Álgebra Moderna II 3 abril.

Clase pasada: $x^2+y^2=p$ con $p \in \mathbb{Z}$ primo y $x, y \in \mathbb{Z}$ sii $p \equiv 1 \pmod 4$.

Hoy: ¿Podemos resolver $x^2+dy^2=p$ usando las mismas ideas?

$d=3$. ¿Qué primos $p \in \mathbb{Z}$ se pueden escribir como $p=x^2+3y^2$ con $x, y \in \mathbb{Z}$?

en general:

¿Cuándo un entero $m \in \mathbb{Z}$

puede escribirse como

$$m = ax^2 + bxy + cy^2$$

con $D = b^2 - 4ac$ fijo?

PREGUNTA: ¿Cuales son los elementos primos de $R = \mathbb{Z}[\sqrt{-3}]$?

analizar $\mathbb{Z} \longrightarrow \mathbb{Z}[\sqrt{-3}]$.

¿Que primos de $\mathbb{Z}$ permanecen

Primos en $\mathbb{Z}[\sqrt{-3}]$?

Pistas: $7 = (2+\sqrt{-3})\overline{(2+\sqrt{-3})}$

$13 = (2+3\sqrt{-3})\overline{(2+3\sqrt{-3})}$

Conjetura: si $p \equiv 1 \pmod 6 \iff$ $p = x^2+3y^2$. ← EJER

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

entender → $\cong \mathbb{Z}/p\mathbb{Z}[x]/(x^2+3)$

¿Cuándo es este anillo campo? ↗

x^2+3 irred en $\mathbb{Z}/p\mathbb{Z}$ $\Leftrightarrow$

$(p) \subset \mathbb{Z}[\sqrt{-3}]$ Maximal.

¿Es $R=\mathbb{Z}[\sqrt{-3}]$ DIP?

¿Es " " Dominio Euclideano?

Supongamos:

$$x^2+3 = (x+a)(x-a) \qquad a \in \mathbb{Z}/p\mathbb{Z}$$

$$\Rightarrow -a^2 \equiv 3 \pmod{p}$$

$$\Rightarrow \boxed{a^2 \equiv -3 \pmod{p}}$$

$a \in (\mathbb{Z}/p\mathbb{Z})^* = \{1, \dots, p-1\}$

CASOS:

$p = 7, 13, \dots$