Strutture Discrete

Appunti delle lezioni della Professoressa Sabina Rossi

Ibrahima Tely Barry

Anno Accademico 2024-2025

Indice

Capitolo 0

Note al lettore

Questi appunti sono realizzati esclusivamente a scopo didattico, con l'intento di fornire un supporto integrativo allo studio. Non sostituiscono né le lezioni né il libro di testo, ma possono essere utilizzati come materiale aggiuntivo per chiarire o approfondire alcuni argomenti.

Ci tengo a sottolineare che gli appunti non devono essere venduti o distribuiti a fini di lucro.

Infine, non escludo la possibilità che possano esserci errori o imprecisioni. Invito quindi i lettori a utilizzare questi appunti con spirito critico e a fare riferimento alle fonti originali per ulteriori chiarimenti.

Capitolo 1

Logica

La logica si occupa dello studio di proposizioni che possono risultare vere o false. Questi due valori sono indicati come vero e falso e le proposizioni di questo tipo comunemente sono chiamate predicati.

1.1 Proposizioni

Definizione 1.1:

Una proposizione è un'affermazione che è vera o falsa, ma non può essere contemporaneamente vera e falsa.

Definizione 1.2:

Una proposizione composta si ottiene da proposizioni semplici mediante l'uso dei connettivi logici e quantificatori, vediamone alcuni esempi:

- 5 è un numero primo e 8 è un numero pari
- *Un* numero è pari se e solo se è divisibile per 2
- *Ogni* numero naturale è somma di 2 numeri primi
- $\forall x \, \exists y$ tale che $P(x, y)$

1.2 Predicati

Definizione 1.3:

I predicati sono enunciati che dipendono da una o più variabili a proposito di un certo insieme D, detto dominio.

La logica si occupa e unifica postulati come l'algebra detta algebra di Boole. Tale algebra è definita su un insieme D i cui valori sono vero (V) e falso (F).

Un predicato atomico con variabili $P(x)$ esprime una relazione tra oggetti, possibilmente specificati mediante variabili, e denota un valore di verità quando le variabili vengono interpretate in un dominio.

Esempi:

- x divide 12
- $x + 5 = 10$
- x è dispari
- $x \leq 10$
- $P(x) \wedge P(y)$

Predicati atomici con variabili

Definizione 1.4:

Un predicato con variabili $P(x)$ esprime una relazione tra oggetti mediante variabili, e denota valori di verità, quando le variabili vengono interpretate in un dominio. Per esempio:

- x divide 22.

Supponiamo che il dominio sia 2, se x divide 22 allora $x = 2$ e $x = 11$.

Connettivi Logici

Definizione 1.5:

I connettivi logici sono operatori che combinano una o più proposizioni (affermazioni che possono essere vere o false) per formarne di nuove e più complesse. Questi connettivi sono essenziali in logica matematica, logica proposizionale e informatica per costruire espressioni logiche e dedurre inferenze.

Predicati Composti

Per creare espressioni logiche più complesse partendo da proposizioni semplici, si utilizzano tre simboli principali:

- Il simbolo $\neg$ rappresenta la negazione.
- Il simbolo $\wedge$ rappresenta la congiunzione (”e”).
- Il simbolo $\vee$ rappresenta la disgiunzione (”o”).

Sia P una proposizione. L’espressione $\neg P$ si legge ”non P” e rappresenta la negazione di P. Se P è vero, $\neg P$ sarà falso, e viceversa.

Sia Q un’altra proposizione. L’espressione $P \vee Q$ si legge ”P o Q” e rappresenta la disgiunzione tra P e Q, mentre $P \wedge Q$ si legge ”P e Q” e rappresenta la congiunzione tra P e Q.

Valori di verità dei connettivi logici

Le proposizioni composte, formate da proposizioni atomiche e dagli operatori $\wedge$, $\vee$, e $\neg$, devono avere valori di verità ben definiti. Ciò significa che ciascuna proposizione composta è vera o falsa, a seconda dei valori di verità delle proposizioni che la compongono.

Ora definiamo i valori di verità per le principali operazioni logiche:

Disgiunzione

Definizione 1.6:

Siano P e Q due proposizioni. La proposizione $P \vee Q$ (disgiunzione) è vera se almeno una delle due proposizioni P o Q è vera. È falsa solo quando sia P che Q sono false.

Congiunzione

Definizione 1.7:

Siano P e Q due proposizioni. La proposizione $P \wedge Q$ (congiunzione) è vera se entrambe P e Q sono vere. Se almeno una delle due è falsa, la congiunzione è falsa.

Negazione

Definizione 1.8:

Sia P una proposizione. La proposizione $\neg P$ (negazione) è vera quando P è falsa, ed è falsa quando P è vera.

Ordine delle Operazioni

Le operazioni logiche seguono un ordine di precedenza, simile a quello delle operazioni aritmetiche:

- La **negazione** ($\neg$) ha la priorità più alta, quindi viene eseguita per prima.
- La **congiunzione** ($\wedge$) ha una priorità maggiore rispetto alla disgiunzione ($\vee$).
- La **disgiunzione** ($\vee$) ha la priorità più bassa.

Pertanto, quando si incontrano più operatori, si segue questo ordine per valutarli. Ora per consolidare i concetti andremo a vedere qualche esempio:

1. Formalizzare le seguenti frasi in logica proposizionale:

   a) Non fa caldo ma c'è il sole

- Definizione delle proposizioni:

$$P : \text{fa caldo}$$

$$Q : \text{c'è il sole}$$

- Traduzione logica della frase:
  - "Non fa caldo" si traduce in $\neg P$
  - "C'è il sole" si traduce in Q
  - "Ma" equivale all'operatore logico $\wedge$ (e)
- Formalizzazione completa:

$$\neg P \wedge Q$$

b) Non piove né fa caldo

- Definizione delle proposizioni:

$$P : \text{piove}$$

$$Q : \text{fa caldo}$$

- Traduzione logica della frase:
  - "Non piove" si traduce in $\neg P$
  - "Non fa caldo" si traduce in $\neg Q$
  - "Né" si traduce con l'operatore logico $\wedge$ (e)
- Formalizzazione completa:

$$\neg P \wedge \neg Q$$

2. Costruire la seguente tabella di verità per le proposizioni P e Q:

P	Q	$P \wedge Q$	$P \vee Q$	$\neg P$
V	V	V	V	F
V	F	F	V	F
F	V	F	V	V
F	F	F	F	V

3. Verificare la seguente espressione logica costruendo la relativa tabella di verità:

$$\big(P \vee Q\big) \wedge \neg\big(P \wedge Q\big)$$

Costruire la tabella di verità per le proposizioni P e Q, e mostrare i passaggi intermedi.

P	Q	$P \vee Q$	$P \wedge Q$	$\neg(P \wedge Q)$	$\big(P \vee Q\big) \wedge \neg\big(P \wedge Q\big)$
V	V	V	V	F	F
V	F	V	F	V	V
F	V	V	F	V	V
F	F	F	F	V	F

Leggi di De Morgan

Se viene applicata la **negazione** alla **disgiunzione**$(\vee)$, si ottiene la **congiunzione** $(\wedge)$ della negazione di due argomenti. Mentre se si applica la negazione ad una congiunzione si ottiene la disgiunzione della negazione di 2 elementi.

$$\neg\big(P \vee Q\big) \equiv \big(\neg P\big) \wedge \big(\neg Q\big)$$

$$\neg\big(P \wedge Q\big) \equiv \big(\neg P\big) \vee \big(\neg Q\big)$$

Esempio Si considerino le due proposizioni semplici:

1. $P = 27$ è un multiplo di 4.

2. $Q = 27$ è un multiplo di 5.

E le proposizioni composte:

1. $\neg\big(P \vee Q\big) = 27$ non è un multiplo di 4 o di 5.

2. $\neg\big(P\big) \wedge \neg\big(Q\big) = 27$ non è un multiplo di 4 e 27 non è un multiplo di 5.

Si intuisce facilmente che queste due proposizioni coincidono.
Pertanto qualunque siano valori di verità di P e Q le proposizioni:

$$\neg\big(P \vee Q\big) \text{ e } \neg\big(P\big) \wedge \neg\big(Q\big)$$

hanno sempre lo stesso valore di verità. In questo caso diciamo che le due proposizioni sono **logicamente equivalenti**.

Esercizio Dimostrare che :

$$\neg\big(P \vee Q\big) = \neg\big(P\big) \wedge \neg\big(Q\big)$$

P	Q	$\big(P \vee Q\big)$	$\neg\big(P \vee Q\big)$
V	V	V	F
V	F	V	F
F	V	V	F
F	F	F	V

P	Q	$\neg P$	$\neg Q$	$\neg\big(P\big) \wedge \neg\big(Q\big)$
V	V	F	F	F
V	F	F	V	F
F	V	V	F	F
F	F	V	V	V

Descrizione logica dello XOR ($\oplus$)

La proposizione $P \oplus Q$ (XOR) è vera se una delle due proposizioni è vera, ma non entrambe. In altre parole:

$$P \oplus Q \text{ è vero se } (P \vee Q) \wedge \neg(P \wedge Q)$$

In simboli logici:

$$P \oplus Q \equiv (P \vee Q) \wedge \neg(P \wedge Q)$$

La tabella di verità per $P \oplus Q$ è la seguente:

P	Q	$P \oplus Q$
V	V	F
V	F	V
F	V	V
F	F	F

Teorema 1.1:

Per ogni numero naturale n:

$$n^2 + n$$

è un numero naturale pari $\{n \in \mathbb{N} \mid 2n\}$.

Dimostrazione 1.1. Dobbiamo dimostrare che esiste un numero naturale tale che per ogni numero naturale n tale per cui n è un numero pari.

Se n è un numero pari allora $n = 2 \cdot r$, dove $r \in \mathbb{N}$.

$$(2r)^2 + 2r = 2\,(2r + 1)$$

Se n è un numero dispari allora $n = 2 + 1 \cdot r$, dove $r \in \mathbb{N}$.

$$(2r + 1)^2 + 2r = 4r^2 + 6r + 2 = 2\left(2r^2 + 3r + 1\right)$$

□

1.3 Equivalenza logica

Le proposizioni:

$$6 > 3 \text{ e } 3 < 6$$

Sono due modi diversi di esprimere lo stesso concetto. Questo accade a causa della definizione dei simboli "maggiore di" ($>$) e "minore di" ($<$):

- La proposizione $6 > 3$ significa che 6 è maggiore di 3.
- La proposizione $3 < 6$ significa che 3 è minore di 6.

Tuttavia, per la definizione dei simboli di maggiore e minore, possiamo dire che queste due proposizioni sono **logicamente equivalenti**. Al contrario, le proposizioni:

- I cani abbaiano e i gatti miagolano.
- I gatti miagolano e i cani abbaiano.

Esprimono lo stesso significato, ma non a partire dal significato delle parole, bensì per la loro forma logica. Qualsiasi coppia di enunciati che abbiano una forma logica simile risulterebbe essere entrambi vera o entrambi falsa. Questo può essere verificato osservando la seguente tavola di verità, dove le variabili P e Q sostituiscono gli enunciati dell'esempio precedente, rispettivamente.

La tavola di verità mostra che per ciascuna combinazione di valori di verità di P e Q, $P \wedge Q$ è vera se e solo se, anche $\neg P \vee Q$ è vera.

In questo caso, le due forme degli enunciati si dicono logicamente equivalenti, e affermiamo che le proposizioni viste in precedenza sono logicamente equivalenti.

P	Q	$P \wedge Q$	$\neg P \vee Q$
V	V	V	V
V	F	F	F
F	V	F	V
F	F	F	F

Definizione 1.9:

Due proposizioni sono chiamate logicamente equivalenti, se e solo se hanno lo stesso valore di verità per ogni sostituzione degli enunciati nello lor variabili. L'equivalenza logica tra due forme di enunciati equivalenti è indicato con:

$$P \equiv Q$$

Due predicati sono logicamente equivalenti se e solo se le loro formule logiche sono equivalenti, se quando vengono sostituiti con le stesse variabili logiche, le formule risultanti producono esattamente gli stessi valori di verità in ogni caso possibile.

Esempio 1.1. Doppia Negazione

$$\neg(\neg P) \equiv P$$

P	$\neg P$	$\neg(\neg P)$
V	F	V
F	V	F

Esempio 1.2. Esempio di non equivalenza:
Consideriamo le due proposizioni:

$$\neg(P \wedge Q) \quad \text{e} \quad \neg P \vee \neg Q$$

P	Q	$\neg P$	$\neg Q$	$\neg(P \wedge Q)$	$\neg P \vee \neg Q$
V	V	F	F	F	F
V	F	F	V	V	V
F	V	V	F	V	V
F	F	V	V	V	V

Questa tavola di verità mostra che $\neg(P \wedge Q)$ e $\neg P \vee \neg Q$ hanno gli stessi valori di verità in tutti i casi, quindi possiamo affermare che sono logicamente equivalenti:

$$\neg(P \wedge Q) \equiv \neg P \vee \neg Q$$

Metodo alternativo per dimostrare la non equivalenza:

Questo metodo utilizza un esempio per dimostrare che $\neg(P \wedge Q) \not\equiv \neg P \vee \neg Q$. Sia l'enunciato $1 < 0$ ed $1 \geq 0$. Allora $\neg(P \wedge Q)$ significa "non è vero che sia $1 < 0$ e $1 \geq 0$", che è vero, poiché $1 < 0$ è falso. D'altra parte, $\neg P \vee \neg Q$ significa "o 1 non è minore di 1 o 1 non è maggiore di 0", che è falso. Questo esempio dimostra che è possibile sostituire valori concreti per P e Q in modo che una delle forme risulti vera e l'altra falsa. Pertanto, le due forme di enunciato non sono logicamente equivalenti.

1.4 Leggi di De Morgan

La negazione di un enunciato con il connettivo $\wedge$ è logicamente equivalente a un enunciato con il connettivo $\vee$ in cui ciascuna delle parti è negata. Allo stesso modo, la negazione di un enunciato con il connettivo $\vee$ è logicamente equivalente a un enunciato con $\wedge$ in cui ciascuna delle parti è negata.

Esempio 1.3. $\neg(P \wedge Q) \equiv (\neg P) \vee (\neg Q)$

P	Q	$\neg P$	$\neg Q$	$P \wedge Q$	$\neg(P \wedge Q)$
V	V	F	F	V	F
V	F	F	V	F	V
F	V	V	F	F	V
F	F	V	V	F	V

Un altro esempio delle leggi di De Morgan è:

$$\neg(P \vee Q) \equiv (\neg P) \wedge (\neg Q)$$

Tavola di verità:

P	Q	$\neg P$	$\neg Q$	$P \vee Q$	$\neg(P \vee Q)$
V	V	F	F	V	F
V	F	F	V	V	F
F	V	V	F	V	F
F	F	V	V	F	V

Esempio 1.4. Usare le leggi di De Morgan per scrivere la negazione di:

$$-1 < x < 4$$

Questa espressione è equivalente alla forma logica:

$$P = (x < 4) \quad \wedge \quad Q = (x > -1)$$

La negazione può essere descritta come:

$$\neg(P \wedge Q) \equiv \neg(x < 4) \vee \neg(x > -1)$$

Applicando le leggi di De Morgan:

$$\neg(x > -1) \vee \neg(x < 4)$$

che diventa:

$$(x \leq -1) \vee (x \geq 4)$$

Quindi, la negazione della disuguaglianza originale è:

$$x \leq -1 \vee x \geq 4$$

1.5 Implicazione

Il ragionamento ipotetico implica il reale al possibile. Quando si fa un inferenza logica o una deduzione, si ragiona a partire dall'ipotesi per arrivare a una conclusione, l'obbiettivo è essere in grado di affermare, se si conosce un certo fatto, allora deve essere vero qualcos'altro. Siano P e Q enunciati. Una proposizione se P allora Q è indicata con:

$$P \implies Q$$

P è detta ipotesi, e Q conclusione. Una proposizione è detta condizionale perché la verità del predicato Q dipende da P. La notazione $P \implies Q$ indica che $\implies$ è un connettivo logico. Che può essere utilizzato per unire enunciati e creare nuovi enunciati.

Esempio 1.5. Supponiamo che tu vada a fare un colloquio di lavoro in un negozio e il proprietario ti faccia la seguente promessa:

"Se ti presenti al lavoro lunedì mattina, allora sarai assunto."

In quale circostanza si può dire che il datore di lavoro ha mentito?

Il datore di lavoro mente se ti presenti al lavoro lunedì e non vieni assunto.

L'esempio serve a dimostrare che l'unica combinazione di circostanze in cui una proposizione condizionale può essere considerata falsa è quando l'ipotesi è vera e la conclusione è falsa. In tutti gli altri casi, l'enunciato è vero.

Tavola di verità:

P	Q	$P \implies Q$
V	V	V
V	F	F
F	V	V
F	F	V

Esempio 1.6. Consideriamo la proposizione:

$$\neg(P \wedge Q) \vee (P \implies Q) \equiv \neg(P \vee Q)$$

P	Q	$\neg Q$	$\neg P \vee Q$	$P \to Q$	$\neg P \vee (P \to Q)$
V	V	F	V	V	V
V	F	V	F	F	F
F	V	F	V	V	V
F	F	V	V	V	V

Esempio 1.7. Consideriamo la proposizione:

$$\neg(P \wedge Q) \vee (P \implies Q) \equiv \neg(P \vee Q)$$

P	Q	$\neg P$	$P \implies Q$	$\neg P \vee Q$
V	V	F	V	V
V	F	F	F	F
F	V	V	V	V
F	F	V	V	V

Modus Ponens

Il Modus Ponens è una forma di ragionamento che si basa sulla seguente struttura logica:

$$P \implies Q$$

Se P è vero e $P \implies Q$ è vero, allora Q deve essere vero. La dimostrazione di un teorema spesso utilizza una catena di deduzioni simili:

$$P_0 \implies P_1 \implies P_2 \implies \cdots \implies P_m = P$$

dove P_0 è un'assioma o postulato.

Forma Contrappositiva

La forma contrappositiva di una proposizione $P \to Q$ è data da:

$$\neg Q \to \neg P$$

Questa forma è logicamente equivalente all'originale $P \to Q$.

Esempio 1.8. P : "Se oggi è Pasqua" Q : "Domani è lunedì"

$\neg Q \to \neg P$: "Se domani non è lunedì, allora oggi non è Pasqua."

1.6 Doppia implicazione

Dire "P se e solo se Q" significa che P è vero se e solo se Q è vero, cioè se P e Q hanno lo stesso valore di verità. L'affermazione può dirsi vera solo se si verifica $P \iff Q$ e $Q \iff P$, cioè quando si verificano entrambi.

Definizione 1.10:

Date due variabili di enunciato P e Q, il bicondizionale $P \leftrightarrow Q$ è vero se e solo se P e Q hanno lo stesso valore di verità, ed è falso quando P e Q hanno valori di verità opposti.

P	Q	$P \iff Q$
V	V	V
V	F	F
F	V	F
F	F	V

Esempio 1.9. Consideriamo l'enunciato: *"John batterà il record mondiale dei 100 metri in meno di 9 secondi."*

(negazione): Se John non batte il record mondiale in meno di 9 secondi, allora non avrà corso in meno di 9 secondi.

(contropositiva): Se John batterà il record mondiale, allora avrà corso in meno di 9 secondi.

P	Q	$\neg P$	$P \implies Q$	$Q \implies P$	$(P \implies Q) \wedge (Q \implies P)$
V	V	F	V	V	V
V	F	F	F	V	F
F	V	V	V	F	F
F	F	V	V	V	V

Questo mostra che $P \implies Q$ è logicamente equivalente a $\neg P \implies \neg Q$.

Esempio 1.10. dimostrare che un numero naturale è un multiplo di 12 se e solo se esso è un multiplo di 3 e un multiplo di 4.

Dimostrazione 1.2. La dimostrazione è divisa in due parti:
$\big(\implies\big)$ se n è un multiplo di 12 allora $n = 12m$. Poiché:

$$12 = 3 \cdot 4 = 4 \cdot 3 \text{ abbiamo:}$$

$$n = 3 \cdot \big(4m\big) \quad \text{e} \quad n = 4 \cdot \big(3m\big)$$

cioè n è un multiplo sia di 3 che di 4.

$\big(\impliedby\big)$ Supponiamo che $n = 3r$ e $n = 4s$ e dimostriamo che $n = 12t$. Da $3r = 4s$ abbiamo che $4s$ è un multiplo di 3, ma 4 non è un multiplo di3, quindi s deve essere un multiplo di 3, cioè $s = 3t$. Ora abbiamo:

$$n = 4s = 4 \cdot \big(3t\big) = 12t$$

Cioè n è un multiplo di 12. □

1.7 Quantificatori

In logica esistono due quantificatori principali:

- $\forall$ - Per ogni (quantificatore universale)
- $\exists$ - Esiste (quantificatore esistenziale)

Un modo per trasformare i predicati in enunciati è esprimere se una certa proprietà è vera per elementi specifici o per tutti gli elementi di un dominio.

Quantificatore universale $\forall$

Sia $P(x)$ un predicato e D il dominio di x. Un enunciato universale ha la forma:

$$\forall x \in D, P(x)$$

ed è definito vero se, e solo se, $P(x)$ è vero per ogni x appartenente al dominio D. È falso se esiste almeno un x per cui $P(x)$ è falso.

Un valore di x per cui $P(x)$ è falso è chiamato controesempio per l'enunciato universale.

Quantificatore esistenziale: L'enunciato esistenziale ha la forma:

$$\exists x \in D, P(x)$$

ed è definito vero se esiste almeno un x per cui $P(x)$ è vero. È falso se $P(x)$ è falso per tutti gli elementi del dominio D.

Esempio 1.11. Sia $D = \mathbb{N}$, dimostrare che:

$$\forall x \in D, P(x)$$

è vero se, e solo se, $P(x)$ è vero per ogni x nel dominio D.

Congettura di Goldbach: ogni numero naturale pari maggiore di 2 è la somma di due numeri primi. Questo è un esempio di una proposizione espressa con un quantificatore universale:

$$\forall x \in \mathbb{N}, P(x) = x \text{ è la somma di due numeri primi.}$$

Esempio 1.12. Supponiamo che D sia l'insieme degli studenti che hanno sostenuto l'esame di matematica discreta. Definiamo $P(x)$ come "superare l'esame". L'enunciato:

$$\forall x \in D, P(x)$$

significa che tutti gli studenti hanno superato l'esame.

Controesempio: Se esiste uno studente x che non ha superato l'esame, l'enunciato universale sarebbe falso, e potremmo scrivere:

$$\exists x \in D, \neg P(x)$$

per indicare l'esistenza di almeno un controesempio

Il quantificatore esistenziale ($\exists$)

Il simbolo $\exists$ rappresenta "esiste" ed è chiamato quantificatore esistenziale. Ad esempio, la frase:

"C'è uno studente iscritto al corso di Matematica Discreta"

si esprime formalmente come:

$\exists P \in E$ tale che P è uno studente iscritto al corso di Matematica Discreta.

Definizione 1.11:

Sia $P(x)$ un predicato e D il dominio di x. Un enunciato esistenziale ha la forma:

$$\exists x \in D, P(x)$$

ed è definito vero se esiste almeno un $x \in D$ per cui $P(x)$ è vero. È falso se $P(x)$ è falso per ogni $x \in D$.

Esempio 1.13. Alcuni studenti superano l'esame. Sia $P(x)$ = "superare l'esame" e D = "l'insieme degli studenti". L'enunciato esistenziale si scrive:

$$\exists x \in D, P(x)$$

La negazione dell'enunciato esistenziale è:

$$\neg(\exists x \in D, P(x)) \equiv \forall x \in D, \neg P(x)$$

che significa "non esiste uno studente che ha superato l'esame".

Esempio 1.14. Sia D = "l'insieme dei programmi". Sia $P(x)$ = "termina". L'enunciato universale si scrive:

$$\forall x \in D, P(x)$$

La sua negazione è:

$$\exists x \in D, \neg P(x)$$

che significa "esiste un programma che non termina".

Tautologia: Una tautologia è una proposizione che è sempre vera, indipendentemente dai valori di verità delle proposizioni che la compongono.

P	$\neg P$	$P \vee \neg P$
V	F	V
F	V	V

Contraddizione: Una contraddizione è una proposizione che è sempre falsa, indipendentemente dai valori di verità delle proposizioni che la compongono.

P	$\neg P$	$P \wedge \neg P$
V	F	F
F	V	F

Definizione 1.12:

Una formula logica F è detta **soddisfacibile** se esiste almeno un'assegnazione dei valori di verità alle variabili che rende vera la formula. Formalmente, F è soddisfacibile se esiste un'interpretazione I tale che:

$$I(F) = \text{Vero}$$

In altre parole, esiste almeno una configurazione dei valori di verità delle variabili tale che l'enunciato risulta vero.
Se non esiste alcuna assegnazione che renda la formula vera, essa è detta **insoddisfacibile**.

Esempio 1.15. Consideriamo la formula $F = P \vee Q$. La formula è soddisfacibile perché ci sono assegnazioni che la rendono vera.

Tavola di verità:

P	Q	$P \vee Q$
V	V	V
V	F	V
F	V	V
F	F	F

La formula $F = P \vee Q$ è soddisfacibile poiché ci sono assegnazioni ($P = V$, $Q = V$) che rendono la formula vera.

Esempio 1.16. Esempio di formula insoddisfacibile:

Consideriamo ora la formula $F = P \wedge \neg P$. Questa formula è insoddisfacibile, poiché non esiste alcuna assegnazione che la renda vera.

Tavola di verità:

P	$\neg P$	$P \wedge \neg P$
V	F	F
F	V	F

In questo caso, la formula $F = P \wedge \neg P$ è insoddisfacibile poiché per entrambe le assegnazioni di P, la formula risulta sempre falsa.

Capitolo 2

Insiemi

2.1 Insiemi

Definizione 2.1:

Un insieme e è una collezione non ordinata di elementi distinti. Le entità che compongono un insieme sono dette i suoi elementi. Diciamo che gli elementi appartengono all'insieme, e che quest'ultimo contiene i suoi elementi.

2.1.1 Rappresentazione degli insiemi

insiemi finiti

Un'insieme finito può essere rappresentato elencando esplicitamente i suoi elementi, racchiusi tra parentisi graffe.

Esempi:

- $X = \{0, 1, 2, 3\}$
- $Y = \{a, b, c, d\}$
- $Z = \{\sqrt{x}, \pi, e\}$
- $A = \{\text{rosso},\ \text{giallo},\ \text{blu},\ \text{viola}\}$

Insiemi infiniti o con un elevato numero di elementi

Un insieme può essere rappresentato anche specificando una proprietà $P(x)$ che risulta vera per ogni elemento dell'insieme e falsa per ogni altro elemento possibile.

Inoltre è possibile definire l'insieme degli elementi x del dominio D che soddisfano $P(x)$ nel seguente modo:

$$\{x \in D \mid P(x) \text{ è vero}\}$$

Se il dominio è evidente dal contesto si può omettere D:

$$\{x \mid P(x)\}$$

Esempi di insiemi infiniti:

- W consiste di tutti i numeri naturali n tale che n è un multiplo di 11:

$$W = \{n \in \mathbb{N} \mid n \text{ è un multiplo di } 11\}$$

- S denota l'insieme dei multipli non negativi di 3.

$$S = \{3x \mid x \in \mathbb{N}\}$$

Alcuni esempi di insiemi infiniti:

- Insieme dei numeri naturali $\mathbb{N} = \{0, 1, 2, 3 \ldots\}$
- Insieme dei numeri interi $\mathbb{Z} = \{\ldots -3, -2, -1, 0, 1, 2, 3, \ldots\}$
- Insieme dei numeri razionali $\mathbb{Q} = \{\ldots -\frac{1}{4}, -\frac{1}{3}, -\frac{1}{2}, \frac{1}{2}, \frac{1}{3}, \frac{1}{4}, \frac{2}{2}, \ldots\}$
- Insieme dei numeri reali $\mathbb{R} = \{\sqrt{3}, \pi, e \ldots\}$

Notazioni:
Se $\mathbb{X}$ è uno degli insiemi sopracitati, si indica con:

- $\mathbb{X}^+$ l'insieme formato dagli elementi positivi di $\mathbb{X}$.
- $\mathbb{X}^-$ l'insieme formato dagli elementi negativi di $\mathbb{X}$.
- $\mathbb{X}^{\geq}$ l'insieme formato dagli elementi non negativi di $\mathbb{X}$, per esempio:

$$\mathbb{Z}^{\geq} = \mathbb{N} \quad \mathbb{Z}^- = \{-3, -2, -1 \ldots\}$$

2.2 Appartenenza

Se X è un insieme, la notazione $x \in X$ significa che x è un elemento di X. La notazione $x \notin X$ significa che x non è un elemento di X. Il simbolo di appartenenza mette in relazione un elemento con un insieme.

$$X = \{0, 1, 2, 3\}, \quad 3 \in X, \quad \{3\} \notin X$$

2.3 Cardinalità degli insiemi

La **cardinalità di un insieme** è una misura che indica il numero di elementi presenti nell'insieme. La cardinalità di un insieme X viene denotata con $|X|$, e rappresenta quanti elementi appartengono all'insieme.

Tipi di cardinalità:

- Un insieme ha **cardinalità finita** se il numero di elementi dell'insieme è un numero intero positivo.
- Un insieme ha **cardinalità infinita** se contiene un numero infinito di elementi.

