

→ NOTAZIONI

DEF: LEGGE DI COMPOSIZIONE

sia $S | S \neq \emptyset$ e $f: S \times S \rightarrow S$

$a, b \in S \rightarrow f(a, b) \in S$

$\Rightarrow f$ è CORRISPONDENZA BINARIA | $(a, b) \xrightarrow{f} f(a, b)$
con (S, f) STRUTTURA ALGEBRICA

se f ADDITIVA : $f(a, b) = a + b \Rightarrow$ lo è anche la struttura $(S, f) = (S, +)$

se MOLTIPLICATIVA $f(a, b) = ab \Rightarrow (S, f) = (S, \cdot)$

PROPRIETÀ

ASSOCIAZIONE

$$\forall a, b, c \quad a + (b + c) = (a + b) + c = a + c + b$$

$$a \cdot (b \cdot c) = (a \cdot b) \cdot c = (a \cdot c) \cdot b$$

ELEMENTO NEUTRO

$$\exists 0 | \forall a \in S \quad a + 0 = 0 + a = a$$

$$a \cdot 1 = 1 \cdot a = a$$

ELEMENTO INVERSO (-)

OPPOSTO (+)

$$a \in S \Rightarrow -a |$$

$$a + (-a) = (-a) + a = 0$$

$$a \cdot a^{-1} |$$

$$a \cdot a^{-1} = a^{-1} \cdot a = 1$$

COMMUTATIVITÀ

(ABEUANITÀ)

$$\forall a, b \in S \quad a + b = b + a$$

$$\forall a, b \in S \quad a \cdot b = b \cdot a$$

→ GRUPPO

sia (S, f) con $f = \{ + \} \Rightarrow (S, f)$ è un GRUPPO se :

- f è associativa
- \exists elemento neutro
- \exists elemento opposto / inverso

$\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$

es. $(\mathbb{Z}, +)$ è un gruppo COMMUTATIVO :

es. $(\mathbb{Q} \setminus \{0\}, \cdot)$ è un gruppo commutativo

es. $(\mathbb{N}, +)$ non è un gruppo

es. (\mathbb{Z}, \cdot) non è un gruppo

→ GRUPPO SIMMETRICO DI ORDINE n

sia $f: X \rightarrow Y \Rightarrow$ si ha che:

- f è **INIEZIONE** se $\forall x, x' \in X \quad f(x) = f(x') \Rightarrow x = x'$
- f è **SURIEZIONE** se $\forall y \in Y \quad \exists x \in X \mid f(x) = y$
- f è **BIEZIONE** se è entrambe le precedenti.

sia $n \in \mathbb{N} \mid n \geq 1 \Rightarrow [n] = \{1, \dots, n\}$

$\Rightarrow S_n = \{f: [n] \rightarrow [n] \mid f \text{ è biieziona}\}$

indichiamo $[n]$ con X .

sia $\varphi, \psi \in S_n \Rightarrow \varphi, \psi: X \rightarrow X$ biiezionate

si definisce $g \circ \varphi: X \rightarrow X$ la **COMPOSTA** di φ e ψ come
 $\forall x \in X \quad (\varphi \circ \psi)(x) = \psi(\varphi(x))$, ovvero
 $x \xrightarrow{\varphi} \varphi(x) \xrightarrow{\psi} \psi(\varphi(x)) = (\psi \circ \varphi)(x)$.

$\forall \varphi, \psi \in S_n \Rightarrow \psi \circ \varphi \in S_n$

sia (S_n, \circ) questo è un **GRUPPO SIMMETRICO DI ORDINE n**

dato che:

- \circ è associativa: $(\varphi \circ \psi) \circ \eta = \varphi \circ (\psi \circ \eta)$
- \exists unità: $\text{id}: X \rightarrow X$ com $\text{id}(x) = x$
 $\forall \varphi \in S_n \quad \text{id} \circ \varphi = \varphi \circ \text{id} = \varphi$
- \exists inverso $\forall \varphi \in S_n \mid \varphi: X \rightarrow X$ biiezionate
 $\Rightarrow \exists \varphi^{-1}: X \rightarrow X$ **INVERSA** definita come:
 $\forall z \in X \quad \varphi^{-1}(z) = x \mid \varphi(x) = z$
quindi ho che $\varphi^{-1} \circ \varphi = \varphi \circ \varphi^{-1} = \text{id}$

S_n ha più proprietà:

1) sia $n \geq 1 \mid X = [n] = \{1, \dots, n\} \Rightarrow \text{Card}(S_n) = n!$

dove $n! = \begin{cases} 1 & \text{se } n = 0 \\ n(n-1)! & \text{se } n > 0 \end{cases}$

2) $f \in S_n$ è rappresentata con una tabella a 2 righe

$$f = \begin{pmatrix} 1 & \dots & n \\ f(1) & \dots & f(n) \end{pmatrix}$$

es. $n=2 \Rightarrow X = [2] = \{1, 2\} \Rightarrow S_n = S_2$

$\text{Card}(S_2) \Rightarrow 2! = 2$

$$\text{id} = \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix} \quad \sigma = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}$$

ogni S_n ha una tabella moltiplicativa associata.

