Equation des deux carrés par les entiers de Gauss

Dorian Cacitti-Holland

2020-2021

Références.

1. Cours d'algèbre de Daniel Perrin

Leçons.

1. 121 Nombres premiers, applications
2. 122 Anneaux principaux, applications
3. 126 Exemples d'équations en arithmétique

Théorême. On considère

$$\Sigma := \{n \in \mathbb{N} \mid \exists (a,b) \in \mathbb{N}^2, n = a^2 + b^2\}$$

Soit $p \in \mathbb{N}$ premier, alors $p \in \Sigma$ si et seulement si $p = 2$ ou $p \equiv 1[4]$.

Démonstration. Commençons par remarquer que $p = 2 = 1^2 + 1^2$, d'où $2 \in \Sigma$.
On suppose désormais $p \in \mathbb{N}$ premier distinct de 2.
Etape 1 : Le sens direct
On suppose $p \in \Sigma$, alors $p = a^2 + b^2$ avec $a, b \in \mathbb{N}$.
Or les carrés dans $\mathbb{Z}/4\mathbb{Z}$ sont 0 et 1, donc $p \equiv 0, 1 + 0, 1[4]$.
Donc, comme p premier impair, $p \equiv 1[4]$.
Etape 2 : Le sens indirect
Réciproquement on suppose $p \equiv 1[4]$.
Donc $(-1)^{\frac{p-1}{2}} = 1$, d'où, par théorème de caractérisation des carrés, -1 est un carré dans $\mathbb{Z}/p\mathbb{Z}$.
Ainsi $X^2 + 1$ admet une racine dans $\mathbb{Z}/p\mathbb{Z}$, d'où $\mathbb{Z}/p\mathbb{Z}[X]/(X^2 + 1)$ n'est pas intègre
Or par division euclidienne sur $\mathbb{Z}[X]$ par $X^2 + 1$, on a l'isomorphisme

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

Puis par théorème d'isomorphisme d'anneaux quotients :

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

Ainsi $\mathbb{Z}[i]/(p) \simeq (\mathbb{Z}/p\mathbb{Z}[X])/(X^2 + 1)$ n'est pas un anneau intègre.
Par conséquent (p) n'est pas un idéal premier et p n'est pas irréductible.

Ainsi il existe $(z, z') \in (\mathbb{Z}[i]\backslash\mathbb{Z}[i]^\times)^2 = (\mathbb{Z}[i]\backslash\{1, -1, i, -i\})^2$ tel que $p = zz'$.
Ainsi $p^2 = N(p) = N(z)N(z')$ puis, comme p premier et z, z' non inversibles, $N(z) = N(z') = p$.
Or si on écrit $z = a + ib \in \mathbb{Z}[i]$ alors on a

$$p = N(z) = a^2 + b^2$$

D'où $p \in \Sigma$. □

Théorême. Si $n \in \mathbb{N}^*$ alors $n \in \Sigma$ si et seulement si pour tout $p \in \mathbb{N}$ premier,

$$p \equiv 3[4] \Rightarrow \nu_p(n) \in 2\mathbb{N}$$

Démonstration.
Etape 1 : Sens direct : On montre par récurrence forte sur $n \in \mathbb{N}\backslash^*$ la propriété :

$$n \in \Sigma \Longrightarrow [\forall p \in \mathcal{P}, p \equiv 3[4] \Rightarrow \nu_p(n) \in 2\mathbb{N}]$$

L'initialisation vient de $1 \in \Sigma$ et

$$\forall p \in \mathcal{P}, p \equiv 3[4] \Rightarrow \nu_p(1) = 0 \in 2\mathbb{N}$$

Soit $n \in \mathbb{N}$ tel que $n > 1$ et $n \in \Sigma$.
On suppose la propriété vraie pour tout $k \in [\![1, n-1]\!]$.
Soit $p \in \mathcal{P}$ tel que $p \equiv 3[4]$.
Si $\nu_p(n) = 0$ alors $\nu_p(n) \in 2\mathbb{N}$.
Puis si $\nu_p(n) > 0$ alors

$$p \mid n = a^2 + b^2 = (a + ib)(a - ib)$$

Or $p \equiv 3[4]$, donc, d'après le théorème précédent, $p \notin \Sigma$.
Ainsi p est irréductible dans $\mathbb{Z}[i]$ (il s'agit de la contraposée du dernier raisonnement de l'étape 2 de la démonstration du théorème précédent).
D'où $p \mid a + ib$ (ou $p \mid a - ib$).
Or $p \in \mathcal{P} \subset \mathbb{Z}$, donc $p \mid a, p \mid b$, d'où $p^2 \mid a^2 + b^2 = n$ et il existe $(a', b') \in \mathbb{N}^2$ tel que $a = a'p, b = b'p$.
D'où

$$\frac{n}{p^2} = a'^2 + b'^2 \in \Sigma$$

Or $\nu_p\left(\frac{n}{p^2}\right) = \nu_p(n) - 2$ et $\frac{n}{p^2} < n$, donc, par hypothèse de récurrence,

$$\nu_p(n) = \nu_p\left(\frac{n}{p^2}\right) + 2 \in 2\mathbb{N}$$

Le théorème de récurrence permet de conclure.
Etape 2 : Sens indirect
Réciproquement on suppose que

$$\forall p \in \mathcal{P}, p \equiv 3[4] \Rightarrow \nu_p(n) \in 2\mathbb{N}$$

Soit $p \in \mathcal{P}$ tel que $p \mid n$.
Alors si $p = 2$ ou $p \equiv 1[4]$ alors d'après le théorème précédent, $p \in \Sigma$.
Puis si $p \equiv 3[4]$ alors, par hypothèse, $\nu_p(n) \in 2\mathbb{N}$, d'où $p^{\nu_p(n)}$ est un carré.
Donc on en déduit, d'après la stabilité de Σ par produit, que $n \in \Sigma$.
En effet la stabilité a lieu car, pour $m \in \mathbb{N}$ on a $m \in \Sigma \iff \exists z \in \mathbb{Z}[i], m = N(z)$ et pour $z, z' \in \mathbb{Z}[i], N(zz') = N(z)N(z')$. □

Lemme. (S'il reste du temps) Soit $p \in \mathbb{N}$ premier alors $p \in \Sigma$ si et seulement si p n'est pas irréductible dans $\mathbb{Z}[i]$.

Démonstration.
Etape 1 : Sens direct
On suppose que $p \in \Sigma$. Alors il existe $(a, b) \in \mathbb{N}^2$ tel que

$$p = a^2 + b^2 = (a + ib)(a - ib)$$

En particulier on a $a \neq 0$ et $b \neq 0$.
Ainsi $a + ib$ et $a - ib$ ne sont pas inversible dans $\mathbb{Z}[i]$ car

$$\mathbb{Z}[i]^\times = \{1, -1, i, -i\}$$

Par conséquent p n'est pas irréductible dans $\mathbb{Z}[i]$.
Etape 2 : Sens indirect (déjà fait dans la démonstration)
Réciproquement on suppose que p n'est pas irréductible dans $\mathbb{Z}[i]$. Alors il existe $(z, z') \in (\mathbb{Z}[i] \backslash \mathbb{Z}[i]^\times)^2 = (\mathbb{Z}[i] \backslash \{1, -1, i, -i\})^2$ tel que

$$p = zz'$$

Ainsi

$$p^2 = N(p) = N(z)N(z')$$

Donc

$$N(z) = N(z') = p$$

Or si on écrit $z = a + ib \in \mathbb{Z}[i]$ alors on a

$$p = N(z) = a^2 + b^2$$

D'où $p \in \Sigma$. □