

(M) ATEMATICA (D) ISCRETA (H) (A)

11-09-2015 - 10:00 - 90%

Tutti i capitoli sono disponibili anche

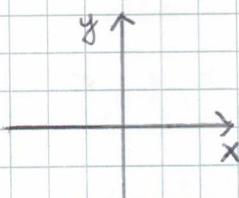
PRODOTTO CARTESIANO

$$S, T \subseteq X$$

$$S \times T := \{(x, y) \mid x \in S \wedge y \in T\}$$

Insieme delle coppie ordinate

$\mathbb{R} \times \mathbb{R} \rightarrow$ il piano cartesiano



Essendo coppie ordinate, l'ordine e'

importante: $(x, y) \neq (y, x)$

$$A = \{a, b, c\} \quad B = \{1, 2\}$$

$$\text{Esempio: } A \times B = \{(a, 1), (a, 2), (b, 1), (b, 2), (c, 1), (c, 2)\}$$

Se $|A| = m$ e $|B| = n$ allora $|A \times B| = |A| \cdot |B|$

per insiemi finiti

N.B. $C \subseteq A \times B$ se $C \subseteq A_1 \times B_1$ con $A_1 \subseteq A$ e $B_1 \subseteq B$
anche se

Un sottoinsieme del prodotto non deve per forza provengere dal prodotto di due sottoinsiemi:

$$\text{Esempio: } C = \{(a, 1), (b, 2)\} \subseteq A \times B$$

Ma $A_1 \not\subseteq A$ e $B_1 \not\subseteq B$ t.c. $C \neq A_1 \times B_1$

$A_1 = \{a, b\}$ $B_1 = \{1, 2\}$; $A_1 \times B_1$ e' piu' grande di C
(ha 4 elementi)

quindi in realtà $C \not\subseteq A$

DEF DI RELAZIONE

Una relazione tra $S \times T$ è un sottoinsieme di $S \times T$

1) RELAZIONE RIFLESSIVA

$R \subseteq S \times S$ è una r. riflessiva se $(x, x) \in R, \forall x \in S$

$x R x$, esempio: $\mathbb{N} \times \mathbb{N}$

$\geq, \leq, =$ e $\{(x, x) | x \in \mathbb{N}\}$

per ogni S , si definisce $\Delta_S = \{(x, x) | x \in S\}$ diagonale S

Osservazione: $R \subseteq S \times S$ è riflessiva $\Leftrightarrow \Delta_S \subseteq R$

2) RELAZIONE SIMMETRICA

$R \subseteq S \times S$ è simmetrica ($\forall (x, y) \in R$: allora $(y, x) \in R$)

$x R y \rightarrow y R x$

3) RELAZIONE ASIMMETRICA

$R \subseteq S \times S$ è asimmetrica $\Leftrightarrow ((x, y) \in R \wedge (y, x) \in R \rightarrow x = y)$

Esempio: \prec

4) RELAZIONE TRANSITIVA

$R \subseteq S \times S$ è transitiva $\Leftrightarrow ((x, y) \in R \wedge (y, z) \in R \rightarrow (x, z) \in R)$

Esempio: divide "a|b", \leq, \geq

Se $a|b$ e $b|c \rightarrow a|c$

{ il divide è anche riflessivo
il divide in \mathbb{N} è asimmetrico

$a|b$ e $b|a \rightarrow a = b$

$$\begin{cases} b = ka \\ a = lb \end{cases} \Rightarrow b = (kl)a \Rightarrow lk = 1 \Rightarrow l = k = 1$$

il divide non è asimmetrica in $T_L, -111 \neq 11-1$ ma ~~1 \neq -1~~

tuttavia resta riflessiva

$$T \times T \leftrightarrow W \times V = T \times V$$

5) RELAZIONE D'ORDINE (una relazione che è riflessiva, simmetrica e transitiva)

Esempio: \leq, \geq , divide su \mathbb{N}

6) RELAZIONE DI EQUIVALENZA (una relazione che è riflessiva, simmetrica e transitiva)

Esempio: ugualanza

7) APPLICAZIONE

Una applicazione $f \in S \times T$ è una relazione t.c.

$$\forall x \in S \exists! y \in T : (x, y) \in f$$

o anche $f(x) = y$

Esempio di dim $S \times T = V \times W \Leftrightarrow S = V \wedge T = W$

$$S \times T = V \times W \Leftrightarrow S = V \wedge T = W$$

$$\rightarrow \text{Up} \ L \ S \times T = V \times W$$

$$\forall (x, y) \in S \times T \rightarrow (x, y) \in V \times W \quad \times$$

$$\forall (z, t) \in V \times W \rightarrow (z, t) \in S \times T \quad \star \star$$

sia $x \in S$ qualsiasi, allora $\forall y \in T$

$$(x, y) \in S \times T \text{ per definizione} \rightarrow \text{da Up. } (x, y) \in V \times W$$

$$\rightarrow x \in V \wedge y \in W \rightarrow S \subseteq V \wedge T \subseteq W$$

Viceversa, $\forall z \in V \wedge \forall t \in W, (z, t) \in V \times W \rightarrow \text{da Up. } (z, t)$

$$S \times T \rightarrow z \in S \wedge t \in T \rightarrow V \subseteq S \wedge W \subseteq T$$

$$S \subseteq V \wedge V \subseteq S \rightarrow S = V$$

$$T \subseteq W \wedge W \subseteq T \rightarrow T = W$$

N.B. l'inclusione è una relazione asimmetrica

$$\leftarrow S \wedge S = V \wedge T = W \rightarrow S \times T = V \times W$$

banale

□

ALTRÉ RELAZIONI

1) RELAZIONE TOTALE

Dati S, T insiemi, $R \subseteq S \times T$ è detta totale se $R = S \times T$

$$\forall (x, y) \in S \times T, x R y$$

2) RELAZIONE VUOTA

$R \subseteq S \times T$ è una relazione vuota se $R = \emptyset$

3) RELAZIONE OPPOSTA

R^{op} è detta relazione opposta di R

$$(x, y) \in R^{op} \Leftrightarrow (y, x) \in R$$

Esempio:

$$\text{Se } R = \leq, \text{ si avrà } R^{op} = \geq$$

4) RELAZIONE BINARIA - TERNARIA - N-ARIA

$R \subseteq S \times S$ è detta relazione binaria

$R \subseteq S \times S \times S$ è detta ternaria

$R \subseteq \underbrace{S \times \dots \times S}_m$ è detta n-aria

$$\mathbb{R}^5 = \{(a, b, c, d, e) \mid a, b, c, d, e \in \mathbb{R}\}$$

$$(1, \sqrt{2}, 3, -7, \pi) \in \mathbb{R}^5$$

OSSERVAZIONE: Se $|S| = m$ e $|T| = n$

Quante sono le possibili relazioni tra S e T ?

$$|P(S \times T)| = 2^{|S \times T|} = 2^{m \cdot n}$$

APPLICAZIONI

S, T insiemi

$f \subseteq S \times T$ è applicazione ($f: S \rightarrow T$) se $\forall x \in S \exists ! y \in T : (x, y) \in f$
 $(f(x) = y)$

$$S = \{1, 2, 3\} \quad T = \{a, b, c\}$$

$$f_1 = \{(1, a), (1, b), (2, c)\}$$

$$f_2 = \{(1, a), (2, a), (3, c)\}$$

f_1 non è applicazione

f_2 è applicazione (non ci sono coppie diverse con la stessa componente in x)

$$f_1 \subseteq \mathbb{R} \times \mathbb{R}$$

$$f_1 = \{(x, y) \mid x = y^2\}$$

$$f_2 = \{(x, y) \mid y = x^2\}$$

f_1 non è applicazione : $(4, 2), (4, -2) \in f_1$

f_2 è applicazione : $(2, 4), (-2, 4) \in f_2$

DEFINIZIONE :

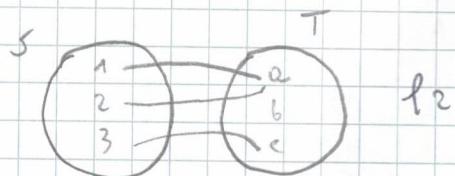
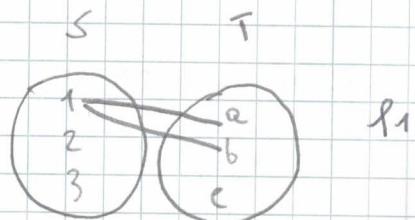
$f \subseteq S \times T$ applicazione, S è detto **DOMINIO** di f e

T è detto **CODOMINIO** di f

$\text{Im}(f) \subseteq T$ **IMMAGINE** di f

$$\text{Im}(f) := \{y \in T \mid (x, y) \in f\}$$

$$= \{f(x) \mid x \in S\}$$



DEFINIZIONE:

Se $S = \mathbb{N}$ o $S = \mathbb{N}_0$ $f \in S \times T$ è detta successione ($x \mapsto f(x)$)

$f \in \mathbb{N}_0 \times T$ $f: \mathbb{N}_0 \rightarrow T$ $f(m) = a_m, b_m, c_m$

(m, a_m) dove $a_m \in T$

Esempio: $f(m) = 2 + m$ $f \in \mathbb{Z} \times \mathbb{Z}$

$f(m) = m^3 + 1$ $f \in \mathbb{Z} \times \mathbb{N}$

$f(-2) = -7 \notin \mathbb{N}$

È comunque una relazione (non totale) ma non è applicazione
perché $f(-2) \notin \mathbb{N}$ cioè $\nexists m \in \mathbb{N} \mid -2 = f(m)$

Le x del dominio devono comparire tutte soltanto una volta

PROPOSIZIONE

$x_1, x_2 \in S \quad \forall f \in S \times S$ applicazione si ha:

- 1) Se $x_1 \subseteq x_2 \rightarrow f(x_1) \subseteq f(x_2)$ non vale ↗, né il viceversa
 - 2) $f(x_1 \cup x_2) = f(x_1) \cup f(x_2)$
 - 3) $f(x_1 \cap x_2) \subseteq f(x_1) \cap f(x_2)$
 - 4) $f(x_1 \setminus x_2) \supseteq f(x_1) \setminus f(x_2)$
- $f[X] = f(X) = \{f(x) \mid x \in X\}$

DIMOSTRAZIONI

1)



$x_1 \subseteq x_2$

th $f(x_1) \subseteq f(x_2)$

di applicazione

$y \in f(x_1)$ per definizione $\exists x \in X_1 \mid (x, y) \in f \quad (f(x) = y)$
 poiché $X_1 \subseteq X_2$, si ha $x \in X_2 \rightarrow y = f(x) \in f[X_2]$

perché $X_1 \subsetneq X_2 \not\Rightarrow f[X_1] \subsetneq f[X_2]$

Se $f \subseteq \mathbb{R} \times \mathbb{R}$, $f(x) = 3 \quad \forall x \in \mathbb{R}$

$$X_1 = \{1, 2, 5\}$$

$$X_1 \subsetneq X_2 \text{ ma } f[X_1] = \{3\} = f[X_2]$$

$$X_2 = \{1, 2, 3, 4, 5\}$$

$$f[X_1] = \{f(1), f(2), f(5)\} = \{3\}$$

$$f[X_2] = \{f(1), f(2), f(3), f(4), f(5)\} = \{3\}$$

3)

$$f(X_1 \cap X_2) \subseteq f(X_1) \cap f(X_2)$$

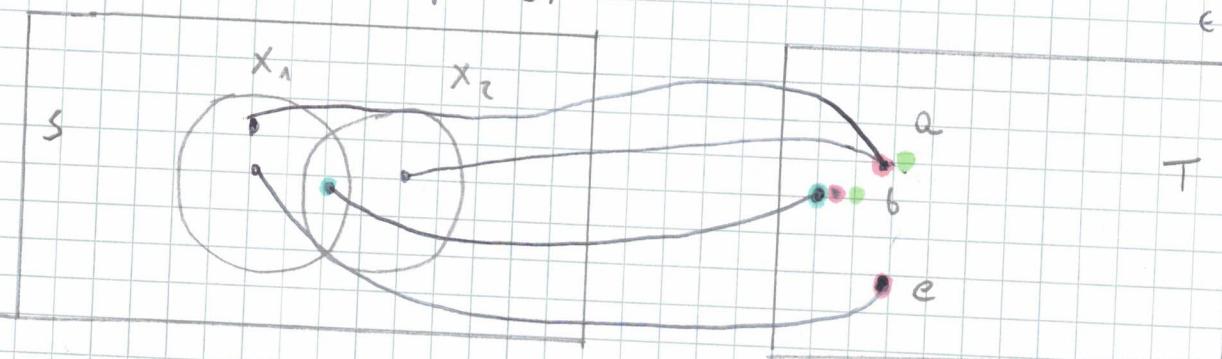
per def. di applicazione

$$y \in f(X_1 \cap X_2) \rightarrow \exists x \in X_1 \cap X_2 \mid (x, y) \in f$$

per definizione di intersezione $\rightarrow x \in X_1 \wedge x \in X_2 \quad \{(x, y) \in f\}$

$$\rightarrow y \in f(X_1) \wedge y \in f(X_2)$$

$$\rightarrow y \in f(X_1) \cap f(X_2)$$



$$f(X_1) \cap f(X_2) \supseteq f(X_1 \cap X_2), \quad f(X_1) \cap f(X_2) = \{a, b\}$$

Quindi sono diversi (per questo

vale \subseteq e non $=$)

$$f(X_1 \cap X_2) = \{b\}$$

DEFINIZIONE

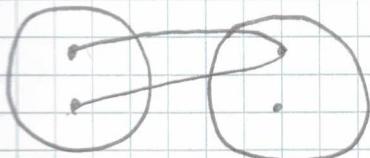
$f \in S \times T$ è INIETTIVA se:

$$x_1, x_2 \in S \text{ con } x_1 \neq x_2 \rightarrow f(x_1) \neq f(x_2)$$

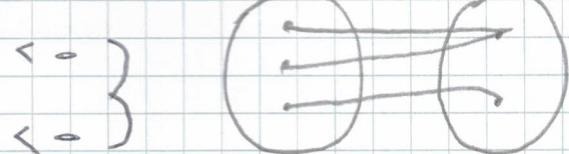
$f \in S \times T$ è SURIETTIVA se:

$$\text{Im}(f) = T$$

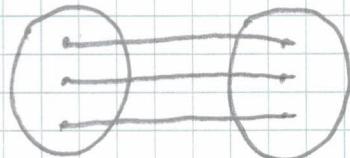
$f \in S \times T$ è BIETTIVA se è sia iniettiva che suriettiva



mè iniettiva
mè suriettiva



suriettiva ma non iniettiva



è biettiva

PROPOSIZIONE

Dati S, T finiti e non vuoti

$$\exists f: S \rightarrow T \text{ iniettiva} \Leftrightarrow |S| \leq |T|$$

$$\exists f: S \rightarrow T \text{ suriettiva} \Leftrightarrow |S| \geq |T|$$

$$\exists f: S \rightarrow T \text{ biettiva} \Leftrightarrow |S| = |T|$$

DEFINIZIONE DI CONTROIMMAGINE DI Y

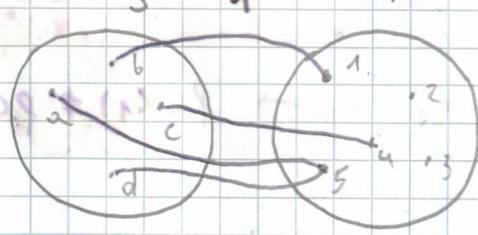
$f \in S \times T$ applicazione e preso $y \in T$

$$f^{-1}[y] = f^{-1}(y) = \{x \in S \mid f(x) \in y\}$$

$$= \{x \in S \mid (x, y) \in f \text{ per qualche } y \in y\}$$

cioè l'insieme delle x in relazione con qualche elemento di y

Esempio:



$$x = \{1, 4, 5\}$$

$$f^{-1}(y) = S$$

S prende sia a che d

$$f(S) = \{1, 4, 5\}$$

$$f(\{b, d\}) = \{1, 5\}$$

$$f^{-1}(\{1, 5\}) = \{b, d, a\}$$

TEOREMA:

