Théorème des deux carrés (121, 122, 127)

Perrin p. 56-57 et 75.

Notation : $\mathbb{Z}[i] := \{a+ib,\ a,b \in \mathbb{Z}\}$ et $\Sigma := \{n \in \mathbb{N} \mid \exists a,b \in \mathbb{Z},\ n = a^2+b^2\}$ et $N : z \longmapsto |z|^2$

Lem 1 : $\mathbb{Z}[i]^\times = \{\pm 1, \pm i\}$.

démo : Soit $z \in \mathbb{Z}[i]^\times$ alors il existe $z' \in \mathbb{Z}[i]$ tel que $zz' = 1$. L'application N est multiplicative donc : $N(zz') = 1 \Rightarrow N(z).N(z') = 1 \Rightarrow N(z) = N(z') = 1$ car $N(z) \in \mathbb{N}$.

Donc $z \in \{\pm 1, \pm i\}$. Ainsi $\mathbb{Z}[i]^\times = \{\pm 1, \pm i\}$.

Lem 2 : $\mathbb{Z}[i]$ est euclidien pour le stathme N.

demo :
- $\mathbb{Z}[i]$ est intègre car inclus dans $\mathbb{C}$.
- Soit $z, t \in \mathbb{Z}[i] \setminus \{0\}$. On a $\frac{z}{t} \in \mathbb{C}$ donc $\frac{z}{t} = x+iy$ alors il existe un unique couple $(a,b) \in \mathbb{N}^2$ tel que

$$a - \frac{1}{2} < x \leq a + \frac{1}{2} \quad \text{et} \quad b - \frac{1}{2} < y \leq b + \frac{1}{2}$$

On pose $q = a+ib$ et $r = z - qt$. Alors $r \in \mathbb{Z}[i]$ et $r = t\left(\frac{z}{t} - q\right)$

Or on a

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

Ainsi $N(r) < N(t)$.

D'où $\mathbb{Z}[i]$ est euclidien

Lem 3 Soit p premier. $p \in \Sigma$ ssi p est réductible dans $\mathbb{Z}[i]$.

démo :

$\Rightarrow$) Si $p \in \Sigma$, on a $p = (a+ib)(a-ib)$ avec a,b non nuls donc $a+ib$ et $a-ib \notin \mathbb{Z}[i]^\times$. D'où p est réductible dans $\mathbb{Z}[i]$.

$\Leftarrow$) Si $p = zz'$ avec $z, z' \in \mathbb{Z}[i] \setminus \mathbb{Z}[i]^\times$. On a $N(p) = N(z)N(z') = p^2$ et comme $N(z)$ et $N(z') \neq 1$ on a nécessairement $p = N(z)$. D'où $p \in \Sigma$.

thm 4 : Soit $p \in \mathbb{N}$ un nombre premier. On a l'équivalence :

$$p \in \Sigma \text{ ssi } p = 2 \text{ ou } p \equiv 1 [\text{mod } 4].$$

démo :

* Mq $p \in \Sigma$ ssi -1 est un carré dans $\mathbb{F}_p^*$.

Par le lemme 2, $\mathbb{Z}[i]$ est principal donc p irréductible dans $\mathbb{Z}[i]$ ssi $\mathbb{Z}[i]/(p)$ est intègre.

On pose $\varphi : \mathbb{Z}[X] \longrightarrow \mathbb{Z}[i]$. Par le 1er thm d'isomorphisme on a $\mathbb{Z}[X]/(X^2+1) \simeq \mathbb{Z}[i]$
$\qquad Q \longmapsto Q(i)$

Donc $\mathbb{F}_p[X]/(X^2+1) \simeq \left(\mathbb{Z}[X]/(p)\right)/(X^2+1) \simeq \left(\mathbb{Z}[X]/(X^2+1)\right)/(p) \simeq \mathbb{Z}[i]/(p)$

Donc $p \in \Sigma$ ssi $\mathbb{F}_p[X]/(X^2+1)$ est non intègre

ssi X^2+1 est réductible dans $\mathbb{F}_p[X]$

ssi -1 est un carré dans $\mathbb{F}_p^*$.

On applique ce critère :

* Si $p = 2$ alors $-1 = 1 = 1^2$ donc -1 est un carré dans $\mathbb{F}_p^*$.
* Si $p > 2$ alors -1 est un carré dans $\mathbb{F}_p^*$ $\underset{\text{lemme 5}}{\text{ssi}}$ $(-1)^{\frac{p-1}{2}} = 1$

ssi $\frac{p-1}{2}$ est pair

ssi $p \equiv 1 [\text{mod } 4]$.

lem 5 Soit p un nombre premier impair, -1 est un carré dans $\mathbb{F}_p$ ssi $(-1)^{\frac{p-1}{2}} = 1$.

démo : Posons $X = \{x \in \mathbb{F}_p,\ x^{\frac{p-1}{2}} = 1\}$. On a $|X| \leq \frac{p-1}{2}$ par intégrité de $\mathbb{F}_p$.

