$\forall$ dada $\alpha \in K$, existe $\beta \in K$ t.q.

$\alpha \cdot \beta = 1$. $\delta(\alpha) \cdot \delta(\beta) = 1 \Rightarrow$

$$\delta(\alpha) = \delta(\beta) = 1$$

$\blacksquare$

entonces, si

$\Rightarrow \alpha \in \mathbb{Z}[i]$ es Unidad

$$\delta(\alpha) = a^2 + b^2 = 1$$

$\Rightarrow$ Unidades $(\mathbb{Z}[i]) = \{1, -1, -i, i\}$.

Primos: si
en $\mathbb{Z}[i]$ $\pi \in R = \mathbb{Z}[i]$ es primo $\Rightarrow$

$R/(\pi)$ es un campo finito $\Rightarrow$

$\left| R/(\pi) \right| = p^n$ para algún $p \in \mathbb{Z}$ primo y $n \geq 1$.

en efecto,

$$\begin{array}{ccc} \mathbb{Z} & \hookrightarrow & R \\ \| & & \downarrow \\ \mathbb{Z} & \xrightarrow[i]{} & R/(\pi) \end{array}$$

$\left\{ \begin{matrix} \text{Núcleo} \\ \text{de } i \end{matrix} \right\} = (p) \leq \mathbb{Z}$

$\uparrow$ primo

esp. vect. sobre $\mathbb{Z}/p\mathbb{Z}$

$$\mathbb{Z}/(p) \longrightarrow R/(\pi)$$

$R/(\pi)$ tiene órden p ó p^2

pues $p = \alpha\pi$ en R

$$p \cdot R \subseteq \pi \cdot R \subseteq R$$

índice p^2 — índice que deseamos calcular !!

Dos casos:

(1) $R/(\pi)$ tiene órden p^2, entonces

$$(\pi) = (p).$$

SE sigue $\pi = u \cdot p$; $p \in R$ es primo.

$\hookrightarrow \# R/(p) = p^2$

(2) $R/(p)$ no es campo. Entonces existe π

$$(p) \subseteq (\pi) \subseteq R \quad y$$

el cociente $R/(\pi) \cong \mathbb{Z}/p\mathbb{Z}$

¿Qué primos 2, 3, 5, 7, ... en $\mathbb{Z}$
son también primos en R?

MORALEJA: ~~Para~~ A cada primo $\pi \in \mathbb{Z}[i]$,
le podemos asociar un primo $p \in \mathbb{Z}$.

↳ Estudiaremos el anillo finito $R/(p)$
con $p \in \mathbb{Z}$ primo.

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

$$\cong \left(\mathbb{Z}[x]/(p)\right)/(x^2+1) \cong \left(\mathbb{Z}/p\mathbb{Z}[x]\right)/(x^2+1)$$

↑ Campo ssi

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

x^2+1 sobre $\mathbb{Z}/p\mathbb{Z}$ no tiene raíces

$\Updownarrow$

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

$p=2$ $\quad x^2+1 \equiv (x+1)^2 \pmod{2}$

raíz Unique $\quad x \equiv -1 \equiv 1.$

en este caso, existe un único primo

$\pi = 1+i$ con

$R \supset (\pi) \supset (2)$

↑ Índice 2.

EJER:
factoriza $2 \in \mathbb{Z}[i]$

EJER

si

$p \equiv 3 \pmod{4}$, entonces x^2+1 irred $\pmod{p}$

& $R/(p)$ campo

↑ primo en R.

Pista: $\#\left(\mathbb{Z}/p\mathbb{Z}\right)^* = p-1 = 2 \cdot (\text{IMPAR})$

Si $p \equiv 1 \pmod 4 \Rightarrow$ $(x-a)(x+a)$ donde $a^2 \equiv -1 \pmod 4$

x^2+1

ORDEN 4 en R^*

$$\#\left(\mathbb{Z}/p\mathbb{Z}\right)^* = p-1 = 2^k \text{ (IMPAR)} \qquad k \geq 2$$

Aquí tenemos un 2-Sylow de orden 2^k pero los elementos de órden 2 en $\mathbb{Z}/p\mathbb{Z}$ son 1 y -1. Por lo tanto $\exists$ un elemento de orden 4: llámalo a.

Entonces, $\hookrightarrow \pi' = (p, i-a)$

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

$\hookrightarrow$ en R $\pi = (p, i+a)$

con π & π' ambos primos en R, y

$$R/(\pi) \cong R/(-\pi) \cong \mathbb{Z}/p\mathbb{Z}$$

FINAL: ✓ ✓ ✗ ✓ ✗ ✗

2, 3, 5, 7, 13, 17, ...