Matematica discreta e logica

Anno accademico 2022/2023
Corso di laurea in Informatica

Nicola Papini

Indice

1 Insiemi, funzioni e relazioni

1.1 Insiemi

Un insieme è definito come una collezione di elementi distinti tra loro. Un insieme non è ordinato, ossia non conta l'ordine degli elementi. Due insiemi si dicono equivalenti se contengono esattamente gli stessi elementi.

Esempi:
$\{4,2,6\} = \{2,4,6\} \quad \mathbb{N} = \{0,1,2,3,\dots\} \quad \mathbb{Z} = \{\cdots -2,-1,0,1,2,\dots\} \quad \mathbb{Q} = \{\frac{a}{b} | a,b \in \mathbb{Z}, b \neq 0\}$

Notazione.

- $x \in A$: x appartiene ad A, analogamente $x \notin A$ significa che x non appartiene ad A.
- $A \subseteq B$: A sottoinsieme di B, ossia ogni elemento di A è anche elemento di B.

  Osservazione 1. $\forall\, A$ *insieme* $\emptyset \subseteq A$. *Inoltre* $A = B \iff A \subseteq B$ *e* $B \subseteq A$

Definizione 1 (Insieme delle parti)**.** *Sia A insieme, allora si dice insieme delle parti di A l'insieme composto da tutti i sottoinsiemi di A.*

$$P(A) = \{x | x \subseteq A\}$$

Esempi:
Sia $A = \{1, \{2\}\}$, allora:
$1 \in A$ Vero, $\{1\} \in A$ Falso, $\{1\} \subseteq A$ Vero, $\{2\} \subseteq A$ Falso, $\{2\} \in A$ Vero, $\{1\} \neq \{\{1\}\}$

Sia $B = \{1,2\}$, allora $P(B) = \{\emptyset, \{1\}, \{2\}, \{1,2\}\}$

1.1.1 Operazioni tra insiemi

Siano A, B insiemi, allora sono definite le seguenti operazioni:

1. Unione, $A \cup B = \{x | x \in A \vee x \in B\}$
2. Intersezione, $A \cap B = \{x | x \in A \wedge x \in B\}$
3. Differenza, $A \setminus B = \{x | x \in A \wedge x \notin B\}$
4. Differenza simmetrica, $A \Delta B = (A \setminus B) \cup (B \setminus A) = (A \cup B) \setminus (A \cap B)$
5. Complementare di un'insieme A rispetto a U, $A^C = \{x \in U | x \notin A\}$. U è definito come insieme Universo, ossia l'insieme che contiene tutti gli elementi.

Proprietà:

- Proprietà commutativa: vale per unione, intersezione e differenza simmetrica.
- Proprietà associativa, vale per unione, intersezione e differenza simmetrica.
- Proprietà distributiva, siano A, B, C insiemi:

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

Definizione 2 (Prodotto cartesiano)**.** *Siano A, B insiemi allora il loro prodotto cartesiano è definito come:*

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

(a, b) è una coppia ordinata di due elementi. Vale l'uguaglianza $(a, b) = (c, d) \iff a = c \wedge b = d$. Inoltre $\{a, b\} = \{b, a\}$ ma $(a, b) \neq (b, a)$, nelle coppie ordinate l'ordine conta.
Esempio:
Siano $A = \{a, b\}$ e $B = \{1, 2, 3\}$, allora $A \times B = \{(a, 1), (a, 2), (a, 3), (b, 1), (b, 2), (b, 3)\}$

Definizione 3 (Relazione)**.** *Siano A,B insiemi, una relazione R di A in B è un sottoinsieme del prodotto cartesiano $A \times B$ cioè $R \subseteq A \times B$. Scrivo aRb se $(a, b) \in R$.*

Esempi:

1. $\leq$ la relazione di minore uguale in $\mathbb{R}$
2. Relazione di uguaglianza
3. Ortogonalità tra retta e piano

La relazione inversa è definita come $R^{-1} = \{(b, a) | (a, b) \in R\}$.

1.2 Funzioni

Definizione 4 (Funzione)**.** *Siano A,B insiemi, F funzione di A in B, A dominio e B codominio, è una relazione $F \subseteq A \times B$ tale che per ogni $a \in A$ esiste un'unica coppia $(a, b) \in F$. Scrivo $b = F(a)$ se $(a, b) \in F$.*

Definizione 5 (Funzione)**.** *Equivalentemente dati A e B insiemi, una funzione $f : A \to B$ è una legge che associa ad ogni elemento $a \in A$ uno e uno solo elemento $b \in B$. Scrivo $b = f(a)$.*

Definizione 6 (Funzione iniettiva)**.** *Una funzione f si dice iniettiva se elementi diversi hanno immagini diverse, ossia se per ogni $a_1, a_2 \in A$ tale che $a_1 \neq a_2$ allora $f(a_1) \neq f(a_2)$. Analogamente se $f(a_1) = f(a_2)$ allora $a_1 = a_2$.*

Definizione 7 (Funzione suriettiva)**.** *Una funzione f si dice suriettiva se per ogni $b \in B$, elemento del codominio, esiste almeno un elemento del dominio $a \in A$ tale che $b = f(a)$. Ossia ogni elemento del codominio è immagine di almeno un elemento del dominio.*

Definizione 8 (Funzione biettiva)**.** *Una funzione f si dice biettiva se f è iniettiva e suriettiva.*

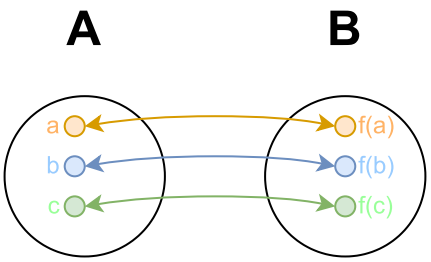


Figure 1: Funzione biettiva

Osservazione 2. *Se F è una funzione non è detto che $F^{-1} = \{(b,a)|(a,b) \in F\}$ sia una funzione. f^{-1} è una funzione se e solo se f è biettiva.*

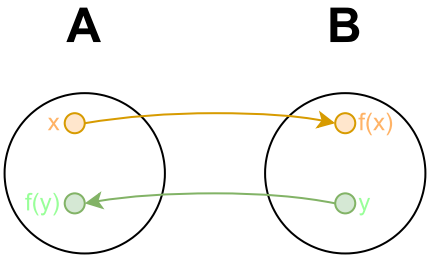


Figure 2: Funzione inversa

Definizione 9 (Composizione di funzioni)**.** *Siano $f : A \to B$ e $g : B \to C$ funzioni allora definisco g composto f, $g \circ f : A \to C$ tale che $\forall\, a \in A \quad g \circ f(a) = g(f(a))$.*

Proprietà:

- $\circ$ non è commutativa cioè $f \circ g \neq g \circ f$
- $\circ$ è associativa cioè $\forall\, f, g, h : A \to A$ vale $(f \circ g) \circ h = f \circ (g \circ h)$.
  Dimostrazione. Per $a \in A$ si ha che

$$(f \circ g) \circ h(a) = f \circ g(h(a)) = f(g(h(a)))$$
$$f \circ (g \circ h)(a) = f(g \circ h(a)) = f(g(h(a)))$$

□

Definizione 10 (Funzione identità)**.** *Sia A insieme, definisco la funzione identità o identica su A come $i_A : A \to A$ tale che $i_A(x) = x \quad \forall\, x \in A$.*

Definizione 11 (Funzione Inversa)**.** *Una funzione $f : A \to B$ si dice invertibile se esiste una funzione $g : B \to A$ tale che:*

$$\begin{cases} g \circ f = i_A \\ f \circ g = i_B \end{cases}$$

Si dice che g è un'inversa sinistra e destra di f.

Proposizione 1. *Sia $f : A \to B$ funzione, allora f è invertibile se e solo se f è biettiva e f^{-1} è la sua inversa sia destra che sinistra, cioè:*

$$\begin{cases} f^{-1} \circ f = i_A \\ f \circ f^{-1} = i_B \end{cases}$$

Proposizione 2. *Siano $f : A \to B$ e $g : B \to C$ funzioni, allora:*

- *Se f e g sono iniettive allora anche la composizione $g \circ f$ è iniettiva.*
- *Se f e g sono suriettive allora anche la composizione $g \circ f$ è suriettiva.*

Dimostrazione.

1. f e g iniettive, siano $a_1, a_2 \in A$ tale che $g \circ f(a_1) = g \circ f(a_2)$. Allora $g(f(a_1)) = g(f(a_2))$ e $f(a_1), f(a_2) \in B$ ma g è iniettiva quindi $f(a_1) = f(a_2)$. Ora, f è iniettiva quindi $a_1 = a_2$. Quindi $g \circ f$ è iniettiva.
2. f e g suriettive, provo che per ogni $c \in C$ esiste $a \in A$ tale che $g \circ f(a) = c$.
   g è suriettiva quindi esiste $b \in B$ tale che $g(b) = c$).
   Analogamente per f esiste $a \in A$ tale che $f(a) = b$.
   Allora $g \circ f(a) = g(f(a)) = g(b) = c$. □

Definizione 12 (Principio di induzione)**.** *Sia $P(n)$ una proprietà dove $n \in \mathbb{N}$. Allora:*

- *I forma. Se $P(0)$ è vera (caso base) e $\forall\, n \in \mathbb{N}$,$P(n) \Rightarrow P(n+1)$ (passo induttivo). Allora $P(n)$ è vera $\forall\, n \in \mathbb{N}$.*
- *II forma. Se $P(0)$ è vera e $\forall\, n \in \mathbb{N}$,$P(0), P(1), P(n) \Rightarrow P(n+1)$. Allora $P(n)$ è vera $\forall\, n \in \mathbb{N}$.*
- *Principio del minimo. Sia $X \subseteq \mathbb{N}$ tale che $X \neq \emptyset$, allora esiste $x_0 = min(X)$, ovvero $x_0 \in X$ e $\forall\, x \in X \quad x_0 \leq x$.*

1.3 Successioni

Definizione 13 (Successione)**.** *Una successione è una funzione $f : A \subseteq \mathbb{N} \to X$. Solitamente gli elementi della successione sono indicati con a_n dove n è l'indice naturale.*

Definizione 14 (Successione ricorsiva)**.** *Una successione ricorsiva è una funzione in cui abbiamo assegnato un valore iniziale $a_0 = b$ e una legge per calcolare un termine della successione in funzione del termine, o termini, che lo precedono.*

Esempio:
Successione di Fibonacci:

$$F_n = \begin{cases} F_0 = 0 \\ F_1 = 1 \\ F_n = F_{n-1} + F_{n-2} \quad n \geq 2 \end{cases}$$

Definizione 15 (Successione di ricorrenza lineare)**.** *$\{a_n\}_{n \in \mathbb{N}}$ successione definita dalla relazione ricorsiva lineare $a_n = c_1 a_{n-1} + c_2 a_{n-2} + \cdots + c_k a_{n-k} + c$ per $k \geq k$ con $c_1, c_2, \ldots, c_k \in \mathbb{R}$ costanti con $k \geq 1$.*

Nel caso in cui il termine noto $c = 0$ allora la relazione ricorsiva lineare si definisce omogenea e avrà quindi la forma $a_n = c_1 a_{n-1} + c_2 a_{n-2} + \cdots + c_k a_{n-k}$.

Definizione 16 (Formula chiusa)**.** *È una formula che permette di calcolare direttamente il termine generico di una relazione di ricorrenza lineare senza dover passare attraverso passaggi intermedi.*

1.3.1 Relazioni ricorsive lineari omogenee

Algoritmo risolutivo di una relazione ricorsiva lineare omogenea:

Data la relazione ricorsiva lineare omogenea di grado k

$$a_n = \alpha_1 a_{n-1} + \alpha_2 a_{n-2} + \cdots + \alpha_k a_{n-k}$$

1. Determinare il polinomio caratteristico
$$P(x) = x^k - \alpha_1 x^{k-1} - \alpha_2 x^{k-2} - \cdots - a_k$$
2. Risolvere $P(x) = 0$ e trovare le radici $x_1, x_2, \ldots, x_n$
3. Se le radici sono tutte distinte allora la formula chiusa è
$$a_n = c_1 x_1^n + c_2 x_2^n + \cdots + c_k x_k^n$$
altrimenti se le radici hanno molteplicità $m_1, m_2, \ldots, m_t$ tali che $m_1 + m_2 + \cdots + m_t = k$
$$a_n = (b_1 + b_2 n + \cdots + b_m n^{m-1}) x_1^n + \cdots + (d_1 + d_2 n + \cdots + d_{m_t} n^{m_t - 1}) x_t^n$$
4. Risolvo il sistema imponendo le condizioni iniziali

Esempi:

1. Uso la successione di Fibonacci
$$F_n = \begin{cases} F_0 = 0 \\ F_1 = 1 \\ F_n = F_{n-1} + F_{n-2} \quad n \geq 2 \end{cases}$$
   (a) Scrivo il polinomio caratteristico di $F_n = F_{n-1} + F_{n-2}$ e trovo le radici:
$$p(x) = x^2 - x - 1$$
$$x_{1,2} = \frac{1 \pm \sqrt{5}}{2} = \Phi$$
   (b) Sostituisco nell'equazione e ottengo:
$$F_n = b_1 (\frac{1+\sqrt{5}}{2})^n + b_2 (\frac{1-\sqrt{5}}{2})^n$$
   (c) Impongo le condizioni iniziali $F_0 = 0$, $F_1 = 1$
$$F_n = \begin{cases} F_0 = b_1 + b_2 = 0 \\ F_1 = b_1 (\frac{1+\sqrt{5}}{2}) + b_2 (\frac{1-\sqrt{5}}{2}) = 1 \end{cases}$$
$$F_n = \begin{cases} b_2 = -b_1 \\ b_1 (1+\sqrt{5}) + b_2 (1-\sqrt{5}) = 2 \end{cases}$$
$$F_n = \begin{cases} b_1 = \frac{1}{\sqrt{5}} \\ b_2 = -\frac{1}{\sqrt{5}} \end{cases}$$

(d) Infine ottengo la formula chiusa dell'n-esimo numero della serie di Fibonacci

$$F_n = \frac{1}{\sqrt{5}}(\frac{1+\sqrt{5}}{2})^n - \frac{1}{\sqrt{5}}(\frac{1-\sqrt{5}}{2})^n$$

2. Esempio con relazione di ricorrenza lineare omogenea di grado 2.

$$\begin{cases} a_n = a_{n-1} + 6a_{n-2} \\ a_0 = 3,\ a_1 = 5 \end{cases}$$

Si procede in modo analogo a sopra. Quindi:

$$p(x) = x^2 - x - 6 = 0$$

$$x_1 = 3 \qquad x_2 = -2$$

$$a_n = b_1 3^n + b_2(-2)^n$$

Impongo le condizioni iniziali:

$$\begin{cases} b_1 + b_2 = 0 \\ 3b_1 - 2b_2 = 1 \end{cases}$$

$$\begin{cases} b_1 = \frac{1}{5} \\ b_2 = -\frac{1}{5} \end{cases}$$

Infine ottengo la formula chiusa:

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

3. Caso in cui l'equazione caratteristica ha $\Delta = 0$:

$$\begin{cases} a_n = 6a_{n-1} - 9a_{n-2} \\ a_0 = 1,\ a_1 = 2 \end{cases}$$

Scrivo polinomio caratteristico e trovo le radici:

$$p(x) = x^2 - 6x + 9 = 0 = (x-3)^2$$

$$x_1 = x_2 = 3$$

Radice di molteplicità algebrica $m_a(x) = 2$. Impongo le condizioni iniziali:

$$\begin{cases} b_1 = 1 \\ b_2 = -\frac{1}{3} \end{cases}$$

Quindi ottengo la seguente formula chiusa:

$$a_n = 3^n - \frac{1}{3}n3^n = 3^n(1 - \frac{1}{3}n)$$

4. Caso radici con molteplicità maggiore di uno:

$$\begin{cases} a_n = 8a_{n-2} - 16a_{n-4} \\ a_0 = 1 \\ a_1 = 4 \\ a_2 = 28 \\ a_3 = 32 \end{cases}$$

L'equazione caratteristica è

$$P(x) = x^4 - 8x^2 + 16 = (x^2 - 4)^2 = 0$$

quindi le radici sono

$$x_1 = 2 \qquad x_2 = -2$$

con molteplicità

$$m_a(x_1) = 2 \qquad m_a(x_2) = 2$$

segue

$$a_n = (b_1 + b_2 n)2^n + (d_1 + d_2 n)(-2)^n$$

impongo le condizioni iniziali e trovo

$$\begin{cases} b_1 = 1 \\ b_2 = 2 \\ d_1 = 0 \\ d_2 = 1 \end{cases}$$

quindi la formula chiusa della relazione è

$$a_n = (1 + 2n)2^n + n(-2)^n$$

1.3.2 Relazioni ricorsive lineari non omogenee

Sono relazioni della forma

$$a_n = c_1 a_{n-1} + c_2 a_{n-2} + \cdots + c_k a_{n-k} + f(n)$$

Algoritmo risolutivo:

1. Risolvo la parte omogenea e ottengo la sua formula chiusa a_n^0
2. Cerco soluzione particolare di $f(n)$:
   (a) Se $f(n) = cq^n$:
   - Se q non è una radice del polinomio caratteristico $P(x)$ allora $b_n = \alpha q^n$
   - Se q radice di molteplicità m allora $b_n = \alpha n^m q^n$

   (b) Se $f(n)$ è un polinomio di grado K:
   - Se 1 non è radice di $P(x)$ allora $b_n = \alpha_0 + \alpha_1 n + \cdots + \alpha_k n^k$
   - Se 1 è radice di molteplicità m allora $b_n = n^m(\alpha_0 + \alpha_1 n + \cdots + \alpha_k n^k)$

3. Sostituisco b_n in a_n e trovo α
4. Sostituisco α in b_n e trovo la soluzione particolare b_n
5. Sommo a_n^0 e b_n e ottengo la formula chiusa di a_n

Esempio.

$$\begin{cases} a_n = a_{n-1} + a_{n-2} + 3n + 1 \quad n \geq 2 \\ a_0 = 2 \\ a_1 = 3 \end{cases}$$

Risolvo la parte omogenea $a_n = a_{n-1} + a_{n-2}$ quindi

$$P(x) = x^2 - x - 1 = 0$$

con radici

$$x_1 = \frac{1+\sqrt{5}}{2} \qquad x_1 = \frac{1-\sqrt{5}}{2}$$

e ottengo la formula chiusa

$$a_n^0 = c_1 x_1^n + c_2 x_2^n$$

Considero la parte non omogenea $f(n) = 3n + 1$ polinomio in n di grado 1 quindi

$$b_n = c + dn$$

con c, d costanti di determinare. Sostituisco b_n dentro a_n

$$c + dn = c + d(n-1) + c + d(n-2) + 3n + 1 \quad \forall\, n \geq 2$$

$$n(-d-3) + (3d - c - 1) = 0$$

quindi

$$\begin{cases} -d - 3 = 0 \\ 3d - c - 1 = 0 \end{cases}$$

quindi

$$d = -3 \qquad c = -10$$

allora la soluzione particolare è

$$b_n = -3n - 10$$

unisco le due soluzioni e ottengo

$$a_n = a_n^0 + b_n = c_1 x_1^n + c_2 x_2^n - 3n - 10$$

impongo le condizioni iniziali

$$\begin{cases} c_1 + c_2 + 10 = 0 \\ c_1(\frac{1+\sqrt{5}}{2}) + c_2(\frac{1-\sqrt{5}}{2}) - 10 - 3 = 3 \end{cases}$$

e ottengo

$$c_1 = 6 + 2\sqrt{5} \qquad c_2 = 6 - 2\sqrt{5}$$

sostituisco in a_n e ottengo la formula chiusa

$$a_n = (6 + 2\sqrt{5})(\frac{1+\sqrt{5}}{2})^n + (6 - 2\sqrt{5})(\frac{1-\sqrt{5}}{2})^n$$

1.4 Relazioni

Ricordiamo la definizione di relazione su un insieme A. R si dice relazione su un insieme A se $R \subseteq A \times A$. Quindi se $(a_1, a_2) \in \mathbb{R}$ scrivo $a_1 R a_2$

Definizione 17 (Relazione d'ordine parziale)**.** *Sia R relazione su A, R si dice relazione d'ordine parziale se verifica le seguenti proprietà:*

1. *Riflessiva: $\forall\, a \in A \Rightarrow aRa$, ossia (a, a)*
2. *Antisimmetrica: $\forall\, a, b \in A$ se $aRb \wedge bRa \Rightarrow a = b$*
3. *Transitiva: $\forall\, a, b, c \in A$ se $aRb \wedge bRc \Rightarrow aRc$, ossia se $(a, b) \in R$ e $(b, c) \in R \Rightarrow (a, c) \in R$*

Definizione 18 (Relazione d'ordine totale)**.** *Sia R relazione d'ordine su A, R si dice relazione d'ordine totale se $\forall\, a, b \in A$ vale aRb oppure bRa.*

Definizione 19 (Insieme parzialmente ordinato)**.** *Sia A un insieme su cui è definita una relazione d'ordine R, allora la coppia (A, R) si dice insieme parzialmente ordinato. Se la relazione vale per ogni $a, b, c \in A$ allora si dice insieme totalmente ordinato.*

Intuitivamente, in un insieme parzialmente ordinato non si richiede che tutte le coppie di elementi di A siano tra di loro confrontabili,mentre in un insieme totalmente ordinato tutte le coppie sono confrontabili.
Esempi:

1. $(\mathbb{Z}, \leq)$ è un insieme totalmente ordinato.
2. X insieme su cui è definita la relazione d'inclusione $\subseteq$, $(P(X), \subseteq)$ è parzialmente ordinato.
3. Considero $\mathbb{N}$ su cui definisco la relazione di divisibilità $|$ per $a, b \in \mathbb{N}$. Si dice che a divide b e scrivo $a|b$ se $\exists\, c \in \mathbb{N}$ tale che $b = ac$.
   Verifico le tre proprietà:
   (a) $\forall\, a \in \mathbb{N}$ $a|a$ perché $a = a \cdot 1$
   (b) $\forall\, a, b \in \mathbb{N}$, se $a|b$ e $b|a \Rightarrow a = b$.
   Dimostrazione. Per ipotesi $a|b$ quindi $\exists\, c \in \mathbb{N}$ tale che $b = a \cdot c$. Analogamente $\exists\, d \in \mathbb{N}$ tale che $a = b \cdot d$. Quindi $b = a \cdot c = b \cdot d \cdot c \Rightarrow b - b \cdot d \cdot c = 0 \Rightarrow b(1 - dc) = 0$. Ora abbiamo due possibilità:
      i. Se $b = 0$ allora $a = b \cdot d = 0$ cioè $a = b = 0$.
      ii. Se $dc = 1$ poiché $c, d \in \mathbb{N}$ allora $c = d = 1$ quindi $a = b$
   (c) $\forall\, a, b \in \mathbb{N}$ se $a|b$ e $b|c$ allora $a|c$.
   Dimostrazione. Analogamente a quanto fatto prima $\exists\, a_1, b_1 \in \mathbb{N}$ tale che $b = a \cdot a_1$ e $c = b \cdot b_1$.
   Allora $c = b \cdot b_1 = (a \cdot a_1)b_1 = a(a_1 \cdot b_1) = a$ ma $a_1, b_1 \in \mathbb{N}$ quindi $a_1 * b_1 \in \mathbb{N}$ ossia $a|c$.
   Quindi $(\mathbb{N}, |)$ è parzialmente ordinato.

Osservazione 3. $(\mathbb{Z}, |)$ *non è parzialmente ordinato perché non vale la proprietà antisimmetrica. Infatti $2| - 2$ e $-2|2$ ma $2 \neq -2$.*

Insiemi finiti parzialmente ordinati sono rappresentabili attraverso i **Diagrammi di Hasse**.

