Théorème des deux carrés

Leçons : 120, 121, 122, 126

[Per], partie II.6
[Duv], partie 6.1

Théorème

Soit p un nombre premier impair, on note $\Sigma = \left\{n \in \mathbb{N} \middle| \exists a, b \in \mathbb{N}, n = a^2 + b^2\right\}$.
On a : $p \in \Sigma \Leftrightarrow p \equiv 1\,[4]$.

Démonstration :

Pour commencer, quelques mots sur $\mathbb{Z}[\mathrm{i}]$: on définit la "norme" N : $\left|\begin{array}{ccc} \mathbb{Z}[\mathrm{i}] & \to & \mathbb{N} \\ z = a + \mathrm{i}b & \mapsto & z\bar{z} = a^2 + b^2 \end{array}\right.$;
alors N est multiplicative, ce qui signifie que $N(zz') = N(z)N(z')$ pour tous $z, z' \in \mathbb{Z}[\mathrm{i}]$.

Lemme 1

On a : $\mathbb{Z}[\mathrm{i}]^\times = \{\pm 1, \pm \mathrm{i}\}$.

Démonstration du lemme 1 :

$\subset$ Si $z \in \mathbb{Z}[\mathrm{i}]^\times$, alors $N(z)N\left(z^{-1}\right) = N(1) = 1$, donc $N(z) = 1$.
Or $z = a + \mathrm{i}b$, avec $a, b \in \mathbb{Z}$, donc $a^2 + b^2 = 1$ et on a ($a = 0$ et $b = \pm 1$) ou ($a = \pm 1$ et $b = 0$).

$\supset$ Cette vérification est immédiate... ■

Lemme 2

On a l'équivalence : $p \in \Sigma \Leftrightarrow p$ est réductible dans $\mathbb{Z}[\mathrm{i}]$.

Démonstration du lemme 2 :

$\Rightarrow$ Si $p = a^2 + b^2$, alors dans $\mathbb{Z}[\mathrm{i}]$, $p = (a + \mathrm{i}b)(a - \mathrm{i}b)$.
Comme $N(a + \mathrm{i}b) = N(a - \mathrm{i}b) = p > 1$, on sait que $a + \mathrm{i}b$, $a - \mathrm{i}b \notin \mathbb{Z}[\mathrm{i}]^\times$ et donc p est réductible.

$\Leftarrow$ Si $p = zz'$ dans $\mathbb{Z}[\mathrm{i}]$ avec $z, z' \notin \mathbb{Z}[\mathrm{i}]^\times$, on a : $N(p) = N(z)N(z') = p^2$.
Mais on sait que $N(z) \neq 1 \neq N(z')$, donc $N(z) = p$. ■

Comme $\mathbb{Z}[\mathrm{i}]$ est factoriel [1], par le lemme d'Euclide, on a :

$$p \text{ réductible dans } \mathbb{Z}[\mathrm{i}] \Leftrightarrow (p) \text{ non-premier dans } \mathbb{Z}[\mathrm{i}] \Leftrightarrow {}^{\mathbb{Z}[\mathrm{i}]}\!/_{(p)} \text{ non-intègre}$$

Mais comme $\mathbb{Z}[\mathrm{i}] \simeq {}^{\mathbb{Z}[X]}\!/_{\left(X^2+1\right)}$, on a les isomorphismes suivants :

$$\mathbb{Z}[\mathrm{i}]/_{(p)} \underset{2}{\simeq} \mathbb{Z}[X]/_{\left(X^2+1,p\right)} \simeq \left(\mathbb{Z}[X]/_{(p)}\right)/_{\left(\overline{X^2+1}\right)} \simeq \mathbb{F}_p[X]/_{\left(X^2+1\right)}$$

En conséquence, p est réductible dans $\mathbb{Z}[\mathrm{i}] \Leftrightarrow {}^{\mathbb{F}_p[X]}\!/_{\left(X^2+1\right)}$ non-intègre
$\Leftrightarrow X^2 + 1$ réductible dans $\mathbb{F}_p[X]$
$\Leftrightarrow X^2 + 1$ a une racine dans $\mathbb{F}_p$
$\Leftrightarrow -1$ est un carré dans $\mathbb{F}_p$
$\Leftrightarrow (-1)^{\frac{p-1}{2}} = \left(\dfrac{-1}{p}\right) = 1 \Leftrightarrow p \equiv 1\,[4]$ ■

1. Le plus simple pour montrer la factorialité, c'est de montrer que $\mathbb{Z}[\mathrm{i}]$ est euclidien pour la norme N, puis de dire que les anneaux euclidiens sont factoriels (voir en page **??**).

