Somme de deux carrés

Julie Parreaux

2018-2019

Référence du développement : Perrin [1, p.56].

Leçons où on présente le développement : 120 (Anneaux $\mathbb{Z}/n\mathbb{Z}$) ; 126 (Équations arithmétiques).

1 Introduction

Le théorème des deux carrés de Fermat énonce les conditions pour qu'un nombre entier soit la somme de deux carrés parfaits (c'est-à-dire de deux carrés d'entiers) et précise de combien de façons différentes il peut l'être. Dans le cadre des équations diophantiennes (ici c'est le cas) la simplicité de l'énoncé cache une difficulté réelle de démonstration. Certaines des preuves proposées ont aidé à la mise au point d'outils parfois sophistiqués : ici nous utilisons les entiers de Gauss.

2 Théorème des deux carrés de Fermat

Problème : Déterminer $n \in \mathbb{N}$ tel que $n = a^2 + b^2$ avec $a, b \in \mathbb{N}$. Autrement dit, quels sont les entiers de somme deux carrés ? On cherche donc à déterminer $\Sigma = \{n \in \mathbb{N} | n = a^2 + b^2, a, b \in \mathbb{Z}\}$.

Exemple : $0, 1, 2, 4, 5, 8, 9, 10 \in \Sigma$ et $3, 6, 7, 11, 12 \notin \Sigma$

Remarque : Si $n \equiv 3[4]$ alors $n \notin \Sigma$. En effet, si a est paire alors $a^2 \equiv 0[4]$ et si a est impaire, $a^2 \equiv 1[4]$ donc $n \not\equiv 3[4]$.

Schéma du développement

Idée : On utilise les entiers de Gauss pour étudier Σ. En effet, si on se place dans $\mathbb{C}$ et que $n \in \Sigma$, alors $n = (a + ib)(a - ib)$.

1. Étude de l'anneau $\mathbb{Z}[i]$.
   - — $\mathbb{Z}[i]$ est intègre.
   - — $\mathbb{Z}[i]^* = \{-1, -i, 1, i\}$ (lemme 1).
   - — $\mathbb{Z}[i]$ est euclidien donc principal (lemme 2).
2. Preuve dans le cas p premier.
   - $\Leftarrow$ Immédiat par contraposée.
   - $\Rightarrow$ Caractérisation des irréductibles (lemme 3).
3. Preuve du théorème.
   - $\Leftarrow$ Stabilité de Σ par multiplication (lemme 4).
   - $\Rightarrow$ Récurrence.

Théorème. *Soit $n \geq 1$ un entier.*

$$n \in \Sigma \Leftrightarrow v_p(n) \text{ est pair pour } p \equiv 3[4]$$

où $v_p(n)$ est défini par la décomposition en facteur premier de n : $n = \prod_{p \in \mathcal{P}} p^{v_p(n)}$.

Démonstration. *Idée* : On utilise les entiers de Gauss pour étudier Σ. En effet, si on se place dans $\mathbb{C}$ et que $n \in \Sigma$, alors $n = (a+ib)(a-ib)$.
On pose $\mathbb{Z}[i] = \{a+ib \in \mathbb{C} | a, b \in \mathbb{Z}\}$.

Étape 1 : étude de $\mathbb{Z}[i]$.

— $\mathbb{Z}[i]$ est intègre car il est inclut dans $\mathbb{C}$.
— On muni $\mathbb{Z}[i]$ de l'automorphisme $\sigma : z = a+ib \mapsto \overline{z} = a-ib$.
— On muni $\mathbb{Z}[i]$ d'une norme multiplicative $N : z = a+ib \mapsto \overline{z}z = a^2+b^2$

Lemme 1. $\mathbb{Z}[i]^* = \{-1, -i, 1, i\}$

Démonstration. $\subseteq$ — Si $z = a+ib \in Z[i]^*$, alors il existe z' tel que $zz' = 1$.
— En appliquant la norme (multiplicative), $N(zz') = 1 = N(z)N(z')$.
— Comme $N(z), N(z') \in \mathbb{N}$ (définition de la norme), $N(z) = N(z') = 1$.
— On en déduit que $a^2+b^2 = 1$ soit $a = 0$ et $b \in \{1, -1\}$, soit $b = 0$ et $a \in \{1, -1\}$.
$\supseteq$ Immédiat par calcul.

□

Lemme 2. *L'anneaux $\mathbb{Z}[i]$ est euclidien relativement à N donc il est principal.*

Démonstration. Soit $z, t \in \mathbb{Z}[i] \setminus \{0\}$. On cherche $q, r \in \mathbb{Z}[i]$ tel que $z = qt + r$ avec $N(r) < N(t)$.
→ Soit $\frac{z}{t} \in \mathbb{C}$ (possible dans $\mathbb{C}$), alors $\frac{z}{t} = x + iy$. On souhaite alors approcher $\frac{z}{t}$ par des entiers de Gauss.
→ Soit a, b les entiers les plus proches de x, y (existe par les propriétés sur les entiers).
— Posons $q = a+ib$ et on a :

$$\begin{aligned} \left|\frac{z}{t} - q\right| &= |x+iy-a-ib| && \text{(définition)} \\ &= \sqrt{|x-a|^2 + |y-b|^2} && \text{(définition du module)} \\ &\leq \sqrt{\left(\frac{1}{2}\right)^2 + \left(\frac{1}{2}\right)^2} && \text{(entier les plus proches)} \\ &= \sqrt{\frac{2}{4}} && \text{(calcul)} \\ &\leq 1 \end{aligned}$$

— Posons $r = z - qt$ et on a :
- $z \in \mathbb{Z}[i]$ ($z, t, q \in \mathbb{Z}[i]$)
- $r = t\left(\frac{z}{t} - q\right)$ soit $|r| < |t|$. D'où en élevant au carré, $N(r) < N(t)$.

