# Teoría de Números 14 sep

Clase pasada: Teorema de Fermat

Hoy: ¿para qué primos $p \in \mathbb{Z}$ la ecuación $x^2+1=0$ tiene solución módulo $p$? en $\mathbb{Z}/p$.

---

$p \in \mathbb{Z}[i]$ | $p \in \mathbb{Z}$

¿cuándo $p \in \mathbb{Z}$ primo sigue siendo primo en $\mathbb{Z}[i]$?

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

$\mathbb{Z}[i]/(p)$: anillo finito ¿por qué? EJER

$\mathbb{Z}/p[x]/(x^2+1)$: campo sii $x^2+1$ es irreducible sii no tiene raíces en $\mathbb{Z}/p$.

Supongamos $x^2+1=0$ tiene una raíz en $\mathbb{Z}/p$.

$\Rightarrow \exists\ x_0 \in \mathbb{Z}/p$ tal que $x_0^2 \equiv -1 \pmod{p}$

$\Rightarrow x_0$ tiene orden 4 en $(\mathbb{Z}/p)^* = \{1, \dots, p-1\}$

$\Rightarrow 4 \mid p-1$ & por tanto $p \equiv 1 \pmod{4}$.

Conclusión: si $p \equiv 3 \pmod 4$ entonces

$x^2+1=0$ no tiene solución en $\mathbb{Z}/p$.

$\Rightarrow p \in \mathbb{Z}[i]$ es primo

↑ no factoriza de forma no trivial.

Supongamos ahora $p \equiv 1 \pmod 4$

queremos probar que $x^2+1=0$ tiene una solución en $\mathbb{Z}/p$. Es decir $\exists\, a \in \mathbb{Z}/p$ tal que $a^2+1=0$ en $\mathbb{Z}/p$

¡Claro! $a = \left(\frac{p-1}{2}\right)!$ ∎

WILSON + $p \equiv 1 (4)$

Conclusión: $p \in \mathbb{Z}$ primo.

$p \equiv 1 \pmod 4 \iff x^2+1=0$ tiene solución en $\mathbb{Z}/p$.

Def.- Un elemento $c \in \mathbb{Z}/p$ se dice <u>residuo cuadrático</u> módulo $p$ si existe $a \in \mathbb{Z}/p$ tal que $a^2 = c$ en $\mathbb{Z}/p$.