→ ANELLO

quello $A = \{ \} | A \neq \emptyset$ è formato di 2 o più numeri

+ e \cdot \Rightarrow si ha $(A, +, \cdot)$

↪ supporto / sostegno dell'anello

valgono le seguenti proprietà:

1) $(A, +)$ è un gruppo abeliano

2) (A, \cdot) dove \cdot è associativa

3) LEGGI DISTRIBUTIVE: $\forall a, b, c \in A$

$$\text{se } a \cdot (b+c) = a \cdot b + a \cdot c \Leftrightarrow (b+c) \cdot a = ba+ca$$

4) se (A, \cdot) commutativo $\Rightarrow A$ commutativo

5) A unitario se (A, \cdot) ha elt. neutro

es. $(\mathbb{Z}, +, \cdot)$ è un anello commutativo e unitario

→ MATEMATICA

$m, n \geq 1$ $M_{m,n}(\mathbb{R})$ è l'insieme delle matrici a coefficienti reali in \mathbb{R} di dimensione $m \times n$ con m righe e n colonne.

$\Rightarrow M = (m_{i,j})$ con $i \in \{1, \dots, m\}$, $j \in \{1, \dots, n\}$

e $M_{m,n}(\mathbb{R}) = \{M = (m_{i,j}) \text{ con } i \in \{1, \dots, m\}, j \in \{1, \dots, n\}\}$

SOMMA:

considero $(M_{m,n}(\mathbb{R}), +)$ e $A, B \in M_{m,n}(\mathbb{R})$ dove

$A = (a_{i,j})$ e $B = (b_{i,j}) \Rightarrow A + B = (a_{i,j} + b_{i,j})$.

Sono solo se hanno $m \times n$ uguali.

PROPOSIZIONE: sia $m, n \in \mathbb{N}$ | $m, n \geq 1$

$\Rightarrow (M_{m,n}(\mathbb{R}), +)$ è un gruppo abeliano

PRODOTTO:

si considera $m = n \Rightarrow M$ quadrata di ordine n

$A = (a_{i,j})$ e $B = (b_{i,j})$

$A \cdot B = C = (c_{i,j})$ dove $c_{i,j} = \sum_{l=1}^n a_{i,l} \cdot b_{l,j}$

PROPOSIZIONE: $(M_{m,n}(\mathbb{R}), +, \cdot)$ è un'unità
reale e non commutativo.

DIMOSTRAZIONE:

unitàre perché $I_n = I = (m_{i,j})$ matrice di identità
è l'elt neutro

$$m_{i,j} = \begin{cases} 1 & \text{se } i=j \\ 0 & \text{altrimenti} \end{cases} \quad (\text{id})$$

$$I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

$$\forall A \in M_{m,n}(\mathbb{R}) \quad A \cdot I_n = A$$

non abeliano perché il prodotto tra matrici non
è commutativo $A \cdot B \neq B \cdot A$.

es. quello dei polinomi a coefficienti reali in una inde-
terminata x : $\mathbb{R}[x] = \{ \text{polinomi}, p(x) = \sum_{i=0}^n a_i x^i \text{ con}$
 $a_i \in \mathbb{R} \text{ e } n \geq 0 \}$

$(\mathbb{R}[x], +, \cdot)$ è un'unitàre e abeliano.

elt. neutro è $1 = 1 \cdot x^0$

→ CAMPO

anche detto corpo commutativo.

sia $(A, +, \cdot)$ quello $\Rightarrow A$ è un campo se $(A, +)$ e
 $(A \setminus \{0\}, \cdot)$ sono gruppi abeliani.

es. $(\mathbb{Q}, +, \cdot)$ è campo dei numeri razionali.

es. $(\mathbb{R}, +, \cdot)$ è campo dei numeri reali.

→ RELAZIONE

RELAZIONE BINARIA: sia X insieme $| X \neq \emptyset$

sia $R \subseteq X \times X$ relazione binaria.

sia $(a, b) \in R \Rightarrow a R b$.

una **RELAZIONE DI EQUIVALENZA** R è tale su X se:

1) p. riflessiva: $\forall a \in X \quad aRa \Leftrightarrow (a, a) \in R$

2) p. simmetrica: $\forall a, b \in X \quad aRb \Leftrightarrow bRa$

3) p. transitiva: $\forall a, b, c \in X \quad aRb, bRc \Leftrightarrow aRc$

se R di equivalenza $\Leftrightarrow a = b$ equivalente

es. X insieme, $a, b \in X$, aRb e $a = b$

$\Rightarrow R$ d'equivalenza

es. $X = \{\text{rette del piano euclideo}\}$

$r, r' \in X$ e $r R r'$, se $r \parallel r' \Rightarrow R$ d'equivalenza

sia R d'equivalenza su X , $a \in X$ è **CLASSE D'EQUIVALENZA**

di $X | [a] = \{b \in X | aRb\}$. a è **RAPPRESENTANTE** di $[a]$.

l'**INSIEME QUOTIENTE** di X su R (X modulo R) è

l'insieme $X/R = \{[a] | a \in X\}$

osservazioni:

