$(\pi) \subseteq \mathbb{Z}[i] = R$ primo

(1)

(1)

$p = \pi\,\overline{\pi}$

$R \supseteq (\pi) \supseteq (p)$

p^2

se

(1) $\#\left|R/(\pi)\right| = p^2 \Rightarrow (\pi) = (p)$

e $\pi = up$, u unidade.

(2) $\#\left|R/(\pi)\right| = p \iff R/(p)$ é corpo

$\Rightarrow$ Classificar $p \in \mathbb{Z}$ primos t. q.

$R/(p)$ corpo ou não.

$$R/(p) = \mathbb{Z}[i]/(p) = \mathbb{Z}[x]/(x^2+1, p)$$

$$\simeq \mathbb{Z}/p\mathbb{Z}[x]/(x^2+1) \longleftarrow \text{campos } \underline{\text{sii}} \; x^2+1 \text{ irred en } \mathbb{Z}/p\mathbb{Z}.$$

¿Es x^2+1 irred sobre $\mathbb{Z}/p\mathbb{Z}$?

↳ x^2+1 irred $\iff$ tiene raices en $\mathbb{Z}/p\mathbb{Z}$

$\iff \exists x \in \mathbb{Z}/p\mathbb{Z}$ t.q.

$$x^2 \equiv -1 \pmod{p}$$

¿Para que primos p, es -1 residuo cuadrático?

$p=2$ $\quad x^2+1 = (x+1)^2 \Rightarrow x \equiv 1 \equiv -1 \pmod 2$

$\Rightarrow \pi = 1+i$ es primo.

$R_2(\pi) \simeq \mathbb{Z}_{(2)}$.

Supongamos $\exists\ a \in \mathbb{Z}/p\mathbb{Z}$

$$x^2+1 = (x+a)(x-a)$$

$$\Rightarrow \quad a^2 \equiv -1 \pmod{p} \quad \Rightarrow \quad |a| = 4 \text{ en } (\mathbb{Z}/p\mathbb{Z})^* = G$$

si $p \equiv 3 \pmod 4$ entonces $|G| = p-1 = 2$ (IMPAR)

$\hookrightarrow p = 4k-3 = 2(2k-1)$ $\Rightarrow$ no hay elementos de orden 4.

$\Rightarrow x^2+1$ es irred $\pmod p$.

si $p \equiv 1 \pmod 4$ $\quad |\mathbb{Z}/(p-1)\mathbb{Z}| = 2^k$ (Impar) $\quad k \geq 2$

$\Rightarrow \exists$ 2-Sylow de orden 2^k, pero los elementos de orden 2 son 1 y -1

$\Rightarrow \exists\ a \in (\mathbb{Z}/(p-1)\mathbb{Z})^*$ de orden 4.

$\Rightarrow (x^2+1) = (x+a)(x-a)$ //

$\Rightarrow$)

$$R \supsetneq (\pi) \supsetneq (p)$$ <

$R/(p)$ no es campo

$\left| R/(\pi) \right| = p$. donde $\pi \cdot \bar{\pi} = p$

$\bar{\pi} = (p, i-a)$

Teorema (Gauss) $p = a^2 + b^2$ primo $\mathbb{Z}$

$p \neq 2$ $\iff$ $p \equiv 1 \pmod 4$

Dem: $\Rightarrow$) $p \equiv 1 \pmod 4$

$(p) = (\pi)(\bar{\pi})$ en $\mathbb{Z}[i]$ ← DIP $\Rightarrow$ $\pi = (a+bi)$ para algún $a, b \in \mathbb{Z}$.

$\delta(\pi) = \left| \mathbb{Z}[i]/(\pi) \right| = p = a^2 + b^2$

$\Leftarrow$) fácil. ∎

Teorema (Gauss) $n \in \mathbb{Z}$.

$n = x^2 + y^2$ para algún $x, y \in \mathbb{Z}$.

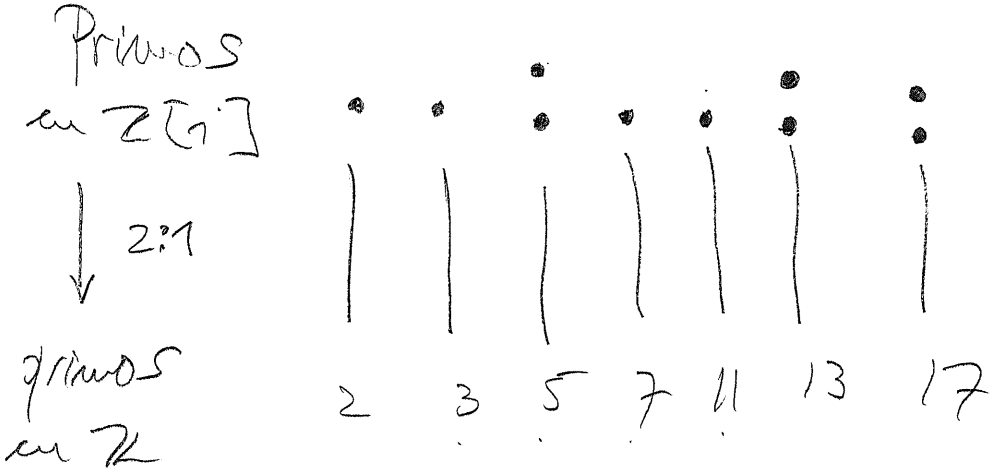
$\Leftrightarrow$ Todo primo $p \mid n$ congruente con 3 módulo 4 tiene un exponente Par.

Dem:

$n \in \mathbb{Z}[i]$ $\quad n = p_1 \cdots p_k$ ← Primos

si $p_j \equiv 3 \pmod 4$ $\quad \delta(p_j) = p_j^2$

□



$$1 - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} + \frac{1}{9} - \frac{1}{11} + \frac{1}{13} - \frac{1}{15} + \frac{1}{17} + \cdots = \frac{\pi}{4}$$