Le but de ce problème est de caractériser, parmi les entiers, ceux qui sont somme de deux carrés. À noter que Lagrange a démontré que tout entier est somme de 4 carrés et que, plus généralement, Hilbert a prouvé, pour tout entier k, l'existence d'un nombre $g(k)$ tel que tout entier est somme d'au plus $g(k)$ puissances k-ièmes.

Dans la partie **I**, on établit quelques résultats généraux sur les anneaux principaux. Ceux-ci peuvent quasiment être considérés comme des résultats de cours, et sont à méditer par ceux qui envisagent de préparer une des leçons sur les pgcd et ppcm. Le cas échéant, cette partie plus théorique peut être laissée de côté dans un premier temps, quitte à admettre les deux résultats fondamentaux encadrés qui y sont prouvés.

Dans la partie **II**, on caractérise les nombres premiers p tels que -1 soit un carré dans $\mathbb{Z}/p\mathbb{Z}$.

La partie **III** établit les propriétés arithmétiques de l'anneau $\mathbb{Z}[i]$ des entiers de Gauss, qui permettent dans la partie **IV** de prouver que tout nombre premier de la forme $4n+1$ est somme de deux carrés.

Les parties **V** et **VI** achèvent l'étude du problème.

Partie I

On rappelle avant tout un peu de vocabulaire :

i. Un anneau intègre est un anneau commutatif dans lequel $ab = 0 \Rightarrow a = 0$ ou $b = 0$.

ii. Un idéal I d'un anneau commutatif A est un sous-groupe additif de A tel que :

$$\forall x \in A, \forall i \in I, ix \in I .$$

iii. Un idéal principal est un idéal I qui se réduit à l'ensemble des multiples de l'un de ses éléments :

$$I \text{ est principal } \Leftrightarrow \exists x_0 \in I \text{ tel que } I = (x_0) = \{x.x_0, x \in A\}$$

iv. Un anneau principal est un anneau intègre dont tout idéal est principal.

v. Les unités d'un anneau A sont les éléments inversibles (pour la multiplication !) de A. Ils forment un groupe multiplicatif.

vi. Si A est un anneau commutatif, et si a et b sont deux éléments de A, on dit que a divise b si :

$$\exists x \in A \text{ tel que } b = ax .$$

vii. Deux éléments a et b d'un anneau commutatif A sont dits premiers entre eux si leurs seuls diviseurs communs sont les unités de A.

viii. Un élément x d'un anneau commutatif A est dit irréductible si x n'est pas une unité de A et si :

$$\forall a, b \in A, x = ab \Rightarrow a \text{ ou } b \text{ est une unité de } A.$$

Enfin, si A est un anneau, A^* désignera l'ensemble des éléments non nuls de A.

1. Soit A un anneau intègre. Prouver que $\forall a, b \in A^*, (a) \subset (b)$ si et seulement si b divise a (on rappelle que (a) désigne l'idéal engendré par a, c'est-à-dire l'ensemble des multiples de a).

En déduire que $(a) = (b)$ si et seulement si il existe une unité u de A telle que $a = ub$ (deux tels éléments de A sont dits associés ; ils jouent le même rôle arithmétique... réfléchir à ce que sont des éléments associés dans $\mathbb{Z}$ ou dans $\mathbb{K}[X]$).

On suppose, jusqu'à la question ***6.*** *incluse, que A est un anneau principal.*

2. Soient a et b deux éléments non nuls de A.

a. Soit $I = (a) + (b) = \{xa + yb \text{ avec } x, y \in A\}$. Vérifier que I est un idéal de A.

En déduire l'existence de d dans A tel que $I = (d)$.

b. En utilisant que a et b sont dans I, prouver que d est un diviseur commun à a et b.

c. En utilisant que d est dans I, prouver que tout diviseur commun c à a et b est un diviseur de d.

d sera dit pgcd de a et b : c'est un diviseur commun à a et b, et c'est "le plus grand" en ce sens que tout autre diviseur commun à a et b le divise.

3. **a.** Déduire de la question **2.** "l'identité de Bézout" :

a et b sont premiers entre eux si et seulement si il existe u et v dans A tels que $ua + vb = 1$.

b. En déduire le "théorème de Gauss" :

si a divise bc et si a est premier avec b, alors a divise c.

4. Prouver que toute suite croissante (au sens de l'inclusion) d'idéaux de A est stationnaire (on considèrera une suite croissante (I_n) d'idéaux de A, et on prouvera que $I = \bigcup_n I_n$ est un idéal de A ; c'est alors que l'on utilisera que A est un anneau principal).

5. Soit x un élément de A^* qui n'est pas une unité. Le but de cette question est de prouver que x possède un diviseur irréductible. On suppose que tel n'est pas le cas.

a. Construire par récurrence une suite (d_n) d'éléments de A telle que :

$d_0 = x$, $\forall n \in \mathbb{N}$, d_n n'est pas une unité, d_{n+1} divise d_n, d_{n+1} et d_n ne sont pas associés.

b. En considérant la suite d'idéaux $((d_n))$, conclure à une impossibilité.

