DEVOIR SURVEILLÉ N°1

MP Laâyoune
2025 - 2026

⋆ ⋆
⋆

MATHÉMATIQUES

DURÉE DE L'ÉPREUVE : **4 heures**

Ce sujet comporte 4 pages numérotées de 1/4 à 4/4, en plus de cette page de garde.

L'usage de la calculatrice est interdit.

⋆ ⋆ ⋆

La qualité de la rédaction et la précision des raisonnements entreront pour une part importante dans l'appréciation des copies.

Tournez la page S.V.P.

Problème 1

Notations et rappels

- Soit n un entier ≥ 2. On note $\mathbb{Z}/n\mathbb{Z}$ l'anneau des classes d'entiers modulo n, et $\mathbb{U}(\mathbb{Z}/n\mathbb{Z})$ le groupe multiplicatif des éléments inversibles de $\mathbb{Z}/n\mathbb{Z}$.
- Pour $n \geq 1$, on note $\mathcal{E}_n = \left\{k \in [\![0, n-1]\!],\ \ k \wedge n = 1\right\}$ et φ ***l'indicatrice d'Euler*** : $\varphi(n) = \operatorname{Card} \mathcal{E}_n$.
- On rappelle que, si G est un groupe (multiplicatif) d'ordre n et de neutre e, alors

$$\text{pour tout } a \in G,\ a^n = e. \text{ En particulier, l'ordre de } a \text{ divise } n.$$

- On rappelle aussi le théorème des restes chinois : Si m, n sont deux entiers ≥ 2 premiers entre eux, alors l'application :

$$\begin{array}{rccc} f & : & \mathbb{Z}/mn\mathbb{Z} & \longrightarrow & \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \\ & & \overline{x}^{mn} & \longmapsto & (\overline{x}^m, \overline{x}^n) \end{array}$$

  est un isomorphisme d'anneaux.
- Pour n entier ≥ 2, on note $\mathcal{D}_n$ l'ensemble des diviseurs poritifs de n.

Partie I : Questions préliminaires.

Q1. Soit G un groupe et $a \in G$ d'ordre fini m.

1. Soit $k \in \mathbb{N}^*$. Montrer que l'ordre de a^k est égal à $\dfrac{m}{m \wedge k}$.
2. En déduire l'ordre de $\overline{k}$ dans le groupe additif $(\mathbb{Z}/n\mathbb{Z}, +)$.

Q2. Soient m, n deux entiers ≥ 2. Montrer que $\mathbb{U}(\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}) = \mathbb{U}(\mathbb{Z}/m\mathbb{Z}) \times \mathbb{U}(\mathbb{Z}/n\mathbb{Z})$.

Partie II : Arithmétiques dans l'anneau $\mathbb{Z}/n\mathbb{Z}$.

Q3. Soit n un entier ≥ 2.

1. Montrer l'équivalence : $\overline{k} \in \mathbb{U}(\mathbb{Z}/n\mathbb{Z}) \iff k \wedge n = 1$.
2. En déduire l'ordre du groupe $\mathbb{U}(\mathbb{Z}/n\mathbb{Z})$.
3. En déduire le théorème d'Euler :

$$\forall k \in \mathbb{N},\ \ k \wedge n = 1 \implies k^{\varphi(n)} \equiv 1\ [n].$$

4. Écrire une fonction `InvPhi(n)` en language Python qui renvoie la liste des inversibles de l'anneau $\mathbb{Z}/n\mathbb{Z}$ et qui calcul le nombre $\varphi(n)$.

Q4. Soit p un nombre premier.

1. Déterminer $\varphi(p)$. En déduire $\max\limits_{0 \leq k \leq n-1} \varphi(k)$.
2. En déduire le petit théorème de Fermat : Si k est un entier et p un nombre premier non diviseur de k, alors

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

Partie III : Calcul de $\varphi(n)$.

Q5. Soit p un nombre premier et r un entier ≥ 1.