1) $\forall a \in X \Rightarrow a \in [a]$

2) $\forall a \in X \quad [a] \neq \emptyset$ perché $aRa \Rightarrow a \in [a]$ \square

3) $aRb \Leftrightarrow [a] = [b]$ perché $a \in [a] = [b] \Rightarrow a \in [b] \Rightarrow aRb$
e perché $bRa \Rightarrow [a] \subseteq [b] \wedge [b] \subseteq [a]$ \square

4) $[a], [b] \in X/R \Rightarrow [a] \cap [b] = \emptyset \oplus [a] = [b]$

5) $X = \bigcup_{a \in X} [a]$ l'unione è disgiunta

↳ **PARTIZIONE**

→ RELAZIONE D'ORDINE

- S insieme | $S \neq \emptyset$, sia \leq una relazione binaria su S .
 qualunque $\leq \in S \times S$. \leq è di **ORDINE PARZIALE** se soddisfa:
 1) p. riflessiva: $\forall x \in S \quad x \leq x$.
 2) p. antisimmetrica: $\forall x, y \in S \quad x \leq y \wedge y \leq x \Rightarrow x = y$
 3) p. transitiva: $\forall x, y, z \in S \quad x \leq y \wedge y \leq z \Rightarrow x \leq z$
 es. \mathbb{N} e \leq come minore o uguale
 $\Rightarrow \forall a, b \in \mathbb{N} \quad a \leq b \Leftrightarrow \exists c \in \mathbb{N} \mid b = a + c$
 es. S insieme e $\mathcal{P}(S) = \{X \mid X \subseteq S\}$
 \hookrightarrow insieme potenza, famiglia / insieme delle parti / partizioni.
 \subseteq relazione di inclusione insiemistica $X \subseteq Y$. È relazione d'ordine.
 es. \mathbb{N} è relazione di divisibilità
 $\Rightarrow a \mid b$ (a divide b) $\Leftrightarrow \exists c \in \mathbb{N} \mid b = a \cdot c$, perché:
 • \mid è riflessiva: $a = a \cdot 1 \Rightarrow a \mid a$
 • \mid è antisimmetrica: $a \mid b \wedge b \mid a \Rightarrow a = b$?
 $a \mid b \Leftrightarrow b = ah$ e $b \mid a \Leftrightarrow a = bk \quad k, h \in \mathbb{N}$
 $\Rightarrow k \cdot h \in \mathbb{N} \Rightarrow k \cdot h = 1 \Rightarrow k = 1 \wedge h = 1$
 $\Rightarrow b = bkh \Rightarrow b = bk \Rightarrow b = 1$
 • \mid è transitiva: $a \mid b \wedge b \mid c \Rightarrow a \mid c$?
 $a \mid b \Leftrightarrow b = ah$ e $b \mid c \Leftrightarrow c = bk$
 $\Rightarrow c = ahk \Rightarrow a \mid c$
 sia (S, \leq) con \leq relazione d'ordine parziale su S
 $\Rightarrow S$ è un **INSIEME PARZIALMENTE ORDINATO** oppure
POSET (Partially Ordered SET)
 una relazione d'ordine è **TOTALE** se vale che
 $\forall x, y \in S \quad x \leq y \vee y \leq x$.
 es. (\mathbb{N}, \leq) , \leq è d'ordine totale.
 es. (\mathbb{N}, \mid) , \mid è solo parziale. $3 \nmid 2$
 es. $(\mathcal{P}(\mathbb{N}), \subseteq)$, \subseteq non è totale. $\{2\} \subsetneq \{3\}$

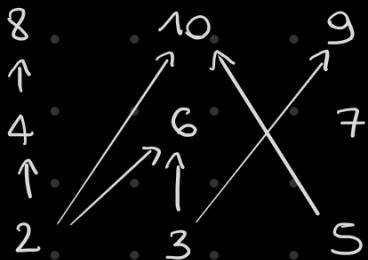
(DAG)

→ RAPPRESENTARE POSET

lo faccio tramite i DIAGRAMMI DI HASSE.

i nodi sono i valori e tra di loro c'è un arco se
c'è una relazione.

$S = \{2, \dots, 10\}$ e l. relazione.



per completare la def di POSET:

$$\begin{array}{|l} \forall x, y \Rightarrow x \leq y, x \neq y \\ \nexists z \in S \mid x \leq z \leq y \end{array}$$

→ PRINCIPIO DI INDUZIONE

sia P_n proprietà com $n \in \mathbb{N}$: se P_0 è vera e se, fissato n , P_n è vera $\Rightarrow P_{n+1}$ è vera.

(base dell'induzione e passo induttivo)

P_n è vera $\forall n \in \mathbb{N}$

es. $\sum_{i=0}^n i = \frac{n(n+1)}{2} \Rightarrow \sum_{i=0}^{n+1} i = \frac{(n+1)(n+2)}{2}$

$$P_0 = \emptyset \quad \checkmark$$

$$\text{dimostro } \frac{n \cdot (n+1)}{2} + (n+1) = \frac{(n+1)(n+2)}{2}$$

$$n^2 + n + 2n + 2 = n^2 + 2n + n + 2 \quad \square$$

→ PRINCIPIO DEL BUON ORDINAMENTO

se $T \subseteq \mathbb{N} \mid T \neq \emptyset \Rightarrow T$ ammette un MINIMO,
ovvero $\exists m \in T \mid \forall t \in T \quad m \leq t$.