Esempio di cardinalità finita:

$$X = \{0, 1, 2, 3\}, \quad |X| = 4$$

Esempio di cardinalità infinita:

$$|\mathbb{N}| = \infty, \quad \mathbb{N} = \{0, 1, 2, 3, \ldots\}$$

2.4 Prodotto cartesiano

Definizione 2.2:

Dato un insieme A e un insieme B, il **prodotto cartesiano** $A \times B$ è l'insieme di tutte le coppie ordinate (a, b), dove $a \in A$ e $b \in B$. Formalmente:

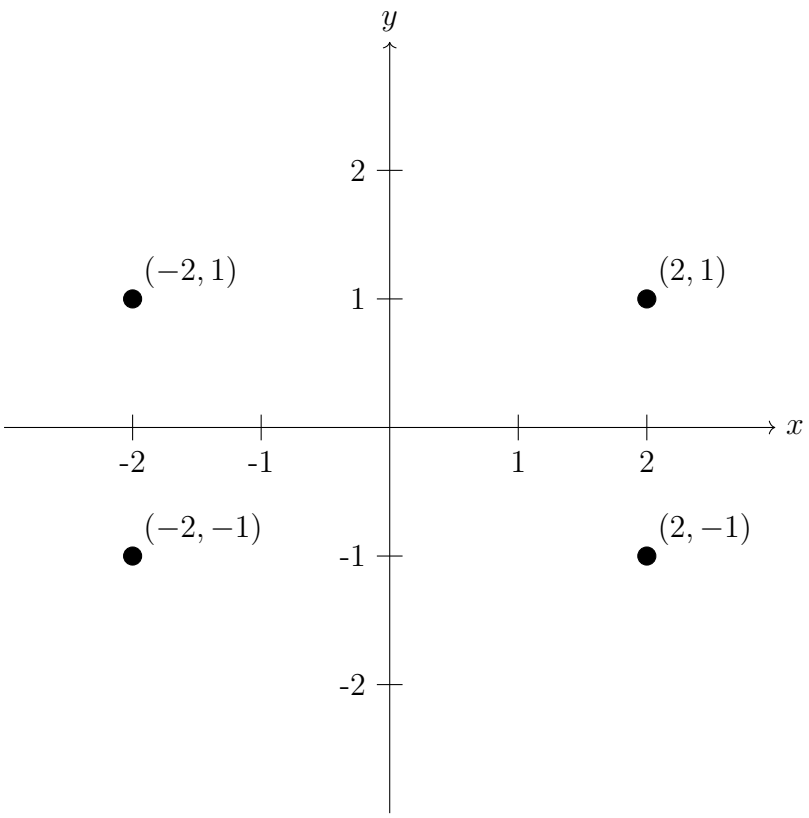
$$A \times B = \{(a, b) \mid a \in A, b \in B\}$$

La cardinalità del prodotto cartesiano è data da:

$$|A \times B| = |A| \times |B|$$

Esempio:

$$\mathbb{R} \times \mathbb{R} = \mathbb{R}^2, \quad |\mathbb{R} \times \mathbb{R}| = |\mathbb{R}^2|$$



Il **prodotto cartesiano** di n insiemi è dato da:

$$A_1 \times A_2 \times \cdots \times A_m = \{(a_1, \ldots, a_m) \mid a_i \in A_i, \text{ per ogni } i = 1, \ldots, m\}$$

$$\prod_{i=1}^{m} A_i$$

La cardinalità del prodotto cartesiano è:

$$|A^m| = |A|^m$$

2.5 Insieme vuoto

Definizione 2.3:

Un insieme vuoto è un insieme che non contiene alcun elemento. Viene denotato con il simbolo $\emptyset$ e la sua cardinalità è 0, poiché non ci sono elementi al suo interno. Formalmente, l'insieme vuoto è definito come l'unico insieme tale che:

$$\forall x \ (x \notin \emptyset)$$

2.6 Sottoinsiemi:

Definizione 2.4:

Un insieme A è un sottoinsieme di un insieme B se e solo se ogni elemento di A è anche un elemento di B. Si denota con:

$$A \subseteq B$$

Ciò rappresenta una relazione tra due insiemi. Formalmente, si ha $A \subseteq B$ se:

$$\forall x \ (x \in A \implies x \in B)$$

Esempio 2.1. Dato l'insieme $A = \{2, 4\}$ e l'insieme $B = \{0, 1, 2, 4\}$, possiamo scrivere:

$$A \subseteq B$$

Equivalenza tra insiemi

Dati insiemi A e B, $A = B$ se e solo se ogni elemento di A è contenuto in B e ogni elemento di B è contenuto in A. Formalmente:

$$A = B \iff A \subseteq B \land B \subseteq A$$

Per dimostrare che $A \subseteq B$, è necessario dimostrare che per ogni elemento $x \in A$, si ha $x \in B$.

Per la confutazione di $A \subseteq B$, è necessario dimostrare che almeno un elemento $x \in A$ non appartiene a B.

Sia $A = \{m \in \mathbb{Z} : m = 6n + 12, n \in \mathbb{Z}\} = \{0, 18, 24, 30, \dots\}$.

Sia $B = \{m \in \mathbb{Z} : m = 3h, h \in \mathbb{Z}\} = \{0, 3, 6, 9, \dots\}$.

Dimostrazione 2.1. Per ogni x, se $x \in A \Rightarrow x \in B$. Sia un generico elemento di A, allora $x = 6n + 12$.

Dimostriamo che x è un generico elemento di B: $x = 6n + 12 \Leftrightarrow x = 3(2n + 4)$, che è multiplo di 3, quindi $x \in B$. Poiché $x \in \mathbb{Z}$, allora x è elemento di B.

□

Per confutare un enunciato è sufficiente produrre un controesempio.

Siano dati $B = \{x \in \mathbb{N} \mid 3x\}$ e $A = \mathbb{Z}$.

$B \subseteq A$? In questo caso, osservando i due insiemi, è facile notare che $B \subseteq A$, quindi produco un controesempio:

Per esempio, $x = 3 \in B$ poiché $x = 3 \cdot 1$ come si osserva, ma $x \notin A$ poiché non esiste alcun numero intero tale che $3 = 6n + 12$. Infatti, $6n + 12 = 3 \Rightarrow n = \frac{-3}{2} \notin \mathbb{Z}$.

2.7 Insieme delle parti

Definizione 2.5:

L'insieme delle parti di un insieme A, indicato come $\wp(A)$, è l'insieme che contiene tutti i sottoinsiemi possibili di A incluso l'insieme vuoto e l'insieme stesso.

Formalmente:

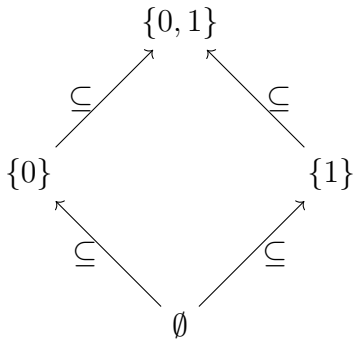
$$\wp(A) = \{B \mid B \subseteq A\}$$

dove B rappresenta l'insieme delle parti di A.

Esempio 2.2. sia $A = \{0, 1\}$ si scriva l'insieme delle parti di A.

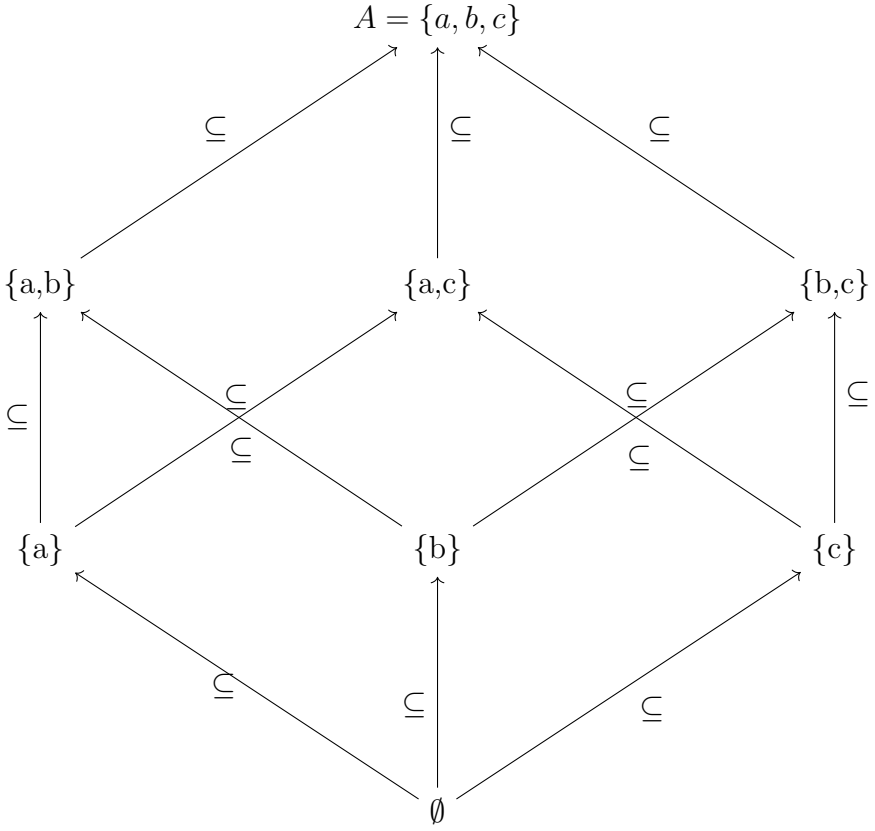
$$\wp(A) = \{\emptyset, \{0\}, \{1\}, \{0, 1\}\}$$

$\wp(A)$ è un insieme parzialmente ordinato dalla relazione $\subseteq$.



Esempio 2.3. Sia $B = \{a, b, c\}$, allora l'insieme delle parti di B è:

$$\mathcal{P}(B) = \{\emptyset, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a, b, c\}\}$$



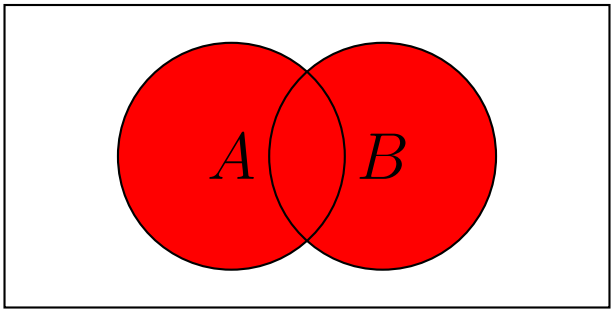
In generale, se $|A| = n$, allora $|\wp(A)| = 2^n$.

2.8 Operazioni tra insiemi

2.8.1 Unione

L'unione tra A e B, indicata con $A \cup B$, è l'insieme di tutti gli elementi che si trovano in almeno uno tra gli insiemi A o B. Formalmente:

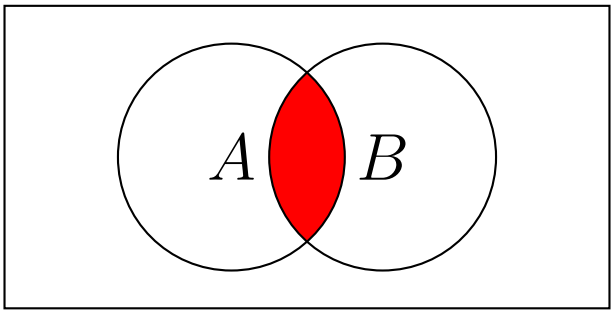
$$A \cup B = \{x \in U \mid x \in A \vee x \in B\}$$



2.8.2 Intersezione:

L'intersezione tra l'insieme A e l'insieme B, indicata con $A \cap B$, è l'insieme degli elementi che appartengono sia ad A che a B. Formalmente:

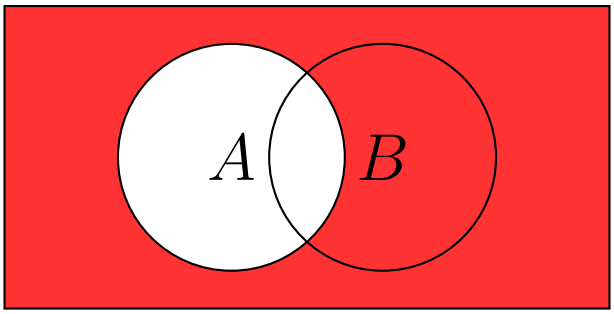
$$A \cap B = \{x \in U \mid x \in A \wedge \ x \in B\}$$



2.8.3 Differenza:

La differenza tra B e A, indicata con $B \setminus A$, è l'insieme degli elementi che appartengono a B ma non appartengono ad A. Formalmente:

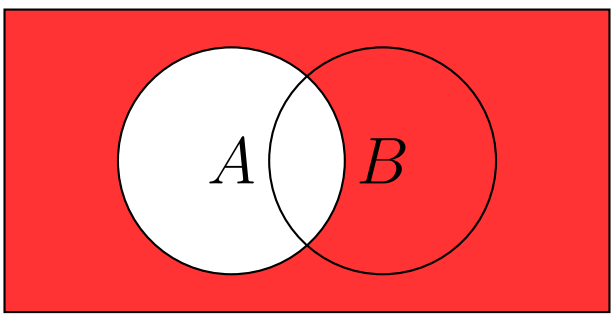
$$B \setminus A = \{x \in U \mid x \in B \wedge \ x \notin A\}$$



2.8.4 Complementare

Il complementare di un insieme A, indicato con $\overline{A}$, è l'insieme degli elementi che appartengono all'universo U, ma che non appartengono ad A.

$$\overline{A} = \{x \in U \mid x \notin A\}$$



2.8.5 Differenza simmetrica

Definizione 2.6:

La differenza tra due insiemi A e B, indicata come $A\Delta B$, è l'insieme degli elementi che appartengono a uno solo dei due insiemi, ma non ad entrambi. Formalmente, la differenza simmetrica tra A e B è data da:

$$A\Delta B = (A \setminus B) \cup (B \setminus A)$$

Dove:

- $A \setminus B$ è la differenza tra A e B, ossia l'insieme degli elementi che appartengono ad A, ma non a B.
- $B \setminus A$ è la differenza tra B e A, ossia l'insieme degli elementi che appartengono a B, ma non ad A.

L'unione di queste due differenze rappresenta la differenza simmetrica.

Proprietà delle operazioni insiemistiche

Proprietà associativa:

$$(A \cup B) \cup C = A \cup (B \cup C) = A \cup B \cup C$$

$$(A \cap B) \cap C = (B \cap C) \cap A = A \cap B \cap C$$

Proprietà distributiva:

$$A \cap (B \cup C) = (A \cap B) \cup (B \cap C)$$

$$A \cup (B \cap C) = (A \cup B) \cap (B \cup C)$$

Proprietà del complementare:

$$A \cup \overline{A} = X \quad \text{(Universo)}$$

$$A \cap \overline{A} = \emptyset$$

Leggi di De Morgan:

$$\overline{A \cup B} = \overline{A} \cap \overline{B}$$

$$\overline{A \cap B} = \overline{A} \cup \overline{B}$$

2.9 Partizioni

Nella teoria degli insiemi, una partizione è un modo per dividere un insieme in sottoinsiemi disgiunti, cioè che non si sovrappongono, in modo che ogni elemento dell'insieme originale appartenga esattamente a uno dei sottoinsiemi.

Definizione 2.7:

Due insiemi si dicono disgiunti se e solo se non hanno alcun elemento in comune.

$$A \cap B = \emptyset$$

Esempio 2.4. Sia $A = \{1, 3, 5\}$ e $B = \{2, 4, 6\}$. Gli insiemi A e B sono disgiunti?

$$A \cap B = \{1, 3, 5\} \cap \{2, 4, 6\} = \emptyset$$

Insiemi mutuamente disgiunti

Gli insiemi $A_1, A_2, \ldots, A_m$ sono mutuamente disgiunti se e solo se, presi due insiemi qualunque A_i e A_j, con $i \neq j$, non hanno elementi in comune. Formalmente:

$$A_i \cap A_j = \emptyset \quad \text{quando } i \neq j$$

Definizione 2.8:

Una **partizione** di un insieme A è una suddivisione di A in sottoinsiemi non vuoti e disgiunti, tali che l'unione di questi sottoinsiemi costituisca l'intero insieme A. In altre parole, una partizione divide l'insieme A in pezzi che non si sovrappongono e che contengono tutti gli elementi di A.

Formalmente, una collezione di sottoinsiemi $\{A_1, A_2, A_3, \ldots, A_m\}$ è una partizione di A se soddisfa le seguenti condizioni:

1. $A_1 \cup A_2 \cup A_3 \cup \cdots \cup A_m = A$
2. $A_i \cap A_j = \emptyset$ per $i \neq j$
3. Nessun sottoinsieme A_i è vuoto

2.10 Unioni e Intersezioni di una collezione infinita di insiemi

Siano $A_0, A_1, A_2, \ldots$ insiemi che sono sottoinsiemi di un insieme universale U, e dato un numero intero non negativo n, possiamo definire le seguenti operazioni di unione e intersezione di una collezione indicizzata di insiemi.

Unione finita e infinita

- La **unione finita** di una collezione di insiemi $A_0, A_1, A_2, \ldots, A_n$ è l'insieme degli elementi di U che appartengono ad almeno uno degli insiemi A_i per $i = 0, 1, 2, \ldots, n$:

$$\bigcup_{i=0}^{n} A_i = \{x \in U \mid x \in A_i \text{ per almeno un intero non negativo } i\}.$$

- La **unione infinita** di una collezione di insiemi $A_0, A_1, A_2, \ldots$ è l'insieme degli elementi di U che appartengono ad almeno uno degli insiemi A_i per $i = 0, 1, 2, \ldots, \infty$:

$$\bigcup_{i=0}^{\infty} A_i = \{x \in U \mid x \in A_i \text{ per almeno un intero non negativo } i\}.$$

Intersezione finita e infinita

- L'**intersezione finita** di una collezione di insiemi $A_0, A_1, A_2, \ldots, A_n$ è l'insieme degli elementi di U che appartengono a tutti gli insiemi A_i per $i = 0, 1, 2, \ldots, n$:

$$\bigcap_{i=0}^{n} A_i = \{x \in U \mid x \in A_i \text{ per tutti } i = 0, 1, 2, \ldots, n\}.$$

- L'**intersezione infinita** di una collezione di insiemi $A_0, A_1, A_2, \ldots$ è l'insieme degli elementi di U che appartengono a tutti gli insiemi A_i per $i = 0, 1, 2, \ldots, \infty$:

$$\bigcap_{i=0}^{\infty} A_i = \{x \in U \mid x \in A_i \text{ per tutti gli interi non negativi } i\}.$$

Le operazioni di unione e intersezione indicizzate permettono di generalizzare la nozione di unione e intersezione a collezioni di insiemi che possono essere finite o infinite. Nel contesto di una **unione**, l'elemento appartiene all'insieme risultante se esiste almeno un sottoinsieme della collezione che contiene l'elemento. Nel caso dell' **intersezione**, l'elemento deve appartenere a tutti i sottoinsiemi della collezione affinché appartenga all'intersezione stessa.

Questa distinzione è cruciale in teoria degli insiemi e in molte aree della matematica, poiché permette di lavorare con collezioni infinite, che sono comuni in analisi matematica, algebra e teoria delle probabilità. Le unioni e le intersezioni infinite sono strumenti essenziali per descrivere limiti e comportamenti asintotici di sequenze di insiemi, con applicazioni dirette anche in teoria della misura e topologia.

Capitolo 3

Relazioni

3.1 Relazioni

Definizione 3.1:

Siano A e B 2 insiemi, si considerano le seguenti relazioni espresse in termini di coppie (x, y) con $x \in A$ e $y \in B$.

Esempio 3.1. Sia $A = B$ un insieme di persone

$$\{(x, y) \mid x \text{ è padre di } y\}$$

$$\{(x, y) \mid x \text{ è amico di } y\}$$

esempio Sia $A = B = \mathbb{Z}$

$$\big\{(x, y) \mid x < y\big\}$$

3.1.1 Relazione binaria

Definizione 3.2:

Una relazione binaria $\mathcal{R}$ tra A e B è un sottoinsieme del prodotto cartesiano, cioè:

$$\mathcal{R} \subseteq A \times B = \{\big(a, b\big) \mid x \in A \land y \in B\}$$

- L'insieme A è detto dominio della relazione.
- L'insieme B è detto codominio della relazione.

In generale una relazione binaria è definita da un predicato P in 2 variabili. A ogni relazione corrisponde un sottoinsieme, ovvero per ogni $R \subseteq A \times B$ esiste un predicato tale che R è l'insieme di coppie che soddisfano il predicato.

Esempio 3.2. Sia $A = \mathbb{Z}$

$$<\subseteq \mathbb{Z}^2 = \mathbb{Z} \times \mathbb{Z}$$

$$<= \{(x, y) \mid x, y \in \mathbb{Z} \land x < y\}$$

$$2 < 3$$

3.1.2 Relazione n-aria

Definizione 3.3:

Siano $A_1, A_2..... \times A_n$. Una relazione n-aria R tra $A_1, A2.... \times A_n$ è un sottoinsieme del prodotto cartesiano $A_1 \times A_2 \times ...A_n$, cioè:

$$\mathcal{R} \subseteq A_1 \times A_2 \times \ldots \times A_n$$

Esempio 3.3. Siano $A_1 = A_2 = A_3 = \mathbb{Z}$

$$\mathcal{R} = \{(x, y, z) \mid x, y, z \in \mathbb{Z} \wedge x + y = z\}$$

Ad esempio: $(2, 3, 5) \in R$ mentre $(1, 2, 4) \notin \mathcal{R}$

3.1.3 Proprietà delle relazioni

Definizione 3.4:

Siano A un inseme e $\mathcal{R} \subseteq A \times A = A^2$ Diciamo che una relazione è:

Proprietà riflessiva

Definizione 3.5:

La proprietà riflessiva in una relazione binaria indica che ogni elemento è in relazione con se stesso.

$$x\mathcal{R}x \ \forall x \in A$$

Esempio 3.4. $\{(x, y) \mid x \leq x\}$ La proprietà riflessiva è soddisfatta poiché un numero può essere minore uguale a se stesso, se al posto di minore uguale la proprietà era definita con minore stretto non era riflessiva siccome un numero non può mai essere minore a se stesso.

Proprietà irriflessiva

Definizione 3.6:

Un insieme è considerato irriflessivo rispetto ad una relazione se nessun elemento di quell'insieme è in relazione con se stesso.

$$\neg(x\mathcal{R}x) \ \forall x \in A$$

Esempio 3.5. $\{(x, y) \mid x < y\}$ La proprietà irriflessiva è soddisfatta poiché un numero non può mai essere minore a se stesso.

Proprietà Simmetrica

Definizione 3.7:

Una relazione è simmetrica se il cambio dell'ordine delle coppie ordinate non cambia la relazione.

$$x\mathcal{R}y \implies x\mathcal{R}y \ \forall x, y \in A$$

Esempio 3.6. $\{(x, y) \mid x \cdot y = 100\}$

La proprietà è simmetrica per la proprietà commutativa della moltiplicazione poiché se $x \cdot y = 100$ allora anche $y \cdot x = 100 \ \forall x, y \in A$

Proprietà Antisimmetrica

Definizione 3.8:

Una relazione è detta antisimmetrica se per ogni coppia di elementi x, y è verificata la seguente condizione:

$$x\mathcal{R}y \implies \neg\big(y\mathcal{R}x\big) \ \forall x \neq y \in A$$

$$x\mathcal{R}y \wedge y\mathcal{R}x \implies x = y \ \forall x, y \in A$$

Osservazione

Le due definizioni sono equivalenti: entrambe esprimono la proprietà fondamentale dell'antisimmetria. In altre parole, se due elementi distinti x e y sono in relazione reciproca, ciò non è possibile nella relazione antisimmetrica, o deve valere che $x = y$. La prima formulazione esprime che se x è in relazione con y, allora y non può essere in relazione con x, per $x \neq y$. La seconda formulazione afferma che se entrambi x e y sono in relazione reciproca, allora devono essere uguali.

Esempio 3.7. $\{(x, y) \mid x \leq y\}$

La proprietà simmetrica, supponiamo che:

$$x = 1 \text{ e } y = 2$$

Non è possibile che: $1 \leq 2$ e $2 \leq 1$.

Proprietà transitiva

Definizione 3.9:

Una relazione è transitiva se, quando 2 elementi sono in relazione e un secondo elemento è in relazione con il terzo.

$$xRy \ \wedge \ yRz \implies xRz$$

Esempio 3.8. $\{(x, y) \mid x < y\}$ Supponiamo che $x = 1$, $y = 2$ e $z = 3$, allora la proprietà transitiva è verificata, dimostro che la proprietà è soddisfatta:

$$\text{Se } 2 < 3 \text{ e } 3 < 5 \text{ allora } 2 < 5$$

Esempio 3.9. Sia $\mathcal{R}$ una relazione definita sull'insieme $\mathbb{Z} \times \mathbb{Z}$. La relazione $\mathcal{R} \subseteq \mathbb{Z} \times \mathbb{Z}$ è definita come:

$$\forall (x, y) \in \mathbb{Z} \times \mathbb{Z}, \quad x \mathcal{R} y \iff x < y$$

a. $57 \mathcal{R} 53$? non sono in relazione poiché $57 \not< 53$.

b. $-17 \mathcal{R} -14$? sono in relazione poiché $-17 < -14$.

c. $143 \mathcal{R} 143$? non sono in relazione poiché $143 \not< 143$.

d. $-35 \mathcal{R} 1$?sono in relazione poiché $-35 < 1$.

Esempio 3.10. Dimostrare che se n è un numero intero dispari allora $1 \mathcal{R} n$ è pari e la funzione è definita come segue:

$$1 \mathcal{R} n \iff 1 - n \; \forall n \in \mathbb{Z}$$

Dimostrazione 3.1. Sia n un numero dispari allora $n = 2k+1$ per qualche numero intero $k \in \mathbb{Z}$. Ora per definizione di $\mathcal{R}$, $1 \mathcal{R} n \iff 1 - \big(2k + 1\big) = 1 - 2k - 1 = -2k$ che è sempre un numero pari quindi abbiamo dimostrato che ogni numero intero dispari sta in relazione con 1. □

Definizione 3.10:

Sia $\mathcal{R}$ una relazione binaria tra A e B, cioè $\mathcal{R} \subseteq A \times B$. La relazione inversa $\mathcal{R}^{-1}$ tra B e A è definita come:

$$\mathcal{R}^{-1} = \{(y, x) \in B \times A \mid (x, y) \in \mathcal{R}\}$$

Esempio 3.11. Sia $A = \{2, 3, 4\}$ e $A = \{2, 6, 8\}$,e $\mathcal{R}$ sia la relazione:

$$x \mathcal{R} y \iff x \mid y \forall \big(x, y\big) \in A \times B$$

a. Indicare esplicitamente quali coppie ordinate appartengono a $\mathcal{R}$ e $\mathcal{R}^{-1}$, e disegnare i diagrammi a frecce per $\mathcal{R}$ e $\mathcal{R}^{-1}$.

- $\mathcal{R} = \{(2, 2), (2, 6), (2, 8), (3, 6), (4, 8)\}$
- $\mathcal{R}^{-1} = \{(2, 2), (6, 2), (8, 2), (6, 3), (8, 4)\}$

b. Descrivere la relazione $\mathcal{R}^{-1}$ in parole.

a. $\mathcal{R}$ contiene le seguenti coppie ordinate: $(2, 2)$, $(2, 6)$, $(2, 8)$, $(3, 6)$, $(4, 8)$. La relazione inversa $\mathcal{R}^{-1}$ contiene le coppie ordinate: $(2, 2)$, $(6, 2)$, $(8, 2)$, $(6, 3)$, $(8, 4)$.

b. La relazione $\mathcal{R}^{-1}$ si ottiene invertendo l'ordine delle coppie della relazione originale $\mathcal{R}$. In altre parole, se (x, y) appartiene a $\mathcal{R}$, allora (y, x) appartiene a $\mathcal{R}^{-1}$.

Diagramma per la relazione R

Esempio 3.12. Sia $A = \{0, 1, 2, 3\}$ e siano definite le relazioni R, S e T su A come segue:

$$R = \{(0,0), (0,1), (0,3), (1,0), (1,1), (2,2), (3,0), (3,3)\}$$
$$S = \{(0,0), (0,2), (0,3), (2,3)\}$$
$$T = \{(0,1), (2,3)\}$$

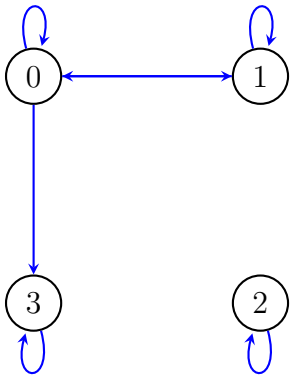
a. R è riflessiva? simmetrica? transitiva?

b. S è riflessiva? simmetrica? transitiva?

c. T è riflessiva? simmetrica? transitiva?

Soluzione

a. Il grafo orientato di R ha l'aspetto mostrato di seguito.

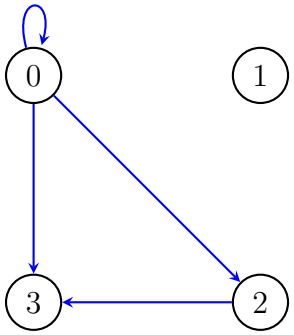


R **è riflessiva**: Ogni punto del grafo diretto ha un ciclo su sé stesso. Questo significa che ogni elemento di A è in relazione con sé stesso, quindi R è riflessiva.

R **è simmetrica**: In ogni caso in cui c'è una freccia da un punto del grafo a un altro, c'è anche una freccia che va dal secondo punto al primo. Questo significa che, ogni volta che un elemento di A è in relazione con un altro tramite R, anche il secondo è in relazione con il primo. Di conseguenza, R è simmetrica.

R **non è transitiva**: C'è una freccia che va da 1 a 0 e una freccia che va da 0 a 3, ma non c'è una freccia che va da 1 a 3. Questo significa che ci sono elementi di A — 0, 1, e 3 — tali che $1\mathcal{R}0$ e $0\mathcal{R}3$, ma non $1\mathcal{R}3$. Di conseguenza, R non è transitiva.

b. S è riflessiva? simmetrica? transitiva?



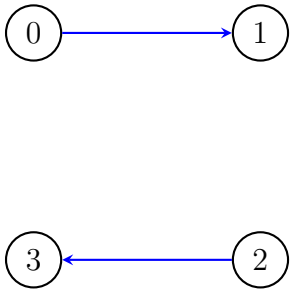
S **non è riflessiva**: Non c'è un ciclo su 1, per esempio. Questo significa che $(1,1) \notin S$, quindi S non è riflessiva.

S **non è simmetrica**: C'è una freccia che va da 0 a 2, ma non c'è una freccia che va da 2 a 0. Quindi $(0,2) \in S$, ma $(2,0) \notin S$, quindi S non è simmetrica.

S **è transitiva**: Esistono tre casi in cui c'è una freccia da un punto del grafo a un secondo punto e una freccia dal secondo punto a un terzo punto: - Ci sono frecce da 0 a 2 e da 2 a 3. - Ci sono frecce da 0 a 0 e da 0 a 2. - Ci sono frecce da 0 a 0 e da 0 a 3.

In ogni caso, esiste una freccia che va dal primo punto al terzo punto. Di conseguenza, S è transitiva.

c. T è riflessiva? simmetrica? transitiva?



T **non è riflessiva**: Non c'è un ciclo su 0, per esempio. Questo significa che $(0,0) \notin T$, quindi T non è riflessiva.

T **non è simmetrica**: C'è una freccia che va da 0 a 1, ma non c'è una freccia che va da 1 a 0. Questo significa che $(0,1) \in T$, ma $(1,0) \notin T$, quindi T non è simmetrica.

