Concours Centrale-Supélec, France

# Session 2004, filière MP

## Mathématiques 2

### Ce que traite le sujet

- Partie I : matrices carrées d'ordre 2 à coefficients entiers
- Partie II : réseaux de C
- Partie III : similitudes directes de centre O laissant stable un réseau

**Sujet reproduit sans retouche à partir de la page suivante.**

Résumé des parties, chapitres de cours liés et autres années :
prepahelp.com/annales/centrale/mp/2004/maths2

Prepa Help ne revendique aucun droit sur le sujet, propriété de l'organisateur du concours.

# MATHÉMATIQUES II

## *Objectif du problème*

Cette introduction est destinée à expliquer le type des résultats obtenus dans le problème. Ce dernier ne commence qu'à partir du I.

Dans la démonstration en 1994 du « dernier théorème » de Fermat par Andrew Wiles, les « courbes elliptiques » jouent un rôle central par le biais de l'action du groupe $SL_2(\mathbb{Z})$ sur le demi-plan ouvert $\mathscr{H} = \{z \in \mathbb{C} : \mathscr{I}m(z) > 0\}$.

En effet, il se trouve que l'ensemble des courbes elliptiques sur le corps $\mathbb{C}$ est en bijection (à un $\mathbb{C}$-isomorphisme près) avec l'ensemble des réseaux de $\mathbb{C}$ (à une similitude près), lui même en bijection avec l'ensemble des orbites du demi-plan $\mathscr{H}$ sous l'action de $SL_2(\mathbb{Z})$. Ce sont quelques propriétés de ces deux derniers ensembles que nous proposons d'étudier dans ce problème.

## *Partie I - Matrices carrées d'ordre 2 à coefficients entiers*

Soit $\mathscr{M}_2(\mathbb{Z})$ l'ensemble des matrices $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ carrées d'ordre 2 à coefficients dans l'anneau $\mathbb{Z}$ des entiers relatifs.

Dans les parties I, II, III, les lettres $a$, $b$, $c$, $d$ désignent des éléments de $\mathbb{Z}$. On pose :

$$I_2 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}.$$

**I.A -** Démontrer que l'ensemble $\mathscr{M}_2(\mathbb{Z})$ est un anneau.

**I.B -**

I.B.1) Démontrer que l'ensemble $GL_2(\mathbb{Z})$ des éléments de $\mathscr{M}_2(\mathbb{Z})$ inversibles dans $\mathscr{M}_2(\mathbb{Z})$ est un groupe pour la multiplication, appelé le groupe des unités de l'anneau $\mathscr{M}_2(\mathbb{Z})$.

I.B.2) Montrer que

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in GL_2(\mathbb{Z}) \text{ si et seulement si } |ad - bc| = 1.$$

# Filière MP

**I.C -** On pose

$$SL_2(\mathbb{Z}) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathcal{M}_2(\mathbb{Z}) : ad - bc = 1 \right\} ;$$

I.C.1) Montrer que $SL_2(\mathbb{Z})$ est un groupe pour la multiplication des matrices.

I.C.2) Déterminer l'ensemble des couples $(c,d) \in \mathbb{Z} \times \mathbb{Z}$ tels que la matrice

$\begin{bmatrix} 3 & 5 \\ c & d \end{bmatrix}$ appartienne à $SL_2(\mathbb{Z})$.

I.C.3) Déterminer l'ensemble des couples $(c,d) \in \mathbb{Z} \times \mathbb{Z}$ tels que la matrice

$\begin{bmatrix} 3 & 5 \\ c & d \end{bmatrix}$ appartienne à $GL_2(\mathbb{Z})$.

I.C.4) Quelle est la condition nécessaire et suffisante portant sur le couple $(a,b)$ de $\mathbb{Z} \times \mathbb{Z}$ pour qu'il existe une matrice

$\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ appartenant à $GL_2(\mathbb{Z})$ ?

