Titre : **Théorème des deux carrés**
Recasages : 121,122,126
Thème : Théorie des anneaux, arithmétique
Références : Perrin - Cours d'algèbre (p. 57,58)

Théorème 1. *Soit $\Sigma := \{n \in \mathbb{N} \mid \exists a, b \in \mathbb{Z} \mid a^2 + b^2 = n\}$, si p est premier, alors on a équivalence entre*

(i) $p \in \Sigma$.

(ii) $p = 2$ *ou* $p \equiv 1[4]$.

Commençons par remarquer que la condition est nécéssaire : soit $a^2 + b^2 \in \Sigma$, si $a = 2k$ est pair, on a $a^2 = 4k^2 \equiv 0[4]$, et si $a = 2k+1$ est impair, on a $a^2 = 4k^2 + 4k + 1 \equiv 1[4]$ de même pour b, donc $a^2 + b^2 \equiv 0, 1$ ou $2[4]$. Comme p est premier, on a bien $p = 2$ ou $p \equiv 1[4]$.
Ensuite, on introduit l'anneau des entiers de Gauss :

$$Z[i] = \{z = a + ib \in \mathbb{C} \mid a, b \in \mathbb{Z}\}$$

(c'est un sous-anneau comme image de $\mathbb{Z}[X]$ par le morphisme d'évalutation des polynômes en i). Pour $z = a + ib \in \mathbb{Z}[i]$, on pose $N(z) = z\overline{z} = a^2 + b^2$, on remarque ainsi que Σ est constitué de l'image de $\mathbb{Z}[i]$ par N.

Proposition 2. *L'anneau $\mathbb{Z}[i]$ est euclidien pour le stathme N. Par ailleurs ses inversibles sont donnés par $\mathbb{Z}[i]^\times = \{\pm 1, \pm i\}$*

Démonstration. L'application N est multiplicative : $N(zz') = N(z)N(z')$ pour $z, z' \in \mathbb{Z}[i]$, en particulier, si $z \in \mathbb{Z}[i]^\times$, alors $1 = N(1) = N(z)N(z^{-1})$, donc $N(z) \in \mathbb{N}$ est un élément inversible : $N(z) = 1 = N(z^{-1})$. Si $z = a + ib$, alors on a

$$a = \pm 1 \text{ et } b = 0 \quad \text{ou} \quad a = 0 \text{ et } b = \pm 1$$

d'où $\mathbb{Z}[i]^\perp \subset \{\pm 1, \pm i\}$, et l'inclusion réciproque est immédiate.
Considérons maintenant $z, z' \in \mathbb{Z}[i]$ avec $z' \neq 0$, on peut considérer $x + iy = \frac{z}{z'} \in \mathbb{C}$. On considère (a, b) l'unique couple d'entiers tel que $|a - x| \leqslant 1/2$ et $|b - y| \leqslant 1/2$ (on prends les parties entières ou les parties entières$+1$ selon les cas). On a

$$N\left(\frac{z}{z'} - (a + ib)\right) = |a - x|^2 + |b - y|^2 \leqslant \frac{1}{2}$$

Donc

$$N(z - z'(a + ib)) \leqslant \frac{N(z)}{2} < N(z)$$

ainsi, $z = z'(a + ib) + (z - z'(a + ib))$ est une division euclidienne de z par z' dans $\mathbb{Z}[i]$ pour le stathme N, ce qui termine la preuve. □

Le lemme suivant fait un lien supplémentaire entre Σ et $\mathbb{Z}[i]$:

Lemme 3. *Soit p premier, on a $p \in \Sigma$ si et seulement si p est réductible dans $\mathbb{Z}[i]$.*

