

PREMIER DEVOIR DE CONTROLE
Section : MP 2

Épreuve : MATHÉMATIQUES II

Durée : 2 heures

L'épreuve comporte deux pages.

• **Notations :** Dans tout ce problème, n est un entier ≥ 2 . On note :

- $\mathcal{D}(n)$ l'ensemble des diviseurs positifs de n .
- $\varphi(n) = \text{Card}(\{k \in \{1, \dots, n\} \mid k \wedge n = 1\})$.
- $\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, \dots, \overline{n-1}\}$ l'ensemble des classes d'équivalence de la congruence modulo n dans $\mathbb{Z}$.
- $\mathcal{U}(\mathbb{Z}/n\mathbb{Z})$ l'ensemble des éléments inversibles de l'anneau $(\mathbb{Z}/n\mathbb{Z}, +, \times)$.
- $\text{ord}(a)$ l'ordre d'un élément a (quand il existe) dans un groupe G .

• **Rappels :** On rappelle que

- L'ensemble $\mathcal{U}(\mathbb{Z}/n\mathbb{Z})$ muni de la multiplication $\times$ est un groupe.
- Une famille $(A_i)_{i \in I}$ de parties d'un ensemble E est dite partition de E si
 1. $E = \bigcup_{i \in I} A_i$
 2. $\forall (i, j) \in I^2, \quad i \neq j \Rightarrow A_i \cap A_j = \emptyset$

• **Objectif :** Il est bien connu que le groupe additif $(\mathbb{Z}/n\mathbb{Z}, +)$ est cyclique. Dans ce problème, on étudiera la cyclicité du groupe multiplicatif $(\mathcal{U}(\mathbb{Z}/n\mathbb{Z}), \times)$ pour certaines valeurs de n .

Les parties II et III sont indépendantes.

I. Préliminaires (8,5 points)

1. Montrer que pour tout $k \in \mathbb{Z}$,

$$\overline{k} \in \mathcal{U}(\mathbb{Z}/n\mathbb{Z}) \Leftrightarrow k \wedge n = 1$$

Que vaut alors $\text{Card}(\mathcal{U}(\mathbb{Z}/n\mathbb{Z}))$?

2. Montrer que l'anneau $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ est un corps si, et seulement si, n est premier.

3. Dans cette question uniquement, on suppose que $n \geq 3$. Déterminer l'ordre de l'élément $\overline{n-1}$ dans le groupe $(\mathcal{U}(\mathbb{Z}/n\mathbb{Z}), \times)$. En déduire que $\varphi(n)$ est pair.

4. Pour tout diviseur positif d de n , on pose $E_d = \{\frac{k}{d} \mid k \in \{1, \dots, d\} \text{ et } k \wedge d = 1\}$

(a) Montrer que la famille $(E_d)_{d \in \mathcal{D}(n)}$ forme une partition de l'ensemble $\{\frac{1}{n}; \frac{2}{n}; \dots; \frac{n}{n}\}$.

(b) En déduire l'identité

$$\sum_{d \in \mathcal{D}(n)} \varphi(d) = n \quad (*)$$

5. Montrer qu'un groupe fini G est cyclique si, et seulement si, il existe $a \in G$ tel que $\text{ord}(a) = \text{Card}(G)$.
6. Soit $(G, \cdot)$ un groupe cyclique de cardinal n et a un générateur de G .
 - (a) Montrer que si f est un morphisme surjectif de G vers un autre groupe G' , alors $f(a)$ est un générateur de G' .
 - (b) Justifier qu'il existe un isomorphisme Ψ de groupe G vers le groupe additif $(\mathbb{Z}/n\mathbb{Z}, +)$.
 - (c) Montrer que pour tout $b \in G$,

$$b \text{ est un générateur de } G \Leftrightarrow \Psi(b) \text{ est un générateur de } \mathbb{Z}/n\mathbb{Z}$$

- (d) Déterminer alors le nombre de générateurs de G .

