum_{n=0}^{+\infty} 10^{-n!}$. Supposons α rationnel. Soit N entier. On a

$$\alpha = \sum_{n=0}^{N} 10^{-n!} + R_N = \frac{p_N}{q_N} + R_N \quad \text{avec} \quad p_N = 10^{N!} \sum_{n=0}^{N} 10^{-n!} \quad q_N = 10^{N!} \quad \text{et} \quad R_N = \sum_{n=N+1}^{+\infty} 10^{-n!}$$

Puis
$$R_N = \sum_{n=N+1}^{+\infty} \frac{1}{10^{n!}} \leqslant \sum_{n=(N+1)!}^{+\infty} \frac{1}{10^n} = \frac{\beta}{10^{(N+1)!}} \quad \text{avec} \quad \beta = \frac{10}{9}$$

La majoration est claire puisque la somme qui majore contient tous les termes de la somme à minorer, plus d'autres positifs. D'après le résultat de la deuxième question, il existe $c > 0$, indépendant de N, tel que

$$\left|\alpha - \frac{p_N}{q_N}\right| \geqslant \frac{c}{10^{N!}}$$

Par conséquent
$$\forall N \in \mathbb{N} \qquad \frac{c}{10^{N!}} \leqslant \left|\alpha - \frac{p_N}{q_N}\right| = R_N \leqslant \frac{\beta}{10^{(N+1)!}}$$

ce qui est absurde. Il s'ensuit que α est irrationnel. Supposons ensuite α algébrique. D'après le résultat de la question précédente, il existe $a > 0$ et d entier avec $d \geqslant 2$, indépendants de N, tel que

$$\left|\alpha - \frac{p_N}{q_N}\right| \geqslant \frac{a}{q_N^d} = \frac{a}{10^{d\,N!}}$$

Par conséquent
$$\forall N \in \mathbb{N} \qquad \frac{a}{10^{d\,N!}} \leqslant \left|\alpha - \frac{p_N}{q_N}\right| \leqslant \frac{\beta}{10^{(N+1)!}}$$

ce qui est encore absurde. On conclut

$$\boxed{\text{Le nombre } \alpha = \sum_{n=0}^{+\infty} 10^{-n!} \text{ est transcendant.}}$$

Remarque : Le réel $\sum_{n=0}^{+\infty} 10^{-n!}$ est un *nombre de Liouville.*

Exercice 9 (***)

Pour n entier, on note $\pi(n)$ le nombre de nombres premiers dans $[\![\,1\,;\,n\,]\!]$.

1. Montrer $\quad \forall n \geqslant 2 \qquad \pi(n) \geqslant \dfrac{\ln d_n}{\ln n} \quad$ avec $\quad d_n = \mathrm{ppcm}(1, 2, \ldots, n)$

2. On pose $\mathrm{J}_n = \displaystyle\int_0^1 t^n (1-t)^n \,\mathrm{d}t$. Montrer

$$\forall n \in \mathbb{N} \qquad 1 \leqslant d_{2n+1} \times \mathrm{J}_n \leqslant \frac{d_{2n+1}}{4^n}$$

3. Conclure que $\qquad \dfrac{n}{\ln n} = \mathrm{O}(\pi(n))$

Corrigé : 1. Soit $n \geqslant 2$. Notons $p_1, \ldots, p_{\pi(n)}$ les nombres premiers dans $[\![\,1\,;\,n\,]\!]$. On a

$$d_n = \prod_{k=1}^{\pi(n)} p_k^{\alpha_k} \quad \text{avec} \quad \alpha_k = \max\{v_{p_k}(\ell),\ \ell \in [\![\,1\,;\,n\,]\!]\}$$

Ainsi $\qquad \forall k \in [\![\,1\,;\,\pi(n)\,]\!] \qquad \exists \ell \in [\![\,1\,;\,n\,]\!] \quad | \quad p_k^{\alpha_k}$ divise ℓ

d'où $\qquad \forall k \in [\![\,1\,;\,\pi(n)\,]\!] \qquad p_k^{\alpha_k} \leqslant n \quad \Longrightarrow \quad d_n \leqslant n^{\pi(n)}$

Passant au logarithme, on obtient

$$\boxed{\forall n \geqslant 2 \qquad \pi(n) \geqslant \frac{\ln d_n}{\ln n}}$$

2. Une étude de fonction montre que $0 \leqslant t(1-t) \leqslant \dfrac{1}{4}$ pour tout $t \in [\,0\,;1\,]$ d'où après intégration

$$\forall n \in \mathbb{N} \qquad 0 < \mathrm{J}_n \leqslant \frac{1}{4^n}$$

En développant par la fomule du binôme sous l'intégrale, on obtient

$$\forall n \in \mathbb{N} \qquad \mathrm{J}_n = \int_0^1 t^n \sum_{k=0}^{n} \binom{n}{k} (-1)^k t^k \,\mathrm{d}t = \sum_{k=0}^{n} \frac{(-1)^k \binom{n}{k}}{n+k+1}$$

d'où $\qquad \forall n \in \mathbb{N} \qquad d_{2n+1} \times \mathrm{J}_n \in \mathbb{Z} \cap \,]\,0\,;+\infty\,[\, = \mathbb{N}^*$