1. Soit $k \in [\![0, p^r - 1]\!]$. Montrer l'équivalence : $k \notin \mathcal{E}_{p^r} \iff p \mid k$.
2. Montrer que $\operatorname{Card}\left([\![0, p^r - 1]\!] \setminus \mathcal{E}_{p^r}\right) = p^{r-1}$.
3. En déduire que $\varphi(p^r) = p^r - p^{r-1}$.

Q6. Soient m, n deux entiers ≥ 2 premiers entre eux.

1. Montrer que l'application

$$\begin{array}{rccc} g & : & \mathbb{U}(\mathbb{Z}/mn\mathbb{Z}) & \longrightarrow & \mathbb{U}(\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}) \\ & & \overline{x}^{mn} & \longmapsto & (\overline{x}^m, \overline{x}^n) \end{array}$$

est bijective. **Indication :** on pourra utiliser le théorème des restes chinois.

2. En déduire que $\varphi(mn) = \varphi(m)\varphi(n)$. **Indication :** on pourra utiliser la question Q2.

Q7. En déduire que, si n est un entier ≥ 2 et $n = p_1^{\alpha_1} \dots p_r^{\alpha_r}$ la décomposition de n en facteurs premiers,

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

Partie IV : L'identité $n = \sum_{d \in \mathcal{D}_n} \varphi(d)$.

Dans cette partie, on va établir par deux méthodes différentes, l'identité $n = \sum_{d \in \mathcal{D}_n} \varphi(d)$.

Première méthode

On se place dans le groupe additif $(\mathbb{Z}/n\mathbb{Z}, +)$. Soit $d \in \mathcal{D}_n$ et $\mathcal{O}_d = \left\{ \overline{k} \in \mathbb{Z}/n\mathbb{Z},\ \overline{k} \text{ est d'ordre } d \right\}$.

Q8. On considère l'application $\begin{array}{rccc} h & : & \mathcal{E}_d & \longrightarrow & \mathcal{O}_d \\ & & k & \longmapsto & \frac{n}{d}.\overline{k} \end{array}$

1. Montrer que h est bien définie. **Indication :** on pourra utiliser la question Q1. 2.
2. Montrer que h est injective.
3. Montrer que h est surjective.
4. Justifier que $(\mathcal{O}_d)_{d \in \mathcal{D}_n}$ forme une partition de $\mathbb{Z}/n\mathbb{Z}$.

Q9. En déduire que, pour tout entier $n \geq 1$, on a l'égalité $n = \sum_{d \in \mathcal{D}_n} \varphi(d)$.

Deuxième méthode

On pose, pour $n \geq 1$, $\Theta(n) = \sum_{d \in \mathcal{D}_n} \varphi(d)$.

Q10. Soit p un nombre premier. Montrer que, pour tout entier r non nul, $\Theta(p^r) = p^r$.
Indication : on pourra utiliser la question Q5. 3.

Q11. Soient m_1, m_2 deux entiers naturels premiers entre eux. On considère l'application

$$\begin{array}{rccc} \phi & : & \mathcal{D}_{m_1} \times \mathcal{D}_{m_2} & \longrightarrow & \mathcal{D}_{m_1 m_2} \\ & & (d_1, d_2) & \longmapsto & d_1 d_2 \end{array}.$$

1. Vérifier que ϕ est bien définie.
2. Montrer que ϕ est injective.
3. Montrer que ϕ est surjective.
4. En déduire la relation $\Theta(m_1)\Theta(m_2) = \Theta(m_1 m_2)$. **Indication :** on pourra utiliser la question Q6. 2.

Q12. Montrer que pour tout entier $n \geq 1$, on a l'égalité $n = \sum_{d \in \mathcal{D}_n} \varphi(d)$.

Problème 2

Notations et rappels

- On appelle forme linéaire sur un $\mathbb{R}$-ev E toute application linéaire de E à valeurs dans $\mathbb{R}$.
- Un hyperplan H d'un $\mathbb{R}$-ev E est le noyau d'une forme linéaire non nulle sur E.
- On rappelle la décomposition $E = H \oplus \text{Vect}(a)$ pour tout $a \in E \setminus H$.