Definizione 20. *Sia $(A, \trianglelefteq)$ insieme parzialmente ordinato con $\trianglelefteq$ relazione d'ordine generica. Dati $a, b \in A$, allora:*

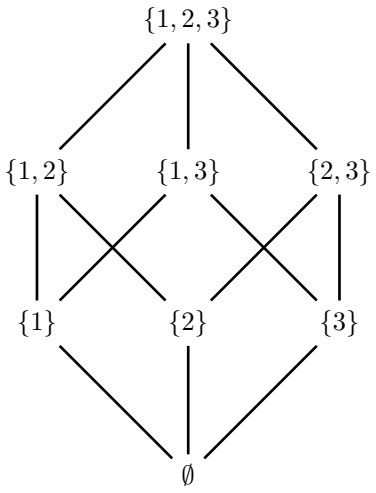
1. *Se $a \trianglelefteq b$ si dice che b sta sopra a*
2. *Se $c \in A$ tale che $a \trianglelefteq c$ e $c \trianglelefteq b$ allora $c = a$ oppure $a = b$. Questo significa che non esistono elementi intermedi tra a e b.*

Per costruire un diagramma di Hasse utilizzo la seguente logica, dato A insieme parzialmente ordinato:

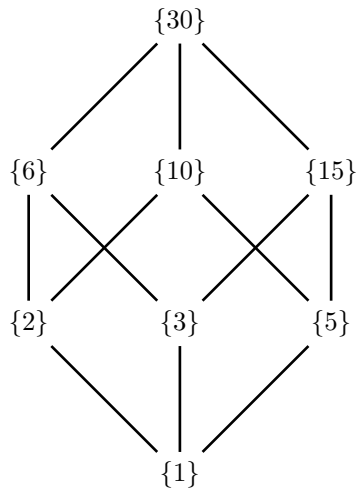
- Rappresento gli elementi di A come vertici.
- Connetto $a, b \in A$ con una linea se b copre a.

Esempi:

1. Sia $X = \{1, 2, 3\}$ con relazione d'inclusione $\subseteq$. $(X, \subseteq)$.



2. $A = \{\text{divisori naturali di } 30\} = \{1, 2, 3, 5, 6, 10, 15, 30\}$. Considero $(A, |)$.



Definizione 21 (Isomorfismo)**.** *Siano $(A_1, \trianglelefteq_1)$ e $(A_2, \trianglelefteq_2)$ insiemi parzialmente ordinati, una funzione $f : A_1 \to A_2$ si dice isomorfismo di insiemi parzialmente ordinati se:*

1. *f è biettiva rispetto alla relazione*
2. *$\forall\, a, b \in A_1$ si ha che $a \trianglelefteq_1 b \iff f(a) \trianglelefteq_2 f(b)$*

Definizione 22 (Massimo/minimo)**.** *Sia A insieme su cui è definita la relazione d'ordine $\trianglelefteq$ e sia $a \in A$. Allora:*

1. *a si dice massimo di A rispetto $a \trianglelefteq$ se $\forall\, b \in A \Rightarrow b \trianglelefteq a$.*
2. *a si dice minimo di A rispetto $a \trianglelefteq$ se $\forall\, b \in A \Rightarrow a \trianglelefteq b$.*
3. *a si dice elemento massimale di A se $\forall\, b \in A$ tale che $a \trianglelefteq b$ vale $b = a$. Ossia a massimale se non c'è alcun elemento che lo copre a parte sé stesso.*
4. *a si dice elemento minimale di A se $\forall\, b \in A$ tale che $a \trianglelefteq a$ vale $b = a$. Ossia a minimale se non c'è alcun elemento che gli stanno sotto a parte sé stesso.*

Proposizione 3. *Se esiste $max(A) = a$ allora a è l'unico elemento massimale di A. Analogamente per il minimo se esiste $max(A) = b$ allora b è l'unico elemento minimale di A.*

Dimostrazione. Guardiamo il caso in cui $a = max(A)$. Si fa in due passi:

1. Se $b \in A$ tale che $a \trianglelefteq b$, poiché $a = max(A) \Rightarrow b \trianglelefteq a$. Quindi $b = a$.
2. Se a' elemento massimale di A, poiché $a = max(A) \Rightarrow a' \trianglelefteq a$. Quindi $a' = a$ per definizione di massimale. □

Definizione 23 (Maggiorante)**.** *Sia $B \subseteq A$, si dice che $a \in A$ è un maggiorante di B in A se $b \trianglelefteq a$ $\forall\, b \in B$.*

Definizione 24 (Minorante)**.** *Sia $B \subseteq A$, si dice che $c \in A$ è un minorante di B in A se $c \trianglelefteq a$ $\forall\, b \in B$.*

Definizione 25 (Estremo superiore)**.** *Sia $B \subseteq A$ tale che A insieme parzialmente ordinato. L'estremo superiore di B in A, $sup_A(B)$, è, se esiste, il minimo dell'insieme dei maggioranti di A*

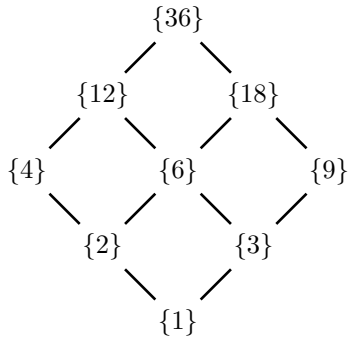
$$M_A(B) = \{a \in A | a \text{ un maggiorante di } B \text{ in } A\}$$

ordinato con la relazione d'ordine indotta.

Definizione 26 (Estremo inferiore)**.** *L'estremo inferiore di B in A, $inf_A(B)$ è, se esiste, il massimo dei minoranti di A, $m_A(B)$.*

Osservazione 4. *Se esiste $\overline{b} = max(B)$ allora $\overline{b} = sup_A(B)$. Analogamente se esiste $b_0 = min(B) \Rightarrow b = inf_A(B)$.*

Esempio:
Sia $A = \{a \in \mathbb{N} | a \text{ divide } 36\} = \{1, 2, 3, 4, 6, 9, 12, 18, 36\}$. Considero l'insieme $B = \{3, 4\}$ e cerco $sup_A(B)$, $inf_A(B)$.



Si può osservare che l'insieme dei maggioranti di B ossia $M_A(B) = \{12, 36\}$, composto da multipli di 3 e 4, ha $min(M_A(B)) = 12$ rispetto alla relazione di divisibilità. Quindi $sup_A(B) = 12 = mcm(3, 4)$.
Analogamente per quanto riguarda l'estremo inferiore si considerano i divisori di 3 e 4, $m_A(B) = \{1\}$, e quindi $inf_A(B) = 1 = MCD(3, 4)$.
Per $B_1 = \{9, 6\}$ si ha $sup_A(B_1) = 18$ e $inf_A(B_1) = 3$.
Per $B_1 = \{4, 6, 9\}$ si ha $sup_A(B_2) = 36$ e $inf_A(B_2) = 1$.

Definizione 27 (Reticolo)**.** *Un insieme parzialmente ordinato $(A, \trianglelefteq)$ si dice reticolo se $\forall\, a, b \in A$:*

- $\exists\ inf_A(\{a, b\})$
- $\exists\ sup_A(\{a, b\})$

Notazione.

- $a \wedge b$ si definisce intersezione reticolare e indica l'inf.
- $a \vee b$ si definisce unione reticolare e indica il sup.

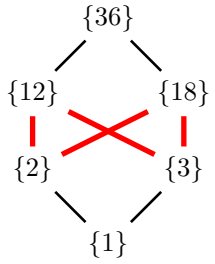
Proprietà algebriche reticoli:
Sia $(A, \trianglelefteq)$ reticolo. Allora:

1. Idempotenza: $\forall\, a \in A\ a \wedge a = a$ e $a \vee a = a$

2. Commutativa: $\forall\, a, b \in A\ a \wedge b = b \wedge a$ e $a \vee b = b \vee a$
3. Associativa: $\forall\, a, b, c \in A\ (a \wedge b) \wedge c = a \wedge (b \wedge c)$ e $(a \vee b) \vee c = a \vee (b \vee c)$
4. Assorbimento: $\forall\, a, b \in A\ (a \wedge b) \vee a = a$ e $(a \vee b) \wedge a = a$
5. $\forall\, a, b \in A\ a \wedge b = a \iff a \trianglelefteq b \iff a \vee b = b$

Esempi.

1. Sia $D_n = \{\text{divisori su } \mathbb{N} \text{ di } n\}$ ordinato con relazione di divisibilità. Allora $(D_n, |)$ è un reticolo, infatti $\forall\, a, b \in D_n$:
   (a) $a \wedge b = mcm(a, b)$
   (b) $a \vee b = MCD(a, b)$
2. Sia $X \neq \emptyset$ insieme, allora $(P(X), \subseteq)$ è un reticolo. E vale che $\forall\, Y, Z \subseteq X$:
   (a) $Y \wedge Z = Y \cap Z$
   (b) $Y \vee Z = Y \cup Z$
3. Sia $A_1 = \{1, 2, 3, 12, 18, 36\}$ ordinato per divisibilità. Questo non è un reticolo, infatti se considero l'insieme $B = \{2, 3\} \subseteq A_1$ si osserva che $\nexists\, sup_A(B)$.



   Si vede graficamente che i vertici $\{2\}$ e $\{3\}$ sono entrambi connessi sia al $\{12\}$ che al $\{18\}$ cioè hanno due maggioranti quindi non esiste il minimo tra i maggioranti.
   Con la stessa logica si può osservare che $\nexists\, inf_A\{12, 18\}$)

Definizione 28 (Sottoreticolo)**.** *Sia A un reticolo e sia $B \subseteq A$, B si dice un sottoreticolo di A se $\forall\, b, c \in B$ si ha :*

1. $b \wedge_A c \in B$
2. $b \vee_A c \in B$

Esempio. Sia $A = \{1, 2, 3, 4, 6, 12, 18, 36\}$ quindi $(A, |)$ reticolo. Allora:

- $B_1 = \{1, 2, 3, 4, 6, 12\} \subseteq A$ è un sottoreticolo di A
- $B_2 = \{1, 2, 3, 12, 18, 36\}$ non è un sottoreticolo di A. Infatti $2 \vee_A 3 = 6 \notin B_2$ e $12 \vee_A 18 = 6 \notin B_2$
- $B_3 = \{1, 4, 6, 36\}$ non è un sottoreticolo di A. Infatti $4 \wedge_A 6 = 2 \notin B_3$ e $4 \vee_A 6 = 12 \notin B_3$

Operazioni reticolari su insiemi notevoli:

$(S, \leq)$	$P(S), \subseteq$	$(\mathbb{N}, \mid)$
$x \wedge y = min\{x, y\}$	$x \wedge y = x \cap y$	$x \wedge y = MCD(x, y)$
$x \vee y = max\{x, y\}$	$x \vee y = x \cup y$	$x \vee y = mcm(x, y)$

Definizione 29 (Relazione di equivalenza)**.** *Sia A insieme e R relazione su A. Allora R relazione di equivalenza su A se verifica le seguenti proprietà:*

1. *Riflessiva:* $\forall\, a \in A$, aRa
2. *Simmetrica:* $\forall\, a, b \in A \quad aRb \Longrightarrow bRa$
3. *Transitiva:* $\forall\, a, b, c \in A \quad aRb \wedge bRc \Longrightarrow aRc$

Esempio. Sia $A = \{X \subseteq \mathbb{N} \mid |X| < \infty\}$ definisco la relazione $X \sim Y$ se $|X| = |Y|$.Allora:

1. $\sim$ è riflessiva: $\forall\, X \in A\ |X| = |X|$
2. $\sim$ è simmetrica: $\forall\, X, Y \in A\ |X| = |Y| \Longrightarrow |Y| = |X|$
3. $\sim$ è transitiva: $\forall\, X, Y, Z \in A$ se $|X| = |Y| \wedge |Y| = |Z| \Longrightarrow |X| = |Z|$

Definizione 30 (Classe di equivalenza)**.** *Data $\sim$ relazione di equivalenza su A insieme. Per $a \in A$ definisco la classe di equivalenza di a rispetto a $\sim$ come $[a]_\sim = \{x \in A | x \sim a\}$. In questo caso l'elemento a si definisce rappresentante della classe.*

Osservazione 5. *Valgono le seguenti:*

- $[a]_\sim \subseteq A$
- $a \in [a]_\sim$

Esempi:

1. $=$ relazione di uguaglianza su A per $a \in A$, $[a]_\sim = \{a\}$
2. $\sim$ su $\mathbb{Q}$ tale che $q \sim r$ se $|q| = |r|$ per $q \in \mathbb{Q}$, $[q]_\sim = \{-q, q\}$

Proposizione 4. *Sia $\sim$ una relazione di equivalenza definita su un insieme A. Allora per $x, y \in A$:*

$$[x]_\sim = [y]_\sim \Longleftrightarrow x \sim y$$

Dimostrazione.

$\Longrightarrow$ Supponiamo per ipotesi che $[x]_\sim = [y]_\sim$. Allora $x \in [x]_\sim = [y]_\sim$ quindi $x \in [y]_\sim \Longrightarrow x \sim y$.

$\Longleftarrow$ Supponiamo per ipotesi che $x \sim y$ e voglio dimostrare che $[x]_\sim = [y]_\sim$ attraverso una doppia inclusione:

- $\subseteq$ Sia $z \in [y]_\sim$ allora $y \sim z$ ma $x \sim y$ e $y \sim z$ quindi per la proprietà transitiva, $x \sim z \Longrightarrow z \in [x]_\sim \Longrightarrow [y]_\sim \subseteq [x]_\sim$.
- $\supseteq$ Sia $w \in [x]_\sim$ allora $x \sim w$ e per la proprietà simmetrica si ha che $w \sim x$ ma $x \sim y$ quindi $w \sim y$. Ora, per ipotesi $x \sim y$ quindi $w \sim y$ ovvero $w \in [y]_\sim \Longrightarrow [x]_\sim \subseteq [y]_\sim$.

Per la doppia inclusività segue che le due classi sono uguali $[x]_\sim = [y]_\sim$. □

Definizione 31 (Insieme quoziente)**.** *Si definisce insieme quoziente di un insieme A rispetto alla relazione $\sim$ come l'insieme di tutte le classi di equivalenza di A, ossia:*

$$\frac{A}{\sim} = \{[a]_\sim | a \in A\}$$

Definizione 32 (Sistema di rappresentanti)**.** *Sia $\sim$ relazione di equivalenza su A insieme. Un sottoinsieme $\{a_i\}_{i\in I}$ di A si dice sistema di rappresentanti se per ogni possibile classe di equivalenza ho scelto uno e un solo elemento.*

Definizione 33. *Sia A un insieme e $F \subseteq P(A)$. F si dice partizione di A se e solo se:*

1. $\forall\, X \in F,\ X \neq \emptyset$
2. $\forall\, X, Y \in F$ *con* $Z \neq Y$ *vale* $X \cap Y = \emptyset$
3. $\underset{X\in F}{U} = A$

Teorema 1. *Sia A insieme e $\sim$ relazione di equivalenza su A. Allora $\frac{A}{\sim}$ è una partizione dell'insieme A.*

Dimostrazione. Dimostro le tre proprietà che definiscono la partizione di un insieme.

1. Siano $\frac{A}{\sim} = \{[a]_\sim | a \in A\}$ e $[x]_\sim \subseteq A$ allora $[a]_\sim \neq \emptyset\ \forall\, x \in A$ perché $x \in [x]_\sim$.
2. Siano $[x]_\sim, [y]_\sim \in \frac{A}{\sim}$ con $[x]_\sim \neq [y]_\sim$, provo che $[x]_\sim \cap [y]_\sim = \emptyset$.
   Suppongo per assurdo che $[x]_\sim \cap [y]_\sim \neq \emptyset$ e sia $z \in [x]_\sim \cap [y]_\sim$. Allora:
   (a) $z \in [x]_\sim$ quindi $z \sim x$, ovvero $x \sim z$ per simmetria.
   (b) $z \in [y]_\sim$ quindi $z \sim y$.
   (c) $x \sim z, z \sim y \Longrightarrow x \sim y$

   Segue che $[x]_\sim = [y]_\sim$ ma questo è assurdo poiché per ipotesi ho scelto $[x]_\sim \neq [y]_\sim$.
3. Devo dimostrare che $\underset{x\in A}{U}[x] = A$, uso la doppia inclusione:

   ($\subseteq$) $\forall\, x \in A,\ [x] \subseteq A \Longrightarrow \underset{x\in A}{U}[x] \subseteq A$

   ($\supseteq$) $\forall\, x \in A,\ x \in [x] \subseteq \underset{x\in A}{U}[x] \Longrightarrow x \in \underset{x\in A}{U}[x] \Longrightarrow A \subseteq \underset{x\in A}{U}[x]$ □

Esempio. Siano:

- $A = \{x, y, z, y\}$
- $F \subseteq P(A) = \{\{x\} m \{y\}, \{z, y\}\}$
- $\sim_F = \{(x,x), (y,y), (z,z), (t,t), (z,t), (t,z)\}$

Quindi

$$\frac{A}{\sim_F} = \{[x], [y], [z], [t]\} = \{\{x\}, \{y\}, \{z, t\}\} = F$$

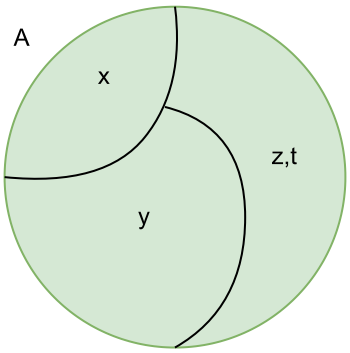


Figure 3: Partizione di A

Osservazione 6. *Siano A insieme, $\epsilon = \{$relazioni di equivalenza su $A\}$ e $P = \{$partizioni di $A\}$. Siano $f\colon \epsilon \to P$ e $g\colon P \to \epsilon$. Allora:*

$$\sim \to \underset{\sim}{A} \qquad p \to \sim_p$$

$$\begin{cases} f \circ g = i_P \\ g \circ f = i_\epsilon \end{cases}$$

Quindi f e g sono biezioni.

Proposizione 5. *Sia $f : A \to B$ funzione, definisco la relazione $\sim_f$ su A, ponendo per $x, y \in A$, $x \sim_f y \iff f(x) = f(y)$. Allora $\sim_f$ relazione di equivalenza su A, equivalenza indotta da f.*

Definizione 34 (Relazione di congruenza modulo n)**.** *Sia $n \geq 2$ $n \in \mathbb{N}$, definisco per $x, y \in \mathbb{Z}$, $x \equiv y (\mathrm{mod}\, n)$, oppure $x \equiv_n y$ (leggo x è congruo a y modulo n), se e solo se $n|(x - y)$.*

Proposizione 6. *$\forall\, n \in \mathbb{N}$, $n \geq 2$, $\equiv_n$ relazione di equivalenza su $\mathbb{Z}$.*

Dimostrazione. Verifico le tre proprietà:

1. Riflessiva: $\forall\, z \in \mathbb{Z}$ $n|(z - z)$ quindi $z \equiv_n z$
2. Simmetrica: $\forall\, x, y \in \mathbb{Z}$ se $x \equiv_n y$ allora $n|(x - y)$, quindi $n|y - x$ cioè $y \equiv_n x$.
3. Transitiva: $\forall\, x, y, zi \in \mathbb{Z}$, se $x \equiv_n y$ e $y \equiv_n z$ allora $n|x - y$ e $n|y - z$ quindi $n|((x + y) + (y - z))$ ossia $n|(x - z)$ quindi $x \equiv_n z$. □

Osservazione 7. *$\equiv_n$ coincide con la relazione $\sim_f$ dove $f : \mathbb{Z} \to \mathbb{Z}$ che associa a ogni elemento $x \in \mathbb{Z}$ il resto della divisione di x per n ossia $f(x) = qn + r$ con $q, r \in \mathbb{Z}$, $0 \leq r \leq n$. Diciamo che due numeri sono congrui modulo n se e solo se hanno lo stesso resto.*

Osservazione 8. *$\{0, 1, 2, 3, \ldots, n - 1$ è un sistema di rappresentanti per $\equiv_n$.*

2 Calcolo combinatorio

L'obiettivo del calcolo combinatorio è quello di contare la cardinalità di insiemi finiti.

Regola della somma. *Se un evento può accadere in n_1 modi e un secondo evento in n_2 modi, diversi dai precedenti, allora ci sono $n_1 + n_2$ modi in cui uno dei due eventi può succedere.*
Esempio. Supponiamo A_1, A_2 insiemi degli eventi tale che $|A_1| = n_1$, $|A_2| = n_2$ e $A_1 \cap A_2 = \emptyset$, allora $|A_1 \cup A_2| = n_1 + n_2$. Se $A_1 \cap A_2 \neq \emptyset$ allora $|A_1 \cup A_2| = n_1 + n_2 - |A_1 \cap A_2$.
In generale se $A_1, A_2, \ldots, A_s$ s insiemi con $|A_i| = n_i \quad \forall\, i = 1, 2, \ldots, s$ e sono a due a due disgiunti, allora $|A_1 \cup A_2 \cup, \ldots, \cup A_S| = \sum_{i=1}^{s} n_i$

Regola della prodotto. *Se un evento può accadere in n_1 modi e un secondo evento, indipendente dal primo, può accadere in n_2 modi allora ci sono $n_1 \cdot n_2$ modi in cui entrambi gli eventi possono accadere.*
Esempi:

1. Ho 3 paia di pantaloni e 4 paia di camicie. Quanti sono i possibili abbigliamenti? Chiamo $A_1 = \{pantaloni\}$ e $A_2 = \{camicie\}$

   $$n_1 = 3 \quad n_2 = 4 \quad n_1 \cdot n_2 = 12$$

   In generale se $A_1, A_2, \ldots, A_s$ s insiemi con $|A_i| = n_i \quad \forall\, i = 1, 2, \ldots, s$ allora $|A_1 \times A_2 \times \cdots \times A_s| = \prod_{i=1}^{s} |A_i|$. Ricorda che $A_1 \times A_2 \times \cdots \times A_s = \{(a_1, a_2, \ldots, a_s) | a_i \in A_i \forall\, i = 1, 2, \ldots, s\}$.

2. Siano A, B insieme con $|A| = n$, $|B| = m|$ con $n, m \in \mathbb{N}$. Determinare il numero delle funzioni $f : A \to B$. Ora, siano $A = \{a_1, a_2, \ldots, a_m\}$, $B = \{b_1, b_2, \ldots, b_m\}$ e $F = \{funzioni\, di\, A\, in\, B\}$.

   - Per $f(a_1)$ ci sono m scelte, ovvero ognuno dei b_j con $j = 1, 2, \ldots, m$
   - Per $f(a_2)$ ci sono m scelte, ovvero ognuno dei b_j con $j = 1, 2, \ldots, m$
   - $\vdots$
   - Per $f(a_n)$ ci sono m scelte, ovvero ognuno dei b_j con $j = 1, 2, \ldots, m$

   Per la regola del prodotto $|F| = \underbrace{m \cdot m \cdot \cdots \cdot m}_{n\ volte} = m^n = |B|^{|A|}$

3. Determinare il numero di funzioni <u>iniettive</u> da A in B. Chiamo $I = \{f \in F | f\, é\, iniettiva\}$. Poiché f è iniettiva, allora:

   - Per $f(a_1)$ ci sono m scelte possibili, tutti gli elementi di B.
   - Per $f(a_2)$ ci sono $m - 1$ scelte in $B \setminus \{f(a_1)\}$
   - $\vdots$
   - Per $f(a_n)$ ci sono $m - (n - 1)$ scelte in $B \setminus \{f(a_1), \ldots, f(a_{n-1}\}$

   Per la regola del prodotto $|I| = m(m-1)(m-2)\ldots(m-n+1) = D(m, n)$, disposizioni semplici.

Osservazione 1. *Se $n = 1 \Longleftarrow D(m, 1) = m$. Se $n = m \Longleftarrow D(m, m) = m!$*

Definizione 1 (Permutazione)**.** *Ogni funzioni biunivoca $f : A \to A$ si chiama permutazione. intuitivamente si dice permutazione su A un qualsiasi ordinamento degli elementi di A.*

$$P_n = n!$$

Esercizio. Determinare il numero di anagrammi delle seguenti parole:

- SOLE $\longrightarrow \#anagrammi = 4! = 24$
- CASA $\longrightarrow \#anagrammi = \frac{4!}{2!} = 12$
- COLTELLO $\longrightarrow \#anagrammi = \frac{8!}{2!\cdot 3!} = 3360$

2.1 Disposizioni e combinazioni semplici

Problema: Dato un insieme di n elementi, in quanti modi si possono scegliere k elementi senza ripetizione fra questi n? Analizziamo i diversi casi:

1. Caso in cui l'ordine della k-upla è importante: $D(n,k) = \frac{n!}{(n-k)!} \to$ numero di disposizioni semplici di classe k.
2. Non è importante l'ordine della k-upla:$C(n,k)\frac{n!}{k!(n-k)!} = \binom{n}{k} \to$ numero di combinazioni semplici di n elementi di classe k.

