

Matematica Discreta

Indice

1. **Insiemi:** insiemi notevoli e proprietà, divisibilità, principio di induzione, insiemi
2. **Relazioni:** relazioni, applicazioni, relazioni d'equivalenza, relazioni d'ordine
3. **Calcolo combinatorio:** principi, permutazioni, disposizioni, combinazioni
4. **Aritmetica:** numeri naturali e seconda forma del principio di induzione, divisibilità tra interi, congruenze, funzione di Eulero, sistemi di equazioni congruentiali
5. **Strutture algebriche:** strutture algebriche, strutture notevoli, sottostrutture, strutture quoziente, omomorfismo, divisori dello zero

1. Insiemi

Insiemi notevoli e proprietà

Insiemi notevoli:

- naturali $\mathbb{N} = \{1, 2, 3, 4, \dots\}$
- interi $\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$
- razionali $\mathbb{Q} = \{\text{frazioni}\}$
- reali \mathbb{R}

Proprietà di somma e prodotto in \mathbb{R} :

- commutatività: $a + b = b + a, ab = ba$
- associatività: $(a + b) + c = a + (b + c), (ab)c = a(bc)$
- distributività: $a(b + c) = ab + ac$
- zero è elemento neutro per la somma: $a + 0 = 0 + a = a$
- 1 è elemento neutro per la moltiplicazione: $a1 = 1a = a$

- legge di annullamento del prodotto: se $ab = 0$ allora $a = 0$ oppure $b = 0$
- per $a, b \in \mathbb{N}$, se $ab = 1$ allora $a = b = 1$

Divisibilità

Relazione di divisibilità in \mathbb{N}_0, \mathbb{Z} :

$a|b$ "a divide b" se esiste $c \in \mathbb{Z}$ tale che $b = ac$, cioè b è multiplo di a

Proprietà:

- $1|a \quad \forall a \in \mathbb{Z}$
- $a|a \quad \forall a \in \mathbb{Z}$
- transitività: $a|b$ e $b|c \Rightarrow a|c$
- per $a, b \in \mathbb{N}_0$, $a|b$ e $b|a \Rightarrow a = b$
- $a|b$ e $a|c \Rightarrow a|b+c$

Principio di induzione

Principio di induzione:

Sia $P(n)$ una proprietà su n.

Per $n_0 \in \mathbb{N}_0$, se:

- $P(n_0)$ è vera
- $P(n_0)$ è vera $\Rightarrow P(n+1)$ è vera per $n \geq n_0$

Allora $P(n)$ è vera $\forall n \geq n_0$

Insiemi

Definizioni:

Un insieme è una collezione di oggetti, detti elementi

Un sottoinsieme S di X è un insieme costituito da parte degli elementi di X: $S \subseteq X$ se $\forall x : x \in S \Rightarrow x \in X$

Un insieme è finito se ha un numero finito di elementi, il numero di elementi è indicato con $|X|$ ed è detto cardinalità

L'insieme delle parti $P(X)$ è l'insieme di tutti i sottoinsiemi di X , ha cardinalità 2^X

Operazioni tra insiemi:

- unione: $S \cup T = \{x | x \in S \vee x \in T\}$
- intersezione: $S \cap T = \{x | x \in S \wedge x \in T\}$
- differenza: $S \setminus T = \{x | x \in S \wedge x \notin T\}$

2. Relazioni

Relazioni

Prodotto cartesiano, relazione:

Dati $S, T \subseteq X$ il prodotto cartesiano $S \times T = \{(x, y) | x \in S \wedge y \in T\}$ è l'insieme delle coppie ordinate

Per insiemi finiti con $|A| = n$ e $|B| = m$ si ha $|A \times B| = |A| \cdot |B|$

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

Tipi di relazione:

- relazione riflessiva: xRx
- relazione simmetrica: $xRy \Rightarrow yRx$
- relazione antisimmetrica: $xRy, yRx \Rightarrow x = y$
- relazione transitiva: $xRy, yRz \Rightarrow xRz$
- relazione d'ordine: RAT
- relazione d'equivalenza: RST
- applicazione: $\forall x \in S, \exists!y \in T : xRy$
- successione: $\forall x \in \mathbb{N}, \exists!y \in T : xRy$

