G O U

Théorème des deux carrés

L 120
L 121
L 122
L 126

Lemme : Soit p un nombre 1er dans $\mathbb{N}$. On a équivalence entre :

(1) p n'est pas irréductible ds $\mathbb{Z}[i]$

(2) $\exists z \in \mathbb{Z}[i]$ tq $p = N(z)$

(3) -1 est un carré modulo p

(4) $p = 2$ ou $p \equiv 1 [4]$

Démonstration : (1) ⇒ (2) Soit p non irréductible ds $\mathbb{Z}[i]$,

$\exists z, z' \in \mathbb{Z}[i] \setminus \mathbb{Z}[i]^\times$ tq $p = z \cdot z'$

alors $p^2 = N(p) = N(z) . N(z')$.

or $N(z) \neq 1$ car $z \notin \{\pm 1; \pm i\}$ donc $N(z) = N(z') = p$

(2) ⇒ (3) Soit $z \in \mathbb{Z}[i]$ tq $p = N(z)$; $z = x + iy$

On a $p = x^2 + y^2$ puis $x^2 + y^2 \equiv 0 [p]$

Or y n'est pas divisible par p donc y inversible ds $\mathbb{Z}/p\mathbb{Z}$

alors $\bar{x}^2 + \bar{i}^2 \bar{y}^2 = 0 \Leftrightarrow \bar{x}^2 \bar{y}^{-2} = -\bar{1}$: -1 est un carré modulo p.

(3) ⇒ (1) Si -1 est un carré modulo p.

Soit $a \in \mathbb{Z}$ tq $\bar{a}^2 = -\bar{1} \Leftrightarrow \bar{a}^2 + \bar{1} = \bar{0}$

Comme $a^2 + 1 = (a - i)(a + i)$, et $\mathbb{Z}[i]$ euclidien,

si p est irréductible, par le lemme d'Euclide $p \mid a - ib$ ou $p \mid a + ib$

alors $\bar{p} \mid a + ib$ ou $\bar{p} \mid a - ib$ donc $p \mid 2a$ et $p \mid 2i$.

Donc $N(p) = p^2$ divise 4. Or $p = 2$ n'est pas irréductible ($2 = (1+i)(1-i)$)

(3) ⇔ (4)

ds $\mathbb{Z}/2\mathbb{Z}$, -1 est un carré.

Si $p \neq 2$, -1 est un carré $\Leftrightarrow \left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = 1 \Leftrightarrow p \equiv 1 [4]$.

Théorème des 2 carrés : Soit $n \in \mathbb{N}^*$. n est somme de 2 carrés

$\Leftrightarrow \forall p \in \mathbb{P}$, $p \equiv 3\ [4]$, on a $v_p(n) \in 2\mathbb{N}$.

Dém° : $\Rightarrow$ Soit $n = x^2 + y^2$ avec $x, y \in \mathbb{Z}$.

Soit p un facteur 1er de n tel que $v_p(n)$ soit impair

On note $d = \text{pgcd}(x, y)$ et $x' = \frac{x}{d}$, $y' = \frac{y}{d}$ alors $x' \wedge y' = 1$

Comme $n = d^2(x'^2 + y'^2)$, et que $v_p(n)$ impair, on a $p \mid x'^2 + y'^2$.

Or $p \nmid x'$ (car sinon $p \mid x'$ et $p \mid y'$) donc x' est non nul de $\mathbb{Z}/p\mathbb{Z}$.

Comme $x'^2 + y'^2 = \bar{0}$, on a : $-1 = (x'^{-1} y)^2$ est un carré

donc d'après l'équivalence, $p = 2$ ou $p \equiv 1\ [4]$.

$\Leftarrow$ Mq $\Sigma = \{n = a^2 + b^2,\ a, b \in \mathbb{N}\}$ est stable par $\times$.

On a $(a^2+b^2)(\alpha^2+\beta^2) = (a\alpha + b\beta)^2 + (a\beta - \alpha b)^2$ d'où la stabilité

Soit $n \in \mathbb{N}^*$, par le TFA, $n = \prod_{p \in \mathbb{P}} p^{v_p(n)}$

alors $n = \left(\prod_{\substack{p \in \mathbb{P} \\ p \equiv 3[4]}} p^{v_p(n)} \right) \times 2^{v_2(n)} \times \prod_{\substack{p \in \mathbb{P} \\ p \equiv 1[4]}} p^{v_p(n)}$

$= \underbrace{\left(\prod_{\substack{p \in \mathbb{P} \\ p \equiv 3[4]}} p^{\frac{v_p(n)}{2}} \right)^2}_{\in \Sigma} \times \underbrace{2^{v_2(n)}}_{\in \Sigma} \times \underbrace{\prod_{\substack{p \in \mathbb{P} \\ p \equiv 1[4]}} p^{v_p(n)}}_{\in \Sigma}$

$\in \Sigma$

Donc par stabilité, $n \in \Sigma$.