DIMOSTRAZIONE: $a, b \in \mathbb{N} \mid b \neq 0, b \leq a$

$$\Rightarrow \exists q, r \in \mathbb{N} \mid a = b \cdot q + r \quad \text{dove } 0 \leq r < b$$

↳ quoziente e resto

• se $b = a \Rightarrow q = 1$ e $r = 0$

• se $b < a \Rightarrow T = \{x \in \mathbb{N} \mid b < x \leq a\} \neq \emptyset$

si applica il buone ordinamento $\Rightarrow T$ ha minimo

$$m = q+1 \text{ con } q \geq 1.$$

$q+1$ minimo di $T \Rightarrow q \notin T \Rightarrow b \cdot q \leq a$

$$b(q+1) > a$$

$$\Rightarrow bq \leq a < b(q+1) \Rightarrow 0 \leq \underbrace{a - bq}_r < b$$

$$\Rightarrow bq + r = a \Rightarrow bq + a - bq = a \quad \square$$

{ sez. 1-2 }
cap. 2

→ PROBLEMI DI ARITMETICA DEGLI INTEGRI

quello $(\mathbb{Z}, +, \cdot)$ commutativo $\Rightarrow xy = yx \quad \forall x, y \in \mathbb{Z}$,
e unitario $\Rightarrow 1 \in \mathbb{Z} \mid 1x = x1 = x \quad \forall x$.

DIVISIBILITÀ IN \mathbb{Z} :

$a, b \in \mathbb{Z} \Rightarrow a | b$ se $\exists c \in \mathbb{Z} \mid b = ac$

la relazione $|$ è d'ordine per \mathbb{N} , ma non per \mathbb{Z}
dato che non è antisimmetrica.

$$\begin{cases} a \cdot (b+c) = ab + ac & \text{p. distributiva sinistra} \\ (b+c) \cdot a = ab + ac & \text{p. distributiva destra} \end{cases}$$

DEF: DOMINIO DI INTEGRITÀ UNITARIO (DIU)

sia $(A, +, \cdot)$ quello $\Rightarrow A$ è DIU se A è quello com-
mutativo unitario | $\nexists x, y \in A \setminus \{0\} \mid xy = 0$, ovvero
non ha divisori dello zero

es. $(\mathbb{Z}, +, \cdot)$ è DIU perché:

$\forall a, b \in \mathbb{Z}$ ho che se $ab = 0 \Rightarrow a = 0 \vee b = 0$.

$\Rightarrow \nexists a, b \in \mathbb{Z} \text{ con } a \neq 0 \wedge b \neq 0 \mid ab = 0$.

DEF: sia $(A, +, \cdot)$ quello commutativo unitario e sia
 $x \in A \mid x \neq 0$

$\Rightarrow x$ è INVERTIBILE in A se $\exists y \in A \mid xy = 1$.

se $A = \mathbb{Z} \Rightarrow$ gli unici elementi invertibili sono
 $x = 1$ o $x = -1$.

DEF: sia $a, b \in \mathbb{Z}$. dato $c \in \mathbb{Z}$, c è DIVISORE COMU-

NE di a, b se $cl_a = cl_b$.

es. $a = 2, b = 4 \Rightarrow c = 2$

DEF: sia A quello DIV e sia $a \in A \setminus \{0\}$ e a non invertibile $\Rightarrow a$ è **IRRIDUCIBILE** se:

$\forall b, c \in A \setminus \{0\} \quad a = bc \Rightarrow b \text{ o } c \text{ invertibile}$.

\hookrightarrow esclusivo

DEF: sia A quello DIV e sia $a \in A \setminus \{0\}$ e a non invertibile $\Rightarrow a$ è **ELEMENTO PRIMO** di A se vale che:
se $a \mid bc$ e $\exists x \in A \setminus \{0\} \quad bc = ax \Rightarrow a \mid b$, ovvero $\exists z \in A \setminus \{0\} \quad b = az$, v $a \mid c$, ovvero $\exists t \in A \setminus \{0\} \quad c = at$.

PROPOSIZIONE: sia A quello DIV. $\forall a \in A$ la primo

$\Rightarrow a$ è irriducibile

DIMOSTRAZIONE:

sia A quello DIV. $\forall a, b, c \in A \setminus \{0\}$, se $ab = ac$
 $\Rightarrow b = c$ (**PROPRIETÀ DI CANCELLAZIONE**)

\hookrightarrow o cancellatività (^{dextra e sinistra})

faccio vedere che vale la proprietà:

$$ab = ac \Rightarrow ab - ac = 0 \Rightarrow a(b - c) = 0$$

A è DIV $\Rightarrow a \neq 0$ oppure $b - c = 0$

$a \neq 0$ per la proprietà $\Rightarrow b - c = 0 \Rightarrow b = c$. \square

$\rightarrow a$ è primo $\Rightarrow a \mid bc \Rightarrow a \mid b$ v $a \mid c$

se $a \mid bc \Rightarrow b$ o c invertibile.