- relazione totale: $\forall(x, y) \in S \times T \ xRy$
- relazione vuota: $R = \emptyset$
- relazione opposta: $(x, y) \in R^{op} \Leftrightarrow (y, x) \in R$
- relazione n-aria: $R \subseteq S \times S \times \dots \times S$

Applicazioni

Definizioni:

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

S è detto Dominio di f , T è detto Codominio di f

Immagine: $Im(f) = \{y \in T | (x, y) \in f\} = \{f(x) | x \in S\}$

Iniettiva, suriettiva, biettiva:

- $f \subseteq S \times T$ è iniettiva se $\forall x_1, x_2 \in S$ con $x_1 \neq x_2 \Rightarrow f(x_1) \neq f(x_2)$
- $f \subseteq S \times T$ è suriettiva se $Im(f) = T$ cioè se $\forall y \in T, \exists x \in S : f(x) = y$
- è biettiva se è sia iniettiva che suriettiva

Proposizione:

Dati S, T finiti e non vuoti

- $\exists f : S \rightarrow T$ iniettiva $\Leftrightarrow |S| \leq |T|$
- $\exists f : S \rightarrow T$ suriettiva $\Leftrightarrow |S| \geq |T|$
- $\exists f : S \rightarrow T$ biettiva $|S| = |T|$

Controimmagine, composizione, inversa:

Controimmagine: $f^{-1}(Y) = \{x \in S | f(x) \in Y\} = \{x \in S | (x, y) \in f \text{ per qualche } y \in Y\} \quad (Y \subseteq T)$

Composizione: $f \subseteq S \times T, g \subseteq T \times W \quad (g \circ f)(x) = g(f(x))$, con $g \circ f \subseteq S \times W$

La composizione non è commutativa, ma è associativa

Inversa: se f è biettiva, f^{-1} è la sua inversa ed è tale che

- $(f \circ f^{-1})(t) = t \quad \forall t \in T$
- $(f^{-1} \circ f)(s) = s \quad \forall s \in S$

Relazioni d'equivalenza

Definizione:

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

- Riflessiva: $\forall x \in S, xRx$
- Simmetrica: $\forall x, y \in S, xRy \Rightarrow yRx$
- Transitiva: $\forall x, y, z \in S, xRy, yRz \Rightarrow xRz$

Partizione:

Una partizione di un insieme S è un insieme $A \subseteq P(S)$ tale che:

- gli insiemi sono non vuoti: $\forall X \in A, X \neq \emptyset$
- a due a due disgiunti: $\forall X, Y \in A, X \cap Y = \emptyset$
- la loro unione è tutto S : $\bigcup_{X \in A} X = S$

Classe di equivalenza, insieme quoziante:

Sia $R \subseteq S \times S$ relazione di equivalenza

La classe di equivalenza di $x \in S$ modulo R è l'insieme: $[x]_R = \{y \in S | yRx\} \subseteq S$

L'insieme quoziante di S modulo R è l'insieme di tutte le classi di equivalenza degli elementi di S : $S \setminus R = \{[x]_R | x \in S\}$

Proposizione:

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

- $x \in [x]_R \quad \forall x \in S \quad ([x]_R \neq \emptyset)$
- se $xRy \Rightarrow [x]_R = [y]_R$

- se $x \not R y \Rightarrow [x]_R \cap [y]_R = \emptyset$

Questo ci dice che $S \setminus R$ è una partizione di S , infatti:

- $\forall [x]_R \neq \emptyset$ (perchè $x \in [x]_R$)
- $\forall [x]_R, [y]_R$ si ha $[x]_R = [y]_R$ ($x R y$) oppure $[x]_R \cap [y]_R = \emptyset$ ($x \not R y$)
- $S = \bigcup \{[x]_R \mid [x]_R \in S \setminus R\}$ perchè $\forall x \in S, \exists y \in S \setminus R : x \in Y$ ($Y = [x]_R$)

Proposizione:

Le seguenti affermazioni sono equivalenti, date $R_1, R_2 \subseteq S \times S$ relazioni d'equivalenza:

- $R_1 = R_2$
- $\forall x \in S, [x]_{R_1} = [x]_{R_2}$
- $S \setminus R_1 = S \setminus R_2$

