Teoría algebraica de Números: Sep 5

Clase pasada: $R = \mathbb{Z}[i]$ & $I \subseteq R$ ideal

Si $R/I \cong \mathbb{Z}/p\mathbb{Z}$, entonces (con $p \in \mathbb{Z}$ primo)

$p \equiv 1 \pmod 4$.

Hoy: ¿Quién es el generador de I en el caso de arriba?

↓

¿Son estos todos los ideales maximales del anillo R?

Teorema (Fermat) Sea $p \in \mathbb{Z}$ primo.

$p = x^2 + y^2$ con $x, y \in \mathbb{Z}$ <u>sii</u>

$p \equiv 1 \pmod 4$.

<u>Demostración:</u> (FRAGMENTO) Sean $R = \mathbb{Z}[i]$ los enteros Gaussianos.

Afirmación: si $I = (\alpha) \leq \mathbb{Z}[i]$ (ideal), entonces la cardinalidad $\left| \mathbb{Z}[i]/I \right| = \delta(\alpha) = a^2 + b^2$

donde $\alpha = a + bi \in \mathbb{Z}[i]$. <u>EJER*</u>

$\Rightarrow$) Supongamos $p = x^2 + y^2$ $x, y \in \mathbb{Z}$.

Entonces $p = |x+iy|$ con $x+iy \in \mathbb{Z}[i]$

$$p = (x+iy)(x-iy)$$

¡$p \in \mathbb{Z}[i]$ factoriza!

Más aún $\left| \mathbb{Z}[i] / (x+iy) \right| = x^2 + y^2 = p$

y dado $I = (x+iy)$ es maximal en R

$\Rightarrow$ $R/I \cong \mathbb{Z}/p\mathbb{Z}$ campo

¿Por qué?

$\Rightarrow$ $p \equiv 1 \pmod 4$