- 1) $y_1 \subseteq y_2 \rightarrow f^{-1}(y_1) \subseteq f^{-1}(y_2)$
- 2) $f^{-1}(y_1 \cup y_2) = f^{-1}(y_1) \cup f^{-1}(y_2)$
- 3) $f^{-1}(y_1 \cap y_2) = f^{-1}(y_1) \cap f^{-1}(y_2)$
- 4) $f^{-1}(y_1 \setminus y_2) = f^{-1}(y_1) \setminus f^{-1}(y_2)$
- 5) $\forall x \in S, x \in f^{-1}(f(x))$
- 6) $f(f^{-1}(y)) \subseteq y$

DEFINIZIONE

$$f \subseteq S \times T, g \subseteq T \times W$$

definisce la **COMPOSIZIONE DI FUNZIONI** $g \circ f$ "f composto g"

$$g \circ f \subseteq S \times W$$

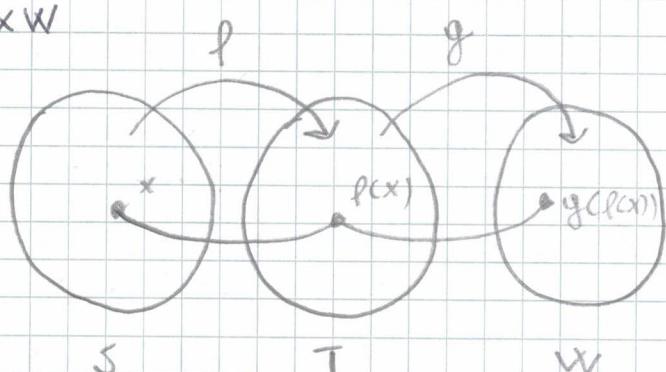
$$(g \circ f)(x) = g(f(x))$$

Esempio:

$$f(x) = x + 3$$

$$g(y) = y^2$$

$$\begin{aligned} (g \circ f)(x) &= g(f(x)) = (f(x))^2 \\ &= (x+3)^2 \end{aligned}$$



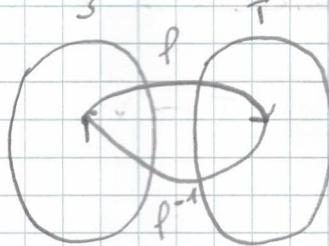
$$\begin{aligned} (f \circ g)(y) &= g(y) + 3 \\ &= y^2 + 3 \end{aligned}$$

DEFINIZIONE

Se f è biettiva, f^{-1} è la sua inversa ed è t.c.

$$(f \circ f^{-1})(t) = t \forall t$$

$$(f^{-1} \circ f)(s) = s \forall s$$

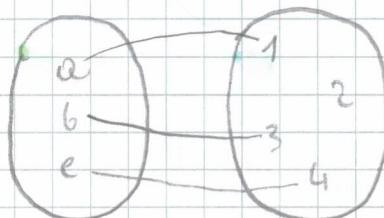


OSSERVAZIONI

Se f non è biettiva, f^{-1} non è una funzione
relazione opposta a f

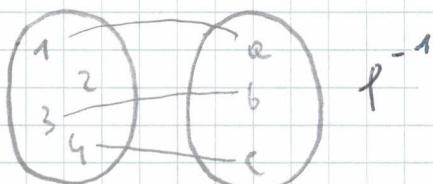
Esempio: $S = \{a, b, c\}$

$$T = \{1, 2, 3, 4\}$$



$$f \subseteq S \times T \quad f = \{(a, 1), (b, 3), (c, 4)\}$$

$$\Rightarrow f^{-1} = f^{\text{op}} = \{(1, a), (3, b), (4, c)\} \subseteq T \times S$$



Quindi se f non è suriettiva,

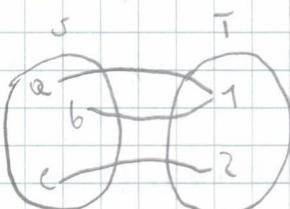
f^{-1} non è ben definita, cioè non è una

funzione perché $\exists x \in T$ che non ha corrispondenti
in S (in questo caso 2)

Se invece f non è iniettiva

$$S = \{a, b, c\}$$

$$T = \{1, 2\}$$

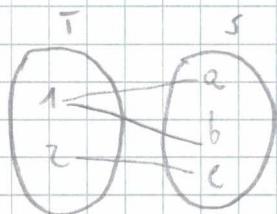


$$f \subseteq S \times T$$

$$f^{-1} \subseteq T \times S$$

$$f = \{(a, 1), (b, 1), (c, 2)\}$$

$$f^{-1} = \{(1, a), (1, b), (2, c)\}$$



f^{-1} non è funzione perché c'è un elemento del dominio
al quale corrispondono due elementi distinti del codominio

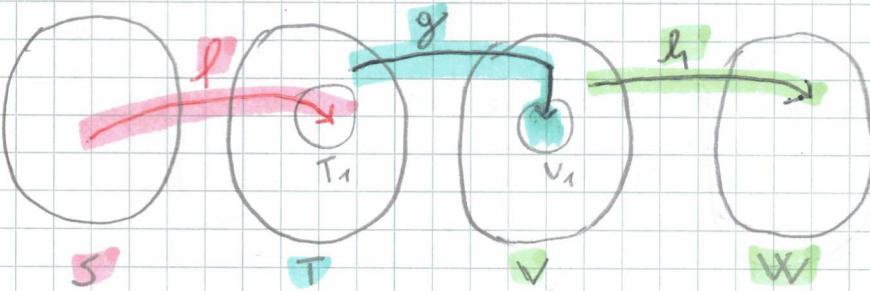
OSSERVAZIONE

La composizione di funzioni non è commutativa: $g \circ f \neq f \circ g$

Mentre è associativa: $h \circ (g \circ f) = (h \circ g) \circ f$

$$f: S \rightarrow T, \quad g: T \rightarrow V, \quad h: V \rightarrow W$$

ha senso fare $h \circ (g \circ f)$ se $T_1 \subseteq T$ & $V_1 \subseteq V$



PROPOSIZIONE

$$f: S \rightarrow T, \quad g: T \rightarrow V$$

- 1) Se f e g sono iniettive $\Rightarrow g \circ f$ è iniettiva
- 2) Se f e g sono suriettive $\Rightarrow g \circ f$ è suriettiva
- 3) Se f e g sono biettive $\Rightarrow g \circ f$ è biettiva
- 4) Se $g \circ f$ è iniettiva $\Rightarrow f$ è iniettiva
- 5) Se $g \circ f$ è suriettiva $\Rightarrow g$ è suriettiva
- 6) Se $g \circ f$ è biettiva $\Rightarrow f$ è iniettiva e g è suriettiva

DIMOSTRAZIONI

1)

$$\text{th: } \forall x_1, x_2 \in S \text{ con } x_1 \neq x_2 \Rightarrow g(f(x_1)) \neq g(f(x_2))$$

Se $x_1 \neq x_2$, poiché f è iniettiva (per ip) si ha $f(x_1) \neq f(x_2)$

Ma allora in T ho $f(x_1) = y_1$ e $f(x_2) = y_2$ con $y_1 \neq y_2$

Poiché g è iniettiva (per ip) si ha $g(y_1) \neq g(y_2)$

$$\Rightarrow g(f(x_1)) \neq g(f(x_2))$$

5) th: $g(T) = V$ (oppure $\text{Im}(g) = V$)

$f: S \rightarrow T$

hp: $g \circ f$ è suriettiva, cioè $g(f(S)) = V$ → $g: T \rightarrow V$ è suriettiva

$g \circ f: S \rightarrow V$

poiché $f: S \rightarrow T$, si ha che

$$\text{Im}(f) = f(S) \subseteq T$$

⇒

$$g(f(S)) \subseteq g(T)$$

per hp. $g(f(S)) = V$

Ma allora $V \subseteq g(T)$. Poiché $g: T \rightarrow V$, si ha sempre che $g(T) \subseteq V \Rightarrow$ ho contemporaneamente $V \subseteq g(T)$ e $g(T) \subseteq V \Rightarrow V = g(T)$

□

RELAZIONI DI EQUIVALENZA E PARTIZIONI

$R \subseteq S \times S$ è di equivalenza se

$$\begin{cases} 1. \forall x \in S \quad xRx \\ 2. \forall x, y \in S, \text{ se } xRy \Rightarrow yRx \\ 3. \forall x, y, z \in S, \text{ se } xRy \wedge yRz \Rightarrow xRz \end{cases}$$

DEFINIZIONE: Una partizione di un insieme S è un insieme

$\mathcal{F} \subseteq P(S)$ tale che:

$$\begin{cases} 1. \forall X \in \mathcal{F} \quad X \neq \emptyset \\ 2. \forall X, Y \in \mathcal{F}, \quad X \cap Y = \emptyset \\ 3. \bigcup_{X \in \mathcal{F}} X = S \end{cases}$$

Esempio:

$$S = \{a, e, i, o, u\}$$

Partizioni: 1) $\{\{S\}\}$ PARTIZIONE TOTALE

2) $\{\{a\}, \{e\}, \{i\}, \{o\}, \{u\}\}$ PARTIZIONE IDENTICA

3) $\{\{a, e\}, \{i, o, u\}\}$

OSSERVAZIONE

\Rightarrow se partizione di $S \Leftrightarrow \forall x \in S \exists ! y \in I \mid x \in y \text{ e } \forall y \in I, y \neq \emptyset$

DEFINIZIONE

Sia $R \subseteq S \times S$ relazione di equivalenza, definiamo la classe di equivalenza di $x \in S$ modulo R come:

$$\text{insieme } [x]_R := \{y \in S \mid y R x\} \subseteq S$$

Si definisce insieme quoziente di S modulo R come:

$$\text{insieme } S/R := \{[x]_R \mid x \in S\} \subseteq P(S)$$

L'applicazione $\pi_R : S \rightarrow P(S)$

$x \mapsto [x]_R$ è detta proiezione canonica

$$\pi_R(x) = [x]_R \quad \pi_R \subseteq S \times P(S)$$

PROPOSIZIONE

S insieme, $R \subseteq S \times S$ relazione di equivalenza. Allora valgono le seguenti affermazioni:

- 1) $x \in [x]_R \quad \forall x \in S$ (questo implica che $[x]_R \neq \emptyset$)
- 2) Se $x R y \Rightarrow [x]_R = [y]_R$
- 3) Se $x \not R y \Rightarrow [x]_R \cap [y]_R = \emptyset$

DIMOSTRAZIONI

1) R è di equivalenza $\Rightarrow \forall x \in S, xRx$ e per definizione

• $[x]_R$ è l'insieme degli elementi di S che sono in relazione con $x \Rightarrow x \in [x]_R$ perché xRx □

2) Se $xRy \Rightarrow$ per definizione si ha $x \in [y]_R$

• dimostriamo che $[x]_R \subseteq [y]_R$:

Sia $z \in [x]_R \Rightarrow$ per definizione zRx . Per transitività:

$$zRx \wedge xRy \Rightarrow zRy \Rightarrow z \in [y]_R$$

• dimostriamo che $[y]_R \subseteq [x]_R$

• Sia $z \in [y]_R \Rightarrow$ per def. zRy . Sappiamo che xRy e per la simmetria di R si ha $yRx \Rightarrow zRy \wedge yRx \Rightarrow zRx$.

$$\Rightarrow z \in [x]_R$$

□

3) $xRy \Rightarrow [x]_R \cap [y]_R = \emptyset$

contradizione

Dimostriamo che $[x]_R \cap [y]_R \neq \emptyset \Rightarrow xRy$

$$\exists z \in [x]_R \cap [y]_R \Rightarrow z \in [x]_R \wedge z \in [y]_R$$

$$\Rightarrow zRx \wedge zRy$$

• Per la simmetria di R , questo implica $xRz \wedge zRy$

Per la transitività di R , otteniamo xRy

□

OSSERVAZIONE: La proposizione precedente ci dice che $S \in \text{S}^*$ è una partizione di S , infatti:

1) $\forall x \in S_R \neq \emptyset$ (perché $x \in P(S_R)$)

2) $\forall [x]_R, [y]_R$, si ha $[x]_R = [y]_R \rightarrow [x]_R \cap [y]_R = \emptyset$
 $x R y \rightarrow x \neq y$

3) $S = \bigcup \{x]_R \mid x]_R \in S_R\}$ perché $\forall x \in S \exists y \in S/R \mid x \in y$
 dove $y = x]_R$

PROPOSIZIONE

Le seguenti affermazioni sono equivalenti: (date $R_1, R_2 \subseteq S \times S$)

$$1) R_1 = R_2$$

Mostriamo che:

$$2) \quad \forall x \in S \quad [x]_{R_1} = [x]_{R_2}$$

$$1) \Rightarrow 2) \Rightarrow 3) \Rightarrow 1)$$

$$3) \quad S/R_1 = S/R_2$$

DIMOSTRAZIONE

1) \Rightarrow 2)

Up: $R_1 = R_2$ und direkte $(x, y) \in R_1 \Leftrightarrow (x, y) \in R_2$

$$\text{Allora } \{ y \in S \mid y R_1 x \} = \{ y \in S \mid y R_2 x \}$$

Per definizione $\{ y \in S \mid y R_1 x \} = [x]_{R_1}$

$$e \quad \{ y \in S \mid y R_2 x \} = [x]_{R_2} \quad e \quad \text{quiudi } \forall x \in S, \text{ si ha } [x]_{R_1}$$

2) => 3)

$$h_p : [x]_{R_1} = [x]_{R_2}$$

$$S_{R_1} = \{ x \in R_1 \mid x \in S \} =$$

$$\{x_{j_{k_2}} \mid x \in S\} = S_{j_{k_2}}$$

3) \Rightarrow 1)

hp. $S/R_1 = S/R_2$ vuol dire che $\forall x \in S \exists y \in S [x]_{R_1} = [y]_{R_2}$

Sappiamo che $x \in [x]_{R_1} = [y]_{R_2}$, allora $x \in [y]_{R_2}$ $\forall y$
quindi per definizione, $x R_2 y$

Devo dimostrare che $[x]_{R_2} = [y]_{R_2}$

• Vediamo che $[x]_{R_2} \subseteq [y]_{R_2}$:

Sia $z \in [x]_{R_2} \Rightarrow z R_2 x$ ma per ipotesi si ha $x R_2 y$ e per la transitività di R_2 , segue $z R_2 y \Rightarrow z \in [y]_{R_2}$

• Vediamo che $[y]_{R_2} \subseteq [x]_{R_2}$

Sia $z \in [y]_{R_2} \Rightarrow z R_2 y$. Per la simmetria di R_2 , da $x R_2 y$

segue $y R_2 x$ e per transitività si ha che $z R_2 x \Rightarrow z \in [x]_{R_2}$

Abbiamo dimostrato che $\forall x \in S, [x]_{R_1} = [y]_{R_2} = [x]_{R_2}$

e cioè $\forall x \in S \forall y \in S x R_1 y \Leftrightarrow x R_2 y$, il che equivale a $R_1 = R_2$ \square

TEOREMA FONDAMENTALE SULLE RELAZIONI DI EQUIVALENZA

Sia $S \neq \emptyset$, allora valgono le seguenti affermazioni:

- 1) Se $R \subseteq S \times S$ è di equivalenza, allora S/R è una partizione di S .
- 2) Se γ è una partizione di S , $\exists! R_\gamma \subseteq S \times S$ relazione di equivalenza tale che $\gamma = S/R_\gamma$.

DIMOSTRAZIONI

1) Già osservata.

2) Definiamo $R_\gamma \subseteq S \times S$ come:

$$x R_\gamma y \iff \exists y \in \gamma \mid x, y \in Y$$

(i) R_γ è di equivalenza:

• R_γ è riflessiva: $x R_\gamma x, \forall x \in S$?