Teorema fondamentale sulle relazioni d'equivalenza:

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

- se $R \subseteq S \times S$ è di equivalenza, allora $S \setminus R$ è una partizione di S
- se F è una partizione di S , $\exists! R_F \subseteq S \times S$ relazione d'equivalenza tale che $F = S \setminus R_F$

Relazioni d'ordine

Definizione:

$R \subseteq S \times S$ è d'ordine se è:

- Riflessiva: $\forall x \in S, xRx$
- Antisimmetrica: $\forall x, y \in S, xRy, yRx \Rightarrow x = y$
- Transitiva: $\forall x, y, z \in S, xRy, yRz \Rightarrow xRz$

Ordine stretto, insieme ordinato, ordine totale, omomorfismo d'ordine:

Se invece è Antisimmetrica e Transitiva ma **non** Riflessiva, è di **ordine stretto**

DATO (S, \leq)
ORDINE STRETTO: $x \leq y \Leftrightarrow x \leq y \wedge x \neq y$

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

Siano $(S, \leq), (T, \preceq)$ due insiemi ordinati, $f : S \rightarrow T$ è omomorfismo d'ordine se $\forall x, y \in S, x \leq y \Rightarrow f(x) \preceq f(y)$ *l'f PRESERVA L'ORDINE*

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

Minimo, massimo:

Un minimo per (S, \leq) è un elemento $a \in S$ tale che $a \leq x, \forall x \in S$

Un massimo per (S, \leq) è un elemento $a \in S$ tale che $x \leq a, \forall x \in S$

Lemma: massimo e minimo, se esistono, sono unici

Minimale, massimale:

Un elemento $c \in S$ è detto minimale se $\nexists a \in S : a \leq c$

Un elemento $c \in S$ è detto massimale se $\nexists a \in S : c \leq a$

Lemma: ogni insieme ordinato finito ha massimali e minimali; se è totalmente ordinato, ha massimo e minimo

Insieme bene ordinato, lemma:

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

Lemma: se (S, \leq) è bene ordinato, allora è totalmente ordinato (ma non viceversa)

Minorante, maggiorante:

Un elemento $w \in S$ è detto maggiorante per X se $x \leq w, \forall x \in X$

Un elemento $w \in S$ è detto minorante per X se $w \leq x, \forall x \in X$

Estremo inferiore, estremo superiore:

Dato (S, \leq) e $X \subseteq S, X \neq \emptyset$,

$M = \{w \in S | w \text{ è minorante per } X\}$ insieme dei minoranti

$N = \{w \in S | w \text{ è maggiorante per } X\}$ insieme dei maggioranti

*

L'estremo inferiore di X è il più grande dei minoranti, cioè è tale che:

- $k \leq x, \forall x \in X$
- $\forall s : s \leq x, \forall x \in X \Rightarrow s \leq k$

L'estremo superiore di X è il più piccolo dei maggioranti, cioè è tale che:

- $x \leq h, \forall x \in X$
- $\forall s : x \leq s, \forall x \in X \Rightarrow h \leq s$

Reticolo:

Sia (L, \leq) insieme ordinato. L è detto reticolo se $\forall x, y \in L$ esistono sempre $\inf\{x, y\}$ e $\sup\{x, y\}$ ($x \wedge y, x \vee y$)

Proprietà:

- idempotenza: $x \vee x = x \wedge x = x$
- commutatività: $x \vee y = y \vee x, x \wedge y = y \wedge x$
- associatività: $x \vee (y \vee z) = \sup\{x, y, z\} = (x \vee y) \vee z, x \wedge (y \wedge z) = \inf\{x, y, z\} = (x \wedge y) \wedge z$
- assorbimento: $x \wedge (x \vee y) = x \vee (x \wedge y) = x$

Reticolo distributivo, limitato, complementato:

(L, \leq) reticolo è **distributivo** se $\forall x, y, z \in L$ valgono le seguenti proprietà distributive:

- $x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z)$
- $x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)$

Un reticolo è **limitato** se possiede un massimo e un minimo (1 e 0)

