20 Entiers de Gauss et théorème des deux carrés

ref : Perrin

THÉORÈME 20.1 *1. L'anneau $\mathbb{Z}[i] = \{a + ib, a, b \in \mathbb{N}\}$ est euclidien pour le stathme $N(a + ib) = a^2 + b^2$.*

2. Soit p un nombre premier. Alors p est somme de deux carrés si et seulement si $p = 2$ ou $p = 1 \mod 4$.

PREUVE. idée : $a^2 + b^2 = (a + ib)(a - ib)$. D'où le lien entre somme de deux carrés et irréductibles de $\mathbb{Z}[i]$.

$\mathbb{Z}[i]$ est euclidien :

Soit $z \in \mathbb{Z}[i]$ et $w \in \mathbb{Z}[i] \setminus \{0\}$. Il existe $q \in \mathbb{Z}[i]$ tel que $r' = \frac{z}{w} - q$ soit de norme inférieure à $\frac{1}{\sqrt{2}}$. Alors $z = wq + wr'$ avec $N(wr') \leq \frac{N(w)}{\sqrt{2}} < N(w)$. On a donc bien une division euclidienne.

Inversibles de $\mathbb{Z}[i]$: Les inversibles sont de norme 1 car $zz' = 1 \Rightarrow N(z)N(z') = 1$ dans $\mathbb{Z}$, donc $N(z) = N(z') = 1$. On vérifie réciproquement que les entiers de Gauss de norme 1 à savoir $\{1, -1, i, -i\}$ sont inversibles.

Nombres premiers et irréductibles de $\mathbb{Z}[i]$ Notons Σ l'ensemble des nombres premiers somme de deux carrés.

LEMME 20.2 *$p \in \Sigma \Leftrightarrow p$ n'est pas irréductible dans $\mathbb{Z}[i]$.*

PREUVE. Si $p = a^2 + b^2$ alors $a \neq 0$ et $b \neq 0$ et $p = (a + ib)(a - ib)$ avec $(a + ib)$ et $(a - ib)$ non inversibles.

Réciproquement, si p est réductible, il s'écrit $p = zz'$ avec z, z' non inversibles. Donc $N(p) = p^2 = N(z)N(z')$, puis $N(z) = N(z') = p$ car p est premier. Ainsi p est la norme d'un élément, c'est-à-dire une somme de deux carrés. □

Réduction modulo p :

Par factorialité de $\mathbb{Z}[i]$, p réductible $\Leftrightarrow$ (p) non premier dans $\mathbb{Z}[i] \Leftrightarrow \mathbb{Z}[i]/(p)$ non intègre.

Regardons quand cela se produit.

On a l'isomorphisme $\mathbb{Z}[i] \simeq \mathbb{Z}[x]/(X^2 + 1)$. En effet, par propriété universelle de l'anneau des polynômes, on a un morphisme surjectif $\varphi : \mathbb{Z}[X] \to \mathbb{Z}[i]$ défini de manière unique par $\varphi(X) = i$. Son noyau contient clairement l'idéal $(X^2 + 1)$. Réciproquement, si $P \in \ker \varphi$, par division euclidienne unitaire dans $\mathbb{Z}[X]$, il existe Q, R tel que $P = (X^2 + 1)Q + R$ avec $\deg(R) \leq 1$. Et $R(i) = 0$ implique $R = 0$ car R est de degré ≤ 1. Le théorème d'isomorphisme donne alors l'isomorphisme souhaité.

Ce même théorème permet d'intervertir l'ordre des quotients :

$$\mathbb{Z}[i]/(p) = \mathbb{Z}[X]/(p, X^2 + 1) = \mathbb{F}_p[X]/(X^2 + 1)$$

Ce dernier anneau est intègre si et seulement si $(X^2 + 1)$ est irréductible si et seulement si il n'a pas de racines car c'est un polynôme de degré 2.

On obtient donc, p réductible dans $\mathbb{Z}[i]$ si et seulement si -1 est un carré dans $\mathbb{F}_p$.

-1 est-t-il un carré dans $\mathbb{F}_p$? :

Si $p = 2$, tous les éléments sont des carrés, car $x \to x^2$ (Frobenius) est un morphisme de corps, donc injectif est bijectif par cardinal.

Si $p > 2$, x est un carré dans $\mathbb{F}_p$ si et seulement si $x^{\frac{p-1}{2}} = 1$. En effet, si $x = y^2$, $x^{\frac{p-1}{2}} = y^{p-1} = 1$ car $\mathbb{F}_p^*$ est d'ordre $p-1$. Il y a $\frac{p-1}{2}$ carrés non nuls, car le noyau du frobenius est d'ordre 2, qui sont tous racines de l'équation $X^{\frac{p-1}{2}} = 1$ de degré $\frac{p-1}{2}$. Par cardinal, on a l'équivalence souhaitée.

La condition est donc : $p \in \Sigma \Leftrightarrow p = 2$ ou $p = 1 \mod 4$. □

Leçons concernées : Anneaux principaux, nombres premiers.