Esempi:

1. In quanti modi si possono assegnare le medaglie a 50 atleti? $n = 50$, $k = 3 \to D(50,3) = \frac{50!}{47!} = 50 \cdot 49 \cdot 48$
2. Quanti sono i possibili podi, senza ordine, di 50 atleti? $C(50,3) = \frac{50\cdot 49\cdot 48\cdot \cancel{47}!}{3!\cdot \cancel{47}}$

Definizione 2 (Disposizione semplice)**.** *Si dice disposizione semplice di n oggetti di classe k, con $k \leq n$, un qualsiasi ordinamento di k elementi mutuamente distinti in A.*

$$D(n,k) = \frac{n!}{(n-k)!}$$

Definizione 3. *Si dice combinazione di n oggetti di classe k, con $k \leq n$, un sottoinsieme di cardinalità k di un insieme di cardinalità n.*

$$C(n,k) = \frac{n!}{k!(n-k)!}$$

2.2 Disposizioni e combinazioni con ripetizione

Problema: In quanti modi si possono scegliere k elementi, anche coincidenti, fra gli elementi di un insieme di n elementi? Anche in questo caso distinguiamo due casi:

1. Se è importante l'ordine $D^r(n,k)$ Disposizioni con ripetizione
2. Altrimenti $C^r(n,k)$ combinazioni con ripetizione

Definizione 4 (Disposizione con ripetizione)**.** *Si dice disposizione con ripetizione di n oggetti di classe k un qualsiasi ordinamento di k elementi, non necessariamente distinti, di A. k può essere minore uguale o maggiore di n.*

$$D^r(n,k) = n^k$$

Definizione 5. *Si dice combinazione con ripetizione di n oggetti di classe k un raggruppamento non ordinato (detto multinsieme di k elementi di A, eventualmente anche ripetuti.*

$$C^n(n,k) = \binom{k+n-1}{k} = \frac{(n+k-1)!}{(n-1)!k!}$$

Teorema 1. *Se A è un insieme finito $|A| = n$ allora $|P(A)| = 2^n$.*

Dimostrazione. Poniamo $Y = \{\text{funzioni da A in } \{0,1\}\}$ e sappiamo che

$$|Y| = |\{0,1\}|^{|A|} = 2^n$$

Definisco

$$\mathcal{X} : P(A) \to Y$$

e prendo per ogni $B \in P(A)$, ossia $B \subseteq A$ quindi $\mathcal{X}(B)$ funzione caratteristica di B, cioè la funzione definita da

$$(\mathcal{X}(B))(a) = \begin{cases} 0 \text{ se } a \notin B \\ 1 \text{ se } a \in B \end{cases}$$

Quindi $\mathcal{X}(B) : A \to \{0,1\}$ cioè $\mathcal{X}(B) \in Y$. Dimostro che $\mathcal{X}$ è biettiva:

1. Iniettività. Siano $B_1, B_2 \in P(A)$ con $B_1 \neq B_2$ allora posso supporre che $b \in B_1 \setminus B_2$ altrimenti esiste $b \in B_2 \setminus B_1$. Allora nel primo caso

   $$\mathcal{X}(B_1)(b) = 1$$

   $$\mathcal{X}(B_2)(b) = 0$$

2. Suriettività. Voglio dimostrare che per ogni $f \in Y$ trovo $B \in P(A)$ tale che $f = \mathcal{X}(B)$. Sia $f \in Y$ allora $f : A \to \{0,1\}$. Considero $\{a \in A | f(a) = 1\} = B$ allora $B \subseteq A$ cioè $B \in P(A)$ e vale che per ogni $x \in A$

   $$\mathcal{X}(B)(x) = 1 \iff x \in B \iff f(x) = 1$$

   Ciò prova che $\forall\, a \in A$ vale $\mathcal{X}(B)(a) = f(a)$ ovvero

   $$\mathcal{X}(B) = f$$

   cioè $\mathcal{X}$ è suriettiva.

Quindi $\mathcal{X}$ è una biezione e allora

$$|P(A)| = 2^n$$

□

2.3 Coefficiente binomiale

$$\binom{n}{k} = \frac{n!}{k|(n-k)!}$$

$\binom{n}{k}$ è il numero dei sottoinsiemi di k elementi di un insieme di cardinalità n.
Esempio. $X = \{a, b, c, d\}$ $|X| = 40$

- # di sottoinsiemi di cardinalità 2 di $X = \binom{4}{2} = \frac{4!}{2!2!} = 6$.
  Questi sono $\{a, b\}, \{a, c\}, \{a, d\}, \{b, c\}, \{b, d\}, \{c, d\}$
- # di sottoinsiemi di cardinalità 3 di $X = \binom{4}{3} = \frac{4!}{3!1!} = 4$.
- # di sottoinsiemi di cardinalità 4 di $X = \binom{4}{4} = \frac{4!}{4!0!} = 1$.
- # di sottoinsiemi di cardinalità 1 di $X = \binom{4}{1} = \frac{4!}{1!3!} = 4$.
- # di sottoinsiemi di cardinalità 0 di $X = \binom{4}{0} = \frac{4!}{0!4!} = 1$. Ovvero $\emptyset$.

Quindi sia X insieme tale che $|X| = n$, allora:

$$\sum_{k=0}^{n} = |P(X)|$$

Proprietà dei coefficienti binomiali
Sia k tale che $0 \leq k < n$. Allora:

1. $\binom{n}{0} = 1$. Attenzione $0! = 1$
2. $\binom{n}{1} = n$
3. $\binom{n}{n} = 1$
4. $\binom{n}{k} = \binom{n}{n-k} = \frac{n!}{(n-k)!(n-n+k)!} = \frac{n!}{(n-k)!k!}$

Formula del binomio di Newton. Se $n \in \mathbb{N}$ allora:

$$(x+y)^n = \sum_{K=0}^{n} \binom{n}{k} x^k y^{n-k}$$

Per esempio $(x+y)^5 = x^5 + 5x^4y + 10x^3y^2 + 10x^2y^3 + 5xy^4 + y^5$. Si ritrovano i valori dell'n-esimo livello del Triangolo di Tartaglia come coefficienti dei vari termini.

$n=0$						1					
$n=1$					1		1				
$n=2$				1		2		1			
$n=3$			1		3		3		1		
$n=4$		1		4		6		4		1	
$n=5$	1		5		10		10		5		1
$n=6$	1	6		15		20		15		6	1

Teorema 2. *Sia X un insieme $|X| = n$ allora $|P(X)| = 2^n$*

Dimostrazione. Per ogni $0 \leq k \leq n$ chiamo $P_k(X) = \{Y | Y \subseteq X \wedge |Y| = k\}$. Allora $P(X) = \bigcup_{k=0}^{n} A_k$.

$$|P(X)| = |\bigcup_{k=0}^{n} P_k(X)| = \sum_{k=0}^{n} \binom{n}{k} = \sum_{k=0}^{n} \binom{n}{k} 1^k 1^{n-k} = (1+1)^n = 2^n$$

□

Principio di inclusione ed esclusione P.I.E

$$|A \cup B| = |A| + |B| - |A \cap B|$$

In generale

$$|A_1 \cup A_2 \cup \cdots \cup A_n| = \sum_{i=1}^{n} |A_i| - \sum_{1 \leq i < j < n} |A_i \cap A_j| + \sum_{1 \leq < i < j < k < n} |A_i \cap A_k \cup A_k| - \cdots + (-1)^{n+1} |A_1 \cup A_2 \cup \cdots \cup A_n|$$

$$|A_1 \cup A_2 \cup \cdots \cup A_n| = \sum_{\emptyset \neq I \subseteq \{1,2,\ldots,k\}} (-1)^{|I|+1} |\bigcap_{i \in I} A_i|$$

Numero di funzioni suriettive di A in B
Siano A, B insiemi, $|A| = n$ $|B| = m$. Se $m \geq n$, il numero di funzioni suriettive da A in B è dato da

$$S(n,m) = \sum_{j=0}^{m} (-1)^j \binom{m}{k} (m-j)^n$$

Dimostrazione. Procediamo per passi:

1. Per ogni $b \in B$ chiamo F_b l'insieme di tutte le funzioni $f : A \to B$ tale che $Im(f) = f(A) \subseteq B \setminus \{b\}$, ovvero $\forall\, a \in A\, f(a) \neq b$

$$\{\textit{funzioni suriettive}\} = \{f | f : A \to B\} \setminus \bigcup_{b \in B} F_b$$

2. Poiché ogni elemento di F_b non è una funzione suriettiva e viceversa se $g : A \to B$ non è suriettiva, esiste un certo $c \in B$ tale che $g(a) \neq c \,\forall\, a$ cioè $g \in F_c$.

3. Allora il numero di funzioni suriettive è la cardinalità della differenza

$$S(n,m) = |\{f | f : A \to B\}| - |\bigcup_{b \in B} F_b| = m^n - |\bigcup_{b \in B} F_b|$$

4. Uso il principio di inclusione ed esclusione per calcolare $|\bigcup_{b \in B} F_b|$.
Per ogni $J \subseteq B$ sia $F_j = \bigcap_{b \in j} F_b = \{f | f : A \to B \vee Im(f) \subseteq B \setminus J\}$ se $|J| = J$ allora $|F_j| = (m-j)^n$. Questo è il numero di funzioni da un insieme di n elementi in uno di $(m-j)$ elementi e ci sono $\binom{m}{j}$ sottoinsiemi di B di cardinalità j.

$$|\bigcup_{b \in J} F_b| = \sum_{\emptyset \neq J \subseteq B} (-1)^{|J|+1} |\bigcap_{b \in B} F_b| = \sum_{\emptyset \neq J \subseteq B} (-1)^{|J|+1} |F_j| =$$

$$\sum_{j=1}^{m=|B|} (-1)^{j+1} \binom{m}{j} (m-j)^n = m^n + \sum_{j=1}^{m} (-1)^j \binom{m}{j} (m-j)^n$$

E quindi otteniamo:

$$\sum_{j=0}^{m}(-1)^j\binom{m}{j}(m-j)^n$$

□

2.4 Cardinalità

Definizione 6 (Equipotenza)**.** *Siano A e B due insiemi. Diciamo che hanno la stessa cardinalità, oppure che sono equipotenti, se esiste una corrispondenza biunivoca tra i due insiemi, cioè esiste $f : A \to B$ che sia biettiva. In tal caso si scrive $A \sim B$.*

Osservazione 2. *$\sim$ è una relazione di equivalenza fra la classe degli insiemi. Infatti:*

1. *$\sim$ è riflessiva, $\forall\, A$ insieme prendi $f = id_A : A \to A$ quindi $id_A(a) = A \,\forall\, a \in A \Longrightarrow A \sim A$*
2. *$\sim$ è simmetrica, se vale $A \sim B$ allora esiste $f : A \to B$ biunivoca e quindi esiste $f^-1 : B \to A$ biunivoca $\Longrightarrow B \sim A$.*
3. *$\sim$ è transitiva, se $A \sim B$ e $B \sim C$, allora esistono $f : A \to B$ e $g = B \to C$ biunivoche. Quindi $g \circ f : A \to C$ biunivoca $\Longrightarrow A \sim C$.*

Definizione 7 (Cardinalità)**.** *Si chiama cardinalità di un insieme A la classe di equivalenza rispetto $a \sim a$ cui A appartiene. Si scrive $|A|$ o $Card(A)$.*

Definizione 8. *Un insieme A è finito se $\exists n \in \mathbb{N}$ tale che $A \sim I_n = \{1, 2, 3, 4, \ldots, n\}$, $I_0 = \emptyset$. Altrimenti A si dice infinito.*

Osservazione 3. *Per gli insiemi finiti $|A|$=numero di elementi di A. Ovviamente se $n \neq m$ allora $I_n \not\sim I_m$. Quindi A è finito se e solo se non può essere messo in corrispondenza biunivoca con un suo sottoinsieme proprio. Ciò non vale se A è infinito.*

Definizione 9 (Insieme numerabile)**.** *Ogni insieme equipotente ad $\mathbb{N}$ si dice numerabile. $|\mathbb{N}| = \aleph_0$, si legge Aleph zero.*

Teorema 3. *Ogni unione numerabile o finita di insiemi numerabili è numerabile.*

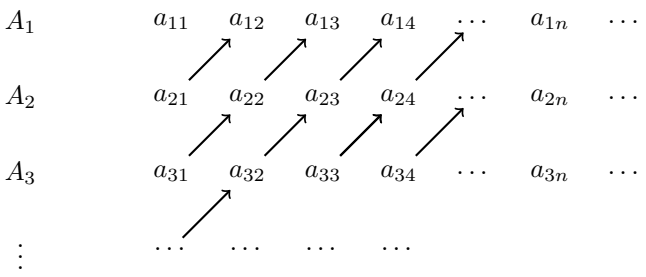
Dimostrazione. Analizziamo il caso più generale di unione numerabile di insiemi numerabili $A_1, A_2, \ldots, A_n, \ldots$, cioè $A_n \sim \mathbb{N}$, tale che siano a due a due disgiunti. Considero l'unione:

$$X = A_1 \cup A_2 \cup \cdots \cup A_n \cdots = \bigcup_{j \in \mathbb{N}} A_j$$

Per ipotesi ogni insieme A_j è numerabile, ossia $A_j \sim \mathbb{N}$ e quindi posso scrivere

$$A_j = \{a_{j_1}, a_{j_2}, a_{j_3}, \ldots, a_{j_n}, \ldots\} \quad \forall\, j \in \mathbb{N}$$

Adesso dobbiamo mettere in corrispondenza biunivoca l'insieme X con l'insieme $\mathbb{N}$. Procediamo con il procedimento diagonale di Cantor:



L'idea è quella di disporre gli insiemi considerati in una matrice infinita e trovare un modo di contare i suoi elementi. Osserviamo che non è possibile contare gli elementi in orizzontale o verticale poiché sia righe che colonne sono infinite, quindi procediamo a contare in diagonale e notiamo che in questo modo è possibile perché le diagonali sono finite. Ora, considero la diagonale j-esima, cioè

$$D_j = \{(a_{j,1}, a_{j-1,2}, a_{j-2,3} \dots\} = \{a_{h,k} \in X | h + k = j + 1\}$$

Ogni elemento $a_{h,k} \in X$ appartiene a una e una sola diagonale, precisamente a D_{h+k-1} quindi posso definire una corrispondenza biunivoca tra X e $\mathbb{N}$:

$$f : X = \bigcup_{j \in \mathbb{N}} A_j \to \mathbb{N}$$

$$f(a_{h,k}) = (\sum_{j=1}^{h+k-2} j) + k$$

quindi gli elementi di X vengono numerati:

$$a_{11} \to 1 \quad a_{21} \to 2 \quad a_{12} \to 3$$

$$a_{31} \to 4 \quad a_{22} \to 5 \quad \dots$$

ossia X è in corrispondenza biunivoca con $\mathbb{N}$ e quindi è numerabile. □

Corollario 1. $\mathbb{Z}, \mathbb{Q}, \mathbb{N} \times \mathbb{N}$ *sono numerabili.*

Dimostrazione.

1. $\mathbb{Z} = \{0, 1, 2 \dots\} \cup \{-1, -2, -3, \dots\} = \mathbb{N} \cup B = \{-n | n \in \mathbb{N}\}$ è ovvio che $B \sim \mathbb{N} \Rightarrow$ per il teorema allora anche $\mathbb{Z}$.
2. $\mathbb{N} \times \mathbb{N} = \{(a, b) | a, b \in \mathbb{N}$, poniamo $\forall\, h \in \mathbb{N}\ A_h = \{(h, 0), (h, 1), (h, 2) \dots\} = \{(h, n) | n \in \mathbb{N}\}$. Ognuno di questi h è numerabile ($f : \mathbb{N} \to A_h$ con $n \to (h, n)$ è una biezione). Quindi $\mathbb{N} \times \mathbb{N} = \bigcup_{h \in \mathbb{N}} A_h$ è numerabile per il teorema.
3. $\mathbb{Q} = \{\frac{x}{y} | x, y \in \mathbb{Z}$ *e* $y \neq 0\}$ è numerabile.

Principio della piccionaia. *Siano A, B insiemi finiti e sia $|A| = n$ e $|B| = m$. Allora $n \leq m \iff \exists$ una funzione iniettiva $f : A \to B$. Se invece $n > m$, allora ogni funzione $f : A \to B$ non è mai iniettiva.*

Questo è anche chiamato principio del portalettere. L'intuizione è che se $n + k$ oggetti ($k \neq 0$), in questo caso piccioni, sono messi in n cassetti, allora necessariamente almeno un cassetto deve contenere più di un oggetto.

Proposizione 1. *Un insieme arbitrario A ha cardinalità inferiore ($\leq$) a quella di B insieme se esiste una funzione iniettiva da A in B.*

$$|A| \leq |B| \iff \exists\, h : A \to B \, iniettiva$$

Teorema 4. *Per ogni insieme A vale $|A| < |P(A)|$.*

Dimostrazione. Procedo in due passi:

1. Provo che $|A| \leq |P(A)|$.
   Questo significa trovare una $f : A \to P(A)$ iniettiva. Considero f definita come $f(a) = \{a\}$ $\forall\, a \in A$. La funzione associa ad ogni elemento di A l'insieme composto solo da quell'elemento. Questa funzione è banalmente iniettiva, infatti se $a \neq b$ allora $\{a\} \neq \{b\}$.

2. Provo che $|A| \neq |P(A)|$.
   Questo significa provare che non può esistere una funzione biunivoca tra i due. Per assurdo sia $g : A \to P(A)$ una biezione. Ora, considero

   $$U = \{a \in A | a \notin g(a)\}$$

   In pratica U è formato da tutti gli elementi di A che non appartengono all'insieme a cui sono associati. Quindi $U \subseteq A$ cioè $U \in P(A)$. Poiché g è una funzione biunivoca esiste un unico $c \in A$ tale che $g(c) = U$. Allora si hanno due casi:

   (a) Se $c \in U$ allora $c \in \{a \in A | a \notin g(a)\}$ e quindi $c \notin g(c)$ cioè $c \notin U$ e questo è assurdo perché avevamo supposto che $c \in U$.

   (b) Se $c \notin U$ allora non vale $c \notin g(c)$ cioè $c \in g(c)$ cioè $c \in U$ e questo è assurdo perchè avevamo supposto che $c \notin U$.

□

Corollario 2. *Se A insieme numerabile allora $|P(A)|$ ha cardinalità più che numerabile.*

$$|P(\mathbb{N})| = 2^{\mathbb{N}} \geq \aleph_0 = |\mathbb{N}|$$

Da queste osservazioni e grazie al matematico Cantor si arriva all'idea che esistono infiniti più infiniti di altri. Per esempio l'insieme dei numeri reali $|\mathbb{R}| \sim 2^{\mathbb{N}} = |P(\mathbb{N})|$, ovvero esistono più numeri reali dei numeri naturali nonostante siano entrambi infiniti. Consiglio di guardare la dimostrazione di Cantor su questo ultimo fatto.

3 Numeri Interi

$\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$ insieme dotato di due operazioni, somma e prodotto, $(\mathbb{Z}, +, \cdot)$ è un anello commutativo.

Definizione 1 (Anello commutativo)**.** *Un insieme A dotato di due operazioni:*

- *Somma* $+$: $A \times A \to A$
  $(a, b) \to a + b$
- *Prodotto* $\cdot$: $A \times A \to A$
  $(a, b) \to a \cdot b$

si dice che A è un anello commutativo se valgono le seguenti proprietà:

1. *$+$ è commutativa cioè $\forall\, a, b \in A$ vale $a + b = b + a$*
2. *$+$ è associativa cioè $\forall\, a, b, b \in A$ vale $(a + b) + b = a + (b + c)$*
3. *Deve esistere un elemento neutro, lo zero, per la somma cioè esiste $0_A \in A$ tale che $\forall\, a \in A$ $a + 0_A = a$*
4. *Ogni elemento ammette un unico inverso per la somma cioè $\forall\, a \in A\, \exists!\, b \in A$ tale che $a+b = 0_A$ (si indica b=-a).*
5. *Il prodotto è commutativo cioè $\forall\, a, b \in A$ vale $a \cdot b = b \cdot a$*
6. *il prodotto è associativo cioè $\forall\, a, b, c \in A$ vale $a \cdot (b \cdot c) = (a \cdot b) \cdot c$*
7. *Esiste un unico elemento neutro rispetto al prodotto, l'unità, cioè esiste $1_A \in A$ tale che $\forall\, a \in A$ vale $a \cdot 1_A = a$*
8. *Valgono le leggi distributive, $\forall\, a, b, c \in A$:*
   - $a \cdot (b + c) = ab + ac$
   - $(a + b) \cdot c = ac + bc$

In $\mathbb{Z}$ presi due numeri arbitrari possiamo sempre dividerli ottenendo un quoziente e un resto. Questa prende il nome di Divisione Euclidea.

Proposizione 1. *Dati $a, b \in \mathbb{Z}$ con $b \neq 0$ esistono q e $r \in \mathbb{Z}$ tale che:*

$$\begin{cases} a = b \cdot q + r \\ 0 \leq r < |b| \end{cases}$$

Inoltre q e r sono unici.

Dimostrazione. Per prima cosa dimostriamo l'esistenza di r e q.Distinguiamo due casi:

1. Caso in cui $a \geq 0$.
   Consideriamo l'insieme
   $$S = \{n \in \mathbb{N} | n = a - bm,\, m \in \mathbb{Z}\}$$
   Allora $S \subseteq \mathbb{N}$ e $S \neq \emptyset$ perchè $a = a - b \cdot 0$ e poiché $a \geq 0 \Longrightarrow a \in S$. Applico il principio del buon ordinamento (Ogni sottoinsieme di $\mathbb{N}$ ha minimo) e quindi esiste $r = min(S)$.

Poiché $r \in S$ allora $r \geq 0$ ed esiste un certo $q \in \mathbb{Z}$ tale che $r = a - bq$. Ora, se $r < |b|$ abbiamo finito.
Suppongo che $r \geq |b|$. Allora

$$r = a - bq = a - bq + |b| - |b| = a - b(a \pm 1) + |b|$$

Quindi

$$r - |b| = a - b(q \pm 1)$$

A questo punto, considerando $q \pm 1$ come numero intero, si ha che $r - |b| \in S$ poiché $r - |b| \geq 0$.
Ma $r - |b| < r$ perchè $b \neq 0 \Longrightarrow |b| \geq 1$ cioè $r - |b| \in S$ e

$$r - |b| < r = min(S)$$

Questo è assurdo per definizione di minimo e quindi $r < |b|$.

2. Caso in cui $a < 0$.
   Allora consideriamo $-a > 0$ e per il caso precedente esistono $\overline{q}, \overline{r} \in \mathbb{Z}$ tali che

$$\begin{cases} -a = b\overline{q} + \overline{r} \\ 0 \leq \overline{r} < |b| \end{cases}$$

   ora, se $\overline{r} = 0$ si ha che $a = b(-\overline{q}) + 0$ quindi ponendo $q = -\overline{q}$ e $r = \overline{r} = 0$ ho finito.
   Se invece $\overline{r} > 0$ allora posso scrivere

$$a = b(-\overline{q}) - \overline{r} = b(-\overline{q}) - \overline{r} + |b| - |b| = b(-\overline{q} \pm 1) + (|b| - \overline{r})$$

   Pongo

$$q = -\overline{q} + 1 \qquad r = |b| - \overline{r} > 0$$

   ed è ho finito.