Dato (L, \leq) limitato e $x \in L$, se esiste $\bar{x} \in L$ tale che $x \vee \bar{x} = 1$ e $x \wedge \bar{x} = 0$, \bar{x} è **complemento** di x

Lemma: in un reticolo limitato e distributivo, il complemento è unico

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

Algebra di Boole:

Un reticolo distributivo, limitato, complementato è detto algebra di Boole

Teorema di Stone:

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

Allora esiste S insieme tale che (L, \leq) è isomorfo (omomorfismo biettivo) a $(P(S), \subseteq)$

Le algebre di Boole finite hanno tutte cardinalità del tipo 2^n dove $n = |S|$

3. Calcolo combinatorio

Principi

Principio di addizione:

Siano A, B insiemi finiti con $A \cap B = \emptyset$, allora $|A \cup B| = |A| + |B|$

Principio 2:

Sia A finito, $C \subseteq A$, allora:

- $|A \setminus C| = |A| - |C|$
- $\forall B$ insieme qualunque $|A \setminus B| = |A| - |A \cap B|$

Principio di inclusione-esclusione:

Siano A, B finiti, allora $|A \cup B| = |A| + |B| - |A \cap B|$

Forma generale:

Sia $k \geq 2$ e siano A_1, \dots, A_k insiemi finiti, allora si ha:

$$|\bigcup_{i=1}^k A_i| = \sum_{i=1}^k |A_i| - \sum_{1 \leq i < j \leq k} |A_i \cap A_j| + \sum_{1 \leq i < j < h \leq k} |A_i \cap A_j \cap A_h| + \dots + (-1)^k |\bigcap_{i=1}^k A_i|$$

Principio di moltiplicazione:

Siano S, T finiti, allora $|S \times T| = |S| \cdot |T|$

Insieme potenza:

Siano S, T insiemi, $T^S = \{f : S \rightarrow T | f \text{ funzioni}\}$ è detto insieme potenza e $|T_S| = |T|^{|S|}$

Principio dei cassetti:

Dati $n, m \in \mathbb{N}, n > m$, se si vogliono riporre m oggetti in n scatole, almeno una scatola conterrà 2 oggetti

Forma forte:

Sia $n \in \mathbb{N}$ e si considerino i numeri naturali $q_1, \dots, q_n \geq 2$. Si ponga $k = q_1 + \dots + q_n - n + 1$. Se k oggetti sono ripartiti in n scatole, allora o la prima contiene almeno q_1 oggetti, o la seconda almeno q_2 oggetti, ..., o la n -esima almeno q_n oggetti

Permutazioni, disposizioni, combinazioni

Fattoriale:

Dato $n \in \mathbb{N}_0$, chiamiamo fattoriale di n il prodotto $n \cdot (n-1) \cdot (n-2) \cdot \dots \cdot 2 \cdot 1$

Proposizione:

Se X è finito, $|X| = n$, allora il numero di applicazioni biettive $f : X \rightarrow X$ è $n!$

Permutazioni:

Un'applicazione biettiva di X in X (finito) è detta permutazione, e $|P_X| = n!$ se $|X| = n$

Proposizione:

Se $\exists f : X \rightarrow Y$ biettiva, allora esiste $g : P_X \rightarrow P_Y$ biettiva

Permutazioni con ripetizione:

Ho n oggetti da permutare di cui n_1 sono uguali tra loro, \dots , n_k sono uguali tra loro:
$$\frac{n!}{n_1!n_2!\dots n_k!}$$

Disposizioni:

Numero delle disposizioni di n oggetti su h posti: $D_{n,h} = n(n-1)..(n-h+1) = \frac{n!}{(n-h)!}$

Proposizione:

$$D_{n,h} = \{\text{applicazioni iniettive di } X \text{ in } Y\}$$

Disposizioni con ripetizione:

Il numero delle disposizioni di n oggetti su h posti è n^h , e corrisponde al numero di tutte le funzioni da un insieme di cardinalità h ad uno di cardinalità n

Combinazioni:

Dati $n, h \in \mathbb{N}_0$ con $0 \leq h \leq n$ si chiama **coefficiente binomiale** il numero delle combinazioni semplici di n oggetti su h posti, e si indica con $\binom{n}{h} = \frac{n!}{(n-h)!h!} = \frac{D_{n,h}}{h!}$

