

Thm (des deux carrés de FERMAT): Posons $\Sigma = \{n \in \mathbb{N}_{\geq 2} \mid \exists (a,b) \in \mathbb{N}^2 : n = a^2 + b^2\}$, notons $\mathcal{P}$ l'ensemble des nombres premiers.
 $n \in \Sigma \Leftrightarrow (\forall p \in \mathcal{P}, p \equiv 3 \pmod{4} \Rightarrow 2 \mid v_p(n))$

Heuristique de la preuve:

1. On commence par le cas p premier: $p \in \Sigma \Leftrightarrow p \not\equiv 3 \pmod{4}$

a. On montre que $\mathbb{Z}[i]$ est principal en montrant qu'il est euclidien.

b. On montre les équivalences:

$p \in \Sigma \Leftrightarrow p$ réductible dans $\mathbb{Z}[i]$
 $\Updownarrow \leftarrow$ factoriabilité de $\mathbb{Z}[i]$
 p non premier dans $\mathbb{Z}[i]$

$X^2 + 1$ réductible dans $\mathbb{F}_p[X] \Leftrightarrow -1$ n'est pas un carré modulo p
 $\Updownarrow \leftarrow$ factoriabilité de $\mathbb{F}_p[X]$
 $X^2 + 1$ non premier dans $\mathbb{F}_p[X]$

$p \not\equiv 3 \pmod{4}$

$\mathbb{Z}[i]_{\langle p \rangle}$ non intègre $\Leftrightarrow \mathbb{F}_p[X]_{\langle X^2+1 \rangle}$ non intègre

