# 4

## Théorème des deux carrés.

Références :
- Skandalis, exo 3.11 p. 95
- Gourdon, sujet d'étude 3 p. 49
- Autres preuves dans Oraux X-ENS 1 p. 194-195

Recasages :
- 104 : Nombres premiers. Propriétés et applications.
- 165 : Idéaux d'un anneau commutatif. Exemples.
- 302 : Exercices faisant intervenir les notions de congruence et de divisibilité dans $\mathbb{Z}$.
- 305 : Exercices illustrant l'utilisation des nombres premiers

Soit $p \in \mathbb{P}$. Les assertions suivantes sont équivalentes :
(1) $\exists a, b \in \mathbb{Z}$ tq $a^2 + b^2 = p$.
(2) $p \in \mathbb{Z}[i]$ n'est pas irréductible dans $\mathbb{Z}[i]$.
(3) $-1$ est un carré modulo $p$.
(4) $p \equiv 1\ [4]$ ou $p \equiv 2\ [4]$.

Remarque : Si $p = 2$ :
$$\begin{cases} 2 = 1^2 + 1^2 = (1+i)(1-i) \\ -1 \equiv 1 \equiv 1^2\ [2] \end{cases}$$
Toutes les assertions sont bien vérifiées.
On s'intéresse donc au cas où $p$ est impair.

(1) $\Rightarrow$ (4) :

$$\left.\begin{array}{l} k \equiv 1\ [4] \Rightarrow k^2 \equiv 1\ [4] \\ k \equiv 2\ [4] \Rightarrow k^2 \equiv 0\ [4] \\ k \equiv 3\ [4] \Rightarrow k^2 \equiv 1\ [4] \\ k \equiv 4\ [4] \Rightarrow k^2 \equiv 0\ [4] \end{array}\right\} \Rightarrow p = a^2 + b^2 \equiv 1 \text{ ou } 2\ [4]$$
car $p \in \mathbb{P}$ donc $p \not\equiv 0\ [4]$.

**(4) ⇔ (3) :**

**Lemme :** Notons $K = \{x^2 \mid x \in \underbrace{(\mathbb{Z}/p\mathbb{Z})^*}_{= \mathbb{F}_p^*}\}$.
Soit $p \in \mathbb{P} \setminus \{2\}$.
Alors $-1 \in K \Leftrightarrow p \equiv 1 \ [4]$

**Preuve du lemme :**
Soit $\varphi : (\mathbb{F}_p^*, \cdot) \longrightarrow (\mathbb{F}_p^*, \cdot)$
$x \longmapsto x^2$

* C'est un morphisme et $\mathrm{Im}(\varphi) = K$.
* $\mathrm{Ker}(\varphi) = \{x \in \mathbb{F}_p^* \mid x^2 = 1\} = \{-1 ; +1\}$
* $\mathrm{Ker}(\varphi)$ est un sous-gpe commutatif de $\mathbb{F}_p^*$, donc il est distingué.

Donc par le thm d'isomorphisme on a :

$$\frac{|\mathbb{F}_p^*|}{|\mathrm{Ker}\,\varphi|} = \frac{p-1}{2} = |\mathrm{Im}\,\varphi| = |K|$$

D'où : $x \in K \Leftrightarrow x^{\frac{p-1}{2}} = 1$ car :

$\Rightarrow$ $x \in K \Rightarrow (x^2)^{\frac{p-1}{2}} = x^{p-1} = 1$ par le petit thm de Fermat.

$\Leftarrow$ Le polynôme $X^{\frac{p-1}{2}} - 1$ admet au plus $\frac{p-1}{2}$ racines. Or $|K| = \frac{p-1}{2}$, donc ts les éléments de $K$ sont racines de $X^{\frac{p-1}{2}} - 1$

Finalement :

$$-1 \in K \Leftrightarrow (-1)^{\frac{p-1}{2}} = 1$$
$$\Leftrightarrow \frac{p-1}{2} \equiv 0 \ [2]$$
$$\Leftrightarrow p \equiv 1 \ [4]$$

Ainsi si $-1$ est un carré modulo $p$, soit $p$ impair et alors $\Leftrightarrow p \equiv 1[4]$, soit $p$ pair et $\Leftrightarrow p \equiv 2[4]$.

## (3) => (2):

$-1$ est un carré modulo $p$ (3)
$\Rightarrow \exists x \in \mathbb{N}^*$ tq $-1 \equiv x^2 [p]$
$\Rightarrow p \mid x^2+1$ et $p$ réductible dans $\mathbb{Z}[i]$.

En effet, si l'on suppose $p$ irréductible dans $\mathbb{Z}[i]$:
$\mathbb{Z}[i]$ est un anneau principal, donc $p$ est premier dans $\mathbb{Z}[i]$.
Or $p \mid x^2+1 \Rightarrow p \mid (x+i)(x-i)$
$\Rightarrow p \mid x+i$ ou $p \mid x-i$ dans $\mathbb{Z}[i]$.
En passant dans $\mathbb{Z}$, on a alors $\begin{cases} p \mid x \\ p \mid 1 \end{cases}$
$\Rightarrow x \wedge 1 \neq 1$, donc $x$ et $1$ ne sont pas premiers entre eux, ce qui est absurde.
(1 est premier avec tout...)

## (2) => (1):

Soit $p = xy$ avec $x, y \in \mathbb{Z}[i]$ non inversibles.
$\Rightarrow x, y \notin \mathbb{Z}[i]^\times$.

$\varphi$ morphisme

$\varphi(p) = p^2 = \varphi(x) \cdot \varphi(y) \Rightarrow \varphi(x) = \varphi(y) = p$.

Prenons $x = a+ib$.
Alors $p = \varphi(x) = a^2 + b^2$.