$a \mid bc \Rightarrow bc = a \cdot 1$ con 1 unità di A

$\Rightarrow a \mid bc \Rightarrow a \mid b$ v $a \mid c$

in entrambi i casi procedo ugualmente

$$a \mid b \Rightarrow b = ak$$

$$a \mid bc \Rightarrow a \mid akc \Rightarrow a \cdot 1 = a \cdot kc \Rightarrow 1 = kc = ck$$

$\Rightarrow c$ è invertibile $\Rightarrow a$ è irriducibile. \square

$(\mathbb{Z}, +, \cdot)$ è DIV \Rightarrow vale la proposizione in \mathbb{Z} .

→ MCD

se \mathbb{Z} (quello) e $a, b \in \mathbb{Z} \mid a, b \neq 0$. $d \in \mathbb{Z}$ è MCD se soddisfa:

$$1) d \mid a \wedge d \mid b$$

$$2) d' \in \mathbb{Z} \mid d' \mid a \wedge d' \mid b \Rightarrow d' \mid d$$

$$\text{es. } \text{MCD}(a=2, b=4) = 2$$

$$\text{es. } \text{MCD}(a=2, b=3) = 1$$

$$\text{es. } \text{MCD}(a=6, b=9) = 3$$

$$\text{es. } \text{MCD}(a=4, b=8) = 4$$

→ $\text{MCD}(a, b)$ si scrive anche (a, b)

se $d = (a, b) \Rightarrow$ anche $-d = (a, b)$, ma per convenzione si prende il positivo.

PROPOSIZIONE: $a, b \in \mathbb{Z} \mid a, b \neq 0$. per la **DIVISIONE**

EUCLIDEA (o CON RESTO)

$$\exists! q, r \in \mathbb{Z} \mid a = bq + r \text{ con } 0 \leq r < |b|$$

$$\text{es. } a=15, b=4$$

$$15 = 4 \cdot 3 + 3 \text{ con } q=3, r=3 \text{ e } 0 \leq 3 < 4$$

r è **RESTO** di ab e q è **QUOTIENTE** di ab .

THM: siamo $a, b \in \mathbb{Z} \mid a, b \neq 0 \Rightarrow$

$$1) \exists d \in \mathbb{Z} \mid d = (a, b)$$

$$2) \text{ se } d = (a, b) \Rightarrow \exists \alpha, \beta \in \mathbb{Z} \mid d = \alpha a + \beta b$$

↳ **IDENTITÀ DI BEZOUT** (si dice BEZU)

DIMOSTRAZIONE:

$$\text{sia } S \subseteq \mathbb{Z} \mid S = \{as + bt \mid s, t \in \mathbb{Z}\}$$

$$S \neq \emptyset \text{ perché: } \begin{cases} \text{se } a > 0 \Rightarrow t=0 \wedge s>0 \\ \text{se } a < 0 \Rightarrow t=0 \wedge s<0 \end{cases}$$

per il principio del minimo su S :

$$\exists d \in S \mid d = \min S \Leftrightarrow \forall c \in S \quad d \leq c$$

$$\text{sia } d = \min S \Rightarrow d = as_0 + bt_0 > 0 \text{ con } s_0, t_0 \in \mathbb{Z}$$

$$\textcircled{1}. \quad d' \mid a \wedge d' \mid b \Rightarrow d' \mid d$$

$$\begin{aligned}
 d &= as_0 + bt_0 \Rightarrow d' \mid a \Rightarrow a = d'h \quad \text{com } h \in \mathbb{Z} \\
 &\Rightarrow d' \mid b \Rightarrow b = d'k \quad \text{com } k \in \mathbb{Z} \\
 &\Rightarrow d = d'h s_0 + d'k t_0 \Rightarrow d = d'(h s_0 + k t_0) \\
 &\Rightarrow d' \mid d \\
 &\bullet d \mid a \wedge d \mid b \\
 a &= dq + r \left\{ \begin{array}{l} 0 \leq r < d \wedge a = dq \Rightarrow d \mid a \text{ se } r = 0 \\ \downarrow \quad \quad \quad 0 < r < d \wedge \text{contraddizione se } r > 0 \end{array} \right. \\
 \text{perché } a - dq &= a - q(as_0 - bt_0) = a(1 - q_{s_0}) - qb t_0 \\
 \text{che non è } < d \text{ perché } d \text{ è minimo.} \\
 \text{stesso ragionamento con } b \quad \square
 \end{aligned}$$

② segue dalla ①. \square

ALGORITMO DI DIVISIONE EUCLIDEA per calcolo di (a, b)

si considera $a \geq b > 0$.