2. Je tape les explications pour un isomorphisme, adaptez ceci pour trouver les autres. Ce passage me semble absolument indispensable à savoir rédiger pour pouvoir présenter ce développement.
Notons $\pi_{X^2+1} : \mathbb{Z}[X] \to {}^{\mathbb{Z}[X]}\!/_{\left(X^2+1\right)}$ et $\pi_{\overline{p}} : {}^{\mathbb{Z}[X]}\!/_{\left(X^2+1\right)} \to \left({}^{\mathbb{Z}[X]}\!/_{\left(X^2+1\right)}\right)/_{(\overline{p})}$ les projections canoniques.
Alors $\operatorname{Ker} \pi_{\overline{p}} \circ \pi_{X^2+1} = \left\{f \in \mathbb{Z}[X] \middle| \exists u \in \mathbb{Z}[X], \overline{f} = \overline{pu}\right\} = \left\{f \in \mathbb{Z}[X] \middle| \exists u, v \in \mathbb{Z}[X], f = pu + \left(X^2+1\right)v\right\} = \left(p, X^2+1\right)$.
En conséquence, ${}^{\mathbb{Z}[X]}\!/_{\left(p, X^2+1\right)} \simeq \left({}^{\mathbb{Z}[X]}\!/_{\left(X^2+1\right)}\right)/_{(\overline{p})} \simeq \mathbb{Z}[\mathrm{i}]/_{(p)}$.

Corollaire

Soit $n \in \mathbb{N}^*$, qu'on décompose en facteurs premiers : $n = \prod_{p\in\mathcal{P}} p^{\nu_p(n)}$ (où $\mathcal{P}$ désigne l'ensemble des nombres premiers).
On a l'équivalence : $n \in \Sigma \Leftrightarrow \left(\forall p \in \mathcal{P}, p \equiv 3\,[4] \Rightarrow \nu_p(n) \equiv 0\,[2]\right)$.

Démonstration :

Lemme 3

Σ est stable par multiplication.

Démonstration du lemme 3 :

En effet, on sait déjà que $n \in \Sigma \Leftrightarrow \exists z \in \mathbb{Z}[\mathrm{i}], n = N(z)$.
En conséquence, si $n, n' \in \Sigma$, alors $nn' = N(z)N(z') = N(zz') \in \Sigma$. ■

$\Leftarrow$ On décompose n de la façon suivante :

$$n = \underbrace{\left(\prod_{\substack{p\in\mathcal{P}\\ p\equiv 3\,[4]}} p^{\frac{\nu_p(n)}{2}}\right)^2}_{\text{Carré parfait}} \underbrace{\left(\prod_{\substack{p\in\mathcal{P}\\ p\not\equiv 3\,[4]}} p^{\nu_p(n)}\right)}_{\substack{\text{Somme de 2 carrés}\\ \text{(lemme 3)}}}$$

$\Rightarrow$ Soit $n = a^2 + b^2 \in \Sigma$, on note $\delta = a \wedge b$, $a' = \frac{a}{\delta}$ et $b' = \frac{b}{\delta}$.
Ainsi, $a' \wedge b' = 1$ et $n = \delta^2\left(a'^2 + b'^2\right)$.
Soit p un diviseur premier impair de $a'^2 + b'^2$; alors dans $\mathbb{Z}[\mathrm{i}]$, on a : $p|(a' + \mathrm{i}b')(a' - \mathrm{i}b')$.
- Par l'absurde, supposons p irréductible dans $\mathbb{Z}[\mathrm{i}]$.
  Le lemme d'Euclide nous indique que $p|(a' + \mathrm{i}b')$ ou que $p|(a' - \mathrm{i}b')$; mais par passage au conjugué, si p divise l'un, alors p divise l'autre.
  Donc p divise les deux, puis par somme et différence, on obtient : $p|2a'$ et $p|2\mathrm{i}b'$ dans $\mathbb{Z}[\mathrm{i}]$.
  En passant à la norme, on en déduit : $p^2\big|4a'^2$ et $p^2\big|4b'^2$, dans $\mathbb{Z}$.
  Mais on sait que p est impair, et donc $p|a'$ et $p|b'$.
  Contradiction !
- On peut donc écrire $p = xy$ dans $\mathbb{Z}[\mathrm{i}]$, avec en plus $N(x) \neq 1 \neq N(y)$ (ce qui signifie, rappelons-le, que x et y peuvent être pris non-inversibles).
  En passant à la norme, on obtient : $p^2 = N(x)N(y)$; puis, p étant premier, on obtient : $p = N(x)$.
  En conséquence, $p \in \Sigma$, d'où $p \equiv 1\,[4]$.

Ainsi, on a montré que les facteurs premiers congrus à 3 modulo 4 sont "dans" le δ^2, c'est-à-dire d'exposant pair. ■

Références

[Per] D. PERRIN – *Cours d'algèbre*, Ellipses, 1996.
[Duv] D. DUVERNEY – *Théorie des nombres*, 2e éd., Dunod, 2007.