Strutture Discrete

Riassunto realizzato da Stefano Mavilla

1 Parte 1

1.1 Logica Proposizionale

Le logiche sono Linguaggi Formali, composti dalla **sintassi** e dalla **semantica**. La **Logica Proposizionale** è la logica più semplice e si occupa di fatti o affermazioni e della loro veridicità, inoltre:
• è connessa al mondo binario 0/1 dei calcolatori;
• è conosciuta come Logica Booleana.

Le Variabili Proposizionali possono essere **Vere (1)** o **False (0)** e ogni variabile proposizionale è una "Formula" proposizionale.
Ogni formula può essere costruita usando Connettivi Logici:
• Negazione (si legge "non"): $\neg$
• Disgiunzione Logica (si legge "0"): $\vee$
• Congiunzione Logica (si legge "e"): $\wedge$
• Implicazione Logica (si legge "se...allora..."): $\Rightarrow$
• Coimplicazione Logica (si legge "se e solo se"): $\iff$

Se P e Q sono formule:
• $\neg P$ (o $\neg Q$) è una formula;
• $P \vee Q$ è una formula;
• $P \wedge Q$ è una formula;
• $P \Rightarrow Q$ è una formula;
• $P \iff Q$ è una formula;

Nelle formule logiche ci sono **regole di precedenza**, aggirabili con le parentesi. Inoltre la $\neg$ ha precedenza **maggiore**, mentre $\vee$ e $\wedge$ hanno la **stessa** precedenza.

Esempi:
• $\neg p \vee q$, la negazione è solo su p.
• $\neg(p \vee q)$, la negazione si applica sull'intera disgiunzione.

Una Interpretazione I su P è una funzione $I : P \to \{0, 1\}$ (o $P \to \{F, T\}$). Date due formule P e Q è un interpretazione I che assegna un valore di verità alle variabili presenti, si calcola il valore di verità di tutta la formula $I(P)$ o $I(Q)$. Si usano le Tavole della Verità:

P	$\neg P$
T	F
F	T

P	Q	$P \vee Q$	$P \wedge Q$	$P \Rightarrow Q$	$P \iff Q$
F	F	F	F	T	T
F	T	F	T	T	F
T	F	F	T	F	F
T	T	T	T	T	T

Soddisfacibilità ed Insoddisfacibilità:
• Data una formula P, essa è **soddisfacibile** se esiste un interpretazione I delle variabili proposizionali presenti nella formula, ovvero un'assegnazione del valore di verità T/F per ogni variabile proposizionale, tale che $I(P)$ è vera.
• Data una formula P, essa è **insoddisfacibile** se non esiste un interpretazione I delle variabili proposizionali presenti nella formula, ovvero un'assegnazione del valore di verità T/F per ogni variabile proposizionale, tale che $I(P)$ è vera.
• Una formula P si dice **Tautologia** se per ogni interpretazione I delle variabili proposizionali presenti nella formula, ovvero un'assegnazione del valore di verità T/F per ogni variabile proposizionale, la formula risulta vera.

Esempi:

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

P	Q	$\neg P \Rightarrow Q$	$P \Rightarrow (\neg P \Rightarrow Q)$
F	F	F	T
F	T	T	T
T	F	T	T
T	T	T	T

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

Principi Fondamentali della Logica Proposizionale:
• **Principio del Terzo Escluso**: $p \vee \neg p$ è una Tautologia, ovvero sempre vera.
• **Principio di Non Contraddizione**: $p \wedge \neg p$ è Insoddisfacibile, ovvero sempre falsa.

Equivalenze Logiche e Proprietà:
• Due formule P e Q sono **equivalenti** se P è vera $\iff$ Q è vera e si scrive: $p \equiv q$
• Commutatività della Disgiunzione: $p \vee q \equiv q \vee p$
• Commutatività della Congiunzione: $p \wedge q \equiv q \wedge p$
• Associatività della Disgiunzione: $p \vee (q \vee r) \equiv (p \vee q) \vee r$
• Associatività della Congiunzione: $p \wedge (q \wedge r) \equiv (p \wedge q) \wedge r$
• Doppia Negazione: $\neg(\neg p) \equiv p$
• Contrapposizione: $p \Rightarrow q \equiv \neg q \Rightarrow \neg p$
• Eliminazione Implicazione: $p \Rightarrow q \equiv \neg p \wedge q$
• Eliminazione Doppia Implicazione: $p \iff q \equiv (p \Rightarrow q) \wedge (q \Rightarrow p)$

Leggi di De Morgan:
• La negazione della congiunzione è equivalente alla disgiunzione delle negazioni: $\neg(p \wedge q) \equiv \neg p \vee \neg q$
• La negazione della disgiunzione è equivalente alla congiunzione delle negazioni: $\neg(p \vee q) \equiv \neg p \wedge \neg q$

Distributività:
• Distributività della congiunzione sulla disgiunzione:
$p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$
• Distributività della disgiunzione sulla congiunzione:
$p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$

Giustificazione Logica:
Sia P un insieme di formule e p una formula, P giustifica p se ogni interpretazione di I che soddisfa tutte le formule di P soddisfa anche $p : \mathbf{P} \models p$

Esempi:

$\boldsymbol{P}$=$\{p, p \Rightarrow q\}$, $\boldsymbol{P} \models q$

P	Q	$P \Rightarrow Q$	Q	
F	F	T	F	P falsa
F	T	T	T	P falsa
T	F	F	F	$P \Rightarrow Q$ falsa
T	T	T	T	vera

$\boldsymbol{P}$=$\{p \vee r,\ q \vee \neg r\}$ allora $\boldsymbol{P} \models p \vee q$

P	Q	R	$P \vee R$	$Q \vee \neg R$	$P \vee Q$	
F	F	F	F	T	F	
F	F	T	T	F	F	
F	T	F	F	T	T	
T	F	F	T	T	T	vera
F	T	T	T	T	T	vera
T	F	T	T	F	T	
T	T	F	T	T	T	vera
T	T	T	T	T	T	vera

Forme Normali:
Le formule del calcolo proposizionale si possono trasformare in forme standardizzate:
• Forma Normale **Congiuntiva** (CNF): una formula p è in CNF se scritta come congiunzione di disgiunzioni. **Esempio**: $(p \vee q) \wedge (\neg p \vee \neg r \vee s)$
• Forma Normale **Disgiuntiva** (DNF): una formula p è in DNF se scritta come disgiunzione di congiunzioni. **Esempio**: $(p \wedge q) \vee (\neg p \wedge \neg r \wedge s)$

Algoritmo di Trasformazione in Forma Normale:
• Fase N.1: Elimina le doppie implicazioni $p \iff q$ dalla formula sostituendole con $(p \Rightarrow q) \wedge (q \Rightarrow p)$
• Fase N.2: Elimina le implicazioni $p \Rightarrow q$ dalla formula sostituendole con $\neg p \vee q$
• Fase N.3: Sposta le negazioni $\neg$ a ridosso delle variabili proposizionali, usando De Morgan ed eliminando le doppie negazioni.
Esempio: $\neg(\neg p \vee \neg r \vee s) \rightarrow (p \wedge r \wedge \neg s)$

• Fase N.4a: Per costruire una CNF bisogna distribuire la congiunzione sulla disgiunzione ed eliminare le tautologie. **Esempio**: $(p \wedge q) \vee (\neg p \wedge \neg r \wedge s)$ da trasformare: $(p \vee (\neg p \wedge \neg r \wedge s)) \wedge (q \vee (\neg p \wedge \neg r \wedge s)) \equiv$
$(p \vee \neg p) \wedge (p \vee \neg r) \wedge (p \vee s) \wedge (q \vee \neg p) \wedge (q \vee \neg r) \wedge (q \vee s) \equiv$
$(p \vee \neg r) \wedge (p \vee s) \wedge (q \vee \neg p) \wedge (q \vee \neg r) \wedge (q \vee s)$.
• Fase N.4b: Per costruire una DNF bisogna distribuire la disgiunzione sulla congiunzione ed eliminare disgiunti insoddisfacibili e ripetizioni. **Esempio**: $(p \vee q) \wedge (\neg p \vee \neg r) \equiv$
$(p \wedge \neg p) \vee (p \wedge \neg r) \vee (q \wedge \neg p) \vee (q \wedge \neg r) \equiv$
$(p \wedge \neg r) \vee (q \wedge \neg p) \vee (q \wedge \neg r)$

1.2 Insiemistica

Un Insieme è caratterizato dagli elementi che gli appartengono.
Due insiemi A e B sono uguali se hanno gli stessi elementi e, per specificarne un insieme, è sufficiente elencarne gli elementi tramite parentesi graffe.
Singoletto: Insieme costituito da un solo elemento, esempio T={a}.
Insieme Vuoto: Con $\emptyset$ si indica l'Insieme vuoto, ovvero un insieme senza elementi.
Se P è una proprietà ben definita, possiamo definire l'insieme $\{x : P(x)\}$. Una P è ben definita per ogni valore si x quando $P(x)$ può assumere solo i 2 valori Vero o Falso.
Cardinalità: Dato un'insieme A, il numero di elementi che lo costituisce è denominato Cardinalità dell'insieme ed è denotata con $|A|$.
• Se $|A|$ è un numero intero l'insieme è finito, altrimenti è infinito.
• La cardinalità dell'insieme vuoto è zero. $\emptyset = 0$
• La cardinalità dell'insieme costituito dai numeri pari (risp. dispari) è ∞.

Relazione di Inclusione:
Due insiemi A e B, essi sono in una Relazione di Inclusione se tutti gli elementi di A sono anche elementi di B e A si dirà **sottoinsieme** di B:
$A \subseteq B \iff (\forall x)(x \in A \Rightarrow B)$.
• Se $A = B$ allora $A \subseteq B$
• Se $A \neq B$ allora $A \subset B$ o $B \supset A$

Insieme Discreto:
Un insieme A si dice **discreto** se è possibile ordinare i suoi elementi in maniera tale che tra un qualunque elemento e il suo successivo nell'ordinamento dato, non vi sono altri elementi dell'insieme.

• Ogni insieme finito è discreto, compreso quello vuoto.

Operazioni tra Insiemi:
L'**Unione** di due insiemi A e B è l'insieme formato da quegli elementi che appartengono ad almeno uno dei due insiemi A e B:
$A \cup B$=$\{x : x \in A$ oppure $x \in B\}$
Esempio: Se A=$\{1,2,3\}$ e B=$\{3,4,5\}$ allora $A \cup B$= $\{1,2,3,4,5\}$

L'**Intersezione** di due insiemi A e B è l'insieme formato da quegli elementi che appartengono ad entrambi gli insiemi A e B: $A \cap B$=$\{x : x \in A$ e $x \in B\}$
Esempio: Se A=$\{1,2,3\}$ e B=$\{3,4,5\}$ allora $A \cap B$= $\{3\}$
• Due insiemi A e B si dicono **disgiunti** se la loro intersezione è vuota, ovvero: $A \cap B = \emptyset$

Cardinalità dell'Unione:
Se A e B sono insiemi finiti allora $|A \cup B| = |A| + |B| - |A \cap B|$, ovvero la cardinalità dell'unione dei due insiemi è la somma delle cardinalità meno la cardinalità dell'intersezione.
• Se gli insiemi sono disgiunti allora: $|A \cup B| = |A| + |B|$

Proprieà di Unione ed Intersezione:
• **Commutativa**: $A \cup B = B \cup A$,$A \cap B = B \cap A$
• **Associativa**: $A \cup (B \cup C) = (A \cup B) \cup C$, $A \cap (B \cap C) = (A \cap B) \cap C$
• **Idempotenza**: $A \cup A = A$, $A \cap A = A$
• **Distributiva**:
L'unione si distribuisce all'intersezione: $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$
L'intersezione si distribuisce all'unione: $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$
• **Assorbimento**:
L'unione tra un insieme con uno che lo contiene produce l'insieme dato: $A \cup (A \cap B) = A$
L'intersezione tra un insieme con uno che lo contiene produce l'insieme dato: $A \cap (A \cup B) = A$

Differenza di due Insiemi:
Denotata con $A \backslash B$ è l'insieme formato da quegli elementi del primo insieme A che non appartengono al secondo insieme B, ovvero:
$A \backslash B = \{x : x \in A$ e $x \notin B\}$
Esempio: Se $A = \{1, 2, 3\}$ e $B = \{3, 4, 5\}$ allora $A \backslash B = \{1, 2\}$
• Cardinalità della differenza: con A e B finiti allora $|A \backslash B| = |A| - |A \cap B|$

Diagranni di Venn:
Rappresentazione classica della relazione di due o più insiemi.
Il Diagramma di Venn di n insiemi è formato da 2^n regioni.

Complemento di un Insieme:
Dato l'insieme universo U e $A \subseteq U$, l'insieme $U \backslash A$ è detto **complemento** di A.
Il complemento di un insieme A è l'insieme di tutti gli elementi che non appartengono ad A, si indica $A^C = U \backslash A$ oppure con $\overline{A} = U \backslash A$.
Esempio: Se $A = \{1, 2, 3\}$ e $U = \{1, 2, 3, 4, 5\}$ allora $\overline{A} = \{4, 5\}$

Proprietà del Complemento:
• Il complemento del complemento di un insieme è l'insieme stesso:
$(A^C)^C = A$
• $(A \cap B)^C = A^C \cup B^C$
• $(A \cup B)^C = A^C \cap B^C$
• Se U è finito e $A \subseteq U$ allora $|A^C| = |U| - |A|$.

Differenza Simmetrica di due insiemi:
L'insieme formato da quegli elementi del primo o del secondo insieme che non appartengono ad entrambi. La notazione usata è Δ, quindi:
$A \Delta B = (A \backslash B) \cup (B \backslash A)$.
Esempio: Se $A = \{1, 2, 3\}$ e $B = \{3, 4, 5\}$ allora $A \Delta B = \{1, 2, 4, 5\}$

Proprietà della Δ:
• **Commutativa**: $A \Delta B = B \Delta A$
• **Associativa**: $A \Delta (B \Delta C) = (A \Delta B) \Delta C$
• $A \Delta B = (A \backslash B) \cup (B \backslash A) = (A \cup B) \backslash (A \cap B)$
• Cardinalità della $\Delta = |A \Delta B| = |(A \backslash B) \cup (B \backslash A)| = |A \backslash B| + |B \backslash A| = |A| - |A \cap B| + |B| - |B \cap A| = |A| + |B| - 2|A \cap B|$.

Esempio Dimostrazione: $(A \backslash B) \cup (B \backslash A) = (A \cup B) \backslash (A \cap B)$
Si dimostra prima $(A \backslash B) \cup (B \backslash A) \subseteq (A \cup B) \backslash (A \cap B)$.
Sia $x \in (A \backslash B) \cup (B \backslash A)$. Si hanno due casi:
• $x \in (A \backslash B) \rightarrow x \in A$ e $x \notin B$. Allora $x \in A \rightarrow x \in A \cup B$ e $x \notin A \cap B$ visto che $x \notin B$. Infine $x \in (A \cup B) \backslash (A \cap B)$.
• $x \in (B \backslash A) \rightarrow x \in B$ e $x \notin A$. Allora $x \in B \rightarrow x \in A \cup B$ e $x \notin A \cap B$ visto che $x \notin A$. Infine $x \in (A \cup B) \backslash (A \cap B)$.
Per entrambi i casi $x \in (A \cup B) \backslash (A \cap B)$ quindi
$(A \backslash B) \cup (B \backslash A) \subseteq (A \cup B) \backslash (A \cap B)$

Si dimostra ora $(A\backslash B) \cup (B\backslash A) \supseteq (A \cup B)\backslash(A \cap B)$.
Sia $x \in A \cup B)\backslash(A \cap B)$. $x \in A \cup B$ e $x \notin A \cap B$ quindi x apparterrà solo ad uno dei due insiemi. Si hanno due casi:
• $x \in A$ e $x \notin B$, quindi $A\backslash B$. Allora $x \in (A\backslash B) \cup (B\backslash A)$.
• $x \notin A$ e $x \in B$, quindi $B\backslash A$. Allora $x \in (A\backslash B) \cup (B\backslash A)$.
Allora per entrambi i casi avremo $(A\backslash B) \cup (B\backslash A) \supseteq (A \cup B)\backslash(A \cap B)$.
Per concludere: $(A\backslash B) \cup (B\backslash A) = (A \cup B)\backslash(A \cap B)$.

Insieme delle Parti:
Dato un Insieme T consideriamo un insieme i cui elementi sono tutti sottoinsiemi di T, chiamato **Insieme delle Parti** di T e si indica con $P(T)$ e $pow(T)$. È anche detto **Famiglia di Insiemi**.
Es: Sia $T = \{1, 2, 3\}$ allora $P(T) = \{\emptyset, \{1\}\{2\}\{3\}\{1, 2\}\{1, 3\}\{2, 3\}\{1, 2, 3\}\}$.

Cardinalità dell'Insieme delle Parti:
Sia T un insieme finito, con $|T| = n$, $|P(T)| = 2^n$.
Es: $T = \emptyset \rightarrow |P(T)| = 1$, $|T| = 1 \rightarrow |P(T)| = 2$, $|T| = 2 \rightarrow |P(T)| = 4$, $|T| = 3 \rightarrow |P(T)| = 8$

Proprietà dell'Insieme delle Parti:
Prima proprietà: $P(A \cap B) = P(A) \cap P(B)$. Si dimostra con due casi:
• Caso $\subset$: Supponiamo l'insieme $X \in P(A \cap B)$, allora $X \subset A \cap B$ quindi $X \subset A$ e $X \subset B$. Allora concludiamo che $X \in P(A)$ e $X \in P(B)$ da cui $X \in P(A) \cap P(B)$.
• Caso $\supset$: Supponiamo l'insieme $X \in P(A) \cap P(B)$, allora $X \in P(A)$ e $X \in P(B)$. Quindi $X \subseteq A$ e $X \subseteq B$ ovvero $X \subseteq A \cap B$ che implica $X \in P(A \cap B)$.
Seconda proprietà: $P(A \cup B) \supset P(A) \cup P(B)$. Si dimostra supponendo un insieme $X \in P(A \cup B)$ tale che $X \notin P(A) \cup P(B)$ per qualche insieme A e B. Si hanno due casi:
• Caso $\supset$: Supponiamo l'insieme $X \in P(A) \cup P(B)$, allora $X \in P(A)$ oppure $X \in P(B)$. Nel primo caso avremo $X \subseteq A$ mentre nel secondo $X \subseteq B$. In entrambi i casi $X \subseteq A \cup B$ da cui $X \in P(A \cup B)$.
• Caso $\neq$: Sia $A = \{1, 2\}$ e $B = \{1, 3\}$. L'insieme $A \cup B = \{1, 2, 3\}$ appartiene a $P(A \cup B)$ ma non a $P(A) \cup P(B)$.