- 1) $a = bq_1 + r_1$ com $0 \leq r_1 < b$ $\begin{cases} r_1 = 0 \Rightarrow \text{END} \\ r_1 > 0 \Rightarrow \text{NEXT} \end{cases}$
- 2) $b = r_1 q_2 + r_2$ $0 \leq r_2 < r_1$ "
- 3) $r_1 = r_2 q_3 + r_3$ $0 \leq r_3 < r_2$ "
- ...
- n) $r_{n-2} = r_{n-1} q_n + r_n$
- n+1) $r_{n-1} = r_n q_{n+1} + r_{n+1}$ dove $r_{n+1} = 0$

$$\Rightarrow (a, b) = r_n$$

$$\text{es. } a = 3522, b = 321$$

$$3522 = 321 \cdot 10 + 312$$

$$321 = 312 \cdot 1 + 9$$

$$312 = 9 \cdot 34 + 6$$

$$9 = 6 \cdot 1 + 3$$

$$6 = 3 \cdot 2 + 0 \Rightarrow (3522, 321) = 3$$

per l'identità di Bezout ho: $3 = \alpha 3522 + \beta 321$

$$9 - 6 = 3$$

$$9 - (312 - 9 \cdot 34) = 35 \cdot 9 - 312$$

$$35(321 - 312) - 312 = 35 \cdot 321 - 36 \cdot 312$$

$$35 \cdot 321 - 36 \cdot (3522 - 321 \cdot 10)$$

$$3 = -36 \cdot 3522 + 395 \cdot 321$$

$\hookrightarrow \alpha$

$\hookrightarrow \beta$

DEF: FATTORIZZAZIONE

$n \in \mathbb{N} \mid n > 1$. la fattorizzazione è il prodotto

$n = a_1 a_2 \dots a_n$ com $a_i \in \mathbb{N} \mid n \geq 1$

se gli a_i primi \Rightarrow è una FATTORIZZAZIONE IN PRIMI

TEOREMA FONDAMENTALE DELL'ARITMETICA dei $\mathbb{Z} \in \mathbb{L}$

$\forall p$ non primo $\Rightarrow \exists q, t \in \mathbb{N} \mid p = qt \wedge 1 < q, t < p$

se $n \in \mathbb{N} \mid n > 1 \Rightarrow$ valgono le condizioni:

1) $n = p_1^{h_1} p_2^{h_2} \dots p_s^{h_s}$ fattorizzazione di n dove:
 $s \geq 1, h_i \geq 1$, p_i e p_1, \dots, p_s primi com $p_i^{h_i} = p_1 \dots p_i$
per h_i volte

$$\text{es. } n = 20 = 2^2 \cdot 5 = p_1^{h_1} p_2^{h_2}$$

com $p_1 = 2, h_1 = 2, p_2 = 5, h_2 = 1, s = 2$

2) la fattorizzazione è UNICA

se $n = p_1^{h_1} \dots p_s^{h_s}$ dove p_i primi, $h_i \geq 1$.

e $n = q_1^{m_1} \dots q_t^{m_t}$ dove q_i primi, $m_t \geq 1$.

$\Rightarrow s = t, p_1 = q_1 \dots p_s = q_t, h_1 = m_1 \dots h_s = m_t$

DIMOSTRAZIONE:

① per induzione su $n \in \mathbb{N} \mid n > 1$

:BI: $n = 2$. 2 è primo

$$\Rightarrow 2 = p_1^{h_1} \text{ con } h_1 = 1$$

:PI: $n \in \mathbb{N} \mid n > 2$

$\rightarrow n$ primo: $n = p_1^{h_1}$ com $p_1 = n, h_1 = 1$

$\rightarrow n$ non primo: $\exists a, b \in \mathbb{N} \mid n = ab$ com $1 < a, b < n$

per l'hyp induttiva su $a, b < n \Rightarrow a, b$ hanno fattorizzazione in primi |

$$a = p_1^{h_1} \dots p_s^{h_s} \text{ e } b = q_1^{e_1} \dots q_{s_2}^{e_{s_2}}$$

com p_i e q_i primi

$\Rightarrow n = ab = (p_1^{h_1} \dots p_s^{h_s})(q_1^{e_1} \dots q_t^{e_t}) \Rightarrow$ se i primi e otengo la fattorizzazione. \square

es. $n = 200 \Rightarrow a = 10, b = 20$

$$\Rightarrow n = (2 \cdot 5) \cdot (2^2 \cdot 5) = 2^3 \cdot 5^2$$

② sia $n \in \mathbb{N} | n > 1$. per ① n ha una fattorizzazione in primi $| n = p_1 p_2 \dots p_m$ con $m \geq 1$ e p_i primi
 $m =$ lunghezza della fattorizzazione

es. $20 = 2 \cdot 2 \cdot 5 \Rightarrow m = 3$

per induzione sul più piccolo $m | n = p_1 p_2 \dots p_m$
dove p_i primi

• B1: $m=1 \Rightarrow n = p_1 \Rightarrow$ è unica perché se ne esiste altra per $n \Rightarrow n = q_1^{h_1} \dots q_s^{h_s}$ con $h_i \geq 1$, q_i primi
 $\Rightarrow n = p_1 = q_1 \dots q_s$
ma $q_1 | q_1^{h_1} \dots q_s^{h_s} \Leftrightarrow q_1 | n$, ma $n = p_1 \Rightarrow q_1 | p_1$
 $\Rightarrow p_1 = q_1 \times$ ma p_1 è primo $\Rightarrow p_1 = q_1, x = 1$
 \Rightarrow contraddizione perché $q_1 = \dots = q_s = 1$ e
 $q_i > 1$ perché primi.