T **è transitiva**: La condizione di transitività è vacuamente vera per T. Questo significa che non ci sono coppie ordinate che abbiano il potenziale di "collegare" due coppie attraverso il secondo elemento di una coppia come primo della successiva. Gli unici elementi in T sono $(0,1)$ e $(2,3)$, e questi non possono collegarsi tra loro. Di conseguenza, T è transitiva.

3.1.4 Relazione d'ordine parziale

Definizione 3.11:

Sia A un insieme. Una relazione binaria $\mathcal{R}$ su A ($\mathcal{R} \subseteq A \times A$) è detta una **relazione d'ordine parziale** (o **ordinamento parziale**) se soddisfa le seguenti proprietà:

- **Riflessiva**: Per ogni elemento $x \in A$, x è sempre in relazione con sé stesso. Formalmente:
$$\forall x \in A, \quad x \mathcal{R} x$$
- **Antisimmetrica**: Per ogni coppia di elementi distinti $x, y \in A$, se x è in relazione con y, allora y non è in relazione con x. Formalmente:
$$\forall x, y \in A,\ x \neq y \implies (x \mathcal{R} y \implies \neg(y \mathcal{R} x))$$
- **Transitiva**: Per ogni tre elementi $x, y, z \in A$, se x è in relazione con y e y è in relazione con z, allora x è in relazione con z. Formalmente:
$$\forall x, y, z \in A,\ (x \mathcal{R} y \wedge y \mathcal{R} z) \implies x \mathcal{R} z$$

Inoltre, possono esistere elementi $x, y \in A$, con $x \neq y$, tali che né $x \mathcal{R} y$ né $y \mathcal{R} x$. In altre parole, ci possono essere elementi che non sono confrontabili.

Esempio 3.13. La relazione $\subseteq$ è un ordine parziale sull'insieme dei sottoinsiemi di A.

$$A = \{a, b, c\} \quad \subseteq \quad \mathcal{P}(A)$$
$$\mathcal{P}(A) = \Big\{\emptyset, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a, b, c\}\Big\}$$

Dimostro che la relazione è una relazione d'ordine parziale:
Prima di tutto verifico che la relazione rispetta la proprietà riflessiva.

La proprietà riflessiva è soddisfatta?

$$X \subseteq X \quad \text{per ogni } X \in \mathcal{P}(A)$$

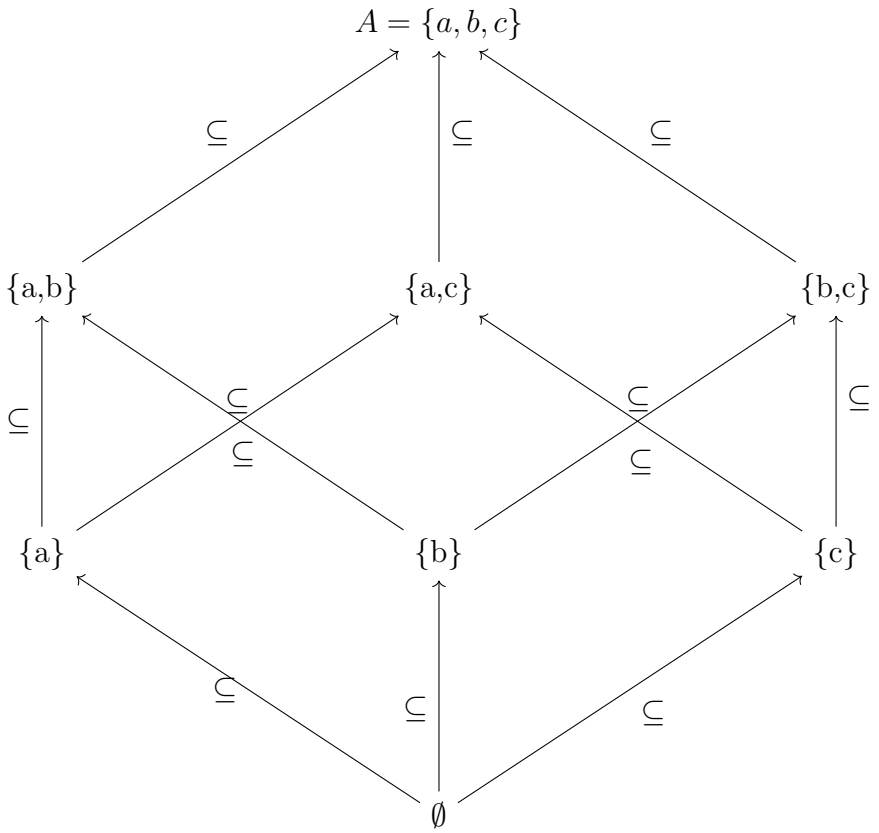
La proprietà è verificata poiché ogni sottoinsieme è contenuto in se stesso.

La proprietà antisimmetrica è soddisfatta? La proprietà antisimmetrica richiede che, se $X \subseteq Y$ e $Y \subseteq X$, allora $X = Y$.

Ad esempio, se consideriamo $X = \{a\}$ e $Y = \{a, b\}$, abbiamo $X \subseteq Y$ ma non $Y \subseteq X$, quindi non c'è contraddizione. Se invece $X \subseteq Y$ e $Y \subseteq X$, allora X e Y devono essere uguali.

La proprietà transitiva è soddisfatta? Se $X \subseteq Y$ e $Y \subseteq Z$, allora $X \subseteq Z$. Quindi, la proprietà è verificata.

Concludiamo che la relazione di inclusione $\subseteq$ è un ordine parziale su $\mathcal{P}(A)$.



Nella partizione ci sono elementi non confrontabili i quali sono:

- $\{a\} \not\subseteq \{b, c\}$
- $\{b, c\} \not\subseteq \{a\}$

3.1.5 Relazione d'ordine totale

Definizione 3.12:

Una relazione binaria $\mathcal{R}$ su un insieme A ($\mathcal{R} \subseteq A \times A$) è detta una **relazione d'ordine totale** (o **ordinamento totale**) se soddisfa le condizioni di un ordinamento parziale ed è verificata la seguente ulteriore proprietà:

$$\forall x, y \in A, \quad (x \mathcal{R} y \text{ oppure } y \mathcal{R} x)$$

Questo significa che qualsiasi coppia di elementi x, y dell'insieme A deve essere confrontabile attraverso la relazione $\mathcal{R}$.

Esempio 3.14. La relazione $\leq$ su $\mathbb{Z}$ è una relazione d'ordine totale.
Dimostro che la proprietà è una relazione d'ordine totale:
La proprietà riflessiva è soddisfatta?

$$7 \leq 7$$

La proprietà è riflessiva $\forall x \in A$

La proprietà antisimmetrica è soddisfatta?

$$7 \leq 15 \text{ ma } 15 \not\leq 7$$

La proprietà è antisimmetrica $\forall x, y \in A$

La proprietà transitiva è soddisfatta?

$$7 \leq 15 \ \wedge \ 15 \leq 20 \implies 7 \leq 20$$

La proprietà è transitiva $\forall x, y \in A$

3.1.6 Relazione d'ordine parziale stretta

Definizione 3.13:

Sia A un insieme. Una relazione binaria $\mathcal{R}$ su A ($\mathcal{R} \subseteq A \times A$) è detta una **relazione d'ordine parziale stretta** (o **ordinamento parziale stretto**) se soddisfa le seguenti proprietà:

- **Irriflessiva**: Per ogni elemento $x \in A$, non si verifica mai che x sia in relazione con sé stesso. Formalmente:

$$\forall x \in A, \quad \neg(x \mathcal{R} x)$$

- **Antisimmetrica**: Per ogni coppia di elementi distinti $x, y \in A$, se x è in relazione con y, allora y non è in relazione con x. Formalmente:

$$\forall x, y \in A, \ x \neq y \implies (x \mathcal{R} y \implies \neg(y \mathcal{R} x))$$

- **Transitiva**: Per ogni tre elementi $x, y, z \in A$, se x è in relazione con y e y è in relazione con z, allora x è in relazione con z. Formalmente:

$$\forall x, y, z \in A, \ (x \mathcal{R} y \wedge y \mathcal{R} z) \implies x \mathcal{R} z$$

Esempi

- $\subset$ su $\mathcal{P}(A)$;
- $<$ su $\mathbb{Z}$.

3.1.7 Catena

Definizione 3.14:

Un sottoinsieme X di un insieme parzialmente ordinato A è una **catena** se gli elementi di X sono confrontabili a due a due.

Esempio 3.15. : Si consideri l'insieme $\mathbb{N}$ con la relazione $<$:

$$0 < 1 < 2 < 3 < 4 \cdots$$

3.1.8 Anticatena

Definizione 3.15:

Un sottoinsieme X di un insieme parzialmente ordinato A è una **anticatena** se gli elementi di X sono inconfrontabili a due a due.

Esempio 3.16. : Si consideri l'insieme $\mathbb{N}$ con la relazione $n_1 < n_2$ se n_1 è un divisore di n_2. L'insieme dei numeri primi maggiori di 3 forma una anticatena:

$$3,\ 5,\ 7,\ 11,\ \cdots$$

3.1.9 Ordinamento ben fondato

Definizione 3.16:

Un ordinamento parziale $\leq$ su un insieme A è detto **ben fondato** se non ammette catene discendenti infinite, ovvero non esistono catene della forma:

$$a_0 > a_1 > a_2 > \cdots > a_n > \cdots$$

Esempio 3.17. L'ordine naturale $\leq$ su $\mathbb{N}$, definito da: $x \leq y$ se esiste $k \in \mathbb{N}$ tale che $y = x + k$, è un ordinamento ben fondato:

$$0 \leq 1 \leq 2 \leq \cdots$$

Esempio 3.18. L'ordine naturale $\leq$ su $\mathbb{Z}$, definito da: $x \leq y$ se esiste $k \in \mathbb{N}$ tale che $y = x + k$, non è un ordinamento ben fondato, infatti:

$$0 > -1 > -2 > -3 > \cdots$$

è una catena discendente infinita.

Definizione 3.17:

Sia A un insieme e sia $\mathcal{R}$ una relazione d'ordine parziale su A. Due elementi $x, y \in A$ si dicono **confrontabili** (o **comparabili**) se vale almeno una delle seguenti condizioni:

$$x\mathcal{R}y \quad \text{oppure} \quad y\mathcal{R}x$$

Al contrario, due elementi $x, y \in A$ si dicono **inconfrontabili** (o **incomparabili**) se non vale nessuna delle due condizioni sopra, ovvero:

$$\neg(x\mathcal{R}y) \quad \text{e} \quad \neg(y\mathcal{R}x)$$

3.2 Relazione di equivalenza

Definizione 3.18:

Sia A un insieme. Una relazione binaria $\mathcal{R}$ su A ($\mathcal{R} \subseteq A \times A$) è detta una **relazione di equivalenza** se soddisfa le seguenti proprietà:

- **Riflessiva**: Per ogni elemento $x \in A$, x è sempre in relazione con sé stesso. Formalmente:
$$\forall x \in A, \quad x \mathcal{R} x$$
- **Simmetrica**: Per ogni coppia di elementi $x, y \in A$, se x è in relazione con y, allora anche y è in relazione con x. Formalmente:
$$\forall x, y \in A, \ (x \mathcal{R} y \implies y \mathcal{R} x)$$
- **Transitiva**: Per ogni tre elementi $x, y, z \in A$, se x è in relazione con y e y è in relazione con z, allora x è in relazione con z. Formalmente:
$$\forall x, y, z \in A, \ (x \mathcal{R} y \land y \mathcal{R} z) \implies x \mathcal{R} z$$

Esempio 3.19. Sia A l'insieme degli studenti.
Sia $\mathcal{R}$ la relazione definita come:

$$\mathcal{R} = \{(x, y) \mid x \text{ e } y \text{ abitano nello stesso comune}\}$$

- $\mathcal{R}$ **è riflessiva**: Questo perché ogni studente x abita nello stesso comune di sé stesso. Quindi, per ogni $x \in A$, vale $(x, x) \in \mathcal{R}$.
- $\mathcal{R}$ **è simmetrica**: Se x abita nello stesso comune di y, allora anche y abita nello stesso comune di x. Di conseguenza, per ogni coppia di studenti $x, y \in A$, se $(x, y) \in \mathcal{R}$, allora $(y, x) \in \mathcal{R}$.
- $\mathcal{R}$ **è transitiva**: Se x abita nello stesso comune di y e y abita nello stesso comune di z, allora x abita nello stesso comune di z. Quindi, per ogni tripla di studenti $x, y, z \in A$, se $(x, y) \in \mathcal{R}$ e $(y, z) \in \mathcal{R}$, allora $(x, z) \in \mathcal{R}$.

3.2.1 Classi di equivalenza

Definizione 3.19:

Supponiamo che A sia un insieme e che $\mathcal{R}$ sia una relazione di equivalenza su A. Per ogni elemento $a \in A$, la **classe di equivalenza di** a, indicata con $[a]$ e chiamata semplicemente la **classe di** a, è l'insieme di tutti gli elementi $x \in A$ tali che x è in relazione con a tramite $\mathcal{R}$.
In simboli:
$$[a] = \{x \in A \mid x \, \mathcal{R} \, a\}$$

Esempio 3.20. Sia $\mathcal{R}$ una relazione su $\mathbb{R} \times \mathbb{R}$:

$$x\mathcal{R}y \iff x = y$$

- La relazione $\mathcal{R}$ è **riflessiva** se, per ogni $x \in R$:

  $$x\mathcal{R}x$$

  che equivale a $x = x$.

- La relazione $\mathcal{R}$ è **simmetrica** se, per ogni coppia di elementi $x, y \in R$:

  $$x\mathcal{R}y \implies y\mathcal{R}x$$

  che equivale a dire che se $x = y$, allora $y = x$.

- La relazione $\mathcal{R}$ è **transitiva** se, per ogni $x, y, z \in R$:

  $$(x\mathcal{R}y \land y\mathcal{R}z) \implies x\mathcal{R}z$$

  che equivale a dire che se $x = y$ e $y = z$, allora $x = z$.

Classi di equivalenza di $\mathcal{R}$

Per ogni $n \in R$:

$$[n] = \{x \in R \mid x\mathcal{R}n\} = \{x \in R \mid x = n\} = \{n\}$$

In altre parole, per ogni $n \in R$, la classe di equivalenza $[n]$ è data da:

$$[n] = \{n\}$$

Di conseguenza ci sono infinite classi equivelenza $\forall n \in \mathbb{R}$

Capitolo 4

Funzioni

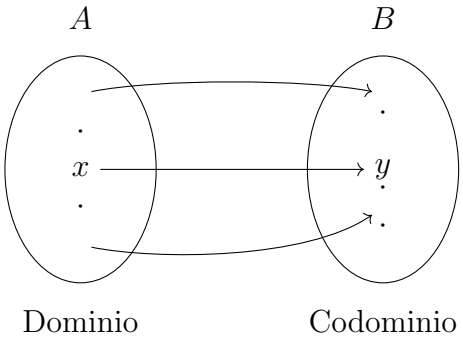
Definizione 4.1:

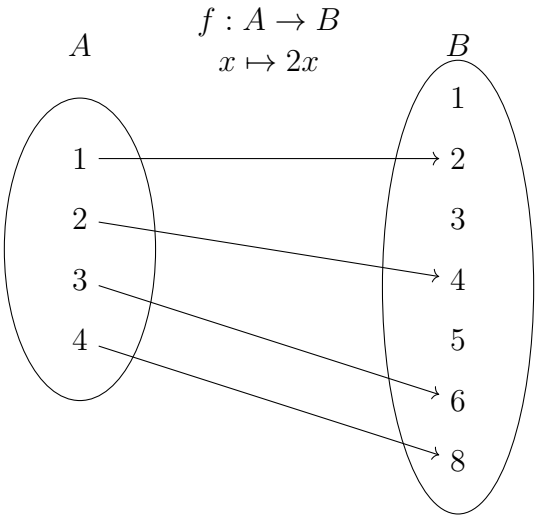
Una funzione f da un insieme A a un insieme B, è un sottoinsieme C_f del prodotto cartesiano $A \times B$ dove A è il dominio e B il codominio, che soddisfi il seguente requisito:

$$\forall x \in A \exists! (x, y) \in C_f$$

In particolare, la coppia $(x, y) \in C_f$ specifica l'immagine di x, ossia $y = f(x)$. Quindi:

$$C_f = \{(x, y) \in A \times B \mid y = f(x)\}$$





$f(x) = 2x$
$f(x)$ è l'immagine di x tramite f

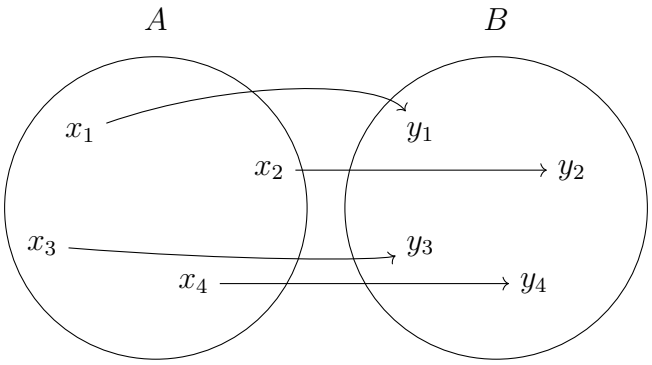
Definizione 4.2:

sia f una funzione che:

$$f : A \to B$$

L'immagine è l'insieme:

$$f(A) = \{f(x) \in B \mid x \in A\}$$



Definizione 4.3:

Data una funzione $f : A \to B$, per un elemento $y \in B$, la controimmagine di y tramite f è l'insieme di tutti gli elementi in X che vengono mappati in y attraverso f. In altre parole, ogni $x \in A$ per cui $f(x) = y$ è considerato una controimmagine di y. La controimmagine di y è definita come:

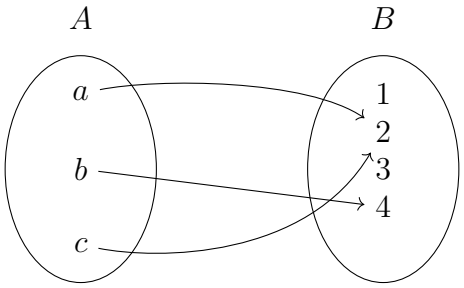
$$f^{-1}(y) = \{x \in X \mid f(x) = y\}$$

Esempio 4.1. $f : A \to B$

$$A = \{a, b, c\} \; B = \{1, 2, 3, 4\}$$

consideriamo le seguenti immagini:

- $f(a) = 2$
- $f(b) = 4$
- $f(c) = 2$



Si calcoli la controimmagine di :

- $\{2\} \subseteq B$
$$f^{-1}(\{2\}) = \{a, c\}$$
- $\{4\} \subseteq B$
$$f^{-1}(\{4\}) = \{b\}$$
- $\{1, 3\} \subseteq B$
$$f^{-1}(\{1, 3\}) = \emptyset$$

4.1 Proprietà delle funzioni

le funzioni possono essere caratterizzate da diverse proprietà che descrivono il modo in cui gli elementi dell'insieme di partenza vengono mappati in quelli dell'insieme di arrivo. Queste proprietà sono fondamentali per comprendere la natura della funzione e la relazione tra i due insiemi su cui opera.

Le principali proprietà che esamineremo sono l'iniettività, la suriettività e la biiettività:

- Una funzione è detta **iniettiva** (o *uno-a-uno*) se ogni elemento dell'insieme di arrivo è immagine di al più un elemento dell'insieme di partenza. Ciò significa che due elementi distinti dell'insieme di partenza non possono essere mappati nello stesso elemento dell'insieme di arrivo.

- Una funzione è detta **suriettiva** (o *su*) se ogni elemento dell'insieme di arrivo è immagine di almeno un elemento dell'insieme di partenza. In altre parole, la funzione "copre" tutto l'insieme di arrivo.

- Una funzione è detta **biiettiva** se è sia iniettiva che suriettiva. In questo caso, ogni elemento dell'insieme di arrivo è immagine di un solo elemento dell'insieme di partenza e viceversa. Una funzione biiettiva stabilisce quindi una corrispondenza biunivoca tra i due insiemi.

Nei paragrafi seguenti, forniremo una definizione dettagliata di ciascuna di queste proprietà, con esempi che illustrano il loro significato e le loro applicazioni.

4.1.1 Funzioni iniettive

Definizione 4.4:

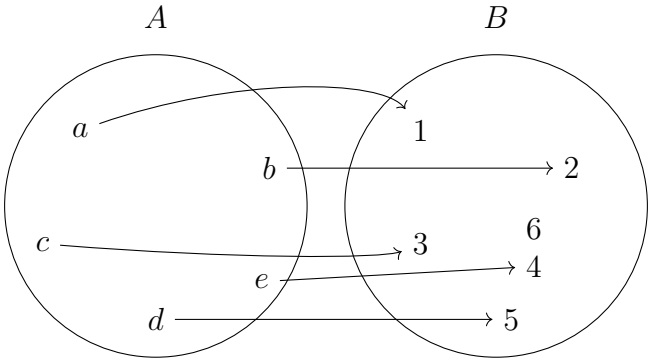
Sia f una funzione che va da un insieme A a un insieme B. f è una funzione iniettiva se e solo se per ogni elemento x_1 e x_2 appartenenti ad A.

$$f(x_1) = f(x_2) \implies x_1 = x_2$$

In simboli:

$$f : A \to B \text{ è iniettiva } \iff \forall x_1, x_2 \in A, \text{ se } f(x_1) = f(x_2) \implies x_1 = x_2$$

Una funzione $f : A \to B$ non è iniettiva $\iff$ $\exists$ elementi $x_1 \wedge x_2 \in A$ con $f(x_1) = f(x_2) \wedge x_1 \neq x_2$.



Per dimostrare che $f : A \to B$ è iniettiva è sufficiente provare che se $x_1, x_2 \in A$ con $f(x_1) = f(x_2) \implies x_1 = x_2$. Invece per dimostrare che non è iniettiva è sufficiente trovare due elementi $x_1, x_2 \in A$ con $x_1 \neq x_2$ e $f(x_1) = f(x_2)$

Esempio 4.2. $f : \mathbb{N} \to \mathbb{N}$

$$f(n) = 2n$$

Dimostrazione 4.1. Voglio dimostrare che f è iniettiva.

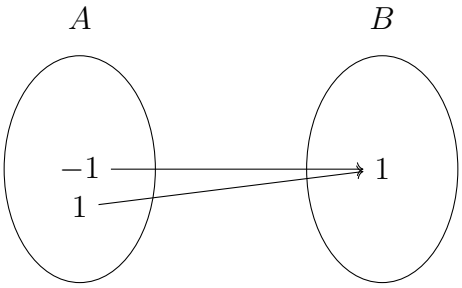
Siano $n1, n2 \in N$:

$$2n_1 = 2n_2 \implies n_1 = n_2$$

Ho dimostrato che f è iniettiva. □

Esempio 4.3. $f : \mathbb{Z} \to \mathbb{Z}$

$$f(x) = x^2$$



Dimostrazione 4.2. Per dimostrare che f non è iniettiva è sufficiente trovare una coppia $x_1, x_2 \ni' x_1 \neq x_2 \wedge f(x_1) = f(x_2)$. f non è iniettiva poiché:

$$f(-2) = 4 = f(2)$$

□

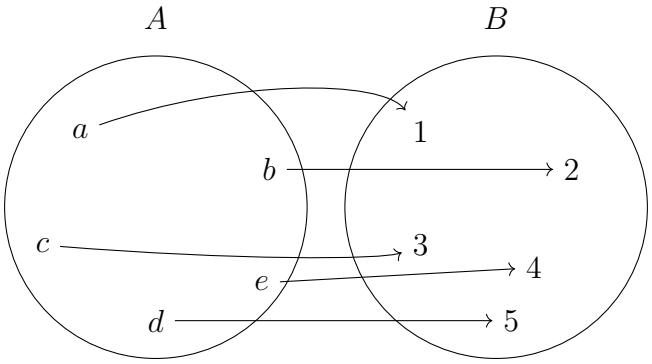
4.1.2 Funzioni suriettive

Definizione 4.5:

Sia f una funzione che va da un insieme A a un insieme B. F è suriettiva se e solo se, preso un qualsiasi elemento $y \in B$, è possibile trovare un elemento $x \in A$ con la proprietà che $y = f(x)$ In simboli:

$$f : A \to B \text{ è iniettiva } \forall y \in B,\ \exists x \in A \ni' \ f(x) = y$$

Una funzione $f : A \to B$ non è suriettiva $\iff \exists y \in B \ni' \forall x \in A,\ f(x) \neq y$



Esempio 4.4. Dimostrazione o controesempio per la suriettività delle funzioni
Definiamo $f : \mathbb{R} \to \mathbb{R}$ e $h : \mathbb{N} \to \mathbb{N}$ come segue:

$$f(x) = \frac{x}{2} + 3 \quad \text{per ogni } x \in \mathbb{R}$$

$$h(n) = \frac{n}{2} + 3 \quad \text{per ogni } n \in \mathbb{Z}$$

Parte (a): La funzione f è suriettiva?

La funzione $f : \mathbb{R} \to \mathbb{R}$ è definita dalla regola $f(x) = \frac{x}{2} + 3$ per tutti i numeri reali x. Per dimostrare che f è suriettiva, dobbiamo mostrare che

$$\forall y \in \mathbb{R},\ \exists x \in \mathbb{R} \text{ tale che } f(x) = y.$$

Sostituendo la definizione di f, supponiamo che y sia un numero reale e cerchiamo un numero reale x tale che $y = \frac{x}{2} + 3$.

Calcoli preliminari: Se esiste un numero reale x tale che $f(x) = y$, allora deve valere:

$$\frac{x}{2} + 3 = y$$

$$\frac{x}{2} = y - 3 \quad \text{(sottraendo 3 da entrambi i membri)}$$

$$x = 2(y - 3) \quad \text{(moltiplicando entrambi i membri per 2)}$$

Quindi, se esiste tale numero x, deve essere uguale a $x = 2(y - 3)$.

Esiste un tale numero? Sì. Per mostrare questo, poniamo $x = 2(y - 3)$ e verifichiamo che (1) x è un numero reale e che (2) f invia effettivamente x a y.

Risposta formale: Se $f : \mathbb{R} \to \mathbb{R}$ è la funzione definita dalla regola $f(x) = \frac{x}{2} + 3$ per tutti i numeri reali x, allora f è suriettiva.

Dimostrazione: Sia $y \in \mathbb{R}$. [Dobbiamo mostrare che $\exists x \in \mathbb{R}$ tale che $f(x) = y$.] Poniamo $x = 2(y - 3)$. Allora x è un numero reale, poiché la somma, la differenza e il prodotto di numeri reali sono reali. Di conseguenza:

$$f(x) = f\left(2(y - 3)\right) \quad \text{(per sostituzione)}$$

$$= \frac{2(y - 3)}{2} + 3 \quad \text{(per la definizione di } f\text{)}$$

$$= (y - 3) + 3 = y \quad \text{(per proprietà algebriche)}$$

Questo è ciò che volevamo dimostrare. □

Parte (b): La funzione h è suriettiva?

La funzione $h : \mathbb{Z} \to \mathbb{Z}$ è definita dalla regola $h(n) = \frac{n}{2} + 3$ per ogni intero n.

Per dimostrare che h è suriettiva, sarebbe necessario dimostrare che

$$\forall m \in \mathbb{Z},\ \exists n \in \mathbb{Z} \text{ tale che } h(n) = y.$$

Supponiamo che m sia un numero intero e cerchiamo di mostrare che esiste un intero n tale che $\frac{n}{2} + 3 = y$.

Calcoli preliminari

Supponiamo che esista un numero naturale n tale che $h(n) = y$. Allora deve valere:

$$\frac{n}{2} + 3 = y$$

Isoliamo n:

$$\frac{n}{2} = y - 3 \quad \text{(sottraendo 3 da entrambi i membri)}$$

$$n = 2(y - 3) \quad \text{(moltiplicando entrambi i membri per 2)}$$

Quindi, per un dato $m \in \mathbb{N}$, possiamo ottenere un valore per n come $n = 2(m-3)$. Tuttavia, questo valore di n non sarà sempre un numero naturale, poiché potrebbe risultare negativo o non intero.

Controesempio

Consideriamo il caso in cui $y = 2$: - Se $y = 2$, allora

$$n = 2(2 - 3) = 2 \cdot (-1) = -2,$$

che non è un numero naturale.

Poiché non esiste alcun $n \in \mathbb{N}$ che soddisfi $h(n) = -2$, la funzione non è suriettiva su $\mathbb{N}$. □

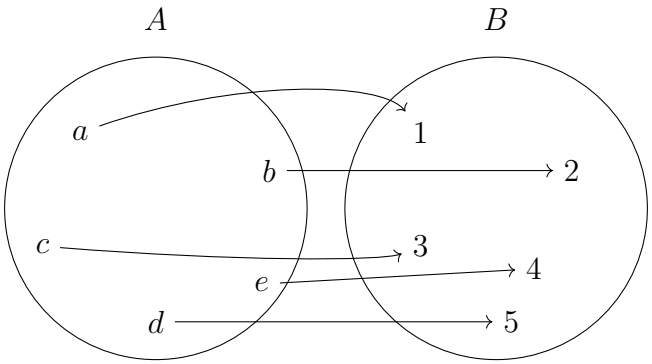
4.1.3 Funzioni biiettive

Consideriamo una funzione $f : A \to B$che sia sia iniettiva e suriettiva. Dato un qualsiasi elemento $x \in A$, esiste un' unico elemento corrispondente $y = f(x) \in B$. Inoltre, dato un qualsiasi elemento $y \in B$, esiste un elemento $x \in A$ tale che $f(x) = y$ e vi è solo uno specifico x che soddisfa questa condizione.

Pertanto, una funzione che è sia uno-a-uno che su stabilisce una corrispondenza tra gli elementi di A e gli elementi di B, abbinando ciascun elemento di A a un unico elemento di B e ciascun elemento di B a un unico elemento di A. Tale corrispondenza è detta corrispondenza biunivoca o biiezione.

Definizione 4.6:

Una corrispondenza biunivoca da un insieme A a un insieme B è una funzione che è sia iniettiva che suriettiva.



Esempio 4.5. $f : \mathbb{R} \to \mathbb{R}$

$$f(x) = 4x - 1$$

- f è iniettiva ?

Dimostrazione 4.3. Siano x_1 e $x_2 \in \mathbb{R} \ni' f(x_1) = f(x_2) \implies x_1 = x_2$

Se $f(x_1) = f(x_2)$ allora:

$$4x_1 - 1 = 4x_2 - 1$$

$$4x_1 = 4x_2 \implies x_1 = x_2$$

abbiamo dimostrato che $f(x1) = f(x_2)$ allora $x_1 = x_2$ e $x_1 = x_2$, cioè

- f è suriettiva ?