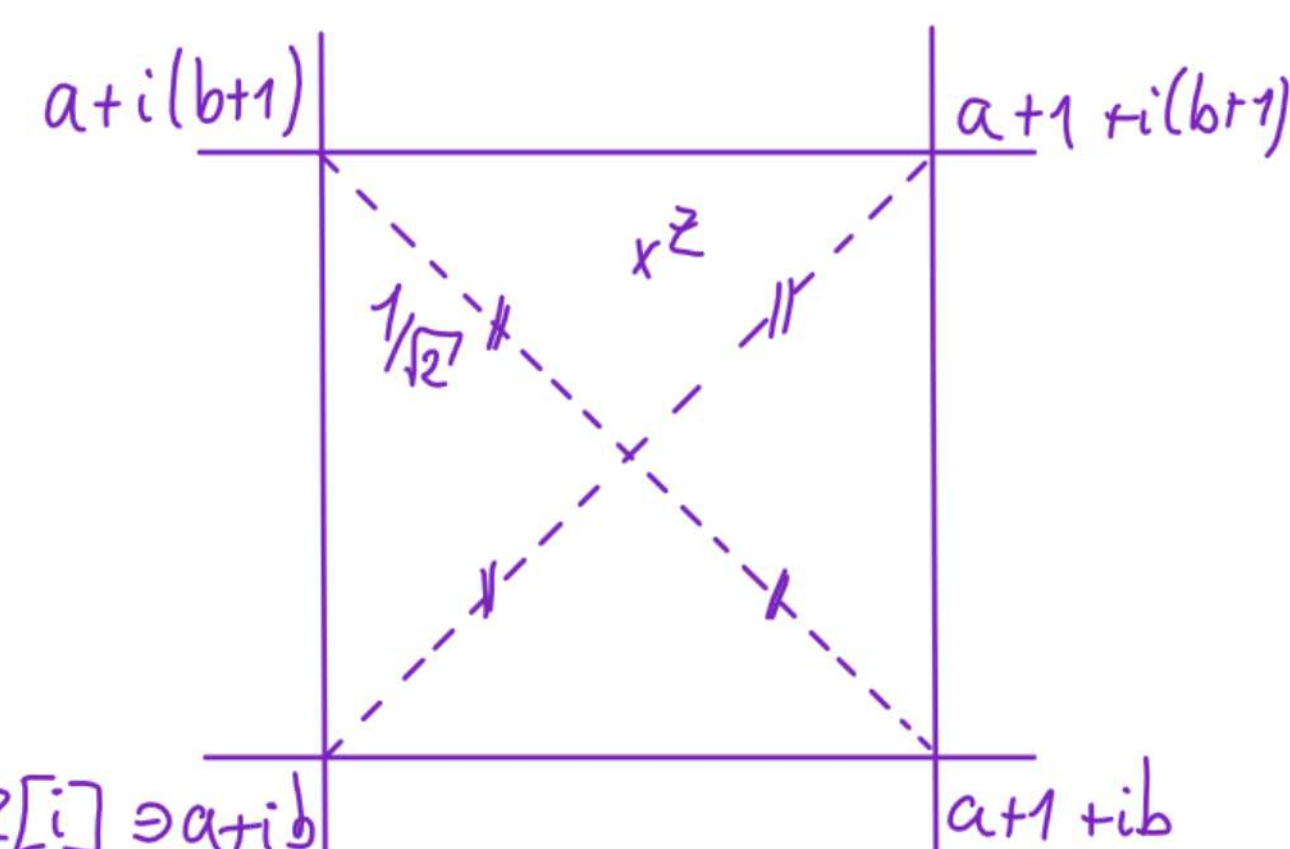
2. On se ramène au cas général

1. a. NB: $\mathbb{Z}[i] = \mathbb{Z} + i\mathbb{Z} = \text{eval}_i(\mathbb{Z}[X]) \simeq \frac{\mathbb{Z}[X]}{\langle X^2+1 \rangle}$

• Montrons que $\mathbb{Z}[i]^\times = \{\pm 1, \pm i\}$: l'inclusion réciproque est immédiate. Soit $z \in \mathbb{Z}[i]$. Alors $1 = |z z^{-1}|^2 = |z|^2 |z^{-1}|^2$, mais $(|z|^2, |z^{-1}|^2) \in \mathbb{N}^2$ donc $|z|^2 = |z^{-1}|^2 = 1$, donc en écrivant $z = a + ib$, on a $(a,b) \in \{(1,0), (0,1)\}$, i.e. $(a,b) \in \{(1,0), (-1,0), (0,1), (0,-1)\}$, i.e. $z \in \{\pm 1, \pm i\}$.

• Montrons que $\mathbb{Z}[i]$ est euclidien pour $|\cdot|^2$:

▷ Soit $z \in \mathbb{C}$. Il existe $q \in \mathbb{Z}[i]$ tel que $|z - q|^2 < \frac{1}{2}$, d'après le dessin ci-contre. (NB: $a = \lfloor \text{Re}(z) \rfloor$, $b = \lfloor \text{Im}(z) \rfloor$. Comme $a \leq \text{Re}(z) < a+1$, on a $|a - \text{Re}(z)| \leq \frac{1}{2}$ ou $|(a+1) - \text{Re}(z)| \leq \frac{1}{2}$. De même avec $\text{Im}(z)$).



▷ Soient $z_1 \in \mathbb{Z}[i]$ et $z_2 \in \mathbb{Z}[i] \setminus \{0\}$. Il existe $q \in \mathbb{Z}[i]$ tel que $|\frac{z_1}{z_2} - q|^2 < \frac{1}{2}$ d'après le point précédent. Posons $r = z_1 - z_2 q \in \mathbb{Z}[i]$. On a $|r|^2 = |z_1 - q z_2|^2 = |\frac{z_1}{z_2} - q|^2 |z_2|^2 < \frac{1}{2} |z_2|^2 < |z_2|^2$, CQFD.

• Montrons que $p \in \Sigma \Leftrightarrow p$ réductible dans $\mathbb{Z}[i]$:

▷ Supposons que $p \in \Sigma$. Il existe $(a,b) \in \mathbb{N}^2$ tel que $p = a^2 + b^2$. Comme p est premier dans $\mathbb{Z}$, p n'est pas un carré, donc $ab \neq 0$, donc $a \pm ib \notin \mathbb{Z}[i]^\times$, et $p = a^2 + b^2 = (a+ib)(a-ib)$ est une factorisation non triviale de p dans $\mathbb{Z}[i]$.