De plus $\varphi : \mathbb{F}_p^* \longrightarrow \mathbb{F}_p^*$ est un mdg. Par le 1er thm d'isomorphisme on a
$\qquad x \longmapsto x^2$

$\mathbb{F}_p^*/\mathrm{Ker}\varphi \simeq \mathbb{F}_p^{*2}$ et $\mathrm{Ker}\varphi = \{\pm 1\}$.

Donc $|\mathbb{F}_p^{*2}| = \frac{p-1}{2}$.

De plus $\mathbb{F}_p^{*2} \subset X$ car $x \in \mathbb{F}_p^{*2}$ on a $\exists a \in \mathbb{F}_p^*$ tq $x = a^2$, $x^{\frac{p-1}{2}} = a^{p-1} = 1$ donc $x \in X$.

Ainsi $\mathbb{F}_p^{*2} = X$ par égalité des cardinaux.

Questions : théorème des deux carrés

- $\{\pm 1, \pm i\} \subset \mathbb{Z}[i]^\times$?

  $(-1)(-1) = 1$, $1 \cdot 1 = 1$, $i(-i) = 1$

- $(a,b) \in \mathbb{N}^2$ unique couple ?

  Si on prend $\lfloor x \rceil = a$ et $\lfloor y \rceil = b$ alors (a,b) est unique tel que

  $$a - \frac{1}{2} < x \leq a + \frac{1}{2} \quad \text{et} \quad b - \frac{1}{2} < y \leq b + \frac{1}{2}.$$

- $$\left(\mathbb{Z}[X]/(p)\right)/(X^2+1) \simeq \left(\mathbb{Z}[X]/(X^2+1)\right)/(p).$$

On considère $\varphi : \begin{array}{ccc} \mathbb{Z}[X] & \longrightarrow & \left(\mathbb{Z}[X]/(X^2+1)\right)/(p) \\ Q & \longmapsto & \overline{\overline{Q(X)}^{X^2+1}}^{p} \end{array}$. φ est un morphisme d'anneaux

- φ est surjectif : composée de projections canoniques qui sont surjectives
- $\operatorname{Ker}\varphi = (p, X^2+1)$ (car (p) et (X^2+1) sont étrangers) :

  * On a $(p, X^2+1) \subset \operatorname{Ker}\varphi$.
  * Soit $P \in \operatorname{Ker}\varphi$, alors $\overline{P} \in (p)$ donc $\exists\, \overline{Q(X)} \in \mathbb{Z}[i]/(X^2+1)$ tq $\overline{P(X)} = p\,\overline{Q(X)}$

  Or $\overline{Q(X)} \in \mathbb{Z}[i]/(X^2+1)$ donc $\overline{Q(X)} = Q(X) + (X^2+1)\mathbb{Z}[X]$.

  D'où $\overline{P(X)} = p\left(Q(X) + (X^2+1)\mathbb{Z}[X]\right)$

  Ainsi $P \in (p, X^2+1)$.

D'où $\operatorname{Ker}\varphi = (p, X^2+1)$

On conclut par le 1er thm d'isomorphisme, en faisant de même en échangeant (X^2+1) et (p), on arrive à mq

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

- $\mathbb{F}_p[X] / (X^2+1)$ est non intègre ssi X^2+1 est réductible dans $\mathbb{F}_p[X]$.

  Comme $\mathbb{F}_p$ est un corps, on a $\mathbb{F}_p[X]$ est principal.

  Donc X^2+1 est irréductible sur $\mathbb{F}_p[X]$ ssi (X^2+1) est un idéal premier de $\mathbb{F}_p[X]$.

- X^2+1 réductible dans $\mathbb{F}_p[X]$ ssi -1 est un carré dans $\mathbb{F}_p^*$.

  Un polynôme de degré 2 est réductible dans un corps ssi il admet des racines.

  aX^2+bX+c avec $a \neq 0$ alors $X^2+b'X+c'$.

  si il est réductible alors $\exists P,Q$ tq $X^2+b'X+c' = P(X).Q(X)$. avec $\deg P + \deg Q = 2$.

  mais $\deg P$ et $\deg Q \geq 1$. Donc $\deg P = \deg Q = 1$

  D'où $X^2+b'X+c'$ a des racines.

  $\hookrightarrow$ Soit $a \in \mathbb{F}_p$ une racine alors $a^2+1=0 \Leftrightarrow a^2=-1$.