# Théorème des deux carrés

Référence : [Per96] p.56-58.

Le problème est la suivant : on souhaite déterminer quels entiers $n \in \mathbb{N}$ sont somme de deux carrés. On pose :

$$\Sigma = \{n \in \mathbb{N}; n = a^2 + b^2; (a, b) \in \mathbb{N}^2\}$$

Par exemple :
- $0 = 0^2 + 0^2 \in \Sigma$ ;
- $1 = 1^2 + 0^2 \in \Sigma$ ;
- $2 = 1^2 + 1^2 \in \Sigma$ ;
- $4 = 2^2 + 0^2 \in \Sigma$ ;
- $5 = 2^2 + 1^2 \in \Sigma$ ;
- $8 = 2^2 + 2^2 \in \Sigma$ ;
- $9 = 3^2 + 0^2 \in \Sigma$ ;
- $10 = 3^2 + 1^2 \in \Sigma$ ;
- ....

Par contre $3, 6, 7, 11, 12 \notin \Sigma$. Cela met en évidence une première proposition :

**Proposition 0.1** *Si $n = 3[4]$ alors $n \notin \Sigma$.*

**Démonstration** En effet :
- Si $a$ est pair, alors $a^2 = 0[4]$ ;
- Si $a$ est impair, alors $a^2 = 1[4]$.

Donc en combinant les différentes possibilités, on a nécessairement $a^2 + b^2 = 0, 1, 2[4]$.

Faisons le lien avec l'anneau $\mathbb{Z}[i]$.
Si $n \in \Sigma$, alors $n = a^2 + b^2$ et $n$ s'écrit donc dans $\mathbb{C}$, $n = (a + ib)(a - ib)$ et cette relation a lieu en fait dans $\mathbb{Z}[i] = \{a + ib; (a, b) \in \mathbb{Z}\}$.
En particulier si $p$ est un nombre premier de $\mathbb{N}$ qui est somme de deux carrés, il n'est plus irréductible dans $\mathbb{Z}[i]$, par exemple $5 = (2 + i)(2 - i)$. Donc a priori, si on détermine les entiers qui s'écrivent sous forme de deux carrés, on pourra s'en servir pour déterminer les éléments irréductibles de $\mathbb{Z}[i]$.

**Proposition 0.2 (Propriétés de l'anneau des entiers de Gauss)**
1. *$\mathbb{Z}[i]$ est un anneau intègre inclus dans $\mathbb{C}$ ;*
2. *L'application :*
$$\begin{aligned} \sigma : \mathbb{Z}[i] &\longrightarrow \mathbb{Z}[i] \\ a + ib &\longmapsto a - ib \end{aligned}$$
*est un automorphisme.*
3. *L'application :*
$$\begin{aligned} N : \mathbb{Z}[i] &\longrightarrow \mathbb{N} \\ a + ib &\longmapsto (a + ib)(a - ib) = a^2 + b^2 \end{aligned}$$
*est une norme multiplicative, ie $N(zz') = N(z)N(z')$.*

**Remarque :** On admet ici ces propriétés qui se démontrent assez facilement.

**Proposition 0.3** *Les inversibles de $\mathbb{Z}[i]$ sont $1$, $-1$, $i$ et $-i$.*

**Démonstration**

- Soit $z \in \mathbb{Z}[i]^*$, alors il existe $z' \in \mathbb{Z}[i]$ tel que $zz' = 1$, donc $N(zz') = N(z)N(z') = 1$ et comme $N(z), N(z') \in \mathbb{N}$, alors nécessairement $N(z) = N(z') = 1$.
  Ainsi si $z = a + ib$, on a $N(z) = a^2 + b^2 = 1$ si et seulement si $a$ ou $b$ est nul et l'autre vaut $\pm 1$. D'où le fait que $z$ soit égal à $1$, $-1$, $i$ ou $-i$.
- Inversement, on vérifie que $1$, $-1$, $i$ et $-i$ sont bien inversibles.

**Remarque :** $z \in \mathbb{Z}[i]^*$ si et seulement si $N(z) = 1$.

**Proposition 0.4 (Stabilité de $\Sigma$)** *L'ensemble $\Sigma$ est stable par multiplication.*

**Démonstration** Traduisons le fait que $n \in \Sigma$ en terme d'entiers de Gauss :

$$n \in \Sigma \Leftrightarrow \exists z \in \mathbb{Z}[i]; n = N(z)$$

Alors si $n, n' \in \Sigma$, on a $n = N(z)$ et $n' = N(z')$ et par multiplicativité de la norme, on a le résultat.