▷ Supposons que $p = z z'$ avec $(z, z') \in (\mathbb{Z}[i] \setminus \mathbb{Z}[i]^\times)^2$. Alors $p^2 = |z|^2 |z'|^2$, mais $|z|^2 \in \mathbb{N}$ et $|z|^2 \neq 1$ car $z \notin \mathbb{Z}[i]^\times$, de même pour $|z'|^2$, donc $|z|^2 = |z'|^2 = p$ car p est premier. Or $|z|^2 \in \Sigma$, donc $p \in \Sigma$.

• Montrons que p est premier dans $\mathbb{Z}[i] \Leftrightarrow -1$ n'est pas un carré modulo p :

Comme $\mathbb{Z}[i]$ est euclidien, il est principal, a fortiori factoriel, donc:

p est irréductible dans $\mathbb{Z}[i] \Leftrightarrow p$ premier dans $\mathbb{Z}[i] \Leftrightarrow \frac{\mathbb{Z}[i]}{\langle p \rangle}$ intègre.

Or $\frac{\mathbb{Z}[i]}{\langle p \rangle} \simeq \frac{\mathbb{Z}[X]}{\langle p, X^2+1 \rangle} \simeq \frac{(\mathbb{Z}/p\mathbb{Z})[X]}{\langle X^2+1 \rangle} \simeq \frac{\mathbb{F}_p[X]}{\langle X^2+1 \rangle}$, donc:

$$\frac{\mathbb{Z}[i]}{\langle p \rangle} \text{ int\`egre} \Leftrightarrow \frac{\mathbb{F}_p[X]}{\langle X^2+1 \rangle} \text{ int\`egre} \Leftrightarrow X^2+1 \text{ premier dans } \mathbb{F}_p[X]$$

EXPLIQUER
À L'ORAL
AVEC L'HÉURISTIQUE

$\Leftrightarrow X^2+1$ irr\'eductible dans $\mathbb{F}_p[X]$ (par factorialit\'e de $\mathbb{F}_p[X]$)
 $\Leftrightarrow X^2+1$ n'a pas de racine dans $\mathbb{F}_p[X]$ (car de degr\'e 2 sur un corps)
 $\Leftrightarrow -1$ n'est pas un carr\'e modulo p

À PASSER

• Montrons que -1 est un carr\'e modulo $p \Leftrightarrow p \equiv 1 [4]$:

▷ Crit\`ere d'EULER: Supposons $p \geq 3$. Montrons que $\forall \bar{x} \in \mathbb{F}_p^\times$, $\bar{x}$ est un carr\'e $\Leftrightarrow \bar{x}^{\frac{p-1}{2}} = \bar{1}$:

Posons $c: \bar{x} \in \mathbb{F}_p^\times \mapsto \bar{x}^2$ et $l: \bar{x} \in \mathbb{F}_p^\times \mapsto \bar{x}^{\frac{p-1}{2}}$. Ce sont des morphismes de groupe, donc $p-1 = \#\mathbb{F}_p^\times = \#\text{Ker}(c) \# \text{Im}(c) = \#\text{Ker}(l) \# \text{Im}(l)$. D'apr\`es le th\'eor\`eme de LAGRANGE, $c \circ l = l \circ c = \bar{1}$, donc $\text{Im}(c) \subseteq \text{Ker}(l)$ et $\text{Im}(l) \subseteq \text{Ker}(c)$. Comme $\forall \bar{x} \in \text{Ker}(c)$, $\bar{0} = \bar{x}^2 - \bar{1} = (\bar{x}-1)(\bar{x}+1)$ donc $\bar{x} = \pm 1$ par int\'egrit\'e. De l\`a, $\#\text{Im}(l) \leq \#\text{Ker}(c) \leq 2$ donc $\#\text{Ker}(l) \geq \frac{p-1}{2}$. Or $\text{Ker}(l) \subseteq \mathbb{Z}(X^{\frac{p-1}{2}} - \bar{1})$ donc $\#\text{Ker}(l) \leq \#\mathbb{Z}(X^{\frac{p-1}{2}} - \bar{1}) \leq \frac{p-1}{2}$, donc $\#\text{Ker}(l) = \frac{p-1}{2}$, puis $\text{Ker}(l) = \text{Im}(c)$ par cardinalit\'e, i.e. $\bar{x}$ est un carr\'e $\Leftrightarrow \bar{x} \in \text{Im}(c) \Leftrightarrow \bar{x} \in \text{Ker}(l) \Leftrightarrow \bar{x}^{\frac{p-1}{2}} = \bar{1}$.

