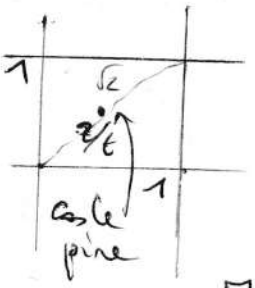
Théorème des deux carrés

Perrin.

Lm 1 : $\mathbb{Z}[i] = \{a+ib,\ a,b\in\mathbb{Z}\}$ est euclidien muni de $N : a+ib \mapsto a^2+b^2$.

Dem : Soit $z\in\mathbb{Z}[i]$ et $t\in\mathbb{Z}[i]\setminus\{0\}$. Notons $\frac{z}{t} = x+iy$ $x,y\in\mathbb{R}$.
On choisit a et b les entiers les plus proches de x et de y ($|x-a|\le\frac12$, $|y-b|\le\frac12$).
Posons $q = a+ib$, on a : $\left|\frac{z}{t} - q\right| \le \frac{\sqrt{2}}{2} < 1$.



Si on pose $r = z - qt$ on a :
$N(r) = N\left(\frac{z}{t} - q\right) N(t) \le \frac{1}{4} N(t) < N(t)$ □

Lm 2 : $\mathbb{Z}[i]^\times = \{\pm 1, \pm i\}$

Dem : $\{\pm1,\pm i\} \subset \mathbb{Z}[i]^\times$ ok.
Soit $z\in\mathbb{Z}[i]^\times$ alors $zz^{-1} = 1 \overset{N}{\Rightarrow} \underbrace{N(z)}_{\in\mathbb{N}}\underbrace{N(z^{-1})}_{\in\mathbb{N}} = N(1) = 1$
Donc $N(z)\in\mathbb{N}^\times$ i.e. $N(z)=1$.
Soit $a^2+b^2 = 1$ (pour $t = a+ib$) i.e. $\begin{cases} a = \pm 1 \\ b = 0 \end{cases}$ ou $\begin{cases} a = 0 \\ b = \pm 1 \end{cases}$.
Donc $t\in\{\pm1,\pm i\}$. □

Lm 3 : Notons $\sum = \{m\in\mathbb{N},\ \exists a,b\in\mathbb{N},\ m = a^2+b^2\}$.
Soit $p\in\mathbb{P}$, $p\ge 3$: $p\in\sum$ ssi p est réductible dans $\mathbb{Z}[i]$.

Dem : Si $p = a^2+b^2 = (a+ib)(a-ib)$ alors p est réductible dans $\mathbb{Z}[i]$.
car si $a+ib\in\mathbb{Z}[i]^\times$ ou si $a-ib\in\mathbb{Z}[i]^\times$ car $p = a^2+b^2 \Rightarrow a\neq 0$ et $b\neq 0$.
Si $p = zz'$ avec $z,z'\notin\mathbb{Z}[i]^\times$ alors $N(p) = p^2 = N(z)N(z')$ et puisque $p\in\mathbb{P}$
$N(z)\in\{1,p,p^2\}$. On $z\notin\mathbb{Z}[i]^\times \Rightarrow N(z)\neq 1$. De même $N(z')\neq 1$.
Nécessairement $N(z) = N(z') = p$. Alors $p = a^2+b^2$ où $z = a+ib$. □

Lm 4 : $x\in\mathbb{F}_p^2$ ssi $x^{\frac{p-1}{2}} = 1$.

Dem : Notons $X = \{x\in\mathbb{F}_p,\ x^{\frac{p-1}{2}} = 1\}$. Déjà $|X| \le \frac{p-1}{2}$ car $X^{\frac{p-1}{2}} - 1$ a au plus $\frac{p-1}{2}$ racines.
Si $x\in\mathbb{F}_p^2$, $x\neq 0$ alors $x^{\frac{p-1}{2}} = (y^2)^{\frac{p-1}{2}} = y^{p-1} = 1$ (Lagrange) i.e. $x\in X$.
$\varphi : \mathbb{F}_p^\times \to \mathbb{F}_p^2\setminus\{0\}$, $x\mapsto x^2$ a pour noyau ± 1 (intégrité). $= |\mathbb{F}_p^2\setminus\{0\}|$
Donc $|\mathrm{Im}\,\varphi| = |\mathbb{F}_p^2\setminus\{0\}| = \frac{|\mathbb{F}_p^\times|}{2} = \frac{p-1}{2}$. Et $\mathrm{Im}\,\varphi\subset X$ donc $\frac{p-1}{2} = |\mathrm{Im}\,\varphi| \le |X| \le \frac{p-1}{2}$
Donc $X = \mathbb{F}_p^2\setminus\{0\}$ par inclusion et cardinalité. □

Théorème 5 : Soit $p \in \mathbb{P}$, $p \geq 3$. $p \in \sum$ ssi $p \equiv 1 [4]$.

Dem : D'après Lem 1, $\mathbb{Z}[i]$ est euclidien donc principal donc factoriel.