Adesso dimostriamo l'<u>unicità</u>:
Siano

$$\begin{cases} a = bq + r \\ 0 \leq r < |b| \end{cases} \quad \begin{cases} a = bq_1 + r_1 \\ 0 \leq r_1 < |b| \end{cases} \Longrightarrow \begin{cases} q = q_1 \\ r = r_1 \end{cases}$$

Suppongo l'esistenza di due quozienti e due resti diversi e mostro che in realtà coincidono.
Considero

$$a = bq + r = bq_1 + r_1$$

Se $r = r_1$ allora $bq = bq_1 \Longrightarrow q = q_1$ ed ho finito.
Se $r \neq r_1$ posso supporre, senza perdere di generalità, $r_1 > r$. Quindi

$$0 < r_1 - r = (a - bq_1) - (a - bq) = bq - bq_1) = (b(q - q_1)$$

Applico il valore assoluto e trovo

$$|b||q - q_1| = |r - r_1|$$

Ma $r - r_1 > 0$ quindi

$$|b||q - q_1| = |r - r_1| = r - r_1 \leq r_1 \leq |b|$$

Ora, poiché $b \neq 0$ anche $|b| \neq 0$ quindi posso dividere e ottengo

$$|q - q_1| < 1$$

Ossia

$$|q - q_1| = 0 \Longrightarrow q = q_1$$

Quindi da $bq + r = bq_1 + r_1$ segue che $r = r_1$. □

Definizione 2. *Siano $a, b \in \mathbb{Z}$ diremo che b divide a, e scriveremo $b|a$, se esiste $q \in \mathbb{Z}$ tale che $a = b \cdot q$. Ossia il resto r della divisione è uguale a zero.*

Definizione 3 (MCD)**.** *Siano $a, b \in \mathbb{Z}$ diremo che un elemento $d \in \mathbb{Z}$ è un massimo comune divisore tra a e b se:*

1. *$d|a \wedge d|b$*
2. *Se ogni volta che esiste un $c \in \mathbb{Z}$ tale che $c|a$ e $c|b$ allora $c|d$. Ossia d è il massimo tra tutti i numeri che dividono a e b.*

Osservazione 1. *se d è un massimo comune divisore allora anche $-d$ lo è, $a = dq = (-d)(-q)$. Si indica con $MCD(a, b)$ il massimo comune divisore positivo.*

Proprietà MCD:

1. $MCD(a, b) = MCD(b, a) = MCD(|a|, |b|)$
2. $MCD(ab, ac) = |a| \cdot MCD(b, c)$
3. $MCD(a, 0) = |a| \ \forall\, a \neq 0$ questo perchè $MCD(0, 0)$ non è definito.

Definizione 4 (Coprimi)**.** *Diremo che $a, b \in \mathbb{Z}$ sono coprimi se $MCD(a, b) = 1$.*

Osservazione 2. $MCD(a, b) = |b| \Longleftrightarrow b|a$

Proposizione 2. *Siano $a, b \in \mathbb{Z}$ tale che $a = bq + r$ con $b \neq 0$ e $0 \leq r < |b|$. Allora $MCD(a, b) = MCD(b, r)$.*

Dimostrazione. Siano $d = MCD(a, b)$ e $f = MCD(b, r)$. Allora per definizione $d|a$ e $d|b$ quindi posso scrivere $a = dx$ e $b = dy$ con $x, y \in \mathbb{Z}$. Proviamo la doppia divisibilità, ossia che $f|d$ e $d|f$.

1. Proviamo $d|f$.
   Si ha che
   $$r = a - bq = dx - dyq = d(x - qy)$$
   Quindi $d|r$. Allora $d|b$ e $d|r$ e per definizione di $f = MCD(b, r)$ segue che $d|f$.

2. Proviamo che $f|d$.
   Per ipotesi $f = MCD(b, r)$ quindi $f|b$ e $f|r$ e chiamo $b = ft$ e $r = fs$ con $t, s \in \mathbb{Z}$. Segue che
   $$a = bq + r = ftq + fs = f(tq + s)$$
   Quindi $f|a$. Ora, $f|a$ e $f|b$ e quindi per definizione di $d = MCD(a, b)$ segue che $f|d$.

Ora, poiché $f|d$ e $d|f$ cioè $d = fw$ e $f = dy$ con $w, y \in \mathbb{Z}$. Poiché $f, d \geq 0 \Longrightarrow w, y \geq 0$ e quindi

$$d = fw = dyw$$

divido per d

$$1 = yw \Longleftrightarrow w = y = 1$$

Ossia $d = f$. □

Proposizione 3. *Siano $a, b \in \mathbb{Z}$, se $(a, b) \neq (0, 0)$ allora esiste $MCD(a, b)$.*

Dimostrazione. Si basa sull'esempio pratico, usando l'algoritmo di Euclide:
Siano $a, b \in \mathbb{Z}$ e $b \neq 0$ allora scrivo $a = bq + r$ e ,per quanto appena dimostrato, vale $MCD(a, b) = MCD(b, r)$.
Algoritmo Euclideo. Mi permette di trovare l'MCD tra due numeri interi a, b. Poiché $MCD(a, b) = MCD(|a|, |b|)$ posso supporre che $a, b \geq 0$. Inoltre dal fatto che $MCD(a, b) = MCD(b, a)$ posso supporre $a \geq b \geq 0$. Itero il seguente procedimento:

1. Divido a per b, $a = bq_1 + r_1$ con $0 \leq r_1 < b$ $MCD(a, b) = MCD(b, r_1)$
   - Se $r_1 = 0$ ho finito $MCD(b, r_1) = b = MCD(a, b)$
2. Se $r_1 > 0$ allora $b = r_1 q_2 + r_2$ con $0 \leq r_2 < r_1$
   - Se $r_2 = 0$ allora $MCD(b, r_1) = r_1 = MCD(a, b)$
3. Se $r_2 > 0$ allora $r_1 = r_2 q_3 + r_3$ con $0 \leq r_3 < r_2$
   - Se $r_3 = 0$ allora $MCD(a, b) = r_2$
4. Se $r_3 > 0$ allora $r_2 = r_3 q_4 + r_4$ con $0 \leq r_4 < r_3$

   ⋮

Ora, osservo che la successione dei resti $r_1 > r_2 > r_3 > r_4 > \cdots > r_n \geq 0$ è strettamente decrescente e quindi esiste un minimo intero n tale che $r_n > 0$ e $r_{n+1} = 0$. Allora si ha:

$$MCD(r_n, r_{n+1}) = r_n = MCD(r_{n-1}, r_n) = \cdots = MCD(a, b)$$

e quindi

$$r_n = MCD(a, b)$$

è l'ultimo resto non nullo. □

Teorema 1 (Formula di Bezout)**.** *Siano $a, b \in \mathbb{Z}$ tale che $(a, b) \neq (0, 0)$ e $d = MCD(a, b)$. Allora esistono $\alpha, \beta \in \mathbb{Z}$ tale che*

$$d = a\alpha + b\beta$$

Inoltre d divide ogni intero della forma $ax + by$ con $x, y \in \mathbb{Z}$.

Dimostrazione. Sia

$$S = \{n \in \mathbb{N}_{>0} | \exists\ x, y \in \mathbb{Z}\ t.c.\ n = ax + by\}$$

Allora $S \neq \emptyset$ poiché basta prendere $x = a$ e $y = b \Longrightarrow aa + bb = a^2 + b^2 > 0$ quindi $a^2 + b^2 \in S$. Allora per il principio del buon ordinamento esiste $c = min(S)$. Ora, provo che $c = d$ mostrando prima che $c|d$ e poi che $d|c \Longrightarrow c = d$.

1. Poiché $c \in S$ posso scrivere $c = a\alpha + b\beta$ per opportuni $\alpha, \beta \in \mathbb{Z}$. Dal fatto che $d = MCD(a, b)$ si ha che
$$d|a \wedge d|b$$
e quindi
$$d|a\alpha \quad d|b\beta$$
da cui segue
$$d|(a\alpha + b\beta) = c$$
cioè
$$d|c$$

2. Per dimostrare che $c|d$ basta provare che $c|a$ e $c|b \implies c|d$ per le proprietà dell'MCD. Mostro che $c|a$:
Faccio la divisione con resto di a per c, allora esistono unici $q, r \in \mathbb{Z}$ tale che $a = cq + r$ con $0 \leq r < c$. Faccio vedere che $r = 0$ procedendo per assurdo.
Suppongo che $r \neq 0$ allora $0 < r < c$ da cui segue
$$r = a - cq = a - (a\alpha + b\beta)q = a(1 - \alpha q) + b(-\beta)$$
Osservo che $(1 - \alpha q), (-\beta) \in \mathbb{Z}$ quindi $r \in S$ ma $r < c = min(S)$ e questo è assurdo per definizione di minimo di un insieme. Quindi deve essere che $r = 0$, cioè:
$$a = cq \implies c|a$$
Similmente si ottiene lo stesso risultato per quanto riguarda $c|b$.
Pertanto
$$c|MCD(a, b) = d$$
e quindi
$$\begin{cases} c|d \\ d|c \\ d, c > 0 \end{cases} \implies c = d$$
Infine proviamo che $d = min(S) = MCD(a, b)$ divide ogni elemento $m = ax + by$ con $x, y \in \mathbb{Z}$. Divido m per d quindi $m = dt + p$ con $t, p \in \mathbb{Z}$, $0 \leq < p < d$. Se $p \neq 0$ allora
$$0 < p < d = min(S)$$
$$p = m - dt = ax + by - (a\alpha + b\beta)t = a(x - \alpha t) + b(y - \beta t) \in S$$
e
$$p < min(S) = d$$
ma questo è assurdo. Segue che $p = 0$ cioè $m = dt \implies d|m$. □

Esempio. Sia $MCD(168, 22) = 2$ trovare $\alpha, \beta \in \mathbb{Z}$ tale che $MCD(168, 22) = 2 = 168\alpha + 22\beta$
$$168 = 22 \cdot 7 + 14 \implies 14 = 168 + 22(-7)$$
$$22 = 14 \cdot 1 + 8 \implies 8 = 22 - 14 = 22 - (18 + 22(-7)) = 168(-1) + 22(8)$$

$$14 = 8 \cdot 1 + 6 \Longrightarrow 6 = 14 - 8 = 168(1 - (-1)) + 22(-7 - 8)$$

$$8 = 6 + 2 \Longrightarrow 2 = 8 - 6 = 168(-1 - 2) + 22(8 - (-15)) = 168(-3) + 22(23)$$

Quindi

$$\alpha = -3 \quad \beta = 23$$

Definizione 5 (mcm)**.** *Siano $x, y \in \mathbb{Z}$ tale che $(x, y) \neq (0, 0)$, allora $[x, y] = mcm(x, y) = \frac{|xy|}{MCD(x,y)} \in \mathbb{Z}$. Alternativamente si definisce minimo comune multiple tra x e y ogni intero $z \in \mathbb{Z}$ tale che:*

1. *$x|z \wedge y|z$*
2. *$\forall\, w \in \mathbb{Z}$ tale che $x|w$ e $y|w$ vale $z|w$.*

Teorema 2 (Teorema di Lamè)**.** *Siano $a, b \in \mathbb{N}$ con $a \geq b > 0$. Allora il numero $D(a, b)$ di divisioni necessarie per trovare l'$MCD(a, b) = d$ è minore o uguale di $5k$ dove k è il numero di cifre decimali di b.*

Dimostrazione. Sia $D(a, b) = n + 1$ con $n \in \mathbb{N}$ allora $d = MCD(a, b) = r_n$. Ricordiamo

$$a = bq_1 + r_1 \quad 0 \leq r_1 < b$$

$$b = r_1 q_2 + r_2 \quad 0 \leq r_2 < r_1$$

$$r_1 = r_2 q_3 + r_3 \quad 0 \leq r_3 < r_2$$

$$\vdots$$

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

Ora, $\forall\, i = 1, 2, 3, \ldots, n$ i quozienti $q_i \geq 1$. Inoltre $q_{n+1} \geq 2$ poiché altrimenti $r_{n-1} = r_n$ e questo sarebbe assurdo.
Quindi vale $r_n \geq 1 = f_2$ dove $\{f_n\}$ è la successione di Fibonacci. Allora:

$$r_{n-1} = r_n q_{n-1} \geq 2r_n \geq 2 = f_3$$

$$r_{n-2} = r_{n-1} q_n + r_n \geq r_{n-1} + r_n \geq f_2 + f_3 = f_4$$

$$\vdots$$

$$r_1 = r_2 q_3 + r_3 \geq r_2 + r_3 \geq f_n + f_{n-1} = f_{n+1}$$

$$b = r_1 q_2 + r_2 \geq \cdots \geq f_{n+1} + f_n = f_{n+2}$$

Ora, una proprietà della successione di Fibonacci $\{f_n\}_{n \in \mathbb{N}}$ è che $f_n \geq \phi^{n-2}$, dove $\phi = \frac{1+\sqrt{5}}{2}$ numero Aureo. Quindi:

$$b \geq f_{n+2} \geq \phi^n$$

Applico il logaritmo

$$\log_{10} b \geq \log_{10} \phi^n = n \log_{10} \phi$$

Quindi poiché $\log_{10}(\frac{1+\sqrt{5}}{2}) > \frac{1}{5}$

$$\log_{10} b > \frac{n}{5}$$

Se b ha k cifre, allora

$$10^{k-1} \leq bz10^k$$

$$k-1 \leq \log_{10} b < k$$

Quindi

$$n < 5\log_{10} b < 5k$$

Ora, poiché $n, 5k \in \mathbb{N} \implies n < 5k$ equivale a $n+1 \leq 5k$ cioè

$$D(a,b) \leq 5k$$

. □

3.1 Rappresentazioni b-adiche

$2019 = 2 \cdot 10^3 + 0 \cdot 10^2 + 1 \cdot 10 + 9 \cdot 10^0$ base 10 = scrivo il numero come somma di potenze di 10. In base 2 le cifre ammesse sono {0,1}, infatti:

$$\begin{array}{cc|c} 2019 = 2(1009) + 1 & 63 = 2(31) + 1 & 1 = 2 \cdot 0 + 1 \\ 1009 = 2(504) + 1 & 31 = 2(15) + 1 & \\ 504 = 2(252) + 0 & 15 = 2(7) + 1 & \\ 252 = 2(126) + 0 & 7 = 2(3) + 1 & \\ 126 = 2(63) + 0 & 3 = 2(1) + 1 & \end{array}$$

Quindi

$$2019 = (11111100011)_2 = 1 \cdot 2^{10} + 1 \cdot 2^9 + 1 \cdot 2^8 + \dots$$

Proposizione 4. *Sia $b \in \mathbb{Z}$ tale che $b \geq 2$. Allora per ogni numero $n > 0$ esistono e sono unici un $k \in \mathbb{N}$ e $n_i \in \{0, 1, 2, \dots, b-1\}$ con $n_k \neq 0$ tali che*

$$n = n_k b^k + n_{k-1} b^{k-1} + \dots + n_1 b + n_0$$

Dimostrazione. Dimostro l'esistenza per induzione su n.

1. Se $n = 1$ allora $k = 0$ e $n_k = n_0 = 1$ quindi $1 = 1$ e $n = n_0$.
2. Sia $n = n_k b^k + n_{k-1} b^{k-1} + \dots + n_1 b + n_0$ vera per ogni m con $0 < m < n$, proviamolo per n. Divido con resto n per $b \neq 0$. Allora esistono $q, r \in \mathbb{N}$ tale che $n = bq + r$ e $0 \leq r < b$. Ora, $q < n$ perchè $b \geq 2$.
   - Se $q = 0$ prendo $k = 0$ e $n_0 = r = n$.
   - Se $q > 0$ allora $0 < q < n$ e per ipotesi induttiva ho che esistono $h \in \mathbb{N}$, $m_i \in \{0, \dots, b-1\}\, \forall\, i = 0, \dots, h$ con $m_h \neq 0$ tali che:

     $$q = m_h b^h + m_{h-1} b^{h-1} + \dots + m_1 b + m_0$$

     Allora da $n = bq + r$ segue

     $$n = b(m_h b^h + m_{h-1} b^{h-1} + \dots + m_1 b + m_0) + r =$$

     $$m_h b^{h+1} + \dots + m_1 b^2 + m_0 b + r$$

     Si prende $k = h + 1$, $n_i = m_{i-1}\ \forall\, i = 1, \dots, k$ e $n_0 = r$

Dimostro l'unicità.
Sia $n \geq 1$ tale che

$$n = n_k b^k + \cdots + n_1 b + n_0 = l_y b^t + \cdots + l_1 b + l_0$$

con $k, t \in \mathbb{N}$, $n_j, l_i \in \{0, 1, \ldots, b-1\}$, $n_k \neq 0$ e $l_t \neq 0$. Provo che $k = t$ e $\forall\, i = 0, \ldots, k$ $n_i = l_i$.

$$n = \underbrace{(n_k b^{k-1} + \cdots + n_2 b + n_1)}_{q} b + \underbrace{n_0}_{r}$$

poiché $0 \leq n_0 < b$ si ha

$$q = n_k b^{k-1} + \cdots + n_2 b + n_1$$

è il quoziente di n diviso b e $r = n_0$ è il resto della divisione. Analogamente per

$$n = (l_1 b^{t-1} + \cdots + l_2 b + l_1) b + l_0$$

quindi

$$\begin{cases} n_0 = l_0 \\ l_1 b^{t-1} + \cdots + l_2 b + l_1 = n_k b^{k-1} + \cdots + n_2 b + n_1 \end{cases}$$

Questo perchè $q < n$ e quindi per ipotesi induttiva si ha che q ha una sola scrittura in base b. Quindi

$$k - 1 = t - 1$$

$$n_j = l_j \qquad \forall\, j = 1, \ldots, k$$

ossia

$$k = t \qquad n_j = l_j \;\forall\, j = 0, \ldots, k$$

□

3.2 Equazioni Diofantee

Teorema 3. *Dati $a, b, n \in \mathbb{Z}$ con $(a, b) \neq (0, 0)$, allora:*

- *L'equazione*

$$ax + by = n \tag{1}$$

  ha soluzioni se e solo se $MCD(a, b) = d$ divide n.

- *Se (x_0, y_0) è una soluzione di (1) allora l'insieme di tutte e solo le soluzioni è*

$$S = \{(x_0 + \frac{b}{d}k), y_0 - \frac{a}{d}k) | k \in \mathbb{Z}\}$$

Dimostrazione. Prima dimostro il punto 1.

$\Longrightarrow$ Sia (x_0, y_0) una soluzione di (1) e proviamo che $d|n$. Allora vale $ax_0 + by_0 = n$, ora $d = MCD(a, b)$ quindi $d|a$ e $d|b$ scrivo $a = da'$ e $b = db'$ con $a', b' \in \mathbb{Z}$. Quindi

$$n = a_0 + by_0 = da'x_0 + db'y_0 = d(a'x_0 + b'y_0 = d\underbrace{(a'x_0 + b'y_0)}_{\in \mathbb{Z}}$$

ossia $d|n$.

$\Longleftarrow$ Viceversa sia $d|n$ e provo che esiste una soluzione intera di (1). $d = MCD(a,b)$ quindi per Bezout esistono $\alpha, \beta \in \mathbb{Z}$ tale che $d = a\alpha + b\beta$. Poiché $d|n$ scrivo $n = dt$ con $t \in \mathbb{Z}$ opportuno. Allora:

$$n = dt = (a\alpha + b\beta)t = a(\alpha t) + b(\beta t)$$

La coppia $(\alpha t, \beta t) \in \mathbb{Z} \times \mathbb{Z}$ è soluzione di (1).

Dimostro il punto 2.

$\subseteq$ Sia $(x_0 + \frac{b}{d}k, y_0 - \frac{a}{d}k) \in S$ provo che è soluzione dell'equazione. Facilmente si vede che $x_0 + \frac{b}{d}k, y_0 - \frac{a}{d}k \in \mathbb{Z}$ quindi

$$a(x_0 + \frac{b}{d}k) + b(y_0 - \frac{a}{d}k) = ax_0 + \frac{ab}{d}k + by_0 - \frac{ab}{d}k = ax_0 + by_0 = n$$

$\supseteq$ Viceversa sia $(\overline{x}, \overline{y})$ una soluzione intera dell'equazione, provo che $(\overline{x}, \overline{y}) \in S$. Allora $a\overline{x}, b\overline{y} = n = ax_0 + by_0$ quindi

$$a(\overline{x} - x_0) = b(y_0 - \overline{y}) \tag{2}$$

Quindi $d|a \wedge d|b$ cioè $\frac{a}{d}, \frac{b}{d} \in \mathbb{Z}$. Ora $\frac{b}{d}$ è coprimo con $\frac{a}{d}$ cioè $MCD(\frac{a}{d}, \frac{b}{d}) = 1$. Quindi (2) implica che $\frac{b}{d}|(\overline{x} - x_0)$ cioè esiste $k \in \mathbb{Z}$ tale che $\overline{x} - x_0 = \frac{b}{d}k$ quindi $\overline{x} = x_0 + \frac{b}{d}k$ e da (2) si trova $\overline{y} = y_0 - \frac{a}{d}k$, segue che

$$(\overline{x}, \overline{y}) = \{x_0 + \frac{b}{d}k, y_0 - \frac{a}{d}k\} \in S$$

□

Definizione 6 (Invertibile)**.** *Un elemento $a \in \mathbb{Z}$ è invertibile se esiste $b \in \mathbb{Z}$ tale che $a \cdot b = 1$. Segue che gli unici invertibili di $\mathbb{Z}$ sono +1 e -1.*

Definizione 7 (Irriducibile)**.** *Un elemento $a \in \mathbb{Z}$ è irriducibile se:*

- *$a \neq 0 \wedge a \neq \pm 1$ (non è invertibile)*
- *Ogni volta che $a = bc$ allora o $b = \pm 1$ o $c = \pm 1$.*

Definizione 8 (Primo)**.** *Un elemento $a \in \mathbb{Z}$ è primo se:*

- *$a \neq 0$ e $a \neq \pm 1$*
- *Ogni volta che $a|bc$ allora o $a|b$ o $a|c$, con $b, c \in \mathbb{Z}$*

Proposizione 5. *Un elemento di $\mathbb{Z}$ è primo se e solo se è irriducibile.*

Dimostrazione.

$\Longrightarrow$ Sia $a \in \mathbb{Z}$ elemento primo, provo che a è irriducibile.
Per ipotesi $a \neq 0$ e $a \neq \pm 1$. Per provare che a è irriducibile suppongo che sia $a = bc$ con $b, c \in \mathbb{Z}$ e provo che o $b = \pm 1$ o $c = \pm 1$.
Poiché $a = bc$ si ha che $a|bc$ e quindi, essendo a primo, $a|b$ cioè $b = ah$ per qualche $h \in \mathbb{Z}$. Oppure $a|c$ cioè $c = ak$ per qualche $k \in \mathbb{Z}$.
Se fosse $b = ah$ allora si ottiene $a = bc = ah$ e poiché $a \neq 0$, trovo $1 = hc$ ma questo implica che $c = \pm 1$. Si ragiona analogamente se fosse $c = ak$ e si ottiene quindi $1 = kb$ quindi $b = \pm 1$.

$\Longleftarrow$ Viceversa, sia $a \in \mathbb{Z}$ irriducibile proviamo che è un primo in $\mathbb{Z}$. Per ipotesi $a \neq 0$ e $a \neq \pm 1$.
Suppongo che $a|bc$ con $b, c \in \mathbb{Z}$ e provo che $a|b$ o $a|c$.
Poiché $a|bc$ segue che esiste $h \in \mathbb{Z}$ tale che $bc = ah$. Suppongo che $a \nmid b$ e provo che $a|c$.
Considero $MCD(a, b) = d$, $d|a$ e $d|b$ ora a è un elemento irriducibile, quindi non ha divisori proprio, cioè

$$d = \begin{cases} |a| \\ 1 \end{cases}$$

Ora, poiché $a \nmid b$ segue che $d = 1$. Quindi $MCD(a, b) = 1$, applico Bezout, quindi esistono $\alpha, \beta \in \mathbb{Z}$ tale che $1 = \alpha a + \beta b$. Moltiplico per c:

$$c = ac\alpha + bc\beta = ac\alpha + ah\beta = a(c\alpha + h\beta)$$

ovvero $a|c$. □

Teorema 4 (Teorema fondamentale dell'Aritmetica)**.** *Sia $n \in \mathbb{N}$ tale che $n > 1$. Allora n ammette una scrittura essenzialmente unica nella forma*

$$n = p_1^{a_1} \cdot_2^{a_2} \cdot \cdots \cdot p_s^{a_s}$$

con $s \in \mathbb{N}$, $s \geq 1$, $p_1, p_2, \ldots, p_s$ irriducibili distinti e positivi e $a_1, a_2, \ldots, a_s \in \mathbb{Z}_{\geq 1}$.