▷ Si $p=2$, alors $-1 \equiv 1 [p]$ est un carr\'e modulo p .

▷ Supposons $p \geq 3$. D'apr\`es le crit\`ere d'EULER:

$$-1 \text{ est un carr\'e modulo } p \Leftrightarrow (-1)^{\frac{p-1}{2}} = 1 \Leftrightarrow \frac{p-1}{2} \text{ est pair} \Leftrightarrow p \equiv 1 [4].$$

2. • Montrons que Σ est stable par produit: remarquons que $n \in \Sigma \Leftrightarrow \exists z \in \mathbb{Z}[i]: n = |z|^2$. Il suffit alors de remarquer que $\forall (z, z') \in \mathbb{Z}[i]$, $zz' \in \mathbb{Z}[i]$ et $|z|^2 \cdot |z'|^2 = |zz'|^2$.

• Soit $n \in \mathbb{N}_{\geq 2}$, \\'ecrivons $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r} q_1^{\beta_1} \cdots q_s^{\beta_s}$ sa d\'ecomposition en produit de facteurs premiers de n , o\`u  $p_1, \dots, p_r$  sont les facteurs premiers de  $n$  congrus \`a $3 \bmod 4$.

▷ Supposons que $\forall p \in \mathcal{P}$, $p \equiv 3 [4] \Rightarrow 2 \nmid v_p(n)$, i.e. $\alpha_1, \dots, \alpha_r$ sont pairs. D'apr\`es le th\'eor\`eme dans le cas premier, $q_1, \dots, q_s$ sont sommes de deux carr\'es. Comme $\forall i \in [1, r]$, $p_i^{\alpha_i} = (p_i^{\alpha_i/2})^2 + 0^2 \in \Sigma$, on a bien $n \in \Sigma$ en vertu du point pr\'ec\'edent.

▷ Soit $p \in \mathcal{P}$ tel que $p \equiv 3 [4]$. Montrons par r\'ecurrence: $\forall n \in \Sigma$, $\mathcal{H}_n: "2 \nmid v_p(n)"$

▷ $\min \Sigma = 2 = 1^2 + 1^2$, et $2 \nmid v_p(2) = 0$ car $p \equiv 3 [4]$ donc $p \neq 2$.

▷ Soit $n \in \Sigma$, supposons que $\forall k < n$, $k \in \Sigma \Rightarrow 2 \nmid v_p(k)$. Si $v_p(n) = 0$, alors $2 \nmid v_p(n) = 0$. Sinon, $p \mid n$, mais $n \in \Sigma$ donc il existe $(a, b) \in \mathbb{N}^2$ tel que $n = a^2 + b^2 = (a+ib)(a-ib)$. D'apr\`es l'\\'etude pr\'ec\'edente, p est premier dans $\mathbb{Z}[i]$, donc $p \mid a+ib$ ou $p \mid a-ib$, mais p, a et b sont entiers, donc $p \mid a$ et $p \mid b$, donc $p^2 \mid n$, mais $v_p(\frac{n}{p^2}) = v_p(n) - 2$. Comme $\frac{n}{p^2} \in \Sigma$ et $\frac{n}{p^2} < n$, par hypoth\`ese de r\'ecurrence, $2 \nmid v_p(\frac{n}{p^2})$, donc $2 \nmid v_p(n)$.