Théorème des deux carrées

Jojo

April 2019

1 Entiers de Gauss et théorème des deux carrées

Références : [2] p56 et [1]

Recasages. 121-122-126-142

On ce propose ici de caractériser les éléments de l'ensemble :

$$\Sigma = \{n \in \mathbb{N} | \exists a, b \in \mathbb{N} \ tq \ n = a^2 + b^2\} \tag{1}$$

Soit $\mathbb{Z}[i] = \{a + bi | a, b \in \mathbb{Z}\}$ l'ensemble des entiers de Gauss. On le munit de la norme :

$$\begin{aligned} N : &\mathbb{Z}[i] \to \mathbb{N} \\ &z \to z\overline{z} \end{aligned} \tag{2}$$

La multiplicativité de N ce déduit aisément de celle de $z \to \overline{z}$ et de la commutativité de $\mathbb{C}$.

Proposition 1. $\mathbb{Z}[i]^\star = \{\pm 1, \pm i\}$

Démonstration. L'inclusion de l'ensemble de droite dans celui de gauche est facile. Soit $z \in \mathbb{Z}[i]^\star$, $\exists z' \in \mathbb{Z}[i]$ tel que zz'=1. Et donc N(zz')=N(z)N(z')=1. Comme N est à valeure dans les entiers naturels On en déduit que N(z)=1. z s'écrit donc $z = a + ib$, avec a et b des entiers tel que $a^2 + b^2 = 1$. Donc a ou b est nul, et le non nul du couple vaut plus ou moins un ce qui ce réécrit : $z \in \{\pm i, \pm 1\}$. □

Donnons une première propriété de Σ.

Proposition 2. Σ est stable par multiplication.

Démonstration. Vu la définition on a :

$$n \in \Sigma \leftrightarrow \exists z \in \mathbb{Z}[i] \ tq \ n = N(z) \tag{3}$$

Soit donc $n, n' \in \Sigma$, $\exists z, z' \in \mathbb{Z}[i]$ tels que $n = N(z)$ et $n' = N(z')$. Par multiplicativité de N on a nn'=N(z)N(z')=N(zz')$\in \Sigma$. □

Remarque 1. La preuve de cette propriété démontre l'efficacité de l'introduction des entiers de Gauss. Notons que la multiplicativité de N est l'identité dites de Lagrange, qui ce réécrit :

$$(a^2 + b^2)(c^2 + d^2) = (ac - bd)^2 + (ad + bc)^2 \tag{4}$$

Comme on a établit la stabilité de Σ par multiplication, l'étude des éléments de cet ensemble peut ce ramener à l'étude des nombres premiers qui sont dans Σ.

La poursuite de l'étude de Σ nécessite de préciser la structure arithmétique de $\mathbb{Z}[i]$.

Théorème 1. *$(\mathbb{Z}[i], N)$ est euclidien, donc principal.*

Démonstration. Soit $z, t \in \mathbb{Z}[i] - \{0\}$. Considérons $\frac{z}{t} \in \mathbb{C}$. Posons $\frac{z}{t} = x + iy,\ x, y \in \mathbb{R}$. Et soit $q = a + ib$ l'entier de Gauss tel que a (respect b) est l'entier le plus proche de x (respect y). Si x ou y $\in \mathbb{N} + \frac{1}{2}\mathbb{N}$ prendre par exemple l'entier inférieur. On a par inégalité triangulaire :

$$|\frac{z}{t} - q| \leq \frac{\sqrt{2}}{2} < 1 \tag{5}$$

Et posons $r = z - qt \in \mathbb{Z}[i]$. On a donc :

$$|r| = |t||\frac{z}{t} - q| < |t| \tag{6}$$

En élevant la dernière inégalité au carrée on trouve N(r)<N(t). On a bien écrit z=qt+r où N(r)<N(t). □

On peut maintenant passer au théorème suivant :

Théorème 2. *Soit p un nombre premier :*

$$p \in \Sigma \leftrightarrow p = 2 \text{ ou } p = 1 \ mod(4) \tag{7}$$

Démonstration. Soit $p \in \Sigma$. On écrit $p = a^2 + b^2\ a, b \in \mathbb{N}$. Si a est impair $a^2 = 1$ mod(4). Si a est pair $a^2 = 0 mod(4)$, idem pour b donc p est congru à 0, 1 ou 2 modulo 4. Mais si p est congru à 0 modulo 4, p n'est pas premier. Donc p est bien congru à 1 ou 2 modulo 4.

Pour l'implication réciproque utilisons le lemme suivant :

Lemme 3.

$$p \in \Sigma \leftrightarrow\ \ p \in \mathbb{N} \text{ et } p \text{ est réductible dans } \mathbb{Z}[i] \tag{8}$$

Démonstration. Soit $p \in \Sigma$. $\exists a, b \in \mathbb{Z}$ tel que $p = a^2 + b^2$. Alors on peut écrire dans $\mathbb{Z}[i]$, $p = (a+ib)(a-ib)$, et p étant premier a et b son non nuls, donc $a - ib$ et $a + ib$ ne sont pas dans $\mathbb{Z}[i]^\star$. Donc p est bien réductible dans $\mathbb{Z}[i]$.

Pour l'implication réciproque si $p = zz'$, $z, z' \notin \mathbb{Z}[i]^\star$, alors $N(p) = N(z)N(z') = p^2$, et comme $N(z), N(z') \neq 1$ on a forcément $p = N(z)$ d'où $p \in \Sigma$. □

Par principalité de $\mathbb{Z}[i]$, $\mathbb{Z}[i]$ est factoriel et donc p n'est pas irréductible ssi (p) est non premier i.e $\mathbb{Z}[i]/(p)$ est non intègre. On utilise l'isomorphisme :

$$\mathbb{Z}[i] \cong \mathbb{Z}[X]/(X^2 + 1) \tag{9}$$

On en déduit les isomorphismes suivant :

$$\mathbb{Z}[i]/(p) \cong \mathbb{Z}[X]/(X^2 + 1, p) \cong [\mathbb{Z}[X]/(p)]/(X^2 + 1) \cong \mathbb{Z}/p\mathbb{Z}[X]/(X^2 + 1) \tag{10}$$

et donc p n'est pas irréductible ssi $(X^2 + 1)$ n'est pas irréductible dans $F_p[X]$ ssi $X^2 + 1$ a une racine dans F_p ssi p congru à 1 ou 2 modulo 4. □

Concluons :

Théorème 4. *Soit $n \in \mathbb{N}^\star$ dont la décomposition en facteurs premiers est*

$$n = \prod_{p \in P} p^{v_p(n)} \tag{11}$$

Alors $n \in \Sigma \leftrightarrow v_p(n)$ est pair pour p congru à 3 mod 4.

Pour la culture : (cf [1])

Théorème 5. *(Des trois carrées)*
$n \in \mathbb{N}$ est somme de trois carrées ssi il n'est pas de la forme $n = 4^a(8m + 7)$

Théorème 6. *(Des quatres carrées)*
Soit $n \in \mathbb{N}$ alors il existe des entiers x,y,z,t tels que $n = x^2 + y^2 + z^2 + t^2$

Références

[1] M.Hindry. *Arithmétique : primalité et codes, théorie analytique des nombres, équations diophantiennes, courbes elliptiques*. 2007.

[2] Daniel Perrin. *Cours d'Algèbre*. 1996.