Donc p irréductible dans $\mathbb{Z}[i]$ ssi $\langle p \rangle = p\mathbb{Z}[i]$ est premier

ie $p \in \sum$ ssi $\mathbb{Z}[i]/\langle p \rangle$ est non intègre (Lem 3)

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

ainsi $p \in \sum$ ssi $\dfrac{\mathbb{F}_p[X]}{\langle X^2+1 \rangle}$ est non intègre ssi X^2+1 est réductible dans $\mathbb{F}_p[X]$

ssi X^2+1 a une racine dans $\mathbb{F}_p[X]$

ssi -1 est un carré modulo p

ssi $(-1)^{\frac{p-1}{2}} = 1$ (Lem 4)

ssi $\frac{p-1}{2}$ est pair ssi $p-1 = 4k$ ssi $p = 4k+1$.

ssi $p \equiv 1 [4]$.

Rq : $p = 2 \in \sum$ $(p = 1^2 + 1^2)$. Donc pour $p \in \mathbb{P}$ on a : $p \in \sum$ ssi $\begin{cases} p \equiv 1 [4] \\ \text{ou} \\ p = 2 \end{cases}$

Corollaire 6 : Si $n = \prod_{p \in \mathbb{P}} p^{v_p(n)}$ on a : $n \in \sum$ ssi $(\forall p \in \mathbb{P}, p \equiv 3 [4] \Rightarrow v_p(n) \equiv 0 [2])$

Dem : $n \in \sum$ ssi $\exists z \in \mathbb{Z}[i]$ tq $n = N(z)$. Par multiplicativité de N, on a que $\sum$ est stable par $\times$.

($\Leftarrow$) Pour montrer que $n \in \sum$, il suffit de montrer que $\forall p \in \mathbb{P}$ $p^{v_p(n)} \in \sum$

si $p \equiv 1 [4]$ c'est le Thm 5. Si $p \equiv 3 [4]$, alors $v_p(n) \equiv 0 [2]$ (hypothèse)

si $p = 2$ c'est la remarque. alors $p^{v_p(n)} = p^{2k} = (p^2)^k \equiv 3^k [4] \equiv 1 [4]$

c'est le Thm 5 ensuite.

Donc $\forall p \in \mathbb{P}$ $p^{v_p(n)} \in \sum$ donc $n \in \sum$.

($\Rightarrow$) Supposons $n = a^2 + b^2 \in \sum^*$, prenons $p \in \mathbb{P}$ tq $p \equiv 3 [4]$.

Montrons $v_p(n) \equiv 0 [2]$. Le Thm 5 et le Lem 3 montrent : $p \equiv 3 [4] \Rightarrow p \notin \sum \Rightarrow p$ irréductible dans $\mathbb{Z}[i]$ principal

si $v_p(n) = 0$ ok, sinon puisque $p \mid n = a^2 + b^2 = (a+ib)(a-ib)$

on a $p \mid a+ib$ ou $p \mid a-ib$. Par conjugaison, $p \mid 2a$ et $p \mid 2ib$.

Donc $p \mid a$ et $p \mid b$ on peut diviser par 2 (sinon $p = 2 \not\equiv 3 [4]$). Donc $p^2 \mid a^2 + b^2 = n$.

D'où $v_p\left(\frac{n}{p^2}\right) = v_p(n) - 2$ et $\frac{n}{p^2} = \left(\frac{a}{p}\right)^2 + \left(\frac{b}{p}\right)^2 \in \sum$. On montre par récurrence que $v_p(n)$ est pair.

Ainsi par HR, $v_p\left(\frac{n}{p^2}\right)$ est pair donc $v_p(n)$ aussi. $\in \sum$ et $< n$

pour $n \in \sum^*$ et $n \leq k$. (récurrence forte)

□

Rappel 1 : (Thm d'isomorphisme) A anneau, I, J deux idéaux tq $I \subset J$.
$(A/I)/(J/I) \simeq A/J$ en tant qu'anneaux.

Dem : On note $\pi : A \to A/I$ le mor. surj canonique. Puisque $I \subset J$, $\pi(J) = J/I$ et un idéal de A/I. De plus, on peut factoriser $\pi_2 : A \to A/J$ par I et obtenir le morph. surj $\varphi : A/I \to A/J$ dont le noyau est J/I et par le 1er th d'iso $(A/I)/(J/I) \simeq A/J$. □

Rappel 2 : Pour $p \in \mathbb{P}$, $(\mathbb{Z}(X)/(X^2+1))/(p) \simeq (\mathbb{Z}/p\mathbb{Z})(X)/(X^2+1)$.
$\simeq \mathbb{Z}(X)/(p, X^2+1)$
$\simeq (\mathbb{Z}(X)/\langle p \rangle)/\langle X^2+1 \rangle$

Dem : $A = \mathbb{Z}[X]$
$J = \langle p, X^2+1 \rangle$, $I = \langle X^2+1 \rangle$
$J/I \simeq \langle p \rangle$.

On a $(A/I)/(J/I) \simeq (\mathbb{Z}(X)/(X^2+1))/\langle p \rangle$
Rappel 1 $\simeq A/J \simeq \mathbb{Z}[X]/\langle p, X^2+1 \rangle$
Rappel 1 $I = \langle p \rangle$, $J = \langle X^2+1, p \rangle$
$\simeq (\mathbb{Z}(X)/\langle p \rangle)/\langle X^2+1 \rangle$. □