Démonstration. Si $p = a^2 + b^2 \in \Sigma$, on a $p = N(a + ib) = (a + ib)(a - ib)$. Si $a = 0$ (resp $b = 0$), on a $p = b^2$ (resp $p = a^2$) ce qui est impossible car p est premier, donc $a, b \neq 0$ et $a + ib$ n'est pas inversible : p est réductible.
Réciproquement, si $p = zz'$ est réductible (avec donc $z, z' \notin \mathbb{Z}[i]^\times$), on a

$$p^2 = N(p) = N(z)N(z')$$

Comme par hypothèse, $N(z)$ et $N(z')$ sont différents de 1, on a $N(z) = N(z') = p$, donc $p \in \Sigma$ □

Comme l'anneau $\mathbb{Z}[i]$ est principal (car euclidien), p y est réductible si et seulement si l'idéal (p) n'est pas premier, autrement dit si $\mathbb{Z}[i]/(p)$ n'est pas intègre.
Considérons (X^2+1) dans $\mathbb{Z}[X]$, l'évaluation des polynômes en i donne $\mathbb{Z}[i] \simeq \mathbb{Z}[X] \big/ (X^2+1)$.
Par ailleurs, on a également $\mathbb{Z}[X] \big/ (p) \simeq \mathbb{F}_p[X]$, d'où

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

on peut exhiber directement l'isomorphisme au centre mais c'est long et rébarbatif. Cet isomorphisme donne la chaîne d'équivalences suivante

$$\begin{aligned}
\mathbb{Z}[i] \big/ (p) \text{ est intègre} &\Leftrightarrow \mathbb{F}_p[X] \big/ (X^2+1) \text{ est intègre} \\
&\Leftrightarrow (X^2+1) \text{ est premier dans } \mathbb{F}_p[X] \\
&\Leftrightarrow X^2+1 \text{ est irréductible dans } \mathbb{F}_p[X] \\
&\Leftrightarrow X^2+1 \text{ admet une racine dans } \mathbb{F}_p[X]
\end{aligned}$$

(car $\mathbb{F}_p[X]$ est principal, et X^2+1 est de degré 2). On a donc que $p \in \Sigma$ si et seulement si -1 est un carré dans $\mathbb{F}_p$, on conclut alors par le lemme suivant :

Lemme 4. *Soit p un nombre premier, -1 est un carré dans $\mathbb{F}_p$ si et seulement si $p = 2$ ou $p \equiv 1[4]$*

Démonstration. Le cas $p = 2$ se règle immédiatement, on peut donc supposer p impair.
On considère l'application

$$\varphi : \begin{array}{ccc} \mathbb{F}_p^* & \longrightarrow & \mathbb{F}_p^* \\ x & \longmapsto & x^{\frac{p-1}{2}} \end{array}$$

Il s'agit d'un morphisme de groupe. Son noyau est donnée par les racines non nulles du polynôme $X^{\frac{p-1}{2}} - 1$, il contient donc au plus $\frac{p-1}{2}$ éléments. Si $x = y^2$ est un carré non nul dans $\mathbb{F}_p$, on a $\varphi(x) = y^{p-1} = 1$ donc $\mathbb{F}_p^{*2}$ est inclus dans $\operatorname{Ker} \varphi$. Par ailleurs, $\mathbb{F}_p^{*2}$ est l'image de $\mathbb{F}_p^*$ par le morphisme $x \mapsto x^2$, de noyau $\{\pm 1\}$, donc $\mathbb{F}_p^{*2}$ est de cardinal $\frac{p-1}{2}$, on a donc $\mathbb{F}_p^{*2} = \operatorname{Ker} \varphi$ par cardinalité.
Donc -1 est un carré dans $\mathbb{F}_p$ si et seulement si $(-1)^{\frac{p-1}{2}} = 1$, ce qui est équivalent à $p \equiv 1[4]$. □

Comme N est une application multiplicative, Σ est stable par produit, on a donc le corollaire suivant

Corollaire 5. *Soit $n \in \mathbb{N}$, $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ sa décomposition en produit de facteurs premiers, on a équivalence entre*

- *$n \in \Sigma$*
- *Pour tout $i \in [\![1, r]\!]$ tel que $p_i \equiv 3[4]$, on a α_i pair.*