**Exercice 1.** Racines carrées matricielles.

1. Racines carrées d'une matrice diagonale.

   Dans cette question, on considère la matrice $D = \begin{pmatrix} 1 & 0 \\ 0 & 4 \end{pmatrix}$.

   (a) Soit $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$. Que valent $DM$ et $MD$ ?
   Montrer que si $M$ commute avec $D$, elle est diagonale.
   La réciproque est-elle vraie ?

   (b) Soit $X \in M_2(\mathbb{R})$ telle que $X^2 = D$. Justifier que $X$ est diagonale.

   (c) Prouver que l'équation $X^2 = D$ possède exactement quatre solutions dans $M_2(\mathbb{R})$ que l'on explicitera.

2. Racines carrées d'une matrice diagonalisable.

   Dans cette question, on considère les matrices $A = \begin{pmatrix} 4 & 3 \\ 0 & 1 \end{pmatrix}$ et $P = \begin{pmatrix} 1 & 1 \\ -1 & 0 \end{pmatrix}$.

   (a) Prouver que $P$ est inversible et calculer $P^{-1}$. Vérifier que $A = PDP^{-1}$.

   (b) Soit $X \in M_2(\mathbb{R})$. Établir que

   $$X^2 = A \iff \left(P^{-1}XP\right)^2 = D.$$

   (c) Résoudre sur $M_2(\mathbb{R})$ l'équation $X^2 = A$.

**Exercice 2.** Matrices de permutations.

Dans cet exercice, $n$ est un entier naturel non nul.

On note $S_n$ l'ensemble des permutations de $[\![1, n]\!]$, c'est-à-dire des bijections de cet intervalle d'entiers vers lui-même. Nous savons que $(S_n, \circ)$ est un groupe, la loi $\circ$ étant la composition des applications.

Soit $\sigma \in S_n$. On note $P_\sigma = (a_{i,j})_{1 \leq i,j \leq n}$ la matrice de $M_n(\mathbb{R})$ définie par

$$\forall (i,j) \in [\![1, n]\!]^2 \quad a_{i,j} = \delta_{i,\sigma(j)} = \begin{cases} 1 & \text{si } \sigma(j) = i \\ 0 & \text{sinon.} \end{cases}$$

1. Exemples.

   (a) Dans cette question (seulement), $n = 3$. On définit $\gamma \in S_3$ par

   $$\gamma(1) = 2, \quad \gamma(2) = 3, \quad \gamma(3) = 1.$$

   Écrire la matrice $P_\gamma$.

   (b) Retour à $n$ quelconque. Que vaut $P_{\text{id}}$ ?

   (c) Comment s'interprète la trace d'une matrice de permutation ?

2. Montrer que
   $$\forall (\sigma, \sigma') \in (S_n)^2 \quad P_\sigma P_{\sigma'} = P_{\sigma \circ \sigma'}.$$

3. Montrer que

   $$\forall \sigma \in S_n \quad P_\sigma \in GL_n(\mathbb{K}) \quad \text{et} \quad (P_\sigma)^{-1} = P_{\sigma^{-1}}.$$

4. Notons $P_n(\mathbb{R})$ l'ensemble $\{P_\sigma \mid \sigma \in S_n\}$.
   Justifier qu'il s'agit d'un sous-groupe de $GL_n(\mathbb{R})$ isomorphe à $S_n$.

**Problème** : Entiers sommes de deux carrés.

L'objectif de ce problème est de déterminer quels sont les entiers naturels qui sont somme de deux carrés.

On pose $\mathbb{Z}[i] = \{a + ib \mid a \in \mathbb{Z}, b \in \mathbb{Z}\} \subset \mathbb{C}$ et $\mathbb{Z}[i]^* = \mathbb{Z}[i] \setminus \{0\}$.

Pour $z \in \mathbb{C}$, on pose $N(z) = z\overline{z}$.