Dimostrazione.

1. Dimostriamo l'esistenza. Procediamo per induzione su n.
   (a) Per $n = 2$ cioè $s = 1$, $p = 2$ e $a_1 = 1$.
   (b) Sia vero per ogni intero $1 < m < n$ e proviamolo per n. Se n è irriducibile allora abbiamo finito, poiché $n = n$ e quindi prendo $s = 1$, $p_1 = n$ e $a_1 = 1$.
   Sia n riducibile e sia $n = ab$ con $a, b \in \mathbb{Z}$ tale che $a \neq \pm 1$ e $b \neq \pm 1$. Ora, poiché $n > 1$ vale $n = ab$ con $a, b > 1$. Abbiamo $1 < a < n$ e $1 < b < n$. Applico l'ipotesi induttiva e scrivo

   $$a = q_1^{\alpha_1} q_2^{\alpha_2} \ldots q_r^{\alpha_r} \text{ con } q_i \text{ irriducibili, distinti e positivi}$$

   e

   $$b = t_1^{\beta_1} t_2^{\beta_2} \ldots t_h^{\beta_h} \text{ con } t_i \text{ irriducibili, distinti e positivi.}$$

   Quindi

   $$n = q_1^{\alpha_1} q_2^{\alpha_2} \ldots q_r^{\alpha_r} t_1^{\beta_1} t_2^{\beta_2} \ldots t_h^{\beta_h}$$

   è una fattorizzazione in irriducibili.

2. Dimostriamo l'essenziale unicità per induzione sul numero m di fattori irriducibili di una fattorizzazione di lunghezza minima per n.
   (a) Se $m = 1$ allora esiste una fattorizzazione per n della forma $n = p_1$, ciò significa che n è irriducibile e quindi per la proposizione precedente, n è primo.
   Ora se fosse

   $$n = q_1^{\beta_1} \cdot \cdots \cdot q_r^{\beta_r} \tag{3}$$

   con q_i irriducibili, distinti e positivi. Ora, poiché n è primo,

$$n|q_1^{\beta_1} \cdot q_j^{\beta_j} \dots q_r^{\beta_r} \Longrightarrow \exists\ j \text{ tale che } n|q_j$$

Ora q_j è irriducibili quindi $n|q_j$ e $n > 1 \Longrightarrow n = q_j$.
Divido (2) per $n = q_j$, trovo

$$1 = q_1^{\beta_1} \cdot q_j^{\beta_j - 1} \dots q_r^{\beta_r}$$

poiché $q \neq \pm 1$ segue che $\beta_i = 0\ \forall i \neq j$ e $\beta - 1 = 0 \Longrightarrow \beta_j = 1$ cioè

$$q_1^{\beta_1} \dots q_r^{\beta_r} = q_j = n \text{ e } n = n$$

è l'unica fattorizzazione.

(b) Siano

$$n = p_1^{a_1} \cdot \dots \cdot p_s^{a_s} = q_1^{b_1} \cdot \dots \cdot q_t^{b_t} \tag{4}$$

con $p_i, q_j > 0$ irriducibili, e supponiamo che sia $a_1 + a_2 + \dots + a_j = m$.
$p_1|n$ e p_1 è irriducibile e quindi è primo. Come prima

$$p_1|q_1^{b_1} \cdot \dots \cdot q_t^{b_t}$$

si ha che esiste $k \in \{1, \dots, t\}$ tale che $p_1|q_k$ ma q_k è irriducibile e quindi $p_1 = q_k$. Divido (3) per $p_1 = q_k$ e trovo

$$p_1^{a_1 - 1} \cdot \dots \cdot p_s^{a_s} = q_1^{b_1} \dots q_k^{b_k - 1} \dots q_t^{b_t}$$

Poiché a sinistra ho $m-1$ fattori irriducibili posso applicare l'induzione e trovo che le due scritture sono identiche, cioè $s = t$, $\{p_1, \dots, p_s\} = \{q_1, \dots, q_t\}$ con gli stessi esponenti, segue l'unicità della scrittura per n. □

Teorema 5 (Teorema di Euclide)**.** *I numeri interi primi sono infiniti.*

Dimostrazione. Supponiamo per assurdo che i numeri primi positivi siano finiti e siano esattamente i seguenti $p_1, p_2, \dots, p_N$.
Allora considero il numero

$$n = p_1 \cdot p_2 \cdot \dots \cdot p_N + 1$$

quindi, per il teorema fondamentale dell'aritmetica, n ammette una fattorizzazione in prodotto di primi. In particolare esiste almeno un primo che divide n. Cioè esiste un p_j con $j = 1, \dots, N$ tale che $p_j|n$. Ma ciò è assurdo perchè $n = p_1 \cdot p_2 \cdot \dots \cdot p_N + 1$ e n diviso per p_j ha resto 1. Quindi i primi sono infiniti. □

Proposizione 6. *Se p è un numero primo di $\mathbb{Z}$ e $p > 0$ allora $\sqrt{p} \notin \mathbb{Q}$.*

Dimostrazione. Per assurdo. Sia $\sqrt{p} = \frac{a}{b}$ con $a, b \in \mathbb{Z}$, $b \neq 0$ e $MCD(a, b) = 1$. Posso elevare al quadrato $p = \frac{a^2}{b^2}$ cioè $p \cdot b^2 = a^2$ e quindi $p|a^2$. Per il teorema fondamentale dell'aritmetica se $a = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_p^{\alpha_p}$ allora

$$a^2 = p_1^{2\alpha_1} p_2^{2\alpha_2} \dots p_p^{2\alpha_p}$$

quindi esiste j tale che $p|p_j$ ma $p|a$ e $2\alpha_j$ è l'esponente di p di a^2.
D'altra parte $a^2 = b^2 p$ e l'esponente di p del numero pb^2 deve essere dispari, infatti

$$b^2 = q_1^{2\beta_1} q_2^{2\beta_2} \dots q_k^{2\beta_k}$$

se $q_h = p$ allora l'esponente di p in pb^2 è $1 + 2\beta_h$ dispari. Ossia a sinistra l'esponente di p è pari mentre a destra è dispari e questo è assurdo perchè le due fattorizzazioni devono essere identiche. □

Esempio. $p = 2 \Longrightarrow \sqrt{2} = \frac{a}{b} \Longrightarrow 2b^2 = a^2$ quindi a^2 è pari e allora $4|a^2$ e scrivo $a^2 = 4u$.

$$2b^2 = 4u \Longrightarrow b^2 = 2u$$

Ma questo è assurdo perchè avevamo supposto che a, b fossero coprimi cioè $MCD(a, b) = 1$ e invece, essendo entrambi pari, sono divisibili per due.

Teorema 6 (Teorema fondamentale dei numeri primi)**.** *Sia* $\Pi(x)$ *il numero di numeri primi* p *compresi tra 1 e* x *con* $x \in \mathbb{R}$, $x > 0$. *Allora*

$$\Pi(x) \simeq \frac{x}{\log x} \qquad x \to \infty$$

Definizione 9 (Primo di Fermat)**.** *Un numero primo di Fermat* p *è un primo della forma*

$$p = 2^m + 1$$

Osservazione 3. *Se* $2^m + 1$ *è un primo allora* $m = 2^n$ *per qualche* $n \in \mathbb{N}$.

Definizione 10 (Primo di Mersenne)**.** *Un numero primo di Mersenne* p *è un primo della forma*

$$p = 2^k - 1$$

4 Congruenze

Sia $(A, +, \cdot, 0_A, 1_A)$ un anello commutativo.

Definizione 1 (Invertibile)**.** *Sia $a \in A$, a si dice invertibile in A se esiste $b \in A$ tale che $a \cdot b = 1_A$.*

Definizione 2 (Divisore dello zero)**.** *Un elemento $a \in A$ è un divisore dello zero (d.d.z) se:*

- $a \neq 0$
- $\exists\ b \in A,\ b \neq 0_A$ *tale che* $a \cdot b = 0_A$

$\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ *non hanno d.d.z.*

Definizione 3 (Campo)**.** *Un campo è un anello commutativo A in cui ogni elemento $a \in A$ tale che $a \neq 0$ è invertibile.*

Definizione 4 (Dominio di Integrità)**.** *Un anello commutativo che è privo di d.d.z si chiama Dominio di Integrità.*

Definizione 5 (Irriducibile)**.** *Sia A un dominio e $a \in A$. Allora diremo che a è un elemento irriducibile se:*

- $a \neq 0_A$ *e a non è invertibile*
- *Ogni volta che $a = b \cdot c$ con $b, c \in A$ allora b o c è invertibile.*

Definizione 6 (Primo)**.** *a si dice elemento primo di A se :*

- $a \neq 0_A$ *e non è invertibile*
- *Ogni volta che $a|b \cdot c$ allora $a|b$ o $a|c$.*

In generale, vale sempre $\{elementi\ primi\} \subseteq \{elementi\ irriducibili\}$. Se $A = \mathbb{Z}$ allora vale l'uguaglianza.

4.1 Classi di resto modulo n

Sia $n \geq 2$ e $n \in \mathbb{N}$. La relazione di congruenza $\equiv$ modulo n, $a \equiv b (mod\, n)$ se e solo se $n|(a - b)$ $\forall\, a, b \in \mathbb{Z}$.

Definizione 7 (Classe di congruenza)**.** *Per ogni $a \in \mathbb{Z}$ indichiamo $\overline{a}$ la sua classe di congruenza modulo n.*

$$\overline{a} = \{b \in \mathbb{Z} | b \equiv a (mod\, n)\}$$

Indichiamo con $\mathbb{Z}_n = \frac{\mathbb{Z}}{\equiv} = \{\overline{a} | a \in \mathbb{Z}\}$ l'insieme quoziente, ossia l'insieme di tutte le classi di equivalenza.

Teorema 1. *Se $n \geq 2$ allora $\mathbb{Z}_n = \{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{n-1}\}$ e ha $n = |\mathbb{Z}_n|$ elementi.*

Dimostrazione. Se $a \in \mathbb{Z}$ allora divido a per $n \implies$ esistono unici $q, r \in \mathbb{Z}$ tale che $a = qn + r$ e $0 \leq r < n$. Questo significa che

$$n|qn = (a - r)$$

ovvero

$$a \equiv r(mod\, n)$$

ossia

$$\overline{a} = \overline{r}$$

di conseguenza $\in \{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{n-1}\}$.
Infine per provare che sono tutte distinte, $i \neq j$ con $i, j \in \{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{n-1}\}$ e $0 < |i - j| < n$ allora $i \not\equiv j(mod\, n)$ cioè

$$i \not\equiv j$$

quindi $\{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{n-1}\}$ ha esattamente n elementi. □

4.2 Operazioni su $\mathbb{Z}_n$

Definiamo due operazioni su $\mathbb{Z}_n$ che lo rendono un Anello commutativo.

1. Somma $+$: $\begin{array}{rl} \mathbb{Z}_n \times \mathbb{Z}_n \to & \mathbb{Z}_n \\ (\overline{a}, \overline{b}) & \to \overline{a} + \overline{b} = \overline{a + b} \end{array}$
2. Prodotto $\cdot$: $\begin{array}{rl} \mathbb{Z}_n \times \mathbb{Z}_n \to & \mathbb{Z}_n \\ (\overline{a}, \overline{b}) & \to \overline{a} \cdot \overline{b} = \overline{a \cdot b} \end{array}$

Le definizioni di somma e prodotto di $\mathbb{Z}_n$ sono ben poste per il seguente teorema.

Teorema 2. *Siano $a, b, c, d \in \mathbb{Z}$, se $a \equiv c(mod\, n)$ e $b \equiv d(mod\, n)$ allora*

$$a + b \equiv c + d(mod\, n)$$

$$a \cdot b \equiv c \cdot d(mod\, n)$$

cioè

$$\begin{cases} \overline{a} = \overline{c} \\ \overline{a} = \overline{c} \end{cases} \implies \begin{cases} \overline{a + b} = \overline{c + d} \\ \overline{a \cdot b} = \overline{c \cdot d} \end{cases}$$

Dimostrazione.

1. Per ipotesi abbiamo che $a - c = nh$ e $b - d = nk$ con $h, k \in \mathbb{Z}$. Allora

   $$a + b - (c + d) = a - c + b - d = nh - nk = n(h - k)$$

   cioè

   $$n|(a + b) - (c + d) \implies a + b \equiv c + d(mod\, n)$$

2. Si ha che

   $$ab - cd = ab - ad + ad - cd = a(b - d) + d(a - c) = a(nk) + d(nh) = n(ak + dh)$$

   cioè

   $$ab \equiv cd(mod\, n)$$

□

Esempio.

1. Sia $\mathbb{Z}_4 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}\}$

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{0}$	$\overline{1}$	$\overline{2}$

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{0}$	$\overline{2}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

   $\mathbb{Z}_4$ non è un Dominio di integrità, ad esempio $\overline{2}$ è un d.d.z. infatti $\overline{2} \cdot \overline{2} = \overline{4} = \overline{0}$.

2. Sia $\mathbb{Z}_9 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}, \overline{6}, \overline{7}\}$ cerco d.d.z. e invertibili.
   (a) $\overline{0}$ non è né d.d.z. né invertibile
   (b) $\overline{1}$ è invertibile, $\overline{1} \cdot \overline{1} = \overline{1}$
   (c) $\overline{2}$ è d.d.z, $\overline{2} \cdot \overline{4} = \overline{0}$
   (d) $\overline{3}$ è invertibile, $\overline{3} \cdot \overline{3} = \overline{9} = \overline{1}$
   (e) $\overline{4}$ è d.d.z, $\overline{4} \cdot \overline{2} = \overline{0}$
   (f) $\overline{5}$ è invertibile, $\overline{5} \cdot \overline{5} = \overline{1}$
   (g) $\overline{6}$ è d.d.z, $\overline{6} \cdot \overline{4} = \overline{0}$
   (h) $\overline{5}$ è invertibile, $\overline{7} \cdot \overline{7} = \overline{1}$

   Quindi

$$\{d.d.z\} = \{\overline{2}, \overline{4}, \overline{6}\}$$
$$\{invertibili\} = \{\overline{1}, \overline{3}, \overline{5}, \overline{7}\}$$
$$\{\mathbb{Z}_9\} = \{\overline{0}\} \cup \{\overline{2}, \overline{4}, \overline{6}\} \cup \{\overline{1}, \overline{3}, \overline{5}, \overline{7}\}$$

Vale sempre $\mathbb{Z}_n = \{\overline{0} \cup \{d.d.z\} \cup \{invertibili\}$

Proposizione 1. *Sia $n \in \mathbb{Z}$, allora:*

- *Se n è primo $\Longrightarrow \mathbb{Z}_n = \{\overline{0}\} \cup \{invertibili\}$ è un campo finito e dominio*
- *Se n non è primo $\Longrightarrow \mathbb{Z}_n$ ha d.d.z e non è un dominio.*

Dimostrazione. Dimostriamo il secondo punto.
Possiamo scrivere n come $a \cdot b = n$ con $a \cdot b > 1$ e $a, b < n$. Allora $\overline{a} \neq \overline{0}$ e $\overline{b} \neq \overline{0}$ e

$$\overline{a} \cdot \overline{b} = \overline{a \cdot b} = \overline{n} = \overline{0}$$

Allora $\overline{a}$ e $\overline{b}$ sono d.d.z. □

4.3 Criteri di divisibilità

Sia $n \in \mathbb{N}$ e sia $n = a_k a_{k-1} \dots a_1 a_0$ la sua scrittura in base $b = 10$ con $a_i = \{0, 1, \dots, 9\}$ cioè $n = a_k \cdot 10^k + a_{k-1} \cdot 10^{k-1} + \dots + a_1 \cdot 10 + a_0$.

4.3.1 Divisibilità per 3 e per 9

n è divisibile per tre, ossia $3|n$, se e solo se la somma delle cifre $a_0 + a_1 + \cdots + a_k$ è divisibile per tre. Analogo per 9.
Dimostrazione. Dimostriamo il caso 9, il caso 3 si dimostra in modo analogo.
Osservo che $10^t \equiv 1^t \equiv 1(mod\,9)$ quindi:

$$n = a_k \cdot 10^k + a_{k-1} \cdot 10^{k-1} + \cdots + a_1 \cdot 10 + a_0 \equiv a_k + a_{k-1} + \cdots + a_1 + a_0\,(mod\,9)$$

quindi

$$9|n \iff 9|a_k + a_{k-1} + \cdots + a_1 + a_0$$

□

4.3.2 Divisibilità per 2 e per 5

Osservo che $10 \equiv 0(mod\,2)$ quindi

$$10^t \equiv 0(mod\,2)$$

segue che

$$n = a_k 10^k + \cdots + a_1 10 + a_0 \equiv a_0(mod\,2)$$

cioè $2|n$ se e solo se $2|a_0$. Per cinque si ragiona analogamente.

4.3.3 Divisibilità per 4 e per 25

n è divisibile per $4/25$ se le ultime due cifre decimali a_1a_0 sono divisibili per $4/25$. *Dimostrazione.* Osservo che $100 = 2^2 5^2 \Rightarrow 100 \equiv 0(mod\ 4/25)$. Allora vale che $t \geq 2$, con $t = h + 2$ e $h \geq 0$, $10^t \equiv 10^h(100) \equiv 0(mod\ 4/25)$. Allora

$$n = \underbrace{a_k 10^k + \cdots + a_2 10^2}_{\equiv 0 mod(\ 4/25)} + a_1 10 + a_0 \equiv a_1 10 + a_0(mod\ 4/25)$$

Segue che

$$4|n \iff 4|a_1a_0$$
$$25|n \iff 25|a_1a_0$$

□

4.3.4 Divisibilità per 11

n è divisibile per 11 se e solo se $a_0 - a_1 + a_2 - a_3 + \cdots + (-1)^n a_n$ è divisibile per 11. Ovvero se la somma delle cifre in posizione pari meno quella delle cifre in posizione dispari è divisibile per 11.
Dimostrazione. Si ha che $10 \equiv -1(mod\ 11)$ quindi $10^t \equiv (-1)^t(mod\ 11)$ quindi

$$\begin{cases} 10^{2t} \equiv 1(mod\ 11) \\ 10^{2t+1} \equiv -1(mod\ 11) \end{cases}$$

Allora

$$a_0 + a_1 10 + \cdots + a_k 10^k \equiv a_0 - a_1 + a_2 \cdots + (-1)^k a_k(mod\ 11) \equiv S_p - S_d(mod\ 11)$$

segue che $11|m \iff 11|S_p - S_d$ □

4.4 Ancora congruenze

Lemma 1. *Sia p un numero primo positivo $p > 0$, allora $\forall\, x, t \in \mathbb{Z}$ vale*

$$(x+y)^p \equiv x^p + y^p (mod\, n)$$

Dimostrazione. Per Newton

$$(x+y)^p = \sum_{k=0}^{p} \binom{p}{k} x^{p-k} y^k = x^p + y^p + \sum_{k=1}^{p-1} \binom{p}{k} x^{p-k} y^k$$

Provo che quando $1 \leq k \leq p-1$ allora $p|\binom{p}{k}$ cioè $\binom{p}{k} \equiv 0 (mod\, p)$. Infatti $\binom{p}{k} \in \mathbb{N}$ e

$$\binom{p}{k} = \frac{p(p-1)(p-2)\dots(p-k+1)}{k!} = \frac{N}{k!}$$

dove $N = p(p-1)(p-2)\dots(p-k+1)$. Ora, $p|N$, e inoltre $p \nmid k!$ perchè $1 \leq k < p$ e se p dividesse $k!$ allora p dovrebbe dividere un j con $1 \leq j < k$ perchè p è primo. Questo è impossibile perchè $1 \leq j < p$. Segue che $p \nmid k!$ e quindi

$$p|\frac{N}{k!}$$

$N = \frac{N}{k!} k! \Longrightarrow p|N$ e p è primo $\Longrightarrow p|\frac{N}{k!} k \Longrightarrow p|\frac{N}{k!} = \binom{p}{k}$. Segue che

$$(x+y)^p \equiv x^p + y^p + \sum 0) x^p + y^+ (mod\, p)$$

□

Teorema 3. *Sia $a \in \mathbb{Z}$ e $p \in \mathbb{P}$ con $p > 0$, allora*

$$a^p \equiv a\, (mod\, p)$$

Dimostrazione. Distinguiamo due casi:

1. Caso $a > 0$. Procedo per induzione su a.
   (a) Se $a = 0$ allora $0^p \equiv 0(mopp)$
   (b) Sia $a > 0$ e assumo che valga $a^p \equiv a\, (mod\, p)$. Provo che vale $(a+1)^p \equiv a+1\, (mod\, p)$. Per il lemma 1
   $$(a+1)^p \equiv a^p + 1^p (mod\, p)$$
   per ipotesi induttiva
   $$(a+1)^p \equiv a + 1 (mod\, p)$$
2. Caso $a < 0$. Osservo che $0 = (a + (-a))^p \equiv a^p + (-a)^p (mod\, p)$. Quindi
   $$a^p \equiv -(-a)^p (mod\, p)$$
   ora $-a > 0$ e per il caso precedente vale
   $$(-a)^p \equiv -a (mod\, p)$$
   Quindi trovo che
   $$a^p \equiv -(-a)^p (mod\, p) \equiv -(-a)(mod\, p) \equiv a (mod\, p)$$

□

Corollario 1. *Sia $p \in \mathbb{P}$ $p > 0$ e $a \in \mathbb{Z}$. Allora:*

- *se $MCD(a,p) \neq 1$ si ha che $a^{p-1} \equiv 0(mod\, p)$*
- *se $MCD(a,p) = 1$ si ha che $a^{p-1} \equiv 1(mod\, p)$*

Dimostrazione.

1. Quando $MCD(a,p) \neq 1$ poiché p è primo $MCD(a,p) = p$ cioè $p|a$ cioè
$$a \equiv 0(mod\, p)$$
e quindi
$$a^{p-1} \equiv 0(mod\, p)$$
2. Quando $MCD(a,p) = 1$ per il teorema di Fermat si ha che
$$a^p - a \equiv 0(mod\, p)$$
quindi
$$a(a^{p-1} - 1) \equiv 0(mod\, p)$$
cioè
$$p|a(a^{p-1} - 1)$$
Poiché p è primo segue che o $p|a$ ma questo è falso perchè si avrebbe $MCD(a,p) = p \neq 1$. Oppure $p|a^{p-1}$ cioè
$$a^{p-1} - 1 \equiv 0(mod\, p)$$

□

Esempio. Determinare il resto della divisione per 13 del numero 5648^{321}. Ossia risolvere $5648^{321}(mod\, 13)$. Osservo che $p = 13$ è primo e maggiore di zero. Quindi

$$a = 5648 = 13 \cdot 434 + 6 \equiv 6(mod\, 13)$$

Ora devo fare $6^{321}(mod\, 13)$. Applico il corollario di Fermat

$$6^{12} \equiv 1(mod\, 13)$$

. Ora prendo 321 e lo divido con resto per 12.

$$321 = 12 \cdot 26 + 9$$

$$6^{321} = 6^{12 \cdot 26 + 9} = (6^{12})^{26} \cdot 6^9 \Longrightarrow (6^{12})^{26} \cdot 6^9 \equiv 1^{26} \cdot 6^9 (mod\, p)$$

$$6^2 = 36 = 26 + 10 \equiv 10(mod\, 13)$$

$$6^3 = 6^2 \cdot 6 \equiv 10 \cdot 6 = 60 = 52 + 8 \equiv 8(mod\, 13)$$

$$6^9 = (6^3)^3 = 8^3 = 512 = 13 \cdot 39 + 5 \equiv 5(mod\, p)$$

In conclusione

$$5648^{321} \equiv 5(mod\, p)$$

Proposizione 2. *La congruenza $ax \equiv b(mod\, n)$ ha soluzioni se e solo se $MCD(a,n)|b$.*

Dimostrazione. Risolvere la congruenza $ax \equiv b(mod\, n)$ equivale a risolvere l'equazione diofantea $ax \pm ny = b$. Sappiamo che è risolvibile se e solo se $MCD(a,n)|b$. □

Forma generale delle soluzioni di $ax \equiv b(mod\, n)$ quando $MCD(a,n)|b$. Se $x_0 \in \mathbb{Z}$ è una soluzione di $ax \equiv b(mod\, n)$ allora l'insieme di tutte e sole le soluzioni è

$$S = \{x_0 + k \cdot \frac{n}{d} | k \in \mathbb{Z}\}$$

Inoltre tra queste soluzioni abbiamo che $x_0, x_0 + \frac{n}{d}, x_0 + 2 \cdot \frac{n}{d}, \ldots, x_0 + (d-1)\frac{n}{d}$ queste sono tutte:

1. Non congruenti tra di loro $mod\, n$.
2. Ogni soluzione di $ax \equiv b(mod\, n)$ è congrua ad una sola di queste $mod\, n$

Dimostrazione.