Poiché γ è partizione, ogni suo elemento appartiene a un $y \in \gamma$ cioè, $\forall x \in S \exists y \in \gamma \mid x \in y$

$$x R_\gamma x$$

• R_γ è simmetrica: $x R_\gamma y \Rightarrow y R_\gamma x$

$$\text{Se } x R_\gamma y \Rightarrow \exists y \in \gamma \mid x, y \in Y \Leftrightarrow \exists y \in \gamma \mid y, x \in Y$$

$$\Rightarrow y R_\gamma x$$

• R_γ è transitiva: $x R_\gamma y \wedge y R_\gamma z \Rightarrow x R_\gamma z$

$$\begin{aligned} x R_\gamma y &\Leftrightarrow \exists y_1 \in \gamma \mid x, y \in y_1 \\ y R_\gamma z &\Leftrightarrow \exists y_2 \in \gamma \mid y, z \in y_2 \end{aligned} \quad \left. \begin{array}{l} \text{cioè } y \in y_1 \cap y_2 \\ \text{ma } y_1 = y_2 \end{array} \right\} \quad \text{cioè } y \in y_1 \cap y_2$$

Poiché γ è partizione, se $y_1 \neq y_2$ si ha $y_1 \cap y_2 = \emptyset$

ma allora $y_1 = y_2$, e quindi $x, y, z \in y_1$

$$\text{Allora } \exists y_1 \in \gamma \mid x, z \in y_1 \Leftrightarrow x R_\gamma z$$

ii) Vediamo che $\gamma = S/R_\gamma$

Sia $x \in S \Rightarrow \exists! x \in \gamma \mid x \in X$

Dimostriamo che $X = \{x \in \gamma \mid x \in X\}$: infatti così dimostriamo che l'unico insieme in γ che contiene x coincide con l'unico insieme in S/R_γ che contiene x

Vediamo che $X \subseteq \{x \in \gamma \mid x \in X\}$

Sia $z \in X$, poiché anche $x \in X$, si ha $x, z \in X \wedge x \in \gamma$

$\Rightarrow x R_\gamma z \Rightarrow z \in \{x \in \gamma \mid x \in X\}$

Vediamo che $\{x \in \gamma \mid x \in X\} \subseteq X$

Sia $z \in \{x \in \gamma \mid x \in X\} \Rightarrow \exists x \in \gamma \mid x, z \in X$

così ho che $x \in Z \wedge x \in X$. Poiché γ è una partizione, si ha $X = Z \Rightarrow z \in X$

iii) R_γ è l'unica relazione tale che $S/R_\gamma = \gamma$

Se R_1 è t.c. $S/R_1 = \gamma$, allora $S/R_\gamma = \gamma = S/R_1$

per l'equivalenza (1) \Leftrightarrow (3) della proposizione precedente si ha $R_\gamma = R_1$ \square

OSSERVAZIONE

$$f: R \rightarrow P^*(P(S))$$

$R =$ insieme delle r.e. su S

$$\text{ossia } R \mapsto S_R$$

$$P^*(P(S)) = \{ Y \subseteq P(S) \mid Y \text{ è partizione di } S\}$$

il teorema precedente ci dice che f è biettiva

$$\forall Y \exists ! R_Y \mid S_{R_Y} = Y$$

$\sim P(R_Y)$

DEFINIZIONE

Se f è $S \times T$ applicazione, la relazione indotta da f è

$$\underline{x R_Y y \Leftrightarrow f(x) = f(y)}$$

$$(x, y) \in R_Y \subseteq S \times S$$

Esempio :

$$S = \mathbb{N}_0 \quad Q R b \Leftrightarrow a+b \text{ è pari}$$

$$1) a R a \text{ perché } a+a = 2a \text{ è pari}$$

$$2) a R b \Rightarrow a+b \text{ è pari} \Rightarrow b+a \text{ è pari} \Rightarrow b R a$$

$$3) \text{ se } a R b \text{ e } b R c \Rightarrow a+b \text{ è pari}$$

$$\begin{aligned} & \Rightarrow (a+b)+(b+c) \text{ è pari} \\ & b+c \text{ è pari} \quad \text{e } a+2b+c \text{ è pari} \\ & (a+c)+2b \text{ è pari} \end{aligned}$$

$a+b$ è anche pari perché due numeri sommati, danno un numero pari se sono entrambi pari o entrambi dispari

$$\mathbb{N}_0 / R = \{ \mathbb{N}_0, \mathbb{N}_P \}$$

$a \in \mathbb{N}_0 \Rightarrow (b R a \Leftrightarrow a+b \text{ è pari}) \Rightarrow$ poiché a è dispari,
sarà b dispari $\Rightarrow b \in \mathbb{N}_d$

$$a \in \mathbb{N}_P \Rightarrow (b R a \Leftrightarrow a+b \text{ è pari})$$

Esercizio 16

$$e = \{1, 2, 3, 4, 5, 6, 7, 8, 9\} \quad R \subseteq e \times e \quad xRy \Leftrightarrow x + 2y \in 3\mathbb{Z}$$

$\{0, 3, 9\} = \{9, 3, 0\}$

$$120 = 8 \cdot 5 + 5$$

1) riflessività: $xR x$ perché $x + 2x = 3x \in 3\mathbb{Z}$

2) simetria: $xRy \Rightarrow x+2y \in 3\mathbb{Z}$ si ha che $y+2x = (x+2y)$

$+ (x-y) \in 3\mathbb{Z}_L$ perché $(x+2y) \in 3\mathbb{Z}_L$ per ip.

3) transitivita': $x R y \wedge y R z \Rightarrow x R z$

$$y \in \mathbb{R}^2 \quad \left\{ \begin{array}{l} y + 2z \in 3\mathbb{Z} \end{array} \right.$$

devo dimostrare che $x + z \in 3\mathbb{Z}$

$$x+2z = \underline{x+2z+3y} - 3y \quad \in 37L$$

$$(x+2y) + (y+2z)$$

$$\begin{array}{c} | \\ (x+2y) \\ \in 37L \end{array} \quad \begin{array}{c} | \\ (y+2z) \\ \in 37L \end{array}$$

$$C/R = \{ [a]_R \mid a \in C \}$$

$$[1]_R = \{1, 4, 7\}$$

$$1+2\cdot 1 = 3 \in \mathbb{Z}$$

$$1+2\cdot 2 = 5 \notin \pi_L$$

$$1 + 2 \cdot 3 = 7 \text{ } \cancel{+} \text{ } 37$$

$$4 + 2 \cdot 1 = 6 \in 37L$$

$$1 + 2 \cdot 4 = 9 \text{ E3L}$$

$$4 + 2 \cdot 2 = 8 \text{ g} 37\text{L}$$

... - - -

$$4 + 2 \cdot 3 = 10 \text{ & } 31L$$

1.

$$4 + 2 \cdot 4 = 12 \in 3\mathbb{N}$$

$$\dots \\ 2 \cdot 7 = 18 \in 314$$

$$[2]_R = \{2, 5, 8\}$$

$$2+2 \cdot 3 = 8 \text{ €} \text{ IVA}$$

Vedo solo questi

$$2+2 \cdot 5 = 12 \text{ €} \text{ IVA}$$

Sapendo che 1, 4, 7 non ci sono
perché 2 € [1]_R

$$2+2 \cdot 6 = 16 \text{ €} \text{ IVA}$$

$$2+2 \cdot 8 = 16 \text{ €} \text{ IVA}$$

$$[3]_R = \{3, 6, 9\}$$

$$3+2 \cdot 6 = 15 \text{ €} \text{ IVA}$$

$$3+2 \cdot 9 = 21 \text{ €} \text{ IVA}$$

$$\begin{aligned} e_R &= \{[1]_R, [2]_R, [3]_R\} \\ &= \{\{1, 4, 7\}, \{2, 5, 8\}, \{3, 6, 9\}\} \end{aligned}$$

RELAZIONI D'ORDINE

$R \subseteq S \times S$ è d'ordine se e solo se

<p>Esempio: \leq (IR, usuale)</p> <p>ordine "naturale", usuale</p>	<p>Riflessiva $\forall x \in S \quad xRx$</p> <p>Asimmetrica $xRy \wedge yRx \Rightarrow x=y$</p> <p>transitiva $xRy \wedge yRz \Rightarrow xRz$</p>
---	---

(INo, \leq) relazione d'ordine

$S \neq \emptyset$ ($P(S)$, \subseteq) $A R B \Leftrightarrow A \subseteq B$ relazione d'ordine

NOTAZIONE

Se R è d'ordine su $S \times S$, la si dice con " \leq ", anche se S non è insieme numerico

DEFINIZIONE

Un insieme ordinato è una coppia (S, \leq) con \leq relazione d'ordine binaria su S

DEFINIZIONE

Se \leq è totale, cioè $\forall x, y \in S$ si ha $x \leq y \vee y \leq x$, allora S si dice totalmente ordinato o catena

Esempio: (\mathbb{N}_0, \leq) è catena

$(P(S), \subseteq)$ non è catena

Se $S = \{a, b\}$ si ha $\{a\} \not\subseteq \{b\}$ e $\{b\} \not\subseteq \{a\}$

$\{a\}$ e $\{b\}$ non sono confrontabili

(\mathbb{N}_0, \leq) non è catena, $2 \times 3 \neq 3 \times 2$

DEFINIZIONE

Dato (S, \leq) definiamo l'ordine stretto < come:

$$x < y \Leftrightarrow x \leq y \wedge x \neq y$$

Esempio:

$(P(S), \subseteq)$ inclusione stretta

NON E' UNA
RELAZIONE
D'ORDINE

DEFINIZIONE

$(S, \leq), (T, \leq)$ due insiemti ordinati

$f: S \rightarrow T$ applicazione si detto omomorfismo d'ordine se:

$$\forall x, y \in S, x \leq y \Rightarrow f(x) \leq f(y)$$

" f preserva la relazione d'ordine"

applicazione identica

Esempio: (\mathbb{N}_0, \leq) e (\mathbb{N}_0, \leq) $\text{id}_{\mathbb{N}_0}: \mathbb{N}_0 \rightarrow \mathbb{N}_0$

$$m \mapsto m$$

non e' omomorfismo

se $\text{id}_{\mathbb{N}_0}: (\mathbb{N}_0, \leq) \rightarrow (\mathbb{N}_0, \leq)$ perche' $2 \leq 3$ ma $2 \nleq 3$

$$x \leq y \quad f(x) \neq f(y)$$

Invece, se $\text{id}_{\mathbb{N}_0}: (\mathbb{N}, \leq) \rightarrow (\mathbb{N}, \leq)$ e' omomorfismo

infatti se $a \leq b \Rightarrow b = a + k \Rightarrow a \leq b$

Esempio

$$S = \{1, 2, 3, 4\} \quad B = \{a, b, c, d\}$$

$$(S, \leq) \quad 1 \leq 2 \leq 3 \leq 4$$

$$b \leq a \leq d \leq c$$

$$f(1) = b$$

g che manda 1 in a e 2 in b

$$f(2) = a$$

non e' omomorfismo

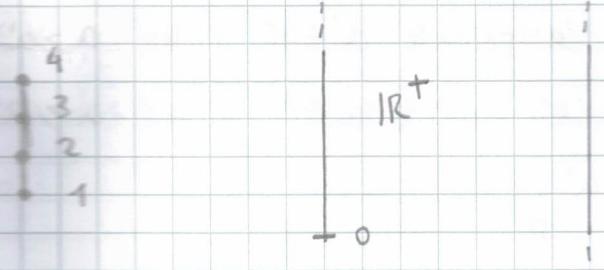
e' omomorfismo

$$f(3) = d$$

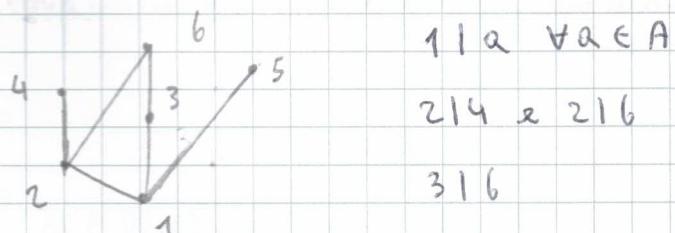
$$\leq = \{(1,2), (2,3), (3,4), (2,2), (1,1), (3,4), \dots\}$$

$$f(4) = c$$

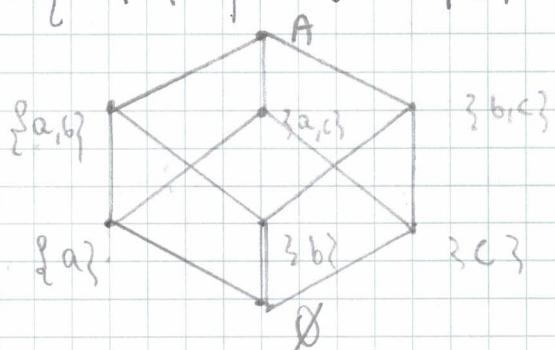
DIAGRAMMA DI HASSE: rappresentazione grafica di un insieme ~~con~~ ordinato



Esempio: $A = \{1, 2, 3, 4, 5, 6\}$, (A, \leq)



Esempio: $A = \{a, b, c\}$, $(P(A), \subseteq)$



DEFINIZIONE

Un minimo per (S, \leq) è un elemento $a \in S$ s.t. $a \leq x \forall x \in S$

Un massimo per (S, \leq) è un elemento $a \in S$ s.t. $x \leq a \forall x \in S$

Li denotereemo con $\min(S)$ e $\max(S)$ rispettivamente

LEMMA

Se $a = \max(S)$ e $a' = \max(S) \Rightarrow a = a'$

Se $b = \min(S)$ e $b' = \min(S) \Rightarrow b = b'$

DIMOSTRAZIONE DI MAXIMA E MINIMA

- Se $a = \max(S) \Rightarrow \forall x \in S a \geq x$ e poiché $a \in S$ si ha $a \geq a$
Se $a' = \max(S) \Rightarrow \forall x \in S a' \geq x$ e poiché $a \in S$ si ha $a' \geq a$
Ma allora per l'assimmetria $a = a'$ \square

DEFINIZIONE

Un elemento $a \in S$ è detto **minimale** se $\forall x \in S a \leq x$

Un elemento $a \in S$ è detto **massimale** se $\forall x \in S a \geq x$

LEMMA

(S, \leq)

1) Se $a = \min(S) \Rightarrow a$ è minimale

Se $b = \max(S) \Rightarrow b$ è massimale

2) Se $a = \min(S)$ e c è minimale $\Rightarrow a \leq c$

Se $a = \max(S)$ e c è massimale $\Rightarrow a \geq c$

(Se c'è un minimo, non ci sono "altri" minimale)

LEMMA

Se (S, \leq) è totalmente ordinato:

1) Se c è minimale $\Rightarrow c$ è minimo

2) Se c è massimale $\Rightarrow c$ è massimo

DIMOSTRAZIONE

1) Sia c minimale e sia $x \in S \setminus \{c\}$, ma poiché S è catena,
se $c \neq x$ si avrà $x \leq c$, cioè $x \leq c$
ma c è minimale \Rightarrow deve essere $c = x$ ma $c \neq x \Rightarrow$ ho trovato
un assurdo e deve essere $c \leq x$ \square

2) Sia e massimale e per assurdo $\exists x \mid x \geq e$. Ma x è estremo superiore
 $\Rightarrow e \leq x$, poiché e è massimale, necessariamente $e = x$, ma (questo)
contraddice l'ipotesi $x \geq e$. Ho trovato un assurdo $\Rightarrow e \geq x$ e e è
massimo

LEMMA

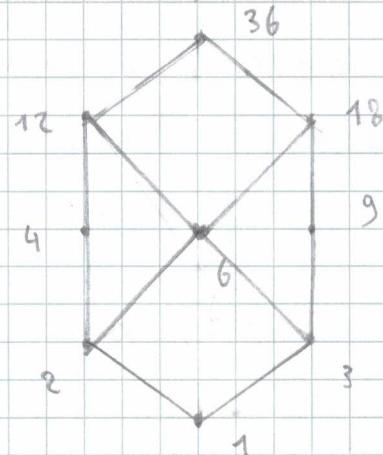
Ogni insieme ordinato finito ha massimali e minimali
Se è totalmente ordinato, ha massimo e minimo

Esempio

$$A = \{m \in \mathbb{N} \mid m \mid 36\} = \{2, 3, 4, 6, 9, 12, 18, 36, 1\}$$

(A, |)

36		2	divisori di 36:
18		2	$1, 2, 2^2, 3, 3^2, 3^2 \cdot 2$
9		3	$2 \cdot 3, 2^2 \cdot 3, 3^2 \cdot 2^2$
3		3	
1			



DEFINIZIONE 1.3 Sia S un insieme non vuoto. Si dice **bene ordinato** se ogni suo sottoinsieme non vuoto ha un minimo: $\forall X \subseteq S \setminus \emptyset \Rightarrow \exists \min(X)$

