

*** III ***

RICHIAMI

Notazione:

Dati $a, b \in \mathbb{Z}$ scriviamo $a|b \Leftrightarrow \exists c \in \mathbb{Z}$ tale che $b = ac$ ($\Leftrightarrow$ l'equazione $ax = b$ è risolubile).

Osservazione 1: Dati $a, b, n \in \mathbb{Z}$ si ha:

$a|b \Leftrightarrow -a|b \Leftrightarrow a|-b$; equivalentemente:

$$\{\text{divisori di } n\} = \{\text{divisori di } -n\} = -\{\text{divisori di } n\}$$

Osservazione 2: Dati $a, b, c \in \mathbb{Z}$ si ha:

$$a|\pm a$$

$$a|b \text{ e } b|a \Leftrightarrow a = \pm b$$

$$a|b \text{ e } b|c \Rightarrow a|c$$

Osservazione 3: Dati $a, b, c \in \mathbb{Z}$ si ha:

$$a|b \Rightarrow ac|bc;$$

$$ac|bc, \ c \neq 0 \Rightarrow a|b$$

$$a|b \Rightarrow a|bc$$

$$a|b \text{ e } a|c \Rightarrow a|b + c$$

Osservazione 4: Dato $a \in \mathbb{Z}$ si ha:

$$1|a \text{ e } a|0;$$

$$a|1 \Leftrightarrow a|b \ \forall b \Leftrightarrow a = \pm 1$$

$$0|a \Leftrightarrow b|a \ \forall b \Leftrightarrow a = 0;$$

Definizione:

Dati $a, b \in \mathbb{Z}$ si dice massimo comun divisore (MCD) tra a e b un numero $d \in \mathbb{Z}$ tale che:

i) $d|a$ e $d|b$;

ii) se $d'|a$ e $d'|b$ allora $d'|d$

Osservazione:

i) $d \text{ è } MCD(a, b) \Leftrightarrow -d \text{ è } MCD(a, b)$;

ii) se d_1 e d_2 sono MCD tra a e b allora $d_1 = \pm d_2$.

In particolare il massimo comun divisore è *definito a meno del segno* e la condizione aggiuntiva $d \geq 0$ definisce univocamente *il* massimo comun divisore *non negativo*.

Osservazione:

- i) a è $MCD(a, b) \Leftrightarrow a|b$; in particolare a è $MCD(a, 0)$ e $MCD(0, 0) = 0$.
- ii) $a = bq + r \Rightarrow MCD(a, b) = MCD(b, r)$.
- iii) d è $MCD(a, b) \Rightarrow dc$ è $MCD(ac, bc) \forall c$.
- iv) se d è $MCD(a, b)$ allora $d'|a$ e $d'|b \Rightarrow |d'| \leq |d|$.
- v) $MCD(a, b) = 1, a|bc \Rightarrow a|c$.

Definizione

Dati $a, b \in \mathbb{Z}$ si dice minimo comune multiplo (mcm) tra a e b un numero $m \in \mathbb{Z}$ tale che:

- i) $a|m$ e $b|m$;
- ii) se $a|m'$ e $b|m'$ allora $m|m'$

Osservazione:

- 1) $mcm(a, b)$ è definito a meno del segno.
- 2) $mcm(a, 0) = 0$ per ogni $a \in \mathbb{Z}$.

Esercizio

Siano $a, b \in \mathbb{Z}$ non entrambi nulli e sia d un $MCD(a, b)$.

Dimostrare che $\frac{ab}{d}$ è $mcm(a, b)$.

E se $a = b = 0$?

Esercizio

(1) Siano $a, b, c \in \mathbb{Z}$; (a, b, c) si dice terna pitagorica se $a^2 + b^2 = c^2$.

Sia (a, b, c) una terna pitagorica; dimostrare che:

- i) $(-a, b, c), (a, -b, c), (a, b, -c)$ sono terne pitagoriche;
 - ii) Sia $d \in \mathbb{Z}$; allora $d|a$ e $d|b \Leftrightarrow d|a$ e $d|c \Leftrightarrow d|b$ e $d|c \Leftrightarrow d|a, d|b$ e $d|c$;
equivalentemente $MCD(a, b) = MCD(a, c) = MCD(b, c) = MCD(a, b, c)$.
 - iii) $4|a$ oppure $4|b$;
 - iv) se $4|a$ e $4 \nmid b$ allora $MCD(c - b, c + b) = 2MCD(b, c)$.
- (2) Una terna pitagorica (a, b, c) si dice ridotta se:
- a) $a, b, c \geq 0$;
 - b) $MCD(a, b) = 1$;
 - c) $4|a$.

Dimostrare che esistono infinite terne pitagoriche ridotte e costruirle.