

→ GRUPPO

un **GRUPPO** $(G, *)$ è un insieme dotato di un'operazione binaria che verifica le proprietà:

1) associativa, $(a * b) * c = a * (b * c) \quad \forall a, b, c \in G$

2) \exists elt. neutro | $e * a = a * e = a \quad \forall a \in G$

3) $\forall a \in G \exists a' \in G$ inverso ad a | $a * a' = a' * a = e$

se $*$ è commutativa $\Rightarrow G$ è **ABEUANO** (o commutativo).

PROPOSIZIONE: l'elt. neutro è unico.

l'elt. inverso è unico.

un sottogruppo S di G non vuoto è un gruppo verso la medesima operazione di G : e è l'inverso $\in S$.

→ PERMUTAZIONI

un **GRUPPO SIMMETRICO** è un insieme di permutazioni. $|S_n| = n!$ si indica con σ la permutazione

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix} = (123)(45) \rightsquigarrow \text{prodotto di cicli}$$

S_n è associativo e ha elt neutro e inverso: se ha più di 3 elt \Rightarrow non è chiuso.

$A_n \subseteq S_n$ contiene le permutazioni pari (con segno +1) e $|A_n| = n!/2$.

il n° di trasposizioni, che formano un ciclo, dà la parità:

es. $\sigma = (123)(45)$ ↗ ordine 3 ↘ ordine 2

$$\text{Ordine } (\sigma) = \text{mcm}(3, 2) = 6$$

es. $\sigma = (143) = (13)(14)$ è pari (2 trasposizioni)

es. $\sigma = (142)(35)$

$$\sigma^{-1} = (241)(53)$$

es. generale

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 6 & 5 & 2 & 3 & 1 \end{pmatrix} = (1\ 4\ 2\ 6)(3\ 5)$$

$$\text{Ordine } (\sigma) = \text{mcm}(4, 2) = 4$$

$$\sigma = (14)(12)(16)(35) \Rightarrow \text{pari}$$

$$\sigma^{-1} = (6\ 2\ 4\ 1)(5\ 3)$$

$$\Rightarrow (a_1\ a_2\ \dots\ a_k) = (a_1\ a_2)(a_1\ \dots)\ \dots\ (a_1\ a_k)$$

per scomporre i cicli in trasposizioni

VISTI
DA
SOLA

APPUNTI LEZIONI

→ ANELLO

a) se $A = \{ \} \mid A \neq \emptyset$ è insieme di 2 o più elementi finiti
+ e: \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 $m, n \in \mathbb{N} \mid m, n \geq 1$

$\Rightarrow (M_{m,n}(\mathbb{R}), +)$ 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 anello unitario e non commutativo

dimo: unitario perché $I_n = I = (m_{i,j})$ matrice di identità è l'el. neutro

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

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

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

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

es. anello dei polinomi a coefficienti reali in una indeterminata 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 anello unitario e abeliano.

el. neutro è $1 = 1 \cdot x^0$

→ CAMPO

anche detto corpo commutativo.

sia $(A, +, \cdot)$ anello $\Rightarrow A$ 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: $\forall a \in X \quad a Ra \Leftrightarrow (a, a) \in R$

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

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

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

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

$\Rightarrow R$ d'equivalenza

es. $X = \{zette del piano euclideo\}$

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

sia R d'equivalenza su X , $a \in X$ è **CLASSE D'EQUIVALENZA** di X | $[a] = \{b \in X \mid aRb\}$. a è **RAPPRESENTANTE** di $[a]$.

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

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

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'insieme è disgiunto

\hookrightarrow **PARTIZIONE**

→ RELAZIONE D'ORDINE

Si dice \leq relazione binaria su S .

quindi $\leq \in S \times S$. \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. transitività: $\forall x, y, z \in S \quad x \leq y \wedge y \leq z \Rightarrow x \leq z$

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, famiglie / insieme delle parti / partizioni.