Famiglie Infinite:
Una famiglia di insiemi di dice **infinita** se ha un numero infinito di elementi, mentre si dice **finita** se ne ha un numero finito. Non riguarda la cardinalità.
Esempi:
• $F = \{P, D\}$ con P insieme dei numeri pari e D insieme dei numeri dispari. Sono entrambi insiemi infiniti ma la famiglia è **finita**.
• $F = \{P_1, P_2, P_3, ...\}$ dove $P_i = \{2^1, 2^2, ..., 2^i\}$. La famiglia è **infinita** ma i suoi elementi sono insiemi finiti.

Unione ed Intersezione di Famiglie infinite:
• $\bigcup_{X \in F} X = \{x : \exists X, X \in F, x \in X\}$
• $\bigcap_{X \in F} X = \{x : \forall X \in F, x \in X\}$

Insiemi Chiusi:
Dato un insieme $\mathbb{U}$, se un operazione può essere completata all'interno di $\mathbb{U}$ allora si dice che $\mathbb{U}$ è chiuso rispetto a tale operazione.
Esempi: L'insieme $\mathbb{N}$ è chiuso rispetto alla somma e al prodotto, ma non lo è rispetto alla sottrazione. L'insieme $\mathbb{Z}$ è chiuso rispetto alla sottrazione, ma non lo è rispetto alla divisione.

Chiusura rispetto ad Unione ed Intersezione:
Sia F una famiglia di insiemi:
• F è chiusa rispetto all'unione se per ogni coppia di insiemi X e $Y \in F$ anche $X \cup Y \in F$.
• F è chiusa rispetto all'intersezione se per ogni coppia di insiemi X e $Y \in F$ anche $X \cap Y \in F$.
• **Famiglia Complemento**: Sia $F \subseteq P(U)$. Per ogni $X \in F$ il complementare di F rispetto ad U, ovvero $X^C = U \backslash X$ è anche elemento di $P(U)$. Possiamo quindi definire $F^C = \{X^C : X \in F\}$.
Teorema: La famiglia F è chiusa rispetto all'unione se e solo se la famiglia F^C è chiusa rispetto all'intersezione. **Dimostrazione**:
Sia F chiusa rispetto all'unione e siano $X, Y \in F^C$. Esistono $A, B, \in F$ tali che $X = A^C$ e $Y = B^C$. Quindi $X \cap Y = A^C \cap B^C$, per De Morgan $= (A \cap B)^C$. Poiché $A \cup B \in F$ si ha che $(A \cup B)^C \in F^C$. **Viceversa**:
Sia F^C chiusa rispetto all'intersezione e siano $A, B \in F^C$. Sappiamo che $A^C, B^C, A^C \cup B^C \in F$. Ma per De Morgan $A^C \cap B^C = (A \cup B)^C$ quindi $A \cup B \in F$.

Chiusura con operazione generica *
Data $F \subseteq U$ ed un operazione generica * sugli insiemi di F. La chiusura di F rispetto a * è la più piccola famiglia $F_* \supseteq F$ tale che F_* è chiusa rispetto a *. F_* contiene tutti e soli gli insiemi di F e tutti gli elementi ottenubili con * su 2 o più elementi di F.
Esempio: Con $F = \{\{1,2,3\},\{1,2\},\{1,3\},\{2,4\}\}$ non chiusa rispetto alla unione. La sua chiusura sarà $F' = \{\{1,2,3\},\{1,2\},\{1,3\},\{2,4\},\{1,2,3,4\},\{1,2,4\}\}$.
Con F' è chiusa rispetto all'unione ma non è la chiusura di F:
$F'' = \{\{1,2,3\},\{1,2\},\{1,3\},\{2,4\},\{1,2,3,4\},\{1,2,4\},\{1,3,4\}\}$.
Costruzione di una Chiusura rispetto ad Unione ed Intersezione:
Sapendo che $|F| = m$:
• Costruisco F' con tutti gli elementi di F
• $\forall i = 2$ fino ad m calcolo F_i usando tutte le coppie di elementi $x \in F$ e $y \in F_{i-1}$ e mettendo $X \cup Y$ o $(X \cap Y)$ in F_i.
• Pongo infine: $F_\cup = \bigcup_{i=1}^{m} F_i$ o $F_\cap = \bigcap_{i=1}^{m} F_i$

Definizione di Partizione:
Una F è una partizione di U se gli elementi di F sono sottoinsiemi di U, dette parti, che coprono U senza sovrapporsi:
• $\forall X \in F$ si ha che $X \subseteq U$
• $U_{X \in F} X = U$
• $\forall X, Y \in F, X \neq Y$ si ha $X \cap Y = \emptyset$.
Es: Sia $U = \{1,2,3,...,12\}$ l'insieme numerico che rappresenta i mesi dell'anno.
Allora $F = \{\{1,3,5,,7,8,10,12\},\{2\},\{4,8,9,11\}\}$ è una partizione.

Coppie Ordinate:
Consideriamo due elementi x e y e creiamo una coppia (x,y):
• $(x,y) \neq (y,x)$, tranne se $x = y$;
• $(x,y) = (x',y') \iff x = x'$ e $y = y'$;
• $(x,y) \neq \{x,y\}$.

Insieme Prodotto:
Siano A e B due insiemi non vuoti, l'insieme prodotto di A e B è $A \times B$, l'insieme di tutte le coppie ordinate (x,y) con $x \in A$ e $y \in B$. Quindi $A \times B = \{(x,y) : x \in A \text{ e } y \in B\}$.
• La cardinalità di un insieme prodotto è $|A \times B| = |A| \cdot |B|$
• La definizione di insieme prodotto si estende al caso di un numero finito qualsiasi di insiemi $A_1, ...A_n$, con le loro n-uple ordinate $(x_1, ..., x_n)$.

Paradosso di Russell:
Partendo dal concetto intuitivo di insieme deduciamo che in generale un insieme **non appartiene** a sé stesso. Però possiamo anche immaginare la possibilità di un insieme che appartiene a sé stesso. Ad esempio, l'insieme di tutti gli insiemi che hanno un numero infinito di elementi, sicuramente appartiene a sé stesso.
Se assumiamo che una qualunque "proprietà" possa definire un insieme, possiamo anche costruire l'insieme di tutti gli insiemi che non appartengono a se stessi, ovvero $S = \{A : A \text{ è un insieme e } A \in A\}$.
E allora $S \in S$?
• Se $S \in S$ dalla definizione di S deduciamo che $S \notin S$.
• Se $S \notin S$ dalla definizione di S deduciamo che $S \in S$.
Per evitare questa evidente contraddizione imponiamo che la definizione di insieme deve implicitamente includere che tale insieme sia anche sottoinsieme di un insieme conosciuto. Se $S \nsubseteq U$, allora: $S = \{A : A \subseteq U, A \neq A\}$.

1.3 Relazioni e Funzioni

Relazione Binaria:
Sia U un insieme non vuoto con relazione binaria indichiamo un predicato in 2 variabili definito sugli elementi di $U \times U$, ovvero $R \subseteq U \times U$.
• Il sottoinsieme di $U \times U : \{(x, y) : (x, y) \in U \times U \text{ e } R(x, y)\}$ è costituito da tutte le coppie per cui vale la relazione ed è il grafico della relazione, si denota con $R(x, y)$ o $(x, y) \in R$.
• Con due insieme A e B diventa $\{(x, y) : (x, y) \in A \times B \text{ e } R(x, y)\}$

Funzione:
Una Relazione f definita $A \times B$ si dice funzione di A(dominio) in B(codominio) se, per ogni $x \in A$, esiste uno ed uno solo $y \in B$ tale che $(x, y) \in f$.
• Notazione Classica: $f : A \to B$
• $\forall x \in A$ l'unico elemento $y \in B$ tale che $(x, y) \in f$ si indica con $f(x)$.
Funzioni Particolari:
• Dato $A, f : A \to A | \forall x, f(x) = x$, si dice **Applicazione Identica** di A.
• Dati A e $B, f : A \times B \to A | \forall (x, y),\ f(x, y) = x$ si dice proiezione canonica su A.
• Dati A e $B, f : A \times B \to B | \forall (x, y),\ f(x, y) = y$ si dice proiezione canonica su B.

Immagine:
Dato $f : A \to B$ e un sottoinsieme X di A si dice **Immagine** di X il sottoinsieme di B costituito dagli elementi che provengono da qualche elemento di X, Si indica con $f(X) = \{y : y \in B \text{ e } (\exists x \in X) | f(x) = y\}$
Funzione Suriettiva:
Data un'applicazione $f : A \to B$ se l'immagine $f(A) = B$ allora la funzione si dice **suriettiva**.
Es: L'applicazione identica in un qualunque insieme e le proiezioni canoniche su $X \times Y$.
Funzione Iniettiva:
Data un'applicazione $f : A \to B$ se porta elementi distinti ad elementi distinti allora la funzione si dice **iniettiva**: $\forall x, y \in A$, se $x \neq y$, allora $f(x) \neq f(y)$.
Es: L'applicazione identica in un qualunque insieme e la funzione $f(n) = n + 1$.
Funzione Biiettiva:
Data un'applicazione $f : A \to B$ si dice **biiettiva** se è sia iniettiva che suriettiva.
Es: L'applicazione identica in un qualunque insieme e la funzione $f(n) = 2n$.

Teorema:
Se A e B sono due insiemi finiti ed esiste una funzione iniettiva $f : A \to B$ allora $|A| \leq |B|$. **Dimostrazione:**
Consideriamo $f(A)$, sapendo che $f(A) \subseteq B$ e che ogni elemento di $f(A)$ è immagine di uno ed un solo elemento di A (essendo f iniettiva), affermo che in $f(A)$ ci sono tanti elementi quanti ce ne sono in A. $|A| = |f(A)| \leq |B|$.

Proprietà delle Relazioni:
Sia U un insieme con $R(x, y)$ definita in $U \times U$ essa è:
• **Riflessiva**: se $\forall x \in U$ risulta vero $R(x, x)$
• **Simmetrica**: se $\forall x, y \in U$ se $R(x, y)$ risulta vero allora lo è anche $R(y, x)$
• **Transitiva:** se $\forall x, y, z \in U$ se $R(x, y)$ e $R(y, z)$ sono vere allora anche $R(x, z)$.
Una relazione riflessiva, simmetrica e transitiva si dice **Relazione di Equivalenza** ed è indicata con $x \approx y$.

Classe di Equivalenza:
Si chiama **Classe di Equivalenza** di x l'insieme di tutti gli elementi di U equivalenti ad x, ovvero $[x] = \{y \in U : x \approx y\}$.

Teorema:
Due Classi di Equivalenza o sono disgiunte o coincidono. **Dimostrazione**: Siano $[x]$ e $[z]$ due classi di equivalenza e supponiamo che esse abbiano un elemento w in comune: pertanto $w \approx x$ e $w \approx z$. Per la proprietà transitiva $x \approx z$.
Sia $y \in [x]$, cioè $y \approx x$. Per la proprietà transitiva $y \approx z$, cioè $y \in [z]$. Quindi $[x] \leq [z]$. Analogamente si dimostra $[z] \leq [x]$.

Classi di Equivalenza e Partizioni:
Data una relazione di equivalenza R su U, consideriamo la famiglia F costituita da tutte le classi di equivalenza.
F è un sottoinsieme di $P(U)$ tale che:
• $\forall X \in F$ si ha che $X \neq \emptyset$ e $\bigcup_{X \in F} X = U$, infatti $\forall x \in U, x \in [X]$.
• $\forall X, Y \in F, X \neq Y$ si ha $X \cap Y = \emptyset$
Una relazione di equivalenza di R individua una partizione F su U che viene detta **Insieme Quoziente** di U rispetto ad R ed è indicata con U/R.
Applicazione Canonica sul Quoziente:
Data in U una relazione R risulta individuata l'applicazione **suriettiva** $U \to U/R$ che porta ogni $x \in U$ nella sua classe di equivalenza $[x]$.

Relazione di Pre-Ordine (o Pre-ordinamento):
Si dice **pre-ordine** una relazione **binaria** assegnata in un insieme che gode delle proprietà riflessiva e transitiva.
• Non vale **sempre** la proprietà **simmetrica**: $R(x, y) \neq R(y, x)$
• Un insieme U su cui è definita una relazione di pre-ordine si dice pre-ordinato.
Esempi:
• Ogni relazione di equivalenza è un pre-ordinamento;
• La relazione $x \leq y$ nell'ambito degli interi/razionali/reali è un pre-ordinamento.

Relazione di Ordine (o Ordinamento):
Si dice **ordine** una relazione di pre-ordine che gode della proprietà **antisimmetrica**. Una relazione R in un insieme U vale della proprietà **antisimmetrica** se: $\forall x, \forall y \in U$ si ha che: $(R(x, y)$ e $R(y, x)) \to x = y$.
• Un insieme U su cui è definita una relazione di ordine si dice ordinato.

Massimo e Massimale di un Insieme:
Un elemento M di un insieme ordinato U si dice **massimo** se $\forall x \in U$ si ha $x \leq M$. Si dice **Massimale** se non vi è alcun elemento di U che lo supera.

Minimo e Minimale di un Insieme:
Un elemento m di un insieme ordinato U si dice **minimo** se $\forall x \in U$ si ha $m \leq x$. Si dice **Minimale** se non vi è alcun elemento di U ad esso inferiore.
Osservazioni:
• Ogni elemento che sia massimo (risp. minimo) è anche massimale (risp. minimale) ma non viceversa;
• Un insieme ordinato può avere più massimali (risp. minimali) ma non può avere più di massimo (risp. minimo);
• In un insieme ordinato non sempre accade che due elementi x e y siano tra loro confrontabili, cioè sussista una delle due relazioni $x \leq y$ o $y \leq x$.

Insiemi Totalmente Ordinati:
Un ordinamento $\leq$ definito in un insieme U si dice **totale** o **lineare** se per ogni coppia (x, y) di elementi di U si ha $x \leq y$ oppure $y \leq x$, altrimenti si dirà **parziale**.
• Un sottoinsieme T di un insieme ordinato U sarà anch'esso ordinato.

1.4 Hitting Set

Definizione formale:
Siano U un insieme finito, $H \subseteq U$ e sia $\mathbb{A}$ una famiglia di sottoinsiemi di U tutti diversi dall'insieme vuoto. Diciamo che H è un **Hitting Set** per $\mathbb{A}$ se e solo se $\forall A \in A$ si ha $A \cap H \neq \emptyset$.
Es: Sia $U = \{a, b, c, d, e\}$ e sia $\mathbb{A} = \{\{a, b, c\}, \{a, d, e\}, \{b, c, d\}, \{c, d, e\}\}$.
L'insieme $\{a, b, c\}$ è un **HS** per $\mathbb{A}$ mentre $\{b, c\}$ o $\{d, e\}$ non lo sono.

Hitting Set Minimo:
Siano U un insieme finito, $H \subseteq U$ e sia $\mathbb{A}$ una famiglia di sottoinsiemi di U tutti diversi dall'insieme vuoto.
• Se H è un **HS** e $\forall x \in H$ l'insieme $H \backslash \{x\}$ non è un **HS**, diciamo che H è un **HS** minimale.
• Se H è un **HS** tale che $|H| = min\{|K| : K$ è un Hitting Set $\mathbf{A}\}$ allora H è un **HS** minimo.
Esempio: Sia $U = \{a, b, c, d, e\}$ e sia $\mathbb{A} = \{\{a, b, c\}, \{a, d, e\}, \{b, c, d\}, \{c, d, e\}\}$.
L'insieme $\{a, b, c\}$ è un **HS** ma non è un minimale poiché $\{a, c\}$ è un **HS**.
$\{a, c\}$ è anche minimo, visto che nessun elemento da solo è presente in tutti gli insiemi di $\mathbb{A}$.

Trovare un HS minimo:
Bisogna provare per tutti i sottoinsiemi di U. Tuttavia:
• È inefficiente, in quanto in $|U|$ i sottoinsiemi non vuoti sono $2^{|U|} - 1$. Es: se $|U| = 100$, il numero totale di operazione sarebbe dell'ordine di $1,26 \cdot 10^{30}$.
• Inoltre se gli insiemi di $\mathbb{A}$ sono tutti disgiunti bisognerebbe prendere tutti gli elementi per un **HS**. Es: Sia $U = \{a, b, c, d, e\}$ e sia $\mathbb{A} = \{\{a, b, c\}, \{a, d, e\}, \{c, d\}, \{c, d, e\}, \{d\}, \{e\}\}$. L'**HS** minimo sarà $\{a, d, e\}$.

Algoritmo Greedy:
Prende come primo elemento di U quello che appartiene al maggior numero di elementi di $\mathbb{A}$.
Per tutti gli elementi di $\mathbb{A}$ a cui x_1 non appartiene, scegliamo l'elemento x_2 che appartiene alla maggior parte di essi e così via.
Esempio: Sia $U = \{a, b, c, d, e, f\}$ e sia $\mathbb{A} = \{\{a, b, e\}, \{a, b, f\}, \{b, d\}, \{a, c, f\}, \{a, c, e\}, \{c, e, f\}\}$:
• L'elemento a appartiene a 4 insiemi e viene scelto. Rimangono 2 insiemi disgiunti, $\{b, d\}$ e $\{c, e, f\}$.
• Da questi bisogna scegliere 2 elementi, ad es: $\{d, f\}$ e formeremo $H = \{a, d, f\}$, un **HS** minimale ma non minimo.
• L'**HS** minimo è $\{b, c\}$
• Un altro **HS** che l'algoritmo può tornare è $\{a, b, c\}$ che non è minimale.

2 Parte 2

2.1 Teoria dei Numeri Interi

Insiemi Numerici:
$N \subset Z \subset Q \subset R \subset C$
Operazioni sui Numeri:
• **Somma**: (N, Z, Q, R, C);
• **Prodotto**: (N, Z, Q, R, C);
• **Sottrazione**: (Z, Q, R, C);
• **Divisione**: (Q, R, C);

Valore Assoluto:
Il Valore Assoluto di un numero intero relativo $n \in Z$ è l'intero $|n| \geq 0$ definito come:

$$|n| = \begin{cases} n & n \geq 0 \\ -n & n < 0 \end{cases}$$

Proprietà del Valore Assoluto:
Per ogni $n, m \in Z$ si ha:
• $|n| = 0 \iff n = 0$
• $|n \cdot m| = |n| \cdot |m|$
• $n + |n| \geq 0$ (e $n + |m| = 0$) $\iff n \leq 0$

Definizione Assiomatica dell'Insieme $\mathbb{N}$:
• $0 \in N$
• Ogni numero $a \in N$ ha un successore $S(a)$
• Numeri naturali hanno successori distinti.