(S, \leq) insieme ordinato, S si dice **bene ordinato** se ogni suo sottoinsieme non vuoto ha un minimo: $\forall X \subseteq S \setminus \emptyset \Rightarrow \exists \min(X)$

Esempio: (\mathbb{N}, \leq) è bene ordinato

(\mathbb{Z}, \leq) non è bene ordinato: $\{-m \mid m \in \mathbb{N}\}$ non ha minimo

LEMMA

Se (S, \leq) è bene ordinato, allora è totalmente ordinato.
(non vale il contrario)

DIMOSTRAZIONE

$$\forall x, y \in S, \{x, y\} \in P(S) \Rightarrow \exists \min\{x, y\}$$

Allora $x \leq y \circ y \leq x$

Se $\min\{x, y\} = x$ Se $\min\{x, y\} = y$

□

DEFINIZIONE

(S, \leq) insieme ordinato, $X \subseteq S$, $X \neq \emptyset$

$w \in S$ è detto **minorante per X** se $w \leq x \quad \forall x \in X$

$w \in S$ è detto **maggiorante per X** se $w \geq x \quad \forall x \in X$

Esempio:

$$S = \{ m \in \mathbb{N} : m \mid 24 \}$$

(S, 1)

$$X = \{ 2, 4, 12 \}$$

MINORANTI di $X = 2, 1$

è anche $\min(X)$

MAGGIORANTI di $X = 12, 24$

è anche $\max(X)$

OSSERVAZIONE

Il minimo di $X \subseteq S$, se esiste, è anche minorante

Il massimo di $X \subseteq S$, se esiste, è anche maggiorante

Esempio: $\{0, 1\} \subseteq \mathbb{R}, (\mathbb{R}, \leq)$

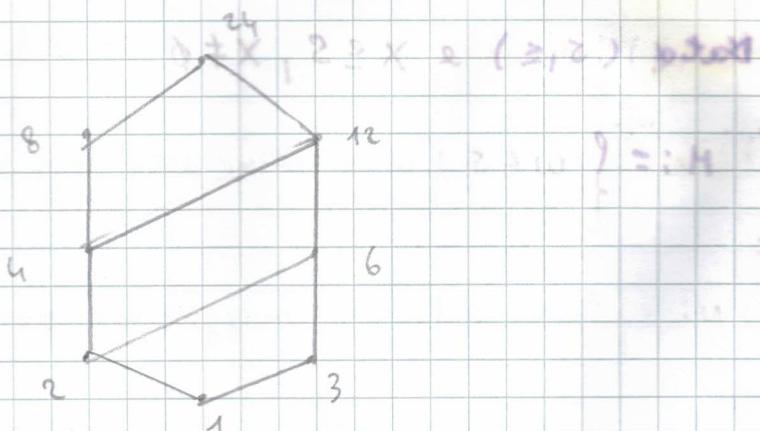
$\{x \in \mathbb{R} \mid x \geq 1\}$ è insieme di maggioranti \rightarrow sono infiniti

•

Se prendo $X \subseteq S$, $= \{8, 12\}$
insieme
dell'esempio precedente

Allora: MINORANTI DI $X = 1, 2, 4$

MAGGIORANTI DI $X = 24$



DEFINIZIONE

Dato (S, \leq) e $x \in S, x \neq \emptyset$

$$M := \{ w \in S \mid w \text{ è minorante per } x \}$$

$$N := \{ w \in S \mid w \text{ è maggiorante per } x \}$$

L'estremo inferiore di x è $\max(M)$, cioè il più grande dei minoranti, denotato con $\inf_S(x)$ o $\inf(x)$

$$K = \inf_S(x) \Leftrightarrow \begin{cases} K \leq x \quad \forall x \in X \\ \forall s : s \leq x \quad \forall x \in X \Rightarrow s \leq K \\ s \text{ è minorante} \end{cases}$$

L'estremo superiore di x è $\min(N)$, cioè il più piccolo dei maggioranti, denotato con $\sup_S(x)$ o $\sup(x)$

$$h = \sup_S(x) \Leftrightarrow \begin{cases} x \leq h \quad \forall x \in X \\ \forall s : x \leq s \quad \forall x \in X \Rightarrow h \leq s \\ s \text{ è maggiorante} \end{cases}$$

Esempio: $S = \{a, b, c\}$

$(P(S), \subseteq)$

$$X = \{\{a, b\}, \{c\}, \{a\}\}$$

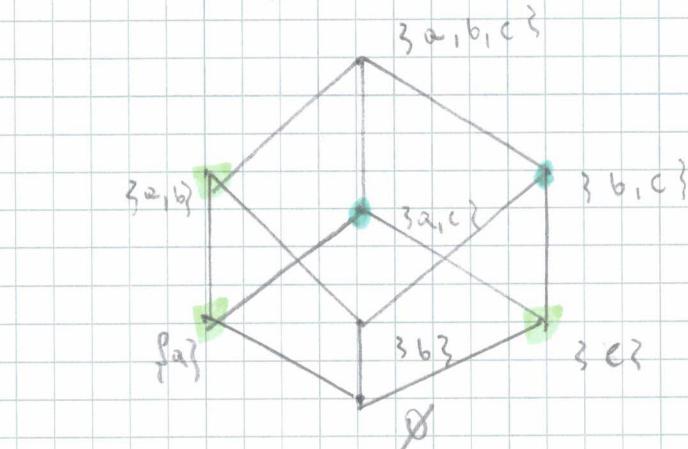
MINORANTI: \emptyset

MAGGIORANTI: S

$$x = \{\{a, c\}, \{b, c\}\}$$

MINORANTI: $\emptyset, \{c\}$

MAGGIORANTI: S



$$\inf(x) = \{c\} = \{a, c\} \cap \{b, c\}$$

$$\sup(x) = S = \{a, c\} \cup \{b, c\}$$

LEMMA

$\forall S \neq \emptyset \quad (P(S), \subseteq)$ ordinato e $\forall A \subseteq P(S)$

$$\inf(A) = \bigcap_{x \in A} x \quad \sup(A) = \bigcup_{x \in A} x$$

DIMOSTRAZIONE

per $A = \{A, B\} \subseteq P(S)$

$$\inf(A) = \bigcap_{x \in A} x = A \cap B \quad \sup(A) = \bigcup_{x \in A} x = A \cup B$$

Notiamo che $A \cap B$ è minorente per $A = \{A, B\}$ perché $A \cap B \subseteq A$ e $A \cap B \subseteq B$

Sia ora c altro minorente per A , cioè $c \subseteq A$ e $c \subseteq B$, ma allora $c \subseteq A \cap B$ e $A \cap B$ è il più grande dei minoranti

Si ha che $A \subseteq A \cup B$ e $B \subseteq A \cup B \Rightarrow A \cup B$ è maggiorante

Se: $A \subseteq c$ e $B \subseteq c$ si ha $A \cup B \subseteq c \Rightarrow A \cup B$ è il più piccolo dei maggioranti \square

LEMMA

Dato (S, \leq) , $x \neq 0$ $x \subseteq S$

1) Se $\exists a \in \min(x) \Rightarrow a = \inf(x)$

2) Se $\exists a \in \max(x) \Rightarrow a = \sup(x)$

DIMOSTRAZIONE

2) Se $\exists a \in \max(x)$, per definizione di massimo, si ha $a \geq x \quad \forall x \in x$, cioè a è maggiorante per x

Sia k un altro maggiorante per x , cioè $k \geq x \quad \forall x \in x$

poiché $a \in \max(x)$, si ha $a \in x$, e quindi in particolare $k \geq a$

Abbiamo provato che a è il più piccolo dei maggioranti e cioè

$$a = \sup(x) \quad \square$$

Esempio: (\mathbb{N}_0, \leq) \leq $\in \mathbb{N}_0$ limite, $x = \{x_1, \dots, x_m\}$

$$\inf(x) = \text{MCD}(x_1, \dots, x_m)$$

$$\sup(x) = \text{mem}(x_1, \dots, x_m)$$

DEFINIZIONE

(S, \leq) ordinato. S si detto **reticolo** se:

$$\forall x, y \in S \text{ esistono sempre } \inf\{x, y\} \text{ e } \sup\{x, y\}$$

$$x \wedge y$$

$$x \vee y$$

PROPRIETÀ

(S, \leq) reticolo. Allora $\forall x, y, z \in S$

$$1) x \vee x = x \wedge x = x \quad \text{idempotenza di } \vee, \wedge$$

$$2) x \vee y = y \vee x \quad] \text{ commutatività di } \vee, \wedge$$

$$3) x \wedge y = y \wedge x \quad]$$

$$4) x \vee (y \vee z) = \sup\{x, y, z\} = (x \vee y) \vee z \quad] \text{ associatività di } \vee \text{ e } \wedge$$

$$5) x \wedge (y \wedge z) = \inf\{x, y, z\} = (x \wedge y) \wedge z \quad]$$

$$6) x \wedge (x \vee y) = x \vee (x \wedge y) = x \quad \text{assorbimento}$$

DIMOSTRAZIONI

$$1) x \vee x = \sup\{x, x\} = x$$

$$2), 3) x \vee y = \sup\{x, y\} = \sup\{y, x\} = y \vee x$$

$$x \wedge y = \inf\{x, y\} = \inf\{y, x\} = y \wedge x$$

$$4) \underbrace{(x \vee y)}_w \vee z = \underbrace{\sup\{x, y, z\}}_t$$

$$w = \sup\{x, y\} \Rightarrow w \geq x \text{ e } w \geq y \quad \left. \begin{array}{l} \\ \end{array} \right\} s \geq x, s \geq y, s \geq z$$

$$s = w \vee z = \sup\{w, z\} \Rightarrow s \geq w \text{ e } s \geq z \quad \left. \begin{array}{l} \\ \end{array} \right\} s \geq x, s \geq y, s \geq z$$

$\Rightarrow s$ è maggiorante per $\{x, y, z\}$

$$\text{Sia } k \text{ altro maggiorante per } \{x, y, z\} \Rightarrow \begin{cases} k \geq x \\ k \geq y \\ k \geq z \end{cases}$$

$\Rightarrow k$ è maggiorante per $\{x, y\} \Rightarrow k \geq \sup\{x, y\} = w$

$\Rightarrow k \geq w$ e $k \geq z$ e cioè è maggiorante per $\{w, z\}$ (3,1)

$\Rightarrow k \geq \sup\{w, z\} = s$

Allora s è più piccolo di qualsiasi altro maggiorante \Rightarrow

$$s = \sup\{x, y, z\}$$

$$xv(\underbrace{y \vee z}_w) = \sup\{x, y, z\}$$

$$w = \sup\{y, z\} \quad w \geq y \quad w \geq z \quad \left. \begin{array}{l} s \geq x \\ s \geq y \\ s \geq z \end{array} \right\} s \geq x, s \geq y, s \geq z$$

$$s = \sup\{x, w\} \quad w \geq z \quad s \geq w \quad \left. \begin{array}{l} s \geq x \\ s \geq y \\ s \geq z \end{array} \right\} s \geq x, s \geq y, s \geq z$$

\bullet s è maggiorante per $\{x, y, z\}$

Sia k altro maggiorante, cioè $k \geq x, k \geq y, k \geq z$

Quindi k è maggiorante per $\{y, z\}$ $k \geq \sup\{y, z\} = w$

Ma allora k è maggiorante per $\{x, w\}$

$$\Rightarrow k \geq \sup\{x, w\} = xv(y \vee z) \quad \square$$

DEFINIZIONE

(L, \leq) è reticolo se $\exists \inf\{x, y\}$ e $\sup\{x, y\} \forall x, y \in L$

DEFINIZIONE

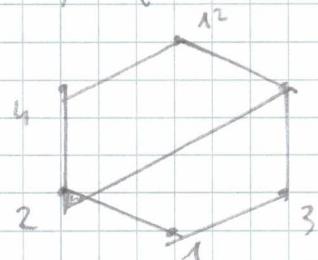
(L, \leq) vettore è distributivo se valgono le seguenti proprietà distributive:

$$\begin{aligned} x \vee (y \wedge z) &= (x \vee y) \wedge (x \vee z) \\ x \wedge (y \vee z) &= (x \wedge y) \vee (x \wedge z) \end{aligned} \quad \left. \begin{array}{l} \\ \end{array} \right\} \forall x, y, z \in L$$

Esempio

$$A = \{m \in \mathbb{N} \mid m \mid 12\} = \{1, 2, 3, 4, 6, 12\}$$

(A, \mid)



$$2 \vee (\underbrace{4 \wedge 3}_{1}) = 2 \vee 1 = 2$$

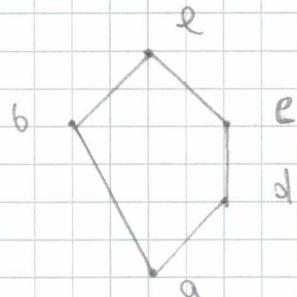
$$(2 \vee 4) \wedge (2 \vee 3) = 4 \wedge 6 = 2$$

Esempio

$$A = \{a, b, c, d, e\}$$

$$e \vee (d \wedge b) = e \vee a = e$$

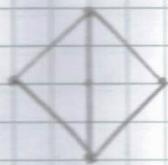
$$(c \vee d) \wedge (c \vee b) = c \wedge e = c$$



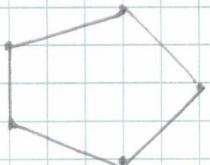
$$\begin{aligned} \text{Ma } d \vee (b \wedge c) &= d \vee a = d \\ (d \vee b) \wedge (d \vee c) &= e \wedge e = e \end{aligned} \quad \left. \begin{array}{l} \\ \end{array} \right\} \text{ma } \underline{d \neq e}$$

TEOREMA

Un reticolo è distributivo \Leftrightarrow non contiene



0



A = 2

(3,3)

DEFINIZIONE

Un reticolo è **limitato** se possiede un massimo e un minimo

Questi elementi li indichiamo con 1 e 0 rispettivamente

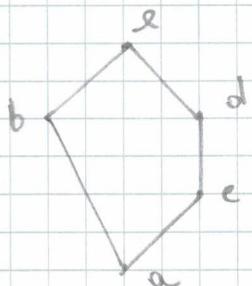
Oppure con T e L (Top e Bottom)

Dato $x \in L$, se $\exists \bar{x} \in L \mid x \vee \bar{x} = 1$ e $x \wedge \bar{x} = 0$, questo \bar{x} lo chiameremo

(L, \leq) limitato

complemento di x

Esempio:



Dato b , sia c che d sono complementi di b

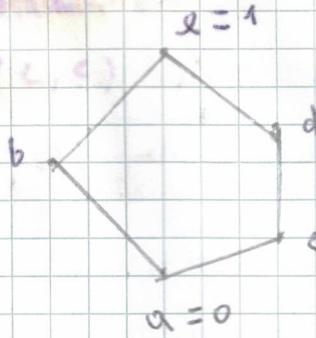
$$\text{perché } \begin{cases} b \vee c = l = 1 \\ b \wedge c = a = 0 \end{cases} \quad \text{e} \quad \begin{cases} b \vee d = l = 1 \\ b \wedge d = a = 0 \end{cases}$$

LEMMA

In un reticolo limitato e distributivo, il complemento (se esiste) è unico

DEFINIZIONE

Un reticolo (L, \leq) è detto **complementato** se ogni suo elemento ha un complemento

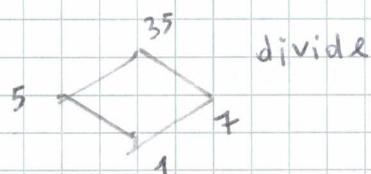
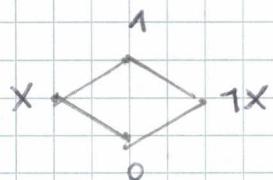


L è complementato e non distributivo

DEFINIZIONE

Un reticolato limitato, complementato e distributivo è detto **algebra di Boole**

Boole \Rightarrow se il complemento è unico, lo indico con $\neg x$



TEOREMA DI STONE

Sia (L, \leq) una algebra di Boole finita,

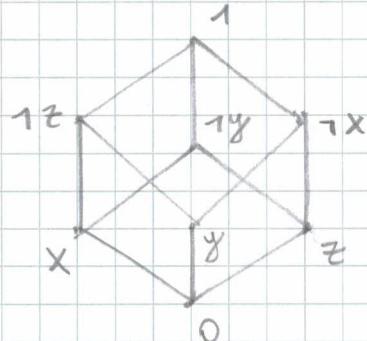
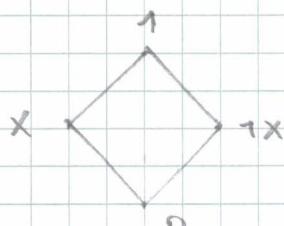
Allora $\exists X$ insieme t.c. (L, \leq) è **isomorfo** a $(P(X), \subseteq)$

esiste un omomorfismo biettivo

N.B. Le algebre di Boole finite hanno tutte cardinalità del tipo 2^m (dove $m = |X|$)



$\{0, 1\}$



$(P(\{a\}, \{b\}, \{c\}), \subseteq)$

$x = \{a\}$ $y = \{b\}$ $z = \{c\}$

DEFINIZIONE - ASSIOMI DI PEANO

Preso una terna $(\mathbb{N}_0, f, 0)$, $f: \mathbb{N}_0 \rightarrow \mathbb{N}_0$ t.c.