## Partie I : Présentation de l'anneau $\mathbb{Z}[i]$.

1. Propriétés générales.
   (a) Vérifier que $\mathbb{Z}[i]$ est un sous-anneau de $(\mathbb{C}, +, \times)$.
   (b) i. Établir que pour tout $u \in \mathbb{Z}[i]$, $N(u) \in \mathbb{N}$.
   ii. Établir que pour tout $(u, v) \in (\mathbb{Z}[i])^2$, $N(uv) = N(u)N(v)$.
   (c) Un élément $u \in \mathbb{Z}[i]$ est dit inversible ssi il existe $v \in \mathbb{Z}[i]$ tel que $uv = 1$.
   Montrer que si $u$ est inversible alors $N(u) = 1$.
   Déterminer alors l'ensemble, noté $U$, des éléments inversibles de $\mathbb{Z}[i]$.

2. Divisibilité dans l'anneau $\mathbb{Z}[i]$.
   Pour $u$ et $v$ dans $\mathbb{Z}[i]$, on dit que $u$ **divise** $v$ dans $\mathbb{Z}[i]$ ssi il existe $s \in \mathbb{Z}[i]$ tel que $v = su$. On note alors $u \mid v$. Soit $(u, v, w) \in (\mathbb{Z}[i])^3$.
   (a) Montrer que la relation $\mid$ est transitive.
   (b) Montrer que si $u \mid v$ et $u \mid w$ alors $\forall (z, z') \in (\mathbb{Z}[i])^2$ $u \mid (vz + wz')$.
   (c) Montrer que si $u \mid v$ et $v \mid u$ alors $u = \pm v$ ou $u = \pm iv$.
   (d) Montrer que si $u \mid v$ alors $N(u) \mid N(v)$ dans $\mathbb{Z}$.
   (e) Déterminer les diviseurs de $1 + i$ dans $\mathbb{Z}[i]$.

3. Division euclidienne dans $\mathbb{Z}[i]$.
   (a) Montrer que pour tout $z \in \mathbb{C}$, il existe $u \in \mathbb{Z}[i]$ tel que $N(z - u) < 1$.
   Ce $u$ est-il unique ?
   (b) Montrer que pour tout $u \in \mathbb{Z}[i]$ et tout $v \in \mathbb{Z}[i]^*$, il existe un couple $(q, r)$ dans $\mathbb{Z}[i] \times \mathbb{Z}[i]$ tel que $u = vq + r$ et $N(r) < N(v)$.

## Partie II : Arithmétique dans $\mathbb{Z}[i]$.

4. Soit $\delta \in \mathbb{Z}[i]$. On définit l'ensemble $\delta\mathbb{Z}[i] = \{\delta u \mid u \in \mathbb{Z}[i]\}$.
   Montrer que $\delta\mathbb{Z}[i]$ est un sous-groupe de $(\mathbb{Z}[i], +)$.

5. Soit $u, v \in \mathbb{Z}[i]$ avec $u \neq 0$ ou $v \neq 0$. On note
$$I(u, v) = \{uz + vz' \mid z, z' \in \mathbb{Z}[i]\}.$$
   (a) Vérifier que $u$ et $v$ appartiennent à l'ensemble $I(u, v)$.
   (b) Justifier que l'ensemble $A = \{N(w) \mid w \in I(u, v) \setminus \{0\}\}$ possède un plus petit élément $d > 0$.
   (c) Soit $\delta$ un élément de $I(u, v)$ tel que $N(\delta) = d$.
   Établir que $I(u, v) = \delta\mathbb{Z}[i]$.
   *On pourra utiliser la division euclidienne présentée en I-3-(b).*
   (d) Montrer que $\delta$ divise $u$ et $v$ Montrer que pour tout $w \in \mathbb{Z}[i]$,
$$(w \mid u \text{ et } w \mid v) \iff w \mid \delta.$$
   On dit que $\delta$ est un PGCD de $u$ et $v$.

6. Soient $u$ et $v$ dans $\mathbb{Z}[i]$ tels que $u \neq 0$ et $v \neq 0$.
   On dit que $u$ et $v$ sont **premiers entre eux** si et seulement si leur PGCD $\delta$, défini en II-5-(d) appartient à $\{\pm 1, \pm i\}$.
   Dans cette question 6, on suppose que $u$ et $v$ sont premiers entre eux.
   (a) Justifier qu'il existe $z$ et $z'$ dans $\mathbb{Z}[i]$ tels que $uz + vz' = 1$.
   (b) Soit $w \in \mathbb{Z}[i]$. Montrer que si $u$ divise $vw$, alors $u$ divise $w$.

