

# Théorème des deux carrés de Fermat

Nous démontrons le théorème des deux carrés de Fermat (qui donne des conditions sur la décomposition en facteurs premiers d'un entier pour que celui-ci soit somme de deux carrés) à l'aide de l'anneau des entiers de Gauss  $\mathbb{Z}[i]$ .

**Lemme 1.** Soit  $p \geq 3$  un nombre premier. Alors  $x \in \mathbb{F}_p^*$  est un carré si et seulement si  $x^{\frac{p-1}{2}} = 1$ .

[I-P]  
p. 137

*Démonstration.* On pose  $X = \{x \in \mathbb{F}_p \mid x^{\frac{p-1}{2}} = 1\}$ , et on note  $S$  l'ensemble des carrés de  $\mathbb{F}_p^*$ . Comme un polynôme de degré  $d$  sur  $\mathbb{F}_p$  possède au plus  $d$  racines, on a  $|X| \leq \deg(X^{\frac{p-1}{2}} - 1) = \frac{p-1}{2}$ .

D'autre part, si  $x \in S$ , on peut écrire  $x = y^2$  et on a donc  $x^{\frac{p-1}{2}} = y^{p-1} = 1$  car  $|\mathbb{F}_p^*| = p-1$ . Donc,  $S \subseteq X$ .

Pour conclure, calculons le cardinal de  $S$ . Pour cela, considérons le morphisme

$$\begin{array}{ccc} \mathbb{F}_p^* & \rightarrow & S \\ x & \mapsto & x^2 \end{array}$$

dont le noyau est  $\{x \in \mathbb{F}_p^* \mid x^2 = 1\} = \{\pm 1\}$  qui est de cardinal 2. En appliquant le premier théorème d'isomorphisme, et en considérant les cardinaux; on obtient  $|S| = \frac{p-1}{2}$ . Donc  $S = X$ .  $\square$

Introduisons maintenant des notations qui seront utiles pour la suite.

**Notation 2.** On note

$$N : \begin{array}{ccc} \mathbb{Z}[i] & \rightarrow & \mathbb{N} \\ a + ib & \mapsto & a^2 + b^2 \end{array}$$

et  $\Sigma$  l'ensemble des entiers qui sont somme de deux carrés.

*Remarque 3.*  $n \in \Sigma \iff \exists z \in \mathbb{Z}[i] \text{ tel que } N(z) = n$ .

**Lemme 4.** Voici quelques propriétés sur  $N$  et  $\mathbb{Z}[i]$  dont nous aurons besoin :

- (i)  $N$  est multiplicative.
- (ii)  $\mathbb{Z}[i]^* = \{z \in \mathbb{Z}[i] \mid N(z) = 1\} = \{\pm 1, \pm i\}$ .
- (iii)  $\mathbb{Z}[i]$  est euclidien de stathme  $N$ .

*Démonstration.* (i) On a  $\forall z, z' \in \mathbb{C}, |zz'||^2 = |z|^2 |z'|^2$  (par multiplicativité de  $(.)^2$  et de  $|\cdot|$ ). Et  $N$  n'est que la restriction de  $|\cdot|^2$  à  $\mathbb{Z}[i]$ . Il est également tout-à-fait possible de montrer cette propriété par un calcul direct.

- (ii) Soit  $z \in \mathbb{Z}[i]^*$ . On a  $N(z)N(z^{-1}) = N(zz^{-1}) = N(1) = 1$ . Comme  $N$  est à valeurs dans  $\mathbb{N}$ , on a  $N(z) = N(z^{-1}) = 1$ . En écrivant  $z = a + ib$ , on a  $N(z) = a^2 + b^2 = 1$ , d'où  $a = \pm 1$  ou  $b = \pm 1$ . Réciproquement,  $\pm 1$  et  $\pm i$  sont bien inversibles dans  $\mathbb{Z}[i]$  et de module 1.

(iii) Soient  $z, t \in \mathbb{Z}[i]$ . On pose  $\frac{z}{t} = x + iy \in \mathbb{C}$  avec  $x, y \in \mathbb{R}$ . Soient  $a, b \in \mathbb{Z}$  tels que :

- $|x - a| \leq \frac{1}{2}$ .
- $|y - b| \leq \frac{1}{2}$ .

(Ces nombres existent bien, ne pas hésiter à faire un dessin pour s'en convaincre.) On pose  $q = a + ib \in \mathbb{Z}[i]$ , et on a

$$\left| \frac{z}{t} - q \right| = (x - a)^2 + (y - b)^2 \leq \frac{1}{4} + \frac{1}{4} < 1$$

On pose alors  $r = z - qt$ , et on a bien

$$z = tq + r \text{ et } N(r) = r^2 = |t|^2 \left| \frac{z}{t} - q \right|^2 < |t|^2 = N(t)$$

□

**Lemme 5.** Soit  $p$  un nombre premier. Si  $p$  n'est pas irréductible dans  $\mathbb{Z}[i]$ , alors  $p \in \Sigma$ .