1. Per assurdo prendiamo due indici $0 \leq i, j \leq d-1$ con $i \neq j$ e suppongo che $x_0 + i\frac{n}{d} \equiv x_0 + j\frac{n}{d}(mod\, n)$. Allora vale
$$i \cdot \frac{n}{d} \equiv j \cdot \frac{n}{d}(mod\, n)$$
cioè
$$(i-j) \cdot \frac{n}{d} \equiv 0(mod\, n)$$
Ricordo che $d = MCD(a,n)|n$. Quindi $n = d \cdot \frac{n}{d}$ con $\frac{n}{d} \in \mathbb{Z}$ quindi $(i-j) \cdot \frac{n}{d} = t \cdot n = t \cdot d \cdot \frac{n}{d}$ con $t \in \mathbb{Z}$. Trovo che $(i-j) = t \cdot d$ cioè $d|(i-j)$. Ora però $i < d$ e $j < d$ quindi $|i-j| < d$. Devo avere che $(i-j) = h \cdot d$ per $h \in \mathbb{Z}$ perché $d|(i-j)$ e $0 \leq |i-j| = |h| \cdot d < d$. L'unica possibilità è che $h = 0$ cioè $i - j = 0$ ovvero $i = j$.
2. Sia $x_0 + k\frac{n}{d}$ con $k \in \mathbb{Z}$ una arbitraria soluzione di $ax \equiv b(mod\, n)$. Prendo k e lo divido con resto per d. Allora esistono $q, r \in \mathbb{Z}$ tale che
$$k = qd + r \quad 0 \leq r \leq d.1$$
Abbiamo che $x_0 + k\frac{n}{d} = x_0 + (qd + r)\frac{n}{d} = x_0 + qn + r\frac{n}{d} = x_0 + r\frac{n}{d}(mod\, n)$

Corollario 2. *Se $MCD(a,n) = 1$ la congruenza $ax \equiv b(mod\, n)$ ammette infinite soluzioni intere che stanno in un'unica classe di congruenza modulo n.*

Esempio. $3x \equiv 1(mod\, 5)$ $a = 3$ $n = 5$ $b = 1$ $MCD(a,n) = d = 1$
Una soluzione banale è $x_0 = 2 \Longrightarrow$ tutte le soluzioni sono $x_0 + kn = 2 + 5k, k \in \mathbb{Z}$.Le soluzioni sono tutti gli elementi della classe $\overline{2} \in \mathbb{Z}_5$.

Teorema 4 (Teorema cinese del resto)**.** *Siano $m_1, m_2, \ldots, m_s \in \mathbb{N}$ positivi e tali che $MCD(m_i, m_j) = 1 \, \forall \, i \neq j$. Allora per ogni scelta di $r_1, r_2, \ldots, r_s \in \mathbb{Z}$ il sistema di congruenza*

$$\begin{cases} x_1 \equiv r_1(mod\, m_1) \\ x_2 \equiv r_2(mod\, m_2) \\ \vdots \\ x_s \equiv r_s(mod\, m_s) \end{cases}$$

ammette un'unica soluzione modulo $m_1 \cdot m_2 \cdot m_3 \cdot \cdots \cdot m_s$.

Dimostrazione. Chiamo $M = m_1 \cdot m_2 \cdot m_3 \cdot \cdots \cdot m_s$ e $M_i = \frac{M}{m_i}$ $\forall\, i = 1, 2, \ldots, s$.
Allora $MCD(M_i, m_i) = 1$ poiché $\forall\, k \neq i$ $MCD(m_j, m_i) = 1$. Quindi per ogni i la congruenza

$$M_i x \equiv r_i (mod\, m_i)$$

ha soluzione unica modulo m_i, chiamo x_i una soluzione particolare, questo lo posso fare $\forall\, i = 1, \ldots, s$.
Considero il numero

$$y = M_1 x_1 + M_2 x_2 + \cdots + M_s x_s$$

e vediamo che y risolve il sistema cioè che per ogni $i = 1, \ldots, s$

$$y \equiv r_i (mod\, m_i)$$

infatti

$$y = M_1 x_1 + M_2 x_2 + \cdots + M_s x_s \equiv 0 + 0 + \cdots + M_i x_i + 0 + \cdots + 0 \equiv M_i x_i \equiv r_i (mod\, m_i)$$

questo perchè x_i è soluzione di $M_i x \equiv r_i (mod\, m_i)$. □

Esempio.

$$\begin{cases} x \equiv 3 (mod\, 4) \\ x \equiv 2 (mod\, 3) \\ x \equiv 4 (mod\, 3) \end{cases} \implies \begin{array}{r} m_1 = 4 \quad m_2 = 3 \quad m_3 = 5 \\ M = m_1 \cdot m_2 \cdot m_3 = 60 \\ M_1 = \frac{60}{4} = 15 \quad M_2 = \frac{60}{3} = 20 \quad M_3 = \frac{60}{5} = 12 \end{array}$$

Per risolvere il sistema devo risolvere:

$$\begin{cases} 15 x_1 \equiv 3 (mod\, 4) \\ 20 x_2 \equiv 2 (mod\, 3) \\ 12 x_3 \equiv 4 (mod\, 5) \end{cases}$$

Quindi

$$\begin{cases} x_1 = 1 \\ x_2 = 1 \\ x_3 = 2 \end{cases}$$

La soluzione del sistema modulo 60 è

$$y = M_1 x_1 + M_2 x_2 + M_3 x_3 = 59$$

Definizione 8 (Funzione di Eulero)**.** *Sia* $n \in \mathbb{Z}_{>0}$

$$\varphi(n) = |\{1 \leq k \leq n | MCD(k, n) = 1\}|$$

Teorema 5 (Eulero-Fermat)**.** *Sia n un intero positivo e $a \in \mathbb{Z}$ tale che $(a.n) = 1$. Allora*

$$a^{\varphi(n)} \equiv 1 (mod\, n)$$

Definizione 9 (Unità)**.** *Sia A anello commutativo, le unità di A sono*

$$U(A) = \{a \in A | a\ invertibile\}$$

Proposizione 3. *Sia $n \in \mathbb{Z}$ $n \geq 2$ allora le unità dell'anello $\mathbb{Z}_n$ sono*

$$U(\mathbb{Z}_n) = \{\overline{k} | (k, n) = 1\}$$

Proposizione 4. *Sia $n \in \mathbb{Z}$ $n \geq 2$ allora ogni elemento diverso da $\overline{0}$ di $\mathbb{Z}_n$ è invertibile oppure un divisore dello zero.*

Dimostrazione. Se $\overline{a} \in \mathbb{Z}_n$ tale che $\overline{a} \neq \overline{0}$, ovvero $n \nmid a$, e $\overline{a} \in U(\mathbb{Z}_n)$, cioè $(a, n) = d \neq 1$. Quindi osservo che $\frac{n}{d}$ è un intero, $1 < \frac{n}{d} < n$; quindi $\overline{\frac{n}{d}} \neq \overline{0}$. Ma

$$\overline{a}\frac{\overline{n}}{d} = \frac{\overline{an}}{d} = \frac{\overline{a}}{d}\overline{n} = \frac{\overline{a}}{d}\overline{0} = \overline{0}$$

□

Dalla proposizione 3 segue

$$n \geq 2 \quad \varphi(n) = |U(\mathbb{Z}_n)|$$

Proprietà di φ.

1. Se $a, b \in \mathbb{Z}_{>0}$ tale che $(a, b) = 1$, allora $\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$
2. Se p primo positivo e $m \geq 0$ allora $\varphi(p^m) = p^{m-1}(p - 1)$

Esempio. $\varphi(2^3 \cdot 3^4 \cdot 5^2 \cdot 7) = \varphi(2^3)\varphi(3^4)\varphi(5^2)\varphi(7) = 25920$

Definizione 10 (Isomorfismo tra anelli)**.** *Siano A,B anelli commutativi, una funzione biunivoca $f : A \to B$ e tale che $\forall\, a_1, a_2 \in A$ vale:*

- $f(a_1 +_A a_2) = f(a_1) +_B f(a_2)$
- $f(a_1 \cdot_A a_2) = f(a_1) \cdot_B f(a_2)$
- $f(1_A) = 1_B$

si dice un isomorfismo tra A e B. A e B si dicono isomorfi e scrivo $A \simeq B$.

Definizione 11. *Siano A_1, A_2 anelli commutativi, su $A_1 \times A_2 = \{(a_1, a_2) | a_1 \in A_1, a_2 \in A_2\}$ definisco:*

- $(a_1, a_2) + (b_1, b_2) = (a_1 + b_1, a_2 + b_2)$
- $(a_1, a_2) \cdot (b_1, b_2) = (a_1 \cdot b_1, a_2 \cdot b_2)$

$A_1 \times A_2$ è un anello commutativo prodotto diretto di A_1 e A_2.

- $0_{A_1 \times A_2} = (0_{A_1}, 0_{A_2})$
- $1_{A_1 \times A_2} = (1_{A_1}, 1_{A_2})$
- $|A_1 \times A_2| = |A_1| \cdot |A_2|$ *se finite*

Teorema 6. *Sia n intero, $n \geq 2$, $n = a \cdot b$ con $a, b \in \mathbb{Z}$ interi positivi, $(a, b) = 1$. Allora l'anello*

$$Z_n \simeq \mathbb{Z}_a \times \mathbb{Z}_b$$

Dimostrazione. Provo che

$$\begin{array}{rccc} f\colon & \mathbb{Z}_n & \to & \mathbb{Z}_a \times \mathbb{Z}_b \\ & [x]_{\equiv_n} & \to & ([x]_{\equiv_a}, [x]_{\equiv_b}) \end{array}$$

è biettiva.
Per il teorema cinese dei resti, poiché $n = ab$ e $(a, b) = 1$ allora $\forall\, c, d \in \mathbb{Z}$ esiste un'unica soluzione di modulo n del sistema

$$\begin{cases} x \equiv c(mod\ a) \\ x \equiv d(mod\ b) \end{cases} \tag{5}$$

Quindi per ogni $([c]_{\equiv_a}, [d]_{\equiv_b}) \in \mathbb{Z}_a \times \mathbb{Z}_b$ esiste un unico $[x]_{\equiv_n}$ tale che $f([x]_{\equiv_n}) = ([c]_{\equiv_a}, [d]_{\equiv_b})$. Segue che f è suriettiva.
Suppongo che $x, y \in \mathbb{Z}$ tale che $f([x]_{\equiv_n}) = f([y]_{\equiv_n})$ ovvero $([x]_{\equiv_a}, [x]_{\equiv_b}) = ([y]_{\equiv_a}, [y]_{\equiv_b})$ e mostro che $[x]_{\equiv_n} = [y]_{\equiv_n}$.

$$\begin{cases} [x]_{\equiv_b} = [y]_{\equiv_a} \\ [x]_{\equiv_b} = [y]_{\equiv_b} \end{cases} \implies \begin{cases} a|(x-y) \\ b|(x-y) \end{cases}$$

Quindi $n = ab = mcm(a.b)|(x - y)$ ovvero $n|(x - y) \Rightarrow x \equiv y(mod\ n) \Rightarrow [x]_{\equiv_n} = [y]_{\equiv_n}$. Segue che f è iniettiva e quindi biettiva. Ora mostro le proprietà di un Isomorfismo tra anelli:

1. $$f([x_1]_{\equiv_n} + [x_2]_{\equiv_n}) = f([x_1 + x_2]_{\equiv_n} = ([x_1 + x_2]_{\equiv_a}, [x_1 + x_2]_{\equiv_b} =$$
   $$([x_1]_{\equiv_a}, [x_1]_{\equiv_b}) + ([x_2]_{\equiv_a}, [x_2]_{\equiv_b} = f([x_1]_{\equiv_n}) + f([x_2]_{\equiv_n}$$
2. Analogo ma con $\cdot$
3. $f([1]_{\equiv_n}) = ([1]_{\equiv_n}, [1]_{\equiv_n}) = 1_{\mathbb{Z}_a \times \mathbb{Z}_b}$

□

Proposizione 5. *Se $f : A \to B$ isomorfismo allora $U(B) = f(U(A))$ quindi*

$$|U(A)| = |U(B)|$$

perchè f è una biezione.

Corollario 3. *(a,b)=1* $\implies \varphi(a, b) = \varphi(a) \cdot \varphi(b)$

Dimostrazione. $\varphi(ab) = |U(\mathbb{Z}_{ab})|$ e $\mathbb{Z}_{ab} \simeq \mathbb{Z}_a \times \mathbb{Z}_b$. Per la proposizione 5 si ha che

$$|U(\mathbb{Z}_{ab} \simeq \mathbb{Z}_a \times \mathbb{Z}_b)| = |U(\mathbb{Z}_a) \times U(\mathbb{Z}_b)| = |U(\mathbb{Z}_a)| \cdot |U(\mathbb{Z}_b)| = \varphi(a)\varphi(b)$$

□

Proposizione 6. *Siano A,B anelli commutativi e $f : A \to B$ isomorfismo, allora $f_{U(A)} : U(A) \to U(B)$ è una biezione.*

Proposizione 7. *Siano A,B anelli commutativi, allora*

$$U(A \times B) = U(A) \times U(B)$$

4.5 Crittografia RSA

Si base sul fatto che la fattorizzazione in numeri primi di un numero è un problema non trattabile dal punto di vista computazionale. Ogni utente U possiede una coppia di interi positivi che è di dominio pubblico

$$(n_u, e_u)$$

- n_u, chiamato modulo, è il prodotto di due numeri primi distinti p, q che devono essere segreti e molto grandi, più di 200 cifre.
- e_u, chiamato esponente pubblico, è un intero positivo coprimo con $\varphi(n_u)$ ossia $MCD(e_u, \varphi(n_u)) = 1$. Osservo che
$$\varphi(n_u) = \varphi(p)\varphi(q) = (p-1)(q-1)$$
- Inoltre calcolo d_u, esponente privato, tale che
$$d_u e_1 \equiv 1 (mod\ \varphi(n_u))$$

Quindi la chiave pubblica è (n_u, e_u) e quella privata (n_u, d_u). La chiave del metodo RSA sta nel fatto che per calcolare d_u a partire da e_u non basta conoscere n_u ma serve sapere la sua fattorizzazione che, come già detto, è un problema non trattabile da un punto di vista computazionale.
Esempio. Siano A, B utenti e M messaggio. A vuole mandare un messaggio M a B. A procede andando nell'elenco delle chiavi pubbliche per cercare la chiave di B e se $M > n_b$ allora A dovrà spezzare M in vari blocchi che risultino minori di n_b.

$$\begin{cases} 1 < M < n_b \\ (M, n_b) = 1 \end{cases}$$

Ora A manda $M^{e_B} (mod\ n_B)$ e B decodifica il messaggio con il suo esponente private d_B:

$$(M^{e_B})^{d_B} = M^{e_B d_B} \equiv M (mod\ n_B)$$

ricordando che d_B è conosciuto solo a B per $e_B d_B \equiv 1 (mod\ \varphi(n_B))$ e teorema di Eulero-Fermat.
Per verificare che il messaggio sia effettivamente mandato da A, questo lo firma con una firma F, tramite il suo d_A

$$F^{d_A} \mod n_A)$$

e B lo trasforma con

$$(F^{d_A})^{e_A} \equiv F (mod\ n_A)$$

Quindi, riassumendo, il metodo si basa sull'elevato costo computazionale della fattorizzazione in primi e sul sistema di chiavi pubbliche e private.

Proposizione 8 (Test di primalità)**.** *Sia $n \in \mathbb{Z}$, allora se esiste $a \in \mathbb{Z}$ tale che*

$$a^n \not\equiv a (mod\, n)$$

allora n non è primo.

Teorema 7 (Teorema di Wilson)**.** *Sia $p \in \mathbb{P}$ primo, allora*

$$(p-1)! \equiv -1 (mod\, p)$$

5 Strutture Algebriche

Definizione 1 (Operazione binaria)**.** *Sia S insieme, un'operazione binaria su S è un' applicazione*

$$\begin{aligned} *\colon S \times S &\to S \\ (a,b) &\to a*b \end{aligned}$$

Esempi: $(\mathbb{Z},+)$, $(\mathbb{R},*)$

Definizione 2 (Semigruppo)**.** *Se $*$ è associativa cioè se $\forall\, a,b,c \in S$ vale $(a*b)*c = a*(b*c)$ allora l'insieme*

$$(S,*)$$

si chiama Semigruppo.

Definizione 3 (Monoide)**.** *Un Semigruppo $(S,*)$ che ha un elemento neutro $e \in S$ tale che $\forall\, a \in S$ vale $a*e = e*a = a$ si chiama Monoide.*

$$(S,*,e)$$

Osservazione 1. *Se S è un Monoide esiste un unico elemento neutro.*

Dimostrazione. Siano e e e' due elementi neutri per S, allora

$$e = e*e'$$

e

$$e' = e*e'$$

quindi

$$e = e'$$

□

Definizione 4 (Gruppo)**.** *Un gruppo è un Monoide $(G,*,e)$ tale che ogni elemento ha un inverso, cioè:*

- *$*$ è associativa*
- *Esempio. $e \in G$ elemento neutro $g*e = e*g = g\ \forall\, g \in G$*
- *$\forall\, g \in G$ esiste $g' \in G$ tale che $g*g' = g'*g = e$, g' si dice inverso di g.*

D'ora in poi scriveremo $(G,\cdot,1_G)$ al posto di $(G,*,e)$. Questa si chiama notazione moltiplicativa.

Osservazione 2. *Sia $(G,\cdot,1_G)$ un gruppo. Allora $\forall\, g \in G\ \exists\,!\ g^{-1} \in G$ tale che $g\cdot g^{-1} = g-1\cdot g = 1_G$. Inoltre vale*

$$(g^{-1})^{-1} = g \qquad (g\cdot h)^{-1} = g^{-1}\cdot h^{-1}$$

Dimostrazione. Siano g' e g'' due inversi per g. Allora

$$g' = 1_G \cdot g' = (g''\cdot g)g' = g''(g\cdot g') = g''\cdot 1_G = g''$$

□

Definizione 5 (Gruppo Abeliano)**.** *Un gruppo $(G, \cdot, 1_G)$ si dice Abeliano se $\cdot$ è commutativo cioè se $\forall\, g, h \in G$ vale $g \cdot h = h \cdot g$.*

Esempi di gruppi:

- $(\mathbb{Z}, +, 0)$ è un gruppo Abeliano.
- $(\mathbb{R}^*, \cdot, 1)$ è un gruppo Abeliano. $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$. L'inverso di $a \in \mathbb{R}^*$ è $a^{-1} = \frac{1}{a}$.
- $(\mathbb{Z}_n, +, \overline{0})$ è un gruppo Abeliano. L'inverso di $\overline{a}$ è $-\overline{a} = \overline{(-a)}$.
- $(U(\mathbb{Z}_n, \cdot, 1)$ è un gruppo abeliano di ordine $|U(\mathbb{Z}_n)| = \varphi(n)$.

Notazione additiva $(G, +, 1_G)$ utilizzata quando G è Abeliano.

Proposizione 1 (Legge di cancellazione)**.** *Siano $(G, \cdot, 1_G)$ un gruppo e siano $a, b, c \in G$. Allora:*

1. *Se $a \cdot b = a \cdot c \Longrightarrow b = c$*
2. *Se $b \cdot a = c \cdot a \Longrightarrow b = c$*

Dimostrazione.

$$b = 1_G \cdot b = a^{-1} \cdot a \cdot b = a^{-1}(ab) = a^{-1}(ac) = (a^{-1}a)c = 1_G \cdot c = c$$

□

5.1 Sottogruppi

Definizione 6. *Sia $(G, \cdot, 1_G)$ un gruppo e $H \subseteq G$. Allora diciamo che H è un sottogruppo (e scriveremo $H \leq G$) se:*

1. *$1_g \in H$*
2. *H è chiuso per inversi, cioè se $h \in H$ allora $h^{-1} \in H$*
3. *H è chiuso per il "prodotto" (si intende l'operazione definita sul gruppo), cioè se $x, y \in H$ allora $x \cdot y \in H$*

Esempio. $(\mathbb{Z}, +, 0)$ con $H = 3\mathbb{Z} = \{3z | z \in \mathbb{Z}\}$. Allora $H \leq \mathbb{Z}$. Infatti:

1. $0 = 0 \cdot 3 \in H$
2. $3z \in H \Longrightarrow -3z = 3(-z) \in H$
3. $3m + 3n = 3(m + n) \in H$

Proposizione 2. *Sia $(G, \cdot, 1_G)$ un gruppo e $H \subseteq G$. Allora $H \leq G$ se e solo se:*

- *$H \neq \emptyset$*
- *$\forall\, x, y \in H$ vale $x \cdot y^{-1} \in H$*

Dimostrazione. Dimostriamo la doppia implicazione.

$\implies$ Sia $H \leq G$ allora $1_G \in H$ e quindi $H \neq \emptyset$. Inoltre se $x, y \in H$ allora, poiché H è un sottogruppo, $y^{-1} \in H$ e $x \cdot y^{-1} \in H$.

$\impliedby$
1. Poiché $H \neq$ prendo $x \in H$ e allora $x \cdot x^{-1} = 1_G \in H$
2. Ora, se $h \in H$ faccio $\_G \cdot h^{-1} = h^{-1} \in H$
3. Infine, prendo $x, y \in H$, allora per il punto 2 $y^{-1} \in H$ e quindi $x(y^{-1})^{-1} = x \cdot y \in H$

□

Definizione 7 (Classe laterale sinistra)**.** *Siano G un gruppo, $H \leq G$ e $x \in G$. Definiamo il sottoinsieme di G*

$$xH = \{x \cdot h | h \in H\}$$

classe laterale sinistra di x modulo H. Inoltre su G definiamo una relazione binaria $\sim_H$ ponendo $\forall\, x, y \in G$ $x \sim_H y$ se $x^{-1}y \in H$ e se $y \in xH$.

Proposizione 3. *$\sim_H$ è una relazione di equivalenza.*

Dimostrazione. Verifico le tre proprietà:

1. Riflessiva, $\forall\, x \in G$ $x \sim_H x$. Infatti $x \sim_h x$ è vera se $x^{-1}x \in H$ e questo è vero perché $x^{-1}x = 1_H \in H$.
2. Simmetrica, suppongo che $x \sim_H y$ sia vera, allora $x^{-1}y \in H$, ora H è un sottogruppo quindi è chiuso per inversi, allora $(x^{-1}y)^{-1} \in H$. Ma $(x^{-1}y)^{-1} = y^{-1}(x^{-1})^{-1} = y^{-1}x \in H$ cioè $y \sim_H x$ è vera.
3. Suppongo
$$\begin{cases} x \sim_H y \\ y \sim_H z \end{cases} \implies \begin{cases} x^{-1}y \in H \\ y^{-1}z \in H \end{cases}$$
e quindi $(x^{-1}y)(y^{-1}z) = x^{-1}yy^{-1}z = x^{-1}z \in H$ cioè $x \sim_H z$. □

Osservazione 3. *Per ogni $x \in G$ considero la sua classe di equivalenza:*

$$[x]_{\sim_H} = \{y \in G | y \sim_H x\}$$

allora

$$\begin{gathered} x \sim_H y \iff x^{-1}y \in H \iff \exists\, h \in H \text{ t.c. } x^{-1}y = h \\ \iff x(x^{-1}y) = xh \text{ per un } h \in H \\ \iff y = xh \text{ per un } h \in H \iff y \in xH \end{gathered}$$

Definizione 8 (Indice)**.** *Sia $H \leq G$ sottogruppo di un gruppo G. Si chiama indice di H in G il numero di classi laterali distinte di H in G cioè*

$$|\frac{G}{\sim_H}| = [G : H]$$

Teorema 1 (Teorema di Lagrange)**.** *Sia G un gruppo di cardinalità finita $|G|$ e sia $H \leq G$. Allora*

$$|G| = [G : H] \cdot |H|$$

Dimostrazione. Proviamo innanzitutto che le classi laterali di G modulo H contengono ciascuna esattamente $|H|$ elementi. Infatti presa xH esiste una biezione tra H e xH

$$\begin{aligned} \sigma_x \colon H &\to xH \\ h &\to xh \end{aligned}$$

Mostro che σ_x è una biezione:

- σ_x è iniettiva. Siano $h, k \in H$ e sia $\sigma_x(h) = \sigma_x(k)$. Allora

  $$xh = xk \Rightarrow h = k$$

  Quindi σ_x è iniettiva.