Assioma del Buon Ordinamento:
Se S è un qualunque insieme non vuoto di numeri, allora in S esiste un elemento minimo, ovvero esiste $s \in S$ tale che $s \leq t$ per ogni $t \in S$.

Principio di Induzione:
Sia P un'affermazione riguardante i numeri naturali se:
• Caso Base: $P(0)$ è vera
• Passo Induttivo: Per ogni numero naturale n se $P(n)$ è vera,
allora è vera anche per $P(n+1)$ e per ogni altro numero naturale.
Dimostrazione:
Per assurdo poniamo che esista un $n \in N$ per cui $P(n)$ è falsa:
$S = \{n : n \in N \text{ e } P(n) \text{ è falsa}\}$.
Supponendo che S non è vuoto, per l'Assioma del Buon Ordinamento esiste in S un elemento minimo $s \neq 0$, poiché $P(0)$ è vera e per definizione $P(s)$ è falsa. Poiché $S \subset N$ deve essere $s > 0$ ed esisterà il predecessore $s - 1$ e dal momento che $s - 1 < s$ abbiamo che $s - 1 \neq S$ quindi $P(s-1)$ è vera.
Ma per il passo induttivo $P(s)$ è vera, quindi abbiamo una contraddizione.
Esempio: Dato un insieme finito A allora $|P(A)| = 2^{|A|}$.
• Caso Base: $|A| = 0 \to P(A) = \{\emptyset\}$ e quindi $|P(A)| = 1 = 2^0$
• Passo Induttivo: Supponiamo che sia vero per tutti gli insiemi A tali che $0 < |A| = n - 1$ dimostrandolo per n.

Sia A un insieme tale che $|A| = n$ e sia $a \in A$. Allora $A' = A \backslash \{a\}$ ha una cardinalità di $n-1$ elementi, quindi $|P(A')| = 2^{n-1}$.
Quindi $P(A') \subset P(A)$ e gli elementi di $P(A) \backslash P(A')$ sono tutti i sottoinsiemi di A che contengono a e sono esattamente tanti quanti sono gli elementi di $P(A')$ infatti la funzione $f_a : P(A)' \to P(A) \backslash P(A')$ che associa ad ogni elemento $X \in P(A')$ l'elemento $X \cup \{a\}$ è una corrispondenza biunivoca.
Quindi $|P(A)| = 2 \cdot |P(A')| = 2 \cdot 2^{n-1} = 2^n$.

Esempio 2: dato un intero $n \geq 1$ si ha che $1 + 2 + ... + (n-1) + n = \frac{n(n+1)}{2}$:
• Caso base: $n = 1 \to 1 = \frac{1(1+1)}{2}$ è vero
• Passo Induttivo: Supponiamo sia vero per n verificandolo per $n+1$.
Essendo vero per n abbiamo $\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$. Allora $\sum_{i=1}^{n+1} i + (n+1) = \frac{n(n+1)}{2} + n + 1 = \frac{n(n+1)+2(n+1)}{2} = n^2 + 3n + 2 = (n+1)(n+2)$ è verificato.

Floor e Ceiling: Sia $x \in R$:
• **Floor** è il più grande numero intero minore o uguale ad x, è denotato con $\lfloor x \rfloor$.
• **Ceiling** è il più piccolo numero intero maggiore o uguale ad x, è denotato con $\lceil x \rceil$.
• Esempi:

x	$\lfloor x \rfloor$	$\lceil x \rceil$
3,8	3	4
-3,8	-4	-3
3	3	3
-3	-3	-3

Divisione tra Interi:
Dati due interi $a, b \in Z$ con $b \neq 0$, chiamati rispettivamente dividendo e divisore, esistono unict due interi relativi q, r, denominati rispettivamente quoziente e resto, tali che: $a = q \cdot b + r$ con $0 \leq r < |b|$.
• **Modulo**: il resto $r > 0$ della divisione è detto **modulo** ed è denotato con $a \ mod \ b$
• **Floor**: con a e $b > 0$, q è l'intero più grande che è minore o uguale a $\frac{a}{b}$ ovvero $\lfloor \frac{a}{b} \rfloor$.
Dimostrazione 1° caso ($a \geq 0$ **e** $b > 0$)**:**
Consideriamo $S = \{a - kb : k \in N, a - kb \geq 0\}$ non vuoto, poiché per $k = 0$ abbiamo $a \in S$. Per l'Assioma del Buon Ordinamento, l'insieme S ha un minimo, $r \geq 0$.

Denotiamo con q il valore di k tale che $r = a - qb$ da cui $a = qb + r$. Se $r = a - qb$ è il minimo di S allora q è il massimo in N, tale che $a - qb \geq 0$, ovvero $q = \lfloor \frac{a}{b} \rfloor$. Se esistesse $k > q \mid a - kq \geq 0$ avremmo $(a - qb) - (a - kb) = (k - q)b \geq 0$ ma questo contraddirebbe l'ipotesi che $a - qb$ è il minimo di S.
Esempi:
• $a = 1,\ b = 10 : q = \lfloor \frac{1}{10} \rfloor = 0$ e $1 = 0 \cdot 10 + 1 \rightarrow r = 1$, ovvero $1\ mod\ 10 = 1$
• $a = 19,\ b = 10 : q = \lfloor \frac{19}{10} \rfloor = 1$ e $19 = 1 \cdot 10 + 9 \rightarrow r = 9$, ovvero $19\ mod\ 10 = 9$

Dimostrazione 2° Caso ($a < 0, b > 0$):
Consideriamo $|a| > 0 \rightarrow |a| = -a$. Esistono q' e $0 \leq r' < b$ tali che $|a| = q'b + r'$ e qundi $-a = q'b + r' \rightarrow a = (-q')b + (-r')$.
Se $r' = 0$ è dimostrato.
Se $r' > 0$ abbiamo $0 < b - r' < b$ e riscriviamo $a = (-q)'b - b + b + (-r') = (-q' - 1)b + (b - r')$ prendendo come $q = -q' - 1$ e come $r = b - r'$ lo abbiamo dimostrato. Esempi:
• $a = -1, b = 10$: per $a = 1$ abbiamo $q' = 0$ e $r' = 1$. Per $a = -1$, $q = 0 - 1 = -1$ e $r = 10 - 1 = 9$. Infatti $-1 = (-1) \cdot 10 + 9$ e quindi $-1\ mod\ 10 = 9$
• $a = -19, b = 10$: per $a = 19$ abbiamo $q' = 1$ e $r' = 9$. Per $a = -19$, $q = -1 - 1 = -2$ e $r = 10 - 9 = 1$. Infatti $-19 = (-2) \cdot 1$ e quindi $-19\ mod\ 10 = 1$

Dimostrazione 3° Caso ($a > 0, b < 0$):
Consideriamo $|b| > 0$ e sappiamo che $|b| = -b$. Esistono q' ed $0 \leq r' < |b|$ tali che $a = q'|b| + r'$ e quindi $a = q'(-b) + r' \rightarrow a = (q')b + r'$.
Prendendo come $q = q'$ e come $r = r'$ il 3° caso è dimostrato. Esempio:
• $a = 14, b = -4$: per $b = 4$ abbiamo $q = 3$ e $r = 2$. Per $b = -4$ abbiamo $q = -3$ e $r = 2$. Infatti $14 = -3 \cdot (-4) + 2$ e quindi $14\ mod\ (-4) = 2$

Dimostrazione 4° Caso ($a < 0, b < 0$):
Consideriamo $|a| > 0$ e $|b| > 0$ e quindi $|a| = -a$ e $|b| = -b$. Esistono q' e $0 \leq r' < |b|$ ovvero $0 \leq r' < -b$ tali che $|a| = q'|b| + r'$. Usando i valori di q' ed r' e agendo come nel 2° caso abbiamo $a = (-q' - 1)|b| + |b| - r' = (q' + 1)b - b - r'$.
Prendendo come $q = q' + 1$ e come $r = -b - r'$, il 4° caso è dimostrato. Esempio:
• $a = -14, b = -4$: per $a = 14$ e per $b = 4$ abbiamo $q = 3$ e $r = 2$. Per $a = -14$ $b = -4$ abbiamo $q = 4$ e $r = 2$. Infatti $-14 = 4 \cdot (-4) + 2$ e quindi $-14\ mod\ (-4) = 2$

Teorema di Unicità del Quoziente e Resto:
Dati $a, b \in Z$ supponiamo per assurdo che esistono $q_1 \neq q_2$ e $r_1 \neq r_2$ tali che $0 \leq r_1 < |b|$, $0 \leq r_2 < |b|$ e $a = bq_1 + r_1$ e $a = bq_2 + r_2$. Sottraendo membro a membro otteniamo $0 = b(q_1 + q_2) + (r_1 - r_2)$ ovvero $b(q_2 - q_1) = r_1 - r_2$ e passando ai valori assoluti $|b(q_2 - q_1) = |b| \cdot |(q_2 - q_1)| = |r_1 - r_2|$.
Distinguiamo i 2 casi:
• $r_1 \geq r_2 : |r_1 - r_2| = r_1 - r_2 \leq r_1 < |b|$. $|b| > r_1 - r_2 = |r_1 - r_2| = |b| \cdot |q_2 - q_1|$ da cui otteniamo $1 > |(q_2 - q_1)| \geq 0$ e quindi, essendo q_1 e q_2 numeri interi, deduciamo che $|(q_2 - q_1)| = 0$ ovvero $q_1 = q_2$. Deduciamo con $b(q_2 - q_1) = r_1 - r_2$ che $r_1 = r_2$.
• $r_1 < r_2 : |r_2 - r_1| = r_2 - r_1 < r_2 < |b|$. $|b| > r_2 - r_1 = |r_2 - r_1| = |b| \cdot |q_2 - q_1|$ da cui otteniamo $1 > |(q_2 - q_1)| \geq 0$ e quindi, essendo q_1 e q_2 numeri interi, deduciamo che $|(q_2 - q_1)| = 0$ ovvero $q_1 = q_2$. Deduciamo con $b(q_2 - q_1) = r_2 - r_1$ che $r_1 = r_2$.

Definizione di Divisibilità:
Dati due interi relativi $n, m \in Z$ si dice che m è un divisore di n se esiste un intero relativo $k \in Z$ tale che $n = k \cdot m$. Notazione: $m|n$ e $m \nmid n$.
Esempi: $2|8$, $-5|15$, $5 \nmid 16$, $3 \nmid -7$.
Numero Pari:
Un numero n si dice **pari** se il resto della sua divisione per 2 è uguale a 0, ovvero esiste un intero k tale che $n = 2k$.
Numero Dispari:
Un numero n si dice **dispari** se il resto della sua divisione per 2 è uguale a 1, ovvero esiste un intero k tale che $n = 2k + 1$.
Somma dei primi n numeri dispari uguale a n^2:
Si dimostra per induzione:
• Caso base: $n = 1 \rightarrow n^2 = 1^2 = 1$
• Passo induttivo: Supponiamo che la somma dei primi $n-1$ numeri dispari sia uguale a $(n-1)^2$. Essendo i numeri dispari nella forma $2k+1$ con $0 \leq k \leq n-1$, l'ennesimo numero dispari sarà uguale a $2(n-1)+1$ che se sommiamo a $(n-1)^2$ otteniamo $(n-1)^2 + 2(n-1) + 1 = n^2 - 2n + 1 + 2n - 2 + 1 = n^2$.

Proprietà della Divisibilità:
Siano $a, b, c \in Z$:
• **Somma**: se $a|b$ e $a|c$ allora $a|(b + c)$. **Dimostrazione**:
Dato che $a|b$ esiste x tale che $b = ax$ e dato che $a|c$ esiste y tale che $c = ay$. Quindi $b + c = ax + ay = a(x + y)$ e ponendo $z = x + y$ abbiamo un intero tale che $b + c = az$, dimostrando che $a|(b + c)$.

• **Prodotto**: se $a|b$ allora $a|bc$. **Dimostrazione**:
Dato che $a|b$ esiste x tale che $b = ax$, quindi $bc = axc$ che dimostra $a|bc$.
• **Transitività**: se $a|b$ e $b|c$ allora $a|c$.
Dimostrazione: Dato che $a|b$ esiste x tale che $b = ax$ e dato che $b|c$ esiste y tale che $c = yb$. Quindi $by = axy$, ossia $c = axy$ e, ponendo $z = xy$, abbiamo un intero tale che $c = az$ che dimostra $a|c$.
• **Quadrato**: se $a|b$ allora $a|b^2$.
Dimostrazione: Conseguenza del caso prodotto.
• **Combinazione Lineare**: se $a|b$ e $a|c$ allora $a|(hb + kc)$ $\forall h, k \in Z$.
Dimostrazione: Dato $a|b$ avremo $a|hb$ $\forall h \in Z$ e dato $a|c$ avremo $a|kc$ $\forall k \in Z$, allora $a|(hb + kc)$.
• **Numero 0**: Ogni intero relativo $a \in Z$ è divisore di 0, ovvero 0 è multiplo di qualunque intero relativo, cioè $a|0$. Il numero 0 è divisore solo di sé stesso.
Dimostrazione:
- $\forall a \in Z$ abbiamo $a \cdot 0 = 0$, quindi $a|0$.
- Se $0|a$ allora esiste x tale che $0 \cdot x = a$. Ma $0 \cdot x = 0$ e quindi $a = 0$.
• **Antisimmetrica**: Siano $a, b \in Z$, se $a|b$ e $b|a$ allora $|a| = |b|$, ossia $a = \pm b$.
Dimostrazione:
Dalle ipotesi abbiamo che $a = bx$ e $a = by$, quindi $a = axy$. Abbiamo allora che $a(xy - 1) = 0$ che implica che $a = 0$ oppure $xy = 1$. Se il prodotto fra interi è nullo almeno uno dei fattori deve essere nullo. Quindi:
- Se $a = 0$ allora $b = 0x \to b = 0$ ovvero $0 = 0y$ e la proprietà è dimostrata.
- Se $xy = 1$ allora o sono entrambi uguali a 1 o a -1. Quindi $y = \pm 1$ e $a = \pm b$.
• **Divisori Banali**: Siano $a \in Z$. Allora $\pm a|a$ e $\pm 1|a$.

Minimo Comune Multiplo (MCM):
Siano $a, b \in Z$ entrambi non nulli, si chiama Minimo Comune Multiplo tra a e b un terzo intero $m \in N$ tale che m è il più piccolo multiplo sia di a che di b, ovvero:
• $a|m$ e $b|m$ cioè a e b sono entrambi divisori di m.
• Se x è un multiplo comune di a e b, ovvero $a|x$ e $b|x$, allora $m|x$ cioè m divide ogni altro multiplo comune di a e b.

Massimo Comune Divisore (MCD):
Siano $a, b \in Z$ entrambi non nulli, si chiama Massimo Comune Divisore tra a e b un terzo intero $d \in Z$ tale che:
• $d|a$ e $d|b$ cioè d è un divisore sia di a che di b
• Se x è un divisore comune di a e b, ovvero $x|a$ e $x|b$, allora $x|d$ cioè d è multiplo di ogni altro divisore comune di a e b.

Algoritmo di Euclide:
L'algoritmo si basa sul Principio d'Induzione. Siano a e $b \in N$ e sia $b \leq a$:
• Caso Base: se $b = 0$ allora $MCD(a, b) = a$
• Passo Induttivo: visto che $a = qb + r$ con $0 \leq r < b$ allora $MCD(a, b) = MCD(b, a \ mod \ b) = MCD(b, r)$.
Notiamo che se $b|a$ allora $a = qb$ ed $r = 0$, quindi $MCD(a, b) = MCD(b, 0) = b$ per il caso base.
Dimostrazione della Correttezza dell'algoritmo:
Se $a = qb + r$ con $r \neq 0$ e $0 < r < b$ allora $MCD(a, b) = MCD(b, r)$:
• Se d è un divisore di a e b allora esistono h e k tali che $a = hd = qkd + r$. Quindi $r = d(h - qk)$ e quindi d è anche un divisore di r.
• Se d è un divisore di b ed r allora esistono h e k tali che $a = qb+r = qkd+hd$. Quindi d è anche un divisore di a visto che $a = d(qk + h)$
Esempio: $MCD(330, 156) = x_1 = 330$ e $x_2 = 156$.
$x_3 = 330\%156 = 18 \rightarrow 156 \cdot 2 + 18$. $x_4 = 156\%18 = 12 \rightarrow 18 \cdot 8 + 12$.
$x_5 = 18\%12 = 6 \rightarrow 12 \cdot 1 + 6$. $x_6 = 12\%6 = 0 \rightarrow 6 \cdot 2 + 0$. $MCD(330, 156) = 6$
Teorema:
Siano $a, b \in N$ non entrambi uguali a 0, allora esistono $h, k \in Z$ tali che $MCD(a, b) = a \cdot h + b \cdot k$.

Numeri Primi e Coprimi:
Si definisce Numero **Primo** un intero $p \in Z$, tale che p ha come unici divisori quelli banali e tale che $p \neq \pm 1$.
Due numeri $a, b \in Z$ si dicono **Coprimi** se $MCD(a, b) = 1$.
Osservazioni:
• Sappiamo allora che esistono $h, k \in Z$ tali che $a \cdot h + b \cdot k = 1$. Vale anche il viceversa.
• Siano $a, b \in N$ non entrambi uguali a 0, se esistono $h, k \in Z$ tali che $ah + bk = 1$, allora $MCD(a, b) = 1$.
Dimostrazione: Sia $d = MCD(a, b)$. Quindi $d|a$ e $d|b$ allora $d|(ah + bk)$. Ma l'unico divisore positivo di 1 è proprio 1 stesso, quindi $d = 1$.

Proprietà dei Numeri Coprimi:
• Due numeri interi consecutivi sono coprimi.
Dimostrazione: Siano n e $n + 1$ due numeri interi consecutivi, allora per $h = 1$ e $k = -1$ abbiamo $1 = h(n + 1)k(n)$ ovvero $1 = n + 1 - n \rightarrow 1 = 1$.
• Siano $a, b, c \in Z$ tali che $c|a \cdot b$ e c, a coprimi allora $c|b$. *Osservazioni*:
- L'ipotesi di Comprimalità è fondamentale, $9|3 \cdot 6$ ma $9 \nmid 3$ e $9 \nmid 6$.
- Un numero primo p divide almeno a o b di $p|a \cdot b$.

