Théorème des 2 carrés

Perrin p57

Théorème : i) $\mathbb{Z}[i]^* = \{\pm 1, \pm i\}$

ii) $\mathbb{Z}[i]$ est euclidien relativement à $N : z = a+ib \mapsto a^2+b^2 = |z|^2$.

iii) Soit p premier, p est somme de 2 carrés $\Leftrightarrow p = 2$ ou $p \equiv 1 [4]$.

Preuve :

i) Soit $z \in \mathbb{Z}[i]^*$, alors il existe $z' \in \mathbb{Z}[i]^*$ tel que $zz' = 1$

Alors $1 = N(z)N(z') = N(zz')$ et comme $N(z), N(z') \in \mathbb{N}$, on a $N(z) = N(z') = 1$

Si $z = a+ib$, alors $N(z) = a^2+b^2 = 1 \Leftrightarrow a = \pm 1$ et $b = 0$ ou $a = 0$ et $b = \pm 1$.

On a alors $z \in \mathbb{Z}[i]^* \Leftrightarrow N(z) = 1$.

ii) Soient $z, t \in \mathbb{Z}[i] \setminus \{0\}$. Pour faire la division euclidienne de z par t, on considère $\frac{z}{t} \in \mathbb{C}$, on a donc $\frac{z}{t} = x + iy \in \mathbb{C}$

Ainsi, $\exists (a,b) \in \mathbb{Z}$ tel que $|x-a| \leq \frac{1}{2}$ et $|y-b| \leq \frac{1}{2}$. Soit $q = a+ib$ et $r = z - qt$.

Alors $r \in \mathbb{Z}[i]$ et $N(r) = |r|^2 = |z-qt|^2 = |t|^2 \left|\frac{z}{t} - q\right|^2$

	$\Leftarrow \mathbb{Z}$	$a+ib$
	$\frac{z}{t}$	$\leq \frac{1}{2}$

$= |t|^2 |(x-a)^2 - (y-b)^2| \leq \frac{|t|^2}{2} < N(t)$

Donc on a bien $z = qt + r$ avec $N(r) < N(t)$ donc $\mathbb{Z}[i]$ est euclidien donc principal.

iii) On note $\Sigma = \{n \in \mathbb{N} \mid n = a^2+b^2 \text{ où } a, b \in \mathbb{N}\}$

Soit p premier :

Lemme 1 : $p \in \Sigma \Leftrightarrow p$ n'est pas irréductible dans $\mathbb{Z}[i]$

Dem :

$\Rightarrow$ Si $p = a^2+b^2$ alors $p = (a+ib)(a-ib)$ avec $a, b \neq 0$ donc $(a+ib)$ et $(a-ib) \in \mathbb{Z}[i]^*$ car $z = a+ib$ et $\bar{z} = a-ib$ et $N(z) = z\bar{z} = a^2+b^2 = p \neq 1$

Donc p n'est pas irréductible dans $\mathbb{Z}[i]$

$\Leftarrow$ Si $p = zz'$ avec $z, z' \notin \{\pm 1, \pm i\}$, on a $N(p) = N(zz') = N(z)N(z') = p^2$ et comme $N(z) \neq 1$, $N(z') \neq 1$ et p premier.

On a $N(z) = N(z') = p = a^2+b^2$ donc $p \in \Sigma$.

Comme $\mathbb{Z}[i]$ est euclidien, donc principal donc Factoriel

$p \in \Sigma \Leftrightarrow p$ n'est pas irreductible dans $\mathbb{Z}[i] \Leftrightarrow (p) = p\mathbb{Z}[i]$ n'est pas premier $\Leftrightarrow \mathbb{Z}[i]/(p)$ pas intègre

On étudie l'isomorphisme $\mathbb{Z}[i] \simeq \mathbb{Z}[X]/(X^2+1)$

Par le Théorème d'isomorphisme, on a : $\mathbb{Z}[i]/(p) \simeq \mathbb{Z}[X]/(X^2+1,p) \simeq [\mathbb{Z}[X]/(p)]/(X^2+1) \simeq \mathbb{Z}/p\mathbb{Z}[X]/(X^2+1)$

$\mathbb{Z}[X] \to \mathbb{Z}[i] \to \mathbb{Z}[i]/(p)$ et $\mathbb{Z}[X] \to \mathbb{Z}/p\mathbb{Z}[X] \to \mathbb{Z}/p\mathbb{Z}[X]/(X^2+1)$

$f : P \longmapsto \overline{P(i)}$ $\quad \ker(f) = (X^2+1, p)$ $\quad g : P \longmapsto \overline{P}$ $\quad \ker(g) = (X^2+1, p)$

On a donc montré les équivalences : $p \in \Sigma \Leftrightarrow (p)$ pas premier

$\Leftrightarrow \mathbb{Z}[i]/(p)$ pas intègre $\Leftrightarrow \mathbb{F}_p[X]/(X^2+1)$ pas intègre

$\Leftrightarrow (X^2+1)$ pas premier

$\Leftrightarrow X^2+1$ pas irreductible dans $\mathbb{F}_p[X]$

$\Leftrightarrow -1 \in \mathbb{F}_p^{*2}$.

Lemme : $|\mathbb{F}_p^{*2}| = \frac{p-1}{2}$ et $|\mathbb{F}_p^{2}| = \frac{p+1}{2}$ pour $p > 2$.

Dem : On a $\varphi : \mathbb{F}_p^* \longrightarrow \mathbb{F}_p^{*2}$, $x \longmapsto x^2$ un morphisme donc par le Thm d'isomorphisme, $\mathbb{F}_p^*/\ker(\varphi) \simeq \mathbb{F}_p^{*2}$.

D'où $|\mathbb{F}_p^*/\ker(\varphi)| = \frac{p-1}{2} = |\mathbb{F}_p^{*2}|$ et $|\mathbb{F}_q^{2}| = |\mathbb{F}_q^{*2}| + |0| = \frac{q+2}{2}$

Lemme : $p > 2$ premier, $x \in \mathbb{F}_p^{*2} \Leftrightarrow x^{\frac{p-1}{2}} = 1$.

Dem : On pose $X = \{x \in \mathbb{F}_p \mid x^{\frac{p-1}{2}} = 1\}$ on a $|X| \leq \frac{p-1}{2}$

Or $x \in \mathbb{F}_p^{*2} \Rightarrow x = y^2$ donc $x^{\frac{p-1}{2}} = y^{p-1} = 1$ par Lagrange car $|\mathbb{F}_p^*| = p-1$

Donc $\mathbb{F}_p^{*2} \subset X$ donc par cardinalité, $X = \mathbb{F}_p^{*2}$.

Corollaire : p premier ≥ 2 alors -1 est un carré dans $\mathbb{F}_p \Leftrightarrow p \equiv 1 [4]$

Dem : $-1 \in \mathbb{F}_p^{*2} \Leftrightarrow (-1)^{\frac{p-1}{2}} = 1 \Leftrightarrow \frac{p-1}{2}$ est pair $\Leftrightarrow p \equiv 1 [4]$.

Donc $(-1) \in \mathbb{F}_p^{*2} \Leftrightarrow p \equiv 1 [4]$ ou $p = 2$

$\Updownarrow$

$p \in \Sigma$