CONCOURS D'ADMISSION 2025

FILIERE UNIVERSITAIRE INTERNATIONALE
FORMATION FRANCOPHONE
FUI-FF_Session 2_Printemps

Épreuve d'entraînement n°1

MATHEMATIQUES

Durée : 3 heures

L'utilisation des calculatrices n'est pas autorisée pour cette épreuve

La présentation, la lisibilité, l'orthographe, la qualité de la rédaction, la clarté, la précision et la concision des raisonnements entreront pour une part importante dans l'appréciation des copies.
Les candidats sont invités à encadrer dans la mesure du possible les résultats de leurs calculs. L'usage de tout document et de tout matériel électronique est interdit.

Ce devoir comporte 2 exercices (de cours) et 1 problème : **le résultat des exercices est indispensable pour traiter le problème**. Les questions doivent être traitées dans l'ordre. Si le candidat saute une question, il le signale sur sa copie.

I) Exercice 1 - L'anneau des entiers de Gauss, étude préliminaire

On note :

$$\mathbb{Z}[\mathrm{i}] = \{P(\mathrm{i}), P \in \mathbb{R}[X]\}$$

1. Montrer que $\mathbb{Z}[\mathrm{i}]$ est un sous-anneau de $\mathbb{C}$.
2. Montrer que $\mathbb{Z}[\mathrm{i}] = \{a + \mathrm{i}b \mid (a,b) \in \mathbb{Z}^2\}$.
3. On définit
$$N : (a+\mathrm{i}b) \in \mathbb{Z}[\mathrm{i}] \longmapsto (a+\mathrm{i}b)(a-\mathrm{i}b)$$
Montrer que N est à valeurs dans $\mathbb{N}$.
4. *Inversibles.*
   (a) Montrer que l'ensemble des inversibles de $\mathbb{Z}[\mathrm{i}]$ est donné par :
   $$\mathbb{Z}[\mathrm{i}]^* = \{z \in \mathbb{Z}[\mathrm{i}] \mid N(z) = 1\}$$
   (b) Montrer que
   $$\mathbb{Z}[\mathrm{i}]^* = \{\pm 1; \pm \mathrm{i}\}$$
5. (a) Montrer que $\mathbb{Z}[\mathrm{i}]$ est euclidien avec le stathme N.
   (b) En déduire que $\mathbb{Z}[\mathrm{i}]$ est principal.
6. Soit π un irréductible de $\mathbb{Z}[\mathrm{i}]$. Montrer que si $\pi \mid \alpha_1 \dots \alpha_n$, alors $\pi \mid \alpha_i$ pour un certain $i \in [\![1, n]\!]$.

II) Exercice 2 - Les carrés de $\mathbb{F}_p$

Soit p un nombre premier.

1. Soit G un groupe fini. Soit φ un morphisme de groupes. Montrer que
$$|G| = |\mathrm{Ker}\,\varphi||\mathrm{Im}\,\varphi|$$
2. On considère
$$\varphi : \left\{ \begin{array}{ccc} \mathbb{F}_p^* & \longrightarrow & \mathbb{F}_p^* \\ x & \longmapsto & x^2 \end{array} \right.$$
Dénombrer les carrés de $\mathbb{F}_p$.

3. (a) Montrer que si -1 est un carré dans $\mathbb{F}_p$, alors $p = 2$ ou $p \equiv 1[4]$.
   (b) Montrer la réciproque.

III) Problème - Le théorème des deux carrés

Si p est un nombre premier et $n \in \mathbb{N}^*$, on désigne par $v_p(n)$ la valuation p-adique de l'entier n. On conserve les notations des deux exercices précédents. Fixons par ailleurs

$$\Sigma_2 = \{n \in \mathbb{N} \mid \exists (a,b) \in \mathbb{N}^2, n = a^2 + b^2\}$$

A) Caractérisation des irréductibles de $\mathbb{Z}[i]$

Le but de cette partie est de démontrer le Lemme suivant, qui nous sera utile à la démonstration du théorème des deux carrés.

Lemme III.A.1

Soit p un nombre premier. Alors les propositions suivantes sont équivalentes :

- $p \in \Sigma_2$
- p est réductible dans $\mathbb{Z}[i]$.
- $p = 2$ ou $p \equiv 1[4]$.