È relazione di inclusione inclusistica $X \subseteq Y$ è relazione d'ordine.

es. \mathbb{N} è relazione di divisibilità

$\Rightarrow a|b$ (a divide b) $\Leftrightarrow \exists c \in \mathbb{N} \mid b = a \cdot c$, perché

• | è riflessiva: $a = a \cdot 1 \Rightarrow a|a$

• | è antisimmetrica: $a|b \wedge b|a \Rightarrow a=b?$

$a|b \Leftrightarrow b = ah$ e $b|a \Leftrightarrow a = bk$ $k, h \in \mathbb{N}$

$\Rightarrow k \cdot h \in \mathbb{N} \Rightarrow k \cdot h = 1 \Rightarrow k=1 \wedge h=1$

$\Rightarrow b = bkh \Rightarrow b = bk \Rightarrow b = 1$

• | è transitiva: $a|b \wedge b|c \Rightarrow a|c?$

$a|b \Leftrightarrow b = ah$ e $b|c \Leftrightarrow c = bk$

$\Rightarrow c = ahk \Rightarrow a|c$

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. $(\mathbb{N}, |)$, | è solo parziale. $3 \nmid 2$

es. $(P(\mathbb{N}), \subseteq)$, \subseteq non è totale. $\{2\} \subsetneq \{3\}$

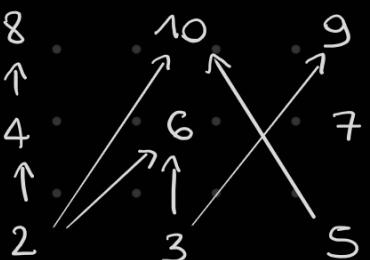
→ RAPPRESENTARE POSET

(DAG)

lo faccio tramite i DIAGRAMMI DI HASSE.

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

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



per completare le def di POSET:

$\forall x, y \Rightarrow x \leq y, x \neq y$
 $\nexists z \in S \mid x \leq z \leq y$

→ 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 $\forall n \in \mathbb{N}$

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

$$P_0 = 0 \quad \checkmark$$

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

$$n^2 + n + 2n + 2 = n^2 + 2n + n + 2$$

□

→ PRINCIPIO DEL BUON ORDINAMENTO

sia $T \subseteq \mathbb{N} \mid T \neq \emptyset \Rightarrow T$ 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

$$\text{se } b = a \Rightarrow q = 1 \text{ e } r = 0$$

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

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

$$m = q+1 \quad \text{com } q \geq 1$$

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

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

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

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

→ PROBLEMI DI ARITMETICA DEGLI INTEGRI

quello $(\mathbb{Z}, +, \cdot)$ commutativo $\Rightarrow xy = yx \quad \forall x, y \in \mathbb{Z}$,

{ sez. 1-2 }
{ cap. 2 }

e unitario $\Rightarrow \exists 1 \in \mathbb{Z} \mid 1x = x = x \forall x$.

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 commutativo unitario $| \nexists x, y \in A \setminus \{0\} | xy = 0$, ovvero
non ha divisori dello zero.

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

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

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

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

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

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 COMUNE** di a, b se $c | a$ e $c | b$.

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

DEF: sia A quello DIU e sia $a \in A | a \neq 0$ e a non invertibile $\Rightarrow a$ è **IRRIDUCIBILE** se:

$\forall b, c \in A | a = bc \Rightarrow b$ o c invertibili.

↳ esclusivo

DEF: sia A quello DIU e sia $a \in A | a \neq 0$ e a non invertibile $\Rightarrow a$ è **ELEMENTO PRIMO** di A se vale che:

se $a | bc$ e $\exists x \in A | bc = ax \Rightarrow a | b$, ovvero $\exists z \in A | b = az$, v $a | c$, ovvero $\exists t \in A | c = at$.

PROPOSIZIONE: sia A quello DIU. $\forall a \in A$ | a primo

$\Rightarrow a$ è irriducibile

DIMOSTRAZIONE:

sia A quello DIU. $\forall a, b, c \in A$ | $a \neq 0$, se $ab = ac$
 $\Rightarrow b = c$ (**PROPRIETÀ DI CANCELLAZIONE**)

\hookrightarrow o cancellatività (^{d' sinistra e'})

farò vedere che vale la proprietà:

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

$$A \text{ è DIU} \Rightarrow a = 0 \text{ oppure } b - c = 0$$

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

$$\rightarrow a \text{ è primo} \Rightarrow a \mid bc \Rightarrow a \mid b \vee a \mid c$$

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

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

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

in entrambi i casi procedo ugualmente

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

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

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

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

\rightarrow MCD

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

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

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

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

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

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

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

$\rightarrow \text{MCD}(a, b)$ 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)

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

es, $a = 15, b = 4$

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

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:

sia $S \subseteq \mathbb{Z} \mid S = \{as + bt > 0 \mid s, t \in \mathbb{Z}\}$

$S \neq \emptyset$ 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 :