Dimostrazione: Siano $a, b, c \in Z$ tali che $c|a \cdot b$ e c, a coprimi. Quindi esiste h tale che $hc = ab$ ed esistono k, k' tali che $1 = ka + k'c$.
Moltiplicando per b ambo i termini otteniamo $b = kab + k'cb$ da cui $b = khc + k'cb = c(kh + k'b)$ e quindi $c|b$.
• Siano $a, b, c \in Z$ tali che $a|c$ e $b|c$, se a e b sono coprimi allora $a \cdot b|c$.
- L'ipotesi di coprimalità è fondamentale, $4|12$ e $6|12$ ma $24 \nmid 12$.
Dimostrazione: Siano $a, b, c \in Z$ tali che $a|c$ e $b|c$ ed a, b coprimi. Allora esistono h, k, h', k' tali che $c = ah$, $c = bk$ e $1 = ah' + bk'$. Moltiplicando per c ambo i termini otteniamo $c = ah'c + bk'c = ah'bk + bk'ah = ab(h'k + k'h)$ e quindi $ab|c$.

Teorema della Fattorizzazione degli Interi:
Ogni intero $n > 1$ si può esprimere come prodotto di numeri primi positivi ed in modo unico a meno dell'ordine dei fattori.
Dimostrazione Esitenza Fattorizzazione di n:
Per **assurdo**, se esistessero interi > 1 che non siano prodotto di numeri interi positivi, potremmo costruire l'insieme $S = \{n : n \in N$, non prodotto di numeri primi$\}$. Per l'Assioma del Buon Ordinamento, scegliamo s come minimo dell'insieme S. Per definizione s **non è primo**, perché se lo fosse sarebbe prodotto di primi positivi e quindi non sarebbe in S.
Quindi s ha divisori diversi da quelli banali e quindi almeno un divisore positivo $1 < d < s$. Esiste quindi $c \in N$ tale che $s = d \cdot c$ e anche $1 < c < s$. Poiché c e d sono minori di s allora c e d sono prodotti di primi positivi e quindi anche s lo è.
Dimostrazione Unicità:
Sia $n = p_1 \cdot p_2 \cdot ... \cdot p_r = q_1 \cdot q_2 \cdot ... \cdot q_s$ con p_i e q_j numeri primi positivi. Bisogna dimostrare che $r = s$ e che possiamo riordinare i numeri primi positivi ed avere $p_i = q_i$ per ogni i. Si dimostra per induzione su r.
• Caso Base: $r = 1$. Se $n = p_1$ allora n è primo e quindi, da $p_1 = q_1 \cdot q_2 \cdot ... \cdot q_s$ otteniamo che $s = 1$ e $q_r = q_s$
• Passo Induttivo: Supponiamo che la tesi sia vera per r e dimostriamola per $r + 1$. Se $n = p_1 \cdot p_2 \cdot ... \cdot p_{r+1} = q_1 \cdot q_2 \cdot ... \cdot q_s$ è divisore di almeno uno dei fattori primi p, allora $q_1 = p_1$. Siccome il numero di fattori coincide in entrambi i membri $(r = s - 1)$ il teorema è dimostrato.

Teorema di Euclide
I numeri primi sono **infiniti**.

Dimostrazione:
Supponiamo per assurdo che i numeri primi sono finiti e che esiste n tale che i numeri primi sono p_n. Consideriamo $h = p_1 \cdot p_2 \cdot ... \cdot p_n$ e $k = p_1 \cdot p_2 \cdot ... \cdot p_{n+1}$, h e k sono coprimi per proprietà. Tuttavia k non può essere primo perché è diverso da $p_1 \cdot p_2 \cdot ... \cdot p_n$ che abbiamo supposto essere tutti i numeri primi, quindi dal Teorema della Fattorizzazione sappiamo che k si può scrivere in modo unico come prodotto di primi positivi. Ma questi devono essere compresi entro p_n e quindi k non sarebbe coprimo per h, il ché è un assurdo.

Densità dei primi:
Sia $n \in N$ e sia $\pi(n)$ il numero di "numeri primi" minori o uguali ad n. Allora:

$$\lim_{n \to \infty} = \frac{\pi(n)}{\frac{n}{\ln n}} = 1$$

Esempi:
• per $n = 100$ stimati $\frac{100}{\ln 100} = \frac{100}{4{,}6} \approx 22$ (effettivi 25);
• per $n = 1000$ stimati $\frac{1000}{\ln 1000} = \frac{1000}{6{,}9} \approx 145$ (effettivi 168);

Teorema di Bertrand:
Per ogni $n \geq 2$ esiste un numero primo p tale che $n < p < 2n$.

Crivello di Erastone:
Il Crivello di Erastone è un algoritmo che permette di calcolare tutti i numeri primi compresi tra 2 ed n.
• Si scrivono tutti i numeri in sequenza da 2 ad n;
• Si cancellano i multipli di ogni numero prima partendo dal 2, i rimanenti saranno primi. Esempio:

2	3	4	5	6		2	3		5		
7	8	9	10	11		7		9		11	
12	13	14	15	16	→		13		15		→
17	18	19	20	21		17		19		21	
22	23	24	25	26			23		25		

	2	3		5			2	3		5	
	7				11		7				11
→		13				→		13			
	17		19				17		19		
		23		25				23			

Criteri di Divisibilità:
• Divisibilità per 2: n è divisibile per 2 solo se n è pari.
Esempio: 12, 38, 1536.
• Divisibilità per 3: n è divisibile per 3 solo se la sua somma delle cifre è un numero divisibile per 3.
Esempio: $1590 \to 1+5+9+0 = 15 \to 1+5 = 6$, divisibile per 3.
• Divisibilità per 5: n è divisibile per 5 solo se la cifrà dell'unità è 0 oppure 5.
• Divisibilità per 7; n è divisibile per 7 solo se $q - 2r$ è divisibile per 7.
Dimostrazione:
Supponiamo n sia divisibile per 7. Esisterà h tale che $n = 7h$. Dividendo n per 10 otteniamo $n = 10q + r$. Abbiamo: $7h = 10q + r \to 7h - 21r = 10q - 20r \to 7(h - 3r) = 10(q - 2r)$. Quindi 7 divide il prodotto $10(q - 2r)$ e non divide 10 allora dividerà $q - 2r$.
Viceversa, supponiamo $q - 2r$ sia divisibile per 7. Allora esiste k tale che $q - 2r = 7k$ e quindi $q = 7k + 2r$.
Allora $n = 10q + r = 10(7k + 2r) = 70k + 21r = 7(10k + 3r)$.
Esempi:
- $84 = 8 - 2 \cdot 4 = 0$ quindi $7|84$;
- $581 = 58 - 2 \cdot 1 = 56 = 7 \cdot 8$ quindi $7|581$.
• Divisibilità per 9: n è divisibile per 9 solo se la somma delle sue cifre è un numero divisibile per 9.
Dimostrazione:
Il numero n è caratterizzato dalla seguente:

$$\sum_{i=0}^{k} a^i \cdot 10^i$$

dove a_0 sono le unità, a_1 le decine, ed in generale a_i il coefficiente della potenza 10^i. Quindi, $a_0, a_1, ..., a_k$ sono le cifre che rappresentano il numero. Otteniamo allora che:

$$n - m = \sum_{i=0}^{k} a^i \cdot 10^i - \sum_{i=0}^{k} a^i \cdot (10^i - 1) = \sum_{i=0}^{k} a_i \cdot 9 \cdot b_i = 9 \cdot \sum_{i=0}^{k} a^i \cdot b^i$$

Esempi:
- 199 non è divisibile per 9 però $199 - 19 = 180$ è divisibile per 9;
- 640 non è divisibile per 9 però $640 - 10 = 630$ è divisibile per 9;

• Divisibilità per 11: n è divisibile per 11 se la differenza tra la somma delle cifre di posto **dispari** (a) e la somma delle cifre di posto **pari** (b) è divisibile per 11.
Esempio: 14894, con $a = 1 + 8 + 4 = 13$ e $b = 4 + 9 = 13$ allora $a - b = 0$, quindi è divisibile per 11.
• Divisibilità per altri numeri primi: Un intero $n = 10q + r$ è divisibile per p se e solo se $q + a \cdot r$ è divisibile per p, con i seguenti valori di p ed a:

p	a
7	-2
13	4
17	-5
19	2
23	7

Esempio: $n = 96577$, $q = 9657$ e $r = 7$
Vogliamo vedere se è divisibile per 13, quindi: $q + 4r = 9657 + 28 = 9685$.
Si reitera quindi il processo fino a quando non abbiamo un numero banale:
$q = 968$, $r = 5 \rightarrow 968 + 20 = 988$.
$q = 98$, $r = 8 \rightarrow 98 + 32 = 130$.
$q = 13$, $r = 0 \rightarrow 13 + 0 = 13$ quindi 96577 è divisibile per 13.

Radice Numerica:
Dato $n \in N$ la **radice numerica** di n, denotata con $p(n)$ è la somma delle cifre reiterata sino ad ottenere una sola cifra.
Esempio: $198 = 1 + 9 + 8 = 18 = 1 + 8 = 9 \rightarrow p(198) = 9$

Dimostrazione: $\sqrt{2}$ (non) è razionale:
Supponiamo per assurdo che $\sqrt{2}$ non sia un numero razionale.
Assumiamo che presi a e $b \in N$, abbiamo che $\sqrt{2} = \frac{a}{b}$ con $MCD(a, b) = 1$.
In tal modo, la frazione sarà **ridotta**, di conseguenza almeno uno dei 2 numeri deve essere **dispari**. Elevando al quadrato abbiamo: $2 = \frac{a^2}{b^2}$ ovvero $2b^2 = a^2$.
Il quadrato di a è pari, quindi anche a è pari.
Esisterà quindi k tale che $2k = a$. Avremo allora $2b^2 = a^2 = 4k^2$ e quindi $b^2 = 2k^2$. Allora anche b è pari, ma questo è un assurdo.

2.2 Aritmetica Modulare

L'aritmetica modulare riguarda il calcolo sui resti delle divisioni tra interi rispetto ad un divisore fissato.

Congruenze:
Dati $a, b, m \in Z$, a è in relazione con b se $m|(a-b)$ ovvero se $a-b$ è un multiplo di m. Si scriverà $a \equiv b(mod\ m)$ se sono in relazione, altrimenti $a \not\equiv b(mod\ m)$.
Esempi:
- $12 \equiv 9(mod\ 3)$: $12\ mod\ 3 = 0$ e $9\ mod\ 3 = 0$
- $-15 \equiv 9(mod\ 4)$: $-15\ mod\ 4 = 1$ e $9 \equiv 4 = 1$

Osservazione:
Per ogni $a \in Z$ e ogni $m \in N$ abbiamo che $a \equiv a\ mod\ m(mod\ m)$, infatti per il Teorema della Divisione abbiamo $a = qm + r$ con $0 \leq r \leq |m|$ ovvero $a = qm + a\ mod\ m \Rightarrow a - (a\ mod\ m) = qm$.
Proprietà delle Congruenze:
• **Riflessiva**: $\forall a \in Z \Rightarrow a \equiv a(mod\ m)$ in quanto $0 = a - a$ è multiplo di m.
• **Simmetrica**: Se $a \equiv b(mod\ m)$ allora $a - b = km$ per qualche $k \in Z$, quindi moltiplicando per -1 otteniamo $b - a = (-k)m$ ossia $b \equiv a(mod\ m)$.
• **Transitiva**: Se $a \equiv b(mod\ m)$ e $b \equiv c(mod\ m)$ sappiamo che esistino $h, k \in Z$ tali che $a - b = hm$ e $b - c = km$. Sommando membro a membro le ultime due uguaglianze otteniamo: $a - c = (h + k)m$ e quindi $a \equiv c(mod\ m)$.

Conseguenze Notevoli:
• Modulo 0: $a \equiv b(mod\ 0)$ se e solo se $a - b = k \cdot 0$, ovvero $a - b = 0 \rightarrow a = b$.
• Modulo 1: $a \equiv b(mod\ 1)$ se e solo se $a - b = k \cdot 1$, ovvero $a - b$ è multiplo di 1.
• Modulo 2: $a \equiv b(mod\ 2)$ se e solo se $a - b = k \cdot 2$, ovvero $a - b$ è un numero pari.

Invarianza rispetto alla Somma e al Prodotto:
Dato $m \in N$ e dati $a, b \in Z$ tali che $a \equiv b(mod\ m)$ e $c, d \in Z$ tali che $c \equiv d(mod\ m)$, abbiamo:
• $a + c \equiv b + d(mod\ m)$. **Dimostrazione**:
Per Ipotesi esistono $k_1, k_2 \in Z$ tale che $a - b = k_1 m$ e $c - d = k_2 m$.
Quindi $(a + c) - (b - d) = (a - b) + (c - d) = (k_1 + k_2)m$.

• $a \cdot c \equiv b \cdot d (mod\ m)$. **Dimostrazione**:
Per Ipotesi esistono $k_1, k_2 \in Z$ tale che $a - b = k_1 m \rightarrow a = b + k_1 m$ e $c - d = k_2 m \rightarrow c = d + k_2 m$.
Quindi $ac - bd = (b + k_1 m)(d + k_2 m) - bd = bk_2 m + dk_1 m + k_1 k_2 m^2 = m(bk_2 + dk_1 + k_1 k_2 m)$.

Proprietà Invarianza rispetto alla Somma e al Prodotto:
Dati $a.b.m \in N$, visto che $a \equiv a (mod\ m)$ e $b \equiv b (mod\ m)$ allora valgono le seguenti proprietà:
• P1: $(a + b) \equiv (a\ mod\ m + b\ mod\ m)(mod\ m)$, ossia
$(a + b)\ mod\ m = (a\ mod\ m + b\ mod\ m)(mod\ m)$
• P2: $(a \cdot b) \equiv (a\ mod\ m \cdot b\ mod\ m)(mod\ m)$, ossia
$(a \cdot b)\ mod\ m = ((a\ mod\ m) \cdot (b\ mod\ m))(mod\ m)$
• P3: $a^n \equiv (a\ mod\ m)^n (mod\ m)$
• P4: Dati $a.b.h, k, m \in N$ allora $a^h \cdot b^k \equiv (a^h\ mod\ m)(b^k\ mod\ m)(mod\ m)$
ovvero $a^h \cdot b^k\ mod\ m = (a\ mod\ m)^h \cdot (b\ mod\ m)^k \cdot mod\ m$
Esempi:
- Per P1: $60\ mod\ 7 = ((50\ mod\ 7) + (10\ mod\ 7)) mod\ 7 = (1 + 3)\ mod\ 7 = 4$
- Per P2: $60\ mod\ 7 = ((6\ mod\ 7)(10\ mod\ 7))\ mod\ 7 = (6 \cdot 3)\ mod\ 7 = 18\ mod\ 7 = 4$
- Per P3: $(13\ mod\ 10)^2\ mod\ 10 = 9\ mod\ 10 = 9$
- Per P4: $41503\ mod\ 5$. Abbiamo $41503 = 121 \cdot 343 = 11^2 \cdot 7^3$ quindi:
$41503\ mod\ 5 = (11^2\ mod\ 5)(7^3\ mod\ 5)\ mod\ 5 = (11\ mod\ 5)^2 (7\ mod\ 5)^3\ mod\ 5 = (1 \cdot 8)\ mod\ 5 = 3$

Divisione Modulare:
Siano $a, b \in N$ e $a, b > 0$. Allora esiste un elemento $x \in N$ tale che $a \cdot x \equiv 1 (mod\ b)$ se e solo se a e b sono coprimi.
L'elemento x, denotato con $a^{-1}\ mod\ b$ o solo a^{-1} viene detto **Inverso** di $a\ mod\ b$.
Esempi:
- $a = 5$, $b = 3$: $a^{-1} = 2$, infatti $2 \cdot 5\ mod\ 3 = 10\ mod\ 3 = 1$
- $a = 9$, $b = 7$: $a^{-1} = 4$, infatti $4 \cdot 9\ mod\ 7 = 36\ mod\ 7 = 1$
- $a = 9$, $b = 11$: $a^{-1} = 5$, infatti $5 \cdot 9\ mod\ 11 = 45\ mod\ 11 = 1$

Funzione di Eulero:
Dato $n > 0$, con $\phi(n) = |\{x : x \in N, 0 < x \leq n \text{ e } MCD(n,x) = 1\}|$, contiamo quanti sono i numeri che precedono n e che sono ad esso coprimi:
• 1° Caso: se n è primo, tutti i predecessori di n sono ad esso coprimi e quindi: $\phi(n) = n - 1$.
Esempi: $\phi(2) = 1$; $\phi(3) = 2$, $\phi(5) = 4$
• 2° Caso: la potenza di n prima, ovvero p^k con $k \geq 2$, quindi:
$\phi(p^k) = p^k - p^{k-1}$.
Esempi: $\phi(2^3) = 2^3 - 2^2 = 8 - 4 = 4$; $\phi(3^3) = 3^3 - 3^2 = 27 - 9 = 18$
• 3° Caso: se n è prodotto di due numeri primi distinti, ovvero $n = p_1 \cdot p_2$, si procede similmente al 1° Caso: $\phi(n) = (p_1 - 1)(p_2 - 1)$
Esempi: $\phi(6) = \phi(2 \cdot 3) = 1 \cdot 2 = 2$; $\phi(15) = \phi(3 \cdot 5) = 2 \cdot 4 = 8$
• Caso Generale: Sia $n = h \cdot k$, dove h e k sono interi coprimi maggiori di zero. Allora: $\phi(n) = \phi(h) \cdot \phi(k)$. Esempi:
- $\phi(4 \cdot 9) = \phi(2^2) \cdot \phi(3^2) = 2 \cdot 6 = 12$;
- $\phi(5 \cdot 8) = \phi(5) \cdot \phi(2^3) = 4 \cdot (8 \cdot 4) = 16$

Teorema di Eulero:
Siano $n, m > 0$, se $MCD(n,m) = 1$ allora $n^{\phi(m)} \equiv 1(mod\ m)$.
Esempio:
$n = 12$, $m = 5$: $12^{\phi(5)} \equiv 1(mod\ 5) = 12^4\ mod\ 5 = 1 \Rightarrow 20736\ mod\ 5 = 1$
Conseguenze del Teorema di Eulero:
• **Lemma N°1**: Sia $m > 1$ e sia $C_m = \{x : 0 < x < m,\ MCD(x,m) = 1\}$. Allora:
- Per ogni $x \in C_m$ esiste $y \in C_m$ tale che $x \cdot y \equiv 1(mod\ m)$
- $C_m^{-1} = \{x^{-1}\ mod\ m : x \in C_m\} = C_m$
Esempio: Per $m = 5$ abbiamo $C_5 = \{1,2,3,4\}$ e $1^{-1}\ mod\ 5 = 1,\ 2^{-1}\ mod\ 5 = 3,\ 3^{-1}\ mod\ 5 = 2,\ 4^{-1}\ mod\ 5 = 4$. Quindi $C_5^{-1} = \{1,2,3,4\}$.