1. Montrer que si $p \in \Sigma_2$, alors p est réductible dans $\mathbb{Z}[i]$.
2. Supposons p réductible dans $\mathbb{Z}[i]$.
   (a) Montrer qu'il existe $a, b \in \mathbb{Z}[i]$ non-inversibles tels que $N(p) = N(a)N(b)$.
   (b) Montrer que $N(a) = N(b) = p$.
   (c) Montrer que $p \in \Sigma_2$.
3. (a) Montrer que la somme de deux carrés n'est jamais congrue à 3 modulo 4.
   (b) Supposons $p \in \Sigma_2$. Montrer que si $p \neq 2$, alors $p \equiv 1[4]$.
4. On suppose que $p \equiv 1[4]$. Par l'absurde, on suppose p irréductible dans $\mathbb{Z}[i]$.
   (a) Montrer qu'il existe $x \in \mathbb{Z}$, tel que $p \mid x^2 + 1$.
   (b) Montrer que p divise $x + i$ ou p divise $x - i$.
   (c) Aboutir à une contradiction, et conclure.

B) Démonstration du théorème des deux carrés

Théorème III.B.1: Théorème des deux carrés de Fermat

Soit $n \in \mathbb{N}^*$. n est une somme de deux carrés *si et seulement si* pour tout p premier tel que $p \equiv 1[4]$, p a une valuation paire dans la décomposition en facteurs premiers de n.

On peut reformuler ce théorème ainsi avec les notations de l'énoncé :

$$n \in \Sigma_2 \iff (\forall p \text{ premier}, p \equiv 1[4] \Rightarrow v_p(n) \in 2\mathbb{N})$$

1. Montrer que Σ_2 est stable par multiplication. En déduire la réciproque du théorème précédent.

Fixons p un nombre premier vérifiant $p \equiv 3[4]$. On montre par récurrence forte pour tout $k \in \mathbb{N}$ la propriété suivante :

$$\mathcal{P}_k : \text{« Pour tout } n \in \Sigma_2 \backslash \{0\} \text{ avec } v_p(n) \leqslant k, \text{ l'entier } v_p(n) \text{ est pair »}.$$

L'initialisation est évidente. Soit $k \in \mathbb{N}$ tel que $\forall j \leqslant k, \mathcal{P}_j$ est vraie. On montre $\mathcal{P}_{k+1}$. Soit $n = a^2 + b^2 \neq 0$ tel que $v_p(n) \leqslant k+1$.

2. Montrer que $p \mid a$ et $p \mid b$.
3. Montrer que $p^2 \mid n$.
4. En appliquant l'hypothèse de récurrence à un entier bien choisi, montrer $\mathcal{P}_{k+1}$.

C) Prolongement : le théorème des quatre carrés

Nous allons démontrer le théorème suivant :

Théorème III.C.1: Théorème des quatre carrés de Lagrange

Tout entier positif peut s'exprimer comme la somme de quatre carrés.

C.1 Lemme de Chevalley

Lemme III.C.1

Pour tout nombre premier impair p, il existe des entiers naturels a et b tels que $p \mid 1 + a^2 + b^2$.

Posons

$$\Sigma_4 = \{n \in \mathbb{N} \mid \exists (a,b,c,d) \in \mathbb{N}^4, n = a^2 + b^2 + c^2 + d^2\}$$

1. Soient $a, b \in \left[\!\left[0, \dfrac{p-1}{2}\right]\!\right]$. Montrer que les a^2 et les $-b^2 - 1$ sont incongrus deux-à-deux modulo p.
2. Prouver qu'il existe $a, b \in \left[\!\left[0, \dfrac{p-1}{2}\right]\!\right]$ tels que $a^2 \equiv -b^2 - 1[p]$ et conclure.
3. Soit $m = \min\{n \in \mathbb{N}^* \mid np \in \Sigma_4\}$. Montrer que $m < p$.

C.2 Lemme principal et démonstration

Lemme III.C.2: Lemme principal

Tout nombre premier impair p est somme de quatre carrés.

On considère

$$m = \min\{n \in \mathbb{N}^* \mid np \in \Sigma_4\} < p$$

On souhaite montrer que $m = 1$. Par l'absurde, on suppose $m > 1$.

4. Soient $(x_1, x_2, x_3, x_4) \in \mathbb{N}^4$ tels que $mp = \sum_{k=1}^{4} x_k^2$. Montrer qu'il existe $(y_1, y_2, y_3, y_4) \in \left[\!\left[\frac{-m+1}{2}, \frac{m}{2} \right]\!\right]^4$ et $r \in [\![0, m-1]\!]$ tels que $mr = \sum_{k=1}^{4} y_k^2$.
5. *Identité des quatre carrés d'Euler.* Montrer les identités suivantes :

$$\begin{aligned}(a^2+b^2+c^2+d^2)(p^2+q^2+r^2+s^2) &= (ap+bq+cr+ds)^2 + (aq-bp-cs+dr)^2 \\ &\quad + (ar+bs-cp-dq)^2 + (as-br+cq-dp)^2\end{aligned}$$

$$\begin{aligned}(a^2+b^2+c^2+d^2)(p^2+q^2+r^2+s^2) &= (ap+bq+cr+ds)^2 + (aq-bp+cs-dr)^2 \\ &\quad + (ar-bs-cp+dq)^2 + (as+br-cq-dp)^2\end{aligned}$$

6. Prouver qu'il existe $(z_1, z_2, z_3, z_4) \in \mathbb{N}^4$ tels que $(mp)(mr) = \sum_{k=1}^{4} z_k^2$, et tels que pour tout $k \in [\![1, 4]\!]$, $m \mid z_k$.
7. Montrer le lemme principal.
8. Conclure en démontrant le théorème des quatre carrés.