com $m=1 \Rightarrow n$ ha una sola fattorizzazione $n = p_1$

• P1: sia $n \in \mathbb{N} | n > 1 \Rightarrow n = p_1^{h_1} \dots p_s^{h_s}$ e $m = \sum_{i=1}^s h_i$
se n anche $n = q_1^{e_1} \dots q_t^{e_t}$
 $\Rightarrow n = p_1^{h_1} \dots p_s^{h_s} = q_1^{e_1} \dots q_t^{e_t}$
dato che $p_1 | n \Rightarrow \exists q_i$ con $i \in \{1, \dots, t\} | p_1 = q_i$
si assume $p_1 = q_1 \Rightarrow n = p_1^{h_1} \dots p_s^{h_s} = p_1^{e_1} \dots p_t^{e_t}$
semplifico p_1 e ho lunghezza $m-1$
 \Rightarrow per l'ip induktiv $s=t, q_i = p_i, h_i = e_i$
 $\forall i \in \{1, \dots, s\}$ \square

COROLARIO: in \mathbb{N} i primi sono in numero infinito

DIMOSTRAZIONE:

si suppone per assurdo che l'insieme P dei primi
in \mathbb{N} sia finito $\Rightarrow \text{Card}(P) = n | P = \{p_1, \dots, p_n\}$

sia $a = 1 + p_1 \dots p_n \in \mathbb{N} \Rightarrow a \notin \mathbb{P}$ perché $a > p_i \forall i \in \{1, \dots, n\}$
 per il THM dell'aritmetica:

$$a = p_{i_1}^{e_1} \cdots p_{i_k}^{e_k} \text{ con } p_{i_1}, \dots, p_{i_k} \in \mathbb{P}$$

$$\Rightarrow p_{i_1} \mid a \Rightarrow p_{i_1} \mid p_1 \cdots p_n = p_1 \cdots p_{i_1} \cdots p_n$$

$$a = p_1 \cdots p_n = 1$$

$$\Rightarrow p_{i_1} \mid 1 \Rightarrow p_{i_1} = 1 \Rightarrow \text{assurdo perché } p_{i_1} > 1 \quad \square$$

DIVISIONE EUCLIDEA DI POLINOMI (o DIVISIONE CON RESTO):

quello dei polinomi in una indeterminata x coefficienti reali in \mathbb{R} : $\mathbb{R}[x] = \{ p(x) = \sum_{i=0}^n a_i x^i \text{ con } a_i \in \mathbb{R} \}$

si dice **GRADO** di $p(x)$ l' n | $a_n \neq 0$

$$\text{es. } p(x) = 3x^4 + 2x^3 + x^2 + x \Rightarrow \text{grado} = 4$$

si indica con $\delta p(x)$.

PROPOSIZIONE:

seguo $a(x), b(x) \in \mathbb{R}[x]$ con $b(x) \neq 0$

supponiamo $\delta a(x) > \delta b(x)$.

$\Rightarrow \exists! q(x), r(x) \in \mathbb{R}[x] \mid a(x) = b(x)q(x) + r(x)$ dove

$r(x) = 0$ oppure $0 \leq \delta r(x) < \delta b(x)$

$q(x)$ è quoziente e $r(x)$ è resto.

$$\text{es. } a(x) = 3x^4 - 2x^3 + x^2 + 4x - 3$$

$$b(x) = x^2 + 5x - 2$$

$$\delta a(x) = 4 \text{ e } \delta b(x) = 2 \Rightarrow \delta q(x) = 2 \text{ e } \delta r(x) \leq 1$$

$$q(x) = ax^2 + bx + c \text{ e } r(x) = dx + h \text{ con } a, b, c, d, h \in \mathbb{R}$$

$$\Rightarrow 3x^4 - 2x^3 + x^2 + 4x - 3 = (ax^2 + bx + c)(x^2 + 5x - 2) + dx + h$$

$$\Rightarrow 3x^4 + x^3(b+5a) + x^2(c+5b-2a) + x(5c-2b) - 2c + h$$

lo confronto con $a(x)$ per cui ho:

$$\begin{cases} a = 3 \\ b + 5a = -2 \\ c + 5b - 2a = 1 \\ 5c - 2b + d = 4 \\ -2c + h = -3 \end{cases} \quad \begin{cases} a = 3 \\ b = -17 \\ c = 92 \\ d = -490 \\ h = 181 \end{cases}$$

$$\Rightarrow q(x) = 3x^2 - 17x + 92 \quad e \quad r(x) = -490x + 181$$

→ CONGRUENZA MODULARE

$m \in \mathbb{Z} \mid m \geq 1$ gli si associa una relazione d'equivalenza
 ≡ : CONGRUENZA MODULO m in \mathbb{Z} definita come:
 $a, b \in \mathbb{Z} \quad a \equiv b \pmod{m} \text{ se } \exists k \in \mathbb{Z} \mid a - b = mk$
 (anche come $a \equiv b \pmod{m}$ o $a \equiv b$)

$$\text{es. } m = 3 \Rightarrow 6 \equiv 9 \pmod{3} \Leftrightarrow 6 - 9 = -3 = 3 \cdot (-1)$$

