entonces,

$$R/(a_1)/(\bar{a}_2)\cdots/(\bar{a}_m) = \bar{R} = R/(a_1,\dots,a_k).$$

EJEMPLO: $R = \mathbb{Z}[i] = \mathbb{Z} + \mathbb{Z}i$
$= \{a+bi \mid a,b \in \mathbb{Z}\}.$

deseamos:

$2+i = 0$, entonces $I = (2+i)$

$R/I = \bar{R} \longleftarrow$ ¿Qué anillo es este?

1) Identifiquemos $I \cap \mathbb{Z}$.

$\hookrightarrow$ Observemos $5 \in I \cap \mathbb{Z}$.

Claro, $5 = (2+i)(2-i)$

$\Rightarrow \quad I \cap \mathbb{Z} \supset 5\cdot\mathbb{Z}$

$\Rightarrow \quad I \cap \mathbb{Z}$ es $\cong \mathbb{Z}$ or $5\cdot\mathbb{Z}$

2) Si $(2+i)(a+bi) \in \mathbb{Z}$, $\Rightarrow \in 5\cdot\mathbb{Z}$.

$$\underset{\displaystyle 2a-b+\underset{\displaystyle 0}{\underset{\shortparallel}{(2b+a)}}\,i}{\underset{\shortparallel}{(2+i)(a+bi)}} \Rightarrow a=-2b$$

$\Rightarrow \quad 2(-2b)-b=-5b \in 5\cdot\mathbb{Z}$

Por lo tanto, $I \cap \mathbb{Z} = 5\cdot\mathbb{Z}$.

Se sigue que el homomorfismo canónico

$$\mathbb{Z} \longrightarrow R/I = \overline{R}$$

tiene kernel $5\cdot\mathbb{Z}$ e imagen $\mathbb{Z}/5\mathbb{Z}$.

$$\boxed{\text{Por lo tanto } \overline{R} \text{ es un espacio vectorial sobre } \mathbb{Z}/5\mathbb{Z}.}$$

Más aún, el homomorfismo canónico es suprayectivo:

$$j: \mathbb{Z} \longrightarrow R/I = \overline{R}$$

Pues $2+i \equiv 0 \pmod{I}$

$\boxed{i \equiv -2}$ entonces $\overline{a+bi} \in \overline{R}$

$a+b(-2) \leftarrow$ entero en la imagen de $j: \mathbb{Z} \longrightarrow R/I$

$\Rightarrow \quad R/I \cong \mathbb{Z}/5\mathbb{Z}$.

Con más generalidad: si p es un primo con $p \equiv 1 \pmod{4}$ $\quad p = 5, 13, 17, 29, \ldots$
$4k+1$

Es mejor enunciarlo así: Existe un ideal I de R tal que el cociente es Z/pZ
si y solo si p es primo y es congruente con 1 modulo 4.

entonces existe un ideal $I \subseteq R = \mathbb{Z}[i]$

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

Demostración:

Implicación =>

$$f : R \longrightarrow R/I \cong \mathbb{Z}/p\mathbb{Z} \qquad p \text{ primo}$$

$$i \longmapsto f(i)$$ ← ¿Qué elemento es este?

Como $i^2 = -1$, entonces $f(i)^2 = -1 \pmod p$

$\Rightarrow$ $f(i)$ tiene orden 4 en $(\mathbb{Z}/p\mathbb{Z})^*$ grupo.

$\{0, 1, \ldots, p-1\}$

$\Rightarrow$ $p \equiv 1 \pmod 4$.

Implicación (<=

(afirmamos para todo $p \equiv 1 \pmod 4$ primo existe un ideal)

→ es suficiente decir quienes $f(i) \in R/I \cong \mathbb{Z}/p\mathbb{Z}$.

Candidato: $\left(\frac{p-1}{2}\right)! = f(i)$

EJEMPLO:
$-2 = \bar{i} = f(i)$

Tenemos que verificar que

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

$$\equiv$$

Wilson

$$1 \cdot 2 \cdots \left(\frac{p-1}{2}\right)\underbrace{\left(\frac{p+1}{2}\right)}_{(-)}\left(\frac{p+3}{2}\right)\cdots(p-2)(p-1) \equiv -1 \pmod p$$

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

OBSERVAR:

$$\left.\begin{aligned} p-1 &\equiv -1 \pmod p \\ p-2 &\equiv -2 \pmod p \\ &\vdots \\ \frac{p-1}{2} &\equiv \frac{p+1}{2} \pmod p \end{aligned}\right\}$$

$$\left(\frac{p+1}{2}\right)\left(\frac{p+3}{2}\right)\cdots(p-2)(p-1) \equiv (-1)^{\frac{p-1}{2}}\, 1 \cdot 2 \cdots \left(\frac{p-1}{2}\right)$$

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

Por lo tanto

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

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

Construimos el ideal: $I = (p, i-a) \trianglelefteq \mathbb{Z}[i]$

Entonces $\mathbb{Z}[i]/I \cong \mathbb{Z}/p\mathbb{Z}$.

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

con $I = (p, i-a)$.

Pista:

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

Sabemos $I \cap \mathbb{Z} \supseteq \mathbb{Z} \cdot p$, entonces

$I \cap \mathbb{Z}$ es $\mathbb{Z} \cdot p$ ó $\mathbb{Z}$.

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

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

↳ $(i-a)(b+ci) = (-ab-c) + \overbrace{(-ac+b)}^{=0}\, i$

$\Rightarrow$ $\boxed{b=ac}$ entonces $-a(ac) - c = -a($

$= -c(a^2+1)$

$\equiv -c(-1+1) = 0 \pmod{p}$

$\Rightarrow (i-a)(b+ci) \in \mathbb{Z} \cdot p$

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

Por último

$$\mathbb{Z} \longrightarrow R/I \quad \text{es sobreyectivo}$$

pues $i \equiv a$ en R/I.

$$\Rightarrow \quad \underline{\underline{R/I \cong \mathbb{Z}/p\mathbb{Z}}} \quad //$$

$\hookrightarrow$ Teorema (Gauss) $I \subseteq \mathbb{Z}[i]$ ideal.
entonces I es principal.

<u>COROLARIO</u>: $I = (p, i-a)$ es principal.

entonces $\mathbb{Z}[i]/(a+bi) \cong \mathbb{Z}/p\mathbb{Z}$

$$\Rightarrow \quad \boxed{p = a^2 + b^2}$$