

CAPÍTULO III

En A anillo: (P.40)

$$\bullet a|b \Leftrightarrow \exists c \in A : b = ac$$

$$\Downarrow$$

$$\bullet b \in aA \Leftrightarrow ba \in aA$$

$$a|b \wedge b|a$$

$$\bullet a,b \text{ asociados} \Leftrightarrow aA = bA$$

$$\Downarrow$$

$$b = a \cdot u$$

$$U(A)$$

$$\bullet \text{Sean } x,y \in \mathbb{Z}, \text{ con } x^2 | y^2 \Rightarrow x | y \quad (\text{P.41})$$

Sea $\theta: A \setminus U(A) \rightarrow B \setminus U(B)$

$$(1) a \text{ primo} \Leftrightarrow \forall b,c \in A : a|bc \Rightarrow a|b \text{ ó } a|c$$

$$(2) A \text{ dom, } a \in A \text{ primo} \Rightarrow a \text{ irreducible}$$

$$(3) A \text{ dom} \Rightarrow a \text{ irreducible en } aA \text{ maximal (de } A)$$

$$(4) A \text{ DIP, } a \text{ irreducible} \Rightarrow aA \text{ maximal}$$

$\bullet a$ REDUCIBLE (en A)

$$\Leftrightarrow \exists b,c \in A \setminus U(A) : a = bc$$

$\bullet a$ IRREDUCIBLE (en A)

$\Leftrightarrow a$ NO REDUCIBLE & NO UNIDAD

$\bullet a$ PRIMO si: el ideal aA es primo (P.41)

$$\varphi: A \longrightarrow B \text{ isomorf.} \quad (\text{P.41})$$

$$\Leftrightarrow \text{RED en } A \Leftrightarrow \varphi(a) \text{ RED en } B$$

Sea A dom. unitario

$$a \in A \text{ reducible}$$

$$u \in U(A)$$

$$\Downarrow \quad (\text{P.41})$$

$$b = a \cdot u \text{ es reducible}$$

$$\text{En } \mathbb{Z}, p \text{ primo} \Rightarrow p \text{ irreducible}$$

$$p \in \mathbb{Z} \setminus \{1,0,-1\} \text{ primo} \Rightarrow \mathbb{Z}_p \text{ cuerpo} \quad (\text{P.41})$$

(P.44)

M.C.M

M.C.D

Algoritmo de Euclides

\mathbb{Z}_n reducido

$\Downarrow \quad (\text{P.42})$

n es l.bre de cuadrados

Identidad de Bezout:

Dados a,b enteros positivos \Rightarrow

$$\exists x,y \in \mathbb{Z} : d := \text{mcd}(a,b) = ax + by$$

$$(d \in a\mathbb{Z} + b\mathbb{Z})$$

Th. fundamental aritmética (P.47)

Todo entero $n > 1$ se escribe de forma única como $p_1^{e_1} \dots p_r^{e_r}$, e_i enteros > 0 y p_i primos distintos 2 a 2.

ANILLOS DE RESTOS:

$$\bullet \mathbb{Z}_n = \frac{\mathbb{Z}}{n\mathbb{Z}}, n > 1$$

• Los ideales de \mathbb{Z}_n son los cocientes

$$\left\{ \frac{m\mathbb{Z}}{n\mathbb{Z}} : m|n, m \geq 0 \right\} \text{ son principales.}$$

además de \mathbb{Z}_n y el nulo.

$$\bullet \frac{\mathbb{Z}}{n\mathbb{Z}}$$
 ideal primo \Leftrightarrow maximal (P.50)
 Primo que divide a n

$$\bullet \tilde{\tau}: \mathbb{Z} \rightarrow \mathbb{Z}_n \quad (\text{P.51})$$

$$\bullet \tau_n: \mathbb{Z} \rightarrow \mathbb{Z}_n, x \mapsto [x]_n \text{ es el único homomorf. de } \mathbb{Z} \text{ en } \mathbb{Z}_n.$$

$$\bullet n > 1, m > 1. \text{ Existe un homomorf. } \tilde{\tau}: \mathbb{Z}_m \rightarrow \mathbb{Z}_n \Leftrightarrow n|m \text{ (único)}$$

$$p_1, \dots, p_r \text{ primos, } a_1, \dots, a_r \text{ enteros} \quad (\text{P.52})$$

$$U(\mathbb{Z}_n) \cong \prod_{i=1}^r U(\mathbb{Z}_{p_i^{e_i}})$$

grupos multiplicativos

$$ax + ny = b \text{ ec diofántica afín, tiene sol.} \Leftrightarrow d = \text{mcd}(a,n) | b$$

Ejemplos y métodos en (P.53)

Th. Wilson:

$$p \in \mathbb{Z}, \text{ primo} \Rightarrow (p-1)! \equiv -1 \pmod{p}$$

$$\bullet n > 4 \text{ entero no primo} \Rightarrow (n-1)! \equiv 0 \pmod{n} \quad (\text{P.55})$$

$$\bullet \forall n \in \mathbb{Z}_+, \exists \text{ infinitos primos} \equiv 1 \pmod{2^n} \quad (\text{P.57})$$

Suma de cuadrados (+ en (P.58))

Sea $n > 1$ entero l.bre de cuadrados

\Rightarrow Todo $x \in \mathbb{Z}_n$ es suma de dos cuadrados de elementos de \mathbb{Z}_n

Sean n, k enteros, son equivalentes:

i) k y n son primos entre sí

ii) $[k]_n$ es unidad en \mathbb{Z}_n

iii) $[k]_n \neq 0$ y no es divisor de 0

Obs: Si: n no l.bre de cuadrados, no tiene xqüé cumplirse: En \mathbb{Z}_4 solo $[0]_4, [1]_4$ son \square , luego $[3]_4$ no es suma de 2 \square