

ALGEBRA

3) FATTORIZZAZIONE IN \mathbb{Z} E CONSEGUENZE

THM: FONDAMENTALE DEL' ARITMETICA

$n \in \mathbb{Z} \mid n > 1 \Rightarrow n$ è fattorizzabile in un prodotto di numeri irriducibili $p_j > 1$.
ogni $z \in \mathbb{Z}$ ha una unica forma di scrittura in fattorizzazione.

$$a, b \in \mathbb{Z} \Rightarrow \text{mcm}(a, b) = m \mid$$

• m multiplo di a e di b .

• se m' multiplo di a e di $b \Rightarrow m'$ multiplo di m .

$$\mid a \cdot b \mid$$

$$\Rightarrow \text{mcm}(a, b) = \frac{\mid a \cdot b \mid}{\text{mcd}(a, b)}$$

$\exists \infty$ numeri primi

4) I NUMERI RAZIONALI

uso \mathbb{Q} per risolvere $ax = b$ con $a, b \in \mathbb{Z}$ e $a \neq 0$.

$\mathbb{Q} = (\mathbb{Z} \times \mathbb{Z} \setminus \{0\}) / \sim$ e si ha:

$(a, b) \sim (c, d) \Leftrightarrow ad = bc$

i suoi elt. sono $\overline{(a, b)}$

abbiamo le operazioni:

$$\cdot \overline{(a, b)} + \overline{(c, d)} = \overline{(ad + bc, bd)}$$

$$\cdot \overline{(a, b)} \cdot \overline{(c, d)} = \overline{(ac, bd)}$$

i risultati sono in $\mathbb{Z} \times \mathbb{Z} \setminus \{0\}$

le classi $0 = \overline{(0, 1)} = \overline{(0, b)}$ e $1 = \overline{(1, 1)} = \overline{(a, a)}$ sono elt. neutri $\Rightarrow \mathbb{Q}$ è un anello.

Inoltre $\overline{(a, b)} \cdot \overline{(b, a)} = \overline{(ab, ba)} = \overline{(1, 1)}$ $\forall a, b | a \neq 0, b \neq 0$

L'insieme \mathbb{Q} è un campo e estende \mathbb{Z} .

Si scrivono gli elt in \mathbb{Q} come uv^{-1} con $u, v \in \mathbb{Z}$ e $v \neq 0$:

$\Rightarrow \overline{(a, b)} = \overline{(a, 1)} \overline{(1, b)} = a/b$

6) CONGRUENZE: PRIME PROPRIETÀ E APPLICAZIONI

Una relazione di congruenza modulo un intero positivo n

identifica $a, b \in \mathbb{Z} | a - b = d$ e d multiplo di n , quindi:

$a \equiv b \text{ siano } a \equiv b \pmod{n} \Leftrightarrow a - b = nh$ per $h \in \mathbb{Z}$.

Ogni intero $a \equiv r \pmod{n} | 0 \leq r < n$.

Sia $n \in \mathbb{Z} | n > 0 \Rightarrow \equiv_n$ è relazione d'equivalenza.

Presi $a, b, c, d \in \mathbb{Z} \Rightarrow$ valgono le proprietà:

$$a \equiv b \pmod{n}, c \equiv d \pmod{n} \Rightarrow \begin{cases} a + c \equiv b + d \pmod{n} \\ ac \equiv bd \pmod{n} \end{cases}$$

Le classi d'equivalenza sono:

$$\overline{0} = \{kn | k \in \mathbb{Z}\} \text{ e } \overline{1} = \{kn + 1 | k \in \mathbb{Z}\}$$

$$\text{fino } \overline{n-1} = \{kn + n - 1 | k \in \mathbb{Z}\}$$

$$\mathbb{Z}_n = \mathbb{Z}/\equiv_n = \{\bar{0}, \bar{1}, \dots, \bar{n-1}\}$$

$n \in \mathbb{Z} \mid n > 0 \Rightarrow \forall a, b, c, d \in \mathbb{Z} \text{ se } a \equiv b \pmod{n}$

$$\Rightarrow \begin{aligned} &\bullet a+c \equiv b+c \pmod{n} \\ &\bullet ac \equiv bc \pmod{n} \end{aligned}$$

$$\bullet a^i \equiv b^i \pmod{n} \quad \forall i \in \mathbb{N}$$

$$\bullet ac \equiv bc \pmod{n} \Rightarrow a \equiv b \pmod{\frac{n}{d}} \text{ con } d = (c, n)$$

$$\forall p \text{ primo e } x, y \in \mathbb{Z} \Rightarrow (x+y)^p \equiv x^p + y^p \pmod{p}$$