1) $0 \in f(\mathbb{N}_0)$

2) f è iniettiva

3) Se $X \subseteq \mathbb{N}_0$ è t.c.

i) $0 \in X$

ii) da $s \in X \Rightarrow f(s) \in X$, allora $X = \mathbb{N}_0$

f è detta funzione **SUCCESSIONE**

$1 := f(0), 2 := f(f(0)), \dots, m := \underbrace{f(f(\dots(f(0))))}_{m \text{ volte}}$

$m+1 := f(m)$

SECONDA FORMA DEL PRINCIPIO DI INDUZIONE

dato $X \subseteq \mathbb{N}_0$ t.c.

i) $\bar{m} \in X$

ii) dato $t > \bar{m}$ se $(k \in X \wedge \bar{m} \leq k < t)$ implica $t \in X$

allora $m \in X, \forall m \geq \bar{m}$

ALGORITMO DELLA DIVISIONE EUCLIDEA IN \mathbb{N}_0

$b \in \mathbb{N}$. Allora $\forall m \in \mathbb{N}_0$ esistono unici $q, r \in \mathbb{N}_0$ t.c. $m = qb + r$

q è detto **quoziente**, r è detto **resto**, operazione di divisione di m per b

DIMOSTRAZIONE

Induzione su m

• $m = 0$, $m = b \cdot 0 + 0 \Rightarrow \exists q, r$ uguali a 0

• Sia la proprietà vera $\forall k < b$ (passo induttivo com $t = b$)

Sia $m > 0$, $m < b \Rightarrow m = b \cdot 0 + m$

$m \geq b \Rightarrow m - b < m$ (perché $b > 0$)

\Rightarrow passo usare l'ipotesi di induzione su $m - b \Rightarrow \exists q'$ ed r' tali che

$m - b = q' b + r'$, $r' < b \Rightarrow m = q' b + b + r' = \underbrace{(q' + 1)}_{q} b + r'$

\Rightarrow ho dimostrato che m si divide per b , com $q = q' + 1$ e $r = r'$

Vediamo che q ed r sono unici:

$$m = q_1 b + r_1 \Rightarrow q_1 b + r_1 = q_2 b + r_2 \\ m = q_2 b + r_2$$

$$\Rightarrow q_1 b - q_2 b = r_2 - r_1 \Rightarrow (q_1 - q_2) b = r_2 - r_1$$

Possiamo supporre $r_2 \geq r_1$ (se fosse $r_1 \geq r_2$, considero $(q_2 - q_1)b = r_1 - r_2$)

$$\Rightarrow r_2 - r_1 \geq 0 \text{ e quindi } 0 \leq r_2 - r_1 \leq b$$

Così ho $(q_1 - q_2)b < b$ e questo può succedere solo se $q_1 - q_2 = 1$ e cioè $q_1 = q_2$.

Ma se $q_1 = q_2$, in $q_1 b + r_1 = q_2 b + r_2$, semplifico, ed ho $r_1 = r_2$

□

TEOREMA FONDAMENTALE DELL'ARITMETICA

$\forall m \geq 2$ ($m \in \mathbb{N}$) esistono $t \in \mathbb{N}$ e p_1, \dots, p_t numeri primi, tali che

$$m = p_1 \cdot \dots \cdot p_t$$

La decomposizione è unica a meno dell'ordine dei fattori.

DIMOSTRAZIONE

$m = 2$ è già scomposto (ho $t=1$ e $p_1 = 2$)

$m > 2$, suppongo la proprietà vera $\forall k < m$ e la dimostro per m

Sia m non primo $\Rightarrow \exists 1 < a, b < m \mid m = ab$

\Rightarrow per a e b vale l'ip di induzione:

$$\begin{cases} \exists t \in \mathbb{N} \text{ e } p_1, \dots, p_t \\ \exists l \in \mathbb{N} \text{ e } q_1, \dots, q_l \end{cases} \left\{ \begin{array}{l} a = p_1 \cdot \dots \cdot p_t \\ b = q_1 \cdot \dots \cdot q_l \end{array} \right.$$

$$\Rightarrow m = p_1 \cdot \dots \cdot p_t \cdot q_1 \cdot \dots \cdot q_l$$

□

TEOREMA DI EUCLIDE

Esistono infiniti numeri primi

Dimostrazione

Sia $\lambda \in \mathbb{N}$ il numero (finito per assurdo) dei numeri primi.

$$P = \{p_1, p_2, \dots, p_\lambda\} \quad m = p_1 \cdot p_2 \cdot \dots \cdot p_\lambda + 1$$

$\Rightarrow m$ è diviso da qualche primo che appartiene a P , chiamiamolo q
e si ha che $p_1 \cdot \dots \cdot p_\lambda$ è diviso da ogni elemento di P

$$\Rightarrow q | m \text{ e } q | p_1 \cdot \dots \cdot p_\lambda \Rightarrow q | 1$$

$$q | (m - p_1 \cdot \dots \cdot p_\lambda) = 1 \quad \text{Assurdo} (\nexists m \in \mathbb{N} \mid 1 = m \cdot a) \quad \square$$

ERIVELLO DI ERATOSTENE

$$m \in \mathbb{N}, m \geq 2$$

Se m non ammette un divisore primo p con $p^2 \leq m \Rightarrow m$ è primo

Esempio: 151

$$3 \rightarrow 3^2 \leq 151$$

$$11 \rightarrow 121 \leq 151$$

$$3 \times 151$$

$$7 \times 151$$

$$5 \rightarrow 25 \leq 151$$

$$13 \rightarrow 169 > 151$$

$$5 \times 151$$

$$11 \times 151$$

$$7 \rightarrow 49 \leq 151$$

ALGORITMO DELLA DIVISIONE EUCLIDEA \rightarrow $b \geq 0 \wedge m \geq 0 \Rightarrow q, r$ con

$$r < b \text{ t.c. } m = qb + r \quad (m \in \mathbb{N})$$

Proposizioni

Fissato $b \geq 2$, ogni $m \in \mathbb{N}_0$ ha una unica scrittura del tipo:

$$m = e_0 + e_1 b + \dots + e_s b^s \quad \text{per opportuni } s \geq 0, e_0, \dots, e_s \in \{0, 1, \dots, b-1\} \text{ con } e_s \neq 0$$

DIMOSTRAZIONE (solo esistenza)

$\exists e_0, q_0 \text{ eom } e_0 < b \mid m = bq_0 + e_0$ (divisione per b)

$\exists e_1, q_1 \text{ eom } e_1 < b \mid q_0 = bq_1 + e_1$

⋮

ad un certo punto ho trovato $q_s = 0$; succede quando $q_{s-1} = b$

$\exists e_s, q_s \mid q_{s-1} = 0 \cdot b + e_s$

$$m = bq_0 + e_0 = b(bq_1 + e_1) + e_0 = b^2q_1 + be_1 + e_0 =$$

$$= b^2(q_2b + e_2) + be_1 + e_0 =$$

$$= q_2b^3 + b^2e_2 + be_1 + e_0 =$$

⋮

$$= e_sb^s + e_{s-1}b^{s-1} + \dots + e_0 \quad \square$$

DEFINIZIONE

La sequenza e_s, e_{s-1}, \dots, e_0 è detta rappresentazione di m in base b , si scrive anche $(e_s, e_{s-1}, \dots, e_0)_b$

ESEMPIO:

277 in base 8?

$$277 = 34 \cdot 8 + 5$$

$$(277)_{10} = 2 \cdot 10^2 + 7 \cdot 10 + 10^0$$

$$\begin{array}{r} 34 \\ / \\ 4 \cdot 8 + 2 \\ / \\ 4 = 0 \cdot 8 + 4 \end{array}$$

$$(277)_{10} = (425)_8$$

$$\begin{array}{r} 277 \\ 24 \quad | \quad 34 \\ 37 \\ 32 \\ 5 \\ 210 \end{array}$$

$$(347)_8 = 3 \cdot 8^2 + 4 \cdot 8 + 7 \cdot 8^0 = 231$$

* 87 in base 2:

$$87 = 43 \cdot 2 + 1 \quad c_0 = 1$$

$$43 = 21 \cdot 2 + 1 \quad c_1 = 1$$

$$21 = 10 \cdot 2 + 1 \quad c_2 = 1$$

$$10 = 5 \cdot 2 + 0 \quad c_3 = 0$$

$$5 = 2 \cdot 2 + 1 \quad c_4 = 1$$

$$2 = 1 \cdot 2 + 0 \quad c_5 = 0$$

$$1 = 0 \cdot 2 + 1 \quad c_6 = 1$$

$$\therefore (1011011)_2 = 1 \cdot 2^5 + 0 \cdot 2^4 + 1 \cdot 2^3 + 0 \cdot 2^2 + 1 \cdot 2^1 + 0 \cdot 2^0 = 45$$

$$\therefore (1011) = 1 \cdot 2^3 + 0 \cdot 2^2 + 1 \cdot 2^1 + 1 \cdot 2^0 = 11$$

$(2001)_4$ a cosa corrisponde in base 7

$$(2001)_4 \rightarrow (\)_{10} \rightarrow (\)_7$$

$$(2001)_4 = 2 \cdot 4^3 + 1 \cdot 4^0 = (129)_{10}$$

$$\begin{array}{r} 129 \\ \hline 7 | 18 & 3 \\ 59 & \hline 4 | 2 & 0 \\ 3 & \hline 2 | 0 \end{array} \quad \text{cioe'}$$
$$129 = 18 \cdot 7 + 3 \quad c_0 = 3$$
$$18 = 2 \cdot 7 + 4 \quad c_1 = 4$$
$$2 = 0 \cdot 7 + 2 \quad c_2 = 2$$

$$(2001)_4 = (243)_7$$

ALGORITMO DELLA DIVISIONE EUCLIDEA (in TL)

$a, b \in \mathbb{N}$ con $b \neq 0$ $\exists! q, r \in \mathbb{N} \mid a = qb + r$ con $0 \leq r < b$

Notazione: $\text{rest}(a, b) = r$

PROPRIETÀ

1) $\text{rest}(a, b) = \text{rest}(a, -b)$

$$a = qb + r \Rightarrow a = (-q)(-b) + r$$

2) $\text{rest}(-a, b) = \begin{cases} 0 & \text{se } \text{rest}(a, b) = 0 \\ b - \text{rest}(a, b) & \text{se } \text{rest}(a, b) \neq 0 \end{cases}$

$$\begin{aligned} a &= bq + r \rightarrow -a = -bq - r + b - b \\ &= (-1-q)b + b - r \end{aligned}$$

$$a = bq \rightarrow -a = b(-q)$$

Esempio:

$$\text{rest}(19, 3) = 1$$

$$\text{rest}(-19, 3) = 3 - 1$$

$$19 = 6 \cdot 3 + 1$$

$$\begin{aligned} -19 &= 3(-7) + 2 \\ &\downarrow \\ &= -6 - 1 \end{aligned}$$

OSSERVAZIONE

$$x \mid y \Rightarrow \text{rest}(y, x) = 0$$

$$\hookrightarrow \exists k \mid y = kx$$

$$0 \mid y \Leftrightarrow y = 0$$

$$z \mid 0 \quad \forall z \in \mathbb{N} \quad (\text{perché } 0 = z \cdot 0 \quad \forall z \in \mathbb{N})$$

DEFINIZIONE

Dato $a \in \mathbb{Z}$, $D(a) = \{x \in \mathbb{Z} \mid x \mid a\}$ (divisori interi di a)

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

$|D(a)| \geq 4$ perché $1, -1, a, -a$ dividono tutti a

LEMMA

Dati $x, y, z, k \in \mathbb{Z} \mid x = yk + z$, si ha

$$D(x) \cap D(y) = D(z) \cap D(y)$$

Dimostrazione

$$m \in D(x) \cap D(y) \Rightarrow m \mid x \text{ e } m \mid y \Rightarrow m \mid x \text{ e } m \mid -ky$$

$$\exists h: y = mh$$

$$\Rightarrow -ky = -k(mh) = m(-kh)$$

e' diviso da m

$$\Rightarrow m \mid \underbrace{x - ky}_{z} \Rightarrow m \mid z \Rightarrow m \in D(y) \cap D(z)$$

$\therefore z$

Viceversa, se $m \in D(z) \cap D(y) \Rightarrow m \mid z \text{ e } m \mid y \Rightarrow m \mid z \text{ e } m \mid ky$

$$\Rightarrow m \mid \underbrace{ky + z}_x \Rightarrow m \in D(y) \cap D(x)$$

□

DEFINIZIONE

$p \in \mathbb{Z}$ è detto primo se $D(p) = \{1, -1, p, -p\}$

$p \neq \pm 1$

DEFINIZIONE

Dati $a, b \in \mathbb{Z}$, $a, b \neq 0$: il numero $d \in \mathbb{Z}$ è detto **massimo comune divisore** (di a e b) se:

- 1) $d | a$ e $d | b$
- 2) $\forall t \in \mathbb{Z}$: $t | a$ e $t | b$, si ha $t | d$

(inf nel reticolo di divisibilità) (di IN)

LEMMA

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

- 1) d è MCD di a e $b \Leftrightarrow -d$ lo è
- 2) d è MCD di a e $b \Rightarrow$ per ogni altro k che è MCD si ha $k \in \{-d, d\}$

Dimostrazione

1) " \Rightarrow " Sia d un MCD $\Rightarrow a = kd$ e $b = ld$ per opportuni $k, l \in \mathbb{Z}$
 $\Rightarrow a = (-k)(-d)$ $b = (-l)(-d) \Rightarrow -d | a$ e $-d | b$

Sia $t \in \mathbb{Z}$: $t | a$ e $t | b$ ma allora $t | d$ e cioè
 $d = mt$. Ma allora $(-d) = (-m)t$ e cioè $t | -d$

Allora $-d$ è MCD di a e b

" \Leftarrow " analogo

2)

Dalla proprietà 2) della definizione di MCD:

Se k è un altro MCD $\Rightarrow k | d$ e $d | k \Rightarrow k = \pm d$

$$\begin{cases} k | d \Rightarrow d = dk \\ d | k \Rightarrow k = Bd \end{cases} \quad d = (\alpha\beta)d$$

$$\alpha\beta = 1 \Leftrightarrow \begin{cases} \alpha = \beta = 1 \\ \alpha = \beta = -1 \end{cases}$$

□

NOTAZIONE

Se $a \neq -b$ sono MCD di a e b , per convenzione si prende
come $\text{MCD}(a, b)$ il valore positivo

OSSERVAZIONE

Se $d > 0$ $d = \text{MCD}(a, b) = \text{MCD}(-a, b) = \text{MCD}(a, -b) = \text{MCD}(-a, -b)$
 $d = \text{MCD}(2, 6) = \text{MCD}(-2, -6) = \text{MCD}(2, -6) = \text{MCD}(-2, 6)$

LEMMA

$a, b, d \in \mathbb{N}$, $d \geq 0$

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

PROPOSIZIONE

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

DIMOSTRAZIONE

Senza perdere la generalità, assumo $b > 0$

Per la divisione euclidea $\exists q_1, r_1$ con $0 \leq r_1 < b$ t.e., $\exists q_2, r_2$ con $r_2 <$

$$a = q_1 b + r_1 \quad b = q_2 r_1 + r_2$$

Se $r_1 = 0$ ho finito, se $r_1 > 0$ $\exists q_3$ con $0 \leq r_2 < r_1$ t.c.

$$q_3 = q_2 \cdot r_1 + r_3 \dots$$

⋮

Ho trovato una sequenza $b > r_1 > r_2 > \dots > r_{t-1} > r_t = 0$

$$\begin{aligned} D(a) \cap D(b) &= D(b) \cap D(r_1) \stackrel{\text{Lemma precedente}}{=} \\ &= D(r_1) \cap D(r_2) \cap \dots \end{aligned}$$

$$= D(r_{t-1}) \cap D(r_t) \stackrel{r_t = 0}{=} D(r_{t-1}) \cap D(0) = D(r_{t-1}) \cap \mathbb{N} = D(r_{t-1})$$

$$\Rightarrow D(a) \cap D(b) = D(r_{t-1}) \Rightarrow r_{t-1} = \text{MCD}(a, b)$$

□

Esempio:

$$\text{MCD}(1218, 132) = ? \quad \text{MCD}(1218, 132) = 6$$

$$1218 = 132 \cdot 9 + 30$$

$$132 = 30 \cdot 4 + 12$$

$$30 = 12 \cdot 2 + 6$$

$$12 = 6 \cdot 2 + 0$$

ultimo resto non nullo

DEFINIZIONE

$a, b \in \mathbb{N}$ sono detti coprimi se $\text{MCD}(a, b) = 1$

LEMMA

1) $a, p \in \mathbb{N}$, p primo, se $p \nmid a \Rightarrow \text{MCD}(p, a) = 1$

DIMOSTRAZIONE

$D(p) = \{1, -1, p, -p\} \Rightarrow D(a) \cap D(b) = \{-1, 1\}$ perché $p \nmid a$
 $\Rightarrow \text{MCD}(a, b) = 1$

LEMMA

2) $a, b \in \mathbb{N} \setminus \{0\}$, $d = \text{MCD}(a, b)$, allora $\exists a', b'$ t.c.