*Démonstration.* On suppose que  $p$  n'est pas irréductible dans  $\mathbb{Z}[i]$ . On peut donc écrire  $p = uv$  avec  $u, v \in \mathbb{Z}[i]$  non inversibles. Ainsi,

$$p^2 = N(p) = N(uv) = \underbrace{N(u)}_{\neq 1} \underbrace{N(v)}_{\neq 1} \xrightarrow{p \text{ premier}} N(u) = N(v) = p$$

Par la Remarque 3,  $p \in \Sigma$ .

□

**Théorème 6** (Deux carrés de Fermat). Soit  $n \in \mathbb{N}^*$ . Alors  $n \in \Sigma$  si et seulement si  $v_p(n)$  est pair pour tout  $p$  premier tel que  $p \equiv 3 \pmod{4}$  (où  $v_p(n)$  désigne la valuation  $p$ -adique de  $n$ ).

*Démonstration.* Sens direct : On écrit  $n = a^2 + b^2$  avec  $a, b \in \mathbb{Z}$ . Soit  $p \mid n$  tel que  $p \equiv 3 \pmod{4}$ . Montrons que  $p \notin \Sigma$ . On suppose par l'absurde que l'on peut écrire  $p = c^2 + d^2$  avec  $c, d \in \mathbb{Z}$ . On va discerner les cas :

- Si  $c \equiv \pm 1 \pmod{4}$ , alors  $c^2 \equiv 1 \pmod{4}$  (et de même pour  $d^2$ ).
- Si  $c \equiv \pm 2 \pmod{4}$ , alors  $c^2 \equiv 0 \pmod{4}$  (et de même pour  $d^2$ ).

Donc  $p = c^2 + d^2 \equiv 0, 1$  ou  $2 \pmod{4}$  : absurde. En particulier, par le Lemme 5 (en prenant la contraposée),  $p$  est irréductible dans  $\mathbb{Z}[i]$ . Comme  $\mathbb{Z}[i]$  est euclidien (cf. Lemme 4),  $p$  est un élément premier de  $\mathbb{Z}[i]$ . Mais,  $p \mid n = (a + ib)(a - ib)$ . Donc  $p \mid a + ib$  ou  $p \mid a - ib$ . Dans les deux cas, on a  $p \mid a$  et  $p \mid b$ . Ainsi,

$$\left( \frac{a}{p} \right)^2 + \left( \frac{b}{p} \right)^2 = \frac{n}{p^2}$$

donc de deux choses l'une; on a :

$$p^2 \mid n \text{ et } \frac{n}{p^2} \in \Sigma$$

Il suffit alors d'itérer le processus (en remplaçant  $n$  par  $\frac{n}{p^2}$ )  $k$  fois jusqu'à ce que  $p$  ne divise plus  $\frac{n}{p^{2k}}$ . On a alors  $n = p^{2k}u$  avec  $p \nmid u$ . D'où  $v_p(n) = 2k$ .

Réciproque : Soit  $p$  premier diviseur de  $n$  tel que  $p \equiv 3 \pmod{4}$ . Alors  $p^{v_p(n)} = \left(p^{\frac{v_p(n)}{2}}\right)^2$  est un carré, donc  $p^{v_p(n)} \in \Sigma$ .

Soit maintenant  $p$  premier tel que  $p = 2$  ou  $p \equiv 1 \pmod{4}$ . Alors en conséquence du Lemme 1 (le cas  $p = 2$  étant trivial),  $-1$  est un carré de  $\mathbb{F}_p$  ie.  $\exists a \in \mathbb{Z}$  tel que  $-1 \equiv a^2 \pmod{p}$ . Donc  $p \mid a^2 + 1 = (a - i)(a + i)$ . Oui mais,  $p$  ne divise ni  $a - i$ , ni  $a + i$ . Donc  $p$  n'est pas un élément premier de  $\mathbb{Z}[i]$  et n'est donc pas irréductible dans  $\mathbb{Z}[i]$  (toujours parce que  $\mathbb{Z}[i]$  est euclidien, cf. Lemme 4). En vertu du Lemme 5,  $p \in \Sigma$ .

Comme  $N$  est multiplicative, par la Remarque 3, on en déduit que  $\Sigma$  est stable par multiplication. Donc  $n \in \Sigma$  (en décomposant  $n$  en produit de facteurs premiers).  $\square$

*Remarque 7.* Le fait qu'un élément irréductible d'un anneau euclidien est premier est une conséquence directe du lemme d'Euclide, vrai dans les anneaux factoriels (donc à fortiori aussi dans les anneaux euclidiens).

[PER]  
p. 48

# Bibliographie

## **L'oral à l'agrégation de mathématiques**

**[I-P]**

Lucas ISENMANN et Timothée PECATTE. *L'oral à l'agrégation de mathématiques. Une sélection de développements*. 2<sup>e</sup> éd. Ellipses, 26 mars 2024.

<https://www.editions-ellipses.fr/accueil/15218-28346-loral-a-lagregation-de-mathematiques-une-selection-de-developpements-2e-edition-9782340086487.html>.

## **Cours d'algèbre**

**[PER]**

Daniel PERRIN. *Cours d'algèbre. pour l'agrégation*. Ellipses, 15 fév. 1996.

<https://www.editions-ellipses.fr/accueil/7778-18110-cours-d-algebre-agregation-9782729855529.html>.