- σ_x è suriettiva. Per come è definito xH.

Quindi σ_x è una biezione quindi $|H| = |xH|$ e questo vale $\forall\, x \in G$. Ora, poiché σ_x è una relazione di equivalenza, vale che la collezione di tutte le classi laterali sinistre di H in G è una partizione di G.
Se $[G : H] = n$ e $k_1, k_2, \ldots, k_n$ siano le n classi laterali distinte, $k_i = x_i H$). Allora

$$G = \bigcup_{i=1}^{n} k_i = k_1 \cup k_2 \cup \cdots \cup k_n$$

quindi

$$|G| = \sum_{i=1}^{n} |k_i| = \sum_{i=1}^{n} |H| = n|H| = [G : H]|H|$$

□

Corollario 1. *Se G è un gruppo finito e $H \leq G$ allora $|H|$ divide $|G|$.*

Definizione 9 (Potenza)**.** *Sia $(G, \cdot, 1_G)$ un gruppo e siano $g \in G$ e $z \in \mathbb{Z}$. Definiamo*

$$g^z = \begin{cases} g^0 = 1_g & \text{se } z = 0 \\ \underbrace{g \cdot g \cdot \cdots \cdot g}_{z \text{ volte}} & \text{se } z > 0 \\ \underbrace{g^{-1} \cdot g^{-1} \cdot \cdots \cdot g^{-1}}_{\text{-}z \text{ volte}} & \text{se } z < 0 \end{cases}$$

Proprietà:

- $g^{n+m} = g^n \cdot g^m = g^m \cdot g^n \;\forall\, m, n \in \mathbb{Z}$
- $g^{nm} = (g^n)^m$
- $g^{-n} = (g^{-1})^n = (g^n)^{-1}$

Osservazione 4. *Se $g, h \in G$ allora in generale $(g \cdot h)^2 = g \cdot h \cdot g \cdot h \neq g^2 \cdot h^2$.*

Definizione 10 (Sottogruppo ciclico generato)**.** *Sia G un gruppo e $g \in G$. Allora il sottogruppo ciclico generato di g è*

$$< g >:= \{g^z | z \in \mathbb{Z}\}$$

Questo è il più piccolo sottogruppo di g che contiene l'elemento g, cioè se $H \leq G$ e $g \in H$ allora $< g > \subseteq H$.

Definizione 11 (Ordine)**.** *Sia G un gruppo e $g \in G$ chiamiamo ordine di g, e scriveremo $|g|$ il più piccolo intero positivo $n \in \mathbb{N}$, $n \geq 1$, tale che $g^n = 1_G$, se esiste. Altrimenti $|g| = \infty$.*

Esempi:

- $(\mathbb{R}^*, \cdot, 1)$ con -1 ho che $(-1)^2 = 1$ quindi $|-1| = 2$
- $(\mathbb{Z}, +, 0)$ 1 ha ordine infinito rispetto a $+$. Infatti

$$g^z = z \cdot g = \begin{cases} 0_g \text{ se } z = 0 \\ g + g + \cdots + g \text{ se } z > 0 \\ (-g) + (-g) + \cdots + (-g) \text{ se } z < 0 \end{cases}$$

Allora $\forall\, n \in \mathbb{N}\ n \cdot 1 = 1 + 1 + \cdots + 1 = n \neq 0$ se $n \geq 1$. Quindi $|1| = \infty$

Osservazione 5. *Se $g \in G$ e $|g| = n$ allora $< g >= \{1_G, g, g^2, \ldots, g^{n-1}$ e $| < g > | = n$.*

Lemma 1. *Se G è un gruppo finito e $g \in G$, allora l'elemento $g^{|G|} = 1_G$*

Dimostrazione. Considero $< g >$. Vale $< g > \leq G$ quindi per il teorema di Lagrange $| < g > |$ divide $|G|$. Sia $n = | < g > |$ allora $n = | < g > |$ e posso scrivere $|G| = n \cdot k$ per qualche $k \in \mathbb{N}$. Quindi

$$g^{|G|} = g^{n \cdot k} = (g^n)^k = 1_G$$

□

Osservazione 6. *Se $|g| = n$ allora $| < g > | = n$ e $< g >= \{1_G, g, \ldots, g^{n-1}\}$ e $g^a = g^b \iff n|(a-b) \longleftrightarrow a \equiv b (mod\, n)$.*

Osservazione 7. *Se $|g| = \infty$ allora $< g >= \{g^z | z \in \mathbb{Z}\}$ e $g^a = g^b \iff a = b$.*

Dimostrazione. Se $g^a = g^b$ allora $g^{a-b} = g^a \cdot g - b = 1_G$ e allora poiché $|g| = \infty \Longrightarrow a - b = 0$ cioè $a = b$ □

Teorema 2. *Sia $n \in \mathbb{N}$ e sia $a \in \mathbb{Z}$ tale che $MCD(a, n) = 1$. Allora*

$$a^{\varphi(n)} \equiv 1 (mod\, n)$$

.

Dimostrazione. Sia $G = U(Z_n) = \{\overline{x} | MCD(x, n) = 1\}$ quindi $U(\mathbb{Z}_n), \cdot, \overline{1})$ è un gruppo Abeliano di ordine finito $|U(\mathbb{Z}_n)| = \varphi(n)$.
Preso $a \in \mathbb{Z}$ tale che $MCD(a, b) = 1$ allora $\overline{a} \in U(\mathbb{Z}_n)$. Per il lemma 1

$$(\overline{a})^{|U(\mathbb{Z}_n)|} = 1_{U(\mathbb{Z}_n)}$$

cioè

$$(\overline{a})^{\varphi(n)} = \overline{1}$$

quindi

$$(\overline{a^{\varphi(n)}}) = \overline{1}$$

ossia

$$a^{\varphi(n)} \equiv 1 (mod\, n)$$

□

Corollario 2. *Se $n = p \in \mathbb{P}$ allora $a^{p-1} \equiv 1 (mod\, n)$.*

5.2 Gruppi Simmetrici

Sia X insieme e sia

$$Sym(X) = \{f | f : X \to X \, biunivoche\} = \{permutazioni \, su \, X\}$$

.

Definizione 12 (Gruppo simmetrico)**.** $(Sym(X), \circ, id_x)$ *è un gruppo, detto gruppo simmetrico su* X*. Inoltre* $1_{Sym(X)} = id_x$*.*

Se $|X| = n < \infty$ allora $|Sym(X)| = n!$.

Definizione 13 (Supporto di f)**.** *Se* $f \in Sym(X)$ *si definisce supporto di f:*

$$supp(f) = \{x \in X | f(x) \neq x\}$$

Proposizione 4. *Siano* $f, g \in Sym(X)$*, se* $supp(f) \cap supp(g) = \emptyset$ *allora* $f \circ g = g \circ f$*. Si dice che sono due permutazioni a supporto disgiunto commutativo.*

Definizione 14 (Prodotto cicli disgiunti)**.** *Sia* $f \in Sym(X)$ *allora esiste una scrittura di f con prodotto di cicli disgiunti,* $f = c_1 c_2 \dots c_t$ *con* c_i $l_i - ciclo$ $i = 1, \dots, t$*. Tale scrittura è* <u>unica</u> *a meno dell'ordine dei cicli.*

Definizione 15. *L'ordine di f in Sym(X) è pari a*

$$o(f) = mcm(l_1, l_2, \dots, l_t)$$

dove l_i *è la lunghezza del ciclo.*

Definizione 16. *Data* $f \in G$ *con G gruppo finito, l'ordine di f è il minimo numero di applicazioni da ripetere per ottenere l'applicazione identica*

$$o(f) = min\{k \geq 1 | f^k = 1_G\}$$

Osservazione 8. *Data* $f \in G$ *con G gruppo finito e* $o(f) = min\{k \geq 1 | f^k = 1_G\}$ *allora*

$$f^k = 1_g \iff n | k \, per \, k \in \mathbb{Z}$$

Esempi:

1. $n = 7$ e $X = \{1, 2, 3, 4, 5, 6\}$ e siano

$$\begin{array}{l} \sigma : X \to X \\ 1 \to 4 \\ 2 \to 1 \\ 3 \to 3 \\ 4 \to 2 \\ 5 \to 6 \\ 6 \to 5 \end{array} \implies \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 1 & 3 & 2 & 6 & 5 \end{pmatrix} \qquad \begin{array}{l} \tau : X \to X \\ 1 \to 2 \\ 2 \to 3 \\ 3 \to 4 \\ 4 \to 1 \\ 5 \to 5 \\ 6 \to 6 \end{array} \implies \tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 4 & 1 & 5 & 6 \end{pmatrix}$$

Scriviamo le funzioni composte:

$$\sigma \circ \tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 3 & 2 & 4 & 6 & 5 \end{pmatrix} \quad \tau \circ \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 4 & 3 & 6 & 5 \end{pmatrix}$$

Attenzione $\sigma \circ \tau \neq \tau \circ \sigma$.
Scrittura più agevole:

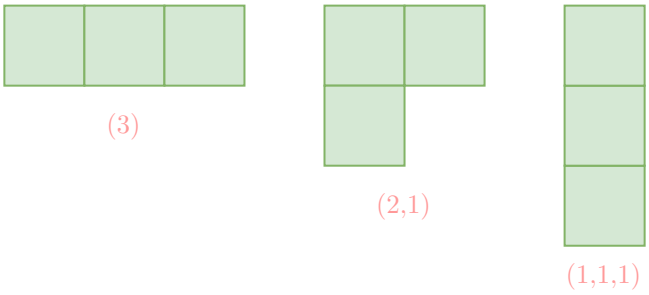
$$\sigma \circ \tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 1 & 3 & 2 & 6 & 5 \end{pmatrix} = (1,4,2)(3)(5,6) = (1,4,2)(5,6)$$

Per convenzione (3) non si riscrive perchè è un punto fisso.
Attenzione (1,4,2) si dice 3-ciclo, analogamente (5,6) è un 2-ciclo.

2. Sia f=(1 3 5 7)(8 9)(2 4 6) allora $o(f) = mcm(4,2,3) = 12$.

Definizione 17 (Partizione)**.** *Dato n numero intero positivo, il vettore $p = (l_1, l_2, \ldots, l_t)$ con $l_i \geq 1$ tale che $l_1 \geq l_2 \geq \ldots l_t$ e $l_1 + l_2 + \cdots + l_t = n$ allora p si definisce una partizione di n.*

Esempio. $n = 3$ $P(3) = 3$ $P(n)$ =numero di partizioni di n, infatti:



Definizione 18 (Relazione di coniugio)**.** *Dati $f, g \in Sym(X)$, si definisce la relazione di coniugio (relazione di equivalenza su Sym(X)):*

$$f \sim g \text{ se esiste } x \in Sym(X) \text{ tale che } g = x^{-1}fx.$$

Proposizione 5. *Se $|X| = n$ allora*

$$\frac{Sym(X)}{\sim} = P(n)$$

Definizione 19 (Trasposizione)**.** *Si definisce trasposizione un 2-ciclo.*

Scrittura di f permutazione come prodotto di trasposizioni:

1. Scrivo f come prodotto di cicli disgiunti $f = c_1 c_2 \dots c_t$ con c_i=cicli disgiunti.
2. per $c = (i, i_2, \dots, i_p)$ p-ciclo scrivo c come prodotto di trasposizioni

$$c = (i, i_p)(i, i_{p-1}) \dots (i, i_2)$$

Esempio. (1 2 3) = (1 3)(1 2) oppure (3 7 5 2) = (3 2) (3 5) (3 7)

Teorema 3. *Per $f \in Sym(X)$ se $f = t_1 \cdot t_2 \cdot t_3 \cdot \dots t_k = s_1 \cdot s_2 \cdot s_3 \cdot \dots s_h$ con $t_1, \dots, t_k$ e $s_1, \dots, s_h$ trasposizioni, allora*

$$k \equiv h (mod\, 2)$$

Definizione 20 (Segno di f)**.** *Il segno di $f = t_1 \cdot t_2 \dots t_k$ permutazione è definito come*

$$sgn(f) = \begin{cases} +1 \text{ se } k \text{ è pari} \\ -1 \text{ se } k \text{ è dispari} \end{cases}$$

Definizione 21. *Data f permutazione allora diremo che:*

- *f è pari se sgn(f)=1*
- *f è dispari se sgn(f)=-1*

Esempio. f=(1 2 3 4)(5 6 7)(8 9)=(1 4)(1 3)(1 2)(5 7)(5 6)(8 9) ha numero di trasposizioni pari a 6 quindi f è pari.

Osservazione 9. $sgn(f \circ g) = sgn(f) \cdot sgn(g)$

Definizione 22 (Gruppo alterno)**.** *Si definisce gruppo alterno su X*

$$Alt(X) = \{f \in Sym(X) | f \text{ è pari}\}$$

5.3 Algebra di Boole: punto di vista reticolare

Definizione 23 (Reticolo)**.** *Un insieme parzialmente ordinato* $(A, \trianglelefteq)$ *si dice reticolo se* $\forall\, a, b \in A$*:*

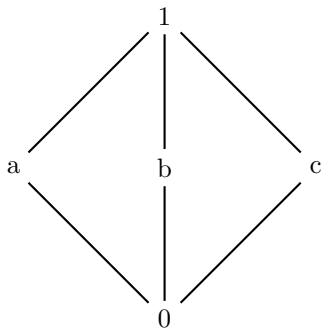
- $\exists\ inf_A(\{a, b\})$
- $\exists\ sup_A(\{a, b\})$

Definizione 24. *A reticolo si dice distributivo se* $\forall\, a, b, c \in A$*:*

- $a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$
- $a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$

Esempio. Dato X insieme e $A = P(X)$, ordinato per inclusione $\subseteq$, allora A è un reticolo distributivo. Vediamo due esempi di reticoli non distributivi:

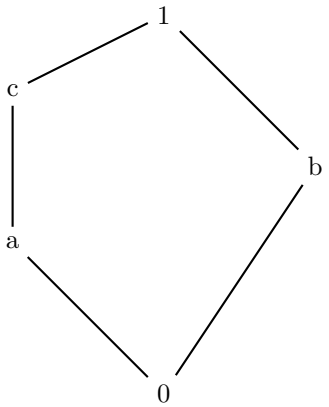
1. Reticolo **diamante**



   Questo reticolo non è distributivo, infatti:

   - $a \wedge (b \vee c) = a$
   - $(a \wedge b) \vee (a \wedge c) = 0$ e $a \neq 0$

2. Reticolo **pentagonale**:



Anche questo reticolo non è distributivo, infatti:

- $a \vee (b \wedge c) = a$
- $(a \vee b) \wedge (a \vee c) = c$ e $a \neq c$

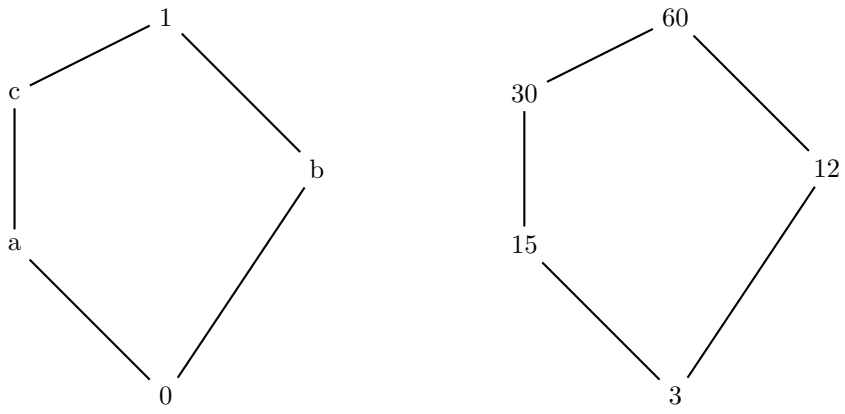
Definizione 25 (Sottoreticolo)**.** *Sia A un reticolo e sia $B \subseteq A$, B si dice un sottoreticolo di A se $\forall\, b, c \in B$ si ha :*

1. $b \wedge_A c \in B$
2. $b \vee_A c \in B$

Definizione 26. *Dati A_1, A_2 reticoli, $f : A_1 \to A_2$ si dice isomorfismo di reticoli se:*

- *f è biettiva*
- *$\forall\, x, y \in A$ vale:*
  - $f(x \wedge_{A_1} y) = f(x) \wedge_{A_2} f(y)$
  - $f(x \vee_{A_1} y) = f(x) \vee_{A_2} f(y)$

Esempio. Questi due reticoli sono isomorfi, ovvero hanno la stessa forma/struttura ma ne vengono cambiate le etichette.



Teorema 4. *Dato A reticolo, A è un reticolo distributivo se e solo se non ha sottoreticoli isomorfi al reticolo pentagonale o al reticolo diamante.*

Definizione 27. *A reticolo si dice complementato se è limitato e:*

1. $\exists\ 1 = max(A), \exists\ 0 = min(A)$
2. *$\forall\, a \in A, \exists\ \overline{a} \in A$ tale che:*
   - $a \vee \overline{a} = 1$
   - $a \wedge \overline{a} = 0$

   $\overline{a}$ si dice a complementato.

Esempio. Dato X insieme e $A = P(X)$ ordinato per $\subseteq$, per $Y \in A$ si ha che $\overline{Y} = X \setminus Y = C_X(Y)$

Definizione 28 (Algebra di Boole)**.** *Un'Algebra di Boole è un reticolo distributivo e complementato.*

Esempio. $X \neq \emptyset$ e $A = P(X)$ ordinato per inclusione $\subseteq$ allora $A = (P(X), \subseteq)$ è un Algebra di Boole. In questo caso:

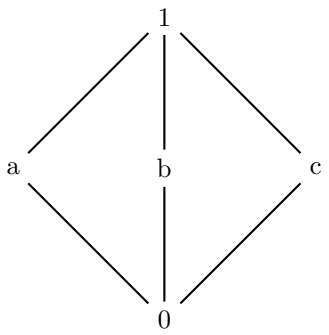
- $\wedge = \cap$
- $\vee = \cup$
- $1 = X$
- $0 = \emptyset$

Osservazione 10. *Dato n intero positivo, sia* $D_n = \{d \in \mathbb{Z}_{>0} |\ d|n\}$ *ordinato per divisibilità. Allora:*

- $(D_n, |)$ *è un reticolo distributivo, infatti* $\forall\, x, y \in D_n$*:*
  - $x \vee y = mcm(x, y)$
  - $x \wedge y = MCD(x, y)$
- D_n *è complementato se e solo se* $n = p_1 \cdot p_2 \dots p_k$ *con* $p_i \in \mathbb{P}$ *primi distinti.*

Osservazione 11. *Se A è un reticolo complementato non sempre il complemento è unico.*

Esempio. Nel reticolo diamante a ha due complementi che sono b e c.



Proposizione 6. *Se A è un reticolo distributivo e complementato, ovvero A è un Algebra di Boole, allora* $\forall\, a \in A$ *esiste un unico complemento di a,*$\overline{a}$*.*

Dimostrazione. Sia $a \in A$ e siano $b, c \in A$ tale che

$$\begin{cases} a \vee b = 1 \\ a \wedge b = 0 \end{cases} \qquad \begin{cases} a \vee c = 1 \\ a \wedge c = 0 \end{cases}$$

Allora

$$b = b \vee 0 = b \vee (a \wedge c) = (b \vee a) \wedge (b \vee c) = 1 \wedge (b \vee c) = (a \vee c) \wedge (b \vee c) = (a \wedge c) \vee c = a \vee c = c$$

Quindi $b = c$, il complemento di a è unico. □

5.4 Algebra di Boole: punto di vista algebrico

Considero $\vee$ e $\wedge$ come operazioni su A. Quindi sia $(A, +, \cdot, \bar{\cdot})$.

Proprietà:

1. Associativa, $\forall\, a, b, c \in A$:
   - $a + (b + c) = (a + b) + c$
   - $a \cdot (b \cdot c) = (a \cdot b) \cdot c$
2. Commutativa, $\forall\, a, b \in A$:
   - $a + b = b + a$
   - $a \cdot b = b \cdot a$
3. Distributiva $\forall\, a, b, c \in A$:
   - $a + (b \cdot c) = (a + b) \cdot (a + c)$
   - $a \cdot (b + c) = ab + ac$
4. Assorbimento, $\forall\, a, b \in A$:
   - $a + (a \cdot b) = a$
   - $a \cdot (a + b) = a$
5. Esistono $0, 1 \in A$ tale che $\forall\, a \in A$:
   - $a + 0 = a$
   - $a \cdot 0 = 0$
   - $a + 1 = 1$
   - $a \cdot 1 = a$
6. Complemento, $\forall\, a \in A$ esiste $\overline{a} \in A$ tale che:
   - $a \cdot \overline{a} = 0$
   - $a + \overline{a} = 1$
7. Leggi di De Morgan, $\overline{a + b} = \overline{a} \cdot \overline{b}$ e $\overline{a \cdot b} = \overline{a} + \overline{b}$
8. $\overline{\overline{a}} = a$

Ora, dato $(A, +, \cdot, \bar{\cdot})$ con le proprietà enunciate, definisco una relazione d'ordine $\leq$ su A ponendo per $a, b \in A$ $a \leq b$ se $a \cdot b = a$ oppure $a + b = b$. Allora $\leq$ è riflessiva, antisimmetrica e transitiva, ovvero $(A, \leq)$ insieme parzialmente ordinato è un reticolo distributivo e complementato, dove $\forall\, a, b \in A$ vale:

$$\begin{cases} a \vee b = a + b \\ a \wedge b = a \cdot b \end{cases}$$

A è un algebra di Boole, definita dal punto di vista algebrico. Quindi un algebra di Boole può essere definita a seconda dei due punti di vista, algebrico e reticolare, che sono tra loro equivalenti poiché

quello che si ottiene è la stessa struttura matematica.

Principio di Dualità. *Ogni proposizione universalmente vera in un'algebra di Boole, rimane universalmente vera scambiando + con · e 0 con 1.*

Proposizione 7. *Sia n intero positivo e $(D_n, |)$, se $p^2|n$, con $p \in \mathbb{P}$, allora $(D_n.|)$ non è complementato.*

Dimostrazione. $p \in D_n$ non ha complemento. Infatti se $a \in D_n$ fosse un complemento, allora

$$\begin{cases} a \vee p = mcm(a,p) = max(D_n) = n \\ a \wedge p = \underbrace{MCD(a,p)}_{\text{ovvero } p \nmid a} = 1 = min(D_n) \end{cases}$$

quindi $p^2 \nmid MCD(a,p)$ quindi è diverso da n. Quindi non esiste un complemento.

Definizione 29 (Atomo)**.** *Sia $(A, \leq)$ un insieme parzialmente ordinato dotato di $0 = min(A)$. Un elemento $a \in A$, $a \neq 0 = min(A)$, si dice atomo di A se è un elemento minimale in $(A \setminus \{0\}, \leq)$.*

Definizione 30 (Atomo alternativa)**.** *Sia $x \in B$ algebra di Boole e $x \neq 0$, è un atomo se per ogni $y \leq x$ vale $y = x$ oppure $y = 0$.*

Osservazione 12. *$x \neq 0$ x è un atomo $\iff$ per $u, v \in B$ se $x = u + v$ allora $u, v \in \{0, x\}$.*

Osservazione 13. *$a \cdot x = x \iff x \leq a$ quindi $a \cdot x = 0 \iff x \not\leq a$*

Lemma 2. *Sia $x \in B$, algebra di Boole, un atomo. Allora:*

1. *$\forall\, a \in B$ vale $a \cdot 0 = 0$ oppure $a \cdot x = x$*
2. *$\forall\, x_1, x_2$ atomi tale che $x_1 \neq x_2$ vale $x_1 \cdot x_2 = 0$*

Dimostrazione.

