Thm Para todos los números primos $p \neq 2$ tenemos

$$p = a^2 + b^2 \quad (a, b, \in \mathbb{Z}) \iff p \equiv 1 \pmod 4$$

Demostración: $\Leftarrow$) Considera el siguiente anillo

$$R = \mathbb{Z}[i] := \{ a + bi \mid \begin{matrix} a, b \in \mathbb{Z} \\ i^2 = -1 \end{matrix} \} \subseteq \mathbb{C}$$

en este anillo:

$$p = a^2 + b^2 = \underbrace{(a+ib)}\ \underbrace{(a-ib)}$$

factores

Qué primos ~~¿cuándo~~ $p \in \mathbb{Z} \subseteq \mathbb{Z}[i]$ factorizan en $\mathbb{Z}[i]$?

(primos aquí)

Lema: $\mathbb{Z}[i]$ es euclidiano, en particular factorial (DFU)

Si $p \equiv 1 \pmod 4$ (!) $\Longrightarrow$ $p \in \mathbb{Z}$ primo

factoriza en $\mathbb{Z}[i]$.

Por lo tanto

$$p = \alpha \cdot \beta \qquad \text{con } \alpha, \beta \in \mathbb{Z}[i]$$

no unidades. (i.e. $N(\alpha) \neq 1$)

entonces

$$N(p) = p^2 = N(\alpha)\, N(\beta) \in \mathbb{Z}$$

$$\Longrightarrow \quad p = N(\alpha) = \alpha_0^2 + \alpha_1^2 \qquad \alpha_0, \alpha_1 \in \mathbb{Z}$$

Falta verificar que un primo $p \in \mathbb{Z}$ de la forma $4k+1$ factoriza en $\mathbb{Z}[i]$

$$\langle p \rangle \subseteq \mathbb{Z}[i] = \mathbb{Z}[x] / \langle x^2+1 \rangle$$

$$\downarrow$$

$$\langle p \rangle \subseteq \mathbb{Z}$$

[Si no factoriza es primo.]

Teoría de Anillos

Def. $\langle p \rangle \subseteq \mathbb{Z}$ ideal primo si $\mathbb{Z}/\langle p \rangle$ es dominio

¿ ideales primos vs. Elementos primos ? de R

Si $p = r \cdot s \Rightarrow R/\langle p \rangle$ no es dominio

i.e. si p no es primo entonces no genera un ideal primo.

argumento:

$r \cdot s = 0$ en $R/\langle p \rangle$

con $r \neq 0$, $s \neq 0$

Prop si $p \in \mathbb{Z}$ primo de la forma $4k+1$

$\Rightarrow \mathbb{Z}[i]/\langle p \rangle$ no es dominio.

Demos:

$$\mathbb{Z}[i]/\langle p \rangle \cong \mathbb{Z}[x]/\langle p, x^2+1 \rangle$$

$$\cong \mathbb{F}_p[x]/\langle x^2+1 \rangle \leftarrow \text{¿dominio?}$$

si x^2+1 tiene raíces en $\mathbb{F}_p$

¡NO!

¿ para qué primos -1 es residuo cuadrático mod p ?

i.e. $-1 \equiv x^2 \pmod p$ para algún $x \in \mathbb{F}_p$.

Eg $p=5$

primos en $\mathbb{Z}$ no en $\mathbb{F}_5$

$\mathbb{F}_5 = \{1,2,3,4,0\} \xrightarrow{z^2} \{1,4,4,1,0\}$

$= \{1,2,0,-2,-1\} \longrightarrow \{1,-1,0,-1,1\}$

$p=7$

$\mathbb{F}_7 = \{1,2,3,0,-3,-2,-1\} \longrightarrow \{1,-3,2,0,2,-3,1\}$

$= \{1,2,3,4,5,6,0\}$
$1\ 2\ 3\ -3\ -2\ -1$

$\Downarrow$

no existe $x \in \mathbb{F}_7$ tal que $x^2 \equiv -1 \pmod 7$.