Proprietà:

- $\binom{n}{h} = \binom{n}{n-h}$
- $\binom{n}{h-1} + \binom{n}{h} = \binom{n+1}{h}$

Proposizioni:

Il numero di sottoinsiemi di ordine h di un sottoinsieme di n elementi è $\binom{n}{h}$

Combinazioni con ripetizione:

Il numero delle combinazioni con ripetizioni di n oggetti tra k è $C'_{n,k} = \binom{n+k-1}{k}$

Binomio di Newton:

Per $a, b \in \mathbb{R}, n \in \mathbb{N}_0$ si ha $(a+b)^n = \sum_{i=0}^n \binom{n}{i} a^{n-i} b^i = \sum_{i=0}^n \binom{n}{i} a^i b^{n-i}$

Lemma: la somma $\binom{n}{0} + \binom{n}{1} + .. + \binom{n}{n} = 2^n$

4. Aritmetica

Numeri naturali e seconda forma del principio di induzione

Assiomi di Peano:

Presi una terna $(\mathbb{N}_0, f, 0)$, $f : \mathbb{N}_0 \rightarrow \mathbb{N}_0$ tale che:

- $0 \notin f(\mathbb{N}_0)$
- f è iniettiva
- se $X \subseteq \mathbb{N}_0$ è tale che

- $0 \in X$
- da $s \in X \Rightarrow f(s) \in X$

allora $X = \mathbb{N}_0$

Successore:

f è detta funzione successore: $1 = f(0), 2 = f(f(0)), \dots, n = f(f..(f(0)))$ n volte,
 $n + 1 = f(n)$

Principio di induzione (seconda forma):

Dato $X \subseteq \mathbb{N}_0$ tale che:

- $\bar{n} \in X$
- dato $t > \bar{n}$ se $k \in X, \forall \bar{n} \leq k < t$ implica $t \in X$

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

Applicazioni del principio di induzione:

Algoritmo della divisione euclidea in \mathbb{N}_0 :

Sia $b \in \mathbb{N}$, allora $\forall n \in \mathbb{N}_0$ esistono unici $q, r \in \mathbb{N}$ tali che $n = qb + r$ con $r < b$

I numeri q e r sono detti rispettivamente il quoziente e il resto della divisione di n per b

Teorema fondamentale dell'aritmetica:

Per ogni $n \geq 2, n \in \mathbb{N}$ esistono $t \in \mathbb{N}$ e p_1, \dots, p_t numeri primi tali che $n = p_1 \cdot \dots \cdot p_t$

La decomposizione è unica a meno dell'ordine dei fattori

Teorema di Euclide:

Esistono infiniti numeri primi

Crivello di Eratostene:

Sia $n \geq 2, n \in \mathbb{N}$. Se n non ammette un divisore primo p con $p^2 \leq n \Rightarrow n$ è primo

Divisibilità tra interi

Algoritmo della divisione euclidea in \mathbb{Z} :

Siano $a, b \in \mathbb{Z}$ con $b \neq 0$, allora $\exists! q, r \in \mathbb{Z} : a = qb + r$ con $0 \leq r < |b|$

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

Proprietà:

- $\text{rest}(a, b) = \text{rest}(a, -b)$
- $\text{rest}(-a, b) = b - \text{rest}(a, b)$ se $\text{rest}(a, b) \neq 0$, $= 0$ se $\text{rest}(a, b) = 0$

Divisori:

Dato $a \in \mathbb{Z}$, $D(a) = \{x \in \mathbb{Z} | x|a\}$ è l'insieme dei divisori interi di a

Se $D(a)$ è finito, $|D(a)| \geq 4$ perchè $1, -1, a, -a$ dividono tutti a

Lemma: dati $x, y, z, k \in \mathbb{Z}$ tali che $x = yk + z$, si ha $D(x) \cap D(y) = D(z) \cap D(y)$

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

Massimo comune divisore:

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:

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

Lemma: dati $a, b \in \mathbb{Z} \setminus \{0\}$

- d è MCD di a e $b \Leftrightarrow -d$ lo è
- d è MCD di a e $b \Leftrightarrow$ per ogni altro k che è MCD si ha $k \in \{d, -d\}$ (è unico a meno del segno)