PROPOSIZIONE: \equiv_m è un'equivalenza in \mathbb{Z}

DIMOSTRAZIONE:

- riflessività: $\forall a \in \mathbb{Z} \quad a \equiv a \pmod{m}$

perché $a - a = 0 = 0 \cdot m$

- simmetria: $a \equiv b \pmod{m} \Rightarrow b \equiv a \pmod{m}$

perché $a \equiv b \Rightarrow a - b = m \cdot k$

$$\Rightarrow b - a = m \cdot -k \Rightarrow b \equiv a$$

- trasitività: $a \equiv b \wedge b \equiv c \Rightarrow a \equiv c$

perché $a - b = m \cdot k$ e $b - c = m \cdot h$

$$\Rightarrow (a - b) + (b - c) = a - c = m \cdot k + m \cdot h \Rightarrow m(k+h), \square$$

PROPOSIZIONE: \equiv_m soddisfa le proprietà:

sia $a \equiv b \pmod{m} \wedge c \equiv d \pmod{m} \Rightarrow$ vale che:

$$1) a + c \equiv b + d \pmod{m}$$

$$2) ac \equiv bd \pmod{m}$$

DIMOSTRAZIONE:

$$\textcircled{1} \quad a \equiv b \Rightarrow a - b = m \cdot h$$

$$c \equiv d \Rightarrow c - d = m \cdot k$$

$$\Rightarrow a - b + c - d = m \cdot h + m \cdot k = m(h+k)$$

$$\Rightarrow a + c \equiv b + d \Leftrightarrow a + c - (b + d) = mq$$

pseudo $q = h+k \quad \square$

$$\textcircled{2} \quad a \equiv b \Rightarrow a - b = m \cdot h$$

$$c \equiv d \Rightarrow c - d = m \cdot k$$

$$\Rightarrow ac - bd = ac - ad + ad - bd = \\ a(c-d) + d(a-b) = amk + dmh = m(ak + dh) \quad \square$$

PROPOSIZIONE: sia $a \in \mathbb{Z} \Rightarrow \exists! r \in \mathbb{Z} \mid a \equiv r \pmod{m}$ com
 $0 \leq r < m$

DIMOSTRAZIONE:

divisione euclidea di a per $m \Rightarrow \exists! q, r \in \mathbb{Z} \mid$

$$a = mq + r \quad \text{com } 0 \leq r \leq m-1$$

$$\Rightarrow \text{si ha } a - r = mq \Rightarrow a = r \pmod{m}. \quad \square$$

(m è fissato, altri metti sarebbe $\equiv q$).

PROPOSIZIONE: sia $m \in \mathbb{Z} \mid m \geq 1$ fissato e sia $a \in \mathbb{Z}$

$\Rightarrow [a] = [r]$ com r resto della divisione di a per m

$$\Rightarrow a = mq + r$$

DIMOSTRAZIONE:

$$a, b \in \mathbb{Z} \quad [a] = [b] \Leftrightarrow a \equiv b \pmod{m}$$

dato che $a \equiv r \pmod{m} \Rightarrow [a] = [r]. \quad \square$

insieme Quoziente di $\mathbb{Z}/\equiv = \{[a] : a \in \mathbb{Z}\}$

si definiscono operazioni su \mathbb{Z}/\equiv come:

$$\cdot [a] + [b] = [a+b]$$

$$\cdot [a] \cdot [b] = [ab]$$

THM: \mathbb{Z}/\equiv è un quello commutativo unitario, chiamato quello delle **CLASSI RESTO MODULO m** .

$$\text{es. } m=3 \Rightarrow \mathbb{Z}/\equiv = \{[r] \mid 0 \leq r \leq 2\} = \{[0], [1], [2]\}$$

si scrivono le tali elle moltiplicazione di + e :

+	[0]	[1]	[2]
[0]	[0]	[1]	[2]
[1]	[1]	[2]	[0]
[2]	[2]	[0]	[1]

·	[0]	[1]	[2]
[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]
[2]	[0]	[2]	[1]

PROPOSIZIONE: sia $m \geq 1$ e $a, b, c \in \mathbb{Z} \mid ac \equiv bc \pmod{m}$ e

$(c, m) = 1$ (coprimo) $\Rightarrow a \equiv b \pmod{m}$

(LEGGE DI CANCELLAZIONE)

DIMOSTRAZIONE:

$$ac - bc = (a - b) \cdot c \Rightarrow km \quad \text{con } k \in \mathbb{Z}$$

per hp $(c, m) = 1 \Leftrightarrow \exists s, t \in \mathbb{Z} \mid cs + mt = 1$ (bezout)

$$a - b = (a - b) \cdot 1 \Rightarrow (a - b)(cs + mt)$$

$$\Rightarrow (a - b) \cdot cs + (a - b) \cdot mt$$