**I.D -** Soient $S$ et $T$ les éléments de $SL_2(\mathbb{Z})$ définis par

$$S = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \text{ et } T = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} .$$

Pour chacune des trois matrices $T$, $S$ et $TS$, répondre aux questions suivantes :

I.D.1) La matrice est-elle diagonalisable, ou à défaut trigonalisable, dans $\mathcal{M}_2(\mathbb{C})$ ? Donner une forme réduite éventuelle ainsi qu'une matrice de passage.

I.D.2) La matrice est-elle diagonalisable, ou à défaut trigonalisable, dans $\mathcal{M}_2(\mathbb{R})$ ? Donner une forme réduite éventuelle ainsi qu'une matrice de passage.

**I.E -** On cherche les matrices $A$ de $SL_2(\mathbb{Z})$ telles que

$$A^2 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = I_2 .$$

I.E.1) Soit $A$ une telle matrice. Montrer que $A$ est diagonalisable dans $\mathscr{M}_2(\mathbb{R})$ et préciser les formes réduites diagonales possibles de $A$.

I.E.2) En déduire l'ensemble des matrices solutions $A$.

**I.F -**

On cherche les matrices $A$ de $SL_2(\mathbb{Z})$ telles que

$$A^2 = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}.$$

I.F.1) Soit $A$ une telle matrice. Montrer que $A$ est diagonalisable dans $\mathscr{M}_2(\mathbb{C})$ et calculer la trace $Tr(A)$ de $A$.

I.F.2) Donner la forme générale des matrices solutions $A$ en fonction des trois paramètres $a$, $b$, $c$ et d'une relation liant ces trois paramètres.

**I.G -**

I.G.1) Démontrer que si deux matrices $U$ et $V$ de $\mathscr{M}_2(\mathbb{R})$ sont semblables en tant que matrices de $\mathscr{M}_2(\mathbb{C})$, alors elles sont semblables dans $\mathscr{M}_2(\mathbb{R})$.

I.G.2) En déduire que les matrices $A$ de $SL_2(\mathbb{Z})$ solutions de l'équation :

$A^2 = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}$ sont semblables dans $\mathscr{M}_2(\mathbb{R})$ à la matrice $S = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$.

## *Partie II - Réseaux de* $\mathbb{C}$

On note $\mathscr{H}$ le demi-plan ouvert défini par $\mathscr{H} = \{z \in \mathbb{C} : Im(z) > 0\}$.

$\mathscr{B} = (\alpha, \beta)$ étant une base de $\mathbb{C}$ considéré comme plan vectoriel réel, on appelle réseau engendré par $\mathscr{B}$ l'ensemble $\Lambda_{\mathscr{B}} = \mathbb{Z}\alpha + \mathbb{Z}\beta = \{u\alpha + v\beta ; (u,v) \in \mathbb{Z}^2\}$.

Pour simplifier les notations, un réseau sera généralement désigné par la lettre $\Lambda$, sans préciser quelle base $\mathscr{B}$ de $\mathbb{C}$ l'engendre.

**II.A -**

II.A.1) De quelle structure algébrique est doté un réseau $\Lambda$ ?

II.A.2) Démontrer que tout réseau $\Lambda$ peut être engendré par une base

$\mathscr{B} = (\alpha, \beta)$ de $\mathbb{C}$ telle que $\frac{\alpha}{\beta} \in \mathscr{H}$.

II.A.3) Démontrer que pour tout quadruplet $(a, b, c, d) \in \mathbb{Z}^4$ et pour tout $z \in \mathbb{C}$ tel que $cz + d \neq 0$, on a

$$Im\left(\frac{az+b}{cz+d}\right) = \frac{ad-bc}{|cz+d|^2} Im(z).$$

**II.B -**

II.B.1) Démontrer que si deux bases $\mathscr{B} = (\omega_1,\omega_2)$ et $\mathscr{B}' = (\omega_1',\omega_2')$ de $\mathbb{C}$ telles que

$$\frac{\omega_1}{\omega_2} \in \mathscr{H} \text{ et } \frac{\omega'_1}{\omega'_2} \in \mathscr{H}$$

engendrent le même réseau $\Lambda$, alors il existe une matrice

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in SL_2(\mathbb{Z}) \text{ telle que } \begin{bmatrix} \omega'_1 \\ \omega'_2 \end{bmatrix} = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} \omega_1 \\ \omega_2 \end{bmatrix}.$$

II.B.2) Étudier la réciproque.