Lemma: siano $a, b, d \in \mathbb{Z}$, $d \geq 0$, $d = MCD(a, b) \Leftrightarrow D(d) = D(a) \cap D(b)$

Proposizione: per ogni $a, b \in \mathbb{Z}$, il $MCD(a, b)$ esiste sempre

$a, b \in \mathbb{Z}$ sono detti **coprimi** se il $MCD(a, b) = 1$

Lemma:

- $a, p \in \mathbb{Z}$, p primo, se $p|a \Rightarrow MCD(p, a) = 1$
- $a, b \in \mathbb{Z} \setminus \{0\}$, $d = MCD(a, b)$, allora $\exists a', b' : a = da', b = db'$ e $MCD(a', b') = 1$

Teorema di Bezout:

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

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

Conseguenze:

- $a, b, c \in \mathbb{Z}$, se $a|bc$ e $MCD(a, b) = 1 \Rightarrow a|c$
- $a, b, p \in \mathbb{Z}$, p primo, se $p|ab \Rightarrow p|a$ oppure $p|b$

Teorema fondamentale dell'aritmetica in \mathbb{Z} :

Sia $z \in \mathbb{Z} \setminus \{-1, 0, 1\}$, allora esistono $k \geq 1$ e $p_1, \dots, p_k \in \mathbb{Z}$ numeri primi tali che $z = p_1 \cdot \dots \cdot p_k$

La rappresentazione è unica a meno dell'ordine dei fattori e del loro segno

Minimo comune multiplo:

Dati $a, b \in \mathbb{Z}$. m è detto **minimo comune multiplo** di a e b se:

- $a|m$ e $b|m$
- $\forall t \in \mathbb{Z}, a|t$ e $b|t \Rightarrow m|t$

Proprietà:

Dati $a, b \in \mathbb{Z}$ e $d = MCD(a, b)$, posto $a = da'$ e $b = db'$, si ha:

- $m = a'b'd$ è un minimo comune multiplo per a, b

- m' è un altro mcm $\Leftrightarrow m' = \pm m$

$$|ab| = MCD(a, b) \cdot mcm(a, b)$$

Congruenze

Relazione $m\mathbb{Z}$:

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

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

Proposizione: $m\mathbb{Z}$ è una relazione d'equivalenza compatibile con le operazioni + e ·, cioè $\forall a, b, c, d \in \mathbb{Z}$ se $a \text{ } m\mathbb{Z} \text{ } c$ e $b \text{ } m\mathbb{Z} \text{ } d$, allora $a + b \text{ } m\mathbb{Z} \text{ } c + d$ e $ab \text{ } m\mathbb{Z} \text{ } cd$

Congruenza:

$m\mathbb{Z}$ è una congruenza (relazione d'equivalenza compatibile con le operazioni di \mathbb{Z}) ed è detta congruenza modulo m

L'insieme quoziante $\mathbb{Z} \setminus m\mathbb{Z}$ si indica con \mathbb{Z}_m ed è detto insieme degli interi modulo m

Indichiamo gli elementi di \mathbb{Z}_m con $[x]_m$ oppure \bar{x}

Proposizione:

Dati $m, x \in \mathbb{Z}$ si ha $[x]_m = \{x + km | k \in \mathbb{Z}\}$ e, se $m \neq 0$, $[x]_m = [rest(x, n)]_m$

Teorema:

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

Lemma:

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

- $a \equiv b \pmod{m} \Leftrightarrow \forall t \in \mathbb{Z}, a + t \equiv b + t \pmod{m}$
- $a \equiv b \pmod{m} \Rightarrow \forall t \in \mathbb{Z}, at \equiv bt \pmod{m}$
- $at \equiv bt \pmod{m} \Rightarrow a \equiv b \pmod{m}$ se $MCD(t, m) = 1$

Lemma:

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

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

Funzione di Eulero

Indicatore di Gauss-Eulero:

$\forall m \in \mathbb{Z}$ sia $\mathbb{Z}_m^* = \{[a]_m | MCD(a, m) = 1\} \subseteq \mathbb{Z}_m$ l'insieme delle classi di equivalenza di numeri coprimi con m