Partie I :

Q1. Dans cette question, $(E, \|.\|)$ est un $\mathbb{R}$-espace vectoriel normé de dimension finie, x_0 un vecteur de E et H un hyperplan de E.

1. On note $\mathrm{d}(x_0, H)$ la distance de x_0 à l'hyperplan H : $\mathrm{d}(x_0, H) = \inf\limits_{y \in H} \|x_0 - y\|$.

   Justifier l'existence d'une suite $(y_n)_{n \geq 0}$ d'éléments de H tels que
   $$\|x_0 - y_n\| \xrightarrow[n \to +\infty]{} \mathrm{d}(x_0, H).$$
2. Montrer que la suite $(y_n)_{n \geq 0}$ possède une valeur d'adhérence dans H.
3. En déduire qu'il existe $y \in H$ tel que
   $$\mathrm{d}(x_0, H) = \|x_0 - y\|.$$
   On dit que la distence de x_0 à H est ***atteinte*** en y.

Q2. Dans cette question, $(E, \|.\|)$ est un $\mathbb{R}$-espace vectoriel normé de dimension quelconque.

1. Montrer que si h est une forme linéaire continue sur E alors le noyau, $\ker h$, est fermé dans E.
2. Soit h une forme linéaire sur E telle que $\ker h$ est fermé dans E. Suspposons h n'est pas continue sur E.
   - **a.** Construire une suite $(t_n)_{n \geq 0} \in E^{\mathbb{N}}$ telle que :
   $$\lim_{n \to +\infty} t_n = 0 \quad \text{et} \quad h(t_n) = 1 \text{ pour tout } n \in \mathbb{N}.$$
   - **b.** En considérant la suite $(t_n - t_0)_{n \geq 0}$, aboutir à une contradiction, puis conclure.
3. Montrer que si H est un hyperplan de E, alors $\overline{H}$ est un sous-espace vectoriel de E.
4. En déduire que tout hyperplan de E est fermé ou dense dans E c-à-d $\overline{H} = H$ ou $\overline{H} = E$.
   Indication : on pourra utiliser la décomposition $E = H \oplus \text{Vect}(a)$ pour tout $a \in E \setminus H$.

Partie II :

On suppose dans cette partie que H est un hyperplan fermé d'un $\mathbb{R}$-espace vectoriel $(E, \|.\|)$ de dimension quelconque. H est le noyau de la forme linéaire h, continue non nulle sur E.

On rappelle que la norme de l'application h subordonnée à la norme de E est définie par :
$$||| h ||| = \sup_{x \neq 0} \frac{|h(x)|}{\|x\|}.$$

Q3. Soit $x_0 \in E$ fixé.

1. Montrer que, pour tout y de H, on a :
   $$\|x_0 - y\| \geq \frac{|h(x_0)|}{||| h |||}.$$
2. En déduire que $\mathrm{d}(x_0, H) \geq \dfrac{|h(x_0)|}{||| h |||}$.
3. Montrer que $\mathrm{d}(x_0, H) = 0 \iff x_0 \in H$.

Q4. On considère dans cette question $x_0 \notin H$.

1. Montrer qu'il existe une suite $(w_n)_{n\geq 0}$ d'éléments de $E \setminus \{0\}$ vérifiant :

$$|||\ h\ |||= \lim_{n\to+\infty} \frac{|h(w_n)|}{\|w_n\|}.$$

2. Justifier que, pour tout entier n, il existe un réel λ_n et un vecteur y_n de H tel que : $w_n = \lambda_n x_0 + y_n$.

3. Prouver que, pour tout entier n :

$$\frac{|h(w_n)|}{\|w_n\|} \leq \frac{|h(x_0)|}{\mathrm{d}(x_0, H)}.$$

Q5. En déduire que, pour tout vecteur $x_0 \in E$, on a :

$$\mathrm{d}(x_0, H) = \frac{|h(x_0)|}{|||\ h\ |||}.$$