# Teoría de Números: 10 septiembre

Clase pasada: Si $\mathbb{Z}[i]/I \cong \mathbb{Z}/p$

con $p \in \mathbb{Z}$ primo, entonces $p \equiv 1 \pmod 4$.

Hoy: Si $p \equiv 1 \pmod 4$, entonces existe un ideal $I \leq \mathbb{Z}[i]$ tal que $\mathbb{Z}[i]/I \cong \mathbb{Z}/p$.

Demostración: consideremos $I = (p, i-a)$

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

Verificar EJER: $\mathbb{Z}[i]/I \cong \mathbb{Z}/p$

¿Por qué esta elección del "a"?

↳

$$\mathbb{Z}[i] \xrightarrow{f} \mathbb{Z}[i]/(p, i-a)$$

$$i \longmapsto f(i) = a$$

homomorfismo de anillos

$$\Rightarrow \boxed{f(i)^2 = a^2 = -1}$$

necesitamos mandar a $i$ a un elemento de orden 4.

Afirmación: $a^2 \equiv -1 \pmod p$ es decir

$$\left[\left(\frac{p-1}{2}\right)!\right]^2 \equiv -1 \pmod p$$

↳ En efecto: $1 \cdot 2 \cdots \left(\frac{p-1}{2}\right)\left(\frac{p+1}{2}\right)\left(\frac{p+3}{2}\right)\cdots(p-1) \equiv -1 \pmod p$

WILSON

EJER

**Teorema de Wilson:** $(p-1)! \equiv -1 \pmod p$

$$\left.\begin{aligned} p-1 &\equiv -1 \pmod p \\ p-2 &\equiv -2 \pmod p \\ &\vdots \\ \frac{p-1}{2} &\equiv -\frac{p+1}{2} \pmod p \end{aligned}\right\} \quad \left(\frac{p+1}{2}\right)\left(\frac{p+3}{2}\right)\cdots(p-2)(p-1) = (-1)^{\left(\frac{p-1}{2}\right)} \cdot 1 \cdot 2 \cdot 3 \cdots \left(\frac{p-1}{2}\right)$$

Pero $\left(\frac{p-1}{2}\right)$ es par. Por lo tanto

$$\left[\left(\frac{p-1}{2}\right)!\right]^2 \equiv -1 \pmod{p}.$$

FIN DE LA demostración de la afirmación

y $a = \left(\frac{p-1}{2}\right)!$ tiene orden 4 en $(\mathbb{Z}/p\mathbb{Z})^*$.

Esto responde la elección de $a = \left(\frac{p-1}{2}\right)!$. FIN

Veamos que $\mathbb{Z}[i]/I \cong \mathbb{Z}/p$, donde $I = (p, i-a)$

1) $I \cap \mathbb{Z} = p\mathbb{Z}$. Sabemos $I \cap \mathbb{Z} \supseteq p\mathbb{Z}$

entonces $I \cap \mathbb{Z} = \mathbb{Z}$ ó $p\mathbb{Z}$.

2) si $(i-a)r \in \mathbb{Z}$ con $r \in \mathbb{Z}[i]$, entonces

$(i-a)r \in p\cdot\mathbb{Z}$.

Justificación $\longrightarrow$ $(i-a)(b+ic) = (-ab-c) + \underbrace{(-ac+b)}_{=0} i$

$\Rightarrow \boxed{b = ac}$ entonces

$$-a(ac) - c = -c(a^2+1)$$
$$= 0 \pmod{p}$$

Por lo tanto, $(i-a)(b+ci) \in \mathbb{Z}\cdot p$

$\Rightarrow I \cap \mathbb{Z} = \mathbb{Z}\cdot p$

Por último, $\mathbb{Z} \longrightarrow \mathbb{Z}[i]/I$ es sobreyectivo pues $i \equiv a$ en $\mathbb{Z}[i]/I$.

$\Rightarrow$ R $\boxed{\mathbb{Z}[i]/I \cong \mathbb{Z}/p\mathbb{Z}}$

**Teorema (Fermat)** $p \in \mathbb{Z}$ primo $(\neq 2)$.

$p = a^2 + b^2$ con $a, b \in \mathbb{Z}$ $\iff$ $p \equiv 1 \pmod 4$.

**Demostración:** $(\Rightarrow)$ ✓

$(\Leftarrow)$ $\exists\ I \subseteq \mathbb{Z}[i]$ ideal tal que

$$R/I \cong \mathbb{Z}/p\mathbb{Z}.$$

$\mathbb{Z}[i]$ es dominio de ideales principales $\Rightarrow$

$I = (A + Bi)$ para $A, B \in \mathbb{Z}$.

$\Rightarrow$ $|R/I| = A^2 + B^2 = p$ ∎

OBSERVAR: $p = (A+Bi)\overline{(A+iB)}$ ¡factoriza en $\mathbb{Z}[i]$!