**II.C -** On considère un réseau $\Lambda$ engendré par une base $\mathscr{B} = (\omega_1,\omega_2)$ de $\mathbb{C}$ telle que

$$\frac{\omega_1}{\omega_2} \in \mathscr{H}$$

Déterminer l'ensemble des couples $(c,d) \in \mathbb{Z}^2$ tels que $\mathscr{B}' = (\omega_1',\omega_2')$ avec $\omega'_1 = 3\omega_1 + 5\omega_2$ et $\omega'_2 = c\omega_1 + d\omega_2$ soit une base de $\mathbb{C}$ engendrant également le réseau $\Lambda$.

**II.D -** Pour tout complexe $\tau \in \mathbb{C}\backslash\mathbb{R}$ on note $\Lambda_\tau$ le réseau engendré par la base $(\tau,1)$ de $\mathbb{C}$. On suppose que $\tau \in \mathscr{H}$. Trouver la condition nécessaire et suffisante pour qu'un élément $\tau' \in \mathscr{H}$ vérifie $\Lambda_{\tau'} = \Lambda_\tau$.

## *Partie III - Similitudes directes de centre O laissant stable un réseau*

Si $\Lambda$ est un réseau et $z$ un nombre complexe, on pose $z\Lambda = \{z\rho \ ; (\rho \in \Lambda)\}$.

On dit que deux réseaux $\Lambda$ et $\Lambda'$ sont semblables s'il existe $\lambda \in \mathbb{C}^*$ tel que $\Lambda' = \lambda\Lambda$.

**III.A -**

III.A.1) Démontrer que tout réseau $\Lambda$ est semblable à un réseau $\Lambda_\tau$ où $\tau \in \mathscr{H}$.

III.A.2) Démontrer que deux réseaux $\Lambda_\tau$ et $\Lambda_{\tau'}$, où $(\tau,\tau') \in \mathscr{H} \times \mathscr{H}$, sont semblables si et seulement si il existe une matrice

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in SL_2(\mathbb{Z}) \text{ telle que } \tau' = \frac{a\tau + b}{c\tau + d}.$$

*La fin de la partie III montre qu'il existe des similitudes directes de centre $O$, autres que des homothéties, laissant stable un réseau donné $\Lambda$.*

**III.B -** Soit $\Lambda$ un réseau.

III.B.1) Indiquer, sans faire de démonstration, le lien existant entre l'ensemble $S(\Lambda) = \{z \in \mathbb{C} \,;\, z\Lambda \subset \Lambda\}$ et l'ensemble des similitudes directes $\sigma$ de centre $O$ laissant stable le réseau $\Lambda$, c'est-à-dire telles que $\sigma(\Lambda) \subset \Lambda$.

III.B.2) Quel est l'ensemble des homothéties de centre $O$ laissant stable le réseau $\Lambda$ ? En déduire l'ensemble $S(\Lambda) \cap \mathbb{R}$.

III.B.3) De quelle structure algébrique est doté l'ensemble $S(\Lambda)$ ?

III.B.4) $\mathscr{B} = (\omega_1, \omega_2)$ étant une base de $\mathbb{C}$, on pose

$\tau = \dfrac{\omega_1}{\omega_2}$. Comparer les ensembles $S\left(\Lambda_{\mathscr{B}}\right)$ et $S(\Lambda_\tau)$.

III.B.5) Quelle relation d'inclusion existe-t-il entre les ensembles $S(\Lambda_\tau)$ et $\Lambda_\tau$ ?