• **Lemma N°2**: Siano $n, m > 1$, tale che $MCD(n,m) = 1$. Sia $C_{n,m} = \{(n \cdot x)\ mod\ m : x \in C_m\}$, allora $C_{n,m} = C_m$.
Esempio: $m = 15$, $n = 13$, $MCD(13,5) = 1$, inoltre $C_5 = \{1,2,3,4\}$ e $C_{13,5} = \{1 \cdot 13\ mod\ 5, 2 \cdot 13\ mod\ 5, 3 \cdot 13\ mod\ 5, 4 \cdot 13\ mod\ 5\}$.
Abbiamo: $13\ mod\ 5 = 3$; $26\ mod\ 5 = 1$; $39\ mod\ 5 = 4$; $52\ mod\ 5 = 2$.
Quindi: $C_{13,5} = C_5$.

• **Piccolo Teorema di Fermat**:
Se p è primo e $MCD(a,p) = 1$, ovvero a non è multiplo di p, allora $a^{p-1} \equiv 1(mod\ p)$. Esempi:
- $p = 3$, $a = 10 : 10^2\ mod\ 3 = 100\ mod\ 3 = 1$ e quindi $10^2 \equiv 1(mod\ 3)$
- $p = 17$, $a = 40 : 40^{16}\ mod\ 17 = 1$ e quindi $40^{16} \equiv 1(mod\ 17)$.

• **Ulteriore conseguenza del Teorema di Eulero**:
Se $MCD(a,n) = 1$, allora $\forall x > 0 \quad a^x \equiv a^{x\ mod\ \phi(n)}(mod\ n)$. Esempio: $12^{50}(mod\ 5).MCD(12,5) = 1$ allora $12^{50} \equiv 12^{50\ mod\ \phi(5)}(mod\ 5) \equiv 12^{50\ mod\ 4}(mod\ 5) \equiv 12^2(mod\ 5) \equiv 4(mod\ 5) = 4$

Inverso Modulare:
Se n e m sono coprimi, allora esiste l'**inverso** di n modulo m, ossia esiste k tale che $n \cdot k \equiv 1(mod\ m)$.
Per calcolare l'inverso modulare possiamo usare il Teorema di Eulero, ovvero: $n^{\phi(m)} \equiv 1(mod\ m)$ che diventa $(n\ mod\ m)^{\phi(m)-1}(mod\ m)$.
Esempio di Inverso Modulare: $11\ mod\ 17$.
$MCD(11,7) = 1$ quindi sono coprimi. $\phi(7) = 6$ e $11\ mod\ 7 = 4$. Calcoliamo: $4^5\ mod\ 7 \equiv (4^2) \cdot 4\ mod\ 7 \equiv (16\ mod\ 7)^2 \cdot 4(mod\ 7) \equiv 4 \cdot 4(mod\ 7) \equiv 16\ mod\ 7 = 2$.

2.3 Problemi irrisolti nella Teoria dei Numeri

Numeri primi di Mersenne:
I numeri primi di Mersenne sono numeri primi nella forma: $M_p = 2^p - 1$ dove p è un numero primo. Esempi:
- $M_2 = 2^2 - 1 = 3$
- $M_3 = 2^3 - 1 = 7$
- $M_5 = 2^5 - 1 = 31$
- $M_7 = 2^7 - 1 = 127$
- $M_{13} = 2^{13} - 1 = 8191$

Tuttavia che p sia primo è una **condizione necessaria ma non sufficente**, in quanto ad esempio $2^{11} - 1 = 2048 - 1 = 2047 = 23 \cdot 89$ non è primo.
I numeri noti di Mersenne sono 51 e non è noto se sono infiniti o meno.

Numeri Perfetti:
Introduciamo prima la funzione sigma σ.
Dato un numero $n \in N$, la funzione sigma $\sigma(n)$ restituisce la somma di tutti i divisori positivi di un numero n: $\sigma(n) = \sum_{0<d,d|n} d$.
La proprietà più banale è che se p è primo allora $\sigma(p) = p + 1$.

Un numero si dice **perfetto** se $\sigma(n) = 2n$, ovvero, essendo n un divisore di sé stesso, se n è uguale alla somma di tutti i suoi divisori propri.
Il primo numero perfetto è 6, infatti $6 = 1 + 2 + 3$ e $\sigma(6) = 12$.
Proprietà: Se $2^n - 1$ è primo, allora $2^{n-1} \cdot (2^n - 1)$ è perfetto (e pari).
Come i numeri di Mersenne, i numeri perfetti noti sono 51 e non è noto se esistono numeri perfetti **dispari** e se sono infiniti.

Numeri Gemelli:
Un ulteriore problema irrisolto è quello dei numeri primi gemelli.
Due numeri primi p_1 e p_2 si dicono **gemelli** se la loro differenza è uguale a 2, ovvero $|p_1 - p_2| = 2$. Esempi:
- $(3, 5), (5, 7), (11, 13), (17, 19)$.
Come per i numeri di Mersenne e i numeri perfetti, non è noto se i numeri gemelli sono infiniti o meno. Inoltre, i numeri primi consecutivi che si differenziano di 4 sono detti numeri primi **cugini**.

Congettura di Goldbach:
La Congettura di Goldbach afferma che ogni numero pari maggiore di 4 può essere scritto come somma di due numeri primi. Non è dimostrabile.
Esempi:
- $6 = 3 + 3 \quad 8 = 3 + 5 \quad 10 = 3 + 7 = 5 + 5 \quad 12 = 5 + 7$
- $14 = 3 + 11 = 7 + 7 \quad 16 = 3 + 13 = 5 + 11 \quad 18 = 5 + 13 = 7 + 11$

Congettura di Collatz:
La Congettura di Collatz, conosciuta anche come **Congettura 3x+1**, lega la teoria dei numeri ad un problema di terminazione di un algortimo iterativo, basato sulla funzione:

$$f(n) = \begin{cases} 1 & \textit{se } n = 1 \\ \frac{n}{2} & \textit{con } n \textit{ pari} \\ 3n + 1 & \textit{con } n \textit{ dispari} \end{cases}$$

Algortitmo di Collatz:

```
legge un intero x>=1
while(x>1){
    if(x mod 2 == 0){
    x = x/2;
    } else {
    x = 3x+1;
    }
}
```

Esempi:
- $3 \to 10,\ 5,\ 16,\ 8,\ 4,\ 2,\ 1$
- $7 \to 22,\ 11,\ 34,\ 17,\ 52,\ 26,\ 13,\ 40,\ 20,\ 10,\ 5,\ 16,\ 8,\ 4,\ 2,\ 1.$

3 Parte 3

3.1 Calcolo Combinatorio

Regola della Somma:
La somma di due insiemi disgiunti A e B è la sua unione $A \cup B$ e quindi $|A| + |B|$.
Esempio: $A =$\{Lettere alfabeto Maiuscolo\} e $B =$\{Lettere alfabeto minuscolo\} $\Rightarrow 26 + 26 = 52$.

Regola del Prodotto:
Il prodotto di due insiemi disgiunti A e B è il prodotto $|A| \cdot |B|$.
Osservazione: Utile per contare le possibili coppie di elementi di due insiemi.
Esempio: Numero di coppie di caratteri alfanumerici, $A = B$ e $|A| = 62$ quindi $62 \cdot 62 = 3844$.

Disposizioni:
• **Disposizioni con Ripetizioni (CONTA L'ORDINE)**:
Si indicano con $F_{n,k}$ (o con $D^r_{n,k}$) e usano la regola del prodotto.
Per ognuno dei k elementi di A bisogna scegliere uno degli elementi n di B : $F_{n,k} = n^k$. Esempi:
- Dati A e B con $|A| = k$, $|B| = n$ quante sono le **applicazioni** di A in B?
Il numero delle Disposizioni con Ripetizione di n elementi di classe k, $F_{n,k}$.

- Le funzioni booleane definite su un insieme di k variabili booleane:
$f : A \to \{0, 1\}$ dove $|A| = k$. Quindi, $F_{2,k} = 2^k$.
- $B = \{a, b\}$. Disposizione di: classe 1 : $(a), (b)$; classe 2 : $(a, a), (a, b)$, $(b, a), (b, b)$; etc.
- Utilizzando le cifre 1,2,3 quanti numeri di 4 cifre si possono formare?
$n = 3$, $k = 4$, r (num. ripetizioni)=4, $F_{n,k} = F_{3,4} = 3^4 = 81$.

• **Disposizioni semplici (CONTA L'ORDINE)**:
Si indicano con $D_{n,k}$ e usano la regola del prodotto. Dati due insiemi A e B, con $|A|$ e $|B|$, con $|A| = k$ e $|B| = n$ tale che $n \geq k$, $D_{n,k} = \frac{n!}{(n-k)!}$. Esempi:
- Dati A e B con $|A| = k$, $|B| = n$ quante sono le **applicazioni iniettive** di A in B? Il numero delle Disposizioni semplici di n elementi di classe k, $D_{n,k}$.
- $B = \{a, b, c\}$. $D_{n,k}$ di: classe 1 : $(a), (b), (c)$; classe 2 : $(a, b), (a, c), (b, a)$, $(b, c), (c, a), (c, b)$; etc. - Quante squadre di calcio diverse posso formare da un gruppo di 50 studenti? (Supponendo che l'ordine diverso degli studenti dia origine a squadre diverse) $D_{50,11} = \frac{50!}{(50-11)!} = \frac{50!}{39!} = 50 \cdot 49 \cdot ... \cdot 40 \approx 1,5 \cdot 10^{18}$
- In quanti modi diversi 5 alunni si possono sedere su 3 sedie numerate?
$n = 5$, $k = 3 \to D_{n,k} = \frac{5!}{(5-3)!} = 5 \cdot 4 \cdot 3 = 60$

• **Permutazioni o Sostituzioni (CONTA L'ORDINE)**:
Sono **disposizioni** di classe n e sono indicate con $D_{n,n}$ o $P_n = n!$ se senza ripetizione e con $D^r_{n,n}$ o $P^r_n = \frac{n!}{r_1! \cdot r_2! \cdot ... \cdot r_k!}$ se con ripetizione. Esempi:
- Il numero delle Permutazioni è il numero delle **applicazioni biiettive** di un insieme in un altro della stessa cardinalità.
- $A = 1, 2, 3 \to P_3 = \{(1, 2, 3), (1, 3, 2), (2, 1, 3), (2, 3, 1), (3, 1, 2), (3, 2, 1)\}$ perché $|P_3| = 3! = 3 \cdot 2 \cdot 1 = 6$.
- Quanti anagrammi, anche senza senso, si possono formare con la parola $LIBRO$? $n = 5$, $k = 5$, nessuna ripetizione.
$P_n = n! \to P_5 = 5! = 5 \cdot 4 \cdot 3 \cdot 2 = 120$
- Quanti anagrammi, anche senza senso, si possono formare con la parola $MAMMA$? $n = 5$, $k = 5$, $r_A = 2$, $r_M = 3$.
$P^r_n = \frac{n!}{r_1! \cdot r_2!} \to P^r_5 = \frac{5!}{3! \cdot 2!} = 5 \cdot 2 = 10$

Combinazioni:
• **Combinazioni semplici (NON CONTA L'ORDINE)**:
Si indicano con $C_{n,k}$ con $n \geq k$, i valori sono anche detti **coefficienti binomiali** ed indicati con $\binom{n}{k} = \frac{n!}{k!(n-k)!}$

Dimostrazione $\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}$:
Dato un insieme A con n elementi, fissamo un elemento $x \in A$.
I sottoinsiemi di k elementi, ovvero $\binom{n}{k}$, si possono ripartire tra:
- I sottoinsiemi che contengono x che sono tanti quanti sono i sottoinsiemi di $k-1$ elementi di $A\backslash\{x\}$, ovvero $\binom{n-1}{k-1}$;
- I sottoinsiemi che non contengono x che sono quanti i sottoinsiemi di k elementi di $A\backslash\{x\}$, ovvero $\binom{n-1}{k}$. Quindi $\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}$.
Quindi $\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}$.
Esempio:
In che modo un negoziante può esporre 4 paia di scarpe tra 10 modelli diversi?
$n = 10$, $k = 4 \rightarrow \binom{10}{4} = \frac{10!}{4!(10-4)!} = \frac{10!}{4!\cdot 6!} = 210$.

• **Combinazioni con Ripetizioni (NON CONTA L'ORDINE)**:
Dato un'insieme di $n > 1$ variabili $\{x_0, x_1, ..., x_{n-1}\}$ e preso un intero k, i monomi di grado k sono $C^k_{n,k} = \binom{n+k-1}{k} = \frac{(n+k-1)!}{k!(n-1)!}$. Esempi:
- Dato $A = \{x, y, z\}$ e monomi di grado 2: $\binom{3+2-1}{2} = \binom{4}{2} = \frac{4!}{2!\cdot 2!} = 2 \cdot 3 = 6$
- Assegnati due contagocce, il primo contenente 5 gocce di colore bianco e il secondo 5 gocce di colore nero. Mischiando tra loro 5 gocce scelte tra i due colori, quanti colori diversi si possono formare?
$n = 2$, $k = 5 \rightarrow C^r_{n,k} = \binom{2+5-1}{5} = \binom{6}{5} = \frac{6!}{5!(6-5)!} = \frac{6!}{5!} = 6$.

Teorema Binomiale (Formula di Newton):
Siano a e $b \in R$, allora vale l'uguaglianza: $(a+b)^n = \sum_{k=0}^{n} \binom{n}{k}\ a^{n-k} \cdot b^k$.
Il teorema deriva dalla definizione dei coefficienti binomiali e consente di elevare ad una qualsiasi potenza un binomio.

Dimostrazione:
La potenza $(a+b)^n$ è il prodotto di n fattori tutti uguali a $(a+b)$. Otteniamo una somma di monomi di grado n in a e b del tipo $a^{n-k} \cdot b^k$ con $0 \leq k \leq n$.
I monomi $a^n b^0 = a^n$ e $a^0 b^n = b^n$ compariranno nella somma una volta sola, esattamente quando da ogni fattore prendiamo rispettivamente a o b.
Il monomio $a^{n-1}b$ comparirà $\binom{n}{n-1}$ volte, ovvero $n-1$ volte.
Allora in generale il monomio $a^{n-k}b^k$ comparirà $\binom{n}{n-k}$ volte, ovvero $n-k$ volte.

Proprietà del Teorema Binomiale:
Se $a = b = 1$ allora:

$$2^n = (1+1)^n = \sum_{k=0}^{n} \binom{n}{k} 1^{n-k} \cdot 1^k = \sum_{k=0}^{n} \binom{n}{k}$$

Invece se, ad esempio, $a = 1$ e $b = 10$ abbiamo:

$$\sum_{k=0}^{n} \binom{n}{k} 1^{n-k} \cdot 10^k = \sum_{k=0}^{n} \binom{n}{k} 10^k = 11^n$$

• **Pigeonhole Principle**:
Il principio afferma che se dobbiamo far entrare $n+1$ piccioni in una piccionaia con n cassette, almeno una cassetta dovrà contenere più di un piccione.
Se abbiamo $n = km + 1$ oggetti da sistemare in m contenitori, allora almeno un contenitore dovrà contenere $k + 1$ oggetti.
Applicazione pratica:
Supponiamo di avere un insieme S di m interi positivi, e sia $0 < n < m$.
Dividiamo m per n ed otteniamo quoziente q e resto r. Allora:
- se $r = 0$ esistono almeno q interi in S tutti congrui modulo n ovvero che hanno lo stesso resto della divisione per n;
- se invece $r \neq 0$ esistono almeno $q + 1$ interi in S tutti congrui modulo n.

Esempi:
- **Coppia di Calzini:** Un cassetto è pieno di calzini neri e blu.
Il numero minimo di calze da prendere per un paio completo è 3, poiché o ne prendiamo 3 dello stesso colore o 2 dello stesso colore e 1 diverso.
- **Insieme di Interi:** Sia S un insieme di $n + 1$ interi diversi. Dimostro che esistono 2 interi a e $b \in S$ tali che $a - b$ è un multiplo di n.
Considero l'insieme di numeri interi $M = \{a \ mod \ n : a \in S\}$.
Dal momento che i resti modulo n sono esattamente n, di sicuro $|M| \leq n$.
Ma gli interi in S sono $n + 1$ quindi esistono due interi $a, b \in S$ tali che $a \ mod \ n = b \ mod \ n$ e $a - b \equiv 0 \ mod \ n$.
- **Numero di Capelli:** Supponiamo che un umano abbia 200000 come numero massimo di capelli. Sapendo che a Catania ci sono 300000 abitanti, ci sono almeno 2 persone con lo stesso numero di capelli?
Si, perché Catania ha più abitanti che numero massimo di capelli, quindi sicuramente 2 persone avranno lo stesso numero di capelli.

3.2 Probabilità

Definizione Classica della Probabilità:
La definizione classica della probabilità di un evento A, scritto come $P(A)$ è il rapporto tra il numero di **casi favorevoli** f_A ed il numero di **casi totali** n, quindi $P(A) = \frac{f_A}{n}$.
• La definizione assume che tutti gli eventi possono accadere con la stessa probabilità, quindi è una definizione *circolare*.
Esempio: Per l'evento "Esce un numero inferiore a 3", lo **spazio dei campioni** è costituito da:
- tutti i possibili esiti, cioè $S = \{1, 2, 3, 4, 5, 6\}$ nel lancio di un dado;
- gli esiti positivi, che sono solo 2, ovvero {1,2}.
Quindi la probabilità di tale evento è $\frac{2}{6} = \frac{1}{3}$.

Definizione Frequentista della Probabilità:
La definizione frequentista della probabilità di un evento A, scritto come $P(A)$ è il limite del rapporto tra il numero di volte in cui si è verificato l'esito di casi favorevoli f_A è il numero degli esperimenti n, quindi:
$P(A) = \lim_{n\to\infty} \frac{f_A}{n}$.
• La definizione frequentista è stata ideata in quanto la definizione classica di probabilità non considera la possibilità di eventi non equiparabili.
• Tuttavia non tutti gli esperimenti sono ripetibili e quindi alcune probabilità non sono calcolabili.

Teoria della Probabilità:
Una distribuzione di probabilità P in uno spazio di campioni S associa, agli eventi, numeri reali che soddisfano i seguenti assiomi:
Siano A e B due eventi qualsiasi (sottoinsiemi di S):
• Assioma n°1: $0 \leq P(A) \leq 1$
• Assioma n°2: $P(S) = 1$ e $P(\emptyset) = 0$
• Assioma n°3: $P(A \cup B) = P(A) + P(B) - P(A \cap B)$
Inoltre:
La probabilità che un evento non si verifichi è uguale a 1 - meno che la probabilità si verifichi: $P(\neg A) = 1 - P(A)$.