Dimostrazione 4.4. Devo dimostrare $\forall y \in \mathbb{R} \exists x \in \mathbb{R} \ni' f(x) = y$

$$y = 4x - 1 \implies x = \frac{y+1}{4} \in \mathbb{R}$$

$$f(x) = f\big(\frac{y+1}{4}\big) = 4 \cdot \big(\frac{y+1}{4}\big) - 1 = y \implies y + 1 - 1 = y \implies y = y$$

Pertanto ho dimostrato che f è suriettiva. Dunque siccome f è sia iniettiva che suriettiva, possiamo concludere dicendo ché è una biiezione.

Esempio 4.6. Consideriamo la funzione $f : \mathbb{Z} \to \mathbb{Z}$ definita da

$$f(x) = 4x - 1$$

- f è iniettiva?

Dimostrazione 4.5. Siano $x_1, x_2 \in \mathbb{Z}$ tali che $f(x_1) = f(x_2)$. Dobbiamo dimostrare che ciò implica $x_1 = x_2$.

Se $f(x_1) = f(x_2)$, allora:

$$4x_1 - 1 = 4x_2 - 1$$

$$4x_1 = 4x_2 \implies x_1 = x_2$$

Abbiamo dimostrato che se $f(x_1) = f(x_2)$, allora $x_1 = x_2$. Pertanto, f è iniettiva.

- f è suriettiva?

Dimostrazione 4.6. Dobbiamo dimostrare che $\forall y \in \mathbb{Z}$, $\exists x \in \mathbb{Z}$ tale che $f(x) = y$.

Consideriamo l'equazione $y = 4x - 1$ e risolviamo per x:

$$y = 4x - 1 \implies x = \frac{y+1}{4}$$

Perché x sia un intero, $y + 1$ deve essere divisibile per 4.

Quindi, f non può coprire tutti gli interi $y \in \mathbb{Z}$ ma solo quelli della forma $y = 4k - 1$, dove $k \in \mathbb{Z}$.

Pertanto, f non è suriettiva su $\mathbb{Z}$.

Poiché f è iniettiva ma non suriettiva, non possiamo concludere che f sia una biiezione su $\mathbb{Z}$.

4.1.4 Funzione inversa

Definizione 4.7:

Se f è una corrispondenza biunivoca da un insieme A a un insieme B, allora esiste una funzione da B a A che "annulla" l'azione di f. In altre parole, questa funzione inversa invia ciascun elemento di B all'elemento di A da cui proviene.
Questa funzione è chiamata funzione inversa di f ed è indicata con f^{-1}.

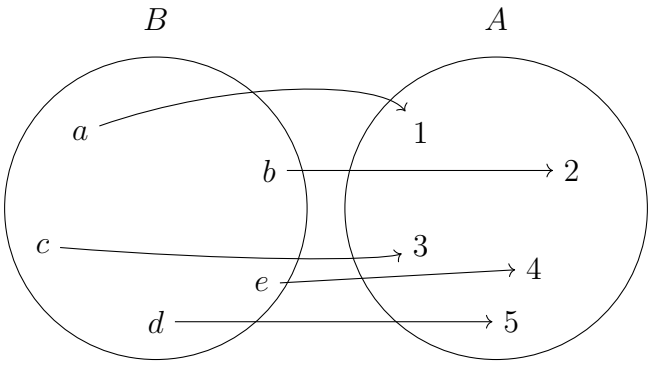
Teorema 4.1:

Supponiamo che $f : A \to B$ sia una corrispondenza biunivoca; cioè, supponiamo che f sia sia iniettiva che suriettiva. Allora esiste una funzione $f^{-1} : B \to A$ definita come segue:
Dato un elemento y in B,

$$f^{-1}(y) = \text{l'unico elemento } x \in A \text{ tale che } f(x) = y.$$

In altre parole,

$$f^{-1}(y) = x \iff y = f(x).$$



Esempio 4.7. $f : \mathbb{R} \to \mathbb{R}$

$$f(x) = 4x - 1$$

- f è iniettiva ?

Dimostrazione 4.7. Siano x_1 e $x_2 \in \mathbb{R} \ni' f(x_1) = f(x_2) \implies x_1 = x_2$
Se $f(x_1) = f(x_2)$ allora:

$$4x_1 - 1 = 4x_2 - 1$$

$$4x_1 = 4x_2 \implies x_1 = x_2$$

abbiamo dimostrato che $f(x1) = f(x_2)$ allora $x_1 = x_2$ e $x_1 = x_2$, cioè

- f è suriettiva ?

Dimostrazione 4.8. Devo dimostrare $\forall y \in \mathbb{R} \exists x \in \mathbb{R} \ni' f(x) = y$

$$y = 4x - 1 \implies x = \frac{y+1}{4} \in \mathbb{R}$$

$$f(x) = f\big(\frac{y+1}{4}\big) = 4 \cdot \big(\frac{y+1}{4}\big) - 1 = y \implies y + 1 - 1 = y \implies y = y$$

Pertanto ho dimostrato che f è suriettiva. Dunque siccome f è sia iniettiva che suriettiva, possiamo concludere dicendo ché è una biiezione, e siccome è una biiezione f è anche invertibile. Dunque la dunzione inversa è :

$$f^{-1}(y) = \frac{y+1}{4} - 1$$

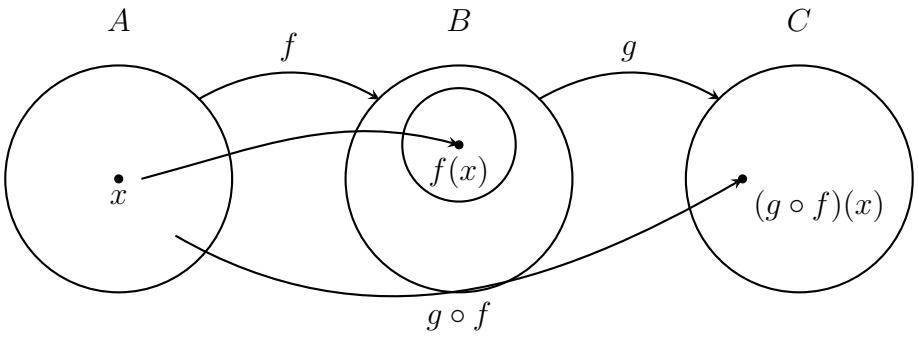
4.2 Composizione di funzioni

Definizione 4.8:

Siano $f : X \to Y$ e $g : Y \to Z$ due funzioni tali che l'immagine di f sia un sottoinsieme del dominio di g. Definiamo una nuova funzione $g \circ f : X \to Z$ come segue:

$$(g \circ f)(x) = g(f(x)) \quad \text{per ogni } x \in X,$$

dove $g \circ f$ si legge "g composta f" e $g(f(x))$ si legge "g di f di x". La funzione $g \circ f$ è chiamata la composizione di f e g.



Esempio 4.8. Siano $f : \mathbb{Z} \to \mathbb{Z}$ la funzione successore e $g : \mathbb{Z} \to \mathbb{Z}$ la funzione quadrato. Allora

$$f(n) = n + 1 \quad \text{per ogni } n \in \mathbb{Z}$$

e

$$g(n) = n^2 \quad \text{per ogni } n \in \mathbb{Z}.$$

(a) Trova le composizioni $g \circ f$ e $f \circ g$.

(b) $g \circ f = f \circ g$? Spiega.

Soluzione

(a) Le funzioni $g \circ f$ e $f \circ g$ sono definite come segue:

$$(g \circ f)(n) = g(f(n)) = g(n + 1) = (n + 1)^2 \quad \text{per ogni } n \in \mathbb{Z},$$

e

$$(f \circ g)(n) = f(g(n)) = f(n^2) = n^2 + 1 \quad \text{per ogni } n \in \mathbb{Z}.$$

(b) Due funzioni da un insieme a un altro sono uguali se, e solo se, assumono sempre gli stessi valori. In questo caso,

$$(g \circ f)(1) = (1 + 1)^2 = 4, \quad \text{mentre} \quad (f \circ g)(1) = 1^2 + 1 = 2.$$

Quindi, le due funzioni $g \circ f$ e $f \circ g$ non sono uguali:

$$g \circ f \neq f \circ g.$$

4.3 Funzione identità

Dato un insieme X, definiamo una funzione I_X da X a X come

$$I_X(x) = x \quad \text{per ogni } x \in X.$$

Definizione 4.9:

La funzione I_A è chiamata la funzione identità su A perché invia ogni elemento di A all'elemento stesso. Pertanto, la funzione identità può essere immaginata come una macchina che invia ogni pezzo di input direttamente all'uscita senza alcuna modifica.

Esempio 4.9. Sia A un insieme qualsiasi e supponiamo che a_{ij}^k e $\varphi(z)$ siano elementi di A. Trova $I_A(a_{ij}^k)$ e $I_A(\Phi(z))$.

Soluzione: Qualsiasi cosa venga inserita nella funzione identità esce invariata, quindi

$$I_A(a_{ij}^k) = a_{ij}^k \quad \text{e} \quad I_A(\Phi(z)) = \Phi(z).$$

Teorema 4.2:

Se f è una funzione da un insieme A a un insieme B, e I_A è la funzione identità su A, e I_B è la funzione identità su B, allora:

(a) $f \circ I_A = f$

(b) $I_B \circ f = f$

Dimostrazione 4.9. *Parte (a):* Supponiamo che $f : A \to B$ e che I_A sia la funzione identità su A, definita come $I_A(x) = x$ per ogni $x \in A$. Vogliamo mostrare che $f \circ I_A = f$.

Per ogni $x \in A$,

$$(f \circ I_A)(x) = f(I_A(x)) = f(x).$$

Quindi, per definizione di uguaglianza tra funzioni, $f \circ I_X = f$, come volevamo dimostrare.

Parte (b): Supponiamo che $f : A \to B$ e che I_B sia la funzione identità su B, definita come $I_B(y) = y$ per ogni $y \in B$. Vogliamo mostrare che $I_B \circ f = f$.

Per ogni $x \in A$,

$$(I_B \circ f)(x) = I_B(f(x)) = f(x).$$

Poiché I_B restituisce ogni elemento di B invariato, l'applicazione di I_B a $f(x)$ restituisce semplicemente $f(x)$.

Pertanto, per definizione di uguaglianza tra funzioni, $I_B \circ f = f$, come volevamo dimostrare. □

Teorema 4.3:

Se $f : A \to B$ è una funzione biunivoca (iniettiva e suriettiva) con funzione inversa $f^{-1} : B \to A$, allora:

(a) $f^{-1} \circ f = I_A$

(b) $f \circ f^{-1} = I_B$

Dimostrazione 4.10. *Parte (a):* Supponiamo che $f : A \to B$ sia una funzione biunivoca con funzione inversa $f^{-1} : B \to A$. Per dimostrare che $f^{-1} \circ f = I_A$, dobbiamo mostrare che per ogni $x \in A$, $(f^{-1} \circ f)(x) = x$.

Per ogni $x \in A$,

$$(f^{-1} \circ f)(x) = f^{-1}(f(x)).$$

Poiché f^{-1} è la funzione inversa di f, sappiamo che per ogni $a \in A$ e $b \in B$,

$$f^{-1}(b) = a \iff f(a) = b.$$

Pertanto, $(f^{-1} \circ f)(x) = x$, come volevamo dimostrare.

Parte (b): Ora dimostriamo che $f \circ f^{-1} = I_B$, ovvero che per ogni $y \in B$,

$$(f \circ f^{-1})(y) = y.$$

Sia $y \in B$ un elemento qualsiasi. Allora,

$$(f \circ f^{-1})(y) = f(f^{-1}(y)).$$

Poiché f^{-1} è la funzione inversa di f, abbiamo la proprietà:

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

Quindi, per ogni $y \in B$,

$$(f \circ f^{-1})(y) = y.$$

Quindi $f \circ f^{-1} = I_B$, come volevamo dimostrare.

4.4 Funzione inclusione

La funzione inclusione è una funzione speciale utilizzata per mappare gli elementi di un insieme A in un insieme B quando A è un *sottoinsieme* di B, cioè $A \subseteq B$. Questa funzione permette di considerare A come "parte" di B, mantenendo ogni elemento di A invariato.

Definizione 4.10:

Siano A e B due insiemi tali che $A \subseteq B$. La *funzione inclusione* è definita come una funzione

$$j : A \to B$$

che mappa ciascun elemento di A su sé stesso in B. Formalmente, per ogni $x \in A$,

$$j(x) = x.$$

In altre parole, la funzione inclusione j "include" ogni elemento di A in B senza modificarne il valore.

La funzione inclusione è una *funzione iniettiva*, ovvero una funzione uno-a-uno. Per capire perché j è iniettiva, ricordiamo che una funzione è iniettiva se e solo se *elementi distinti del dominio hanno immagini distinte nel codominio.* Formalmente, j è iniettiva se:

$$j(x_1) = j(x_2) \Rightarrow x_1 = x_2.$$

Poiché $j(x) = x$ per ogni $x \in A$, è chiaro che se $j(x_1) = j(x_2)$, allora deve essere $x_1 = x_2$. In altre parole, la funzione inclusione non "collassa" nessun elemento di A; ogni elemento di A rimane distinto e viene mappato sullo stesso elemento in B.

Questa proprietà rende la funzione inclusione uno strumento utile per "includere" un insieme all'interno di un altro in modo che gli elementi di A siano trattati come elementi di B, senza alterare le loro caratteristiche o relazioni.

4.5 Le funzioni pavimento e soffitto

Le funzioni pavimento e soffitto sono due funzioni fondamentali nella matematica discreta, utilizzate per arrotondare i numeri reali rispettivamente verso il basso e verso l'alto all'intero più vicino.

4.5.1 Funzione pavimento

Definizione 4.11:

La funzione pavimento (o floor) è indicata con il simbolo $\lfloor \cdot \rfloor$ ed è definita come

$$\lfloor \cdot \rfloor : \mathbb{R} \to \mathbb{Z},$$

mappando ogni numero reale $x \in \mathbb{R}$ all'intero più grande che non superi x. In altre parole, il pavimento di x, denotato come $\lfloor x \rfloor$, è il massimo intero v tale che $v \leq x$. Formalmente, si definisce:

$$\lfloor x \rfloor = \max\{v \in \mathbb{Z} \mid v \leq x\}.$$

Questa funzione è utile quando abbiamo bisogno di "tagliare" la parte decimale di un numero e ottenere il maggiore tra gli interi inferiori a x.

Esempio 4.10. Se $x = 3.7$, allora $\lfloor x \rfloor = 3$ perché 3 è l'intero più grande che non supera 3.7.

Esempio 4.11. Se $x = -2.3$, allora $\lfloor x \rfloor = -3$ poiché -3 è l'intero più grande che non supera -2.3.

4.5.2 Funzione soffitto

Definizione 4.12:

La funzione soffitto (o ceiling) è indicata con il simbolo $\lceil \cdot \rceil$ ed è definita come

$$\lceil \cdot \rceil : \mathbb{R} \to \mathbb{Z},$$

mappando ogni numero reale $x \in \mathbb{R}$ all'intero più piccolo che sia almeno pari a x. Il soffitto di x, denotato come $\lceil x \rceil$, è il minimo intero v tale che $v \geq x$. Formalmente, si definisce:

$$\lceil x \rceil = \min\{v \in \mathbb{Z} \mid v \geq x\}.$$

Questa funzione è utile quando vogliamo arrotondare un numero reale verso l'alto per ottenere il minimo intero che non sia inferiore a x.

Esempio 4.12. Se $x = 3.2$, allora $\lceil x \rceil = 4$ perché 4 è l'intero più piccolo che è maggiore o uguale a 3.2.

Esempio 4.13. Se $x = -2.8$, allora $\lceil x \rceil = -2$ poiché -2 è l'intero più piccolo che è maggiore o uguale a -2.8.

4.6 Funzione f^n

Definizione 4.13:

Sia $f : A \to A$ una funzione da un insieme A in sé stesso. La funzione composta $f \circ f$ (ovvero la composizione di f con sé stessa) si indica con f^2. In generale, la composizione di f con sé stessa n volte, cioè $f \circ f \circ \cdots \circ f$ (con n applicazioni), si indica con f^n.

Esempio 4.14. Sia f la funzione che associa a ogni persona il proprio padre. La funzione f^2 associa a ogni persona il proprio nonno paterno, poiché applica f due volte, risalendo di due generazioni.

4.7 La funzione idempotente

Definizione 4.14:

Sia $f : A \to A$. Diciamo che f è *idempotente* se $f = f^2$. In altre parole, una funzione idempotente è tale che, quando applicata due volte, restituisce lo stesso risultato che si ottiene applicandola una sola volta.

Esempio 4.15. Le funzioni costanti: una funzione costante $f : A \to A$, che assegna a tutti gli elementi di A lo stesso valore, è idempotente perché applicarla più volte non cambia il risultato.

Esempio 4.16. La funzione identità $I : A \to A$: la funzione identità che associa ogni elemento a sé stesso è idempotente, poiché $I \circ I = I$.

Esempio 4.17. Le funzioni pavimento $\lfloor \cdot \rfloor$ e soffitto $\lceil \cdot \rceil$: queste funzioni, che arrotondano rispettivamente verso il basso e verso l'alto, sono idempotenti. Infatti, se applicate a un numero, ulteriori applicazioni non ne modificano il risultato (ad esempio, $\lfloor \lfloor x \rfloor \rfloor = \lfloor x \rfloor$ e $\lceil \lceil x \rceil \rceil = \lceil x \rceil$).

4.8 Funzioni a Più Variabili e Funzioni a Valori Multipli

Esistono due tipi principali di funzioni che coinvolgono più variabili: le funzioni a più variabili e le funzioni a valori multipli. Questi due tipi di funzioni hanno diverse strutture e proprietà.

4.8.1 Funzioni a Più Variabili

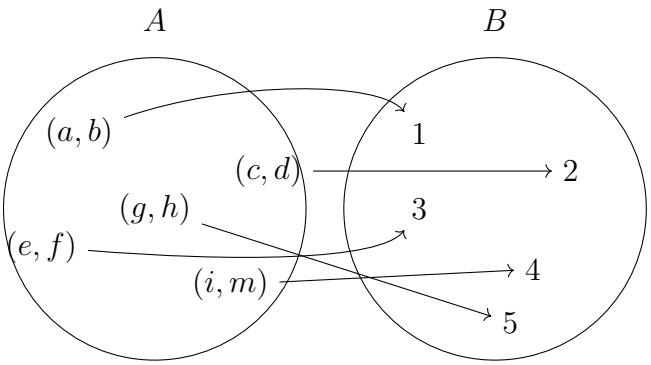
Definizione 4.15:

Una funzione a più variabili è una funzione che prende in ingresso una coppia o una tupla di valori, restituendo un singolo valore come risultato. Questo tipo di funzione associa a ciascuna combinazione di valori di input un unico valore di output.
Formalmente, una funzione $f : A \times B \to C$ è una funzione a più variabili che mappa ogni coppia $(x, y) \in A \times B$ in un singolo elemento $f(x, y) \in C$. In altre parole:

$$f : A \times B \to C.$$

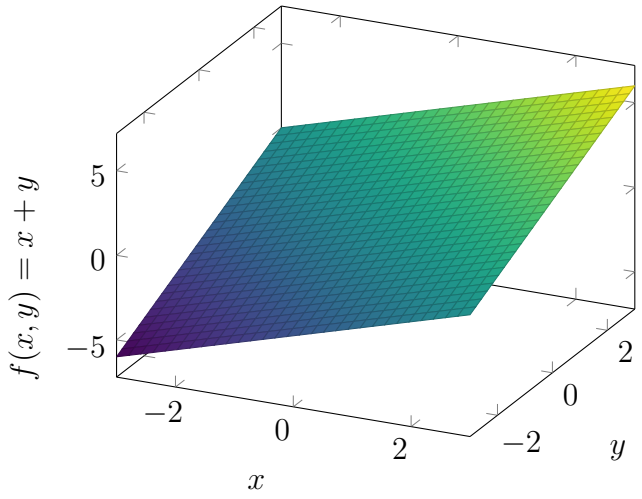
Significa che:

- La funzione f prende in ingresso una coppia di valori (x, y), dove $x \in A$ e $y \in B$.
- La funzione restituisce un singolo valore $f(x, y)$ che appartiene all'insieme C.



Esempio 4.18. Sia $f : \mathbb{N}^2 \to \mathbb{N}$, dove $\mathbb{N}^2$ rappresenta tutte le possibili coppie di numeri naturali. Un esempio è la somma:

$$f(x, y) = x + y.$$



Questa funzione associa a ciascuna coppia (x, y) il risultato $x+y$, che è un singolo numero naturale.

4.8.2 Funzioni a Valori Multipli

Definizione 4.16:

Una funzione a valori multipli è una funzione che, data una coppia o una tupla di valori, restituisce una nuova coppia o tupla di valori. In altre parole, questo tipo di funzione associa a ciascuna combinazione di valori di input un insieme di valori di output, solitamente in forma di una nuova coppia o tupla. Formalmente, una funzione $F : A \times B \to D \times E$ è una funzione a valori multipli che mappa ogni coppia $(x, y) \in A \times B$ in una nuova coppia $(u, v) \in D \times E$. Scriviamo:

$$F : A \times B \to D \times E,$$

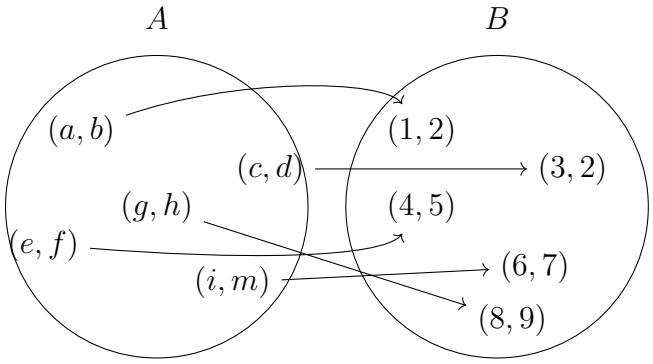
dove:

- La funzione F prende in ingresso una coppia di valori (x, y), dove $x \in A$ e $y \in B$.
- La funzione restituisce una coppia di valori (u, v) con $u \in D$ e $v \in E$.

Questo tipo di funzione viene spesso rappresentato come:

$$F(x, y) = (u(x, y), v(x, y)),$$

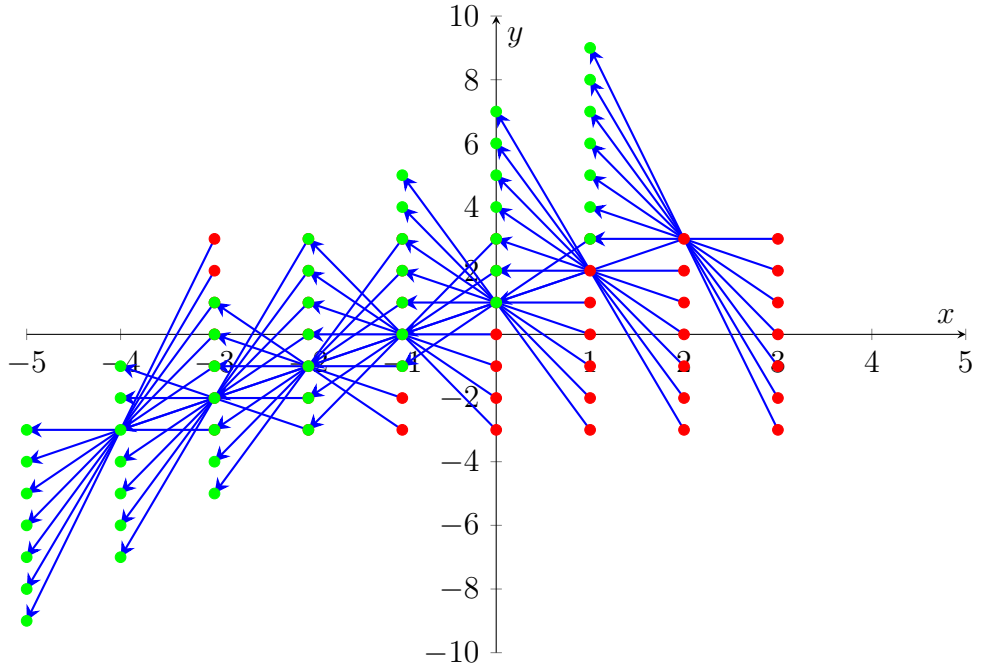
dove $u(x, y)$ e $v(x, y)$ sono le componenti che definiscono i valori di output.



Esempio 4.19. Si consideri la funzione $f : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z} \times \mathbb{Z}$ definita da:

$$f(x, y) = (x - 2, 2x - y).$$

Grafico della funzione $f(x, y) = (x - 2, 2x - y)$



4.8.3 Proprietà delle Funzioni

Proprietà delle Funzioni da $A \times B \to C$ e $A \times B \to D \times E$. Esistono alcune proprietà interessanti per le funzioni sia a più variabili sia a valori multipli, come iniettività, suriettività e biiettività.

1. Iniettività

   - Una funzione a più variabili $f : A \times B \to C$ è iniettiva se coppie distinte producono risultati distinti in C. Formalmente:

     $$f(x_1, y_1) = f(x_2, y_2) \Rightarrow (x_1, y_1) = (x_2, y_2).$$

   - Una funzione a valori multipli $f : A \times B \to D \times E$ è iniettiva se coppie distinte producono coppie di output distinte in $D \times E$:

     $$f(x_1, y_1) = f(x_2, y_2) \Rightarrow (x_1, y_1) = (x_2, y_2).$$

2. Suriettività

   - Una funzione a più variabili $f : A \times B \to C$ è suriettiva se ogni elemento di C è l'immagine di almeno una coppia di valori in $A \times B$:

     $$\forall z \in C,\ \exists (x, y) \in A \times B \text{ tale che } f(x, y) = z.$$

   - Una funzione a valori multipli $F : A \times B \to D \times E$ è suriettiva se ogni coppia in $D \times E$ è l'immagine di almeno una coppia in $A \times B$:

     $$\forall (u, v) \in D \times E,\ \exists (x, y) \in A \times B \text{ tale che } F(x, y) = (u, v).$$

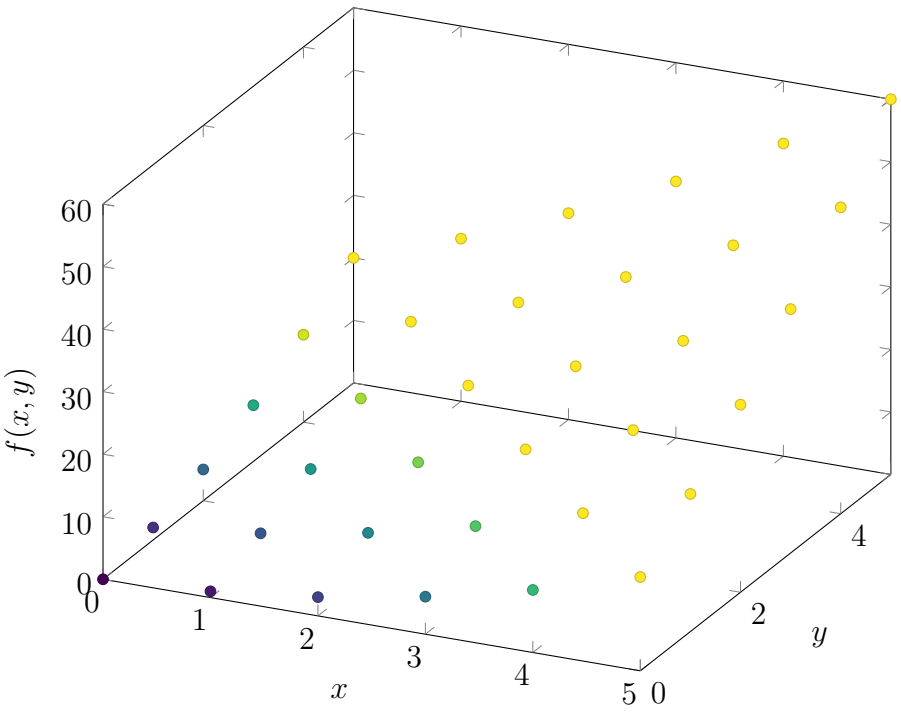
3. Biiettività

   - Una funzione a più variabili $f : A \times B \to C$ è biiettiva se è sia iniettiva che suriettiva, stabilendo una corrispondenza uno-a-uno tra $A \times B$ e C.
   - Una funzione a valori multipli $F : A \times B \to D \times E$ è biiettiva se è sia iniettiva che suriettiva, stabilendo una corrispondenza uno-a-uno tra $A \times B$ e $D \times E$.

Esempio 4.20. Funzione a Due Variabili Biiettiva: Funzione di Cantor La funzione di Cantor è una funzione biiettiva che mappa coppie di numeri naturali $(x, y) \in \mathbb{N}\times\mathbb{N}$ in un singolo numero naturale. È definita come:

$$f(x, y) = \frac{(x + y)(x + y + 1)}{2} + y.$$

Questa funzione stabilisce una corrispondenza uno-a-uno e su tra $\mathbb{N} \times \mathbb{N}$ e $\mathbb{N}$, il che significa che è una funzione biiettiva.



Dimostrazione 4.11. Per dimostrare che $f(x, y)$ è iniettiva, dobbiamo provare che ogni coppia distinta di valori $(x_1, y_1) \neq (x_2, y_2)$ produce un valore distinto di $f(x, y)$.

Supponiamo che $f(x_1, y_1) = f(x_2, y_2)$. Questo implica che:

$$\frac{(x_1 + y_1)(x_1 + y_1 + 1)}{2} + y_1 = \frac{(x_2 + y_2)(x_2 + y_2 + 1)}{2} + y_2.$$

Poiché il valore di $f(x, y)$ dipende unicamente da $x + y$ e y, l'uguaglianza sopra implica che:

$$x_1 + y_1 = x_2 + y_2 \quad \text{e} \quad y_1 = y_2.$$

Dalla seconda uguaglianza, $y_1 = y_2$ implica che $x_1 = x_2$. Quindi, $(x_1, y_1) = (x_2, y_2)$. Pertanto, la funzione è iniettiva.

Per dimostrare che $f(x, y)$ è suriettiva, dobbiamo provare che per ogni numero naturale n esiste una coppia $(x, y) \in \mathbb{N} \times \mathbb{N}$ tale che $f(x, y) = n$.

