Perrin p56
Rombaldi p269

THÉORÈME DES DEUX CARRÉS DE FERMAT

121, 126

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.

$$n \in \Sigma \iff \left(\forall p \in \mathcal{P},\ p \equiv 3\ [4] \Rightarrow 2 \mid v_p(n)\right)$$

ÉCRIRE AU TABLEAU

Heuristique de la preuve :

1▸ On commence par le cas p premier : $p \in \Sigma \iff p \not\equiv 3\ [4]$

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

b▸ On montre les équivalences :

$p \in \Sigma \iff p$ réductible dans $\mathbb{Z}[i]$

$\Updownarrow$ ← factorialité de $\mathbb{Z}[i]$

p non premier dans $\mathbb{Z}[i]$

$\Updownarrow$

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

$\Updownarrow$

X^2+1 non premier dans $\mathbb{F}_p[X]$

$\Updownarrow$ ← factorialité de $\mathbb{F}_p[X]$

X^2+1 réductible dans $\mathbb{F}_p[X]$ $\iff$ -1 n'est pas un carré modulo p

$\Updownarrow$

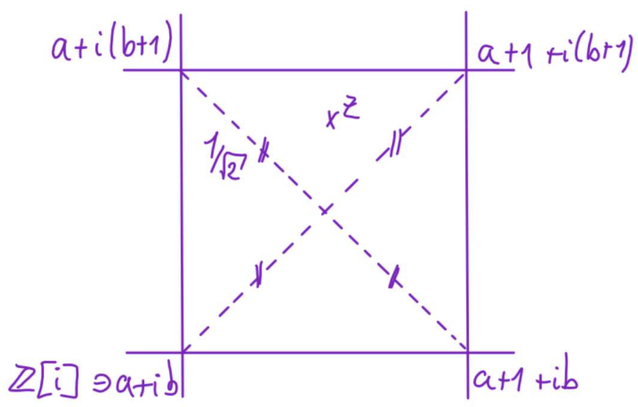
$p \not\equiv 3\ [4]$

2▸ On se ramène au cas général

PAS PLUS QUE 1 MIN (VOIRE PASSER)

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

- Montrons que $\mathbb{Z}[i]^\times = \{\pm 1, \pm i\}$: l'inclusion réciproque est immédiate. Soit $z \in \mathbb{Z}[i]$. Alors $1 = |z z^{-1}|^2 = |z|^2 \cdot |z^{-1}|^2$, mais $(|z|^2, |z^{-1}|^2) \in \mathbb{N}^2$ donc $|z|^2 = |z^{-1}|^2 = 1$, donc en écrivant $z = a + ib^2$, on a $(a^2, b^2) \in \{(1,0),(0,1)\}$, 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 : $a = \lfloor \mathrm{Re}(z) \rfloor$, $b = \lfloor \mathrm{Im}(z) \rfloor$. Comme $a \leq \mathrm{Re}(z) < a+1$, on a $|a - \mathrm{Re}(z)| \leq \frac{1}{2}$ ou $|(a+1) - \mathrm{Re}(z)| \leqslant \frac{1}{2}$. De même avec $\mathrm{Im}(z)$).



  - 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 $\left|\frac{z_1}{z_2} - q\right|^2 < \frac{1}{2}$ d'après le point précédent. Posons $r = z_1 - z_2 q \in \mathbb{Z}[i]$. On a $|r|^2 = |z_1 - q z_2|^2 = \left|\frac{z_1}{z_2} - q\right|^2 |z_2|^2 < \frac{1}{2}|z_2|^2 < |z_2|^2$, CQFD.
- Montrons que $p \in \Sigma \iff p$ 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 $p = zz'$ avec $(z,z') \in (\mathbb{Z}[i] \setminus \mathbb{Z}[i]^\times)^2$. Alors $p^2 = |z|^2 \cdot |z'|^2$, mais $|z|^2 \in \mathbb{N}$ et $|z|^2 \neq 1$ car $z \notin \mathbb{Z}[i]^2$, 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 $\mathbb{Z}[i] \iff -1$ n'est pas un carré modulo p :

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

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

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 :

$\frac{\mathbb{Z}[i]}{\langle p\rangle}$ intègre $\iff$ $\frac{\mathbb{F}_p[X]}{\langle X^2+1\rangle}$ intègre $\iff$ X^2+1 premier dans $\mathbb{F}_p[X]$

EXPLIQUER À L'ORAL AVEC L'HEURISTIQUE

$\iff$ X^2+1 irréductible dans $\mathbb{F}_p[X]$ (par factorialité de $\mathbb{F}_p[X]$)