Ainsi $\qquad \boxed{\forall n \in \mathbb{N} \qquad 1 \leqslant d_{2n+1} \times \mathrm{J}_n \leqslant \dfrac{d_{2n+1}}{4^n}}$

3. On en déduit $\qquad \forall n \in \mathbb{N} \qquad d_{2n+1} \geqslant 4^n$

d'où $\quad \forall n \geqslant 1 \qquad \pi(2n+1) \geqslant \dfrac{\ln d_{2n+1}}{\ln(2n+1)} \geqslant \dfrac{2n \ln 2}{\ln(2n+1)} = \ln 2 \times \dfrac{2n+1}{\ln(2n+1)}(1 + \mathrm{o}(1))$

Par croissance de $n \mapsto \pi(n)$, on a

$$\forall n \in \mathbb{N} \qquad \pi(2n+2) \geqslant \pi(2n+1) \geqslant \ln 2 \times \frac{2n+2}{\ln(2n+2)}(1 + \mathrm{o}(1))$$

Autrement dit $\qquad \pi(n) \geqslant \ln 2 \times \dfrac{n}{\ln n}(1 + \mathrm{o}(1))$

Et on conclut $\qquad \boxed{\dfrac{n}{\ln n} = \mathrm{O}(\pi(n))}$

Remarque : Il s'agit d'une version dégradée et incomplète du *théorème de Tchebycheff* qui fournit l'encadrement

$$\exists \mathrm{N} \qquad \forall n \geqslant \mathrm{N} \qquad \alpha \frac{n}{\ln n} < \pi(n) < \beta \frac{n}{\ln n}$$

avec $\alpha \simeq 0,92$ et $\beta = \simeq 1,1$. On pourra consulter à ce propos le sujet du capes externe de 2008 (épreuve 2) qui propose d'établir un encadrement de ce type (avec des constantes moins bonnes que celles obtenues par Tchebycheff).

Exercice 10 (***)

Soit n entier non nul et p un nombre premier avec $p \geqslant 5$ tels que $p|1+n+n^2$.

1. Établir $\quad n \not\equiv 1\ [p] \qquad n^2 \not\equiv 1\ [p] \qquad n^3 \equiv 1\ [p]$
2. En déduire $\quad 3|p-1 \quad$ puis $\quad 6|p-1$
3. Conclure en montrant qu'il existe une infinité de nombres premiers de la forme $6k+1$ avec k entier non nul.

Corrigé : 1. Si $n \equiv 1\ [p]$, alors $n^2+n+1 \equiv 3\ [p]$ et $3 \not\equiv 0\ [p]$ ce qui contredit $p|1+n+n^2$. Si $n^2 \equiv 1\ [p]$, alors $n^2-1=(n-1)(n+1) \equiv 0\ [p]$ d'où $n \equiv \pm 1\ [p]$ par intégrité dans $\mathbb{Z}/p\mathbb{Z}$ et dans ce cas $n^2+n+1 \equiv 1\ [p]$ ou $\equiv 3\ [p]$ ce qui contredit là encore $p|1+n+n^2$. Enfin, on a $n^2+n+1 \equiv 0\ [p]$ d'où

$$(n-1)(n^2+n+1) \equiv n^3-1 \equiv 0\ [p]$$

On conclut $\quad \boxed{n \not\equiv 1\ [p] \qquad n^2 \not\equiv 1\ [p] \qquad n^3 \equiv 1\ [p]}$

2. Dans $\mathbb{Z}/p\mathbb{Z}$, on a $\bar{n}\bar{n}^2 = \bar{1}$ d'où $\bar{n} \in \mathrm{U}(\mathbb{Z}/p\mathbb{Z})$. On en déduit $o(\bar{n})|p-1$. Or, d'après le résultat de la première question, on a $o(\bar{n})|3$ et $o(\bar{n}) \neq 1$ et $\neq 2$ d'où $o(\bar{n})=3$ ce qui prouve $3|p-1$. Par ailleurs, l'entier p est impair d'où $2|p-1$ et comme $2 \wedge 3 = 1$, on conclut

$$\boxed{6|p-1}$$

3. Supposons qu'il y a un nombre fini de nombres premiers de la forme $6k+1$ avec k entier non nul que l'on note $6k_1+1, \ldots 6k_r+1$ avec r entier non nul (il en existe puisque $7=6+1$). On pose $n = \prod_{i=1}^{r}(6k_i+1)$. On a sans difficulté $n^2+n+1 \equiv 3\ [6]$. Soit q un diviseur premier de n^2+n+1. Si $q \geqslant 5$, alors il vient d'après le résultat de la première question $6|q-1$ d'où q de la forme $6k+1$ ce qui implique $q|n$ et contredit $q|n^2+n+1$. On en déduit $q \in \{2,3\}$. L'entier n^2+n+1 est clairement impair. Le seul diviseur premier de n^2+n+1 est 3 d'où $n^2+n+1=3^\beta$ avec β entier $\geqslant 2$. On a $n=6a+1$ avec a entier non nul d'où

$$n^2+n+1 = 3\left(1+6a+12a^2\right)$$

ce qui contredit $3^2|n^2+n+1$. On conclut

$$\boxed{\text{Il existe une infinité de nombres premiers de la forme } 6k+1 \text{ avec } k \text{ entier non nul.}}$$