Dato un valore $n \in \mathbb{N}$, calcoliamo:

$$z = \left\lfloor \frac{\sqrt{8n+1} - 1}{2} \right\rfloor$$

dove $\lfloor \cdot \rfloor$ rappresenta la funzione pavimento, che restituisce la parte intera di un numero.

Definiamo t come:

$$t = n - \frac{z(z+1)}{2}.$$

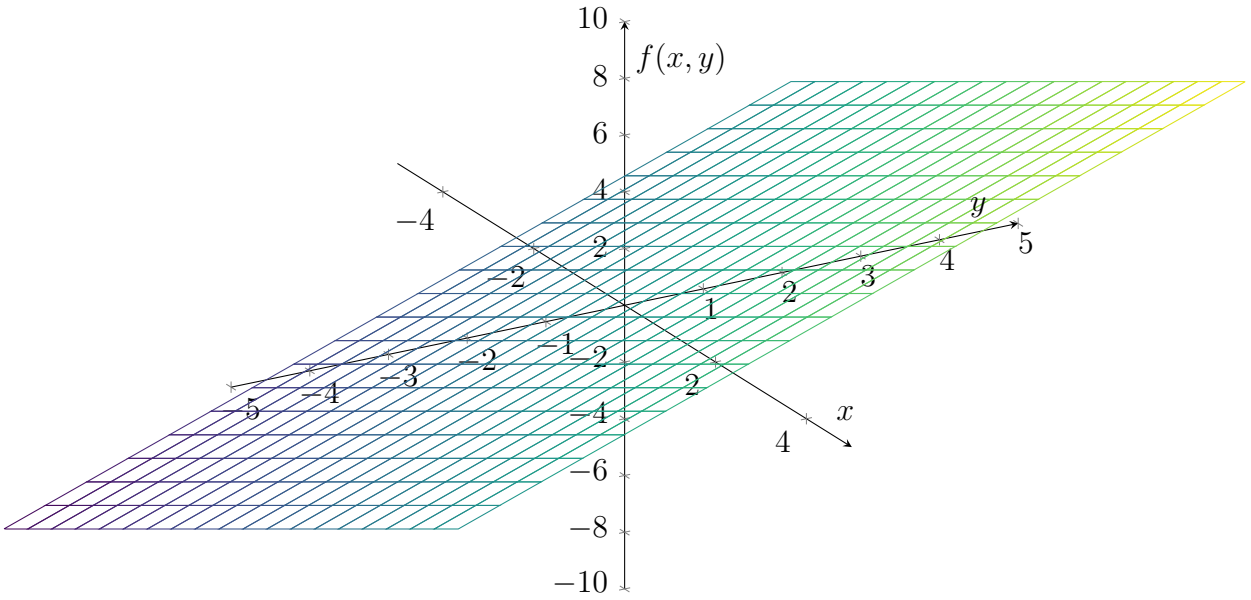
□

Esempio 4.21. Esempio di Funzione a Valori Multipli non biiettiva: Trasformazione Lineare.

Consideriamo la funzione $f : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z} \times \mathbb{Z}$ definita come:

$$f(x, y) = (x + y, x - y).$$

Grafico della funzione $f(x, y) = (x + y, x - y)$



Questa funzione è biiettiva poiché esiste una funzione inversa che permette di recuperare i valori originali (x, y) dalla coppia $(u, v) = f(x, y)$.

Dimostrazione 4.12. Dimostrazione della non Biiettività

- Iniettività Supponiamo che $f(x_1, y_1) = f(x_2, y_2)$, ovvero:

$$(x_1 + y_1, x_1 - y_1) = (x_2 + y_2, x_2 - y_2).$$

Questo implica che:

$$x_1 + y_1 = x_2 + y_2 \quad \text{e} \quad x_1 - y_1 = x_2 - y_2.$$

Risolvendo questo sistema, troviamo che $x_1 = x_2$ e $y_1 = y_2$, quindi la funzione è iniettiva.

- Suriettività

Per dimostrare che la funzione non è suriettiva, mostriamo che esiste una coppia $(u, v) \in \mathbb{Z} \times \mathbb{Z}$ che non è immagine di alcuna coppia $(x, y) \in \mathbb{Z} \times \mathbb{Z}$.

Sia $(u, v) = (1, 0)$. Supponiamo che esistano $x, y \in \mathbb{Z}$ tali che:

$$f(x, y) = (1, 0).$$

Questo implica che:

$$x + y = 1 \quad \text{e} \quad x - y = 0.$$

Risolvendo questo sistema, otteniamo: Sommiamo le due equazioni:

$$(x + y) + (x - y) = 1 + 0 \Rightarrow 2x = 1 \Rightarrow x = \frac{1}{2},$$

Sostituiamo $x = \frac{1}{2}$ in una delle due equazioni, ad esempio $x + y = 1$:

$$\frac{1}{2} + y = 1 \Rightarrow y = \frac{1}{2}.$$

Quindi, la soluzione sarebbe $x = \frac{1}{2}$ e $y = \frac{1}{2}$, ma x e y non appartengono a $\mathbb{Z}$.

Non esiste alcuna coppia $(x, y) \in \mathbb{Z} \times \mathbb{Z}$ tale che $f(x, y) = (1, 0)$. Questo dimostra che la funzione $f(x, y) = (x + y, x - y)$ non è suriettiva su $\mathbb{Z} \times \mathbb{Z}$, poiché non copre tutte le coppie di interi.

4.9 Cardinalità

Definizione 4.17:

- Dato un insieme A, la cardinalità di A si indica con $|A|$ e denota il numero di elementi dell'insieme A.
- Due insiemi A e B hanno la stessa cardinalità (sono equipollenti o equipotenti) se esiste una funzione biiettiva $f : A \to B$.

Contare equivale a costruire una biiezione.

Quante parole ci sono in questa frase? Per rispondere a questa domanda probabilmente utilizzerete un metodo simile a questo:

Quante	parole	ci	sono	in	questa	frase
1	2	3	4	5	6	7

Questo metodo equivale a costruire una biiezione dall'insieme delle parole che compaiono nella frase all'insieme $\{1, 2, 3, 4, 5, 6, 7\}$.

Definizione 4.18:

Sia $n \in \mathbb{N}$, usiamo la notazione $\hat{n} = \{1, 2, \dots, n\}$.
L'insieme A ha cardinalità n (ossia, A ha n elementi, oppure $|A| = n$) se e solo se esiste una funzione biiettiva $f : A \to \hat{n}$ (oppure $f : \hat{n} \to A$).

Sia $n \in \mathbb{N}$ e $\hat{n} = \{1, 2, \dots, n-1, n\}$.

Definizione 4.19:

Un insieme A è formato da un numero finito di elementi se e solo se esiste $n \in \mathbb{N}$ e una corrispondenza biiettiva da A a $\hat{n}$.
Siano A e B due insiemi tali che $|A| = n$ e $|B| = k$ con $n > k$.

- Non esiste alcuna funzione iniettiva da A a B, mentre esistono funzioni iniettive da B a A.
- Esistono funzioni suriettive da A a B, mentre non esiste alcuna funzione suriettiva da B a A.

4.9.1 Insiemi infiniti

- $\mathbb{N}$: insieme dei numeri naturali $\{0, 1, 2, \dots\}$
- $\mathbb{Z}$: insieme dei numeri interi $\{\dots, -2, -1, 0, 1, 2, \dots\}$
- $\mathbb{Q}$: insieme dei numeri razionali
- $\mathbb{R}$: insieme dei numeri reali

4.9.2 Cardinalità di un insieme infinito

Definizione 4.20:

Dato un insieme A, le seguenti condizioni sono equivalenti:

- A è infinito.
- Esiste una funzione biiettiva da A in un suo sottoinsieme proprio.
- Esiste una funzione iniettiva da A in un suo sottoinsieme proprio.
- Esiste una funzione suriettiva da un sottoinsieme proprio di A in A.

4.9.3 Insiemi infiniti equipollenti

Definizione 4.21:

Due insiemi infiniti A e B hanno la stessa cardinalità se esiste una funzione iniettiva da A in B e una funzione iniettiva da B in A.

Esempio 4.22. Siano $\mathbb{P}$ l'insieme dei numeri naturali pari e $\mathbb{D}$ l'insieme dei numeri naturali dispari.

Gli insiemi $\mathbb{P}$ e $\mathbb{D}$ sono equipollenti.

Le funzioni f e f^{-1} definite come segue sono entrambe biiettive:

$$f : \mathbb{P} \to \mathbb{D}, \quad n \to n+1$$

$$f^{-1} : \mathbb{D} \to \mathbb{P}, \quad n \to n-1$$

Esempio 4.23. $\mathbb{P}$ e $\mathbb{Z}$ sono equipollenti

- Consideriamo l'insieme $\mathbb{N}$ dei numeri naturali e l'insieme $\mathbb{Z}$ dei numeri interi.
- Gli insiemi $\mathbb{N}$ e $\mathbb{Z}$ sono equipollenti anche se $\mathbb{N} \subset \mathbb{Z}$.
- **Come si dimostra?**
- L'insieme $\mathbb{N}$ è in corrispondenza biunivoca con l'insieme $\mathbb{Z}$.
- Rappresentazione della corrispondenza biunivoca:

$$\begin{array}{c|cccccccc} \mathbb{Z}: & 0 & -1 & 1 & -2 & 2 & -3 & 3 & \dots \\ \mathbb{N}: & 0 & 1 & 2 & 3 & 4 & 5 & 6 & \dots \end{array}$$

- L'insieme $\mathbb{Z}$ è **numerabile**.

Definizione 4.22:

La cardinalità dell'insieme infinito $\mathbb{N}$ non è un numero naturale. La cardinalità di $\mathbb{N}$ è detta *cardinalità numerabile* e viene indicata con $\aleph_0$ (dove $\aleph$ è la lettera ebraica *aleph*).
Un insieme equipollente a $\mathbb{N}$ si dice *insieme numerabile*.

Dimostrazione 4.13. $\mathbb{N}$ e $\mathbb{Q}^+$ sono equipollenti

Vogliamo dimostrare che l'insieme dei numeri naturali $\mathbb{N}$ e l'insieme dei numeri razionali positivi $\mathbb{Q}^+$ sono **equipollenti**, ovvero che esiste una corrispondenza biunivoca tra i due insiemi.

Definizione dei numeri razionali positivi

Un numero razionale positivo può essere rappresentato nella forma:

$$\mathbb{Q}^+ = \left\{ \frac{p}{q} \mid p, q \in \mathbb{N},\ \mathrm{MCD}(p,q) = 1,\ q \neq 0 \right\}.$$

Pertanto, ogni numero razionale positivo è una frazione ridotta ai minimi termini.

Costruzione di una corrispondenza biunivoca

Per costruire una corrispondenza biunivoca tra $\mathbb{Q}^+$ e $\mathbb{N}$:

1. Disponiamo i numeri razionali positivi $\frac{p}{q}$ in una **griglia infinita**, in cui:

$$\begin{array}{cccc} \frac{1}{1} & \frac{1}{2} & \frac{1}{3} & \cdots \\ \frac{2}{1} & \frac{2}{2} & \frac{2}{3} & \cdots \\ \frac{3}{1} & \frac{3}{2} & \frac{3}{3} & \cdots \\ \vdots & \vdots & \vdots & \ddots \end{array}$$

   Ogni riga p contiene tutte le frazioni con numeratore p e ogni colonna q contiene tutte le frazioni con denominatore q.

2. Per evitare ridondanze, consideriamo solo le frazioni **ridotte ai minimi termini** (cioè, con $\text{MCD}(p, q) = 1$).

3. Seguiamo un percorso a **zig-zag diagonale** nella griglia per contare tutti i razionali:

   - Diagonale 1: $\frac{1}{1}$,
   - Diagonale 2: $\frac{1}{2}, \frac{2}{1}$,
   - Diagonale 3: $\frac{1}{3}, \frac{2}{2}, \frac{3}{1}$,
   - Diagonale 4: $\frac{1}{4}, \frac{2}{3}, \frac{3}{2}, \frac{4}{1}$, e così via.

4. Enumeriamo ciascun razionale assegnandogli un numero naturale n, costruendo una funzione biunivoca $f : \mathbb{N} \to \mathbb{Q}^+$.

Conclusione

Poiché esiste una corrispondenza biunivoca tra $\mathbb{N}$ e $\mathbb{Q}^+$, entrambi gli insiemi hanno la stessa cardinalità, ovvero sono **equipollenti**. In particolare:

$$|\mathbb{N}| = |\mathbb{Q}^+| = \aleph_0.$$

Anche se $\mathbb{N} \subset \mathbb{Q}^+$, l'infinità numerabile di $\mathbb{Q}^+$ implica che i due insiemi sono equipotenti.

Cardinalità di $\mathbb{N}$ e $\mathbb{R}$

L'insieme dei numeri naturali $\mathbb{N}$ è un esempio di insieme infinito **numerabile**, poiché i suoi elementi possono essere messi in corrispondenza biunivoca con l'insieme stesso:

$$|\mathbb{N}| = \aleph_0.$$

L'insieme dei numeri reali $\mathbb{R}$, d'altra parte, ha una cardinalità più grande. Questo perché esiste una funzione iniettiva da $\mathbb{N}$ in $\mathbb{R}$ (ogni numero naturale è un numero reale), ma non esiste una funzione iniettiva da $\mathbb{R}$ in $\mathbb{N}$.

Pertanto:

$$|\mathbb{N}| < |\mathbb{R}|,$$

e l'insieme dei numeri reali è detto **non numerabile**.

Dimostrazione della non numerabilità di $\mathbb{R}$ (Cantor)

Consideriamo l'intervallo $[0,1) \subset \mathbb{R}$. Supponiamo per assurdo che $[0,1)$ sia numerabile. Allora possiamo elencare tutti i numeri di $[0,1)$ come segue:

$$x_1 = 0,235745\ldots, \quad x_2 = 0,147645\ldots, \quad x_3 = 0,351001\ldots, \quad \text{e così via.}$$

Costruiamo ora un nuovo numero x nell'intervallo $[0,1)$, seguendo il **metodo diagonale** di Cantor: - Prendiamo la prima cifra decimale di x_1, la seconda cifra decimale di x_2, la terza cifra decimale di x_3, e così via. - Modifichiamo ciascuna cifra aggiungendo 1 (o, se la cifra è 9, sostituiamo con 0). Questo garantisce che x abbia almeno una cifra diversa da ogni x_i.

Il numero x così costruito non è presente nell'elenco, perché differisce da x_1 nella prima cifra, da x_2 nella seconda cifra, e così via. Questo contraddice l'ipotesi che $[0,1)$ sia numerabile.

Concludiamo quindi che $[0,1)$ (e di conseguenza $\mathbb{R}$) è non numerabile.

La cardinalità del continuo

La cardinalità dell'insieme dei numeri reali $\mathbb{R}$ è indicata con $\mathfrak{c}$ (detta **cardinalità del continuo**). Dunque:

$$|\mathbb{R}| = \mathfrak{c}.$$

Cantor ha dimostrato che:

$$\mathfrak{c} = 2^{\aleph_0}.$$

Questo implica che la cardinalità di $\mathbb{R}$ è maggiore di quella di $\mathbb{N}$:

$$\aleph_0 < \mathfrak{c}.$$

Cardinalità dell'insieme delle parti

Cantor ha anche dimostrato che la cardinalità di ogni insieme A è strettamente minore della cardinalità del suo insieme delle parti $\mathcal{P}(A)$:

$$|A| < |\mathcal{P}(A)| = 2^{|A|}.$$

In particolare:

$$|\mathbb{N}| < |\mathcal{P}(\mathbb{N})| = 2^{\aleph_0} = \mathfrak{c}.$$

Pertanto non esiste un limite superiore per i cardinali transfiniti, poiché di ogni insieme esiste sempre un insieme più numeroso.

Ipotesi del continuo

L'ipotesi del continuo, formulata da Cantor, afferma che non esiste alcun insieme A la cui cardinalità sia strettamente compresa tra quella di $\mathbb{N}$ e quella di $\mathbb{R}$:

$$\neg \exists A : \aleph_0 < |A| < \mathfrak{c}.$$

In altre parole, secondo questa ipotesi:

$$\mathfrak{c} = \aleph_1.$$

Tuttavia, è stato dimostrato che l'ipotesi del continuo è **indecidibile** all'interno della teoria degli insiemi standard (ZFC).

Capitolo 5

Principio di induzione e sommatorie

Definizione 5.1:

Il principio di induzione è una tecnica di dimostrazione che ci permette di dimostrare proprietà con elementi infiniti.
Per provare che $P(x)$ è vera per ogni numero naturale x, è sufficiente dimostrare:

1. **Caso base**: provare che la proprietà è vera per il primo elemento considerato, ovvero 0 per $\mathbb{N}$ e 1 per $\mathbb{N}^+$.
2. **Ipotesi induttiva**: supponiamo che la proprietà sia vera per un numero arbitrario k, ovvero:
$$P(k) \quad \text{è vera.}$$
3. **Passo induttivo**: dimostrare che, sotto questa ipotesi:
   - la proprietà è vera per $k+1$ (induzione standard), ovvero:
   $$P(k) \implies P(k+1),$$
   oppure
   - la proprietà è vera per $k-1$ (induzione a ritroso), ovvero:
   $$P(k) \implies P(k-1).$$

A seconda del contesto e della natura del problema, si può utilizzare uno dei due approcci per completare la dimostrazione.

Esempio 5.1. Dimostrare che la somma dei primi n numeri naturali è uguale a $\dfrac{n(n+1)}{2}$, per ogni numero interno $n \geq 1$.

$$S(n) = 1 + 2 + 4 + \ldots + n = \frac{n(n+1)}{2}$$

- Caso base: $S(1) = \dfrac{1(1+1)}{2} = \dfrac{2}{2} = 1$
- Ipotesi induttiva: Supponiamo che la formula sia vera per un numero naturale arbitrario $k \geq 1$, ovvero:

$$S(k) = 1 + 2 + 4 + \ldots + k = \frac{k(k+1)}{2}.$$

- Passo induttivo : Dobbiamo dimostrare che la formula è vera anche per $S(k+1)$, cioè:

$$\frac{(k+1)(k+2)}{2}$$

$$S(k+1) = S(k) + (k+1).$$

Sostituiamo l'ipotesi induttiva $S(k) = \frac{k(k+1)}{2}$:

$$S(k+1) = \frac{k(k+1)}{2} + (k+1).$$

Mettiamo $k+1$ in evidenza:

$$S(k+1) = \frac{k(k+1) + 2(k+1)}{2}.$$

Fattorizziamo $k+1$ al numeratore:

$$S(k+1) = \frac{(k+1)(k+2)}{2}.$$

La formula è quindi verificata per $k+1$.

Esempio 5.2. Dimostrazione per induzione su n. Dimostrare che $\forall n \in \mathbb{N}$

$$n^3 + 5n = 6m$$

- caso base: verifichiamo che la proprietà è verificata per $n = 0$

$$0^3 + 5(0) = 0$$

che è divisibile per 6 pertanto la base dell'induzione è verificata.

- Ipotesi induttiva : assumiamo chre l'ipotesi è verificata per $n \in \mathbb{N}$ con $n > 0$.

$$n^3 + 5n = 6m$$

- Passo induttivo: Verifichiamo che la proprieta sia vera per $n = n + 1$

$$(n+1)^3 + 5(n+1)$$

$$= n^3 + 5n + 3n^2 + 3n + 6$$

per i potesi induttiva $n^3 + 5n = 6m$

$$6m + 3n^2 + 3n + 6$$

$$= 6k + 3n(n+1) + 6$$

Osservo che $n(n+1)$ è sempre pari dunque $n(n+1) = 2r$. Pertanto ottengo:

$$= 6m + 3 \cdot 2r + 6$$

$$= 6(m + r + 1)$$

è proprio quello che volevo dimostrare, pertanto l'enunciato è verificato per n+1.

5.1 Forma forte del principio di induzione

Definizione 5.2:

Sia $P(n)$ una proprietà definita per interi n, e siano a e b due interi fissati tali che $a \leq b$. Il Principio di Induzione Matematica Forte afferma che, per dimostrare che $P(n)$ è vera per tutti gli interi $n \geq a$, è sufficiente verificare i seguenti due passi:

1. **Passo base**: Dimostrare che $P(a), P(a+1), \ldots, P(b)$ sono tutte vere.
2. **Passo induttivo**: Dimostrare che, per ogni intero $k \geq b$, se $P(i)$ è vera per tutti gli interi i tali che $a \leq i \leq k$, allora $P(k+1)$ è vera.

Se entrambi i passi sono verificati, possiamo concludere che:

$$P(n) \quad \text{è vera per tutti gli interi} \quad n \geq a.$$

Esempio 5.3. Dimostrare che $\forall n \in \mathbb{N} \ni' \ n \geq 2$ è scomponibile per fattori primi

- Caso base: verifichiamo che l'ipotesi sia vera per $n = 2$. Poiché 2 è un numero primo, è scomponibile in fattori primi cioè 2 stesso.
- Ipotesi induttiva :sia $n \geq 2$, supponiamo che la proprietà sia vera per ogni numero $x \ni' 2 \leq x \leq n$, cioè:

  $$\forall x \ni' 2 \leq x \leq n$$

  x è scomponibile in fattori primi.
- Passo induttivo : vogliamo dimostrare che la proprietà è verificata per $n+1$.

  Distinguiamo in 2 casi

  1. $n+1$ è primo allora $n+1$ è scomponibile in fattori primi, la scomposizione è data dal numero stesso.

2. $n+1$ non è primo allora

$$\exists y, z \in \mathbb{N} \ni' \ n+1 = y \cdot 2 \text{ con} y, z \neq 1 \wedge y, z \neq n+1$$

Quindi $2 \leq y \leq n \wedge 2 \leq z \leq n$.
Cioè per l'ipotesi induttiva y e z sono scomponibili in fattori primi e quindi $n+1 = y \cdot z = \underbrace{y_1 \cdot y_k \cdot z_1 \cdot 2h}_{\text{primi}}$

ho trovato una scomposizione $n+1$ in fattori primi.

Esempio 5.4. Dimostrare per induzione forte :

$$u_1 = 3, \ u_2 = 5 \ U_{n+1} = 3u_n - 2u_{n-1}$$

$$u_n = 2^n + 1$$

- Caso base 1: sia $n = 1$
$$u_1 = 2 + 1 = 3$$

- Caso base 2:
$$u_2 = 2^2 + 1$$

- Ipotesi induttiva: Sia $k \in \mathbb{N}^+$ e $k > 2$, assumiamo che sia vero per $r = 1 \dots k$

$$u_r = 2^r + 1$$

- Passo induttivo verifico che l'enunciato sia vero per $k+1$

$$u_{k+1} = 3u_k - 2u_{k-1}$$

Per ipotesi induttiva :

$$3 \cdot \big(2^k + 1\big) - 2(2; k-1+1)$$

$$= 3 \cdot 2^k + 3$$

$$= 2^{k+2}$$

$$3 \cdot 2^k + 3 - 2^k - 2$$

$$= 2^k\big((3 \cdot 1) - 1\big) + (3 - 2)$$

$$= 2^k \cdot 2 + 1$$

=

$$2^{k+1} + 1$$

□

5.2 Ricorsione

La **ricorsione** è uno strumento fondamentale in matematica discreta e informatica, utilizzato per definire funzioni, algoritmi o strutture in termini di se stessi. Si basa sull'idea di scomporre un problema complesso in sottoproblemi più semplici, risolti applicando ripetutamente lo stesso principio.

5.2.1 Struttura di una Definizione Ricorsiva

Una definizione ricorsiva si compone di due parti principali:

- **Caso base:** Specifica il valore o il comportamento della funzione per un caso elementare, che termina la ricorsione.
- **Passo ricorsivo:** Definisce il caso generale esprimendo il valore della funzione in termini dei valori precedenti.

5.2.2 Dimostrazioni di Correttezza

Nella matematica discreta, la ricorsione è strettamente collegata al principio di induzione. Per dimostrare la correttezza di una definizione o algoritmo ricorsivo, è sufficiente verificare:

1. **Correttezza del caso base:** Dimostrare che l'algoritmo produce il risultato corretto per il caso iniziale.
2. **Correttezza del passo ricorsivo:** Supponendo che l'algoritmo sia corretto per un caso generico n, dimostrare che è corretto anche per il caso successivo $n+1$ (o $n-1$, a seconda del contesto).

Esempio 5.5. Funzione potenza di 2 $f(n) = 2^n$
la funzione è definita come segue :

$$f : \mathbb{N} \to \mathbb{N}$$

$$2^n = 2^0 \cdot 2^1 \cdot 2^2 \ldots \cdot 2^n$$

$$f(n) = \begin{cases} 1 \text{ se } n = 0 \\ 2 \cdot f(n-1) \text{ se } n > 0 \end{cases}$$

```
1    int pow(int n){
2        if(n<0)
3            printf(" Non è un numero naturale");
4        if(n == 0 ) // caso base
5            return 1;
6        else
7            return 2 * pow(n-1); // passo ricorsivo
8    }
```

Dimostrazione 5.1. Dimostrazione per induzione su n, voglio dimostrare che pow(n) termina e restituisce 2^n $\forall n \in \mathbb{N}$

- Caso base: sia $n = 0$ allora pow(n) $= 1$, cioè pow(0) $= 2^0$.

- Ipotesi induttiva: sia $n > 0$ e supponiamo che n sia coretta per $n = n - 1$, cioè pow($n - 1$) termina e restituisce 2^{n-1}.

- Passo induttivo: dimostro che la funzione è corretta anche per n cioè pow(n)

$$\text{pow}(n) = 2 \cdot \text{pow}(n-1)$$

  per ipotesi induttiva:

$$2 \cdot 2^{n-1} = 2^n$$

  Pow n termina perchè per ipotesi induttiva pow($n - 1$) termina e la moltiplicazione tra 2 numeri termina sempre.

Esempio 5.6. Funzione fattoriale $f(n) = n!$

La funzione è definita come segue:

$$f : \mathbb{N}^+ \to \mathbb{N}$$

$$f(n) = \prod_{i=1}^{n} i = 1 \cdot 2 \cdot 3 \cdot \ldots \cdot n$$

$$\begin{cases} 1 \text{ se } n = 0, 1 \\ n \cdot f(n-1) \text{ se } n > 1 \end{cases}$$

```
int fact (int n){
    if(n<0)
        printf("non è un numero naturale");

    if(n<2)
        return 1;
    else
        return n * fact(n-1);
}
```

Dimostrazione 5.2. Voglio dimostrare che la funzione fact(n) termina e restituisce il valore di $n!$

- Caso base: Sia $n = 0$. Allora la funzione `fact(n)` restituisce 1, che corrisponde a 0!, e termina.
- Passo induttivo: Sia $n > 0$. Supponiamo la seguente ipotesi induttiva:

  `fact(n-1)` termina e restituisce il valore di $(n-1)!$.

  Dimostriamo che anche `fact(n)` termina e restituisce il valore di $n!$. Infatti:

  $$\texttt{fact(n)} = n \cdot \texttt{fact(n-1)} \quad \text{(per il ramo } \texttt{else}\text{)}.$$

  Per ipotesi induttiva, sappiamo che:

  $$\texttt{fact(n-1)} = (n-1)!.$$

  Quindi:

  $$\texttt{fact(n)} = n \cdot (n-1)! = n!$$

  (dove l'ultima uguaglianza segue dalle regole dell'algebra).
- Terminazione: La terminazione segue dal fatto che:
  - `fact(n-1)` termina per ipotesi induttiva.
  - L'operazione di moltiplicazione tra due numeri naturali termina sempre.

Funzione fattoriale iterativa :

```
int fact(n){
    if(n<0)
        printf(" non è un numero naturale");
    int prod = 1;
    for(int i = 1; i <= n; i++)
        prod *=i;
    return prod;
}
```

Esempio 5.7. I numeri di Fibonacci

Consideriamo un problema riguardante la riproduzione di conigli. Supponiamo che una coppia di conigli raggiunga la maturità e inizi a riprodursi dopo 2 mesi. A partire da quel momento, la coppia si riproduce ogni mese, dando vita a una nuova coppia di conigli.

Definiamo F_n come il numero di coppie di conigli presenti dopo n mesi. Inizialmente, abbiamo $F_0 = 1$ e $F_1 = 1$.

La domanda che ci poniamo è: quante coppie di conigli si avranno dopo n mesi?

Per risolvere questo problema, dobbiamo analizzare come evolve la popolazione di conigli mese per mese, tenendo conto del tempo di maturazione e del tasso di riproduzione delle coppie mature. Al mese $n > 1$ le coppie di conigli si possono partizionare in 2 gruppi:

- le coppie al mese $n - 1$.
- le coppie appena nate che sono tante quante le coppie di 2 mesi prima cioè $n - 2$.

Dunque:

$$F_n = F_{n-1} + F_{n-2}$$

$$F_n = \begin{cases} 1 \text{ se } n = 0, 1 \\ F_{n-1} + F_{n-2} \text{ se } n > 1 \end{cases}$$

```
1   int fib(int n){
2   if(n<0)
3       printf(" non è un numero naturale");
4   if(n<2)
5       return 1;
6   else
7       fib(n-1)+fib(n-2);
8   }
```

Dimostrazione 5.3. Voglio dimostrare che la funzione fib(n) termina e restituisce il valore fib($n-1$)+fib($n-2$).

- Caso base 1: Sia $n = 0$. Allora `fib(n)` restituisce 1 e termina.
- Caso base 2: Sia $n = 1$. Allora `fib(n)` restituisce 1 e termina.
- Passo induttivo: Sia $n > 1$. Supponiamo la seguente ipotesi induttiva:

  La funzione `fib(k)` termina e restituisce il valore corretto per tutti gli $k < n$.

La funzione `fib(n)` è definita come:

$$\texttt{fib(n)} = \texttt{fib(n-1)} + \texttt{fib(n-2)}.$$

Per ipotesi induttiva, sappiamo che:

`fib(n-1)` e `fib(n-2)` terminano e restituiscono valori corretti.

Quindi:

$$\texttt{fib(n)} = \texttt{fib(n-1)} + \texttt{fib(n-2)}.$$

Questo implica che `fib(n)` calcola correttamente il valore $F(n)$, e la funzione termina.