IV) Hors-barème : Une autre démonstration du Lemme III.A.1

Ne traiter cette partie que si toutes les parties précédentes ont déjà été traitées.

Soit A un anneau, et I un idéal bilatère de A. Posons $\sim_I$ la relation d'équivalence (on ne demande pas de le vérifier) :

$$\forall (x, y) \in A^2, x \sim_I y \iff x - y \in I$$

On **admet** qu'alors l'ensemble quotient (l'ensemble des classes d'équivalence) par la relation $\sim$, noté $A/I \overset{\text{déf.}}{=} A/\sim_I$ est muni des lois quotients $\overline{+}$ et $\overline{\times}$, de sorte à ce que A/I ait une

structure d'anneau.
A/I est appelé l'anneau quotient de A par I.

Par exemple,

- A/A est l'anneau trivial (réduit à 0).
- $A/\{0\}$ est isomorphe à A.
- Si $A = \mathbb{Z}$ et $I = n\mathbb{Z}, n \in \mathbb{N}$, alors A/I est $\mathbb{Z}/n\mathbb{Z}$.
- Si $A = \mathbb{R}[X]$ et $I = (X^2+1) = (X^2+1)\mathbb{R}[X]$, A/I est isomorphe à $\mathbb{C}$ (admis)

1. Supposons que p est réductible dans $\mathbb{Z}[\mathrm{i}]$. Alors $p = ab$ avec $(a,b) \in \mathbb{Z}[\mathrm{i}]^2$ non-inversibles. Montrer que l'anneau $\mathbb{Z}[\mathrm{i}]/(p)$ n'est pas intègre.
2. Supposons que $\mathbb{Z}[\mathrm{i}]/(p)$ est intègre. Montrer que p est irréductible dans $\mathbb{Z}[\mathrm{i}]$.

Ainsi, on a démontré que p est irréductible dans $\mathbb{Z}[\mathrm{i}]$ *si et seulement si* $\mathbb{Z}[\mathrm{i}]/(p)$ est intègre.

3. *Premier isomorphisme.* On souhaite montrer que $\mathbb{Z}[\mathrm{i}] \simeq \mathbb{Z}[X]/(X^2+1)$.
   (a) Montrer que $\varphi : \mathbb{Z}[X] \longmapsto \mathbb{Z}[\mathrm{i}]$ défini de façon unique par $\varphi(X) = \mathrm{i}$ est un morphisme d'anneaux surjectif.
   (b) Vérifier que $\operatorname{Ker}\psi$ est un idéal bilatère de $\mathbb{Z}[X]$. Montrer que $\operatorname{Ker}\psi = (X^2+1)$.
   (c) Montrer que ψ « passe au quotient »(c'est-à-dire que ψ est constant sur chaque classe d'équivalence par $\sim_{\operatorname{Ker}\psi}$), et qu'on peut ainsi définir un morphisme :

$$\overline{\psi} : \begin{cases} \mathbb{Z}[X]/\operatorname{Ker}\psi & \longrightarrow & \mathbb{Z}[\mathrm{i}] \\ \overline{Q} & \longmapsto & Q(\mathrm{i}) \end{cases}$$

   (d) Montrer que $\overline{\psi}$ est un isomorphisme d'anneaux.
4. *Deuxième isomorphisme.*
   (a) Montrer le lemme suivant : si A est un anneau, et $a, b \in A$, montrer que :

$$(A/(a))/(b) \simeq A/(a,b) \simeq (A/(b))/(a)$$

   (b) Montrer que $\mathbb{Z}[X]/(p) \simeq \mathbb{F}_p[X]$.
5. Déduire des questions précédentes que $\mathbb{Z}[\mathrm{i}]/(p) \simeq \mathbb{F}_p[X]/(X^2+1)$.
6. Montrer que l'anneau $\mathbb{F}_p[X]/(X^2+1)$ est intègre *si et seulement si* (X^2+1) est irréductible.
7. En déduire que p est réductible dans $\mathbb{Z}[\mathrm{i}]$ *si et seulement si* -1 est un carré dans $\mathbb{F}_p$.