II. Le cas où $n=2^\alpha$ avec $\alpha \in \mathbb{N}^*$ (5 points)

1. Montrer que les groupes $(\mathcal{U}(\mathbb{Z}/2\mathbb{Z}), \times)$ et $(\mathcal{U}(\mathbb{Z}/4\mathbb{Z}), \times)$ sont cycliques.
2. Déterminer l'ordre de chaque élément du groupe $(\mathcal{U}(\mathbb{Z}/8\mathbb{Z}), \times)$. Ce groupe est-il cyclique?
3. Soit α un entier ≥ 4 . Pour tout $a \in \mathbb{Z}$, on note $\bar{a}$ (resp $\hat{a}$) la classe de a modulo 2^α (resp modulo 8).

- (a) Pour tous $a, b \in \mathbb{Z}$, montrer que

- i. si $a \equiv b [2^\alpha]$ alors $a \equiv b [8]$.
- ii. si $\bar{a} \in \mathcal{U}(\mathbb{Z}/2^\alpha\mathbb{Z})$ alors $\hat{a} \in \mathcal{U}(\mathbb{Z}/8\mathbb{Z})$.

On peut ainsi définir une application $f : \mathcal{U}(\mathbb{Z}/2^\alpha\mathbb{Z}) \rightarrow \mathcal{U}(\mathbb{Z}/8\mathbb{Z})$ en posant

$$f(\bar{a}) = \hat{a} \text{ pour tout } a \in \mathbb{Z}$$

- (b) Montrer que f est un morphisme de groupes surjectif.
- (c) Dédire que $(\mathcal{U}(\mathbb{Z}/2^\alpha\mathbb{Z}), \times)$ n'est pas cyclique. (indication: utiliser la question I.6.a).

III. Le cas où n est premier (6,5 points)

Soit p un nombre premier impair. Dans ce cas $\mathbb{Z}/p\mathbb{Z}$ est un corps et $\mathcal{U}(\mathbb{Z}/p\mathbb{Z}) = \mathbb{Z}/p\mathbb{Z} \setminus \{\bar{0}\} = (\mathbb{Z}/p\mathbb{Z})^*$.
Pour tout $d \in \mathcal{D}(p-1)$, on pose

$$\mathcal{O}_d = \{\bar{x} \in (\mathbb{Z}/p\mathbb{Z})^* \mid \text{ord}(\bar{x}) = d\} \text{ et } \mathcal{S}_d = \{\bar{x} \in (\mathbb{Z}/p\mathbb{Z})^* \mid \bar{x}^d = \bar{1}\}$$

On admet qu'un polynôme de degré $d \geq 1$ à coefficients dans un corps k admet au plus d racines dans k .

1. Soit $d \in \mathcal{D}(p-1)$. Vérifier que
 - (a) $\mathcal{O}_d \subset \mathcal{S}_d$ et $\text{Card}(\mathcal{S}_d) \leq d$.
 - (b) $\mathcal{S}_d$ est un sous-groupe de $((\mathbb{Z}/p\mathbb{Z})^*, \times)$.
2. Montrer que s'il existe $\bar{a} \in (\mathbb{Z}/p\mathbb{Z})^*$ tel que $\text{ord}(\bar{a}) = d$, alors $\mathcal{S}_d = \langle \bar{a} \rangle$.
3. En déduire que si $\mathcal{O}_d \neq \emptyset$, alors $\text{Card}(\mathcal{O}_d) = \varphi(d)$. (indiction: utiliser la question I.6.d).
4. Vérifier que $(\mathcal{O}_d)_{d \in \mathcal{D}(p-1)}$ forme une partition de $(\mathbb{Z}/p\mathbb{Z})^*$. En déduire que

$$p-1 = \sum_{d \in \mathcal{D}(p-1), \mathcal{O}_d \neq \emptyset} \varphi(d)$$

5. En utilisant l'identité (*), démontrer que les $\mathcal{O}_d$ sont tous non vides.
6. En déduire que le groupe $((\mathbb{Z}/p\mathbb{Z})^*, \times)$ est cyclique.

Fin de l'énoncé.