# Théorème des deux carrés

Arnaud Girand

18 juin 2012

Référence :
- [Per96], p. 56–58

Prérequis :
- structure de $\mathbb{Z}[i]$.

On considère dans toute la suite l'ensemble suivant : $\Sigma := \{a^2+b^2 \mid a,b \in \mathbb{N}\}$. Il s'agit d'un monoïde commutatif (lemme 2 ).

**Lemme 1 (Théorème des deux carrés, version faible)**
*Soit $p$ un nombre premier.*
*Alors*

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

Démonstration :

Remarquons que (cf. infra) $p \in \Sigma \Leftrightarrow p$ est réductible dans $\mathbb{Z}[i]$. $\mathbb{Z}[i]$ étant euclidien, il est factoriel et donc :

$$\begin{aligned} p \text{ est réductible } &\Leftrightarrow (p) \text{ n'est pas premier} \\ &\Leftrightarrow \mathbb{Z}[i]/(p) \text{ n'est pas intègre} \end{aligned}$$

Or $\mathbb{Z}[i] \cong \mathbb{Z}[X]/(X^2+1)$ ergo :

$$\begin{aligned} \mathbb{Z}[i]/(p) &\cong (\mathbb{Z}[X]/(X^2+1))/(p) \\ &\cong \mathbb{F}_p[X]/(X^2+1) \end{aligned}$$

De fait :

$$\begin{aligned} (p) \text{ n'est pas premier } &\Leftrightarrow X^2+1 \text{ est réductible sur} \mathbb{F}_p \\ &\Leftrightarrow X^2+1 \text{ admet une racine sur } \mathbb{F}_p \\ &\Leftrightarrow -1 \in (\mathbb{F}_p^*)^2 \\ &\Leftrightarrow p = 2 \text{ ou } p \cong 1[4] \end{aligned}$$

La dernière équivalence provient du fait que $x \in (\mathbb{F}_p^*)^2 \Leftrightarrow x^{(p-1)/2} = 1$. On raisonne [1] ensuite sur l'ensemble $X := \{x \in \mathbb{F}_p \mid x^{(p-1)/2} = 1$ qui est de cardinal inférieur ou égal à $\frac{q-1}{2}$ et contient $(\mathbb{F}_p^*)^2$ donc y est égal par égalité de leurs [2] cardinaux respectifs. D'où le résultat.

**Proposition 1 (Théorème des deux carrés)** *Soit $n \geq 2$ un entier dont la décomposition en produit de facteurs premiers est donnée par :*

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

*Alors :*

$$n \in \Sigma \quad \Leftrightarrow \quad \forall p \in \mathcal{P} \text{ tel que } p \equiv 3[4],\ v_p(n) \equiv 0[2]$$

Démonstration :

1. Raisonnement valable sur tout corps fini.
2. Le lecteur pointilleux pourra me reprocher le pluriel ici. Tant pis.

($\Leftarrow$) Clair en combinant les lemmes 2 et 1.

($\Rightarrow$) Soit $p \in \mathcal{P}$ congru à 3 modulo 4. Démontrons le résultat par récurrence[3] "sur $v_p(n)$" i.e montrons que si pour tout $k \geq 0$ et tout $n \in \Sigma$ tel que $v_p(n) \leq k$ alors $v_p(n)$ est pair.
- $k = 0$. 0 est pair.
- Supposons la propriété vrai pour $v_p(n) \leq k$, avec $k \geq 0$ et supposons $v_p(n) \leq k+1$. Alors $p|n = a^2 + b^2 = (a+ib)(a-ib)$ dans $\mathbb{Z}[i]$, avec $a, b \in \mathbb{N}$. De fait, $p$ divise (par exemple) $a + ib$. Comme $p$ est entier, on a de fait $p|a$ et $p|b$ ergo $p^2|n$.

  En posant $a = pa'$ et $b = pb'$ on remarque que $\frac{n}{p^2} = a'^2 + b'^2 \in \Sigma$. Or $v_p\left(\frac{n}{p^2}\right) = v_p(n) - 2 \leq k$ donc par hypothèse de récurrence (comme $\frac{n}{p^2} \in \Sigma$) $v_p(n) - 2$ est pair donc $v_p(n)$ l'est. D'où le résultat.

**Détails supplémentaires :**
- On fait usage du lemme suivant ([Per96], p. 56) :

  **Lemme 2**
  $(\Sigma, \times)$ *est un sous–monoïde de* $\mathbb{N}$.
  Démonstration : Commençons par remarquer que, si note $N$ le stathme usuel sur $\mathbb{Z}[i]$ :

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

  Il est clair que $\Sigma$ est non vide ($0 \in \Sigma$). De plus, si $z, z' \in \mathbb{Z}[i]$, on a $N(z)N(z') = N(zz')$ et donc $\Sigma$ est stable par multiplication. On retrouve au passage l'identité dite de Lagrange :

  $$\forall a, b, c, d \in \mathbb{N}, \quad (a^2 + b^2)(c^2 + d^2) = (ac - bd)^2 + (ad + bc)^2 \tag{1}$$

- *Pour un nombre premier* $p$, $p \in \Sigma \Leftrightarrow$ *$p$ est réductible dans* $\mathbb{Z}[i]$.
  - Pour le sens direct, on suppose $p = a^2 + b^2$. Alors $a$ et $b$ sont non nuls et donc $p = (a+ib)(a-ib)$ est réductible.
  - Réciproquement, si $p = zz'$ avec $z, z'$ n.n.n.i. Alors $N(p) = N(z)N(z') = p^2$. Comme $N(z), N(z') \neq 1$ ils sont égaux à $p$ et donc (par exemple) $p = N(z) \in \Sigma$.

# Références

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

3. Comme pour le grand théorème de Fermat.