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

DIMOSTRAZIONE

Sia per assurdo che $\text{MCD}(a', b') > 1$ (a' e b' esistono per def. di divisibilità) e sia $\text{MCD}(a', b') = k > 1$

$k \mid a'$ e $k \mid b' \Rightarrow k \mid a$ e $k \mid b$ perché a e b sono multipli di

a' e b' $\Rightarrow \exists \alpha, \beta$ t.c. $a' = \alpha \cdot k$ e $b' = \beta \cdot k$

$$\Rightarrow a = d \alpha k \quad \text{e} \quad b = d \beta k$$

ma così ho che $k \mid a$ e $k \mid b$ ma ovviamente

$k \nmid d$ (se $k > 1$) e questo è assurdo perché d è $\text{MCD}(a, b)$

e ogni altro divisore di a e b deve dividere d

□

TEOREMA DI BEZOUT

$\forall a, b \in \mathbb{Z}, d = \text{MCD}(a, b), \exists u, v \in \mathbb{Z} \text{ t.c. } d = ua + vb$

In particolare, se a e b sono coprimi, $1 = ua + vb$

Esempio:

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

$$1218 = 132 \cdot 9 + 30 \rightarrow 30 = 1218 - 132 \cdot 9$$

$$132 = 30 \cdot 4 + 12 \rightarrow 12 = 132 - 30 \cdot 4$$

$$30 = 12 \cdot 2 + 6 \rightarrow 6 = 30 - 12 \cdot 2 \stackrel{30}{=} (132 - 30 \cdot 4) \cdot 2 =$$

$$12 = 6 \cdot 2 + 0 \quad = 30 - 132 \cdot 2 + 30 \cdot 8$$

$$= 30 \cdot 9 - 132 \cdot 2$$

$$= (1218 - 132 \cdot 9) \cdot 9 - 132 \cdot 2$$

$$= 1218 \cdot 9 - 132 \cdot 81 - 132 \cdot 2$$

$$= 1218 \cdot 9 - 132 \cdot 83 = 1218 \cdot 9 + 132(-83)$$

$$u = 9 \quad v = -83$$

CONSEGUENZE

1) $a, b, c \in \mathbb{Z}$, se $a | bc$ e $\text{MCD}(a, b) = 1 \Rightarrow a | c$

DIMOSTRAZIONE

$$a | bc \Rightarrow \exists k: bc = ka$$

$$\text{MCD}(a, b) = 1 \Rightarrow \exists u, v: 1 = au + bv$$

$$\Rightarrow c = c \cdot 1 = c(au + bv) = cau + cbv = cau + kav = \\ = a(cu + kv) \Rightarrow a | c$$

CONSEGUENZE

2) $a, b, p \in \mathbb{Z}$ p primo, se $p | ab \Rightarrow p | a$ oppure $p | b$

DIMOSTRAZIONE

Se $p \nmid a \Rightarrow \text{Med}(a, p) = 1$ (dimostrato prima)

\Rightarrow siamo nel caso 1) e $p \nmid b$

TEOREMA FONDAMENTALE DELL'ARITMETICA (in Tc)

$$z \in \mathbb{N} \setminus \{-1, 0, 1\}$$

$\exists k \geq 1$ e $p_1, \dots, p_k \in \mathbb{P}$ numeri primi tali che $z = p_1 \circ \dots \circ p_k$

La rappresentazione è unica a meno dell'ordine dei fattori e del loro segno cioè se $z = q_1 \dots q_s \Rightarrow s=k$ e viordinando,

$$|p_1| = |q_1| \dots |q_k| = |p_k|$$

DEFINIZIONE

Dati $a, b \in \mathbb{N}$, m si detto minimo comune multiplo (di a e b) se:

- 1) $a \mid m$ e $b \mid m$
- 2) Se t è t.c. $a \mid t$ e $b \mid t \Rightarrow m \mid t$

PROPRIETÀ

Dati $a, b \in \mathbb{N}$ e $d = \text{Med}(a, b)$, posto $a = a'd$ e $b = b'd$ si ha:

- 1) $m = a' \cdot b' \cdot d$ è un minimo comune multiplo per a, b
- 2) m' è un altro mcm $\Leftrightarrow m' = \pm m$

DIMOSTRAZIONE

- 2) uguale al caso del Med

- 1) $a \mid m$ e $b \mid m$ per definizione $m = (a'd)b' = a \cdot b' \Rightarrow a \mid m$
 $m = a'(db') = a' \cdot b \Rightarrow b \mid m$

Sia t altro multiplo comune di a e b , si ha:

$$\begin{aligned} a \mid t \text{ e } b \mid t &\Rightarrow \exists l, k : t = la = lb \quad \left\{ \begin{array}{l} la = a'd \\ lb = b'd \end{array} \right\} \end{aligned}$$

$$\Rightarrow la' = kb' \text{ e sappiamo } \text{Med}(a', b') = 1$$

Allora, da $la' = kb'$ ottengo che $a' \mid kb'$ (kb' è multiplo di a')
 \Rightarrow

$\Rightarrow a' \mid kb'$ e $\text{med}(a', b') = 1 \Rightarrow a' \mid k$ (per un teorema precedente) (per un teorema precedente) dove
 $\Rightarrow \exists s \in \mathbb{N} : k = sa'$
 Ma allora si $u_a \cdot t = kb = kb'sa' = (sa')b'sa' = s \cdot m$
 $\Rightarrow m \mid t$ \square

NOTAZIONE

Indichiamo con $\text{mem}(a, b)$ il valore positivo tra $\pm m$ dato dalla dimostrazione

OSSERVAZIONE

$$m = a'b'd$$

$$\text{mem}(a, b) = a'b' \text{med}(a, b)$$

$$\text{med}(a, b) \cdot \text{mem}(a, b) = \underbrace{a'b' \text{med}(a, b)}_{(a' \text{med}(a, b))} \cdot \underbrace{\text{med}(a, b)}_{b}$$

$$|ab| = \text{med}(a, b) \cdot \text{mem}(a, b)$$

Esempio:

$$\text{med}(494, 214) \text{ e } \text{mem}(494, 214)$$

$$494 = 214 \cdot 2 + 66 \quad \text{med}(494, 214) = 2$$

$$214 = 66 \cdot 3 + 16$$

$$66 = 16 \cdot 4 + 2$$

$$16 = 2 \cdot 8 + 0$$

$$2 = 66 - 16 \cdot 4 = 66 - 4(214 - 66 \cdot 3) = 66 - 4 \cdot 214 + 12 \cdot 66 = 13 \cdot 66 - 4 \cdot 214$$

$$= 13(494 - 214 \cdot 2) - 4 \cdot 214 = 13 \cdot 494 - 26 \cdot 214 - 4 \cdot 214 =$$

$$13 \cdot 494 - 30 \cdot 214$$

$$\text{mem}(494, 214) = \frac{494 \cdot 214}{2}$$

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

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

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

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

$$69 = 17 \cdot 4 + 1$$

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

$$\text{MCD}(689, 534) = 1$$

$$\begin{aligned} 1 &= 69 - 17 \cdot 4 = 69 - 4 \cdot (155 - 69 \cdot 2) = 69 - 4 \cdot 155 + 8 \cdot 69 = \\ 9 \cdot 69 - 4 \cdot 155 &= 9(534 - 155 \cdot 3) - 4 \cdot 155 = 9 \cdot 534 - 27 \cdot 155 - 4 \cdot 155 = \\ 9 \cdot 534 - 31 \cdot 155 &= 9 \cdot 534 - 31(689 - 534 \cdot 1) = 9 \cdot 534 - 31 \cdot 689 + \\ 31 \cdot 534 &= 40 \cdot 534 - 31 \cdot 689 \end{aligned}$$

$$\text{mmcm}(689, 534) = \frac{534 \cdot 689}{1}$$

DEFINIZIONE

$m \in \mathbb{Z} \times \mathbb{Z}$ è la relazione definita da:

$$a \equiv b \Leftrightarrow \exists k \in \mathbb{Z} : a - b = mk$$

$$\Leftrightarrow m \mid a - b$$

$$\Leftrightarrow \exists k \in \mathbb{Z} : a = b + mk$$

PROPOSIZIONE

$m \in \mathbb{Z}$ è una relazione di equivalenza compatibile con le operazioni + e ·.

cioè $\forall a, b, c, d \in \mathbb{Z}$ se $a \equiv b$ e $c \equiv d$ $\begin{cases} a + b \equiv c + d \\ b \equiv d \end{cases} \Rightarrow ab \equiv cd$

DIMOSTRAZIONE (compatibilità)

i) Se $a \equiv b$ e $c \equiv d \Rightarrow a + b \equiv c + d$

$$m \mid a - c \quad m \mid b - d$$

$$\exists k \in \mathbb{Z} : a - c = mk \quad \exists l \in \mathbb{Z} : b - d = ml$$

$$\text{Ma allora } (a + b) - (c + d) = (a - c) + (b - d) = mk + ml = m(k + l)$$

cioè $m \mid (a + b) - (c + d)$ che è equivalente a $ab \equiv cd$

ii) Se $a \equiv b$ e $c \equiv d \Rightarrow ab \equiv cd$

$$\exists k \in \mathbb{Z} : a - c = mk \quad \exists l \in \mathbb{Z} : b - d = ml$$

$$\text{Ma allora } (a - c)b = mkb = (kb)m$$

$$(b - d)c = mlc = (lc)m$$

$$\underline{(a - c)b + (b - d)c} = ab - cb + bc - dc = ab - dc$$

$$(kb)m + (lc)m = (kb + lc)m$$

$$\Rightarrow m \mid ab - dc \Rightarrow ab \equiv cd$$

#

$m \in \mathbb{Z}$ è una congruenza (v.e. compatibile con le operazioni)

ed è detta congruenza modulo m

$$a \equiv b$$

$$a \equiv b \pmod{m}$$

$$a \equiv_m b$$

} notazioni

Esempio

$$11 \equiv 1 \pmod{2} \quad 1+2m$$

$$\begin{array}{cccc} a & b & m & k \\ \cancel{1} & \cancel{1} & \cancel{1} & \cancel{1} \\ 11-1 = 10 & = 2 \cdot 5 & & \end{array}$$

$$-8 \equiv 4 \pmod{12}$$

$$-8-4 = -12 = 12(-1)$$

$$4-(-8) = 12 = 12(1)$$

DEFINIZIONE

L'insieme quoziente $\frac{\mathbb{Z}}{m\mathbb{Z}}$ si indica con \mathbb{Z}_m ed è detto **insieme degli interi modulo m** .

degli interi modulo m , gli elementi di \mathbb{Z}_m li indichiamo con $[x]_m$ oppure \bar{x}

$$\mathbb{Z}_2 = \{ \bar{0}, \bar{1} \} = \{ [0]_2, [1]_2 \}$$

PROPOSIZIONE

Dato $m \in \mathbb{Z}$ e $x \in \mathbb{Z}$ si ha $[x]_m = \{ x + mk : k \in \mathbb{Z} \}$ e se $m \neq 0$
 $[x]_m = [\text{rest}(x, m)]_m$

DIMOSTRAZIONE

Per definizione, si ha $y \in [x]_m \Leftrightarrow x \equiv y \pmod{m} \Leftrightarrow \exists k \in \mathbb{Z} \text{ t.c.}$

$$y-x = mk \Leftrightarrow \exists k \in \mathbb{Z} \text{ t.e. } y = x + mk$$

Se $m \neq 0$, posso dividere per $m \Rightarrow \exists q, r \text{ t.c. } x = mq + r$

$$\Rightarrow x - r = mq \Rightarrow x \equiv r \pmod{m} \Rightarrow [x]_m = [r]_m$$

□

OSSERVAZIONI

- 1) $\mathbb{Z}_{\leq m} = \{x\}$ perché $y \in \mathbb{Z}_{\leq m} \Rightarrow 0 \mid y - x \Rightarrow y \equiv x \pmod{m}$
- 2) $\forall m \neq 0 \quad \mathbb{Z}_{\leq m}$ è infinita, perché sono gli elementi del tipo $x + mk$, con $k \in \mathbb{Z}$
- 3) Se $m > 0$ e si hanno $a, b \in \mathbb{Z}$ con $0 \leq a, b < m$, allora $a \equiv b \pmod{m} \Leftrightarrow a = b$

DIMOSTRAZIONE

- 3)
- " \Leftarrow " Se $a \equiv b \pmod{m} \Rightarrow a \equiv b \pmod{m}$ è banale poiché $m \in \mathbb{Z}$ è di equivalenza
 - " \Rightarrow " Supponiamo che $a \geq b$ e sia per ipotesi $a \equiv b \pmod{m}$
 $\Rightarrow a - b = mk$
ma $a \geq b$ implica che $a - b \geq 0$ e $m \geq 0 \Rightarrow k \geq 0$
allora $a - b \leq a$ e $a - b = mk \leq a$
Ma per ipotesi $a < m \Rightarrow k$ deve essere 0 $\Rightarrow a - b = m \cdot 0 \Rightarrow a - b = 0 \Rightarrow a = b$

TEOREMA

Sia $m > 0$, $\mathbb{Z}_m = \{[0]_m, [1]_m, [2]_m, \dots, [m-1]_m\}$ e $|\mathbb{Z}_m| = m$

DIMOSTRAZIONE

- Da 3) si ha $[a]_m \neq [b]_m \forall a \neq b$ (perché $a \equiv b \pmod{m} \Leftrightarrow a = b$)
Dalla proposizione $\forall x \in \mathbb{Z}, \mathbb{Z}_m = \{\text{rest}(x, m)\}_m$ e $\text{rest}(x, m) \in \{0, 1, 2, \dots, m-1\}$

Esempio:

\Rightarrow

$$28 \equiv x \pmod{3}$$

$$x = \text{rest}(28, 3) = 1 \Leftrightarrow [28]_3 = [1]_3$$

Esempio:

Se ora sono le 16:00, che ora saranno tra 60 ore?

