

## TEMA II.1. ARITMÉTICA DE ENTEROS.

- El *anillo de los enteros*:  $\forall a, b, c \in \mathbb{Z}$ ,

asociativa	$(a + b) + c = a + (b + c)$ ;	asociativa	$(a \cdot b) \cdot c = a \cdot (b \cdot c)$ ;
comutativa	$a + b = b + a$ ;	comutativa	$a \cdot b = b \cdot a$ ;
neutro	$a + 0 = a$ ;	unidad	$a \cdot 1 = a$ ;
opuesto	$a + (-a) = 0$ ;	distributiva	$a \cdot (b + c) = a \cdot b + a \cdot c$ .

- Divisibilidad.  $a|b \Leftrightarrow \exists m \in \mathbb{Z}$  tal que  $ma = b$ .

- Prop.:  $\forall a, b, c, m, n \in \mathbb{Z}$ , i)  $c|a$  y  $c|b \Rightarrow c|ma + nb$ ; ii)  $a|b$  y  $b|c \Rightarrow a|c$ ; iii)  $a|b$  y  $b|a \Rightarrow |a| = |b|$ .
- *Teorema de la división*:  $\forall a, b \in \mathbb{Z}, b \neq 0$ ,  $\exists c, r \in \mathbb{Z}$  únicos, tales que  $a = bc + r$  y  $0 \leq r < |b|$ .
- Máximo común divisor (*mcd*):  $mcd(a, 0) = |a|$  y si  $a, b \neq 0$ ,  $mcd(a, b) = d \Leftrightarrow d|a$  y  $d|b$  y  $d$  es máximo con estas condiciones.
- Prop.: Si  $b \neq 0$ ,  $mcd(a, b) = mcd(b, a) = mcd(\pm a, \pm b) = mcd(b, r)$  donde  $a = bc + r$  y  $0 \leq r < |b|$ .
- *Identidad de Bezout*:  $\forall a, b \in \mathbb{Z}$ , si  $d = mcd(a, b)$  entonces existen  $x, y \in \mathbb{Z}$  tales que  $d = ax + by$ .
- Propiedades del *mcd*:  $\forall a, b, m, d \in \mathbb{Z}$ ,
  - i)  $m|a$  y  $m|b \Rightarrow m|mcd(a, b)$ ;
  - ii)  $mcd(a, b) = d \Rightarrow a = a'd$  y  $b = b'd$  con  $mcd(a', b') = 1$ ;
  - iii) *Teorema de Euclides 1*:  $a|bc$  y  $mcd(a, b) = 1 \Rightarrow a|c$ .
- Números coprimos. Mínimo común múltiplo (*mcm*):  $a, b \neq 0$ ,  $mcm(a, b) = \min\{m \in \mathbb{N} : a|m \text{ y } b|m\}$ .
- Números primos:  $p \in \mathbb{N}$  es primo si  $p > 1$  y los únicos divisores de  $p$  son  $\pm 1$  y  $\pm p$ .
  - Prop.: Sea  $p$  primo.  $\forall a \neq 0$ , el *mcd*( $a, p$ ) es 1 o  $p$ ; si  $p|ab$  y  $p$  no divide a  $a$  entonces  $p|b$ .
  - *Teorema de Euclides 2*. Existen infinitos números primos.
  - *Teorema fundamental de la aritmética*.  $\forall a \neq 0, \pm 1$  existen unos únicos primos  $p_1, \dots, p_s$  tales que  $p_1 < \dots < p_s$  y  $a = \pm p_1^{n_1} \cdots p_s^{n_s}$ .

- Ecuaciones diofánticas.

Conjunto  $\mathcal{S}$  de soluciones de la ecuación  $ax + by = c$  con  $a, b, c \in \mathbb{Z}$  no nulos. Sea  $d = mcd(a, b)$ .

Si  $d$  no divide a  $c$ ,  $\mathcal{S} = \emptyset$ . Si  $d$  divide a  $c$ : 1º se hallan  $a', b', c' \in \mathbb{Z}$  tales que  $a = a'd$ ,  $b = b'd$  y  $c = c'd$ ; 2º se hallan  $x'_0, y'_0 \in \mathbb{Z}$  tales que  $a'x'_0 + b'y'_0 = 1$ ; 3º se hallan  $x_0, y_0 \in \mathbb{Z}$  tales que  $a'x_0 + b'y_0 = c'$ ;

$$4^{\text{o}} \mathcal{S} : \begin{cases} x = x_0 + b't \\ y = y_0 - a't \end{cases} t \in \mathbb{Z}.$$

## TEMA II.2. CONGRUENCIAS.

- $a \equiv b \pmod{n}$ .  $\mathbb{Z}_n = \{\bar{0}, \bar{1}, \bar{2}, \dots, \bar{n-1}\}$ .  $\bar{a} + \bar{b} = \overline{a+b}$ ;  $\bar{a} \cdot \bar{b} = \overline{ab}$ .
- Las unidades de  $\mathbb{Z}_n$ :  $U(\mathbb{Z}_n) = \{\bar{m} \in \mathbb{Z}_n : \exists \bar{l} \in \mathbb{Z}_n \text{ tal que } \bar{m} \cdot \bar{l} = \bar{1}\} = \{\bar{m} \in \mathbb{Z}_n : m \text{ y } n \text{ coprimos}\}$ .
- La  $\varphi$  de Euler:  $\varphi(n) = \text{card}(U(\mathbb{Z}_n))$ .
  - Prop.: Si  $p$  es primo  $\varphi(p) = p-1$  y  $\varphi(p^m) = p^m - p^{m-1}$ ; si  $m$  y  $n$  son coprimos  $\varphi(mn) = \varphi(m)\varphi(n)$ .
  - Teorema de Euler: Sean  $a, n \in \mathbb{Z}$  coprimos, con  $n > 1$ . Entonces  $\overline{a^{\varphi(n)}} = \bar{1}$  en  $\mathbb{Z}_n$ .
- Ecuaciones en  $\mathbb{Z}_n$ :  $\bar{a}x = \bar{b}$  en  $\mathbb{Z}_n$ .
  - Si el *mcd*( $a, n$ ) no divide a  $b$ , la ecuación no tiene solución.
  - Si  $d = mcd(a, n)$  divide a  $b$  hay  $d$  soluciones:  $\bar{x}_0, \bar{x}_0 + \bar{n'}, \dots, \bar{x}_0 + \overline{(d-1)n'}$ , donde  $n = n'd$  y  $x_0$  es la primera componente de una solución  $(x_0, y_0)$  de la ecuación  $ax - ny = b$  en  $\mathbb{Z}$ .