Probabilità Condizionata:
Il verificarsi di un evento può cambiare la probabilità che si verifichi un altro evento. La probabilità di un evento A **condizionata** al verificarsi di un evento B (non nullo) è definita come: $P(A|B) = \frac{P(A \wedge B)}{P(B)}$

Indipendenza tra Eventi:
Due eventi si dicono **indipendenti** se: $P(A|B) = P(A)$ e $P(B|A) = P(B)$.
Quindi se A e B sono indipendenti $P(A \wedge B) = P(A) \cdot P(B)$.
Esempio: Lanciamo un dado 3 volte. La probabilità della sequenza [2,1,6] è la stessa della sequenza [3,3,3], poiché ogni lancio è un evento indipendente ($\frac{1}{6}$ per lancio) e la probabilità di entrambe le sequenti sono $\frac{1}{216}$

Regola di Bayes:
La Regola di Bayes deriva dalla definizione di probabilità condizionata, quindi con 2 eventi A e B abbiamo:

$$P(B|A) = \frac{P(A|B) \cdot P(B)}{P(A)}$$

Osservazione: La Regola di Bayes ha applicazioni nei sistemi diagnostici, ovvero se sappiamo che un evento E causa effetti S, osservando gli effetti S possiamo risalire alla causa.
La regola di Bayes automatizza il processo di diagnosi se conosciamo le probabilità a priori di causa ed effetto.
Esempio: Se $P(E) = \frac{1}{10},\ P(S) = \frac{4}{10}$ e $P(S|E) = \frac{7}{10}$ allora:

$$P(E|S) = \frac{P(S|E) \cdot P(E)}{P(S)} = \frac{\frac{7}{10} \cdot \frac{1}{10}}{\frac{4}{10}} = \frac{7}{40}$$

Teorema della Probabilità Totale:
Sia A un evento e siano $B_1, B_2, .., B_n$ n eventi mutualmente esclusivi, tali che $P(B_i) \neq 0$ per ogni i ed inoltre $P(B_1 \vee B_2 \vee ... \vee B_n) = 1$, ovvero gli eventi sono esaustivi. Allora:
$P(A) = P(A|B_1) \cdot P(B_1) + P(A|B_2) \cdot P(B_2) + ... + P(A|B_n) \cdot P(B_n) = \sum_{i=1}^{n} P(A|B_i) \cdot P(B_i)$.

Dimostrazione:
Dal momento che $B_1, B_2, .., B_n$ n sono eventi esaustivi, almeno uno di loro si deve verificare. Se A si verifica, ci sarà un evento B_j tale che B_j si verifica. Visto che gli eventi B_j sono **mutualmente esclusivi**, abbiamo
$P(A) = P(A \wedge B_1) + ... + P(A \wedge B_n)$, per la definizione di probabilità condizionata abbiamo $\forall i\ P(A \wedge B_i) = P(A|B_i) \cdot P(B_i)$.

Esempio del Teorema della Probabilità Totale:
Ho un mazzo da 52 carte che divido in due mazzi:
• M_1 con 30 carte tra cui 3 assi;
• M_2 con 10 cartte tra cui 1 asso.
Scegliendo un mazzo a caso e una carta a caso, qual'è la possibilità di pescare un asso $P(A)$?
• Scegliendo M_1, abbiamo $P(A|M_1) = \frac{3}{30} = \frac{1}{10}$;
• Scegliendo M_2, abbiamo $P(A|M_2) = \frac{1}{22}$;
Per il Teorema della Probabilità Totale: $P(A) = P(A|M_1) \cdot P(M_1) + P(A|M_2) \cdot P(M_2) = \frac{1}{10} \cdot \frac{1}{2} + \frac{1}{22} \cdot \frac{1}{2} = \frac{1}{20} + \frac{1}{44} = \frac{16}{220} = \frac{4}{55}$

Problemi d'urna:
Le estrazioni da un'urna si classificano in modi diversi seguendo 2 criteri:
• Importanza o meno dell'ordine di estrazione;
• Se l'estrazione presenta o meno il reinserimento.
Esaminiamo i casi possibili:
• $D^r_{n,k} = n^k$, ovvero una disposizione con ripetizione dove ha importanza l'ordine di estrazione e la pallina viene reinserita;
• $D_{n,k} = n(n-1) \cdot ... \cdot (n-k+1)$, ovvero una disposizione semplice dove ha importanza l'ordine di estrazione ma senxa reinserimento della pallina.
• $C_{n,k} = \binom{n}{k} = \frac{n!}{k!(n-k)!}$, ovvero una combinazione semplice dove non ha importanza l'ordine di estrazione e senza reinserimento della pallina.
• $C^r_{n,k} = \binom{n+k-1}{k}$, ovvero una combinazione con ripetizione dove non ha importanza l'ordine di estrazione ma con il reinserimento della pallina.

Esempio PIN:
Qual'è la probabilità di indovinare un PIN da 5 cifre nei primi 3 tentativi?
Sapendo che i codici PIN da 5 cifre sono $10^5 = 10000$:
• Probabilità di sbagliare al 1° tentativo: $\frac{10^5-1}{10^5}$
• Probabilità di sbagliare al 2° tentativo: $\frac{10^5-2}{10^5-1}$
• Probabilità di sbagliare al 3° tentativo: $\frac{10^5-3}{10^5-2}$
Quindi la probabilità di sbagliare tutti e 3 i tentativi è:

$$\frac{(10^5-1)(10^5-2)(10^5-3)}{(10^5)(10^5-1)(10^5-2)} = \frac{10^5-3}{10^5}$$

Mentre la probabilità di indovinare entro i tre tentativi è:

$$1 - \frac{10^5-3}{10^5} = \frac{3}{10^5}$$

Probabilità di lancio di 3 dadi:
Lo spazio dei campioni S sono le triple $[x, y, z]$, corrispondenti al lancio di 3 dadi, quindi la dimensione di S è $6^3 = 216$.
Ma le somme ottenibili sono 16 (da 3 a 18) e non essendo 16 un divisore di 216, alcune somme si possono ottenere un numero diverso di volte:
• Le somme 3 e 18 sono uniche: per $3 : [1, 1, 1]$ e per $18 : [6, 6, 6]$.
• Le somme 4 e 17 sono ottenibili in 3 modi: per $4 : [1, 1, 2], [1, 2, 1].[2, 1, 1]$ mentre per $17 : [6, 6, 5], [6, 5, 6].[5, 6, 6]$
• Ogni altra somma si ottiene in 6 modi diversi.

Variabile Casuale e Valore Atteso:
• Una **variabile casuale** è una funzione X che associa un numero reale ad un evento. Definiamo quindi un evento come il fatto che la variabile X assume un valore x, ovvero $X = x$.
• Il **valore atteso (o medio)** di una variabile casuale X è:

$$E[X] = \sum_x x \cdot P[X \cdot x]$$

Esempio: Se la variabile casuale X contiene il valore assoluto dopo il lancio di un dado, abbiamo che $E[X] = 1 \cdot \frac{1}{6} + 2 \cdot \frac{1}{6} + 3 \cdot \frac{1}{6} + 4 \cdot \frac{1}{6} + 5 \cdot \frac{1}{6} + 6 \cdot \frac{1}{6} = 3,5$

Proprietà di Linearità: Prese due variabili casuali X e Y e la variabile casuale somma $X + Y$ allora $E[X + Y] = E[X] + E[Y]$
Esempio: Lancio di due dadi: $E[X + Y] = E[X] + E[Y] = 3,5 + 3,5 = 7$

Prova di Bernoulli (o Prova Binomiale):
La prova Binomiale è un esperimento probabilistico con due risultati:
• Successo con probabilità p (costante);
• Insuccesso con probabilità $q = 1 - p$;
dove ogni tentativo è indipendente.
Se X è la variabile casuale che tiene conto del numero di tentativi usando la Prova di Bernoulli, abbiamo: $E[X] = 1 \cdot p + 2qp + 3q^2p + ... =$

$$\sum_{k=1}^{\infty} kq^{k-1}p = \frac{p}{q}\sum_{k=0}^{\infty} kq^k = \sum_{k=0}^{\infty} kq^k = \frac{q}{(1-q)^2}$$

poiché per $q < 1$ $\sum_{k=0}^{\infty} q^k = \frac{1}{1-q}$. Quindi il valore atteso del numero di tentativi da fare per ottenere successo è $E[X] = \frac{p}{q}\frac{q}{(1-q)^2} = \frac{p}{p^2} = \frac{1}{p}$.

Esempi:
• Numero atteso di lanci di una moneta per ottenere testa? $\frac{1}{\frac{1}{2}} = 2$
• Numero atteso di lanci di un dado per ottenere 6? $\frac{1}{\frac{1}{6}} = 6$

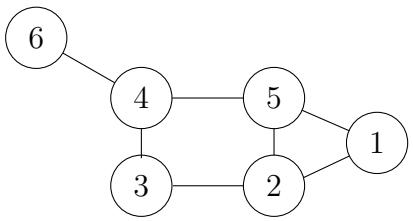
Legge dei Grandi Numeri (Teorema di Bernoulli):
Ci garantisce che la media dei risultati ottenuti dopo un gran numero di tentativi tende al valore medio atteso, eguagliandolo al limite.
Darà quindi un risultato che a lungo termine darà stabilità.
Esempio: Se lanciamo un dado un numero infinito di volte, la media ottenuta sarà esattamente 3,5.
Questa legge vale esclusivamente su un numero grande di tentativi.

4 Parte 4

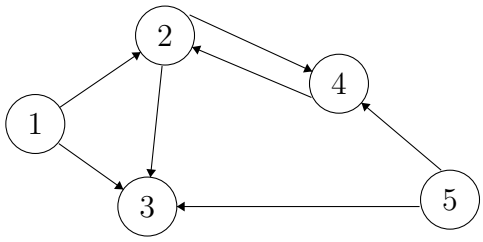
4.1 Teoria dei Grafi

Le basi della Teoria dei Grafi vennero poste da Eulero quando affrontò il problema dei sette ponti di Königsberg.

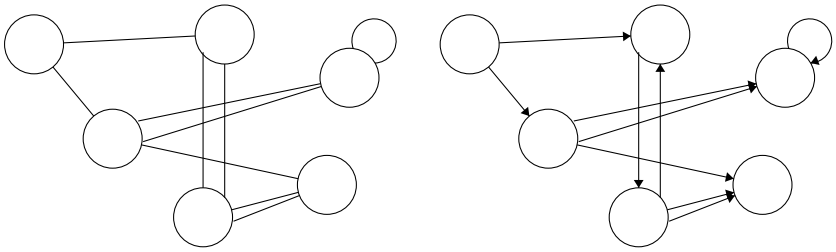
Definizione formale di Grafo:
Denotato con $G = (V, E)$ consiste di:
• Un insieme finito $V = \{1, 2, ..., m\}$ i cui elementi sono chiamati **vertici** o **nodi** del grafo;
• Un insieme finito $E = \{e_1, e_2, ..., e_n\}$ i cui elementi sono sottoinsiemi di V di cardinalità due, ovvero $e_k == \{i, j\}$, con $i, j \in V$. Tali elementi sono detti **archi** del grafo;
• I due nomi che caratterizzano l'arco sono detti "estremi dell'arco" e sono adiacenti;
I grafi si differenziano in due tipologie:
Grafo Non Orientato:
• Un arco che ha come estremo il nodo i si dice **incidente** ad i;
• Un nodo che non è l'estremo di alcun arco si dice **isolato**.



Grafo Orientato (Digrafo):
• Un arco che ha come estremo il nodo i, indipendentemente dal verso dell'arco, si dice **incidente** ad i;
• Gli archi del tipo (i, i) sono archi orientati da un nodo verso sé stesso e sono detti **cappi**.



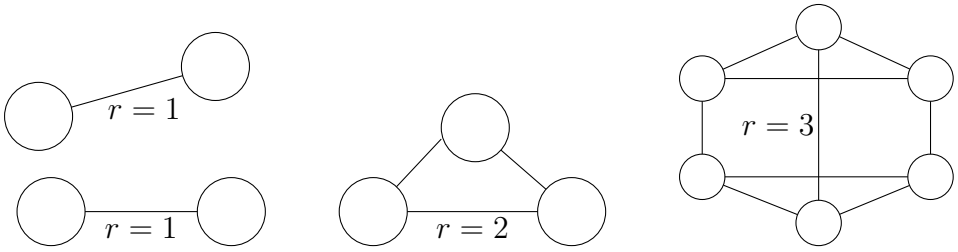
Definizione di Multigrafo:
I grafi con più di un arco che collega coppie di nodi sono detti **multigrafi**.
Esempio: Il grafo dei 7 ponti di Königsberg.



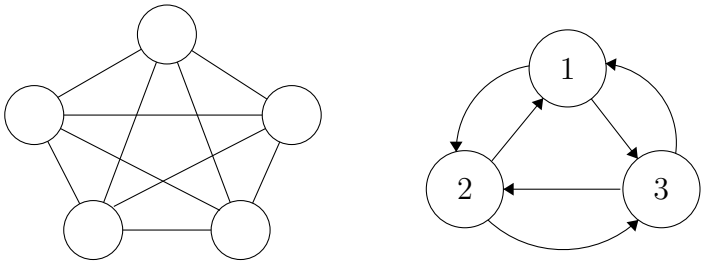
Grado di un Nodo:
Dato $G = (V, E)$ il grado di un nodo $v \in V$ è il numero di archi ad esso incidenti $\delta(v) = \{e \in E : v \in e\}$. Se $G = (V, E)$ è un digrafo, ci sono due nozioni di grado:
• Grado in **ingresso** di un nodo $v \in V$ è il numero di archi *entranti* in v, ovvero $\delta^-(v) = \{e \in E : e = (w, v)$ per qualche $w \in V\}$;
• Grado in **uscita** di un nodo $v \in V$ è il numero di archi *uscenti* da v, ovvero $\delta^-(v) = \{e \in E : e = (v, w)$ per qualche $w \in V\}$. **Esempi**:
- Grafo non orientato: $\delta(1) = 2,\ \delta(2) = 3,\ \delta(3) = 2,\ \delta(4) = 3,$
$\delta(5) = 3,\ \delta(6) = 1$. Sommo i gradi: $2 + 3 + 2 + 3 + 3 + 1 = 14$ e ottengo il doppio del numero di archi, 7.
- Digrafo: $\delta^-(1) + \delta^-(2) + \delta^-(3) + \delta^-(4) + \delta^-(5) = 0 + 2 + 3 + 2 + 0 = 7$
$\delta^+(1) + \delta^+(2) + \delta^+(3) + \delta^+(4) + \delta^+(5) = 2 + 2 + 0 + 1 + 2 = 7,$
la somma dei gradi in ingresso è **uguale** alla somma dei gradi in uscita e la loro somma è il **doppio** del numero degli archi nel grafo.

Teorema delle Strette di Mano:
Sia $G = (V, E)$ un grafo, la somma dei gradi di ogni veritice è uguale al doppio del numero di archi, ovvero $2|E|$.
Osservazione: Una conseguenza di questo teorema è che, in un grafo non orientato, il numero dei vertici di grado dispari è un numero pari.

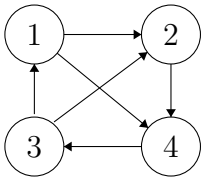
Tipologie di Grafi:
• **Regolari**:
Sia $G = (V, E)$ un grafo non orientato. Se i vertici hanno tutti lo stesso grado r allora G è **regolare** di grado r. *Osservazioni*:
- se un grafo è regolare, allora $|V| = \frac{2|E|}{r}$.
- un grafo regolare di grado r dispari contiene un numero pari di vertici.



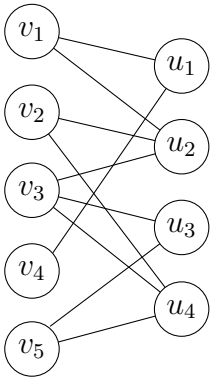
• **Completi**:
Sia $G = (V, E)$ un grafo non orientato. Diciamo che G è **completo** se ogni coppia di vertici è connessa da un arco. *Osservazioni*:
- se $|V| = n$ il numero di archi del grafo è $\binom{n}{2}$, ovvero tutte le possibili coppie (ordinate) di vertici.
- G può essere anche digrafo, con ogni coppia $i, j \in V$ abbiamo $(i, j) \in E$ e $(j, i) \in E$. Se $|V| = n$ allora $n(n-1)$, ovvero tutte le possibili coppie (ordinate) di vertici.

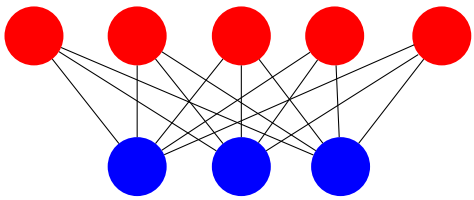


• **Torneo**:
Sia $G = (V, E)$ un grafo completo e orientato. Un **torneo** si ottiene assegnando uno dei due possibili versi ad ogni arco di G.



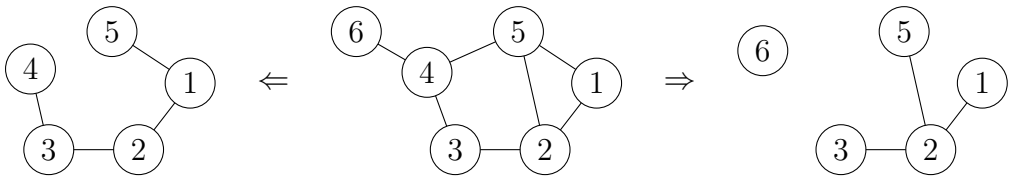
• **Bipartiti**:
Sia $G = (V, E)$ un grafo non orientato. G è detto **bipartito** se possiamo partizionare l'insieme dei vertici in due insiemi V_1 e V_2, affinché gli archi hanno come estremi un vertice in V_1 e uno in V_2.
Osservazione: Un grafo bipartito è completo se esiste un arco per ogni coppia di vertici $v \in V_1$ e $u \in V_2$. Si indica con $K_{n,m}$ con $n = |V_1|$ e $m = |V_2|$.



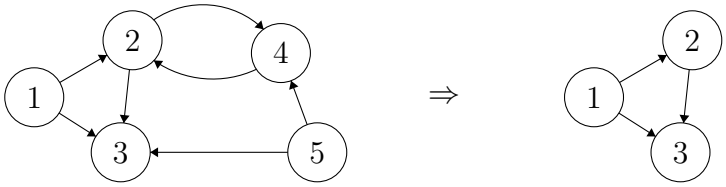


Esempi in figura:
- Grafo n°1: $V_1 = \{v_1, v_2, v_3, v_4, v_5\}$ e $V_2 = \{u_1, u_2, u_3, u_4\}$
- Grafo n°2: $n = 5$ e $m = 3 \Rightarrow G = K_{5,3}$

• **Sottografo**:
Sia $G = (V, E)$ un grafo non orientato o un digrafo. Allora $G' = (V', E')$ è un **sottografo** di G se $V' \subseteq V$, $E' \subseteq E$ ed inoltre per ogni arco $(u, v) \in E'$ i suoi estremi u, v appartengono entrambi a V'.



