

Def- Dato $a \in \mathbb{Z}$, denotiamo con $D(a) = \{x \in \mathbb{Z} \mid x|a\}$ l'insieme dei suoi **divisori**.

$$D(a) \subseteq \mathbb{Z}$$

Se $a \neq -1, 1$ allora $|D(a)| \geq 4$ $\{-a, a, 1, -1\} \subseteq D(a)$

e $D(a)$ è un insieme finito - $D(-1) = D(1) = \{-1, 1\}$
 \hookrightarrow se $a \neq 0$! Se $a=0$, $D(0) = \mathbb{Z}$

LEMMA

$\forall x, y, k, z \in \mathbb{Z}$ tali che $x = ky + z$, allora $D(x) \cap D(y) = D(y) \cap D(z)$ -

Dim
Vediamo che $D(x) \cap D(y) \subseteq D(y) \cap D(z)$ -

Sia $n \in D(x) \cap D(y) \Rightarrow n|x$ e $n|y$ $\Rightarrow \exists h, l$ tali che $x = hn$
 $y = ln$

allora dalle ipotesi, $z = x - ky = hn - khn = (l-kh)n \Rightarrow n|z$ -

$\Rightarrow n \in D(y) \cap D(z)$ -

Vediamo che $D(y) \cap D(z) \subseteq D(x) \cap D(y)$ - Per definizione, se $n \in D(y) \cap D(z)$

allora $n|y$ e $n|z \Rightarrow n|ky \Rightarrow n|\underbrace{ky+z}_x \Rightarrow n \in D(x) \cap D(y)$ -

Def- Sia $p \in \mathbb{Z} \setminus \{-1, 1\}$ - p è detto **Primo** se $D(p) = \{-p, p, -1, 1\}$ -

Def- Dati $a, b \in \mathbb{Z} \setminus \{0\}$, $d \in \mathbb{Z}$ è **massimo comune divisore** di a e b se:
(MCD)

① $d \in D(a) \cap D(b)$ ($d|a$ e $d|b$)

② $\forall t \in \mathbb{Z}$ tale che $t|a$ e $t|b \Rightarrow t|d$ -

Proposizione

Dati $a, b \in \mathbb{Z} \setminus \{0\}$, si ha:

Dati $a, b \in \mathbb{Z} \setminus \{0\}$, si ha:

- ① d è un MCD per a, b $\Leftrightarrow -d$ è un MCD per a, b
② Se d è un MCD di a, b , gli unici MCD di a, b sono d e $-d$.

DM

- ① " \Rightarrow " Ipotesi: d è un MCD per a, b
Tesi: $-d$ è un MCD per a, b

(i) Osserviamo che se d è un MCD per $a, b \Rightarrow \exists h, k$ t.c.

$$a = hd \quad \text{e} \quad b = kd \Rightarrow a = (-h)(-d) \quad \text{e} \quad b = (-k)(-d)$$

$$\Rightarrow \text{quindi } -d \mid a \quad \text{e} \quad -d \mid b \Rightarrow -d \in D(a) \cap D(b)$$

(ii) Sia t tale che $t \mid a$ e $t \mid b$ - Per ipotesi d è un MCD \Rightarrow
 $t \mid d$, così $\exists k$ t.c. $d = kt$ - Allora $-d = (-k)t$ e
quindi $t \mid (-d)$ CVD

- " \Leftarrow " Ipotesi: $-d$ è un MCD
Tesi: d è un MCD

È uguale al verso " \Rightarrow " scambiand d e $-d$ - (Per esercizio)

- ② Supponiamo che d è un MCD per ipotesi e per contraddizione sia t un
altro MCD per a, b - Vediamo che deve essere $t = d$ oppure $t = -d$ -

Se t è un altro MCD per a, b ho $t \mid d$ e $d \mid t$

Quindi $\exists k, h$ tali che $d = tk$ e $t = dh$ $\Rightarrow d = dkh$

perché siamo in \mathbb{Z} , si ha $hk = 1$ $\begin{cases} h=1 \text{ e } k=1 \Rightarrow t=d \\ h=-1 \text{ e } k=-1 \Rightarrow t=-d \end{cases}$

CVD

CONVENTIONE. $\forall a, b \in \mathbb{Z} \setminus \{0\}, \quad \text{MCD}(a, b) = d \geq 0$

$$\text{MCD}(6, 3) = \{-3, 3\} = 3$$

OSSERVAZIONE: $d = \text{MCD}(a, b) = \text{MCD}(-a, b) = \text{MCD}(-a, -b) = \text{MCD}(a, -b)$