$\iff$ X^2+1 n'a pas de racine dans $\mathbb{F}_p[X]$ (car de degré 2 sur un corps)

$\iff$ -1 n'est pas un carré modulo p

À PASSER

- Montrons que -1 est un carré modulo p $\iff$ $p\equiv 1\ [4]$:
  - ▸ Critère d'EULER : Supposons $p\geq 3$. Montrons que $\forall \bar{x}\in\mathbb{F}_p^\times$, $\bar{x}$ est un carré $\iff$ $\bar{x}^{\frac{p-1}{2}}=\bar{1}$:
    Posons $c:\bar{x}\in\mathbb{F}_p^\times\mapsto\bar{x}^2$ et $\ell:\bar{x}\in\mathbb{F}_p^\times\mapsto\bar{x}^{\frac{p-1}{2}}$. Ce sont des morphismes de groupe, donc $p-1=\#\mathbb{F}_q^\times$ $=\#\ker(c)\,\#\mathrm{Im}(c)=\#\ker(\ell)\,\#\mathrm{Im}(\ell)$. D'après le théorème de LAGRANGE, $\varphi\circ\ell=\ell\circ\varphi\equiv\bar{1}$, donc $\mathrm{Im}(c)$ $\subseteq\ker(\ell)$ et $\mathrm{Im}(\ell)\subseteq\ker(c)$. Comme $\forall\bar{x}\in\ker(c)$, $\bar{0}=\bar{x}^2-\bar{1}=(\bar{x}-1)(\bar{x}+1)$ donc $\bar{x}=\pm 1$ par intégrité. De là, $\#\mathrm{Im}(\ell)\leq\#\ker(c)\leq 2$ donc $\#\ker(\ell)\geq\frac{p-1}{2}$. Or $\ker(\ell)\subseteq Z(X^{\frac{p-1}{2}}-\bar{1})$ donc $\#\ker(\ell)\leq\#Z(X^{\frac{p-1}{2}}-\bar{1})\leq\frac{p-1}{2}$, donc $\#\ker(\ell)=\frac{p-1}{2}$, puis $\ker(\ell)=\mathrm{Im}(c)$ par cardinalité, i.e. $\bar{x}$ est un carré $\iff\bar{x}\in\mathrm{Im}(c)\iff\bar{x}\in\ker(\ell)$ $\iff\bar{x}^{\frac{p-1}{2}}=\bar{1}$.
  - ▸ Si $p=2$, alors $-1\equiv 1\ [p]$ est un carré modulo p.
  - ▸ Supposons $p\geq 3$. D'après le critère d'EULER :

$$-1 \text{ est un carré modulo } p \iff (-1)^{\frac{p-1}{2}}=1 \iff \frac{p-1}{2} \text{ est pair} \iff p\equiv 1\ [4].$$

2▸
- Montrons que Σ est stable par produit : remarquons que $n\in\Sigma\iff\exists z\in\mathbb{Z}[i]:n=|z|^2$. 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 $n\in\mathbb{N}_{\geq 2}$, écrivons $n=p_1^{\alpha_1}\cdots p_r^{\alpha_r}q_1^{\beta_1}\cdots q_s^{\beta_s}$ sa décomposition en produit de facteurs premiers de n, où $p_1,\dots,p_r$ sont les facteurs premiers de n congrus à 3 mod 4.
  - ▸ Supposons que $\forall p\in\mathcal{P}$, $p\equiv 3\ [4]\Rightarrow 2\mid v_p(n)$, i.e. $\alpha_1,\dots,\alpha_r$ sont pairs. D'après le théorème dans le cas premier, $q_1,\dots,q_s$ sont sommes de deux carrés. 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 précédent.
  - ▸ Soit $p\in\mathcal{P}$ tel que $p\equiv 3\ [4]$. Montrons par récurrence : $\forall n\in\Sigma$, $\mathcal{H}_n$: " $2\mid v_p(n)$ "
    - ▸ $\min\Sigma=2=1^2+1^2$, et $2\mid v_p(2)=0$ car $p\equiv 3\ [4]$ donc $p\neq 2$.
    - ▸ Soit $n\in\Sigma$, supposons que $\forall k<n$, $k\in\Sigma\Rightarrow 2\mid v_p(k)$. Si $v_p(n)=0$, alors $2\mid v_p(n)=0$. 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'après l'étude précédente, 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 $v_p\left(\frac{n}{p^2}\right)=v_p(n)-2$. Comme $\frac{n}{p^2}\in\Sigma$ et $\frac{n}{p^2}<n$, par hypothèse de récurrence, $2\mid v_p\left(\frac{n}{p^2}\right)$, donc $2\mid v_p(n)$.