THM: PICCOLO TEOREMA DI FERMAT

$$a \in \mathbb{Z} \text{ e } p \text{ primo } \Rightarrow a^p \equiv a \pmod{p}$$

$$\text{se } (a, p) = 1 \Rightarrow a^{p-1} \equiv 1 \pmod{p}$$

CRITERIO DI DIVISIBILITÀ:

per 3/9: sommo cifre e vedo se è multiplo di 3/9

per 2/5: se la cifra 2 destra è divisibile per 2/5

per 4: se le due cifre 2 destra sono divisibili per 4/25

per 2^k : se le ultime k cifre sono divisibili per k

per 11: se $\sum_{i=0}^n (-1)^i a_i$ è divisibile per 11

7) RISOLUZIONE DI CONGRUENZE E THM CINESE DEL RESTO

una CONGRUENZA LINEARE in x è un'equazione tipo

$ax \equiv b \pmod{n}$ con $a, b \in \mathbb{Z}$ e $n \in \mathbb{N}$: ammette soluzioni solo se $(a, n) \mid b$. Le soluzioni ottenibili sono nella forma:

$$x_0 + h \cdot \frac{n}{(a, n)} \quad \text{con } h \in \mathbb{Z} \text{ e } x_0 \text{ soluzione}$$

Sono tutte congruenti tra loro e sono (a, n) .

Se $(a, n) = 1 \Rightarrow ax \equiv b \pmod{n}$ ha solo 1 soluzione

$$\left\{ \begin{array}{l} a_1 x \equiv b_1 \pmod{n_1} \\ a_2 x \equiv b_2 \pmod{n_2} \end{array} \right.$$

$$\left\{ \begin{array}{l} a_1 x \equiv b_1 \pmod{n_1} \\ a_2 x \equiv b_2 \pmod{n_2} \end{array} \right. \quad \text{con } (n_1, n_2) = 1$$

per $i \neq j$

$$\Rightarrow \text{si risolve} \begin{cases} x \equiv c_1 \pmod{n'_1} \\ x \equiv c_2 \pmod{n'_2} \\ \vdots \\ x \equiv c_s \pmod{n'_s} \end{cases}$$

e' necessario che $\text{MCD}(a_k, n_k) \mid b_k \quad \forall k \in \mathbb{N}$

THM: TEOREMA CHINSE DEL RESTO

$$r_1, \dots, r_s \in \mathbb{Z} \mid r_1, \dots, r_s > 0 \mid (r_i, r_j) = 1 \text{ con } i \neq j \Rightarrow \begin{cases} x \equiv c_1 \pmod{r_1} \\ x \equiv c_2 \pmod{r_2} \\ \vdots \\ x \equiv c_s \pmod{r_s} \end{cases}$$

ammette soluzione unica modulo r_1, \dots, r_s

FINE ↑ APPUNTI LIBRO

→ 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

S insieme | $S \neq \emptyset$, si è \leq una 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 $b|a \Leftrightarrow a = bk \quad k, h \in \mathbb{N}$

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

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

• | 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. $\{2\} \subsetneq \{3\}$

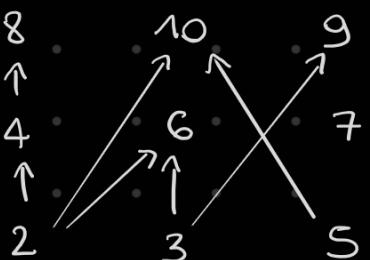
→ RAPPRESENTARE POSET

(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 è DIU $\Rightarrow a = 0$ 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 $a = bc \Rightarrow b$ e c invertibili.

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

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

in entrambi i casi procedo ugualmente

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

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

$\Rightarrow c$ 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: siano $a, b \in \mathbb{Z} \mid a, b \neq 0 \Rightarrow$

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

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

↳ **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 $s_0, t_0 \in \mathbb{Z}$

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

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

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

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

$$\Rightarrow d' \mid d$$

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

$$a = dq + r \quad \begin{cases} 0 \leq r < d \wedge a = dq \Rightarrow d \mid a \text{ se } r = 0 \\ 0 < r < d \wedge \text{contraddizione se } r > 0 \end{cases}$$

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

che non è $< d$ poiché d è minimo.

stesso ragionamento con b □

② segue dalla ① . \square

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

si considera $a \geq b > 0$.

$$1) a = bq_1 + r_1 \quad \text{con } 0 \leq r_1 < b \quad \begin{cases} r_1 = 0 \Rightarrow \text{END} \\ r_1 > 0 \Rightarrow \text{NEXT} \end{cases}$$

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

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

...

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

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

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

es. $a = 3522$, $b = 321$

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

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

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

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

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

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

$$9 - 6 = 3$$

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

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

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

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

$$\hookrightarrow \alpha$$

$$\hookrightarrow \beta$$