$|\mathbb{Z}_m^*|$ è detta indicatore di Gauss-Eulero e si indica con $\varphi(m)$

Se p è primo (coprimo con tutti), $\mathbb{Z}_p^* = \{[1]_p, \dots, [p-1]_p\}$ quindi $\varphi(p) = p - 1$

Per induzione si ha $\varphi(p^n) = p^n - p^{n-1}$

Funzione di Eulero

$$\begin{cases} \varphi(1) = 1 \\ \varphi(n) = |\{m \in \mathbb{N} | m < n \text{ e } MCD(n, m) = 1\}| \end{cases} \quad \text{cardinalità dei coprimi} < n$$

Lemma: $\forall h, k \in \mathbb{N}, \varphi(hk) = \varphi(h) \cdot \varphi(k)$

Teorema piccolo di Fermat:

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

Teorema di Fermat-Eulero:

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

Teorema di Wilson:

Se $p \in \mathbb{N} \setminus \{1\}$, allora p è primo $\Leftrightarrow (p-1) \equiv -1 \pmod{p}$

Sistemi di equazioni congruenziali lineari

Definizione:

Dati $m > 0, a, b \in \mathbb{Z}, ax \equiv b \pmod{m}$ è un'equazione congruenziale lineare

Teorema:

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

Tutte le possibili soluzioni sono gli elementi della classe di equivalenza $[s]_m = \{z \in \mathbb{Z} | az \equiv b \pmod{m}\}$

Teorema:

Dati $m > 0, a, b \in \mathbb{Z}, t \in \mathbb{Z}$ tale che $t|a, t|b, t|m$

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

Osservazione: $s = \{z \in \mathbb{Z} | az \equiv b \pmod{m}\} = \{z \in \mathbb{Z} | \frac{a}{t}z \equiv \frac{b}{t} \}$

ma $s = [s]_{\frac{m}{d}} = [s]_m \cup [s + \frac{m}{d}]_m \cup [s + \frac{2m}{d}]_m \cup \dots \cup [s + \frac{(d-1)m}{d}]_m$

Teorema cinese del resto:

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

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

L'insieme di tutte le soluzioni è $[s]_{m_1 m_2 \dots m_k}$

Generalizzazione: il sistema ha soluzione $\Leftrightarrow MCD(m_i, m_j) | b_i - b_j$ ($m_i \neq m_j$)

5. Strutture algebriche

Strutture algebriche

Operazione interna:

Dato S insieme, $\perp : S \times S \rightarrow S$ applicazione dal prodotto cartesiano $S \times S$ in S è detta **operazione interna** ad S

(S, \perp) è detto **struttura algebrica**

L'operazione può essere:

- commutativa: $x \perp y = y \perp x, \forall x, y \in S$
- associativa: $(x \perp y) \perp z = x \perp (y \perp z), \forall x, y, z \in S$

Elemento neutro, simmetrizzabile, cancellabile:

Un elemento $e \in S$ è detto **elemento neutro** per \perp se $\forall x \in S \begin{cases} x \perp e = x \\ e \perp x = x \end{cases}$

Se (S, \perp) ha elemento neutro $e \in S$, s è **simmetrizzabile** se $\exists y \in S$ tale che $x \perp y = y \perp x = e$

Un elemento $a \in S$ è **cancellabile** se è:

- cancellabile a sinistra: $a \perp x = a \perp y \Rightarrow x = y$
- cancellabile a destra: $x \perp a = y \perp a \Rightarrow x = y$

Operazione esterna:

Dati Ω, S insiemi, una **operazione esterna** su S è

$$\star : \Omega \times S \rightarrow S$$
$$(\alpha, x) \rightarrow \alpha \star x$$

Strutture notevoli

(S, \perp) struttura algebrica è detta:

- ▼ **semigruppo** se \perp è associativa
esempi: $(\mathbb{N}, +)$
- ▼ **monoide** se \perp è associativa ed esiste l'elemento neutro
esempi: $(\mathbb{N}_0, +)$
- ▼ **gruppo** se \perp è associativa, esiste l'elemento neutro e ogni elemento è simmetrizzabile
esempi: $(\mathbb{R}_b^{\mathbb{R}}, \circ)$ biettiva, altrimenti non ha inverso