7. Soit $u \in \mathbb{Z}[i] \setminus \{0, \pm 1, \pm i\}$.
   On dit que $u$ est **irréductible** dans $\mathbb{Z}[i]$ si et seulement si ses seuls diviseurs dans $\mathbb{Z}[i]$ sont $\pm 1$, $\pm i$, $\pm u$, $\pm iu$.
   (a) Soit $v \in \mathbb{Z}[i]$. On suppose que $u$ est irréductible et ne divise pas $v$.
   Montrer que $u$ et $v$ sont premiers entre eux.
   (b) Soient $v, w \in \mathbb{Z}[i]$. On suppose que $u$ est irréductible et divise $vw$.
   Montrer que $u$ divise $v$ ou divise $w$.

## Partie III (*) : Nombres premiers sommes de deux carrés.

Dans cette partie, on cherche à caractériser les nombres premiers qui sont somme de deux carrés, c'est-à-dire qui s'écrivent $a^2 + b^2$ avec $(a, b) \in \mathbb{Z}^2$.

8. Démontrer l'équivalence

$$p \text{ est une somme de deux carrés} \iff p \text{ n'est pas irréductible dans } \mathbb{Z}[i].$$

9. *Théorème de Wilson et racine carrée de $-1$ modulo $p$.*
   (a) Redémontrer (c'est du cours) que

$$\forall x \in [\![1, p-1]\!] \quad \exists! y \in [\![1, p-1]\!] \ \mid \ xy \equiv 1[p].$$

   *Indication : on pourra appliquer le théorème de Bézout à $x$ et $p$.*

   (b) Montrer que 1 et $p-1$ sont les seuls éléments $x$ de $[\![1, p-1]\!]$ tels que

$$x^2 \equiv 1 \ [p].$$

   (c) En déduire le théorème de Wilson :

$$(p-1)! \equiv -1 \ [p].$$

10. Montrer que si $p \neq 2$ et si $p$ est somme de deux carrés, alors $p \equiv 1 \ [4]$.

11. Supposons que $p \equiv 1 \ [4]$.
   (a) En utilisant le théorème de Wilson, démontrer que

$$-1 = \left( \prod_{k=1}^{\frac{p-1}{2}} k \right)^2 \quad [p].$$

   (b) Soit $a$ un nombre entier tel que $a^2 = -1 \ [p]$ ($a$ existe d'après 11-(a)). Démontrer que $p$ n'est pas irréductible dans $\mathbb{Z}[i]$. Qu'en conclure ?

12. Conclure : quels sont les nombres premiers sommes de deux carrés ?

## Partie IV : Nombres sommes de deux carrés.

On note $\Sigma$ l'ensemble des sommes de deux carrés.

$$\Sigma = \{a^2 + b^2 \mid a, b \in \mathbb{Z}\}.$$

Notons $\mathbb{P}$ l'ensemble des nombres premiers.
On rappelle que pour $p \in \mathbb{P}$ et $n \in \mathbb{N}^*$, on note $v_p(n)$ la valuation $p$-adique de $n$, de sorte que

$$n = \prod_{p \in \mathbb{P}} p^{v_p(n)}.$$

On note $\Upsilon = \left\{ n \in \mathbb{N}^* \ \mid \ \forall p \in \mathbb{P} \quad p \equiv 3 \ [4] \implies v_p(n) \text{ est paire} \right\}$.

Le but des questions ci-dessous est de démontrer que $\Sigma \setminus \{0\} = \Upsilon$.

13. (a) Montrer que $\Sigma$ est stable par produit.
   (b) Démontrer que $\Upsilon \subset \Sigma \setminus \{0\}$.

14. Soit $(a, b) \in \mathbb{Z}^2 \setminus \{(0, 0)\}$ et $n = a^2 + b^2$.
   Soit $p$ un nombre premier diviseur de $n$ tel que $p \equiv 3[4]$.
   (a) Montrer que $p$ divise $(a + ib)$ dans $\mathbb{Z}[i]$.
   (b) En déduire que $p^2$ divise $n$ dans $\mathbb{Z}$ et que $\dfrac{n}{p^2} \in \Sigma$.
   (c) Prouver que $v_p(n)$ est paire.

15. Conclure.
   Application : 1789 est-il somme de deux carrés ? et 3578 ? et 5367 ?