[LEMMA]

$\forall a, b, d \in \mathbb{Z}$ con $d \geq 0$

$$d = \text{MCD}(a, b) \Leftrightarrow D(d) = D(a) \cap D(b)$$

DIM

" \Rightarrow "

Sia $n \mid d \Rightarrow d = n \cdot d'$

$$d \in \text{MCD}(a, b) \Rightarrow d \mid a \text{ e } d \mid b \Rightarrow a = k \cdot d \text{ e } b = h \cdot d \Rightarrow$$

$$\Rightarrow a = k \cdot d \cdot n \text{ e } b = h \cdot d \cdot n \Rightarrow n \mid a \text{ e } n \mid b \Rightarrow n \in D(a) \cap D(b)$$

$\& n \in D(a) \cap D(b) \Rightarrow n \mid a \text{ e } n \mid b \text{ e per definizione } d \mid n \text{ o } d \mid n \cdot d$

$$\Rightarrow n \in D(d)$$

" \Leftarrow " $\& D(a) \cap D(b) = D(d) \Rightarrow$ Poché $d \in D(d)$, si ha $d \in D(a) \cap D(b)$

$\Rightarrow d \mid a \text{ e } d \mid b$ (2 della def di MCD)

Sia $t \in D(a) \cap D(b) \Rightarrow t \mid a \text{ e } t \mid b$ - Poché $D(a) \cap D(b) = D(d)$

$\Rightarrow t \in D(d) \Rightarrow t \mid d$ (2 della def di MCD)

Abbiamo dimostrato che $d = \text{MCD}(a, b)$ \square

[PROPOSIZIONE]

$\forall a, b \in \mathbb{Z}$ $\text{MCD}(a, b)$ esiste sempre -

DIM ALGORITMO delle DIVISIONI SUCCESSIVE

Sia $b > 0$ - (NB - se $b = 0$ $\text{MCD}(a, 0) = a$)

$\exists q_1, r_1 \in \mathbb{Z}$ t.c.

$\exists q_2, r_2 \in \mathbb{Z}$

$\exists q_3, r_3 \in \mathbb{Z}$

$$a = q_1 \cdot b + r_1$$

$$b = q_2 \cdot r_1 + r_2$$

$$r_2 = q_3 \cdot r_3 + r_4$$

$$0 \leq r_1 < b$$

$$0 \leq r_2 < r_1 < b$$

$$0 \leq r_3 < r_2 < r_1 < b$$

$$\exists q_3, r_3 \in \mathbb{Z}$$

$$r_2 = \overbrace{q_3}^{\vdots} \cdot r_2 + r_3$$

$$0 \leq r_3 < r_2 < r_1 < b$$

Ad un certo punto il resto sarà zero.

$$r_{t-1} = q_{t+1} \cdot r_t + r_{t+1} \quad \text{con } r_{t+1} = 0$$

$$\text{tb} \quad b > r_1 > r_2 > \dots > r_t > r_{t+1} = 0$$

$$D(a) \cap D(b) = D(b) \cap D(r_1) = D(r_1) \cap D(r_2) = \dots =$$

$$\dots = D(r_{t-1}) \cap D(r_t) = D(r_t) \cap \underbrace{D(r_{t+1})}_{D(0)} = D(r_t)$$

$$D(0) = \mathbb{Z}$$

$$D(r_t) \cap \mathbb{Z} = ?$$

Dall'ultimo lemma, si ha $r_t = \text{MCD}(a, b)$ □

ESEMPIO $\text{MCD}(1218, 132)$

$$\begin{aligned} 1218 &= 132 \cdot 9 + 30 \\ 132 &= 30 \cdot 4 + 12 \\ 30 &= 12 \cdot 2 + 6 \\ 12 &= 6 \cdot 2 + 0 \end{aligned}$$

$$\Rightarrow \text{MCD}(1218, 132) = 6 -$$

DEF - $a, b \in \mathbb{Z}$ sono detti **COPRIMI** se $\text{MCD}(a, b) = 1$ -

LEMMA

① $a, p \in \mathbb{Z}$, con p primo - se $p \nmid a$ allora $\text{MCD}(a, p) = 1$

$$D(p) = \frac{\text{def}}{\{-1, 1, p, -p\}} \Rightarrow \text{se } p \nmid a \quad p \notin D(a) \text{ e } -p \notin D(a)$$