6. Soit x un élément de A^* qui n'est pas une unité.

a. On construit des éléments de A de la façon suivante :

i. si x est irréductible, on pose $p_1 = x$ et le processus s'arrête ;

ii. supposons construits $p_1, \ldots, p_n$; si $\frac{x}{p_1 \cdots p_n}$ est une unité, le processus s'arrêt. Sinon, on considère un diviseur irréductible p_{n+1} de $\frac{x}{p_1 \cdots p_n}$.

Prouver que l'algorithme ainsi défini s'arrête en un nombre fini d'étapes.

En déduire que x possède une décomposition en produit de facteurs irréductibles.

b. Prouver, grâce au théorème de Gauss, que cette décomposition est unique, aux unités près et à l'ordre des facteurs près.

On a ainsi prouvé le théorème fondamental suivant :

Si A est un anneau principal, tout élément non nul de A qui n'est pas une unité se décompose en un produit d'éléments irréductibles de A, et cette décomposition est unique, aux unités près et à l'ordre des facteurs près.

7. Soit A un anneau intègre. On dit que A est un anneau euclidien s'il existe une application ϕ, de $A - \{0\}$ dans $\mathbb{N}$, telle que :

$$\forall x, y \in A, y \neq 0, \exists q, r \in A \text{ tels que } x = qy + r \text{ avec } r = 0 \text{ ou } \phi(r) < \phi(y).$$

a. Donner des exemples d'anneaux euclidiens.

b. Soit A un anneau euclidien, et I un idéal de A, supposé non réduit à $\{0\}$ (sinon $I = (0)$).

i. Prouver l'existence d'un élément non nul x_0 de I tel que :

$$\forall x \in I, x \neq 0, \phi(x_0) \leq \phi(x).$$

ii. Prouver l'inclusion $(x_0) \subset I$.

iii. Prouver, par division euclidienne, l'inclusion inverse $I \subset (x_0)$.

c. En déduire le très important théorème suivant :

Tout anneau euclidien est un anneau principal.

*N.B. : dans les anneaux tels que $\mathbb{Z}$ ou $\mathbb{K}[X]$, voire $\mathbb{Z}[i]$ que l'on étudie un peu plus loin, la définition du pgcd, ainsi que la démonstration des théorèmes de Bézout et de Gauss, se font exactement comme dans le début de cette partie. Mais il peut être intéressant de noter que dans ces trois anneaux, l'existence de la décomposition en produit d'irréductibles peut être notablement simplifiée par rapport à celle, relativement délicate, exposée ici dans les questions **4.**, **5. et 6.**. Il suffit en effet de raisonner par récurrence sur la valeur absolue de x (dans $\mathbb{Z}$) ou sur son degré (dans $\mathbb{K}[X]$) ou sur son module au carré (dans $\mathbb{Z}[i]$), de la façon suivante : on considère un diviseur d de x de valeur absolue (ou de degré, ou de module au carré) minimum ; d est irréductible (sinon un diviseur de d serait un diviseur de x de valeur absolue ou de degré ou de module au carré strictement inférieur à d), et on applique l'hy-*

pothèse de récurrence à x/d, qui est plus petit (en valeur absolue ou en degré ou en module au carré) que x. L'unicité se fait grâce à Gauss comme dans la question ***6.b.****.*

Partie II

On rappelle qu'un polynôme de degré *n* à coefficients dans un corps commutatif $\mathbb{K}$ possède au plus *n* racines dans $\mathbb{K}$.

On cherche dans cette partie les nombres premiers *p* tels que –1 soit un carré dans $\mathbb{Z}/p\mathbb{Z}$.

Puisque dans $\mathbb{Z}/2\mathbb{Z}$, on a $-1 = 1 = 1^2$, on supposera $p \geq 3$, ainsi *p* est impair.

1. Prouver que pour tout *x* non nul de $\mathbb{Z}/p\mathbb{Z}$, on a $x^{p-1} = 1$ (penser au théorème de Lagrange sur l'ordre d'un sous-groupe).

2. Montrer l'existence de x_0 dans $\mathbb{Z}/p\mathbb{Z}$ tel que $x_0^{\frac{p-1}{2}} = -1$.

3. En déduire que si *p* est congru à 1 modulo 4, –1 est un carré dans $\mathbb{Z}/p\mathbb{Z}$.

4. Prouver que si *p* est congru à 3 modulo 4, –1 n'est pas un carré dans $\mathbb{Z}/p\mathbb{Z}$.

5. Application (cette question n'est pas utile pour la suite du problème).

On désire prouver qu'il existe une infinité de nombres premiers de la forme $4k+1$. Pour cela, on suppose qu'il n'en existe qu'un nombre fini, notés $p_1, \ldots, p_n$, et on considère l'entier $P = 4(p_1 \ldots p_n)^2 + 1$.