▼ **gruppo abeliano** se è un gruppo e \perp è commutativa

esempi: $(\mathbb{Z}, +)$

S con due operazioni interne, (S, \perp, \top) è detto:

▼ **anello** se (S, \perp) è un gruppo abeliano, \top è associativa e $a \top (b \perp c) = (a \top b) \perp (a \top c) \quad \forall a, b, c \in S$

▼ **anello unitario** se esiste elemento neutro per \top

esempi: $(M_2(\mathbb{R}), +, \cdot)$ unitario ma non commutativo

▼ **anello commutativo** se \top è commutativa

esempi: $(\mathbb{Z}, +, \cdot)$ commutativo unitario

▼ **corpo** se è un anello unitario e ogni elemento è simmetrizzabile rispetto a \top (tranne l'elemento neutro di \perp)

▼ **campo** se è un corpo e \top è commutativa

esempi: $(\mathbb{Q}, +, \cdot), (\mathbb{R}, +, \cdot)$

Sottostrutture, strutture quoziante

Parte stabile, sottostruttura:

Dato (S, \perp) , $X \subseteq S$, X è detto **parte stabile** (o chiuso) rispetto a \perp se $\forall x, y \in X \Rightarrow x \perp y \in X$

Si definisce in X l'operazione indotta \perp' : $(x, y) \in X \times X \rightarrow x \perp y \in X$, si pone cioè $x \perp' y = x \perp y, \forall x, y \in X$

(X, \perp) è detto sottostruttura S

Teorema:

Sia (S, \perp) monoide e si consideri l'insieme $U(S) = \{x \in S | x \text{ è simmetrizzabile}\}$, allora $U(S)$ è parte stabile di S ed è un gruppo, detto **gruppo degli elementi invertibili**

Lemma:

Sia $m > 0$, $MCD(a, m) = 1 \Leftrightarrow [a]_m$ è invertibile in (\mathbb{Z}_m, \cdot)

Congruenza:

Dati (S, \perp) struttura algebrica, $R \subseteq S \times S$ relazione di equivalenza, R è una **congruenza** se è compatibile con \perp , cioè $(x_1 R y_1 \text{ e } x_2 R y_2) \Rightarrow (x_1 \perp x_2) R (y_1 \perp y_2)$

Struttura quoziante:

L'insieme quoziante $S \setminus R$ eredita la struttura algebrica di S

Si definisce l'operazione quoziante $\perp' : ([x]_R, [y]_R) \in S \setminus R \times S \setminus R \rightarrow [x \perp y]_R \in S \setminus R$

La struttura $(S \setminus R, \perp')$ è detta struttura quoziante

Struttura prodotto:

Siano (S, \perp_S) , (V, \perp_V) due strutture algebriche, la struttura prodotto $(S \times V, \perp)$ è ottenuta in questo modo:

- $S \times V$ è il prodotto cartesiano
- per $(x, y), (z, w) \in S \times V$ si ha $(x, y) \perp (z, w) = (x \perp_S z, y \perp_V w)$

Omomorfismo

Omomorfismo:

Date $(S, *_S)$ e $(T, *_T)$ due strutture algebriche, $f : S \rightarrow T$ funzione è detta **omomorfismo** se $f(x *_S y) = f(x) *_T f(y)$

- **monomorfismo**: omomorfismo iniettivo
- **epimorfismo**: omomorfismo suriettivo
- **isomorfismo**: omomorfismo biettivo
- **endomorfismo**: omomorfismo $f : (S, *) \rightarrow (S, *)$
- **automorfismo**: endomorfismo biettivo

(S, \perp) , R congruenza su S $\pi : S \rightarrow S \setminus R$, $x \rightarrow [x]_R$ è epimorfismo, detto **proiezione canonica** (nel quoziente)

Divisori dello zero

Divisore dello zero:

Un elemento $a \in S$ è detto **divisore dello zero** se $\exists b \in S$ tale che $a \cdot b = 0$ ma $a \neq 0$ e $b \neq 0$

Dominio di integrità:

Un **dominio di integrità** è un anello privo di divisori dello zero