- Conclusione sulla terminazione: La terminazione segue dal fatto che:
  - `fib(n-1)` e `fib(n-2)` terminano per ipotesi induttiva.
  - L'operazione di somma tra due numeri naturali termina sempre.

```
1   int fib(int n) {
2   if (n == 0)
3       return 0;
4
5   if (n == 1)
6       return 1;
7
8   int prev1 = 1; // F(n-1)
9   int prev2 = 0; // F(n-2)
10  int current;
11
12  for (int i = 2; i <= n; i++) {
13      current = prev1 + prev2; // F(n) = F(n-1) + F(n-2)
14      prev2 = prev1; // Aggiorna F(n-2)
15      prev1 = current; // Aggiorna F(n-1)
16  }
17
18  return current;
19  }
```

Approfondimento

Esempio 5.8. Funzione di Binet **(sezione aurea)**

I greci cercarono di trovare un numero x tale che $x^2 = x + 1$. Questo numero si può trovare risolvendo l'equazione

$$x^2 - x - 1 = 0$$

la cui soluzione è:

$$x_{1,2} = \frac{1 \pm \sqrt{5}}{2}$$

Le 2 soluzioni costituiscono la sezione aurea Φ e il suo complemento Ψ.

Binet scoprì che possiamo utilizzare le costanti Φ e Ψ, per calcolare con una certa precisione i numeri di Fibonacci.

La funzione è definita come segue:

$$F : \mathbb{N}^+ \to \mathbb{N}$$

$$F(n) = \frac{1}{\sqrt{5}}\big(\Phi^n - \Psi^n\big)$$

La dimostrazione è per induzione su n

- Caso base : se $n = 1$

  $$F(1) = \frac{1}{\sqrt{5}}\big(\Phi - \Psi\big)$$

  Per la sezione aurea:

  $$= \frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2} - \frac{1-\sqrt{5}}{2}\right)$$

  $$= \frac{1}{\sqrt{5}}\frac{2\sqrt{5}}{2} = \frac{\sqrt{5}}{\sqrt{6}} = 1$$

  la base dell'induzione è verificata.

- Passo induttivo: Supponiamo la validità delle seguente ipotesi induttiva:

  $$\forall k \neq n-1,\ F_k = \frac{1}{\sqrt{5}}\big(\Phi^n - \Psi^n\big)$$

  Per definizione:

  $$F_n = F_{n-1} + F_{n-2}$$

  $$= \frac{1}{\sqrt{5}}\big(\Phi^{n-1} - \Psi^{n-1}\big) + \frac{1}{\sqrt{5}}\big(\Psi^{n-1} + \Phi^{n-2}\big)$$

  $$\frac{1}{\sqrt{5}}\left[\left(\Phi^{n-1} + \Phi^{n-2}\right) - \left(\Psi^{n-1} + \Psi^{n-2}\right)\right]$$

  La dimostrazione si conclude se riusciamo a dimostrare che

  $$\begin{cases} \Phi^n = \Phi^{n-1} + \Phi^{n-2} \\ \Psi^n = \Psi^{n-1} + \Psi^{n-2} \end{cases}$$

  Dividiamo la prima equazione per Φ^{n-2} e la seconda equazione per Ψ^{n-2}

  $$\begin{cases} \Phi^2 = \Phi + 1 \\ \Psi^2 = \Psi + 1 \end{cases}$$

5.3 Sommatorie

Definizione 5.3:

Le sommatorie rappresentano una notazione compatta per descrivere la somma di una sequenza di termini. La notazione generale è:

$$\sum_{i=0}^{n} a_i = a_1 + a_2 + a_3 \ldots + a_n$$

dove i è l'indice di somma, n è il limite superiore, ea_i rappresenta il termine generico. Le sommatorie sono utili per calcolare somme finite e per rappresentare concisamente formule complesse.

Il principio di induzione matematica è uno strumento potente per dimostrare proprietà relative alle sommatorie. Vediamone qualche esempio per capire come procedere:

Esempio 5.9. Dimostrazione per induzione della somma dei primi n numeri dispari
Vogliamo dimostrare la formula:

$$\sum_{i=1}^{n}(2i-1) = n^2.$$

- **Caso base:** Per $n = 1$, il primo numero dispari è 1. La somma è:

$$\sum_{i=1}^{1}(2i-1) = 2(1) - 1 = 1.$$

  D'altra parte, la formula n^2 dà:

$$1^2 = 1.$$

  Quindi, il caso base è verificato.

- **Ipotesi induttiva:** Supponiamo che la formula sia valida per $n = k$, ovvero:

$$\sum_{i=1}^{k}(2i-1) = k^2.$$

- **Passo induttivo:** Dimostriamo che la formula è valida per $n = k + 1$. La somma dei primi $k + 1$ numeri dispari è:

$$\sum_{i=1}^{k+1}(2i-1) = \sum_{i=1}^{k}(2i-1) + (2(k+1) - 1).$$

  Utilizzando l'ipotesi induttiva, sappiamo che:

$$\sum_{i=1}^{k}(2i-1) = k^2.$$

Quindi:

$$\sum_{i=1}^{k+1}(2i-1) = k^2 + (2(k+1)-1).$$

Sviluppiamo i calcoli:

$$\sum_{i=1}^{k+1}(2i-1) = k^2 + 2k + 2 - 1 = k^2 + 2k + 1.$$

Fattorizziamo:

$$\sum_{i=1}^{k+1}(2i-1) = (k+1)^2.$$

Quindi, la formula è verificata per $n = k+1$.

Per il principio di induzione, la formula:

$$\sum_{i=1}^{n}(2i-1) = n^2$$

è vera per ogni $n \in \mathbb{N}$.

Esempio 5.10. Dimostrare che $2^0 + 2^1 + 2 \ldots + 2^n = 2^{n+1} - 1$

$$\sum_{k=0}^{n} 2^k = 2^{n+1} - 1$$

- Caso base: Sia $n = 0$. La somma è:

$$\sum_{i=0}^{0} 2^i = 2^0 = 1.$$

D'altra parte, la formula $2^{n+1} - 1$ dà:

$$2^{0+1} - 1 = 2^1 - 1 = 1.$$

Quindi, il caso base è verificato.

- Ipotesi induttiva: Supponiamo che la formula sia vera per $n = k$, ovvero:

$$\sum_{i=0}^{k} 2^i = 2^{k+1} - 1.$$

- Passo induttivo: Dimostriamo che la formula è vera per $n = k+1$. La somma dei primi $k+1$ termini è:

$$\sum_{i=0}^{k+1} 2^i = \sum_{i=0}^{k} 2^i + 2^{k+1}.$$

Utilizzando l'ipotesi induttiva, sappiamo che:

$$\sum_{i=0}^{k} 2^i = 2^{k+1} - 1.$$

Sostituendo nella somma:

$$\sum_{i=0}^{k+1} 2^i = (2^{k+1} - 1) + 2^{k+1}.$$

Semplificando:

$$\sum_{i=0}^{k+1} 2^i = 2^{k+1} + 2^{k+1} - 1 = 2 \cdot 2^{k+1} - 1 = 2^{k+2} - 1.$$

Quindi la formula è verificata per $n = k + 1$.

Conclusione

Per il principio di induzione, la formula:

$$\sum_{i=0}^{n} 2^i = 2^{n+1} - 1$$

è vera per ogni $n \in \mathbb{N}$.

5.3.1 Proprietà delle sommatorie

Le sommatorie godono di alcune proprietà, andiamo ad enunciarle:

- Proprietà distributiva : Da una somma si possono "portare fuori" le costanti, ossia le espressioni che non dipendono dall'indice

$$\sum_{i=0}^{n} ca_k = c \sum_{i=0}^{n} a_k$$

- Proprietà associativa: permette di spezzare una somma in due o di riunire due somme in una:

$$\sum_{i=0}^{n} \big(a_k + b_k\big) = \sum_{i=0}^{n} a_k + \sum_{i=0}^{n} bk$$

- Proprietà commutativa : L'ordine con cui si sommano i termini può essere cambiato e la somma resta la stessa. Sia p una permutazione definita su tutti i numeri interi (ossia una funzione biiettiva p di $\mathbb{Z}$ in $\mathbb{Z}$)

$$\sum_{i=1}^{n} a_i = \sum_{i=1}^{n} a_{p(i)}$$

5.3.2 Some notevoli

Le somme notevoli sono formule matematiche che offrono soluzioni chiuse per la somma di termini sequenziali specifici. Queste formule sono fondamentali in molte applicazioni matematiche, statistiche e ingegneristiche poiché permettono di calcolare rapidamente la somma di serie numeriche senza dover calcolare singolarmente ogni termine.

Ecco alcune delle somme notevoli più comuni:

- Somma dei primi n numeri naturali:

$$\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$$

- Somma dei quadrati dei primi n numeri naturali:

$$\sum_{i=1}^{n} i^2 = \frac{n(n+1)(2n+1)}{6}$$

Ora procederemo a dimostrare per induzione le somme notevoli:

1. Somma dei Numeri Consecutivi:

   Dobbiamo Dimostrare che:

$$\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$$

   - Caso base: sia $n = 1$

$$\sum_{i=1}^{1} i = 1 = \frac{1(1+1)}{2} = 1$$

   - Ipotesi di induzione: Assumiamo che:

$$\sum_{i=1}^{k} i = \frac{k(k+1)}{2}$$

   - Passo induttivo: Dimostrare per $n = k + 1$:

$$\sum_{i=1}^{k+1} i = \sum_{i=1}^{k} i + (k+1) = \frac{k(k+1)}{2} + (k+1)$$

$$= \frac{k(k+1) + 2(k+1)}{2} = \frac{(k+1)(k+2)}{2}$$

2. Somma dei Quadrati Consecutivi:

   Dobbiamo Dimostrare che:

$$\sum_{i=1}^{n} i^2 = \frac{n(n+1)(2n+1)}{6}$$

- Caso base: sia $n = 1$:

$$\sum_{i=1}^{1} i^2 = 1^2 = 1 = \frac{1(1+1)(2\times 1+1)}{6} = 1$$

- Ipotesi di induzione: Assumiamo che:

$$\sum_{i=1}^{k} i^2 = \frac{k(k+1)(2k+1)}{6}$$

- Passo induttivo: Dimostrare per $n = k + 1$:

$$\sum_{i=1}^{k+1} i^2 = \sum_{i=1}^{k} i^2 + (k+1)^2 = \frac{k(k+1)(2k+1)}{6} + (k+1)^2$$

$$= \frac{k(k+1)(2k+1) + 6(k+1)^2}{6} = \frac{(k+1)(k(2k+1) + 6(k+1))}{6}$$

$$= \frac{(k+1)(2k^2+7k+6)}{6} = \frac{(k+1)(k+2)(2k+3)}{6}$$

Esempio 5.11. Calcolare la seguente sommatoria:

$$\sum_{k=1}^{n} k\big(k+1\big) = \sum_{k=1}^{n} k^2 + k = \sum_{k=1}^{n} k^2 + \sum_{k=1}^{n} +k$$

$$= \frac{n(n+1)(2n+1)}{6} + \frac{n(n+1)(n+2))}{2}$$

$$= \frac{n(n+1)(2n+1)3(n(n+1))}{6} = \frac{n(n+1) + (2n+4)}{6}$$

$$= \frac{\not{2}(n(n+1)(n+2)}{\not{6}\ 3} = \frac{n(n+1)(n+2)}{3}$$

5.3.3 Somme multiple

Definizione 5.4:

Le somme multiple sono un'estensione del concetto di sommatoria e coinvolgono l'esecuzione di sommatorie su più variabili, spesso su insiemi multidimensionali. Consideriamo la notazione e la definizione delle somme multiple, tipicamente viste nelle matrici o in altri contesti in cui più indici sono usati.
Notazione di somma multipla:
Supponiamo di avere una funzione $f(i, j)$ definita su una griglia di indici i e j che variano su certi insiemi. Le somme multiple utilizzano la sommatoria doppia o, più in generale, la sommatoria multipla. La doppia sommatoria si esprime come:

$$\sum_{i=a}^{b}\sum_{j=c}^{d} f(i,j)$$

Interpretazione: Ordine delle sommatorie: La somma interna (rispetto a j) viene eseguita per ogni valore fisso di i. Dopo aver calcolato la somma interna per un dato , si procede alla somma esterna (rispetto a i).

$$\sum_{i=1}^{m}\sum_{j=1}^{n} A_{i,j}$$

Estensione a Somme Multiple: Questo concetto può essere esteso a più indici.

$$\sum_{i=a}^{b}\sum_{j=c}^{d}\sum_{k=e}^{f} f(i,j,k)$$

Esempio 5.12. Calcolare il valore, espresso in funzione di n, della seguente sommatoria:

$$\sum_{k=1}^{n}\sum_{i=1}^{k} 6i$$

$$\sum_{k=1}^{n}\sum_{i=1}^{k} 6i = \sum_{k=1}^{n} 6\sum_{i=1}^{k} i$$

Calcoliamo la somma interna:

$$\sum_{i=1}^{k} i = \frac{k(k+1)}{2}$$

Quindi, abbiamo:

$$\sum_{k=1}^{n} 6 \cdot \frac{k(k+1)}{2} = \sum_{k=1}^{n} 3(k^2+k)$$

$$= 3\left(\sum_{k=1}^{n} k^2 + \sum_{k=1}^{n} k\right)$$

Usiamo le formule per le somme notevoli:

$$\sum_{k=1}^{n} k^2 = \frac{n(n+1)(2n+1)}{6}$$

$$\sum_{k=1}^{n} k = \frac{n(n+1)}{2}$$

Quindi:

$$= 3\left(\frac{n(n+1)(2n+1)}{6} + \frac{n(n+1)}{2}\right)$$

$$= \frac{3}{2}\left(\frac{n(n+1)(2n+1)}{3} + n(n+1)\right)$$

$$= \frac{3}{2}\left(\frac{n(n+1)(2n+1) + 3n(n+1)}{3}\right)$$

$$= \frac{3}{2} \cdot \frac{n(n+1)(2n+3)}{3}$$

$$= \frac{n(n+1)(2n+3)}{2}$$

Capitolo 6

Teoria dei numeri

6.1 Divisione

Definizione 6.1:

Se a e b sono numeri interi con $a \neq 0$, si dice che a divide b se esiste un intero c tale che $b = ac$. Quando a divide b, si dice che a è un divisore di b e che b è un multiplo di a. La notazione $a \mid b$ indica che a divide b. Si scrive $a \nmid b$ quando a non divide b.

Esempio 6.1. Siano n e d due numeri interi positivi. Quanti interi positivi non superiori a n sono divisibili per d?

Gli interi positivi divisibili per d sono tutti gli interi della forma dk, dove k è un intero positivo. Pertanto, il numero di interi positivi divisibili per d che non sono maggiori di n corrisponde al numero di interi k tali che $0 \leq dk \leq n$, o che $0 \leq k \leq \dfrac{n}{d}$. Quindi, ci sono $\lfloor \frac{n}{d} \rfloor$ interi positivi non superiori a n che sono divisibili per d.

Teorema 6.1:

Siano a, b, e c interi, con $a \neq 0$. Allora:

- se $a \mid b$ e $a \mid c$, allora $a \mid (b + c)$;
- se $a \mid b$, allora $a \mid bc$ per ogni intero c;
- se $a \mid b$ e $b \mid c$, allora $a \mid c$.

Corollario 6.1:

Siano a, b, e c interi, con $a \neq 0$, tali che $a \mid b$ e $a \mid c$. Allora $a \mid (mb + nc)$ per ogni m e n interi.

6.1.1 Divisione euclidea

Teorema 6.2:

Per ogni coppia di numeri interi a e b con $b \neq 0$ esiste un'unica coppia di interi q e r tali che

$$a = bq + r$$

Con $0 \leq r \leq |b|$, dove $|b|$ è il valore assoluto di b. Dove :

- a è il dividendo;
- b è il divisore;
- q è il quoziente;
- r è il resto.

Dimostrazione 6.1. Dimostriamo prima che gli interi q ed r esistano e poi proviamo che sono unici. Osserviamo che è sufficiente dimostrare il teorema nel caso $a \geq 0$ e $b > 0$. Infatti,

- se $b < 0$ allora $b = -b'$ e $a = (-b')q + r$ quindi $a = b'(-q) + r$ con $b' > 0$
- se $a < 0$ allora $a = -a'$ e "a diviso b" è uguale a "a' diviso-b" con $a' > 0$

Assumiamo dunque $a \geq 0$ e $b > 0$. Procediamo per induzione su a.

- Caso base: se $a = 0$ basta prendere $q = r = 0$.
- Ipotesi induttiva: sia $a > 0$. Supponiamo che la proprietà sia vera per tutti gli interi $a' < a$ e proviamo che la proprietà è vera per a.

Distinguiamo due casi:

- Se $a < b$, allora è sufficiente prendere $q = 0$ e $r = a$ (con $0 \leq r < |b|$).
- Se $a \geq b$, allora, per ipotesi induttiva, la proprietà è vera per i numeri $(a - b)$ e b, ossia esistono q' e r' tali che $(a - b) = bq' + r'$ con $0 \leq r' < |b|$. Allora:

$$a = b(q' + 1) + r'.$$

Unicità di q e r: Dimostriamo ora che q ed r sono unici. Supponiamo che valgano $a = bq + r$ e $a = bq' + r'$ con $0 \leq r, r' < |b|$. Sottraendo membro a membro, si ottiene:

$$b(q - q') = (r' - r).$$

Dalla relazione $0 \leq r, r' < |b|$, si ha $|r' - r| < |b|$. Pertanto:

$$|b||q - q'| = |r' - r| \quad \text{e dunque} \quad |q - q'| < 1.$$

Dato che q e q' sono interi, segue che $q - q' = 0$, cioè $q = q'$. Inoltre, anche $r' - r = 0$, ossia $r = r'$. Quindi, q ed r sono unici.

Esempio 6.2. Siano $a = 17$ e $b = -3$. Allora

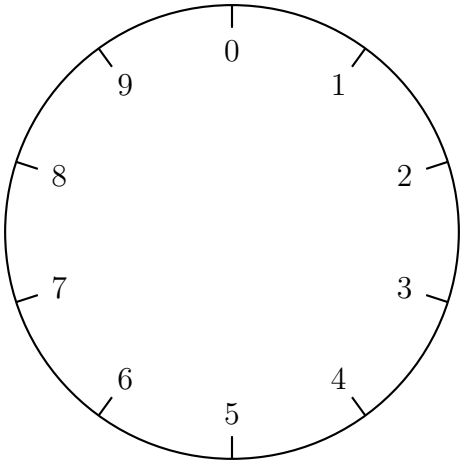
$$17 = (-3) \cdot (-5) + 2$$

Esempio 6.3. Siano $a = -17$ e $b = -3$. Allora

$$-17 = (-3) \cdot (6) + 1$$

6.2 Aritmetica dell'orologio

L'aritmetica modulare è stata introdotta da Carl Friedrich Gauss all'inizio dell'800. Questa aritmetica si basa su un comportamento ciclico, che possiamo visualizzare usando un orologio con $n > 0$ tacche, rappresentanti i numeri da 0 a $n - 1$.



Definizione 6.2:

l'insieme $\mathbb{Z}_n$ è definito come:

$$\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}$$

Su questo insieme, l'operazione di somma e sottrazione è modulare, ovvero rispetta la ciclicità definita dal modulo n.

Scorrimento in senso orario (+1)

- Una mossa +1 consiste nello spostarsi dalla tacca corrente alla successiva in senso orario. Questa operazione corrisponde all'aggiunta di 1:

$$x + 1 \mod n.$$

- Caso speciale: Quando si raggiunge la tacca $n - 1$ e si esegue una mossa +1, si torna a 0:

$$(n-1) + 1 \equiv 0 \pmod{n}.$$

Contrariamente ai numeri naturali, nell'aritmetica modulare il numero 0 è il successore di $n - 1$.

La funzione determinata dalle mosse +1 è una funzione biiettiva:

$$f : \mathbb{Z}_n \to \mathbb{Z}_n.$$

Scorrimento in senso antiorario (-1)

- Una mossa -1 consiste nello spostarsi dalla tacca corrente alla precedente in senso antiorario. Questa operazione corrisponde alla sottrazione di 1:

$$x - 1 \mod n.$$

- Caso speciale:Quando si arriva alla tacca 0 e si esegue una mossa -1, si passa a $n - 1$:

$$0 - 1 \equiv n - 1 \pmod{n}.$$

  Il numero $n - 1$ è il predecessore di 0.

In entrambi i casi, la tacca corrispondente rappresenta il resto della divisione di a per n, che è un numero nell'intervallo $[0, n - 1]$. Questo resto si scrive come:

$$a \mod n \quad \text{oppure} \quad \mod_n(a).$$

Esempio 6.4. Consideriamo l'insieme $\mathbb{Z}_{10} = \{0, 1, 2, \ldots, 9\}$, ovvero un orologio con $n = 10$ tacche. In questo sistema:

- Una mossa 1 corrisponde a spostarsi in senso orario di una tacca.
- Una mossa -1 corrisponde a spostarsi in senso antiorario di una tacca.
- Se si supera il numero 9 (o 0 in senso antiorario), si torna a 0 (o 9 rispettivamente) grazie alla ciclicità del modulo.
- Partendo da 7, eseguendo $+1$, si ottiene 8: $7 + 1 = 8$.
- Partendo da 7, eseguendo -1, si ottiene 6: $7 - 1 = 6$.
- Partendo da 9, eseguendo $+1$, si torna a 0: $8 + 1 \equiv 0 \pmod{10}$.
- Partendo da 2, eseguendo $+1$, si ottiene 3: $2 + 1 = 3$.
- Partendo da 2, eseguendo -1, si ottiene 1: $2 - 1 = 1$.

Definizione 6.3:

Siano a e n due numeri interi, con $n > 1$. Il residuo di a modulo n indicato come $a \mod n$, è il resto non negativo ottenuto quando a viene diviso per n. L'insieme dei numeri $\{0, 1, 2, \ldots, n-1\}$ è chiamato insieme completo dei residui modulo n, è il resto non negativo ottenuto quando a viene diviso per n.
L'insieme dei numeri $\{0, 1, 2, \ldots, n-1\}$ è chiamato insieme completo dei residui modulo n.
Ridurre un numero modulo n significa calcolarne il residuo modulo n. Quando un modulo $n > 1$ è fisso in un contesto e un intero a è dato, spesso omettiamo l'espressione "modulo n" e ci riferiamo semplicemente al residuo di a.

Somma e prodotto modulo n: Definiamo la somma $(+_n)$ e il prodotto $(\cdot_n)$ modulo n sui numeri interi come segue: Siano $a, b \in \mathbb{Z}$:

$$a +_n b = (a + b) \mod n,$$

$$a \cdot_n b = (a \cdot b) \mod n.$$

Il risultato della somma e del prodotto modulo n è sempre un valore compreso tra 0 e $n-1$, quindi rappresentabile in un orologio con n tacche. **??** Per ogni $a, b \in \mathbb{Z}$, valgono:

$$(a + b) \mod n = \big((a \mod n) + (b \mod n)\big) \mod n,$$

$$(a \cdot b) \mod n = \big((a \mod n) \cdot (b \mod n)\big) \mod n.$$

Teorema 6.3:

L'insieme $\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}$, con le operazioni di somma $(+_n)$ e prodotto $(\cdot_n)$, è chiuso rispetto a queste operazioni. In altre parole, per ogni $a, b \in \mathbb{Z}_n$, vale:

$$a +_n b \in \mathbb{Z}_n, \quad a \cdot_n b \in \mathbb{Z}_n.$$

Definizione 6.4:

Sia $n > 0$, $n \in \mathbb{N}$. Consideriamo la relazione $\mathcal{R}$ definita su $\mathbb{Z}$ come:

$$a \mathcal{R} b \iff \text{il resto della divisione di}$$

a per n è uguale al resto della divisione di b per n. In altre parole, $a \,\mathcal{R}\, b \iff a \equiv b \pmod{n}$, dove $a \equiv b \pmod{n}$ significa che $n \mid (a - b)$.

Esempio 6.5. vediamo degli esempi di alcune congruenze:

1. $12 \equiv_{10} 2$: infatti

$$12 = 10 \cdot 1 + 2 \quad \text{e} \quad 2 = 10 \cdot 0 + 2 \quad (\text{resto } 2).$$

2. $-8 \equiv_{10} 2$: infatti

$$-8 = 10 \cdot (-1) + 2 \quad \text{e} \quad 2 = 10 \cdot 0 + 2 \quad (\text{resto } 2).$$

3. $20 \equiv_5 5$: infatti

$$20 = 5 \cdot 4 + 0 \quad \text{e} \quad 5 = 5 \cdot 1 + 0 \quad (\text{resto } 0).$$

4. $5 \equiv_5 15$: infatti

$$5 = 5 \cdot 1 + 0 \quad \text{e} \quad 15 = 5 \cdot 3 + 0 \quad (\text{resto } 0).$$

5. $15 \equiv_5 0$: infatti

$$15 = 5 \cdot 3 + 0 \quad \text{e} \quad 0 = 5 \cdot 0 + 0 \quad \text{(resto 0)}.$$

6. $2 \equiv_8 -6$: infatti

$$2 = 8 \cdot 0 + 2 \quad \text{e} \quad -6 = 8 \cdot (-1) + 2 \quad \text{(resto 2)}.$$

Teorema 6.4:

Sia n un intero con $n > 1$. La congruenza modulo n è una relazione di equivalenza sull'insieme degli interi $\mathbb{Z}$.
Le classi di equivalenza distinte della relazione sono i sottoinsiemi:

$$[0], [1], [2], \ldots, [n-1],$$

dove, per ogni $a \in \{0, 1, 2, \ldots, n-1\}$:

$$[a] = \{m \in \mathbb{Z} \mid m \equiv a \pmod{n}\}.$$

Equivalentemente, possiamo scrivere:

$$[a] = \{m \in \mathbb{Z} \mid m = a + kn, \text{ con } k \in \mathbb{Z}\}.$$

Dimostrazione 6.2. Sia n un intero con $n > 1$. Dimostreremo che la congruenza modulo n è una relazione di equivalenza sull'insieme degli interi $\mathbb{Z}$. Mostreremo che è riflessiva, simmetrica e transitiva. Inoltre, identificheremo le classi di equivalenza distinte.

- Riflessiva: Supponiamo che a sia un intero qualsiasi. Per dimostrare che $a \equiv a \pmod{n}$, dobbiamo dimostrare che $n \mid (a - a)$. Ma:

  $$a - a = 0$$

  e $n \mid 0$ poiché $0 = n \cdot 0$. Pertanto, $a \equiv a \pmod{n}$.

- Simmetrica: Supponiamo che a, b siano interi tali che $a \equiv b \pmod{n}$. Ciò significa che $n \mid (a - b)$, quindi esiste un intero k tale che:

  $$a - b = nk.$$

  Moltiplicando entrambi i membri per -1, otteniamo:

  $$-(a - b) = -nk \implies b - a = n(-k).$$

  Poiché $n \mid (b - a)$, segue che $b \equiv a \pmod{n}$.

- Transitiva: Supponiamo che $a \equiv b \pmod{n}$ e $b \equiv c \pmod{n}$. Ciò implica che $n \mid (a - b)$ e $n \mid (b - c)$. Allora esistono interi k_1 e k_2 tali che:

  $$a - b = nk_1 \quad \text{e} \quad b - c = nk_2.$$

Sommando le due equazioni otteniamo:

$$(a-b)+(b-c) = nk_1 + nk_2 \implies a - c = n(k_1 + k_2).$$

Poiché $n \mid (a-c)$, segue che $a \equiv c \pmod{n}$.

Le classi di equivalenza distinte della relazione sono i sottoinsiemi:

$$[0], [1], [2], \ldots, [n-1],$$

dove, per ogni $a \in \{0, 1, 2, \ldots, n-1\}$:

$$[a] = \{m \in \mathbb{Z} \mid m \equiv a \pmod{n}\}.$$

□

Esempio 6.6. Calcolare il resto della divisione 95758 per 5.
È noto che $10 \equiv_5 0$ quindi riscriviamo 95758 nel seguente modo:

$$95758 = 8 + 5 \cdot 10 + 7 \cdot 10^2 + 5 \cdot 10^3 + 9 \cdot 10^4$$

$$\equiv_5 8 + 5 \cdot (10 \mod 5) + 7 \cdot (10 \mod 5)^2 + 5 \cdot (10 \mod 5)^3 + 9(10 \mod 5)^4$$

$$\equiv_5 8$$

$$\equiv_5 3$$

Quindi il resto della divisione di 95758 per 5 è 3.

Esempio 6.7. Calcolare $3^{128} \mod 7$ Poiché $3^3 = 27 \equiv_7 -1$, dunque abbiamo:

$$3^{128} = (3^3)^{42} * 3^2 \equiv_7 (-1)^{42} \cdot 3^2 = 3^2 \equiv_7 2$$

Pertanto $3^{128} \mod 7$ è uguale a 2.

6.3 Massimo comune divisore

Definizione 6.5:

Dati due interi a e b, resta definito l'insieme dei loro divisori comuni. Il massimo fra i divisori comuni a e b è detto massimo comune divisore ed è denotato con $MCD(a, b)$. Due numeri per i quali il massimo comun divisore è 1 si dicono relativamente primi o coprimi.
Per convenienza, si definisce $MCD(a, 0) = a \ \forall a \in \mathbb{Z}$.

Algoritmo di Euclide per il MCD: Siano a, b due interi positivi con $a > b$. L'algoritmo di Euclide calcola il massimo comun divisore (MCD) di a e b attraverso i seguenti passi iterativi:

1. Si divide il maggiore dei due numeri per il minore.
2. Si sostituisce il maggiore con il minore.
3. Si sostituisce il minore con il resto della divisione.
4. Si ripete il processo fino a quando il resto non diventa 0.
5. Quando il resto è 0, il valore del minore è il MCD.

Esempio 6.8. Calcoliamo MCD$(300, 18)$ applicando l'algoritmo:

$$\begin{aligned} 300 &= 18 \cdot 16 + 12 && \Rightarrow \text{Iterazione successiva: } a = 18, b = 12, \\ 18 &= 12 \cdot 1 + 6 && \Rightarrow \text{Iterazione successiva: } a = 12, b = 6, \\ 12 &= 6 \cdot 2 + 0 && \Rightarrow \text{Restituisce: } \mathrm{MCD}(300, 18) = 6. \end{aligned}$$

Ora vedremo la versione iterativa dell'algoritmo di Euclide:

```
1   int MCD(int a, int b){
2       if(b>a)
3           swap(a,b);
4       while(b!=0){
5           int r = a%b;
6           a=b;
7           b=r;
8       }
9       return a;
10  }
```

Dimostrazione 6.3. Siano $a > 0$, $b > 0$ con $a > b$. Dimostriamo che l'algoritmo di Euclide termina sempre. Chiamiamo a_i, b_i, r_i i valori di a, b, e del resto r all'iterazione i-esima ($i \geq 0$), ossia dopo aver eseguito il test $b \neq 0$. Abbiamo:

$$r_1 = a_0 \mod b_0, \quad a_1 = b_0, \quad b_1 = r_1.$$

In generale:

$$r_i = a_{i-1} \mod b_{i-1}, \quad a_i = b_{i-1}, \quad b_i = r_i.$$

Osserviamo che ad ogni iterazione il resto r_i decresce di almeno un'unità rispetto all'iterazione precedente. Infatti:

$$r_i = a_{i-1} \mod b_{i-1} < b_{i-1} = r_{i-1}.$$

Poiché il resto è sempre non negativo ($r_i \geq 0$), il ciclo non può ripetersi all'infinito. Quindi, esiste un'iterazione k tale che:

$$r_k = 0.$$

Lemma 1:

Indichiamo con C_i l'insieme dei divisori comuni di a_i e b_i. Dimostriamo che, per ogni coppia di iterazioni successive, vale:

$$C_i = C_{i-1}.$$

Dimostrazione 6.4. ($\subseteq$ ia $c \in C_{i-1}$, cioè $c \mid a_{i-1}$ e $c \mid b_{i-1}$. Dimostriamo che $c \in C_i$, cioè $c \mid a_i$ e $c \mid b_i$.