Prouver, grâce à ce qui précède, que *P* ne saurait être divisible par un nombre premier de la forme $4k+3$, puis conclure.

Partie III

On note $\mathbb{Z}[\mathrm{i}] = \{a + \mathrm{i}b \text{ avec } a, b \in \mathbb{Z}\}$. Si $a + \mathrm{i}b$ est dans $\mathbb{Z}[\mathrm{i}]$, on notera $N(a+\mathrm{i}b) = a^2 + b^2$.

1. Prouver que $\mathbb{Z}[\mathrm{i}]$ est un anneau intègre.

2. Montrer qu'un élément x de $\mathbb{Z}[i]$ est inversible dans $\mathbb{Z}[i]$ si et seulement si $N(x) = 1$ (on pourra utiliser, après l'avoir justifiée, la relation $N(xx') = N(x)N(x')$).

En déduire l'ensemble $\mathbb{U}$ des unités de $\mathbb{Z}[i]$.

3. Prouver que pour tous x et y dans $\mathbb{Z}[i]$, y non nul, il existe q et r dans $\mathbb{Z}[i]$ tels que :

$$x = qy + r, \text{ avec } |r| < |y|.$$

Y-a-t-il unicité de q et de r ?

4. Prouver que $\mathbb{Z}[i]$ est un anneau principal.

Partie IV

On recherche dans cette partie les nombres premiers p de $\mathbb{N}$ qui sont somme de deux carrés. Puisque $2 = 1 + 1$, on supposera $p \geq 3$. Bien entendu, puisque l'on vient d'établir que $\mathbb{Z}[i]$ est un anneau principal, le résultat fondamental d'existence et d'unicité d'une décomposition en produit d'irréductibles prouvé dans la partie **I.** pourra librement être utilisé dans $\mathbb{Z}[i]$.

1. Prouver qu'une somme de deux carrés ne peut qu'être congrue à 0, 1 ou 2 modulo 4. Que se passe-t-il donc si p est congru à 3 modulo 4 ?

On suppose dans la suite de cette partie que p est congru à 1 modulo 4.

2. Prouver que si x est un élément irréductible de $\mathbb{Z}[i]$, alors $\forall \alpha, \beta \in \mathbb{Z}[i]^*$, x divise $\alpha\beta$ implique x divise α ou x divise β.

3. **a.** Montrer l'existence de deux entiers k et x_0 tels que $kp = x_0^2 + 1$.

b. On suppose que p divise $x_0 + i$ dans $\mathbb{Z}[i]$. Montrer alors que p divise $x_0 - i$, puis que $p = 2$.

c. Déduire de ce qui précède que p n'est pas irréductible dans $\mathbb{Z}[i]$.

d. En revenant à la définition d'un irréductible, et en utilisant le fait que $N(xx') = N(x)N(x')$, prouver l'existence de deux entiers a et b tels que $p = a^2 + b^2$.

Partie V

On recherche dans cette partie les éléments irréductibles de $\mathbb{Z}[i]$.

1. Prouver que tout nombre premier de la forme $4k+3$ est irréductible dans $\mathbb{Z}[i]$ (on prouvera que si tel n'était pas le cas, un tel nombre serait somme de deux carrés).

2. Prouver que si $z = a + ib$ est dans $\mathbb{Z}[i]$, avec $a^2 + b^2$ premier, alors z est irréductible dans $\mathbb{Z}[i]$.

3. Réciproquement, soit x un irréductible de $\mathbb{Z}[i]$. En considérant l'entier $x\bar{x}$, et sa décomposition en produit de facteurs premiers dans $\mathbb{N}$, prouver que x est, à un facteur inversible près, de l'une des deux formes précédentes.

Partie VI

Soit S l'ensemble des nombres entiers qui sont somme de deux carrés.

1. Prouver que quels que soient les entiers a, b, c, d, on a $(a^2 + b^2)(c^2 + d^2) = (ac - bd)^2 + (ad + bc)^2$.

En déduire que S est stable pour le produit.

2. On désignera par p_i les nombres premiers congrus à 1 modulo 4, et par q_i les nombres premiers congrus à 3 modulo 4.

Prouver que tout entier x dont la décomposition en produit de facteurs premiers est du type suivant :

$$x = 2^n p_1^{\alpha_1} \dots p_k^{\alpha_k} q_1^{\beta_1} \dots q_r^{\beta_r}$$

avec n, $\alpha_1, \dots, \alpha_k$ entiers quelconques, et $\beta_1, \dots, \beta_r$ entiers pairs, est un élément de S.

3. Prouver réciproquement que tout élément de S est de cette forme (on prendra $x = a^2 + b^2$ dans S, et on décomposera $a + ib$ en produit de facteurs irréductibles dans $\mathbb{Z}[i]$).

Fin du problème.