• **Sottografo Indotto**:
Sia $G = (V, E)$ un digrafo e sia $V' \subseteq V$ il sottografo **indotto** da V' è il sottografo $G' = (V, E)$ ottenuto eliminando da G tutti i vertici non appartenenti a V' e tutti gli archi incidenti ad almeno uno dei vertici eliminati.



Isomorfismo tra Grafi:
Dati due grafi $G_1 = (V_1, E_1)$ e $G_2 = (V_2, E_2)$, sia entrambi orientati o meno, si dicono **isomorfi** se esiste un applicazione biunivoca f dall'insieme dei vertici V_1 nell'insieme dei vertici V_2 tale che $(f(u),\ f(v))$ è un arco di di E_2 se e solo se $(u.v)$ è un arco di E_1. La biiezione f è detta **isomorfismo**.

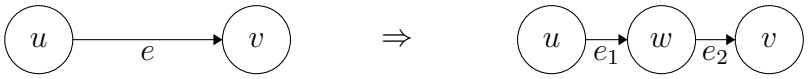
Esempi in figura: Consideriamo $G_1 = (V_1, E_1)$ e $G_2 = (V_2, E_2)$ così definiti:
- $V_1 = \{a, b, c, d\},\ E_1 = \{(a, b), (a, d), (b, c), (b, d), (c, d)\}$
- $V_2 = \{t, u, v, w\},\ E_2 = \{(t, u), (t, v), (u, v), (u, w), (v, w)\}$
Quindi: $f : V_1 \to V_2 \mid f(a) = t,\ f(b) = v,\ f(c) = w,\ f(d) = u$

Conseguenze dell'Isomorfismo:
• Se due grafi G_1 e G_2 sono isomorfi allora $|V_1| = |V_2|$ e $|E_1| = |E_2|$, tuttavia non vale il viceversa;
• Se $f(u) = v$ allora $\delta(u) = \delta(v)$ e per un digrafo $\delta^+(u) = \delta^+(v)$ e $\delta^-(u) = \delta^-(v)$

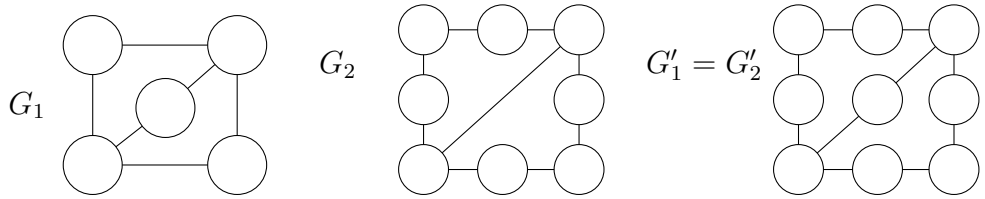
Grafi non Isomorfi:
Considerando i due grafi G_1 e G_2 in figura, non sono isomorfi perché G_1 ha un vertice c tale che $\delta(c) = 1$, invece i nodi di G_2 hanno grado ≥ 2. Inoltre eliminando il vertice c da G_1 si forma un sottografo completo, mentre nessun sottografo di G_2 con 4 vertici è completo.

Per i due grafi orientati G_1 e G_2 disegnati, non sono isomorfi per il diverso grado in uscita del vertice 5. Tuttavia se invertiamo il verso di (2,1) in (1,2), i due grafi diventano isomorfi.

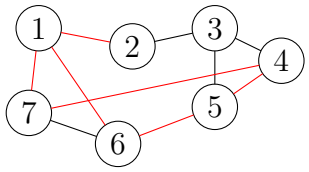
Omeomorfismi:
Sia $G = (V, E)$ un grafo non orientato e sia $e = (u, v)$ un arco di G. Una suddivisione dell'arco $e = (u, v)$ è ottenuta introducendo un nuovo nodo w e sostituendo in G l'arco (u, v) con gli archi $e_1 = (u, w)$ e $e_2 = (w, v)$.

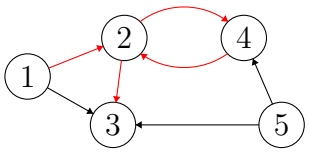


Omeomorfismi tra grafi:
Dati due grafi non orientati $G_1 = (V_1, E_1)$ e $G_2 = (V_2, E_2)$ si dicono **omeomorfi** se attraverso una serie di suddivisioni di archi G_1 e G_2 si possono ottenere due grafi G'_1 e G'_2 che sono isomorfi.



Percorso:
Un percorso (diretto) in un grafo (o in un digrafo) $G = (V, E)$ è una sequenza di nodi adiacenti connessi da archi. Un percorso può attraversare uno stesso vertice, ma non lo stesso arco.

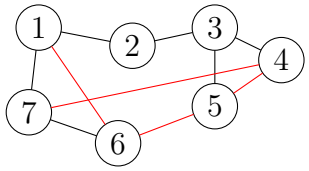
G_1 

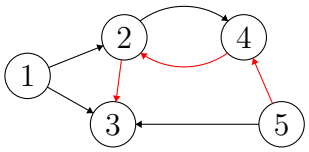


G_2

Esempi in figura: Considerando G_1 non orientato e G_2 orientato:
- Percorso di G_1: $1, 6, 5, 4, 7, 1, 2$
- Percorso di G_2: $1, 2, 4, 2, 3$

Cammino:
Un percorso (diretto) in un grafo (o digrafo) $G = (V, E)$ è detto **cammino** se, la sequenza di nodi adiacenti, oltre a non attraversare uno stesso arco, non attraversa più volte uno stesso nodo.

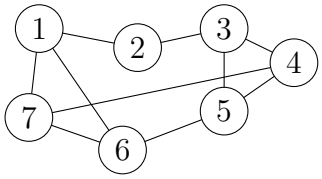
G_1 

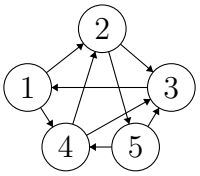


G_2

Esempi in figura: Considerando G_1 non orientato e G_2 orientato:
- Cammino di G_1: $1, 6, 5, 4, 7$
- Cammino di G_2: $5, 4, 2, 3$

Circuito (Percorso Chiuso):
Un percorso (diretto) in un grafo (o in un digrafo) $G = (V, E)$ è detto **circuito** se il percorso è chiuso, ovvero se il 1° nodo è anche quello conclusivo.

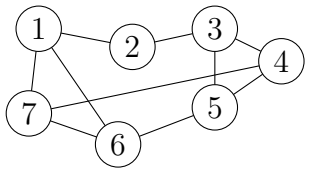
G_1 

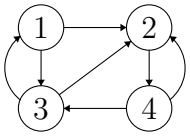


G_2

Esempi in figura: Considerando G_1 non orientato e G_2 orientato:
- Circuito di G_1: $1, 7, 6, 5, 3, 4, 5, 3, 2, 1$
- Circuito di G_2: $1, 2, 5, 4, 2, 3, 1$

Ciclo (Cammino Chiuso):
Un cammino (diretto) in un grafo (digrafo) $G = (V, E)$ è detto **ciclo** se il cammino è chiuso, ovvero se il 1° nodo è anche quello conclusivo.
Osservazione: Se il grafo non è orientato, il minimo di nodi per avere un ciclo è 3, mentre se il grafo è orientato, il minimo è 2.

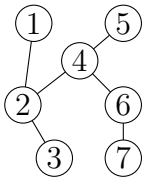
G_1 

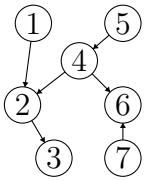


G_2

Esempi in figura: Considerando G_1 non orientato e G_2 orientato:
- Ciclo di G_1: $1, 6, 7, 1$ oppure $3, 4, 5, 3$
- Ciclo di G_2: $4, 2, 4$ oppure $1, 3, 1$

Grafi Aciclici:
Un grafo, o un digrafo, $G = (V, F)$ si dice **aciclico** se non possiede cicli.

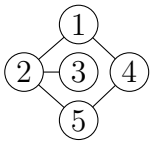


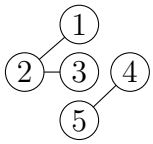


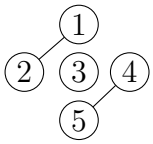
Esempi in figura: Entrambi i grafi in figura sono aciclici.

Vertici Connessi:
Dato un grafo $G = (V, E)$ diciamo che due vertici u, v sono connessi se esiste un cammino da u a v.
- La connessione tra vertici è una relazione di equivalenza.

Componenti connesse:
Sia $G = (V, E)$ un grafo e sia $V = V_1 \cup V_2 \cup ... \cup V_k$ la partizione indotta dalla relazione di connessione tra i vertici.
Sia $G = (V_i, E_i)$ il sottografo indotto da V_i per ogni $i = 1, ..., k$. Tali sottografi si chiamano componenti connesse di G.

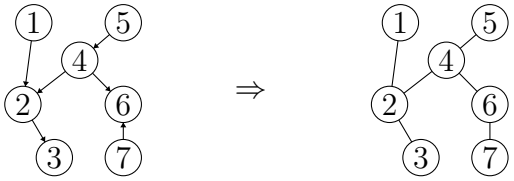






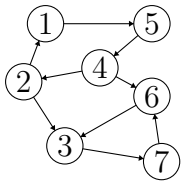
Esempi in figura: 1° Grafo con 1 c.c., 2° Grafo con 2 c.c., 3° Grafo con c.c.

Grafo Connesso:
Un grafo si dice **connesso** se ha una sola componente connessa, cioè se dati comunque due vertici di V, i due vertici sono connessi.
Digrafo Debolmente Connesso:
Un digrafo $G = (V, E)$ si dice **debolmente connesso** se il grafo non orientato ottenuto eliminando da G l'orientamento degli archi è connesso.



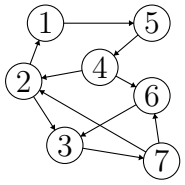
Esempio in figura: Grafo debolmente connesso.

Componenti Fortemente Connesse:
Sia $G = (V, E)$ un grafo e sia $V = V_1 \cup V_2 \cup ... \cup V_k$ la partizione indotta dalla relazione di connessione forte tra i vertici. Sia allora $G = (V_i, E_i)$ il sottografo indotto da V_i per ogni $i = 1, ..., k$. Tali sottografi si chiamano componenti **fortemente connesse** di G.



Esempio in figura: Il grafo in figura ha due componenti fortemente connesse, $V_1\{1, 2, 3, 4\}$ e $V_2 = \{3, 6, 7\}$.

Digrafo Fortemente Connesso:
Dato un grafo orientato $G = (V, E)$, G si dirà **fortemente connesso** se ha una sola componente fortemente connessa.

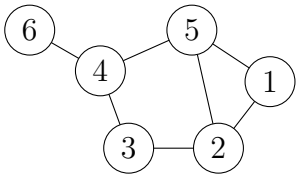


Esempi in figura: Il grafo in figura è fortemente connesso.

Grafi k-connessi:
Sia dato un grafo $G = (V, E)$:
• Il grafo $G = (V, E)$ si dice k-connesso rispetto agli archi se dati due vertci $u, v \in V$ esistono k cammini ad archi disgiunti tra u, v.
- Per disconnettere il grafo è necessario rimuovere almeno k-archi.
• Il grafo $G = (V, E)$ si dice k-connesso rispetto ai vertici se dati due vertci $u, v \in V$ esistono k cammini a nodi disgiunti tra u, v.
- Per disconnettere il grafo è necessario rimuovere almeno k-vertici.

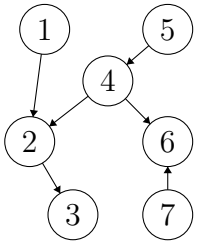
Rappresentazione di un Grafo con Matrice di Adiacenza:
Sia dato un grafo $G = (V, E)$ con $|V| = n$. L'insieme di archi E contiene le informazioni del grafo, ovvero se due nodi sono connessi da un arco oppure no. Supponendo $V = \{1, ..., n\}$, posso costruire una matrice quadrata M di dimensione $n \times n$:
• $M[i, j] = 1$ se i vertici i, j **sono** connessi da un arco;
• $M[i, j] = 0$ se i vertici i, j **non sono** connessi da un arco.
Osservazione: Se il grafo non è orientato, la matrice sarà simmetrica.

Esempio in figura n°1: Il grafo non orientato ha 6 nodi, quindi la sua matrice sarà 6×6.



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

Esempio in figura n°2: Il digrafo ha 7 nodi, quindi la sua matrice sarà 7×7.

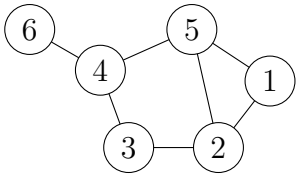


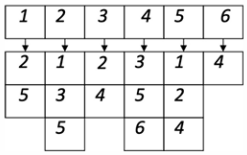
$$M = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}$$

La rappresentazione di un grafo con una Matrice di adiacenza è semplice, ma costosa in termini di spazio, ovvero n^2, ed è uno spreco di risorse se il grafo è **sparso**, ovvero se il numero di archi è basso.

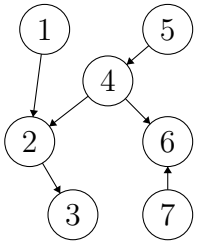
Rappresentazione di un grafo con Liste di Adiacenza:
Dato un grafo $G = (V, E)$ con $|V| = n$, associamo al grafo una lista concatenata di dimensione n, dove ogni elemento della lista è a sua volta una lista concatenata, dove mettiamo, in sequenza non ordinata, tutti i vertici collegati al vertice corrispondente.

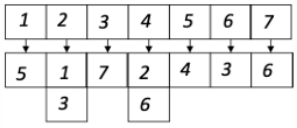
Esempio in figura n°1: Grafo non orientato con 6 nodi.





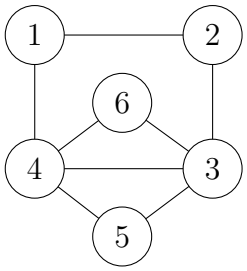
Esempio in figura n°2: Grafo orientato con 7 nodi.





Confronto tra le Rappresentazioni di un Grafo:
• **Visita del grafo**: Le **Matrici** di Adiacenza usano molto più spazio rispetto alle **Liste** di Adiacenza. Tuttavia le matrici verificano se è presente un arco tra due vertici u, v in tempo **costante** mentre con le liste impiega tempo **lineare** n.
• **Grado di un nodo**: Per un grafo non orientato, le **matrici** devono sommare gli elementi di una riga, quindi n controlli (tempo lineare). Le **liste** impiegheranno generalmente meno tempo.
• **Grado in ingresso di un nodo**: Per un digrafo, le **matrici** impiegheranno molto meno tempo delle **liste**, in quanto le prime dovranno sommare tutti i valori della colonna corrispondente al nodo, mentre le seconde dovranno scorrere tutte le liste di tutti i nodi e contare quante volte il nodo in questione appare.

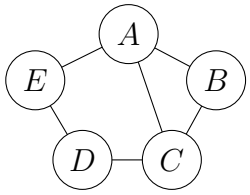
Circuito Euleriano:
Sia $G = (V, E)$ un grafo connesso. Un **circuito euleriano** di G è un circuito che passa per ogni arco di G esattamente una ed una sola volta. Se G possiede un **circuito euleriano**, il grafo si dirà **euleriano**.



Esempio in figura:
Il grafo in figura ha un circuito euleriano: $1 - 2 - 3 - 5 - 4 - 3 - 6 - 4 - 1$

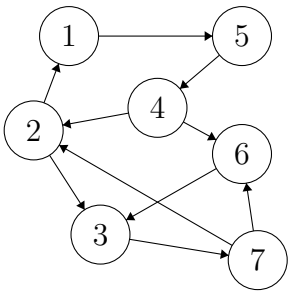
Teorema di Eulero:
Un grafo $G = (V, E)$ è **euleriano** se e solo se è **connesso** ed i suoi vertici hanno tutti grado pari.

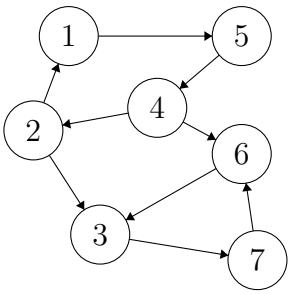
Cammino Euleriano:
Un grafo $G = (V, E)$ possiede un **cammino euleriano** se e solo se è connesso ed i suoi vertici, tranne al più 2, hanno tutti grado **pari**. I due vertici di grado dispari saranno il primo e l'ultimo vertice del cammino.



Esempio in figura: Nel grafo in figura i vertici A e C hanno grado dispari ma possiede un cammino euleriano che passa per tutti gli archi una ed una sola volta: $A - B - C - D - E - A - C$.

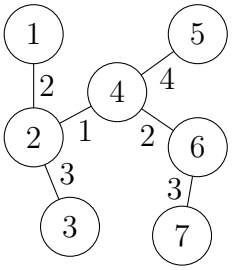
Cammino Hamiltoniano:
Sia $G = (V, E)$ un grafo, o un digrafo, connesso.
Un **cammino hamiltoniano** di G è un circuito che passa una ed una sola volta per tutti i vertici di G. *Osservazioni*:
• Se il cammino è **chiuso**, ovvero un ciclo, esso si dirà **ciclo hamiltoniano**;
• Se un grafo si dirà **hamiltoniano** se possiede un **ciclo hamiltoniano**.

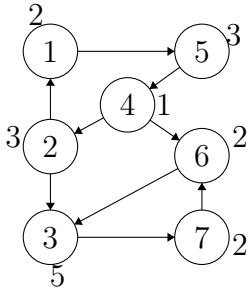




Esempi in figura: Il grafo a sinistra è hamiltoniano in quanto possiede il ciclo hamiltoniano: $1 - 5 - 4 - 6 - 3 - 7 - 2 - 1$.
Il grafo a destra invece non è hamiltoniano.

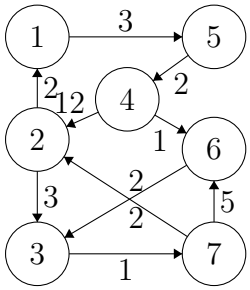
Grafi Pesati:
Un grafo, o un digrafo, $G = (V, E)$ si dice **pesato** se è data un'applicazione $c : E \to R$ oppure $c : V \to R$. I pesi (costi) possono essere associati agli archi e/o ai nodi:
• La somma dei costi associati ai suoi archi α è: $c(v_1, v_2) + c(v_2, v_3) + ... + c(v_{k-1}, v_k)$
• La somma dei costi associati ai suoi nodi α è: $c(v_1) + c(v_2) + ... + c(v_k)$.