Abbiamo:

$$a_i = b_{i-1}, \quad b_i = r_i.$$

Poiché $c \mid a_{i-1}$ e $c \mid b_{i-1}$, dobbiamo dimostrare che $c \mid b_i$. Ricordiamo che:

$$a_{i-1} = qb_{i-1} + r_i,$$

da cui:

$$r_i = a_{i-1} - qb_{i-1}.$$

Poiché $c \mid a_{i-1}$ e $c \mid b_{i-1}$, segue che:

$$c \mid r_i.$$

Quindi $c \in C_i$, e dunque $C_{i-1} \subseteq C_i$.

Abbiamo dimostrato che:

$$C_i = C_{i-1}.$$

Ad ogni iterazione, i divisori comuni di a_i e b_i rimangono invariati. Quando l'algoritmo termina, $b_k = 0$, e il risultato a_k è il massimo tra i divisori comuni di a_0 e b_0. Pertanto, l'algoritmo restituisce correttamente il MCD.

Per il Lemma precedentemente dimostrato, ad ogni iterazione dell'algoritmo i divisori comuni di a_i e b_i sono sempre i divisori comuni di a_0 e b_0, ossia a e b.

Poiché al termine dell'algoritmo il valore di b_i è zero, il valore di a_i restituito è certamente il massimo comune divisore di a_i e b_i. Di conseguenza, il risultato finale è il massimo comune divisore di a e b:

$$\text{MCD}(a, b) = a_i \quad \text{per qualche } i \geq 0.$$

Numero di Iterazioni: Abbiamo dimostrato che l'algoritmo di Euclide termina sempre. Analizziamo ora il numero di iterazioni necessarie per la sua terminazione.

Limite sul Numero di Iterazioni

Indichiamo con T il numero totale di iterazioni dell'algoritmo. Si dimostra che:

$$T \leq 2\lceil \log_2 b \rceil + 1,$$

dove b è il valore iniziale del secondo parametro dell'algoritmo. Questo implica che il numero di iterazioni è proporzionale al logaritmo in base 2 di b.

Relazione con i Numeri di Fibonacci

Si dimostra inoltre che se $T \geq k$, allora:

$$b > F_k,$$

dove F_k è il k-esimo numero di Fibonacci. Questa relazione implica che il numero di iterazioni cresce con il valore iniziale di b, ma è limitato dalla sequenza di Fibonacci.

Esempio 6.9. Calcoliamo MCD$(89, 55)$ applicando l'algoritmo di Euclide.

$$\begin{aligned}
89 &= 55 \cdot 1 + 34 && \Rightarrow \text{MCD}(89, 55) = \text{MCD}(55, 34),\\
55 &= 34 \cdot 1 + 21 && \Rightarrow \text{MCD}(55, 34) = \text{MCD}(34, 21),\\
34 &= 21 \cdot 1 + 13 && \Rightarrow \text{MCD}(34, 21) = \text{MCD}(21, 13),\\
21 &= 13 \cdot 1 + 8 && \Rightarrow \text{MCD}(21, 13) = \text{MCD}(13, 8),\\
13 &= 8 \cdot 1 + 5 && \Rightarrow \text{MCD}(13, 8) = \text{MCD}(8, 5),\\
8 &= 5 \cdot 1 + 3 && \Rightarrow \text{MCD}(8, 5) = \text{MCD}(5, 3),\\
5 &= 3 \cdot 1 + 2 && \Rightarrow \text{MCD}(5, 3) = \text{MCD}(3, 2),\\
3 &= 2 \cdot 1 + 1 && \Rightarrow \text{MCD}(3, 2) = \text{MCD}(2, 1),\\
2 &= 1 \cdot 2 + 0 && \Rightarrow \text{MCD}(2, 1) = 1.
\end{aligned}$$

Il massimo comune divisore di 89 e 55 è:

$$\text{MCD}(89, 55) = 1.$$

Teorema 6.5:

Siano a e b 2 numeri naturali diversi da 0 e sia $d = \text{MCD}(a, b)$. Allora esistono 2 numeri interi x e y tali che:

$$d = ax + by$$

L'equazione $\text{MCD}(a, b) = ax + by$, soddisfatte da opportune coppie di interi x e y, è detta identità di Bezout.

Esempio 6.10. Siano $a = 12$ e $b = 8$. Allora

Teorema 6.6:

Siano a,b e c numeri interi e sia $d = MCD(a, b)$. Allora l'equazione $c = ax+by$ ammette soluzioni intere se e solo se $d|c$ ovvero c'è un multiplo di $MCD(a, b)$. Se a e b sono coprimi, allora l'equazione $1 = ax+by$ e ammette sempre soluzioni intere.

Lemma 2:

Siano a, b e c numeri interi e n un numero naturale tali che c e n sono relativamente primi, cioè $MCD(c, n) = 1$. Allora $ac \equiv_n bc \implies a \equiv_n b$

Esempio 6.11. Trovare una soluzione intera dell'equazione:

$$240x + 36y = 12.$$

Dividiamo tutti i coefficienti per 12 e otteniamo:

$$20x + 3y = 1.$$

Poiché 20 e 3 sono relativamente primi ($\text{MCD}(20, 3) = 1$), esistono soluzioni intere dell'equazione $20x + 3y = 1$.

Si verifica facilmente che:

$$x = -1, \quad y = 7$$

è una soluzione di $20x + 3y = 1$. Moltiplicando x e y per 12, si ottiene che:

$$x = -1, \quad y = 7$$

è una soluzione di $240x + 36y = 12$.

Esempio 6.12. Trovare una soluzione intera dell'equazione:

$$120x + 81y = 12.$$

Dividiamo tutti i coefficienti per 3 e otteniamo:

$$40x + 27y = 4.$$

Poiché 40 e 27 sono relativamente primi ($\text{MCD}(40, 27) = 1$), esistono soluzioni intere dell'equazione $40x + 27y = 1$.

Applichiamo l'algoritmo di Euclide per trovare i coefficienti di Bézout:

$$40 = 27 \cdot 1 + 13, \quad 27 = 13 \cdot 2 + 1, \quad 13 = 1 \cdot 13 + 0.$$

Risolvendo a ritroso:

$$1 = 27 - 13 \cdot 2 = 27 - (40 - 27) \cdot 2 = 27 - 40 \cdot 2 + 27 \cdot 2 = 40(-2) + 27 \cdot 3.$$

Quindi una soluzione di $40x + 27y = 1$ è:

$$x = -2, \quad y = 3.$$

Moltiplicando x e y per 4, otteniamo una soluzione di $40x + 27y = 4$:

$$x = -8, \quad y = 12.$$

Le stesse soluzioni valgono per l'equazione $120x + 81y = 12$.

Esempio 6.13. Trovare una soluzione intera dell'equazione:

$$6x + 2y = 5.$$

Per il Teorema di Bézout generalizzato, non esistono soluzioni intere per l'equazione $6x + 2y = 5$, poiché:

$$\text{MCD}(6, 2) = 2 \quad \text{e} \quad 2 \nmid 5.$$

Pertanto, l'equazione è impossibile da soddisfare con numeri interi.

6.4 Inverso modulo n

Dati due interi a e n, un numero s è detto l'inverso di a modulo n se:

$$a \cdot s \equiv 1 \pmod{n}.$$

L'inverso modulo n esiste se, e solo se, $MCD(a, n) = 1$.

Esempio 6.14. Consideriamo la congruenza:

$$2x \equiv 3 \pmod{5}.$$

Osserviamo che $3 \cdot 2 = 6 \equiv 1 \pmod{5}$. Quindi, 3 è un inverso di 2 modulo 5. Moltiplicando entrambi i membri per 3, otteniamo:

$$6x \equiv 9 \pmod{5}.$$

Poiché $6 \equiv 1 \pmod{5}$, segue che:

$$x \equiv 4 \pmod{5}.$$

Verifica: $2 \cdot 4 = 8 \equiv 3 \pmod{5}$.

Esempio 6.15. Consideriamo $2x \equiv 1 \pmod{4}$. Calcoliamo i residui:

$$2 \cdot 1 \equiv 2 \pmod{4}, \quad 2 \cdot 2 \equiv 0 \pmod{4}, \quad 2 \cdot 3 \equiv 2 \pmod{4}.$$

Poiché $MCD(2, 4) \neq 1$, l'inverso modulo 4 non esiste.

Corollario 6.2:

Se $\gcd(a, n) = 1$, allora esiste un intero s tale che:

$$a \cdot s \equiv 1 \pmod{n}.$$

Dimostrazione: Dato che $MCD(a, n) = 1$, per il Teorema di Bézout esistono s e t tali che:

$$as + nt = 1.$$

Sottraendo nt, otteniamo:

$$as = 1 - nt \quad \Longrightarrow \quad as \equiv 1 \pmod{n}.$$

6.5 Numeri primi

Definizione 6.6:

Un numero naturale $p > 1$ si dice primo se è divisibile per 1 e per se stesso. I primi sono:

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43 \ldots$$

Se p non è primo allora si dice che è un numero composto $p = a \cdot b$ e $a, b \neq 1, p$.

Teorema 6.7:

Per ogni $k \geq 1$, esiste un blocco di k numeri naturali consecutivi tale che nessuno di essi è un numero primo.

Dimostrazione 6.5. Sia $n = k + 1$ Consideriamo i numeri:

$$n! + 2,\ n! + 3,\ n! + 4, \ldots n! + n$$

l primo di essi è divisibile per 2, il secondo 'è divisibile per 3, e così via fino all'ultimo che 'è divisibile per n. Quindi sono tutti numeri composti e ce ne sono $n - 1 = k$.

Esempio 6.16. Sia $k = 5$. Consideriamo i numeri

$$6! + 2,\ 6! + 3,\ 6! + 4,\ 6! + 5,\ 6! + 6$$

sono 5 numeri naturali consecutivi non primi.

Teorema 6.8:

Sia $\pi(N)$ il numero di numeri primi nell'intervallo $1, 2, \ldots, N$. Allora:

$$\pi(N) \sim \frac{N}{\ln N}$$

dove $\ln N$ rappresenta il logaritmo naturale di N.

6.5.1 Fattorizzazione

Definizione 6.7:

Sia $a \in \mathbb{N}$ e $n > 1$, n è sempre esprimibile in modo unico, come un prodotto di fattori primi.

Teorema 6.9:

Ogni numero naturale $n \geq 2$ è esprimibile come prodotto di un numero finito di fattori primi.

Esempio 6.17. $100 = 2^2 \cdot 5^2$

6.5.2 I numeri di Fermat

Definizione 6.8:

La funzione:

$$F(n) = 2^{2^n} + 1, \quad n \in \mathbb{N},$$

genera tutti i numeri di Fermat.

Proprietà dei numeri di Fermat

Non tutti i numeri di Fermat sono primi. Vediamo i valori di $F(n)$ per $n = 0, 1, 2, 3, 4, 5$:

$$\begin{aligned}
F(0) &= 2^{2^0} + 1 = 2^1 + 1 = 2 + 1 = 3 && \text{(primo)},\\
F(1) &= 2^{2^1} + 1 = 2^2 + 1 = 4 + 1 = 5 && \text{(primo)},\\
F(2) &= 2^{2^2} + 1 = 2^4 + 1 = 16 + 1 = 17 && \text{(primo)},\\
F(3) &= 2^{2^3} + 1 = 2^8 + 1 = 256 + 1 = 257 && \text{(primo)},\\
F(4) &= 2^{2^4} + 1 = 2^{16} + 1 = 65536 + 1 = 65537 && \text{(primo)},\\
F(5) &= 2^{2^5} + 1 = 2^{32} + 1 = 4294967297 = 641 \cdot 6700417 && \text{(non primo)}.
\end{aligned}$$

- Per $n = 0, 1, 2, 3, 4$, $F(n)$ genera numeri primi, detti "primi di Fermat".
- Per $n = 5$, $F(5) = 4294967297$ non è primo, ma è il prodotto di 641 e 6700417.
- Ad oggi, non sono noti primi di Fermat maggiori di $F(4)$.

6.5.3 Piccolo teorema di Fermat

Teorema 6.10:

Sia p un numero primo e a un intero tale che $p \nmid a$. Allora:

$$a^{p-1} \equiv 1 \pmod{p}.$$

Dimostrazione 6.6. Supponiamo che p sia un numero primo e a un intero tale che $p \nmid a$. Si osservi che $a \neq 0$, altrimenti p dividerebbe a, in contraddizione con l'ipotesi.

Consideriamo l'insieme:

$$S = \{a, 2a, 3a, \ldots, (p-1)a\}.$$

Affermiamo che nessun elemento di S è congruente modulo p a un altro. Supponiamo per assurdo che esistano s e r con $1 \leq r < s \leq p-1$ tali che:

$$sa \equiv ra \pmod{p}.$$

Allora, per definizione di congruenza modulo p:

$$p \mid (sa - ra), \quad \text{ovvero } p \mid (s - r)a.$$

Poiché $p \nmid a$ (ipotesi) e p è primo, segue che il massimo comun divisore $\gcd(a, p) = 1$. Per il lemma di Euclide, deduciamo che:

$$p \mid (s - r).$$

Ma ciò è impossibile, perché $0 < s - r < p$. Pertanto, tutti gli elementi di S sono distinti modulo p.

Consideriamo la funzione $F : S \to T$, dove:

$$T = \{1, 2, 3, \ldots, (p - 1)\}.$$

F associa ogni elemento di S al suo residuo modulo p. Dalla parte precedente, F è iniettiva. Perché F mappa un insieme finito S di $p - 1$ elementi in un altro insieme finito T con $p - 1$ elementi, segue che F è anche suriettiva.

Pertanto, i residui modulo p degli elementi di S sono esattamente $\{1, 2, 3, \ldots, (p-1)\}$.

Dunque possiamo scrivere:

$$a \cdot 2a \cdot 3a \cdots (p - 1)a \equiv 1 \cdot 2 \cdot 3 \cdots (p - 1) \pmod{p}.$$

Esplicitando:

$$a^{p-1}(p - 1)! \equiv (p - 1)! \pmod{p}.$$

Poiché p è primo, segue che p e $(p - 1)!$ sono coprimi. Applicando il teorema di cancellazione per le congruenze modulari (Teorema 8.4.9), possiamo dividere per $(p - 1)!$:

$$a^{p-1} \equiv 1 \pmod{p}.$$

Abbiamo dimostrato che:

$$a^{p-1} \equiv 1 \pmod{p}.$$

□

Esempio 6.18. Calcolare $5^{236} \mod 13$

$$MCD(5, 13) = 1 \; 5^{13-1} \equiv_{13} 1$$

$$\implies 5^{12} \equiv_{13} 1 \text{ per il piccolo teorema di Fermat}$$

$$5^{236} = (5^{12})^{19} \cdot 5^8 \equiv_{13} (1)^{19} \cdot 5^8 = 5^8$$

$$= (5^2)^4 \equiv_{13} (-1)^4 = 1$$

$$5^{236} mod 13$$

Corollario 6.3:

Questo implica che esistono $p - 1$ soluzioni distinte modulo p dell'equazione. Il valore di x può assumere tutti i numeri da 1 a $p - 1$, perché per ciascuno di essi vale $\gcd(x, p) = 1$, cioè $p \nmid x$.

6.5.4 Funzione di Euelro

La funzione di Eulero, $\phi(n)$, è definita come:

$$\phi(n) = \text{numero di interi positivi } \leq n \text{ che sono relativamente primi con } n.$$

Esempio 6.19. andiamo a vedere alcuni esempi della funzione di Eluero.

$$\begin{aligned} \phi(7) &= 6 \quad \text{perché } 1,2,3,4,5,6 \text{ sono relativamente primi con } 7, \\ \phi(8) &= 4 \quad \text{perché } 1,3,5,7 \text{ sono relativamente primi con } 8, \\ \phi(14) &= 6 \quad \text{perché } 1,3,5,9,11,13 \text{ sono relativamente primi con } 14. \end{aligned}$$

Lemma 3:

$$\begin{aligned} \phi(7) &= 6 \quad \text{perché } 1,2,3,4,5,6 \text{ sono relativamente primi con } 7, \\ \phi(8) &= 4 \quad \text{perché } 1,3,5,7 \text{ sono relativamente primi con } 8, \\ \phi(14) &= 6 \quad \text{perché } 1,3,5,9,11,13 \text{ sono relativamente primi con } 14. \end{aligned}$$

Lemma 4:

Se p è un numero primo, allora per ogni $k > 0$:

$$\phi(p^k) = p^k - p^{k-1} = p^k \left(1 - \frac{1}{p}\right).$$

Esempio 6.20. Calcoliamo $\phi(9) = \phi(3^2)$:

$$\phi(3^2) = 3^2 - 3^1 = 9 - 3 = 6.$$

I numeri coprimi con 9 sono $1, 2, 4, 5, 7, 8$.

Lemma 5:

Se a e b sono relativamente primi, allora:

$$\phi(ab) = \phi(a)\phi(b).$$

Teorema 6.11:

Se n è un intero positivo e a è relativamente primo con n, ossia $MCD(a, n) = 1$, allora:

$$a^{\phi(n)} \equiv 1 \pmod{n}.$$

Esempio 6.21. Calcoliamo $3^{256} \mod 100$.

$$\begin{aligned} \phi(100) = \phi(2^2 \cdot 5^2) = \phi(2^2)\phi(5^2) = (2^2 - 2)(5^2 - 5) = 4 \cdot 20 = 40, \\ 3^{256} = 3^{6 \cdot 40 + 16} = (3^{40})^6 \cdot 3^{16} \equiv 1^6 \cdot 3^{16} \pmod{100}. \end{aligned}$$

Calcoliamo 3^{16}:

$$3^{16} = (3^4)^4 = 81^4 \equiv 1^4 \pmod{100}.$$

Quindi:

$$3^{256} \equiv 1 \pmod{100}.$$

6.5.5 Equazioni modulari

Teorema 6.12:

Siano a e b numeri interi, e n un numero naturale. La congruenza modulare:

$$ax \equiv_n b$$

ha una soluzione se, e solo se:

$$MCD(a, n) \mid b.$$

Dimostrazione 6.7. La congruenza $ax \equiv_n b$ equivale a dire:

$$n \mid (ax - b).$$

Ciò implica che esiste un intero q tale che:

$$ax - b = nq,$$

o, equivalentemente:

$$ax - nq = b.$$

Secondo il Teorema di Bézout, l'equazione $ax - nq = b$ ha soluzioni intere per x e q se, e solo se:

$$MCD(a, n) \mid b.$$

Quindi, $ax \equiv_n b$ ha una soluzione se, e solo se, $\gcd(a, n) \mid b$.

Esempio 6.22. Trovare, se esiste, una soluzione per l'equazione modulare:

$$124x \equiv_{71} 17.$$

Calcoliamo il massimo comun divisore:

$$MCD(124, 71) = 1.$$

Poiché $MCD(124, 71) \mid 17$, la congruenza ammette soluzioni. L'inverso modulo si calcola risolvendo:

$$124y \equiv_{71} 1.$$

Moltiplicando entrambi i membri per -4, otteniamo:

$$(-4) \cdot 124y \equiv_{71} (-4) \cdot 1.$$

Poiché $(-4) \cdot 124 = -496$ e $-496 \equiv_{71} 1$, segue che:

$$y \equiv_{71} -4.$$

Sostituendo l'inverso trovato, otteniamo:

$$x \equiv_{71} 17 \cdot (-4).$$

Calcoliamo:

$$17 \cdot (-4) = -68.$$

Riducendo modulo 71:

$$-68 \equiv_{71} 3.$$

La soluzione è:

$$x \equiv_{71} 3.$$

Verifica:

$$124 \cdot 3 = 372, \quad 372 \mod 71 = 17.$$

Quindi la soluzione è corretta.

Il Teorema Cinese del Resto afferma che un sistema di congruenze:

$$x \equiv a_1 \pmod{n_1}, \quad x \equiv a_2 \pmod{n_2}, \quad x \equiv a_3 \pmod{n_3},$$

ha una soluzione unica modulo $N = n_1 \cdot n_2 \cdot n_3$, se n_1, n_2, n_3 sono coprimi a due a due.

6.5.6 Teorema cinese del resto

Teorema 6.13:

Siano $n_1, \ldots, n_k$ interi positivi a due a due relativamente primi, ossia $\gcd(n_i, n_j) = 1$ per ogni $i \neq j$. Allora il sistema di congruenze lineari:

$$x \equiv a_1 \pmod{n_1}, \quad x \equiv a_2 \pmod{n_2}, \quad \ldots, \quad x \equiv a_k \pmod{n_k},$$

ammette una soluzione unica modulo $N = n_1 n_2 \cdots n_k$.

Esempio 6.23. Siano $n_1, \ldots, n_k$ interi positivi a due a due relativamente primi, ossia $\gcd(n_i, n_j) = 1$ per ogni $i \neq j$. Allora il sistema di congruenze lineari:

$$x \equiv a_1 \pmod{n_1}, \quad x \equiv a_2 \pmod{n_2}, \quad \ldots, \quad x \equiv a_k \pmod{n_k},$$

ammette una soluzione unica modulo $N = n_1 n_2 \cdots n_k$.

Esempio: Risolviamo il sistema:

$$x \equiv 2 \pmod{5}, \quad x \equiv 6 \pmod{7}, \quad x \equiv 3 \pmod{11}.$$

Poiché $5, 7, 11$ sono coprimi, esiste una soluzione unica modulo $N = 5 \cdot 7 \cdot 11 = 385$.

$$\begin{aligned} b_1 &= 7 \cdot 11 = 77, & x_1 \text{ tale che } 77x_1 \equiv 1 \pmod{5} &\implies x_1 = 3, \\ b_2 &= 5 \cdot 11 = 55, & x_2 \text{ tale che } 55x_2 \equiv 1 \pmod{7} &\implies x_2 = 6, \\ b_3 &= 5 \cdot 7 = 35, & x_3 \text{ tale che } 35x_3 \equiv 1 \pmod{11} &\implies x_3 = 6. \end{aligned}$$

La soluzione generale è:

$$x = 2 \cdot 77 \cdot 3 + 6 \cdot 55 \cdot 6 + 3 \cdot 35 \cdot 6 \equiv 377 \pmod{385}.$$

Capitolo 7

Combinatoria

7.1 Spazio campionario ed eventi

Definizione 7.1:

Un esperimento è una procedura o processo che genera risultati. Lo spazio campionario S associato a un esperimento , è l'insieme di tutti i possibili risultati. Gli elementi dello spazio campionario sono chiamati esiti. Come ad esempio:

- L'esperimento di lanciare una moneta ha lo spazio campionario:

$$S = \{\text{Testa}, \text{Croce}\}.$$

- L'esperimento di lanciare un dado standard ha lo spazio campionario:

$$S = \{1, 2, 3, 4, 5, 6\}.$$

- **Spazio campionario**: È l'insieme di tutti i possibili risultati di un processo o esperimento casuale.
- **Evento**: È un sottoinsieme dello spazio campionario.

Esempio 7.1. L'esperimento consiste nel lancio di una moneta. Lo spazio campionario è:

$$S = \{\text{Testa}, \text{Croce}\}.$$

Gli eventi possibili includono:

- $\{\text{Testa}\}$: l'evento "ottenere Testa".
- $\{\text{Croce}\}$: l'evento "ottenere Croce".
- $\{\text{Testa}, \text{Croce}\}$: l'evento "ottenere Testa o Croce".
- $\emptyset$: l'evento "ottenere nessun risultato".

Esempio 7.2. Se l'esperimento consiste nel lancio di un dado standard, lo spazio campionario è:

$$S = \{1, 2, 3, 4, 5, 6\}.$$

Gli eventi possibili includono:

- $\{2, 4, 6\}$: l'evento "ottenere un numero pari".
- $\{1, 3, 5\}$: l'evento "ottenere un numero dispari".
- $\{5\}$: l'evento "ottenere il numero 5".
- $\emptyset$: l'evento vuoto.

7.1.1 Eventi equiprobabili

La probabilità di un evento misura quanto è probabile che l'evento si verifichi quando si esegue un esperimento. Quando gli esiti di uno spazio campionario sono **equiprobabili**, la probabilità di un evento E è il rapporto tra il numero di esiti in E e il numero di esiti nello spazio campionario S. La formula è:

$$P(E) = \frac{\text{numero di esiti in } E}{\text{numero di esiti in } S}. = P(E) = \frac{|E|}{|S|}$$

Esempio 7.3. Se si lancia una moneta standard, lo spazio campionario è:

$$S = \{\text{Testa}, \text{Croce}\}.$$

Ogni esito ha la stessa probabilità di verificarsi.

Calcolo delle probabilità:

- La probabilità di ottenere **Testa** è:

$$P(\{\text{Testa}\}) = \frac{1}{2}.$$

- La probabilità di ottenere **Croce** è:

$$P(\{\text{Croce}\}) = \frac{1}{2}.$$

Esempio 7.4. Se si lancia un dado standard, lo spazio campionario è:

$$S = \{1, 2, 3, 4, 5, 6\}.$$

Ogni esito ha la stessa probabilità di verificarsi.

Calcolo delle probabilità:

- La probabilità di ottenere un numero **pari** (esiti: $\{2, 4, 6\}$) è:

$$P(\{2, 4, 6\}) = \frac{3}{6} = \frac{1}{2}.$$

- La probabilità di ottenere il numero **5** (esito: $\{5\}$) è:

$$P(\{5\}) = \frac{1}{6}.$$

Consideriamo un mazzo ordinario di carte suddiviso in 4 semi: **cuori**, **quadri** (rossi), **fiori** e **picche** (neri). Ogni seme contiene 13 carte, con le seguenti denominazioni:

$$2, 3, 4, 5, 6, 7, 8, 9, 10, J, Q, K, A.$$

Immaginiamo che le carte siano state accuratamente mescolate, in modo che ogni carta abbia la stessa probabilità di essere scelta.

a) Spazio campionario

Lo spazio campionario degli esiti è:

$$S = \{\text{tutte le 52 carte del mazzo}\}.$$

Il numero totale di esiti è:

$$|S| = 52.$$

b) Evento: La carta scelta è una figura nera

Sia E l'evento "la carta scelta è una figura nera". Le figure sono:

$$\{\text{Jack (J), Regina (Q), Re (K)}\}.$$

Nel mazzo ci sono due semi neri (**fiori** e **picche**), ognuno con le 3 figure J, Q, K. Quindi, gli esiti favorevoli sono:

$$E = \{\text{J, Q, K di fiori; J, Q, K di picche}\}.$$

Il numero di esiti favorevoli è:

$$|E| = 6.$$

c) Calcolo della probabilità

La probabilità che la carta scelta sia una figura nera è data da:

$$P(E) = \frac{|E|}{|S|} = \frac{6}{52} = \frac{3}{26} \approx 11,5\%.$$

7.2 Contare gli elementi nelle lise

Definizione 7.2:

Una lista è un insieme ordinato di elementi. Se ogni elemento può essere scelto da un insieme di n elementi, e la lunghezza della lista. r. Generalmente , se m e n sono numeri interi e $m \leq n$, quanti numeri interi ci sono da m a n? Per rispondere a questa domanda, si osserva che $n = m + n - m$, dove $n - m \geq 0$ poiché $n \geq m$. Inoltre:

- L'elemento $m + 0$ è il primo elemento della lista;
- $m + 1$ è il secondo;
- $m + 2$ è il terzo, e così via.

In generale, l'elemento $m + i$ è l'$(i + 1)$-esimo elemento della lista. La lista risulta essere:

$$m(m + 0),\ m + 1,\ m + 2, \ldots, (n - m) + 1$$

Quindi il numero di elementi nella lista è $n - m + 1$. Questo risultato generale è sufficientemente importante da essere enunciato come teorema.

Teorema 7.1:

Se m e n sono numeri interi e $m \leq n$ allora ci sono $n - m + 1$ elementi da m a n inclusi.

Esempio 7.5. a) Quanti numeri ci sono tra 100 e 999 che sono divisibili per 5?

Consideriamo i numeri di tre cifre divisibili per 5. I numeri divisibili per 5 in questo intervallo formano una progressione aritmetica:

$$100, 105, 110, \ldots, 995.$$

Il primo termine della progressione è $a = 100$, l'ultimo termine è $l = 995$, e la differenza comune è $d = 5$.

Per trovare il numero totale di termini n, usiamo la formula del termine generico della progressione aritmetica:

$$l = a + (n - 1)d.$$

Sostituendo i valori:

$$995 = 100 + (n - 1) \cdot 5,$$

$$995 - 100 = (n - 1) \cdot 5 \implies 895 = (n - 1) \cdot 5 \implies n - 1 = 179 \implies n = 180.$$

Quindi, ci sono 180 numeri di tre cifre divisibili per 5.

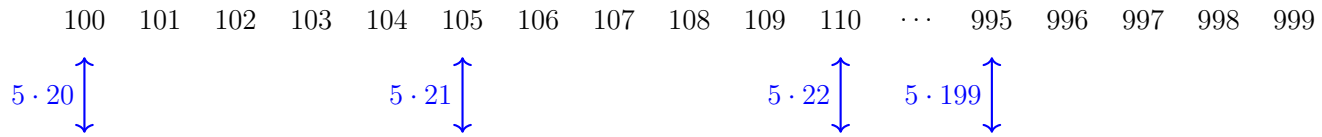
b) Qual è la probabilità che un numero intero di tre cifre scelto casualmente sia divisibile per 5?