$$D(p) \cap D(a) = \{-1, 1\} = D(1) \quad \square$$

② Se $a, b \in \mathbb{Z} \setminus \{0\}$, $d = \text{MCD}(a, b)$, allora $\exists a', b' \in \mathbb{Z}$ tali che

$$a = a' d, \quad b = b' d \quad \text{con} \quad \text{MCD}(a', b') = 1 -$$

$$a = a' d, \quad b = b' d \quad \text{con} \quad \text{MCD}(a', b') = 1$$

$\hookrightarrow (\text{sd})$

TEOREMA di BEZOUT \Rightarrow sd

$\forall a, b \in \mathbb{Z}, \text{ se } d = \text{MCD}(a, b) \exists u, v \in \mathbb{Z} \text{ tali che } d = ua + vb$

ESEMPIO $\text{MCD}(1218, 132)$

$$\begin{aligned}
 1218 &= 132 \cdot 9 + 30 \\
 132 &= 30 \cdot 4 + 12 \\
 30 &= 12 \cdot 2 + 6 \\
 &\quad \xrightarrow{\hspace{10em}} 30 = 1218 - 9 \cdot 132 = 1218 + (-9) \cdot 132 \\
 &\quad 12 = 132 + (-4) \cdot 30 \\
 &\quad \rightarrow b = 30 - 2 \cdot 12 = 30 + (-2) \cdot 12 \\
 &\quad b = 30 + (-2) \cdot 12 = \\
 &\quad = 30 + (132 + (-4) \cdot 30) \cdot (-2) = \\
 &\quad = 30 + (-2) \cdot 132 + 8 \cdot 30 = \\
 &\quad = 9 \cdot 30 + (-2) \cdot 132 \\
 &\quad = 9(1218 + (-9) \cdot 132) + (-2) \cdot 132 = \\
 &\quad = 9 \cdot 1218 + (-81) \cdot 132 + (-2) \cdot 132 = \\
 &\quad = 9 \cdot 1218 + (-83) \cdot 132 \\
 \Rightarrow b &= \underbrace{9 \cdot 1218}_a + \underbrace{(-83) \cdot 132}_b
 \end{aligned}$$

ESEMPIO

$\text{MCD}(689, 534)$

$$689 = 534 \cdot 1 + 155$$

$$534 = 155 \cdot 3 + 69$$

$$534 = 155 \cdot 3 + 69$$

$$155 = 69 \cdot 2 + 17$$

$$69 = 17 \cdot 4 + 1 \quad \text{MCD}$$

$$17 = 1 \cdot 17 + 0$$

$$x - 4(y + (-2)x) = x - 4y + 8x \\ = 9x - 4y$$

$$\begin{aligned} 1 &= 69 - 17 \cdot 4 = 69 + (-4) \cdot 17 = \underbrace{69 + (-4)}_{\text{x}} \underbrace{(155 + (-2) \cdot 69)}_{\text{y}} = \\ &= 69 + (-4) \cdot 155 + (+8) \cdot 69 = (-4) \cdot 155 + (9) \cdot 69 = \\ &= (-4) \cdot 155 + 9 \cdot (534 + (-3) \cdot 155) = \\ &= \cancel{(-4) \cdot 155} + 9 \cdot 534 + \cancel{(-27) \cdot 155} = \\ &= \cancel{(-31) \cdot 155} + 9 \cdot 534 = \\ &= (-31) \cdot (689 - 534) + 9 \cdot 534 = \\ &= (-31) \cdot 689 + \cancel{31 \cdot 534} + \cancel{9 \cdot 534} = \\ &= (-31) \cdot 689 + (40) \cdot 534 \\ \Rightarrow 1 &= \boxed{(-31) \cdot 689 + 40 \cdot 534} \end{aligned}$$

TEOREMA FONDAMENTALE DELL'ARITMETICA (\mathbb{N}) se

Sia $z \in \mathbb{Z} \setminus \{0, \pm 1\}$. $\exists k \in \mathbb{N}$ ed esistono $p_1, \dots, p_k \in \mathbb{Z}$ numeri primi tali che $z = p_1 \cdot \dots \cdot p_k$.

Inoltre la rappresentazione è unica a meno del segno dei fattori e dell'ordine.

ESEMPIO

$$6 = 2 \cdot 3 = (-2)(-3) = (-3)(-2)$$