**Remarque :** On peut également démontrer ce résultat directement via :

$$(a^2 + b^2)(c^2 + d^2) = (ac - bd)^2 + (ad + bc)^2$$

**Remarque :** Cette propriété ramène donc l'étude de $\Sigma$ à celle des éléments premiers de $\Sigma$ puisque tout entier se décompose en produit de facteurs premiers.

**Proposition 0.5 (Caractéristique de l'anneau des entiers de Gauss)** *$\mathbb{Z}[i]$ est euclidien, donc principal.*

**Démonstration** Soient $z, t \in \mathbb{Z}[i] \setminus \{0\}$. Pour effectuer la division euclidienne de $z$ par $t$, on commence par considérer $\dfrac{z}{t} \in \mathbb{C}$.
On approxime ensuite $\dfrac{z}{t}$ par un entier de Gauss $q$.
Si $\dfrac{z}{t} = x + iy$, on prend $q = a + ib$ où $a$ et $b$ sont les entiers les plus proches de $x$ et $y$. On a ainsi :

$$\left|\frac{z}{t} - q\right| \leq \frac{\sqrt{2}}{2} < 1$$

car $|x - a|$ et $|y - b|$ sont $\leq \dfrac{1}{2}$.
On pose alors $r = z - qt$ de sorte que $r \in \mathbb{Z}[i]$ et on a :

$$r = t\left(\frac{z}{t} - q\right)$$

D'où :

$$|r| = |t|\left|\frac{z}{t} - q\right| < |t|$$

et on obtient au carré $N(r) < N(t)$.
On a donc bien écrit $z = qt + r$ avec $N(r) < N(t)$.

**Proposition 0.6 (Théorème des deux carrés pour les nombres premiers)** *Soit $p \in \mathbb{N}$ un nombre premier. Alors :*

$$p \in \Sigma \Leftrightarrow p = 2[4] \quad \text{ou} \quad p = 1[4]$$

**Démonstration**
($\Rightarrow$) Si $p \in \Sigma$, on a déjà vu que si $p = 3[4]$, alors $p \notin \Sigma$.
De plus, $p \neq 0[4]$ car $p$ est un nombre premier donc il ne peut pas être divisible par 4.

($\Leftarrow$) On commence par démontrer un lemme.

**Lemme 0.1** *$p \in \Sigma$ si et seulement si $p$ n'est pas irréductible dans $\mathbb{Z}[i]$ (ie $p$ s'écrit comme un produit de deux éléments non inversibles).*

**Démonstration**

($\Rightarrow$) Soit $p \in \Sigma$, alors $p = a^2 + b^2 = (a+ib)(a-ib)$ et $a$ et $b$ sont non nuls (car $p$ est premier), donc $a+ib$ et $a-ib$ n'appartiennent pas à $\mathbb{Z}[i]^*$ (d'après la détermination de ses éléments faite précédemment), donc $p$ n'est pas irréductible.

($\Leftarrow$) Si $p = z \times z'$ avec $z, z' \neq \pm 1, \pm i$. On a $N(p) = N(z)N(z') = p^2$ et comme $N(z)$ et $N(z') \neq 1$, alors nécessairement $N(z) = N(z') = p$ donc $p \in \Sigma$.

Comme $\mathbb{Z}[i]$ est un anneau principal (d'après ce qu'on a fait précédemment), alors $\mathbb{Z}[i]$ est un anneau factoriel, donc dire que $p$ n'est pas irréductible, c'est dire exactement que l'idéal principal $(p)$ n'est pas premier donc que le quotient $\mathbb{Z}[i]/(p)$ n'est pas intègre.
Pour étudier ce quotient, on considère l'isomorphisme :

$$\mathbb{Z}[i] \simeq \mathbb{Z}[X]/(X^2+1)$$

puis les isomorphismes suivant qui résultent du théorème d'isomorphisme :

$$\mathbb{Z}[i]/(p) \simeq \mathbb{Z}[X]/(X^2+1, p) \simeq \frac{\mathbb{Z}[X]}{p\mathbb{Z}[X]}/(X^2+1) \simeq \frac{\mathbb{Z}}{p\mathbb{Z}}[X]/(X^2+1) \simeq \mathbb{F}_p[X]/(X^2+1)$$

On a donc montré les équivalences : $(p)$ n'est pas premier si et seulement si $X^2+1$ n'est pas irréductible dans $\mathbb{F}_p[X]$ si et seulement si $X^2+1$ a une racine dans $\mathbb{F}_p$.
En résumé $p \in \Sigma$ si et seulement si $-1 \in (\mathbb{F}_p^*)^2$.
Il reste donc à montrer que $-1$ est un carré dans $\mathbb{F}_p^*$ si et seulement si $p = 2[4]$ ou $1[4]$.