Il totale dei numeri di tre cifre è:

$$999 - 100 + 1 = 900.$$

La probabilità che un numero scelto casualmente sia divisibile per 5 è quindi:

$$P(E) = \frac{\text{numero di numeri divisibili per 5}}{\text{numero totale di numeri di tre cifre}} = \frac{180}{900} = \frac{1}{5}.$$



Esempio 7.6. Consideriamo un array $A[1], A[2], \ldots, A[n]$, dove n è un numero intero positivo.

a) Divisione dell'array in due sottoarray

Supponiamo che l'array venga diviso in 2 sottoarray, uno con gli indici centrati su numeri pari, l'altro su numeri dispari:

1. Sottoarray con indici pari:
$$A[2], A[4], \ldots, A[2m],$$
dove $m = \lfloor n/2 \rfloor$ è il numero di elementi con indici pari.

2. Sottoarray con indici dispari:
$$A[1], A[3], \ldots, A[m+1].$$

Entrambi i sottoarray contengono lo stesso numero di elementi, a meno di un elemento nel caso in cui n sia dispari.

b) Probabilità di un elemento con indice pari

Caso (i): n è pari

Se n è pari, ogni indice pari può essere ottenuto dalla sequenza:

$$2, 4, 6, \ldots, n.$$

Questa è una progressione aritmetica con:

$$a = 2, \quad l = n, \quad d = 2.$$

Il numero totale di elementi è:

$$\frac{n}{2}.$$

Poiché l'intero array ha n elementi, la probabilità che un elemento scelto casualmente abbia un indice pari è:

$$P(E) = \frac{\text{numero di elementi con indice pari}}{\text{numero totale di elementi}} = \frac{\frac{n}{2}}{n} = \frac{1}{2}.$$

Caso (ii): n è dispari

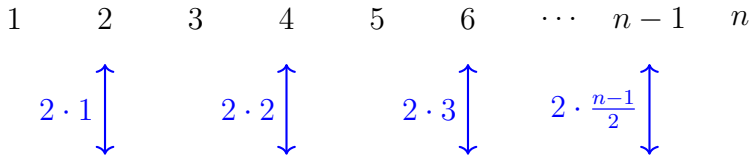
Se n è dispari, il più grande indice pari dell'array è $n-1$. Quindi il numero totale di elementi con indici pari è:

$$\frac{n-1}{2}.$$

La probabilità che un elemento scelto casualmente abbia un indice pari è:

$$P(E) = \frac{\frac{n-1}{2}}{n} = \frac{n-1}{2n}.$$

Rappresentazione Grafica



- Se n è pari, la probabilità che un elemento scelto casualmente abbia un indice pari è:

$$P(E) = \frac{1}{2}.$$

- Se n è dispari, la probabilità è:

$$P(E) = \frac{n-1}{2n}.$$

7.3 Alberi di possibilità e regola della moltiplicazione

7.3.1 Alberi di possibilità

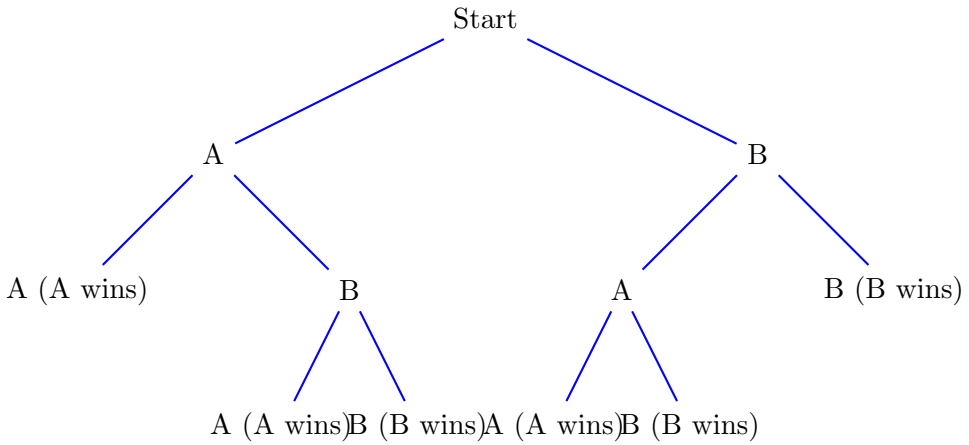
Definizione 7.3:

Gli alberi di possibilità sono strumenti utili per rappresentare graficamente gli esiti di situazioni sequenziali. Ogni ramo rappresenta un possibile risultato della scelta o di un evento. Gli alberi di possibilità aiutano a visualizzare i problemi di conteggio e calcolo delle probabilità, specialmente quando ci sono più livelli o fasi.

Esempio 7.7. Le squadre A e B giocano ripetutamente fino a quando una delle due vince due partite consecutive o si raggiunge un totale di tre partite.

a) Quanti modi esistono per giocare il torneo?

Le possibili modalità di gioco sono rappresentate come percorsi distinti dall'origine (inizio) fino alle foglie (fine). Il grafo che segue rappresenta tutte le combinazioni possibili:



Il grafo mostra che ci sono 10 modi diversi per giocare il torneo.

b) Qual è la probabilità che siano necessarie 3 partite per determinare il vincitore?

Consideriamo il caso $BABB$, in cui sono necessarie tutte e 3 le partite. I percorsi favorevoli che includono una sequenza di 3 partite sono 4.

La probabilità è quindi:

$$P(\text{3 partite}) = \frac{\text{casi favorevoli}}{\text{casi totali}} = \frac{4}{10} = \frac{2}{5} = 40\%.$$

7.3.2 Regola della moltiplicazione

Definizione 7.4:

La regola della moltiplicazione afferma che se un'operazione consiste di k passi e ogni passo può essere eseguito in un numero fisso di modi, allora il numero totale di modi in cui l'operazione può essere completata è il prodotto del numero di modi per ciascun passo.

Teorema 7.2:

Se un'operazione consiste di k passi:

- il primo passo può essere eseguito in n_1 modi;
- il secondo passo può essere eseguito in n_2 modi (indipendentemente da come è stato eseguito il primo passo);
- il k-esimo passo può essere eseguito in n_k modi (indipendentemente da come sono stati eseguiti i passi precedenti).

Tutte le operazioni possono essere eseguite in:

$$n_1 \cdot n_2 \cdot \ldots \cdot n_k \quad \text{modi.}$$

Esempio 7.8. Un PIN è una sequenza di 4 simboli scelti da un insieme di 36 simboli (26 lettere + 10 cifre). Dato che sono permesse ripetizioni, ogni simbolo ha 36 scelte. Il numero totale di PIN possibili è:

$$36 \cdot 36 \cdot 36 \cdot 36 = 36^4 = 1.679.616$$

Esempio 7.9. Consideriamo ora un PIN di 4 simboli scelti senza ripetizioni dallo stesso insieme di 36 simboli. Per il primo simbolo ci sono 36 scelte, per il secondo 35, per il terzo 34, e per il quarto 33. Il numero totale di PIN senza ripetizioni è:

$$36 \cdot 35 \cdot 34 \cdot 33 = 1.413.720$$

La probabilità che un PIN scelto a caso non abbia simboli ripetuti è data dal rapporto tra il numero di PIN senza ripetizioni e il numero totale di PIN. Quindi:

$$P(\text{no ripetizioni}) = \frac{1.413.720}{1.679.616} \approx 0,841$$

Quindi, l'**84%** dei PIN non ha simboli ripetuti.

La regola della moltiplicazione è utile solo quando le scelte nei vari passi del processo sono indipendenti.

Se una scelta influenza le altre, allora è necessario adottare un approccio diverso, tenendo conto delle dipendenze tra le scelte.

Esempio 7.10. Supponiamo che si debba creare un outfit scegliendo:

- una maglietta (3 scelte: rossa, blu, verde),
- un paio di pantaloni (4 scelte: nero, grigio, beige, marrone).

Poiché la scelta della maglietta non influisce su quella dei pantaloni, il numero totale di combinazioni possibili è dato dalla regola della moltiplicazione:

$$3 \cdot 4 = 12 \quad \text{combinazioni.}$$

Supponiamo ora di scegliere una squadra di 2 persone da un gruppo di 3 persone (A, B, C). In questo caso, la scelta di una persona influenza le scelte successive, poiché non è possibile selezionare la stessa persona due volte.

Le combinazioni possibili devono essere calcolate considerando questa dipendenza:

- Per la prima persona ci sono 3 scelte (A, B, C).
- Per la seconda persona, rimangono solo 2 scelte (le due persone non selezionate).

Il numero totale di combinazioni è dato da:

$$3 \cdot 2 = 6 \quad \text{combinazioni totali.}$$

Tuttavia, poiché AB e BA rappresentano la stessa squadra, dobbiamo dividere per 2! per rimuovere le permutazioni interne:

$$\frac{3 \cdot 2}{2} = 3 \quad \text{combinazioni uniche (squadre: } AB, AC, BC).$$

La regola della moltiplicazione si applica direttamente nel caso 1, dove le scelte sono indipendenti. Nel caso 2, le scelte sono dipendenti e richiedono un approccio che tenga conto di queste dipendenze, come l'uso delle combinazioni.

7.4 Permutazioni

Definizione 7.5:

Una permutazione di un insieme di oggetti è un ordinamento degli oggetti in una riga. Per esempio l'insieme degli elementi a, b e c ha 6 permutazioni.

$$abc\ acb\ cba\ bac\ bca\ cabb$$

In generale, dato un insieme di n oggetti, quante permutazioni ha l'insieme? Immaginiamo di formare una permutazione come un'operazione in n passi:

- Scegliamo un elemento da scrivere come primo.
- Scegliamo un elemento da scrivere come secondo.
- $\vdots$
- Scegliamo un elemento da scrivere come n-esimo.

Qualsiasi elemento dell'insieme può essere scelto nel passo 1, quindi ci sono n modi per eseguire il passo 1.
Qualsiasi elemento tranne quello scelto nel passo 1 può essere scelto nel passo 2, quindi ci sono $n-1$ modi per eseguire il passo 2.
In generale, il numero di modi per eseguire ogni passo successivo è uno in meno rispetto al numero di modi per eseguire il passo precedente. Nel momento in cui viene scelto l'ultimo elemento, rimane un solo modo per completare l'operazione.
Quindi, secondo la regola della moltiplicazione, il numero totale di permutazioni è:

$$n \cdot (n-1) \cdot (n-2) \cdots 2 \cdot 1 = n!$$

Teorema 7.3:

Per ogni numero intero n, con $n \geq 1$, il numero di permutazioni di un insieme con n elementi è $n!$-

Esempio 7.11. La parola "computer" è composta da 8 lettere distinte. Il numero totale di anagrammi possibili è:

$$8! = 8 \cdot 7 \cdot 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 = 40.320$$

Se vogliamo calcolare il numero di anagrammi in cui le lettere "co" rimangono vicine, possiamo trattare "co" come un'unica entità.

In questo caso, abbiamo 7 oggetti da disporre:

$$\{\text{"co"}, m, p, u, t, e, r\}.$$

Il numero di anagrammi possibili è:

$$7! = 7 \cdot 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 = 5.040$$

La probabilità che le lettere "co" rimangano vicine è:

$$P = \frac{5.040}{40.320} = \frac{1}{8} = 12,5\%.$$

Esempio 7.12. Quanti sono i possibili anagrammi della parola "Picche"? La parola "Picche" è composta da 6 lettere, con la lettera "c" che si ripete 2 volte.

Il numero totale di anagrammi possibili è dato dalla formula:

$$\frac{6!}{2!} = \frac{6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1}{2 \cdot 1} = 360$$

7.5 Disposizioni semplici

Dato l'insieme $\{a, b, c\}$, ci sono 6 modi per selezionare 2 lettere dall'insieme e scriverle in ordine.

Ecco le disposizioni:

$$ab, ba, ac, ca, bc, cb$$

Ogni ordinamento di questi 2 elementi di $\{a, b, c\}$ è chiamato una disposizione semplice di 2 elementi presi da 3.

Definizione 7.6:

Una **disposizione semplice** di un insieme di n elementi è una selezione ordinata di r elementi presi dall'insieme.
Il numero di disposizioni semplici di r elementi di un insieme di n elementi si indica con:

$$P(n, r).$$

Teorema 7.4:

Se n ed r sono numeri interi con $1 \leq r \leq n$, allora il numero di disposizioni semplici di r elementi di un insieme di n elementi è dato dalla formula:

$$P(n, r) = n \cdot (n-1) \cdot (n-2) \cdots (n-r+1),$$

o, equivalentemente:

$$P(n, r) = \frac{n!}{(n-r)!}.$$

Dimostrazione 7.1. Vogliamo dimostrare che, per ogni numero intero $n \geq 2$, si ha:

$$P(n, 2) + P(n, 1) = n^2.$$

Per il teorema delle disposizioni semplici, il numero di disposizioni semplici di 2 elementi da un insieme di n elementi è:

$$P(n, 2) = \frac{n!}{(n-2)!} = n \cdot (n-1).$$

Sommando i due risultati, otteniamo:

$$P(n,2) + P(n,1) = n \cdot (n-1) + n = n^2 - n + n = n^2.$$

Quindi, la dimostrazione è completa:

$$P(n,2) + P(n,1) = n^2.$$

□

Esempio 7.13. Il numero di disposizioni semplici di 2 elementi da un insieme di 5 elementi è:

$$P(5,2) = \frac{5!}{(5-2)!} = \frac{5 \cdot 4 \cdot 3!}{3!} = 5 \cdot 4 = 20.$$

Esempio 7.14. Il numero di disposizioni semplici di 4 elementi da un insieme di 7 elementi è:

$$P(7,4) = \frac{7!}{(7-4)!} = \frac{7 \cdot 6 \cdot 5 \cdot 4 \cdot 3!}{3!} = 7 \cdot 6 \cdot 5 \cdot 4 = 840.$$

Esempio 7.15. Il numero di disposizioni semplici di 5 elementi da un insieme di 5 elementi è:

$$P(5,5) = \frac{5!}{(5-5)!} = \frac{5!}{1} = 5! = 120.$$

7.6 Contare elementi di insiemi disgiunti

La regola della somma afferma che il numero di elementi in un'unione di insiemi finiti reciprocamente disgiunti è uguale alla somma del numero di elementi in ciascuno degli insiemi che la compongono.

Teorema 7.5:

Supponiamo che esista un insieme finito A sia uguale all'unione di k distinti sottoinsiemi $A_1, A_2, \ldots, A_k$, reciprocamente disgiunti.
Allora si ha:

$$N(A) = N(A_1) + N(A_2) + \cdots + N(A_k),$$

dove N indica la cardinalità di un insieme finito.

Esempio 7.16. Una password di accesso al computer è composta da una a tre lettere scelte dall'alfabeto con ripetizioni consentite. Quante password diverse sono possibili? L'insieme di tutte le password può essere suddiviso in sottoinsiemi costituiti da:

- quelle di lunghezza 1,
- quelle di lunghezza 2,
- quelle di lunghezza 3.

Numero di password di lunghezza 1:

$$26^1 = 26$$

Numero di password di lunghezza 2:

$$26^2 = 676$$

Numero di password di lunghezza 3:

$$26^3 = 17\,576$$

Totale: Dunque, il numero totale di password è:

$$26 + 26^2 + 26^3 = 26 + 676 + 17\,576 = 18\,278$$

Corollario 7.1:

Un'importante conseguenza della regola dell'addizione è il fatto che se il numero di elementi in un insieme A e il numero di elementi in un sottoinsieme $B \subseteq A$ sono noti, allora il numero di elementi che sono in A e non in B è calcolato come:

$$N(A \setminus B) = N(A) - N(B).$$

Esempio 7.17. Dato un PIN di 4 simboli dove possiamo usare le 26 lettere maiuscole e 10 cifre, quanti PIN contengono almeno un simbolo ripetuto?

Dato un PIN di 4 simboli dove possiamo usare le 26 lettere maiuscole e 10 cifre, quanti PIN contengono almeno un simbolo ripetuto?

Osserviamo che, per la regola della differenza, il numero di PIN con almeno una ripetizione è uguale al numero di PIN totali meno il numero di PIN senza ripetizioni. Quindi:

$$\text{Numero di PIN totali} = 36^4$$

$$\text{PIN senza ripetizioni} = 36 \cdot 35 \cdot 34 \cdot 33$$

Soluzione Alternativa

Denotiamo con:

- $P(CA)$: Probabilità che un PIN preso a caso **non contenga ripetizioni**.
- $P(CS - A)$: Probabilità che un PIN preso a caso contenga **almeno una ripetizione**.

Per la regola della probabilità complementare:

$$P(CS - A) = 1 - P(CA)$$

$$P(CS - A) = \frac{\text{N(PIN totali)} - \text{N(PIN senza ripetizioni)}}{\text{N(PIN totali)}}$$

Calcoliamo i valori:

- PIN totali: $36^4 = 1,679,616$
- PIN senza ripetizioni: $36 \cdot 35 \cdot 34 \cdot 33 = 1,326,360$

Quindi, la probabilità che un PIN contenga almeno una ripetizione è:

$$P(CS - A) = \frac{1,679,616 - 1,326,360}{1,679,616} \approx 0.21$$

Il 21% dei PIN contiene almeno un simbolo ripetuto.

7.7 Combinazioni

Siano n e r due numeri interi con $r \leq n$. Una **r-combinazione** di un insieme di n elementi è un sottoinsieme di r elementi scelti tra i n elementi.

Il numero di combinazioni si denota come:

$$\binom{n}{r}$$

che si legge *"n scelto r"* e rappresenta il numero di sottoinsiemi di dimensione r che possono essere scelti da un insieme di n elementi.

Teorema 7.6:

Il numero di sottoinsiemi di dimensione r che possono essere scelti da un insieme di n elementi è indicato dal **coefficiente binomiale**:

$$\binom{n}{r} = \frac{P(n,r)}{r!}$$

dove $P(n,r)$ rappresenta il numero di permutazioni di n elementi presi r alla volta, espresso come:

$$P(n,r) = \frac{n!}{(n-r)!}$$

Sostituendo, otteniamo:

$$\binom{n}{r} = \frac{n!}{r!(n-r)!} = \binom{n}{k} = \frac{n!}{k!(n-k)!}$$

Esempio 7.18. Squadre con vincoli

1. Supponiamo che due membri del gruppo non vadano d'accordo e rifiutino di lavorare insieme. Quante squadre di cinque persone possono essere formate?

   Chiamiamo i due membri C e D.

   - **Squadre che contengono D ma non C:**

   $$\binom{10}{4} = \frac{10!}{4!(10-4)!} = 210$$

   - **Squadre che contengono C ma non D:**

   $$\binom{10}{4} = 210 \quad \text{(stesso calcolo come sopra).}$$

   - **Squadre che non contengono C né D:**

   $$\binom{10}{5} = \frac{10!}{5!(10-5)!} = 252$$

   Totale squadre:

   $$\binom{10}{4} + \binom{10}{4} + \binom{10}{5} = 210 + 210 + 252 = 672$$

2. Supponiamo che due membri del gruppo di dodici insistano nel lavorare insieme: ogni squadra deve includere entrambi o nessuno dei due. Quante squadre di cinque persone possono essere formate?

   Chiamiamo i due membri A e B.

   - **Squadre che contengono A e B:** Se A e B sono nella squadra, rimangono 3 posti da riempire con i rimanenti 10 membri:

   $$\binom{10}{3} = \frac{10!}{3!(10-3)!} = 120$$

   - **Squadre che non contengono né A né B:** In questo caso, tutti i 5 membri vengono scelti tra i rimanenti 10:

   $$\binom{10}{5} = \frac{10!}{5!(10-5)!} = 252$$

   Totale squadre:

   $$\binom{10}{3} + \binom{10}{5} = 120 + 252 = 372$$

3. Supponiamo che il gruppo sia composto da 5 uomini e 7 donne. Quante squadre di cinque persone possono essere formate con tre uomini e due donne?

   Il numero di modi per scegliere 3 uomini dai 5 disponibili è:

$$\binom{5}{3} = \frac{5!}{3!(5-3)!} = \frac{5 \cdot 4 \cdot 3!}{3! \cdot 2!} = 10.$$

   Il numero di modi per scegliere 2 donne dalle 7 disponibili è:

$$\binom{7}{2} = \frac{7!}{2!(7-2)!} = \frac{7 \cdot 6 \cdot 5!}{2 \cdot 1 \cdot 5!} = 21.$$

   Pertanto, il numero totale di squadre con tre uomini e due donne è:

$$\binom{5}{3} \cdot \binom{7}{2} = 10 \cdot 21 = 210.$$

4. Quante squadre di cinque persone contengono almeno un uomo?

   Il numero totale di squadre che si possono formare è:

$$\binom{12}{5} = \frac{12!}{5!(12-5)!} = \frac{12 \cdot 11 \cdot 10 \cdot 9 \cdot 8}{5 \cdot 4 \cdot 3 \cdot 2 \cdot 1} = 792.$$

   Il numero di squadre che contengono solo donne è:

$$\binom{7}{5} = \frac{7!}{5!(7-5)!} = \frac{7 \cdot 6}{2 \cdot 1} = 21.$$

   Pertanto, il numero di squadre con almeno un uomo è:

$$\binom{12}{5} - \binom{7}{5} = 792 - 21 = 771.$$

5. Quante squadre di cinque persone contengono più di un uomo?

   Il numero di squadre senza uomini è dato da:

$$\binom{7}{5} = 21.$$

   Il numero di squadre con esattamente un uomo è dato da:

$$\binom{5}{1} \cdot \binom{7}{4} = 5 \cdot \frac{7 \cdot 6 \cdot 5 \cdot 4}{4 \cdot 3 \cdot 2 \cdot 1} = 5 \cdot 35 = 175.$$

   Pertanto, il numero di squadre con più di un uomo è:

$$\binom{12}{5} - \binom{7}{5} - \binom{5}{1} \cdot \binom{7}{4} = 792 - 21 - 175 = 596.$$

Esempio 7.19. Quante mani di poker da cinque carte possono essere formate da un mazzo di 52 carte?

Il numero totale di mani è:

$$\binom{52}{5} = \frac{52!}{5!(52-5)!} = \frac{52 \cdot 51 \cdot 50 \cdot 49 \cdot 48}{5 \cdot 4 \cdot 3 \cdot 2 \cdot 1} = 2,598,960.$$

La regola della moltiplicazione afferma:

> Se riesci a immaginare che gli elementi da contare possono essere ottenuti tramite un processo a più passaggi (in cui ogni passaggio viene eseguito in un numero fisso di modi, indipendentemente da come sono stati eseguiti i passaggi precedenti), allora puoi usare la regola della moltiplicazione. Il numero totale di elementi sarà il prodotto del numero di modi in cui eseguire ogni passaggio.

Esempio 7.20. Supponiamo di voler creare un codice di sicurezza di 4 simboli, dove:

- Il primo simbolo è una lettera maiuscola (26 possibilità).
- Il secondo simbolo è una cifra (10 possibilità).
- Il terzo simbolo è una lettera maiuscola (26 possibilità).
- Il quarto simbolo è una cifra (10 possibilità).

Utilizzando la regola della moltiplicazione, il numero totale di codici possibili è:

$$26 \cdot 10 \cdot 26 \cdot 10 = 67600.$$

La regola dell'addizione afferma:

> Se riesci a immaginare che l'insieme degli elementi da contare possa essere suddiviso in sottoinsiemi disgiunti, puoi usare la regola dell'addizione. Il numero totale di elementi sarà la somma del numero di elementi in ciascun sottoinsieme.

Supponiamo di contare il numero totale di studenti in una scuola, suddivisi per corso:

- Ci sono 150 studenti in prima superiore.
- Ci sono 140 studenti in seconda superiore.
- Ci sono 130 studenti in terza superiore.
- Ci sono 120 studenti in quarta superiore.
- Ci sono 110 studenti in quinta superiore.

Poiché ogni corso rappresenta un sottoinsieme disgiunto, possiamo utilizzare la regola dell'addizione per calcolare il totale:

$$150 + 140 + 130 + 120 + 110 = 650.$$

A volte, è utile combinare entrambe le regole. Ad esempio:

Quanti studenti indossano magliette rosse o blu?

Supponiamo:

- 50 studenti indossano magliette rosse.
- 40 studenti indossano magliette blu.

Se ogni studente indossa solo una maglietta, possiamo sommare:

$$50 + 40 = 90.$$

7.8 Principio di inclusione esclusione

Definizione 7.7:

La regola di inclusione-esclusione afferma che per due o più insiemi qualsiasi è possibile calcolare la cardinalità della loro unione considerando la sovrapposizione tra gli insiemi. In particolare:

- Per due insiemi: Siano A e B due insiemi qualsiasi, allora:

  $$N(A \cup B) = N(A) + N(B) - N(A \cap B)$$

  La somma $N(A) + N(B)$ considera due volte la cardinalità dell'intersezione $N(A \cap B)$, che quindi deve essere sottratta.

- Per tre insiemi: Siano A, B, e C tre insiemi qualsiasi, allora:

  $$N(A \cup B \cup C) = N(A) + N(B) + N(C) - N(A \cap B) - N(A \cap C) - N(B \cap C) + N(A \cap B \cap C)$$

Questo approccio garantisce che ogni elemento venga contato esattamente una volta.

Esempio 7.21. Siano A, B, e C insiemi di studenti iscritti a tre corsi differenti. Supponiamo che:

$$N(A) = 20, \quad N(B) = 30, \quad N(C) = 25$$

Inoltre, sappiamo che:

$$N(A \cap B) = 10, \quad N(A \cap C) = 5, \quad N(B \cap C) = 8, \quad N(A \cap B \cap C) = 3$$

Applicando la regola di inclusione-esclusione:

$$N(A \cup B \cup C) = N(A) + N(B) + N(C) - N(A \cap B) - N(A \cap C) - N(B \cap C) + N(A \cap B \cap C)$$

$$N(A \cup B \cup C) = 20 + 30 + 25 - 10 - 5 - 8 + 3 = 55$$

Quindi, il numero totale di studenti iscritti ad almeno uno dei tre corsi è 55.

Esempio 7.22. Sia $X = \{1, 2, 3, 4, 5\}$. Quanti sono i sottoinsiemi di X che contengono gli elementi 1 o 5? Utilizziamo il **principio di inclusione-esclusione**. Siano:

$$A = \{\text{sottoinsiemi di } X \text{ che contengono } 1\}$$

$$B = \{\text{sottoinsiemi di } X \text{ che contengono } 5\}.$$

Il numero totale di sottoinsiemi che contengono 1 o 5 è dato da:

$$|A \cup B| = |A| + |B| - |A \cap B|.$$

Calcolo di $|A|$: I sottoinsiemi di X che contengono 1 possono essere ottenuti scegliendo liberamente gli elementi restanti di $\{2, 3, 4, 5\}$, quindi:

$$|A| = 2^4 = 16.$$

Calcolo di $|B|$: I sottoinsiemi di X che contengono 5 possono essere ottenuti scegliendo liberamente gli elementi restanti di $\{1, 2, 3, 4\}$, quindi:

$$|B| = 2^4 = 16.$$

Calcolo di $|A \cap B|$: I sottoinsiemi di X che contengono sia 1 che 5 possono essere ottenuti scegliendo liberamente gli elementi restanti di $\{2, 3, 4\}$, quindi:

$$|A \cap B| = 2^3 = 8.$$

Applichiamo il principio di inclusione-esclusione:

$$|A \cup B| = |A| + |B| - |A \cap B| = 16 + 16 - 8 = 24.$$

Il numero totale di sottoinsiemi di X che contengono 1 o 5 è 24.

Capitolo 8

Conclusione

Questi appunti affrontando argomenti chiave della matematica discreta. Il contenuto spazia dalla logica fino a strumenti sofisticati per il calcolo combinatorio e il principio di induzione, fornendo un quadro completo e sistematico delle idee che stanno alla base di questo ambito della matematica.

1. **Logica**
   Abbiamo analizzato i fondamenti del ragionamento matematico, esplorando proposizioni, connettivi logici, tabelle di verità, implicazioni e regole di inferenza. La logica è stata il punto di partenza per costruire una solida base formale per i concetti successivi.

2. **Insiemi**
   Sono stati introdotti gli strumenti per lavorare con collezioni di oggetti: unioni, intersezioni, differenze, complementi e prodotti cartesiani. Gli insiemi sono stati il linguaggio fondamentale per rappresentare relazioni e funzioni.

3. **Relazioni**
   Abbiamo approfondito il concetto di relazione tra insiemi, classificando relazioni in riflessive, simmetriche, antisimmetriche e transitive. In particolare, ci siamo soffermati sulle relazioni di equivalenza e sugli ordini parziali.

4. **Funzioni**
   Dalle nozioni di dominio e codominio alle funzioni iniettive, suriettive e biettive, abbiamo esplorato la nozione di funzione come mappatura tra insiemi, con particolare attenzione alle composizioni e agli inversi.

5. **Principio di induzione e sommatorie**
   Il principio di induzione è stato trattato come uno strumento essenziale per dimostrare proprietà sugli interi. Sono state esplorate anche le sommatorie, sia come espressioni compatte che come strumenti di calcolo combinatorio.

6. **Teoria dei numeri**
   Abbiamo introdotto concetti di divisibilità, numeri primi, il massimo comune divisore (MCD) e il minimo comune multiplo (mcm), insieme a tecniche come l'algoritmo di Euclide e il Teorema fondamentale dell'aritmetica.

7. **Combinatoria**
   L'arte di contare è stata esplorata in dettaglio, attraverso permutazioni, disposizioni, combinazioni e il principio di inclusione-esclusione. Abbiamo affrontato problemi di conteggio realistici, come la probabilità nei PIN, le disposizioni in squadre e le mani di poker.

8.1 Considerazioni Finali

Questi appunti sono stati elaborati con l'obiettivo di fornire uno strumento integrativo allo studio, utile sia come guida teorica che come riferimento per esercizi pratici. Tuttavia, essi non intendono sostituire testi accademici o le lezioni frontali, ma piuttosto integrarli, rendendo i concetti più accessibili e organizzati.

Bibliografia

[1] Wikipedia. *Funzione di Cantor a due variabi*. Disponibile su: `https://en.wikipedia.org/wiki/Pairing_function`

[2] Giuseppe Lancia. *Matematica Discreta*. Springer-Verlag Italia, 2012. ISBN: 978-8847024919.

[3] Susanna S. Epp. *Discrete Mathematics with Applications*, 4th Edition. Cengage Learning, 2010. ISBN: 978-0495391326.

[4] Kenneth H. Rosen. *Discrete Mathematics and Its Applications*, 7th Edition. McGraw-Hill Education, 2019. ISBN: 978-0073383095.

[5] Sabina Rossi. *Appunti e Slide delle lezioni di Matematica Discreta*, Anno Accademico 2024-2025.