**III.C -** $\tau$ étant un complexe de $\mathbb{C}\backslash\mathbb{R}$, on considère le réseau $\Lambda_\tau$ engendré par la base $(\tau, 1)$ de $\mathbb{C}$.

III.C.1) On suppose que l'ensemble $S(\Lambda_\tau)$ n'est pas réduit à $\mathbb{Z}$. Montrer que $\tau$ est alors racine d'un polynôme du second degré à coefficients dans $\mathbb{Z}$.

III.C.2) Réciproquement, on suppose que $\tau$ est racine non réelle d'un polynôme $P(X) = uX^2 + vX + w$ du second degré à coefficients $u$, $v$, $w$ dans $\mathbb{Z}$.

a) Montrer que $S(\Lambda_\tau)$ n'est pas contenu dans $\mathbb{R}$.

b) Que dire des ensembles $S(\Lambda_\tau)$ et $\Lambda_\tau$ si $u = 1$ ?

## *Partie IV - Action du groupe $\Gamma$ des homographies associées à $SL_2(\mathbb{Z})$ sur l'ensemble $\mathscr{H}$*

*Dans cette dernière partie, on étudie l'action de ce groupe $\Gamma$ sur l'ensemble $\mathscr{H}$. On introduit au IV.D un sous-ensemble fondamental $\mathscr{F}$ de $\mathscr{H}$. On montre aux questions IV.E et IV.F que $\Gamma$ est engendré par les homographies $s$ et $t$ associées aux matrices $S$ et $T$ introduites au I.D et qu'un système de représentants des orbites de $\Gamma$ est constitué par les points de $\mathscr{F}$.*

À toute matrice

$$A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

de $SL_2(\mathbb{Z})$ on associe l'application $g : \mathscr{H} \to \mathbb{C}$ définie par : $\forall \tau \in \mathscr{H},\ g(\tau) = \dfrac{a\tau + b}{c\tau + d}$.

**IV.A -**

IV.A.1) Montrer que l'on a $g(\mathscr{H}) \subset \mathscr{H}$. On identifie dorénavant $g$ avec l'application de $\mathscr{H}$ vers $\mathscr{H}$ qu'elle induit. Lorsque la matrice $A$ parcourt $SL_2(\mathbb{Z})$, l'application correspondante $g$ de $\mathscr{H}$ vers $\mathscr{H}$ décrit un ensemble noté $\Gamma$. Dans la suite de cette question on s'intéresse aux propriétés de la surjection

$$\Phi : \begin{cases} SL_2(\mathbb{Z}) \to \Gamma \\ A \mapsto g \end{cases}$$

IV.A.2) Montrer que $\Phi(A) \circ \Phi(A') = \Phi(AA')$. En déduire que la loi $\circ$ de composition des applications est une loi interne sur $\Gamma$.

IV.A.3) Pour tout $A \in SL_2(\mathbb{Z})$, montrer que $\Phi(A)$ est une bijection de $\mathscr{H}$ sur $\mathscr{H}$ et que l'on a $[\Phi(A)]^{-1} = \Phi(A^{-1})$. En déduire que $(\Gamma, \circ)$ est un groupe.

IV.A.4) Montrer que $\left[\Phi(A) = id_{\mathscr{H}}\right] \Leftrightarrow [A = \pm I_2]$.

IV.A.5)

a) Résoudre l'équation $\Phi(A') = \Phi(A)$.

b) En utilisant les matrices $S$ et $T$ définies en I.D, vérifier que le groupe $(\Gamma, \circ)$ n'est pas commutatif.

**IV.B -**

IV.B.1) Montrer que le cercle $\mathscr{C}(\omega, R)$ de centre $\omega \in \mathbb{C}$ et de rayon $R > 0$ a pour équation

$$|z|^2 - (\omega \bar{z} + \bar{\omega} z) + |\omega|^2 = R^2 .$$

À quelle condition nécessaire et suffisante ce cercle est-il inclus dans $\mathscr{H}$ ?