$$16 + 60 = 76 \equiv x \pmod{24}$$

$76 \equiv 4 \pmod{24} \Rightarrow$ saranno le 4 di mattina, 3 giorni dopo

$$76 = 24 \cdot 3 + 4$$

LEMMA

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

$$1) a \equiv b \pmod{m} \Leftrightarrow \forall t \in \mathbb{Z}, at \equiv bt \pmod{m}$$

$$2) a \equiv b \pmod{m} \Rightarrow \forall t \in \mathbb{Z}, at \equiv bt \pmod{m}$$

$$3) \text{ Se } at \equiv bt \pmod{m} \Rightarrow a \equiv b \pmod{m} \text{ se } \text{MCD}(t, m) = 1$$

DIMOSTRAZIONE

$$1) \exists m \text{ e' congruenza; quindi } t \equiv t \pmod{m} \quad \forall t \in \mathbb{Z} \text{ e } -t \equiv -t \pmod{m}$$

$$\text{allora da } a \equiv b \pmod{m} \Rightarrow at \equiv bt \pmod{m}$$

$$\text{da } at \equiv bt \pmod{m} \Rightarrow at - t \equiv bt - t \pmod{m}$$

$$2) \text{ Segue anche essa dal fatto che } mt \in \mathbb{Z} \text{ e' congruenza}$$

$$3) \text{ Supponiamo che } at \equiv bt \pmod{m} \text{ e sia } \text{MCD}(t, m) = 1$$

$$\text{per ipotesi } \exists k \in \mathbb{Z} : mk = at - bt = (a-b)t$$

$$m \text{ divide il prodotto tra } (a-b) \text{ e } t \text{ e } \text{MCD}(m, t) = 1$$

$$\Rightarrow \text{per un lemma precedente } m \mid a-b \Rightarrow a \equiv b \pmod{m}$$

□

Esempio:

$$12 \equiv 0 \pmod{6}$$

$$4 \cdot 3 \equiv 4 \cdot 0 \pmod{6}$$

$\begin{matrix} \downarrow & \downarrow & \downarrow \\ t & a & t & b & m \end{matrix}$

$$\text{Med}(m, t) = 2 = \text{Med}(6, 4)$$

e infatti $3 \not\equiv 0 \pmod{6}$

perché $6 \nmid 3$

LEMMA

Dato $m \in \mathbb{N}$, si ha:

1) $\forall a \in \mathbb{Z}, \mathbb{Z}_m = \{[a]_m, [a+1]_m, \dots, [a+(m-1)]_m\}$

2) $\forall a \in \mathbb{Z}: \text{Med}(a, m) = 1, \mathbb{Z}_m = \{[0]_m, [a]_m, [2a]_m, \dots, [(m-1)a]_m\}$

DIMOSTRAZIONE

Dal lemma precedente, $\forall a \in \mathbb{Z} \quad x \equiv y \pmod{m} \iff x+a \equiv y+a \pmod{m}$

$$\forall x < m \quad x+a \equiv y+a \quad \square$$

$$y \in [a+k] \text{ con } k < m \quad y = a+k \pmod{m}$$

$$y-a \equiv k \pmod{m}$$

$$a-y \equiv k \pmod{m}$$

$$-1 \equiv x \pmod{3}$$

$$-1 \equiv -1+3 \pmod{3}$$

$$-1 \equiv 2 \pmod{3}$$

Esempio:

$$12 \equiv x \pmod{9}$$

$$12 = 9 \cdot 1 + 3$$

$$[12]_9 = [3]_9$$

$$-1 \equiv x \pmod{9}$$

$$-1 \equiv -1+8 \pmod{9}$$

$$32 \equiv x \pmod{9}$$

$$[32]_9 = [5]_9$$

$$-1 \equiv 8 \pmod{9}$$

$$32 = 9 \cdot 3 + 5$$

DEFINIZIONE

$\forall m \in \mathbb{Z}$ sia $\mathbb{Z}_m^* = \{ [a]_m \mid \text{gcd}(a, m) = 1\} \subseteq \mathbb{Z}_m$

$|\mathbb{Z}_m^*|$ è detto indicatore di Gauss Euler e si indica con $\ell(m)$

Esempio

$$\ell(4) = 2$$

$$\mathbb{Z}_4^* = \{[1]_4, [3]_4\}$$

$$\ell(9) = 6 = |\{1, 2, 4, 5, 7, 8\}|$$

$$\text{Se } p \text{ è primo} \quad \mathbb{Z}_p^* = \{[1]_p, \dots, [p-1]_p\} \Rightarrow \ell(p) = p-1$$

$$\ell(p^2) = p^2 - 5 = p(p-1)$$

Esempio: $25 \rightarrow 5^2$ escludo $0, 5, 10, 15, 20$

$$\text{Inoltre } \ell(p^m) = p^m - p^{m-1} = p^{m-1}(p-1)$$

DEFINIZIONE

La funzione di Euler è $\ell : \mathbb{N} \rightarrow \mathbb{N}$

$$\ell(1) = 1$$

$$\ell(m) = |\{n \in \mathbb{N} \mid n < m \text{ e } \text{gcd}(m, n) = 1\}|$$

LEMMA

$\forall l, k \in \mathbb{N}$, $\ell(lk) = \ell(l) \cdot \ell(k)$, è una funzione moltiplicativa

DIMOSTRAZIONE

Si definisce $\Theta : \mathbb{Z}_{l,k} \rightarrow \mathbb{Z}_l \times \mathbb{Z}_k$

$$[a]_{lk} \mapsto ([a]_l, [a]_k)$$

È una funzione biettiva

□

$$\text{Se } m = p_1^{s_1} \cdots p_k^{s_k} \Rightarrow \ell(m) = \ell(p_1^{s_1}) \cdots \ell(p_k^{s_k}) =$$

$$= (p_1^{s_1} - p_1^{s_1-1}) \cdots (p_k^{s_k} - p_k^{s_k-1})$$

$$\text{Esempio: } \ell(12) = \ell(3 \cdot 2^2) = (3-1)(2^2-2^1) = 2(4-2) = 2 \cdot 2 = 4$$

PICCOLO TEOREMA DI FERMAT

Sia $p \in \mathbb{N}$ e' primo, allora $\forall a \in \mathbb{Z}$, $a^p \equiv a \pmod{p}$

$$32 \equiv 2 \pmod{5}$$

$$32 = 2^5$$

TEOREMA DI FERMAT-EULERO

Sia $m > 1$ e $a \in \mathbb{Z}$ tale che $\text{MCD}(a, m) = 1$, allora $a^{\varphi(m)} \equiv 1 \pmod{m}$

$$3^4 \equiv 1 \pmod{12}$$

(con $\varphi(12) = 4$)

TEOREMA DI WILSON

$p \in \mathbb{N} \setminus \{1\}$, allora p e' primo $\Leftrightarrow (p-1)! \equiv -1 \pmod{p}$

DEFINIZIONE

Dato $m > 0$, $a, b \in \mathbb{Z}$ chiamiamo l'equazione $ax \equiv b \pmod{m}$ **equazione congruenziale lineare**

TEOREMA

Dato $m > 0$, $a, b \in \mathbb{Z}$, l'equazione $ax \equiv b \pmod{m}$ ha soluzione se $\text{MCD}(a, m) = 1$

Detta s tale soluzione si ha $[s]_m = \{z \in \mathbb{Z} \mid az \equiv b \pmod{m}\}$

DIMOSTRAZIONE

Se $\text{MCD}(a, m) = 1 \Rightarrow \exists v, w \in \mathbb{Z}$ t.c. $1 = av + mw$

$$mw = 1 - av \Rightarrow m \mid 1 - av \Rightarrow 1 \equiv av \pmod{m}$$

$$b \cdot 1 \equiv b \cdot av \pmod{m} \Rightarrow \underbrace{a(bv)}_{s= bv} \equiv b \pmod{m}$$

$s = bv$ e' soluzione dell'equazione

Vediamo che $[s]_m \subseteq \{z \in \mathbb{Z} \mid az \equiv b \pmod{m}\}$

$$t \in [s]_m \Rightarrow t \equiv s \pmod{m} \Rightarrow at \equiv as \pmod{m}$$

$$\Rightarrow at \equiv as \pmod{m} \quad \left. \atop \right\} at \equiv s \pmod{m}$$

$$as \equiv b \pmod{m} \quad \left. \atop \right\} as \equiv b \pmod{m}$$

$$\Rightarrow t \in \{z \in \mathbb{Z} \mid az \equiv b \pmod{m}\}$$

Vediamo che $\{z \in \mathbb{Z} \mid az \equiv b \pmod{m}\} \subseteq [s]_m$

Se z è soluzione $\Rightarrow az \equiv b \pmod{m} \Rightarrow$ poiché anche
 $as \equiv b \pmod{m}$ si ha $az \equiv as \pmod{m} \Rightarrow z \equiv s \pmod{m}$
perché $\text{MCD}(a, m) = 1 \Rightarrow z \equiv s \pmod{m}$ implica $[z]_m = [s]_m$
e quindi $z \in [s]_m$

□

Esempio:

$$12x \equiv 8 \pmod{35} \quad \text{MCD}(12, 35) = 1$$

$$35 = 12 \cdot 2 + 11 \quad b = 8$$

$$12 = 11 \cdot 1 + 1$$

$$11 = 1 \cdot 11 + 0$$

$$1 = 12 - 11 \cdot 1 = 12 - (35 - 12 \cdot 2) = 12 - 35 + 2 \cdot 12 = -35 + 3 \cdot 12$$

$$5 = v \cdot b = 3 \cdot 8 = 24$$

$$\begin{matrix} & & & \\ & & & \\ & & & \\ \cancel{-1} = w & m & v & a \end{matrix}$$

L'insieme di tutte le soluzioni è $[24]_{35}$

Verifica

$$\underbrace{12 \cdot 24}_{288} \equiv 8 \pmod{35}$$

$$288 = 8 \cdot 36$$

$$\text{rest}(288, 35) = 8$$

$$8 \cdot 36 \equiv 8 \cdot 1 \pmod{35} \quad \text{MCD}(8, 35) = 1$$

$$36 \equiv 1 \pmod{35}$$

TEOREMA

$m > 0, a, b \in \mathbb{Z}, t \in \mathbb{Z} : t|a, t|b, t|m$

Allora $ax \equiv b \pmod{m}$ ha soluzione $s \in \mathbb{Z} \Leftrightarrow$

$\frac{a}{t}x \equiv \frac{b}{t} \pmod{\frac{m}{t}}$ ha soluzione $s \in \mathbb{Z}$

TEOREMA

L'equazione $ax \equiv b \pmod{m}$ ha soluzioni $\Leftrightarrow \text{MCD}(a, m) | b$

DIMOSTRAZIONE

" \Rightarrow " Sia $s \in \mathbb{Z}$ una soluzione di $ax \equiv b \pmod{m}$.

Allora si ha $as \equiv b \pmod{m}$ e cioè $\exists l \in \mathbb{Z} : ml = as - b$

$$\Rightarrow as - ml = b$$

$$\begin{aligned} \text{Visto che } \text{MCD}(a, m) | a \\ \text{MCD}(a, m) | m \end{aligned} \quad \left. \begin{array}{l} \text{MCD}(a, m) | (as - ml) = b \end{array} \right\}$$

$$\Rightarrow \text{MCD}(a, m) | b$$

" \Leftarrow "

Sia $\text{MCD}(a, m) | b$. Allora se $d = \text{MCD}(a, m)$ si ha
 $d | a, d | b$ e $d | m$. Inoltre $\text{MCD}\left(\frac{a}{d}, \frac{m}{d}\right) = 1$

$$\Rightarrow \frac{a}{d}x \equiv \frac{b}{d} \pmod{\frac{m}{d}}$$
 ha soluzione

Quindi $ax \equiv b \pmod{m}$ ha anch'essa soluzione ed è la stessa

H

OSSERVAZIONE

$$S = \left\{ z \in \mathbb{Z} : az \equiv b \pmod{m} \right\} = \left\{ z \in \mathbb{Z} : \frac{a}{d}z \equiv \frac{b}{d} \pmod{\frac{m}{d}} \right\}$$

$$S = [s]_{\frac{m}{d}} = [s]_m \cup [s + \frac{m}{d}]_m \cup [s + \frac{2m}{d}]_m \cup \dots \cup$$

$$[s + \frac{(d-1)m}{d}]_m$$

Esempio:

$$84x \equiv 108 \pmod{500}$$

$$\text{MCD}(500, 84) = 4$$

$$500 = 84 \cdot 5 + 80$$

$$108 = 4 \cdot 27$$

$$84 = 80 \cdot 1 + 4$$

poiché $4 \mid 108$, ho soluzione

$$80 = 4 \cdot 20 + 0$$

$$\frac{84}{4} x \equiv \frac{108}{4} \pmod{\frac{500}{4}} \rightarrow 21x \equiv 27 \pmod{125} \quad \text{MCD}(125, 21) = 1$$

$$125 = 21 \cdot 5 + 20$$

$$21 = 20 \cdot 1 + 1$$

$$20 = 1 \cdot 20 + 0$$

$$1 = 21 - 20 = 21 - (125 - 21 \cdot 5) = 21 - 125 + 21 \cdot 5 = 125 + 21 \cdot 6$$

$$5 = 6 \cdot 27 = 162$$

$$[162]_{125} = [162]_{500} + [162 + \frac{500}{4}]_{500} + [162 + 2 \cdot \frac{500}{4}] + [162 + 3 \cdot \frac{500}{4}]$$

$$162 = 125 \cdot 1 + 37$$

$$[162]_{125} = [37]_{125}$$

resto

PARTE DELLA DEMOSTRAZIONE DELL'OSSERVAZIONE PRECEDENTE

$$t \in \text{ES} \quad \frac{m}{d}$$

\uparrow
 \downarrow
 se e soltanto se
 $t = s + im \quad i \in \mathbb{Z}$

$$\sum_{i=0}^{d-1} \left[s + \frac{im}{d} \right]_m$$

$$\exists l_i \in \mathbb{Z}: t = s + l_i \frac{m}{d}$$

$$l_i = k d_i \quad \xrightarrow{\hspace{1cm}}$$

(divisione di l_i per d)

$$\exists i, k: t = s + im + km \frac{d}{d}$$

$$= s + (i + kd) \frac{m}{d}$$



TEOREMA CHINESE DEL RESTO

- Siano $m_1, \dots, m_k \in \mathbb{N}$ a due a due coprimi
- $\forall i \neq j \quad \text{MCD}(m_i, m_j) = 1$
- Siano $b_1, \dots, b_k \in \mathbb{Z}$, allora il sistema:

$$\begin{cases} x \equiv b_1 \pmod{m_1} \\ \vdots \\ x \equiv b_k \pmod{m_k} \end{cases} \quad \text{ha soluzione } s$$

L'insieme di tutte le soluzioni è $\text{ES}_{m_1, m_2, \dots, m_k}$

GENERALIZZAZIONE

$$\begin{cases} x \equiv b_1 \pmod{m_1} \\ \vdots \\ x \equiv b_k \pmod{m_k} \end{cases} \quad \text{ha soluzione} \Leftrightarrow \text{MCD}(m_i, m_j) \text{ divide } b_i - b_j \quad (i \neq j)$$

OSSERVAZIONE

Dato il sistema

$$\begin{cases} a_1 x \equiv b_1 \pmod{m_1} \\ \vdots \\ a_k x \equiv b_k \pmod{m_k} \end{cases}$$

$$a_k x \equiv b_k \pmod{m_k}$$

$$\text{ha soluzione} \Leftrightarrow \begin{cases} x \equiv s_1 \pmod{m_1} \\ \vdots \\ x \equiv s_k \pmod{m_k} \end{cases} \quad \text{ha soluzione}$$

dove si è la soluzione di $a_i x \equiv b_i \pmod{m_i}$

Esempio:

$$\begin{cases} x \equiv 4 \pmod{5} \\ x \equiv 3 \pmod{4} \end{cases} \quad \text{MCD}(4, 5) = 1 \quad \text{OK}$$

1) trovo la generica soluzione di $x \equiv 4 \pmod{5}$

$$x - 4 = 4y \cdot 5 \Rightarrow x = 4 + 5y \quad y \in \mathbb{Z}$$

2) impongo $4 + 5y$ come soluzione di $x \equiv 3 \pmod{4}$

$$4 + 5y \equiv 3 \pmod{4} \rightarrow 5y \equiv -1 \pmod{4} \quad (-1 \equiv 3 \pmod{4})$$
$$5y \equiv 3 \pmod{4}$$