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

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

$$①. d' \mid a \wedge d' \mid b \Rightarrow d' \mid d$$

$$d = as_0 + bt_0 \Rightarrow d' \mid a \Rightarrow a = d'h \text{ con } h \in \mathbb{Z}$$

$$\Rightarrow d' \mid b \Rightarrow b = d'k \text{ con } k \in \mathbb{Z}$$

$$\Rightarrow d = d'h s_0 + d'k t_0 \Rightarrow d = d'(hs_0 + kt_0)$$

$$\Rightarrow d' \mid d$$

$$\bullet d \mid a \wedge d \mid b$$

$$a = dq + r \quad \left\{ \begin{array}{l} 0 \leq r < d \wedge a = dq \Rightarrow d \mid a \text{ se } r = 0 \\ 0 < r < d \wedge \text{contraddizione se } r > 0 \end{array} \right.$$

$$\text{perché } a - dq = a - q(as_0 - bt_0) = a(1 - qs_0) - qb t_0$$

che non è $< d$ poiché d è minimo.

stesso ragionamento con b □

② segue dalla ① . □

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

si considera $a \geq b > 0$.

$$1) a = b q_1 + r_1 \quad \text{com } 0 \leq r_1 < b \quad \begin{cases} r_1 = 0 \Rightarrow \text{END} \\ r_1 > 0 \Rightarrow \text{NEXT} \end{cases}$$

$$2) b = r_1 q_2 + r_2 \quad \begin{cases} 0 \leq r_2 < r_1 \end{cases} \quad \backslash$$

$$3) r_1 = r_2 q_3 + r_3 \quad \begin{cases} 0 \leq r_3 < r_2 \end{cases} \quad \backslash$$

...

$$n) r_{n-2} = r_{n-1} q_n + r_n$$

$$n+1) r_{n-1} = r_n q_{n+1} + r_{n+1} \quad \text{dove } r_{n+1} = 0$$

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

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

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

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

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

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

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

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

$$9 - 6 = 3$$

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

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

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

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

$\hookrightarrow \alpha$

$\hookrightarrow \beta$

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} :

(^{Prop}₅₂)

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

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 con $p_i^{h_i} = p_1 \dots p_i$
per h_i volte

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

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

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: $n = p_1^{h_1}$ con $p_1 = n$, $h_1 = 1$

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

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

$$a = p_1^{h_1} \dots p_{s_1}^{h_{s_1}} \text{ e } b = q_1^{e_1} \dots q_{s_2}^{e_{s_2}}$$

con p_i e q_i primi

$$\Rightarrow n = ab = (p_1^{h_1} \dots p_{s_1}^{h_{s_1}})(q_1^{e_1} \dots q_{s_2}^{e_{s_2}}) \Rightarrow$$

no i primi e ottengo 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 $n \in \mathbb{N} \mid n > 1$. 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 $m \mid n = p_1 p_2 \dots p_m$
dove p_i primi

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

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

P1: sia $n \in \mathbb{N} \setminus \{1\} \Rightarrow n = p_1^{h_1} \cdots p_s^{h_s}$ e $m = \sum_{i=1}^s h_i$
se n anche $n = q_1^{e_1} \cdots q_t^{e_t}$
 $\Rightarrow n = p_1^{h_1} \cdots p_s^{h_s} = q_1^{e_1} \cdots q_t^{e_t}$
dato che $p_1 | n \Rightarrow \exists q_i$ con $i \in \{1, \dots, t\}$ | $p_1 = q_i$
si assume $p_1 = q_1 \Rightarrow n = p_1^{h_1} \cdots p_s^{h_s} = p_1^{e_1} \cdots p_t^{e_t}$
semplifico p_1 e ho lunghezza $m-1$
 \Rightarrow per hyp multivq $s=t$, $q_i = p_i$, $h_i = e_i$
 $\forall i \in \{1, \dots, s\}$ \square

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

DIMOSTRAZIONE:

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

sia $a = 1 + p_1 \cdots p_n \in \mathbb{N} \Rightarrow a \notin \mathbb{P}$ perché $a > p_i \forall i \in \{1, \dots, n\}$

per il TM dell'aritmetica:

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

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

$a - p_1 \cdots p_n = 1$

$\Rightarrow p_{i_1} | 1 \Rightarrow p_{i_1} = 1 \Rightarrow$ assurdo perché $p_{i_1} > 1$ \square

DIVISIONE EUCLIDEA DI POLINOMI (o DIVISIONE CON RESTO):

quello dei polinomi in una indeterminata x coefficienti 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 | $a_n \neq 0$

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.

es. $a(x) = 3x^4 - 2x^3 + x^2 + 4x - 3$

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

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

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

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

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

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

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

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

