Teoría de Números : Sep 24

Clase pasada: Enteros algebraicos

Hoy: Símbolo de Legendre

Si $p = x^2 + 3y^2$ con $x, y \in \mathbb{Z}$ $\Rightarrow$ $p \equiv 1 \pmod 3$

¿y el recíproco? (*)

↳ ¿Cuándo p factoriza en $R = \mathbb{Z}[\sqrt{-3}]$?

(*) asume R es DIP. La pregunta que podemos contestar es

¿Cuándo es $(p) \subseteq R$ no maximal?

$(p) \subseteq R$ no es maximal $\Leftrightarrow$ $\left(\frac{-3}{p}\right) = 1$ $\Leftrightarrow$ -3 es residuo cuadrático $/p$.

(símbolo de Legendre)

Def.- El símbolo de Legendre $\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{si } a \text{ es residuo cuadrático mod } p \\ -1 & \text{en otro caso.} \end{cases}$

Proposición: Hay tantos residuos cuadráticos en $\mathbb{Z}/p$ como no residuos cuadráticos

Demostración:

$$\begin{aligned} (\mathbb{Z}/p)^* &\longrightarrow (\mathbb{Z}/p)^* \\ h &\longmapsto h^2 \end{aligned}$$

es homomorfismo de grupos. Además su núcleo es $\{1, -1\}$. ∎

EJER: ¿Qué subgrupos tiene $(\mathbb{Z}/p)^*$?

Pregunta: ¿$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$?

Corolario de la pregunta anterior:

1) si a & b son residuos cuadráticos entonces ab es residuo cuadrático $/p$.

2) si a & b NO son ambos residuos cuadrát. entonces ab sí es residuo cuadrático $/p$.

Concluimos

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

$$\left(\frac{-3}{p}\right) = -1 \quad .$$

Pregunta (EJER): Los residuos cuadráticos en $\mathbb{Z}/p$ ¿forman un subgrupo en $(\mathbb{Z}/p)^*$?