Théorème des deux carrés

30 juin 2013

On note $\Sigma = \{p \in \mathbb{N} \mid \exists a, b \in \mathbb{N} \text{ tels que } p = a^2 + b^2\}$.

Théorème. *Soit p un nombre premier. Alors $p \in \Sigma \Leftrightarrow p = 2$ ou $p \equiv 1[4]$.*

Commençons par étudier trois propositions :

Théorème. *$\mathbb{Z}[i]^\times = \{\pm 1; \pm i\}$ et $\left(\mathbb{Z}[i], |\cdot|^2\right)$ est euclidien (donc principal).*

Démonstration. Soit $z \in \mathbb{Z}[i]^\times$: il existe $z' \in \mathbb{Z}[i]$ tel que $zz' = 1$ donc $|z|\,|z'| = 1$ soit $|z|^2 = 1$. Or, si $z = a + ib$, $|z|^2 = a^2 + b^2$ et $1 = a^2 + b^2 \Leftrightarrow \begin{cases} a = \pm 1 & b = 0 \text{ ou} \\ a = 0 & b = \pm 1 \end{cases}$. Réciproquement, $\{\pm 1; \pm i\} \subset \mathbb{Z}[i]^\times$ ce qui achève la première partie de la preuve. Soient $z, t \in \mathbb{Z}[i] \setminus \{0\}$ et $x, y \in \mathbb{R}$ tels que $\frac{z}{t} = x + iy$. Soient $a, b \in \mathbb{Z}$ les entiers les plus proches de x et y. En particulier, $|x - a| \leq \frac{1}{2}$ et $|y - b| \leq \frac{1}{2}$. On note $q = a + ib$.

$$\left|\frac{z}{t} - q\right|^2 \leq |x - a|^2 + |y - b|^2 \leq \frac{1}{4} + \frac{1}{4} \Rightarrow \left|\frac{z}{t} - q\right| \leq \frac{1}{\sqrt{2}} < 1$$

On pose $r = z - qt$. On a $\left|\frac{r}{t}\right| = \left|\frac{z}{t} - q\right| < 1 \Rightarrow |r| \leq |t| \Rightarrow |r|^2 < |t|^2$. Comme $z = qt + r$ avec $|r|^2 < |t|^2$, $\left(\mathbb{Z}[i], |\cdot|^2\right)$ est euclidien. □

Lemme. *Soit $p \in \mathbb{N}$ premier. Alors $p \in \Sigma \Leftrightarrow p$ n'est pas irréductible dans $\mathbb{Z}[i]$.*

Démonstration. "⇒" : Il existe $a, b \in \mathbb{N}$ tels que $p = a^2 + b^2$. $a \neq 0$ et $b \neq 0$ car sinon $p = a^2$ ou $p = b^2$ et p ne serait pas premier. Or, $p = (a + ib)(a - ib)$ et $\begin{cases} a \neq 0 \\ b \neq 0 \end{cases} \Rightarrow \begin{cases} a + ib \notin \mathbb{Z}[i]^\times \\ a - ib \notin \mathbb{Z}[i]^\times \end{cases}$.

"⇐" : S(il existe $z, z' \in \mathbb{Z}[i] \setminus \{\pm 1; \pm i\}$ tels que $p = zz'$ alors $p^2 = |p|^2 = |z|^2\,|z'|^2$ donc $|z|^2 = p$ et $|z'|^2 = p$ car $|z| \neq 1$, $|z'| \neq 1$ et p est premier donc en notant $z = a + ib$ on $p = a^2 + b^2$. □

Lemme. *Soit $p \in \mathbb{N}$ premier. Alors, -1 est un carré de $\mathbb{Z}/p\mathbb{Z} \Leftrightarrow p = 2$ ou $p \equiv 1[4]$.*

Démonstration. Si $p = 2$, le résultat est trivial. On suppose à présent p impair.

$p \equiv 1[4] \Leftrightarrow \frac{p-1}{2}$ est pair. Or $\frac{p-1}{2} = \#\{q \in \mathbb{Z}/p\mathbb{Z} \setminus \{0\} \mid \exists y \text{ tel que } q = y^2\} =: \#\mathbb{F}_p^{\times 2}$. Or, $\mathbb{F}_p^{\times 2}$ étant un groupe multiplicatif, le théorème de Sylow nous dit qu'il existe un élément d'ordre 2, c'est-à-dire un x tel que $x \neq 1$ et $x^2 = 1$. Or, $X^2 - 1$ étant de degré 2, il a au plus 2 racines, qui sont forcément 1 et -1. Ainsi, $-1 \in \mathbb{F}_p^{\times 2} \Leftrightarrow p \equiv 1[4]$. □

Reprenons la démonstration du théorème :

Démonstration. $\mathbb{Z}[i]$ est principal donc factoriel donc p non irréductible équivaut à (p) n'est pas premier, ce qui équivaut à $\mathbb{Z}[i]/(p)$ n'est pas intègre. Les morphismes suivants :

$$\begin{array}{rccc} \varphi_1 : & \mathbb{Z}[X] & \to & \mathbb{Z}[i] \\ & P & \mapsto & P(i) \end{array}$$

$$\begin{array}{rccc} \varphi_2 : & \mathbb{Z}[X] & \to & \mathbb{Z}[i]/(p) \\ & P & \mapsto & \overline{P(i)} \end{array}$$

$$\begin{array}{rccc} \varphi_3 : & \mathbb{Z}[X] & \to & \mathbb{Z}[X]/(X^2 + 1, p) \\ & P & \mapsto & \tilde{P} \end{array}$$

$$\begin{array}{rccc} \varphi_4 : & \mathbb{Z}[X] & \to & \mathbb{Z}/p\mathbb{Z}[X] \\ & P & \mapsto & \check{P} \end{array}$$

donnent les isomorphismes

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

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

$$\left(\mathbb{Z}[X]/p\right)/(X^2+1) \overset{(3)}{\simeq} \mathbb{Z}[X]/(X^2+1,p)$$

$$\mathbb{Z}/p\mathbb{Z}[X] \overset{(4)}{\simeq} \mathbb{Z}[X]/(p)$$

d'où $\mathbb{Z}[i]/(p) \simeq \mathbb{Z}/p\mathbb{Z}[X]/(X^2+1)$ qui n'est dont pas intègre d'après ce qui précède ce qui siginifie que X^2+1 n'est pas irréductible. On a donc d'après tout ce qui précède $p \in \Sigma \Leftrightarrow (p)$ n'est pas premier $\Leftrightarrow X^2+1$ n'est pas irréductible dans $\mathbb{Z}/p\mathbb{Z}[X] \Leftrightarrow X^2+1$ a une racine dans $\mathbb{Z}/p\mathbb{Z} \Leftrightarrow p = 2$ ou $p \equiv 1[4]$ □

Leçons concernées :
120 Anneaux Z/nZ. Applications.
121 Nombres premiers. Applications.
122 Anneaux principaux. Applications.

Références

[1] Perrin. Cours d'algèbre. Ellipses.