WORLD MEETING FOR WOMEN IN MATHEMATICS

Teoría de Números 21 sep

Clase pasada: Teorema de Fermat

Hoy: ideales en anillos & enteros algebraicos

Teorema (Gauss) Todo primo $p|n$ congruente con 3 módulo 4 tiene un exponente par

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

& $n \in \mathbb{N}$.

Dem: $n \in \mathbb{Z}[i]$ $n = p_1 \cdots p_k$ ← primos

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

EJER

¿Qué primos $p \in \mathbb{Z}$ se descomponen como $x^2+3y^2=p$?

↳ ¿Qué primos factorizan en $R=\mathbb{Z}[\sqrt{-3}]$?

OBSERVACIÓN: R no es Dominio Euclidiano.

↳ -3 es residuo cuadrático módulo p.

Argumento: $\mathbb{Z}[\sqrt{-3}] \cong \mathbb{Z}[x]/(x^2+3)$. entonces

$$\mathbb{Z}[\sqrt{-3}]/(p) = \mathbb{Z}[x]/(x^2+3,p) \cong \mathbb{Z}/p[x]/(x^2+3)$$

No es campo

~~sii~~ -3 es residuo cuadrático $/p$.

entonces

$(p) \subseteq \mathbb{Z}[\sqrt{-3}]$ es maximal

sii -3 es NO residuo cuadrático en $\mathbb{Z}/p$.

&

$(p) \subseteq \mathbb{Z}[\sqrt{-3}]$ no es maximal

sii -3 es residuo cuadrático en $\mathbb{Z}/p$.

Sin embargo, (p) podría no ser maximal aún cuando $p \in \mathbb{Z}[\sqrt{-3}]$ no factoriza: NO sabemos si $\mathbb{Z}[\sqrt{-3}]$ es dominio de ideales principales.

Por tanto podría suceder

$$(p) \subsetneq (g, u) \subseteq \mathbb{Z}[\sqrt{-3}].$$

Recordar: en un DIP se tiene que si $p \in R$ es irreducible, entonces $(p) \leq R$ es maximal.

y recíprocamente.

Definición: Sea $\alpha \in \mathbb{Q}[\sqrt{d}] = K$ con $d \in \mathbb{Z}$ libre de cuadrados.

diremos que α es un entero algebraico en K si $f(\alpha)=0$ con $f \in \mathbb{Z}[x]$ mónico.

Eg: $\mathbb{Z}$ son los enteros algebraicos en $\mathbb{Q}$.

$\mathbb{Z}[i]$ son los enteros algebraicos en $\mathbb{Q}[i]$.

$\mathbb{Z}[\sqrt{-3}]$ NO son los enteros alg en $\mathbb{Q}[\sqrt{-3}]$

Observación: $\mathbb{Z}[\sqrt{-3}] \leq \underbrace{\mathbb{Z}[\omega]}_{\text{con } \omega^2+\omega+1=0.} \leq \mathbb{Q}[\sqrt{-3}]$

Prop. $\mathbb{Z}[\omega]$ son los enteros algebraicos de $\mathbb{Q}[\sqrt{-3}]$. Más aún, $\mathbb{Z}[\omega]$ es dominio Euclidiano.

Dem: Próxima clase.

EJER: ¿Para qué primos $p \in \mathbb{Z}$ es -3 residuo cuadrático módulo p?

¿Es $\mathbb{Z}[\sqrt{-2}]$ dominio de ideales principales?

¿Tiene $\mathbb{Z}[\sqrt{-2}]$ norma?