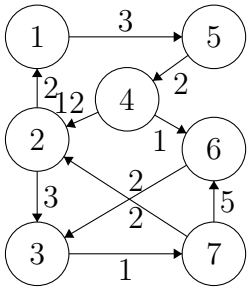
Esempi in figura: Nei grafi in figura il costo del cammino $5 - 4 - 2 - 1$ è:
• Grafo non orientato con peso sugli archi: $4 + 1 + 2 = 7$
• Grafo orientato con peso sui vertici: $3 + 1 + 3 + 2 = 9$

Cammini Minimi e Cammini Massimi:
• Dato un grafo, o un digrafo, $G = (V, E)$ pesato, con funzione $c : E \to R$ oppure $c : V \to R$, si dice cammino di costo **minimo** dal nodo v al nodo w quel cammino che ha costo, rispetto alla funzione c, minimo.
• Dato un grafo, o un digrafo, $G = (V, E)$ pesato, con funzione $c : E \to R$ oppure $c : V \to R$, si dice cammino di costo **massimo** dal nodo v al nodo w quel cammino che ha costo, rispetto alla funzione c, massimo.



Esempi in figura: $\alpha_{1,2} = c(v_1, v_5) + c(v_5, v_4) + c(v_4, v_6) + c(v_6, v_3) + c(v_3, v_7) + c(v_7, v_2) = 3 + 2 + 1 + 2 + 1 + 2 = 11$
$\alpha_{1,2} = c(v_1, v_5) + c(v_5, v_4) + c(v_4, v_6) + c(v_6, v_3) = 2 + 3 + 2 + 1 = 8$

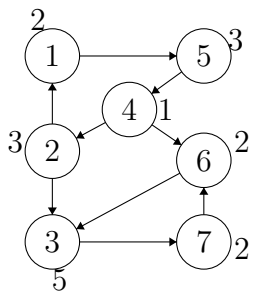
Rappresentazione Grafi Pesati:
Assumendo di avere una funzione peso sugli archi, con i pesi tutti positivi, la rappresentazione più semplice per un grafo, o un digrafo, pesato è quella di una matrice con:
• il peso dell'arco invece di 1;
• 0 se manca l'arco.



$$M = \begin{pmatrix} 0 & 0 & 0 & 0 & 3 & 0 & 0 \\ 2 & 0 & 3 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 12 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 2 & 0 & 0 & 0 \\ 0 & 0 & 2 & 0 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 & 0 & 5 & 0 \end{pmatrix}$$

Esempio in figura: Grafo pesato sugli archi e matrice di adiacenza.

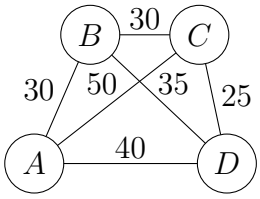
Se abbiamo una funzione peso sui vertici, la soluzione più semplice è:
• costruire la Matrice di Adiacenza M
• costruire il vettore c di lunghezza V



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

$$C = \begin{pmatrix} 2 & 3 & 5 & 1 & 3 & 2 & 2 \end{pmatrix}$$

Il Problema del Commesso Viaggiatore:
Il Problema del Commesso Viaggiatore è caratterizzato come il problema di trovare un **circuito hamiltoniano** che minimizza il costo totale per un grafo pesato, dove ad ogni arco è associato un peso positivo.

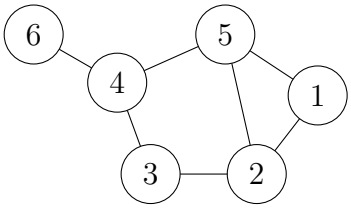


Circuito	Distanza Totale
ABCDA	$30 + 30 + 25 + 40 = 125$
ABDCA	$30 + 35 + 25 + 50 = 140$
ACBDA	$50 + 30 + 35 + 40 = 155$
ACDBA	$50 + 25 + 35 + 30 = 140$
ADBCA	$40 + 35 + 30 + 50 = 155$
ADCBA	$40 + 25 + 30 + 30 = 125$

Esempio in figura: Considero il grafo in figura. Se un commesso viaggiatore deve attraversare tutti e 4 i nodi, partendo da A e tornando ad A, qual'è il percorso che minimizza il costo totale?
Il problema va risolto analizzando tutti i circuiti hamiltoniani.

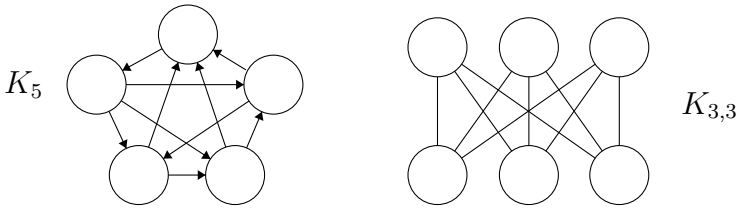
Problema:
Per grafi con un gran numero di vertici questo metodo richiede tempi non umani e, nonostante esistano algoritmi in grado di trovare soluzioni in tempi umani, si basano tutti su questo metodo.

Grafi Planari:
Sia $G = (V, E)$ un grafo non orientato. Diciamo che G è planare se può essere raffigurato in un piano in modo che non si abbiano archi che si intersecano.

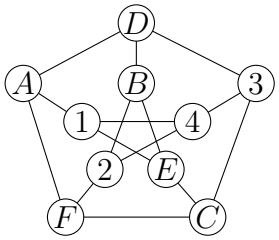


Esempio in figura: Esempio di Grafo Planare.

Teorema di Kuratowski:
Un grafo è planare se e solo se non contiene alcun sottografo che sia **omeomorfo** a K_5 o $K_{3,3}$.



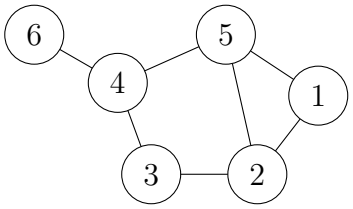
Esistono altri criteri per stabilire se un grafo è planare o meno:
• Se $G = (V, E)$ è un grafo connesso e planare, se $|V| \geq 3$ allora $|E| \leq 3|V|-6$
• Se $G = (V, E)$ è un grafo connesso e planare, se $|V| > 3$ e non ci sono cicli di lunghezza 3 allora $|E| \leq 2|V| - 4$

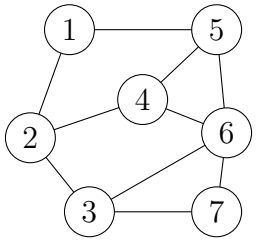


Esempio in figura: Il grafo in figura è il grafo di Petersen, esso non è planare perché:
• Avendo 10 vertici e 15 archi non possono essere applicati i due criteri.
• Ricorrendo a Kuratowski, il grafo presenta un sottografo omeomorfo a $K_{3,3}$, quindi non è planare. (Spiegazione nella pagina successiva)

Infatti:
- I due insiemi sono $V_1 = \{A, B, C\}$ e $V_2 = \{D, E, F\}$.
- Gli archi del $K_{3,3}$ sono $(A, D), (A, F), (B, D), (B, E), (C, E), (C, F)$.
- I tre archi mancanti sono dei cammini disgiunti:
$(A, E) \sim (A, 1), (1, E)$; $(B, F) \sim (B, 2), (2, F)$; $(C, D) \sim (C, 3), (3, D)$.

Formula di Eulero:
Dato un grafo $G = (V, E)$ planare e connesso, con v il numero di vertici, e il numero degli archi e con f il numero delle facce. Allora: $v - e + f = 2$
Per dimostrarlo, bisogna prima enunciare e dimostrare due teoremi che fanno da condizione necessaria.





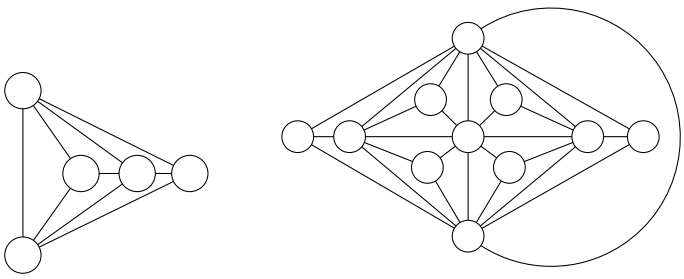
Esempi in figura: Grafi planari e connessi.

1°Teorema:
Sia $G = (V, E)$ un grafo connesso con $|V| \geq 3$ e con $\delta(v) \geq 2$ per ogni v. Allora G possiede un ciclo.
Dimostrazione:
Ordiniamo i vertici e chiamiamoli $v_1, v_2, ..., v_n$ con $n = |V| \geq 3$.
Partiamo allora dal vertice v_1 e costruiamo un cammino il più lungo possibile senza ripetizione di vertici. Supponiamo che il cammino più lungo senza ripetizione di vertici sia $v_1, v_2, ..., v_k$.
Se $k = n$ allora abbiamo trovato un **cammino hamiltoniano**.
In ogni caso, dal vertice v_k possiamo ancora raggiungere un altro vertice, visto che il suo grado è almeno 2.
Dal momento che ci siamo fermati,vuol dire che possiamo raggiungere un vertice già visto, quindi uno tra v_1 dimostra l'esistenza di un ciclo.

2° Teorema:
Sia $G = (V, E)$ un grafo connesso e aciclico. Allora $|E| = |V| - 1$.
Dimostrazione: Si dimostra per induzione su $|V|$.
La dimostrazione è banale per $|V| \leq 2$.
Supponendo $|V| \geq 3$, essendo il grafo connesso ed aciclico deve esistere un nodo di grado 1 (altrimenti avrebbe un ciclo o non sarebbe connesso).
Prendiamo allora un vertice v di grado 1 e rimuoviamolo dal grafo assieme all'arco su esso incidente.
Il grafo indotto da $V \backslash \{v\}$ è connesso, altrimenti dovremmo avere 2 vertici, u, w che sono connessi solo da un cammino passante per v ossia
$u, .., u', v, w, ..., w'$ ma ciò implicherebbe che v ha grado maggiore di 1.
Quindi, tale grafo indotto è connesso ed aciclico e quindi per induzione ha $V - 2$ archi. Aggiungendo v e l'arco ad esso incidente, abbiamo quindi che $|E| = |V| - 1$.

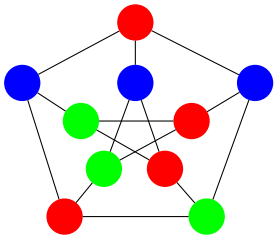
Ora si può dimostrare la Formula di Eulero.
Dimostrazione: Se G possiede un ciclo, togliamo un arco che completa il ciclo. La quantità di archi e di facce si abbassa di un'unità, ma $v - e + f$ rimane invariata.
Ripetiamo la rimozione di archi, affinché il grafo diventi aciclico (rimanendo connesso). Essendo G aciclico, $f = 1$ ed $e = v - 1$ e quindi $v - e + f = 2$.

Grafi Planari Massimali:
Un grafo planare si dice **massimale**, o triangolare, se è planare e se aggiungendo un nuovo arco ad una qualunque coppia di vertici, il grafo non è più planare.
Osservazione: Ogni grafo planare massimale con v vertici ha esattamente $3v - 6$ archi e $2v - 4$ facce.



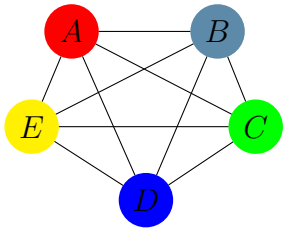
Esempi in figura: Due grafi planari massimali, quello a sinistra con 5 vertici e quello a destra con 11 vertici.

Colorazione di un Grafo:
Un grafo G è k colorabile se è possibile colorare i suoi vertici in maniera tale che, collegando due vertici con un arco, essi abbiano colori diversi, usando al più k-colori.
Con $\chi(G)$ si indica il numero minimo di colori necessari per colorare il grafo.



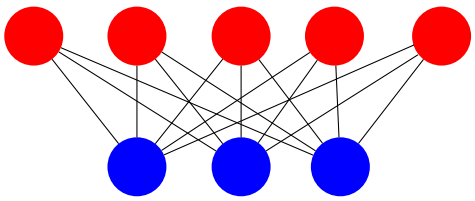
Esempio in figura: Colorazione del grafo di Petersen

Colorazione di un Grafo Completo:
Con un grafo completo K_n ogni vertice è connesso da un arco ad ogni altro vertice, quindi con n vertici servono n colori diversi, ovvero: $\forall n\ ,\ \chi(K_n) = n$.



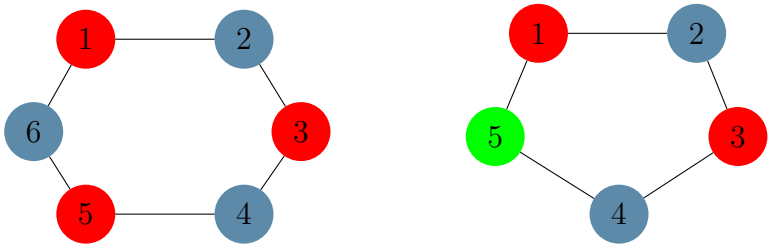
Esempio in figura: Colorazione di un grafo completo K_5.

Colorazione di un Grafo Bipartito:
Con un grafo **bipartito** $G = (V, E)$ essendo l'insieme dei vertici diviso in due insiemi V_1 e V_2, possiamo assegnare un colore ad un insieme e un altro colore all'altro. Quindi tutti i grafi bipartiti sono 2-colorabili.



Esempio in figura: Colorazione di un grafo bipartito $K_{5,3}$.

Colorazione di un Ciclo semplice:
Supponiamo di avere un grafo $G = (V, E)$ che consiste di un semplice ciclo e lo denotiamo con C_n, dove la n è il numero di vertici del grafo:
• Se n è **pari** C_n è 2-colorabile;
• Se n è **dispari** C_n è 3-colorabile.
In generale: $\chi(C_n) = 2 + n \ mod \ 2$.



Esempi in figura: Grafi colorati con n pari ed n dispari.

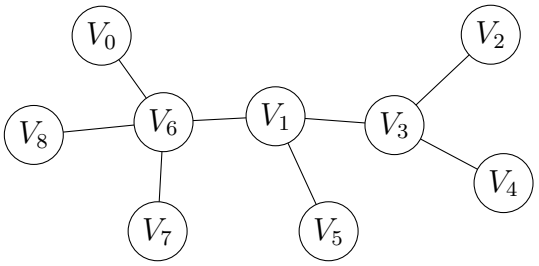
Teorema di Brooks:
Sia $G = (V, E)$ un grafo **connesso** con n vertici e siano $\delta_1 \geq \delta_2 \geq ... \geq \delta_n$ i gradi dei vertici del grafo in ordine **decrescente**. Allora $\chi(G) = \delta_1 + 1$.
Dimostrazione:
Si dimostra per induzione.
Se togliamo, il vertice di grado maggiore v_1 rimaniamo con un grafo con un vertice in meno e colorabile, per ipotesi induttiva, con al più $\delta_2 + 1 \leq \delta_1 + 1$. Aggiungendo il vertice tolto, il caso peggiore è che i δ_1 vertici a lui connessi siano tutti di colore diverso e quindi gli dobbiamo dare il colore rimasto dei $\delta_1 + 1$.

Teorema di Brooks (Versione Forte):
Sia $G = (V, E)$ un grafo **connesso** con n vertici e siano $\delta_1 \geq \delta_2 \geq ... \geq \delta_n$ i gradi dei vertici del grafo in ordine **decrescente**.
Se G non è un grafo **completo** e G non è un **ciclo semplice** con n numero **dispari** di vertici, allora $\chi(G) \leq \delta_1$.

Teorema dei 4 colori:
Sia $G = (V, E)$ un grafo **planare**, allora $\chi(G) \leq 4$.

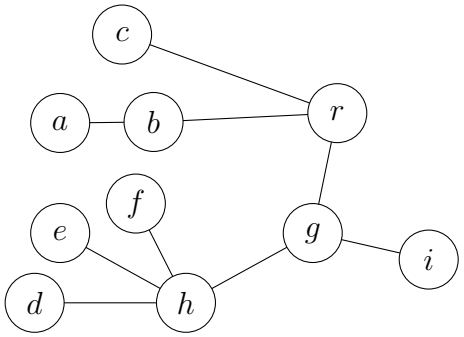
4.2 Alberi

Albero Libero:
Un **albero libero** è un grafo $G = (V, E)$ connesso e aciclico. Inoltre:
• un albero libero con $|V|$ vertici ha esattamente $|V| - 1$ archi;
• Ogni vertice ha almeno grado 1 e ne deve esistere almeno uno di grado 1;
• Se $|V| \leq 2$ tutti i vertici sono detti **terminali**;
• Se $|V| > 2$ i vertici di grado 1 sono detti **terminali** o **foglie**, mentre i vertici di grado maggiore di 1 sono detti **interni**;



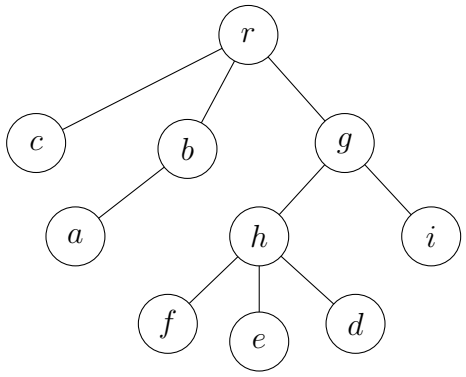
Esempio in figura: L'albero libero in figura ha 9 vertici, di cui 6 sono foglie e 3 sono interni.

Foresta:
Una **foresta** è un insieme di uno o più alberi, quindi un grafo $G = (V, E)$ aciclico. Ogni componente connessa di G è un albero della foresta.



Esempio in figura: La foresta in figura ha 10 vertici, di cui 6 sono terminali (c, a, d, e, f, i) e 4 sono interni (b, r, g, h).

Alberi Radicati:
Dato un albero libero, se scegliamo un nodo come **radice**, i suoi nodi cadono per gravità e otteniamo così un **albero radicato** o semplicemente albero.
Proprietà:
• L'altezza di un albero T è la lunghezza del cammino più lungo dalla radice ad una foglia.
• Il fattore di ramificazione dell'albero è il numero massimo di figli che ognuno dei nodi ha.



Esempio in figura: L'albero in figura ha altezza 3 e fattore di ramificazione 3. La radice ha 3 figli, il nodo g ha 2 figli, le foglie sono caratterizzate come i nodi che non hanno figli, nell'esempio c, a, d, e, f, i.