3) risolvo $5y \equiv 3 \pmod{4}$

$$\text{MCD}(5, 4) = 1$$

$$\begin{array}{l} 5 = 4 \cdot 1 + 1 \\ 4 = 1 \cdot 4 + 0 \end{array} \quad \left. \begin{array}{l} 1 = 5 - 4 \\ 1 = 4 - 1 \cdot 4 \end{array} \right\} \quad y = 6v = 3$$

v coefficiente vicino al 5 (1)

$$6 = 3$$

4) La soluzione è data da (1): $4 + 5 \cdot 3 = 19$

5) La classe delle soluzioni è $[19]_{20}$

Esempio:

$$\begin{cases} x \equiv 2 \pmod{3} \\ x \equiv 3 \pmod{4} \\ x \equiv 4 \pmod{5} \end{cases} \quad \boxed{\text{La generica soluzione è } [19]_{20}}$$

$$\hookrightarrow 19 + 20y, y \in \mathbb{Z}$$

6) Impongo $19 + 20y$ come soluzione di $x \equiv 2 \pmod{3}$

$$19 + 20y \equiv 2 \pmod{3}$$

$$20y \equiv -17 \pmod{3}$$

$$2y \equiv 1 \pmod{3}$$

$$\left\{ \begin{array}{l} -17 = -18 + 1 = (-6)3 + 1 \\ -17 \equiv 1 \pmod{3} \\ 20 = 18 + 2 = 6 \cdot 3 + 2 \\ 20 \equiv 2 \pmod{3} \end{array} \right.$$

7) Risolvo $2y \equiv 1 \pmod{3}$

risultato è $y = -1 \equiv 2 \pmod{3}$

8) Sostituisco in $19 + 20y$

$$S = 19 + 20 \cdot 2 = 59 \rightarrow [59]_{60}$$

ALTRA TECNICA

$$x \equiv 3 \pmod{5}$$

$$x \equiv 3 \pmod{7}$$

$$x \equiv 9 \pmod{11}$$

$$m = 5 \cdot 7 \cdot 11 = 385$$

$$\left. \begin{array}{l} m_1 = 7 \cdot 11 = 77 \\ m_2 = 5 \cdot 11 = 55 \\ m_3 = 5 \cdot 7 = 35 \end{array} \right\} \begin{array}{l} 77x \equiv 1 \pmod{5} \\ 55x \equiv 1 \pmod{7} \\ 35x \equiv 1 \pmod{11} \end{array}$$

Risolvo:

$$1) 77x \equiv 1 \pmod{5} \quad s_1 = 3$$

$$2) 55x \equiv 1 \pmod{7} \quad s_2 = 6$$

$$3) 35x \equiv 1 \pmod{11} \quad s_3 = 6$$

La soluzione è:

$$S = m_1 b_1 s_1 + m_2 b_2 s_2 + m_3 b_3 s_3 = 77 \cdot 3 \cdot 1 + 55 \cdot 3 \cdot 6 + 35 \cdot 9 \cdot 6 \\ = 3573$$

$$\text{La soluzione generica è } [3573]_{305} = [108]_{385}$$

resto di $3573 : 305$

CONGRUENZE MODULO M IN TL (NICOTERA), STRUTTURE ALGEBRICHÉ

La compatibilità della relazione \equiv_m con $+$ e \cdot , ci permette di definire delle operazioni nell'insieme $TL_{m+1} = TL_m$

$\forall a \in TL_m, c \in TL_m \in TL_m$ posso definire $[a]_m + [c]_m = [a+c]_m$

$$[a]_m = [b]_m$$

$$\Rightarrow a \equiv b \pmod{m}$$

$$[c]_m = [d]_m$$

$$\Rightarrow c \equiv d \pmod{m}$$

\Rightarrow per la compatibilità dell'addizione

$$a+c \equiv b+d \pmod{m}$$

$$\Rightarrow [a+c]_m = [b+d]_m$$

Analogamente

$\forall a \in TL_m, c \in TL_m \in TL_m$ posso definire $[a]_m \cdot [c]_m = [ac]_m$

$$[a]_m = [b]_m \quad a \equiv b \pmod{m}$$

$$[c]_m = [d]_m \quad c \equiv d \pmod{m}$$

\Rightarrow per la compatibilità della moltiplicazione

$$ac \equiv bd \pmod{m} \Rightarrow [ac]_m = [bd]_m$$

Esempio:

$$m=2 \quad TL_2 = \{[0], [1]\}, \text{ posso considerare } + \text{ e } \cdot$$

+	[0]	[1]
[0]	[0]	[1]
[1]	[1]	[0]

$[1] + [1] = [2] = [0]$

•	[0]	[1]
[0]	[0]	[0]
[1]	[1]	[1]

$m=3$	$\mathbb{L}_3 = \{\bar{0}, \bar{1}, \bar{2}\}$	$+ \begin{array}{c} \bar{0} \bar{1} \bar{2} \\ \hline \bar{0} \bar{1} \bar{2} \end{array}$	$\bar{1} + \bar{2} = \bar{3} = \bar{0}$
$I \times 3 = \bar{x}$		$\bar{1} \bar{1} \bar{2} \bar{5}$	$\bar{2} + \bar{2} = \bar{4} = \bar{1}$
		$\bar{2} \bar{2} \bar{0} \bar{1}$	

$$m=6 \quad \mathbb{L}_6 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}\}$$

$+ \bar{0} \bar{1} \bar{2} \bar{3} \bar{4} \bar{5}$	$\cdot \bar{0} \bar{1} \bar{2} \bar{3} \bar{4} \bar{5}$
$\bar{0} \quad \bar{1} \quad \bar{2} \quad \bar{3} \quad \bar{4} \quad \bar{5}$	$\bar{0} \quad \bar{1} \quad \bar{2} \quad \bar{3} \quad \bar{4} \quad \bar{5}$
$\bar{1} \quad \bar{2} \quad \bar{3} \quad \bar{4} \quad \bar{5} \quad \bar{0}$	$\bar{1} \quad \bar{0} \quad \bar{1} \quad \bar{2} \quad \bar{3} \quad \bar{4}$
$\bar{2} \quad \bar{3} \quad \bar{4} \quad \bar{5} \quad \bar{0} \quad \bar{1}$	$\bar{2} \quad \bar{0} \quad \bar{2} \quad \bar{4} \quad \bar{0} \quad \bar{2}$
$\bar{3} \quad \bar{4} \quad \bar{5} \quad \bar{0} \quad \bar{1} \quad \bar{2}$	$\bar{3} \quad \bar{1} \quad \bar{3} \quad \bar{5} \quad \bar{2} \quad \bar{4}$
$\bar{4} \quad \bar{5} \quad \bar{0} \quad \bar{1} \quad \bar{2} \quad \bar{3}$	$\bar{4} \quad \bar{2} \quad \bar{4} \quad \bar{0} \quad \bar{3} \quad \bar{5}$
$\bar{5} \quad \bar{0} \quad \bar{1} \quad \bar{2} \quad \bar{3} \quad \bar{4}$	$\bar{5} \quad \bar{3} \quad \bar{0} \quad \bar{2} \quad \bar{4} \quad \bar{1}$

Tabelle addizione; sono tutte simmetriche rispetto alla diagonale principale

$$\forall [a]_m, [b]_m \in \mathbb{L}_m \quad [a]_m + [b]_m = [b]_m + [a]_m = [a+b]_m = [b+a]_m$$

perché + in \mathbb{L}_m è commutativa

Inoltre $[0]$ è elemento neutro rispetto all'addizione

$$\forall [a]_m \quad [a]_m + [0]_m = [a]_m$$

Ogni elemento di \mathbb{L}_m ha un opposto

Nella riga di ogni elemento trovo $[0]_m$

$$\forall [a]_m \in \mathbb{L}_m \quad \exists [b]_m \in \mathbb{L}_m ; \quad [a]_m + [b]_m = [0]_m$$

$-[a]_m$ è l'opposto della classe di $[a]_m$

$$\text{Esempio in } \mathbb{L}_6 : -[5]_6 = [1]_6 ; -[4]_6 = [2]_6 ; -[3]_6 = [3]_6$$

$$\forall [a]_m \in \mathbb{L}_m \quad -[a]_m = [m-a]_m$$

$$\mathbb{L}_{12} \quad -[5]_m = [12-5]_m = [7]_m$$

Sì può provare che τ è associativa.

$\forall a \in \mathbb{L}, b, c \in \mathbb{L}$ m

$$(a\tau b)\tau c = a\tau (b\tau c)$$

$$(a\tau b)\tau c = a\tau (b\tau c) = a\tau (b+c) =$$

$$\text{Essendo } \tau \text{ associativa in } \mathbb{L} : [a+(b+c)] = [a+b+c]$$

$$= a\tau (b+c)$$

$(\mathbb{L}, +)$ + associativa
+ commutativa

$\exists 0 \in \mathbb{L}$ elemento neutro / $\forall a \in \mathbb{L} \exists (a + 0) \in \mathbb{L}$:

Ogni elemento ha opposto /

$$[a + b] = 0$$

Una struttura che possiede queste quattro proprietà è detto **gruppo abeliano**.

DEFINIZIONE

$B \neq \emptyset$, τ operazione in B

(B, τ) è un gruppo abeliano $\Leftrightarrow \tau$ associativa

esiste elemento neutro per τ
ogni elemento ha opposto
+ commutativa

Se manca solo la commutatività allora è un **gruppo**

Esempi: $(\mathbb{N}_0, +)$, $(\mathbb{R}, +)$, $(\mathbb{Q}, +)$

(\mathbb{L}, τ) non è gruppo abeliano.

S insieme, $\tau: S \times S \rightarrow S$, τ biettiva con o è solo gruppo

la composizione è associativa

$\text{id}_S: x \in S \mapsto x \in S$

Ogni elemento ha inverso: $\forall \tau \text{ biettiva} \exists \tau^{-1}$

$$\tau \circ \tau^{-1} = \text{id}_S = \tau^{-1} \circ \tau$$

Manca la commutatività $g \circ f \neq f \circ g$

Consideriamo le tabelle relative a:

Sono tutte **simmetriche** rispetto alla diagonale principale.

• E' comutativa, $\forall [a], [b] \in \mathbb{Z}_m : [a][b] = [b][a]$

• E' associativa, $\forall [a], [b], [c] \in \mathbb{Z}_m : [a][b][c] = ([a][b])[c] = [a][b][c]$

$[1]$ e' elemento neutro

$\forall [a] \in \mathbb{Z}_m : [a][1] = [a] = [a][1]$

• $[1]$ e' elemento neutro?

DEFINIZIONE

$[a] \in \mathbb{Z}_m$, $[a]$ e' invertibile $\Leftrightarrow \exists [b] \in \mathbb{Z}_m : [a][b] = [1]$

$[0]$ non e' mai invertibile, considero $\mathbb{Z}_m \setminus \{0\}$

$[1]$ e' sempre invertibile

II Si puo dimostrare che tutti gli elementi di $\mathbb{Z}_m \setminus \{0\}$ sono invertibili $\Leftrightarrow m$ e' primo

III Considerata $[a] \in \mathbb{Z}_m \setminus \{0\}$, $[a]$ e' invertibile

$$\Leftrightarrow \text{HCD}(a, m) = 1$$

OSSERVAZIONE

Se $a, b \in \mathbb{Z}$

$$ab = 0 \Leftrightarrow \begin{cases} a = 0 \\ b = 0 \end{cases}$$

Legge di annullamento del prodotto

Nella struttura \mathbb{Z}_m non vale perch'e

$$\bar{2} \cdot \bar{2} = \bar{0} \quad \text{nella tabella } \mathbb{Z}_2$$

$$\begin{aligned} \bar{3} \cdot \bar{4} &= \bar{0} \\ \bar{2} \cdot \bar{3} &= \bar{0} \end{aligned} \quad \left. \begin{array}{l} \text{nella tabella } \mathbb{Z}_6 \\ \text{perche' in generale non tutti gli elementi hanno l'inverso} \end{array} \right.$$

$(\mathbb{Z}_m \setminus \{0\}, \circ)$ in generale non e' un gruppo

(perche' in generale non tutti gli elementi hanno l'inverso)

DIMOSTRAZIONE:

$[a][a] \in \mathbb{Z}_m \setminus \{0\}$

$[a][a]$ è invertibile $\Leftrightarrow \text{MCD}(a, m) = 1$

" "
 \Rightarrow "

Supponiamo che $[a][a]$ sia invertibile, allora $\exists [b] \in \mathbb{Z}_m \setminus \{0\}$ t.c.

$$[a][a][b] = [a][b] = [1] \Rightarrow ab \equiv 1 \pmod{m} \Rightarrow m \mid 1-ab$$

$$\Rightarrow 1-ab = mk \text{ con } k \in \mathbb{Z} \Rightarrow 1 = ab + mk$$

Supponiamo che $d > 0$, $d \mid a$, $d \mid b \Rightarrow m = dt$ $a = dh$, $t, h \in \mathbb{Z}$

$$\text{Quindi } 1 = ab + mk = d(hb + tk) = d(mb + tk) \Rightarrow d \mid 1 \Rightarrow d = 1$$

$$\text{MCD}(a, m) = 1$$

" "
 \Leftarrow "

Sia $\text{MCD}(a, m) = 1$, allora per il teorema di Bezout

$$\exists u, v \in \mathbb{Z}: 1 = au + mv$$

$$\text{Allora } mv = 1 - au \Rightarrow m \mid 1 - au \Rightarrow au \equiv 1 \pmod{m}$$

$$\Rightarrow [a][u] = [a][u] - [1] \Rightarrow [0][u] \text{ è invertibile e } [a][u]^{-1} = cu$$

□

In particolare se p è primo, $\forall 1 \leq a \leq p-1$, $\text{MCD}(a, p) = 1$

$\forall [a] \in \mathbb{Z}_p \setminus \{0\}$, $[a][a]$ è invertibile

$(\mathbb{Z}_p \setminus \{0\})^*$ è un gruppo abeliano □

Se m non è primo, non tutti gli elementi di $\mathbb{Z}_m \setminus \{0\}$

Gli elementi invertibili di $\mathbb{Z}_m \setminus \{0\}$ sono tanti quanti

sono gli interi positivi minori di m e coprimi con m

STRUTTURE ALGEBRICHE \rightarrow sono $(\mathbb{N}, +, \cdot)$, \mathbb{Z} , \mathbb{Q} ecc. $(\mathbb{A}, +, \cdot)$

$(G, +)$ gruppo

\Leftrightarrow 1) è associativa, $\forall a, b, c \in G$

$$(a+b)+c = a+(b+c)$$

2) \exists l'elemento neutro rispetto a +

cioè $\exists e \in G$, $a+e=a=e+a \forall a \in G$

3) Ogni elemento possiede il simmetrico rispetto a + (nel caso di + è l'opposto)

$$\forall a \in G \exists -a \in G : -a+a=0$$

gruppo abeliano \Leftrightarrow 4) + è commutativa

$$\forall a, b \in G, a+b=b+a$$

$(A, +, \cdot)$ anello \Leftrightarrow • rispetto alla prima operazione (+) ha

un gruppo abeliano

• la seconda ^{op.} è associativa (\cdot)

• la seconda operazione è distributiva

rispetto alla prima, $\forall x, y, z \in A, x(y+z) = xy+xz$

$$(x+y)z = xz + yz$$

anello commutativo \Leftrightarrow la seconda operazione è anche

commutativa (oltre che associativa e distributiva)

anello unitario \Leftrightarrow \exists elemento

rispetto alla seconda operazione

Esempi: $(\mathbb{L}, +, \cdot)$ anello commutativo unitario

$$(\mathbb{L}_m, +, \cdot) \quad //$$

$$(\mathbb{R}, +, \cdot) \quad //$$

$$(\mathbb{CQ}, +, \cdot) \quad //$$

$(A, +, \cdot)$ campo \Leftrightarrow $(A, +, \cdot)$ è anello commutativo unitario
e invertibile rispetto alla seconda operazione
con a diverso dall'elemento neutro rispetto alla prima operazione

Esempi:

$(\mathbb{R}, +, \cdot)$ è campo

$(\mathbb{Q}, +, \cdot)$ //