

## DIVISIBILIDAD

1. Todo entero (salvo cero) divide a cero:

$$Div(0) = \mathbb{Z} - \{0\}$$

2. Si  $d$  divide a  $a$ , también a su inverso:

$$d|a \Leftrightarrow -d|a \wedge d|-a$$

3. Un divisor es menor que lo que divide.

$$d|a \wedge a \neq 0 \Rightarrow d \leq |a|$$

4. Sólo 1 y  $-1$  son inversibles en  $\mathbb{Z}$ .

5. Antisimetría

$$d|a \wedge a|d \Leftrightarrow a = \pm b$$

Además:

1. Uno divide a todo y todo se divide a sí mismo.

$$\forall a \in \mathbb{Z} 1|a, 1|-a, a|a, -a|a$$

2. Sean  $a, b, d \in \mathbb{Z}, d \neq 0$

$$d|a \wedge d|b \Rightarrow d|a + b \wedge d|ab$$

3. Todo divide un múltiplo de lo que divide.

$$\forall k \in \mathbb{Z} d|a \Rightarrow d|ka$$

4. La potencia de un divisor divide la potencia de lo que divide.

$$d|a \Rightarrow d^n|a^n$$

## Congruencia

1.

$$\forall a_1, a_2, b_1, b_2 \in \mathbb{Z} a_1 \equiv b_1(d) \wedge a_2 \equiv b_2(d) \Rightarrow a_1 + a_2 \equiv b_1 + b_2(d)$$

2.

$$\forall a_1, a_2, b_1, b_2 \in \mathbb{Z} a_1 \equiv b_1(d) \wedge a_2 \equiv b_2(d) \Rightarrow a_1 a_2 \equiv b_1 b_2(d)$$

3.

$$\forall a, b, k \in \mathbb{Z} a \equiv b(d) \Rightarrow ka \equiv kb(d)$$

## Congruencia y resto

Sea  $d \in \mathbb{Z}, d \neq 0$ . Entonces:

1.

$$a \equiv r_d(a) (d), \quad \forall a \in \mathbb{Z}$$

2.

$$a \equiv r(d) \wedge 0 \leq r < |d| \Rightarrow r = r_d(a)$$

3.

$$r_1 \equiv r_2(d) \wedge 0 \leq r_1, r_2 < |d| \Rightarrow r_1 = r_2$$

4.

$$a \equiv b(d) \Leftrightarrow r_d(a) = r_d(b)$$