Prop $x^2+1=0$ tiene solución en $\mathbb{F}_p$ si $p = 1+4k$.

Argumento: $p-1 = 4k$

$-1 \equiv (p-1)! = (1\cdot 2 \cdots 2k)\big((p-1)(p-2)\cdots(p-2k)\big)$

$= (2k)!\,[(-1)^{2k}\,2k!] = (2k!)^2 \pmod p$

Teo Wilson

· Por lo tanto $\langle p \rangle \subseteq \mathbb{Z}[i]$ factoriza.

y $p = a^2 + b^2$ para $a, b \in \mathbb{Z}$.

$\Longrightarrow$ si $p = a^2 + b^2 \Rightarrow p \equiv 1 \pmod 4$

pues $a^2 \equiv 0, 1 \pmod 4$.

¿Qué elementos primos tiene $\mathbb{Z}[i]$?

¿Qué unidades tiene $\mathbb{Z}[i]$?

Pregunta gral: $\mathbb{Z} \hookrightarrow \mathbb{Z}[\alpha]$ con α raíz de $x^2 + ax + b = 0$

¿Qué primos de $\mathbb{Z}$ "sobreviven" en $\mathbb{Z}[\alpha]$?.

Def. $\alpha \in \mathbb{Z}[i]$ es unidad si tiene inverso mult.

Obs. α es unidad sii $N(\alpha) = \alpha_0^2 + \alpha_1^2 = 1$.

Por tanto $\mathbb{Z}[i]^* = \{1, -1, i, -i\} \cong \mathbb{Z}_4 = \langle i \rangle$

↑ grupo de unidades

Thm Si $\alpha \in \mathbb{Z}[i]$ es un elemento primo entonces:

1) $\alpha = p \in \mathbb{Z}$ con $p \equiv 3 \pmod 4$ & p primo en $\mathbb{Z}$

2) $\alpha = a+ib$ con $a^2+b^2 = p$ primo en $\mathbb{Z}$
$a>0$ $|b|>0$.

3) $\alpha = 1+i$

o asociados.

Demostración: 2) & 3) Si $\alpha = rs$ no unidades

entonces $N(\alpha) = a^2+b^2 \in \mathbb{Z}$ primo

$= N(r)N(s) = p \Rightarrow N(r) = 1$

por tanto r es unidad. $N(s) = 1$

1) $N(\alpha) = p^2 = N(s)N(r) \Rightarrow p = N(r)$
$= a^2+b^2$

$\Rightarrow p \equiv 1 (4)$ contradicción. Entonces $p^2 = N(r)$; $N(s)=1$

contradicción. $\Rightarrow$ Por lo tanto $r = p \equiv 3 \pmod 4$

Consideremos $\alpha \in \mathbb{Z}[i]$ primo arbitrario.

$N(\alpha) = \alpha\bar{\alpha} = p_1 \cdots p_r \in \mathbb{Z}$ con $p_i \in \mathbb{Z}$ primos

$\Rightarrow \alpha \mid p_i$ para algún primo p_i en $\mathbb{Z}$.

$\Rightarrow N(\alpha) \mid N(p_i) = p_i^2 \Rightarrow N(\alpha) = p_i$ ó $N(\alpha) = p_i^2$.

si $N(\alpha) = p$ estamos en $p \equiv 1 \pmod 4$

ó $\alpha = i+1$ & $p = 2$.

si $N(\alpha) = p_i^2$ ó asociado $\boxed{\alpha = p_i}$ con $p_i \equiv 3 \pmod 4$ ∎

~~α es rep con $u \in \mathbb{Z}[i]^*$ pues $\frac{N(p)}{N(\alpha)} = 1$~~

Resumiendo

$\mathbb{Z}[i]$

|

$\mathbb{Z}$