($\Leftarrow$) Supposons que $p = 1[4]$. Alors le cardinal de $(\mathbb{F}_p^*)^2$ est $(p-1)/2$ (il suffit de considérer la morphisme $\phi : x \in \mathbb{F}_p^* \longmapsto x^2 \in \mathbb{F}_p^*$ et de remarquer que $(\mathbb{F}_p^*)^2 = Im(\phi)$) est pair, donc d'après le théorème de Cauchy, $\mathbb{F}_p^*$ contient un élément d'ordre 2, ie il existe $x$ tel que $x^2 = 1$ et $x \neq 1$, c'est donc nécessairement $-1$ (puisque les racines de $X^2 - 1$ sont 1 et $-1$).
Supposons maintenant que $p = 2[4]$, alors $p = 2$ (puisque $p$ est premier) et dans ce cas $-1$ est bien un carré de $\mathbb{F}_2$.

($\Rightarrow$) Supposons que $-1$ soit un carré dans $\mathbb{F}_p^*$ et $p \neq 2$, alors il va exister $x \in \mathbb{F}_p^*$ tel que $x^2 = -1$.
D'après le théorème de Lagrange, $x^{(p-1)} = 1$ alors $(-1)^{(p-1)/2} = 1$, ie $(p-1)/2$ est pair, ie $p = 1[4]$.

**Proposition 0.7 (Théorème des deux carrés)** *Soit $n \in \mathbb{N}^*$ et $n \neq 1$, on décompose $n$ est produit de facteurs premiers :*

$$n = \prod_{p \in \mathcal{P}} p^{\nu_p(n)}$$

*Alors $n \in \Sigma$ si et seulement si $\nu_p(n)$ est pair pour $p = 3[4]$.*

**Démonstration**

($\Rightarrow$) On suppose que $n \in \Sigma$, ie $n = a^2 + b^2$ et on pose :

$$n = \prod_{p \in \mathcal{P}} p^{\nu_p(n)}$$

Montrons que si $p = 3[4]$ alors nécessairement $\nu_p(n)$ est pair.
On montre par récurrence que $\forall k \geq 0$, $\forall n \in \Sigma$ tel que $\nu_p(n) \leq k$ alors $\nu_p(n)$ est pair.

- Si $k = 0$, alors $\nu_p(n) \leq 0$, ie $\nu_p(n) = 0$ et 0 est bien pair.
- Supposons le résultat vrai au rang $k$. On suppose que $\forall n \in \Sigma$, $\nu_p(n) \leq k+1$. Montrons qu'alors $\nu_p(n)$ est pair.
  Comme $\nu_p(n)$ est non nul alors $p$ divise $n$, ie $p$ divise $a^2 + b^2 = (a+ib)(a-ib)$. Or $p$ est irréductible dans $\mathbb{Z}[i]$, donc $p$ divise $a+ib$ par exemple. Or $p$ est entier donc $p$ divise $a$ et $p$ divise $b$, en particulier $p^2$ divise $n$. Ainsi si on écrit $a = pa'$ et $b = pb'$, alors $\frac{n}{p^2} = a'^2 + b'^2 \in \Sigma$, donc $\nu_p\left(\frac{n}{p^2}\right) = \nu_p(n) - 2 \leq k$ est pair donc $\nu_p(n)$ l'est aussi.

($\Leftarrow$) On suppose que la décomposition de $n$ est telle que si $p = 3[4]$ alors $\nu_p(n)$ est pair.
Regardons les différentes possibilité modulo 4 pour les nombres premiers intervenant dans la décomposition de $p$.

- soit $p = 0[4]$, ce qui est impossible car alors $p$ serait divisible par 4, ie $p$ ne serait pas premier ;

- soit $p = 1[4]$ et d'après la proposition précédente, on sait qu'alors $p \in \Sigma$ ;
- soit $p = 2[4]$ et d'après la proposition précédente, on sait aussi que $p \in \Sigma$ ;
- soit $p = 3[4]$ et $\nu_p(n)$ est pair, ce qui signifie que $p^2$ divise $n$ et $p^2 = 1[4]$ donc d'après la proposition précédente $p^2 \in \Sigma$.

De plus comme $\Sigma$ est stable par multiplication, alors on obtient bien que $n \in \Sigma$ sous cette condition.

# Références

[Per96] Daniel Perrin. *Cours d'algèbre.* Ellipses, 1996.