□

Étape 2 : preuve dans le cas p premier.

Proposition. *Soit $p \in \mathbb{N}$ un nombre premier.*

$$p \in \Sigma \Leftrightarrow p \equiv 2[4] ou p \equiv 1[4]$$

Démonstration. $\Leftarrow$ Immédiat par contraposée car par la remarque, on a que si $p \equiv 3[4]$ alors $p \notin \Sigma$.
$\Rightarrow$ On utilise le lemme suivant.

Lemme 3. *$p \in \Sigma \Leftrightarrow p$ n'est pas irréductible dans $\mathbb{Z}[i]$.*

Démonstration. $\Rightarrow$ Si $p = a^2+b^2$ alors $p = (a+ib)(a-ib)$ avec $a, b \neq 0$ (sinon pp ne serait pas premier). Par le lemme 1 $a+ib$ et $a-ib$ ne sont donc pas inversibles. Donc p n'est pas irréductible.

$\Leftarrow$ Si $p = zz'$ avec $z, z' \notin \mathbb{Z}[i]$ (définition de ne pas être irréductible), on a $N(p) = N(z)N(z') = p^2$ (par définition de la norme et car p est premier). Comme $N(z), N(z') \in \mathbb{N} \setminus \{0, 1\}$, alors $p = N(z) = a^2 + b^2$ et p est donc premier. Donc $p \in \Sigma$.

□

— Comme $\mathbb{Z}[i]$ est principal (lemme 2), donc factoriel, dire que p est non irréductible, c'est dire que l'idéal $(p) = p\mathbb{Z}[i]$ est non premier. Donc $\mathbb{Z}[i]/(p)$ n'est pas intègre.

— Pour étudier ce quotient, on utilise l'isomorphisme suivant : $\mathbb{Z}[i] \simeq \mathbb{Z}[X]/(X^2+1)$ (division euclidienne). Puis le théorème d'isomorphisme nous donne :

$$\begin{array}{rcll} \mathbb{Z}[i]/(p) & \simeq & \mathbb{Z}[X]/(X^2+1, p) & \text{(définition de } \mathbb{Z}[i]) \\ & \simeq & (\mathbb{Z}[X]/(p))/(X^2+1) & \text{(théorème)} \\ & \simeq & (\mathbb{Z}/p\mathbb{Z}[X])/(X^2+1) & \text{(définition de } \mathbb{Z}/p\mathbb{Z}) \\ & \simeq & (\mathbb{F}_p[X])/(X^2+1) & (p \text{ premier}) \end{array}$$

On en déduit que

$$\begin{array}{rcl} (p) \text{ non premier} & \Leftrightarrow & X^2+1 \text{ non irréductible dans } \mathbb{F}_p \\ & \Leftrightarrow & X^2+1 \text{ a une racine dans } \mathbb{F}_p \\ & \Leftrightarrow & -1 \text{ est un carré dans } \mathbb{F}_p \\ & \Leftrightarrow & p \equiv 1, 2[4] \end{array}$$

□

Étape 3 : preuve du théorème. Montrons maintenant le théorème dans le cas général.

$\Leftarrow$ On utilise le lemme suivant.

Lemme 4. *Σ est stable par multiplication.*

Démonstration. — $n \in \Sigma \Leftrightarrow \exists z \in \mathbb{Z}[i], n = N(z)$ (déjà vu).

— si $n, n' \in \Sigma$, $n = N(z)$ et $n' = N(z')$ donc $nn' = N(zz') \in \Sigma$

□

Σ étant stable par multiplication si $p \equiv 1, 2[4]$ alors $p^{v_p(n)} \in \Sigma$. Sinon, $p \equiv 3[4]$, $p \in \Sigma$ donc comme $v_p(n)$ est pair et $p^{v_p(n)} \in \Sigma$. On conclut par la stabilité de Σ.

$\Rightarrow$ Supposons que $p \equiv 3[4]$. Montrons par récurrence sur $n \in \mathbb{N}$ que $v_p(n)$ est paire.

Initialisation $v_p(0) = 0$ ok

Hérédité soit n tel que pour tout $m < n$, $v_p(m)$ est pair. Si $v_p(n) = 0$ ok. Sinon, $p|n = a^2 + b^2 = (a+ib)(a-ib)$. Comme $p \in \mathbb{Z}$, $p|a$ et $p|b$ donc $p^2|n$. On en déduit que $a = pa'$ et $b = pb'$ soit $\frac{n}{p^2} = a'^2 + b'^2 \in \Sigma$. On en déduit $v_p\left(\frac{n}{p^2}\right) = v_p(n) - 2$ est pair (car $v_p\left(\frac{n}{p^2}\right)$ est pair par hypothèse de récurrence).

□

Références

[1] D. Perrrin. *Cours d'algèbre*. Ellipse, 1996.