IV.B.2) On appelle $s$ l'application de $\mathscr{H}$ vers $\mathscr{H}$ associée à la matrice

$$S = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$$

définie au I.D, c'est-à-dire l'élément $s = \Phi(S)$ de $\Gamma$. Déterminer l'image par $s$ d'un cercle $\mathscr{C}(\omega, R)$ inclus dans $\mathscr{H}$.

**IV.C -**

IV.C.1) Trouver l'image par $s$ d'une droite $\mathscr{D}$ incluse dans $\mathscr{H}$, c'est-à-dire d'une droite $\mathscr{D}$ d'équation $y = \beta$, avec $\beta > 0$.

IV.C.2) Trouver l'image par $s$ d'une demi-droite $\mathscr{D}_+$ d'équation

$\begin{cases} x = \alpha \\ y > 0 \end{cases}$, où $\alpha \in \mathbb{R}$, incluse dans $\mathscr{H}$.

**IV.D -** On introduit le sous-ensemble $\mathscr{F}$ de $\mathscr{H}$, défini par

$$\mathscr{F} = \left\{ \tau \in \mathscr{H} : |\tau| \geq 1, \, | \, Re(\tau)| \leq \frac{1}{2} \right\}.$$

On appelle $t$ l'application de $\mathscr{H}$ vers $\mathscr{H}$ associée à la matrice

$$T = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$$

définie au I.D, c'est-à-dire l'élément $t = \Phi(T)$ de $\Gamma$. Représenter graphiquement l'ensemble $\mathscr{F}$ et ses images $t(\mathscr{F})$ et $t^{-1}(\mathscr{F})$ par les applications $t$ et $t^{-1}$.

**IV.E -** On note $G$ le sous-groupe de $\Gamma$ engendré par l'ensemble $\{s, t\}$. Soit $\tau$ un élément de $\mathscr{H}$.

IV.E.1) Montrer qu'il existe un élément $g_0 \in G$ tel que
$(\forall g \in G) \; Im(g(\tau)) \leq Im(g_0(\tau))$.

IV.E.2) On pose alors $\tau' = g_0(\tau)$. Démontrer qu'il existe un entier $m \in \mathbb{Z}$ tel que

$$\left| \, Re(t^m(\tau')) \right| \leq \frac{1}{2}.$$

IV.E.3) Vérifier que $\left| t^m(\tau') \right| \geq 1$ et en conclure que $t^m(\tau') \in \mathscr{F}$.

**IV.F -** On peut démontrer le résultat suivant, que l'on admettra ici : si $\tau \in \mathscr{F}$ et si pour un élément $g \in \Gamma$, avec $g \neq id_{\mathscr{H}}$, on a $g(\tau) \in \mathscr{F}$ alors $\tau$ est un point frontière de $\mathscr{F}$, autrement dit on a

$$Re(\tau) = \pm \frac{1}{2} \text{ ou } |\tau| = 1.$$

En utilisant ce résultat ainsi que ceux de la section IV.E, démontrer que $G = \Gamma$.

*Indication* : on pourra considérer un point $\tau$ intérieur à $F$ (c'est-à-dire $\tau \in \overset{\circ}{F}$) et son image $g(\tau)$ par $g \in \Gamma$.

---

**••• FIN •••**

---

# Prepa Help

prepahelp.com · classes préparatoires, Maroc et France

## Travailler les chapitres de ce sujet

Prepa Help suit le programme de MP chapitre par chapitre : cours détaillé, méthodes, pièges, exercices et problèmes corrigés pas à pas, tirés des concours. L'essai gratuit donne accès aux chapitres offerts de ta filière, sans carte bancaire.

### Chapitres liés à ce sujet

- ismes et dénombrement
- ble des entiers relatifs
- elles (spé)
- onor
- elles (sup)

### Ouvrir l'essai gratuit

Scanne le code ou clique sur le bouton.

**prepahelp.com/#essai**

Une question sur le concours ou sur ta filière : **écrire sur WhatsApp**

Les autres années et épreuves : prepahelp.com/annales/centrale/mp