1. Per osservazione 13 $a \cdot x \leq x$ quindi $a \cdot x = \{0, x\}$
2. Se $x_1 \neq x_2$ allora $x_1 \leq x_2$ e $x_2 \leq x_1$ quindi $x_1 \cdot x_2 = 0$ □

Proposizione 8. *Se B algebra di Boole, $|B|$ finita. Sia $X = \{x \in B | x \text{ atomo di } B\}$. Allora $X \neq \emptyset$ e se $a \in B$ è tale che $a \cdot x = 0$ $\forall\, x \in X$, allora a=0.*

Dimostrazione. Se per assurdo $a \neq 0$, quindi $Y = \{y \in B | y \leq x,\ y \neq 0\} \neq \emptyset$ finito. Dunque esiste almeno un elemento minimale $x_0 \in Y$ rispetto alla relazione d'ordine indotta.
x_0 è un atomo di B, infatti $x_0 \neq 0$ e se $y \in B, y \neq 0$ tale che $y \leq x_0$ ma $x_0 \leq a$ quindi per transitività $y \leq a$ dunque $y \in Y$, poiché x_0 minimale in Y segue $y = x_0$.
Poiché $x_0 \leq a$, vale $a \cdot x_0 = x_0$ ma x_0 è un atomo, ovvero $x_0 \in X$ di B e per ipotesi $a \cdot x_0 = 0$ e questo è assurdo perchè $x_0 \neq 0$. □

Teorema 5 (Teorema di rappresentazione)**.** *Sia B algebra di Boole finita. Allora ogni $a \in B, a \neq 0$, si scrive in modo unico come somma di atomi di B, a meno dell'ordine degli addendi. Ovvero*

$$a = \sum_{x \in X_a} x \text{ con } X_a \subseteq X = \{\text{atomi di } B\}, X_a = \{x \in X | x \leq a\}$$

Dimostrazione. Siano $a \in B$, $a \neq 0$, $X = \{x \in B | x \text{ atomo}$ e $X_a = \{x \in X | x \leq a\}$.
Dimostro l'esistenza.
Chiamo

$$b = \sum_{x \in X_a} x$$

e provo che $b = a$.

- Provo che $a \cdot b = b$ infatti

$$a \cdot b = a \cdot \sum_{x \in X_a} x = \sum_{x \in X_a} ax = \sum_{x \in X_a} x = b$$

- Provo che $a \cdot \overline{b} = 0$ mostrando che $(a \cdot \overline{b})y = 0 \; \forall \, y \in X$.

  1. Se $y \in X_a$, ricordando che

$$\overline{b} = \overline{\sum_{x \in X_a} x} \underbrace{=}_{De\ Morgan} \prod_{x \in X_a} \overline{x}$$

  allora

$$(a\overline{b})y = a \prod_{x \in X_a} \overline{x}y = a(\prod_{x \in X_a \wedge x \neq y} \overline{x}) \underbrace{y\overline{y}}_{=0} = 0$$

  2. Se invece $y \notin X_a$, allora $ay = 0$ e quindi

$$a\overline{b}y = ay\overline{b} = 0 \cdot \overline{b} = 0$$

Dunque

$$a = a \cdot 1 = a(b + \overline{b}) = a \cdot b + a \cdot \overline{b} = b + 0 = b$$

Dimostro l'unicità.
Siano$X_1, X_2 \subseteq X$ tale che $a = \sum_{x \in X_1} x = \sum_{y \in X_2} y$. Provo che $X_1 = X_2$.

$\subseteq$ Sia $x_1 \in X_1$, allora

$$ax_1 = (\sum_{x \in X_1} x)x_1 = \sum_{x \in X_1} xx_1 = x_1 = 0$$

inoltre

$$0 \neq x_1 = ax_1 = (\sum_{y \in X_2} y)x_1 = \sum_{y \in X_2} yx_1$$

quindi esiste $y \in X_2$ tale che

$$y = x_1$$

ovvero $X_1 \subseteq X_2$

$\supseteq$ Si dimostra in modo analogo.

□

Teorema 6 (Teorema di struttura)**.** *Sia B algebra di Boole finita e sia* $X = \{x | x \text{ atomo di } B\}$. *Allora B è isomorfa all'algebra di Boole di P(X).*

Dimostrazione. Definisco $f : B \to P(X)$ ponendo $f(0) \neq \emptyset$ e, per $a \in B$ con $a \neq 0$, scrivo

$$a = \sum_{x \in X_a} x$$

e definisco $f(a) = X_a$ univocamente determinato. Provo che f è invertibile, infatti:
Sia $g : P(X) \to B$ tale che

$$g(Y) = \sum_{x \in Y} x \in B$$

se $Y \notin \emptyset$ e $g(\emptyset) = 0$. Verifico che

$$\begin{cases} g \circ f = i_B \\ f \circ g = i_{P(X)} \end{cases}$$

Segue che f è biettiva poiché invertibile e quindi è un isomorfismo. □

6 Logica

Definizione 1 (Proposizione)**.** *Una proposizione è un enunciato che può assumere solo valori vero o falso.*

Vero è indicato con il simbolo "1" mentre falso con il simbolo "0".
Esempi:

1. "due è un numero pari", Vero
2. "Esistono infinite coppie di primi (p, q) con $p, q \in \mathbb{P}$ tale che $q = p + 2$, non si può dimostrare.
3. "Che ore sono?", non è una proposizione
4. "Questa affermazione è falsa", non è una proposizione

6.1 Linguaggio della logica proposizionale

Chiamo alfabeto

$$A = L \cup \{\wedge, \vee, \neg, \to, \leftarrow\} \cup \{), (\}$$

dove L è l'insieme delle variabili proposizionali.

Definizione 2 (Formula)**.** *Una stringa α di simboli dell'alfabeto A è una formula se è del tipo:*

1. $\alpha \in L$
2. $\alpha = \neg\beta$ *con* β *formula.*
3. $\alpha = (\beta \wedge \gamma)$*, si può sostituire il connettivo logico* $\wedge$ *con un qualsiasi altro.*

Esempio. Siano $a, b, c \in L$ allora:

- $(a \vee (b \to \neg c))$ formula
- $(a \to b \to c)$ non è una formula perché ambigua
- $(a \to (b \to c))$ formula

Connettivi logici e valori di verità:
Siano α, β proposizioni, allora:

α	$\neg\alpha$
0	1
1	0

α	β	$\alpha \wedge \beta$
0	0	0
0	1	0
1	0	0
1	1	1

α	β	$\alpha \vee \beta$
0	0	0
0	1	1
1	0	1
1	1	1

α	β	$\alpha \to \beta$
0	0	1
0	1	1
1	0	0
1	1	1

α	β	$\alpha \longleftrightarrow \beta$
0	0	1
0	1	0
1	0	0
1	1	1

Osservazione 1. *$\alpha \to \beta$ è sempre vera tranne nel caso in cui α è vera e β è falsa.*

Esempio.

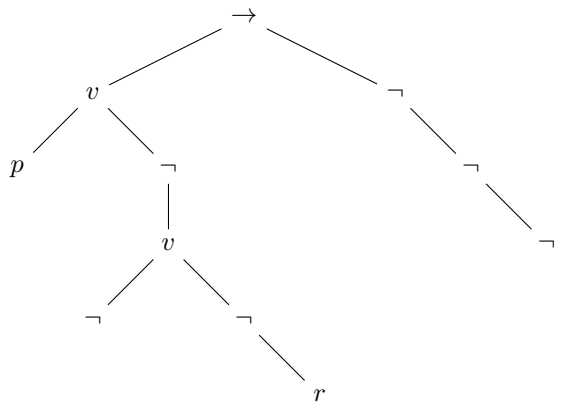
$$\underbrace{\text{"Se due è dispari}}_{\alpha} \text{ allora } \underbrace{\text{il sole gira intorno alla Terra"}}_{\beta}$$

La premessa α è falsa quindi qualsiasi sia l'implicazione β, l'implicazione è vera.

Semantica. (Assegnazione di valori di verità)
Sia $Form(L)$ l'insieme delle formule dell'alfabeto A. Data una valutazione $v : L \to \{0,1\}$ definisco $\widetilde{v} : Form(L) \to \{0,1\}$ nel seguente modo:

- $a \in L$, pongo $\widetilde{v}(\alpha) = v(\alpha)$
- $\alpha = \neg\beta$, con β formula, pongo
$$\widetilde{v}(\alpha) = \begin{cases} 1 \text{ se } \widetilde{v}(\beta) = 0 \\ 0 \text{ se } \widetilde{v}(\beta) = 1 \end{cases}$$
- $\alpha = \beta \wedge \gamma$ allora pongo $\widetilde{v}(\alpha) = min(\widetilde{v}(\beta), \widetilde{v}(\gamma))$
- $\alpha = \beta \vee \gamma$ allora pongo $\widetilde{v}(\alpha) = max(\widetilde{v}(\beta), \widetilde{v}(\gamma))$
- $\alpha = \beta \to \gamma$ allora pongo
$$\widetilde{v}(\alpha) = \begin{cases} 0 \text{ se } \widetilde{v}(\beta) = 1 \text{ e } \widetilde{v}(\gamma) = 0 \\ 1 \text{ altrimenti} \end{cases}$$
- $\alpha = \beta \longleftrightarrow \gamma$ allora pongo
$$\widetilde{v}(\alpha) = \begin{cases} 1 \text{ se } \widetilde{v}(\beta) = \widetilde{v}(\gamma) \\ 0 \text{ altrimenti} \end{cases}$$

Esempio. Sia $(p \vee \neg(q \wedge \neg r)) \to (\neg\neg r))$, costruiamo l'**albero di Parsing**



Valutazione:

$$\begin{cases} p = 1 \\ q = 0 \\ r = 1 \end{cases} \implies v(\alpha) = 1$$

Definizione 3 (Formula soddisfacibile)**.** *Una formula α si dice soddisfacibile se esiste almeno una valutazione v tale che $v(\alpha) = 1$ e si dice che α è vera mediante la valutazione v.*

Definizione 4 (Tautologia)**.** *α è una tautologia se per ogni valutazione v vale $v(\alpha) = 1$.*

Definizione 5 (Contraddizione)**.** *α è una contraddizione se per ogni valutazione v vale $v(\alpha) = 0$.*

Definizione 6 (Conseguenza logica)**.** *Date due formule $\alpha, \beta \in Form(L)$ dico che β è conseguenza logica di α, scrivo $\alpha \models \beta$, se per ogni valutazione v tale che $v(\alpha) = 1$ vale $v(\beta) = 1$.*

Definizione 7. *Date due formule $\alpha, \beta \in Form(L)$ dico che α e β sono logicamente equivalenti, scrivo $\alpha \equiv \beta$, se per ogni valutazione v vale $v(\alpha) = v(\beta)$.*

Esempi:

1. $(a \to b) \wedge \neg c$ soddisfacibile ma non tautologia
2. $(a \vee \neq a)$ tautologia
3. $(a \wedge \neq a$ contraddizione, cioè non soddisfacibile
4. $\alpha \wedge \beta \models \alpha$ per ogni $\alpha, \beta \in Form(L)$
5. $\alpha \equiv \neg\neg\alpha$

Equivalenze logiche:

- $\alpha \to \beta$ è logicamente equivalente a $\neg\beta \to \neg\alpha$, la seconda formula è la contronominale della prima.

α	β	$\alpha \to \beta$	$\neg\beta$	$\neg\alpha$	$\neg\beta \to \neg\alpha$
1	1	1	0	0	1
1	0	0	1	0	0
0	1	1	0	1	1
0	0	1	1	1	1

- $\alpha \to \beta \equiv \neg\alpha \vee \beta$

α	β	$\alpha \to \beta$	$\neg\alpha$	β	$\neg\alpha \vee \beta$
1	1	1	0	1	1
1	0	0	0	0	0
0	1	1	1	1	1
0	0	1	1	1	1

- $\alpha \longleftrightarrow \beta \equiv (\alpha \to \beta) \wedge (\beta \to \alpha) \equiv (\neq \alpha \vee \beta) \wedge (\neg\beta \vee \alpha)$, questo come conseguenza ha che per ogni α formula, esiste $\alpha' \in Form(L)$ tale che $\alpha' \equiv \alpha$ e in α' compaiono solo connettivi $\neg, \wedge, \vee$.
- Per le leggi di De Morgan $\neg(\alpha \wedge \beta) \equiv \neg\alpha \vee \neg\beta$ quindi $\alpha \wedge \beta \equiv \neg(\neg\alpha \vee \neg\beta)$

Osservazione 2. *Ogni formula può essere scritta usando il connettivo logico NOR.*

α	β	$\alpha \downarrow \beta$
1	*1*	*0*
1	*0*	*0*
0	*1*	*0*
0	*0*	*1*

Definizione 8 (Conseguenza logica)**.** *Date $\alpha_1, \alpha_2, \ldots, \alpha_n, \beta \in Form(L)$ allora $\alpha_1, \alpha_2, \ldots, \alpha_n \models \beta$ se per ogni valutazione di verità v tale che $v(\alpha_1) = v(\alpha_2) = \cdots = v(\alpha_n) = 1$ vale anche $v(\beta) = 1$.*

Osservazione 3. *$\alpha_1, \alpha_2, \ldots, \alpha_n \models \beta$ equivale a $\alpha_1 \wedge \alpha_2 \wedge \cdots \wedge \alpha_n \models \beta$.*

6.2 Forma normale congiuntiva (FNC)

Definizione 9 (Letterale)**.** *a oppure $\neg a$ con $a \in L$ variabile proposizionale.*

Definizione 10 (Disgiunzione elementare)**.** *$l_1 \vee l_2 \vee \cdots \vee l_n$ con l_i letterale per $i \in [1, n],\ n \geq 1$*

Definizione 11 (FNC)**.** *$\alpha \in Form(L)$ è in FNC, forma normale congiuntiva se,*

$$\alpha = \alpha_1 \wedge \alpha_2 \wedge \cdots \wedge \alpha_m$$

con α_i disgiunzione elementare per ogni $1 \leq i \leq m$ e $m \geq 1$.

Esempio. Siano $a, b, c \in L$ variabili proposizionali. Allora:

- $a \vee b \vee \neg a$ è in FNC e disgiunzione elementare
- $(a \vee b \vee \neg c) \wedge (b \vee \neg a)$ è in FNC.

Analogamente posso definire la forma normale disgiuntiva scambiando $\wedge$ e $\vee$.

Proposizione 1. *Per ogni formula α esiste una formula α' tale che $\alpha' \equiv \alpha$ e α' è in FNC.*

Algoritmo di trasformazione in FNC:

1. Elimino $\to, \longleftrightarrow$, usando le equivalenze logiche, e ottengo $\alpha_0 \equiv \alpha$ tale che α_0 contiene solo $\neg, \wedge, \vee$.

2. usando le leggi di De Morgan porto $\neg$ accanto alle variabili proposizionali. Per esempio

$$(\neg(\alpha \to \beta)) \equiv \neg(\neg\alpha \vee \beta) \equiv \neg\neg\alpha \wedge \neg\beta \equiv \alpha \wedge \neg\beta$$

3. Uso, eventualmente, le leggi distributive.

Esempio.

$$(a \wedge \neg c) \to (a \longleftrightarrow \neg b) \equiv)\neg(a \wedge \neg c) \vee ((a \to \neg b) \wedge (\neg b \to a)) \equiv$$
$$\neg(a \wedge \neg c) \vee ((\neg a \vee \neg b) \wedge (b \vee a)) \equiv (\neg a \vee c) \vee ((\neg a \vee \neg b) \wedge (b \vee a)) \equiv$$
$$((\neg a \vee c) \vee (\neg a \vee \neg b)) \wedge ((\neg a \vee c) \vee (b \vee a)) \equiv$$
$$(\neg \vee c \vee \neg a \vee \neg b) \wedge (\neg a \vee c \vee b \vee c) \equiv$$
$$\neg a \vee \neg b \vee c$$

Definizione 12. *Insieme di letterali, interpreto $\{l_1, l_2, \ldots, l_n\}$, con l_i letterali, come $l_1 \vee l_2 \vee \cdots \vee l_n$. Un insieme di clausole $\{c_1, c_2, \ldots, c_m\}$, con c_i clausole e $c_i = \{l_{i1}, \ldots, l_{ij}\}$, lo interpreto come*

$$(l_{11} \vee l_{12}, \vee \cdots \vee l_{1j}) \wedge (l_{21} \vee l_{22}, \vee \cdots \vee l_{2j}) \wedge (\ldots) \ldots$$

Esempio. Riprendendo l'esempio precedente la scrittura in clausole di $(\neg \vee c \vee \neg a \vee \neg b) \wedge (\neg a \vee c \vee b \vee c) \equiv$ è la seguente

$$\{\{\neg a, c, \neg a, \neg b\}, \{\neg a, c, b, a\}\} = S_\alpha = \text{Insieme di Clausole}$$

Trasferiamo la semantica da formule FNC a insieme di clausole:

1. Per $c = \{c_1, \ldots, c_n\}$ clausola, v valutazione, $v(c) = 1$ se e solo se $v(l_i) = 1$ per almeno una c_i.
2. Per $S = \{C_1, C_2, \ldots, C_m\}$ insieme di clausole, v valutazione, $v(S) = 1$ se e solo se $v(C_i) = 1$ per ogni C_i.

Notazione:
$\square$ = clausola vuota: $v(\square) = 0$ per ogni valutazione, ossia insoddisfacibile.
$=$ insieme di clausole vuoto: $v(\{\}) = 1$ per ogni valutazione, ossia tautologia.

Definizione 13 (Risolvente)**.** *Date due clausole $C = \{x_1, x_1, \ldots, x_k, a\}$ e $D = \{y_1, y_2, \ldots, y_t, \neg a\}$ con x_i, y_j letterali e a variabile proposizionale. Si chiama risolvente*

$$Ris_a(C, D) = \{x_1, \ldots, x_k, y_1, \ldots, y_y\}$$

con $x_i, y_j \neq a$ e $\neg a$.

6.3 Algoritmo di Davis-Putnam

L'algoritmo di Davis-Putnam è utilizzato per provare la soddisfacibilità di una formula.

1. Elimino le tautologie
2. Scelgo una variabile proposizionale a, chiamata *pivot*
3. Costruisco un nuovo insieme di clausole così costituito

   $S' = \{$clausole che non contengono ne a ne $\neg a\} \cup \{Ris_a(C, D)$ dove $C, D \in S$, $a \in C$ e $\neg a \in D\}$

Ora, abbiamo che S formula è soddisfacibile se e solo se S' è soddisfacibile. Ripetendo il procedimento alla fine ottengo o un insieme di vuote di clausole , oppure una clausola vuota $\square$. Distinguo due casi:

1. in questo caso S è soddisfacibile
2. $\square$ S è insoddisfacibile

Osservazione 4. *A ogni passaggio dell'algoritmo mantengo la soddisfacibilità.*

Esempio. Verificare la validità di $(a \to c) \wedge (b \to c) \models (a \vee b) \to c$.
Questo equivale a verificare che $(a \to c) \wedge (b \to c) \wedge \neg((a \vee c) \to c)$ è insoddisfacibile.
In clausole:

$$S = \{\{\neg a, c\}, \{\neg b, c\}, \{a, b\}, \{\neg c\}\}$$

1. Scelgo pivot a e ottengo $S_1 = \{\{\neg b, c\}, \{\neg c\}, \{b, c\}\}$
2. Scelgo pivot c e ottengo $S_2 = \{\{\neg b\}, \{b\}\}$
3. Scelgo pivot b e ottengo $S_3 = \{\square\}$ quindi S è insoddisfacibile.

Esempio. Insieme di clausole:

$$S = \{\{a, b\}.\{c, d\}, \{e, f\}, \{\neg a, \neg b\}, \{\neg c, \neg d\}, \{\neg e, \neg f\}, \{\neg a, \neg c\}, \{\neg b, \neg d\}, \{\neg c, \neg e\}, \{\neg d, \neg f\}\}$$

1. Pivot a: $S_1 = \{\{c.d\}, \{e, g\}, \{\neg c, \neg d\}, \{\neg e, \neg f\}, \{\neg b, \neg d\}, \{\neg c, \neg e\}, \{\neg d, \neg f\}, \{b, \neg b\}, \{b, \neg c\}\}$
2. Pivot b: $S_2 = \{\{c.d\}, \{e, f\}, \{\neg c, \neg d\}, \{\neg e, \neg f\}, \{\neg c, \neg e\}, \{\neg d, \neg f\}, \{\neg c, \neg d\}\}$
3. Pivot c: $S_3 = \{\{e, f\}, \{\neg e, \neg f\}, \{\neg d, \neg f\}, \{d, \neg d\}, \{d, \neg e\}\}$
4. Pivot d: $S_4 = \{\{e, f\}, \{\neg e, \neg f\}, \{\neg e, \neg f\}\}$
5. Pivot e: $S_5 = \{\{f, \neg f\}\} = \{\}$ Insieme vuoto di clausole quindi S_1 è soddisfacibile.

Trovare v valutazione che soddisfi S_i:

- f è una variabile esodata quindi posso scegliere $v(f)$.
- Assegno $v(e) = 1$ per rendere vera S_4
- Assegno $v(d) = 1$ per rendere vera S_3
- Assegno $v(c) = 0$ per rendere vera S_2
- Assegno $v(b) = 0$ per rendere vera S_1
- Assegno $v(a) = 1$ per rendere vera S

$$v = \begin{cases} a \to 1 \\ b \to 0 \\ c \to 0 \\ d \to 1 \\ e \to 1 \\ f \to 0 \end{cases}$$

Esempio. Trovare se la seguente formula è soddisfacibile o tautologia

$$\varphi := ((c \to (d \wedge f) \wedge ((e \vee f) \to a) \wedge ((c \wedge f) \to b)) \to (c \to b)$$

φ è una tautologia $\iff \neg\varphi$ insoddisfacibile. Quindi:

$$\neg\varphi := \neg(\neg(\dots) \vee (c \to b)) \equiv (\dots) \wedge \neg(c \to b) \equiv$$

$$((\neg c \vee (d \wedge f) \wedge (\neg(e \vee f) \vee a) \wedge (\neg(c \wedge f) \vee b)) \wedge \neg(\neg c \vee b) \equiv$$

$$((\neg c \vee d) \wedge (\neg c \vee f) \wedge ((\neg e \vee a) \wedge (\ \vee \neg f) \wedge (\neg c \vee \neg f \vee b) \wedge c \wedge \neg b$$

In clausole:

$$S_1 = \{\{\neg c, d\}, \{\neg c, f\}, \{\neg e, a\}, \{a, \neg f\}, \{\neg c, \neg f, b\}, \{c\}, \{\neg b\}\}$$

Osservo che a, d sono variabili monopolari $\Rightarrow$ elimino clausole in cui compare.

1. Pivot c: $S_2 = \{\{\neg b\}, \{f\}, \{\neg f, b\}\}$
2. Pivot b: $S_3 = \{\{f\}, \{\neg f\}\}$
3. Pivot f: $S_4 = \{\square\}$

Quindi S_1 è insoddisfacibile ovvero $\neg\varphi$ è insoddisfacibile e quindi φ è una tautologia.

Proposizione 2. *Sia S insieme di clausole, scelgo pivot a e sia S' l'insieme di clausole ottenuto applicando l'algoritmo di Davis-Putnam su S con pivot a. Allora S è soddisfacibile (SAT) se e solo se S' è SAT, ossia S e S' sono equisoddisfacibili.*

Dimostrazione.

$\Rightarrow$ Suppongo S soddisfacibile ovvero esiste valutazione v tale che $v(S) = 1$, provo che anche $v(S') = 1$ cioè $S \models S'$.

$$S' = \{\{\textit{Clausole di S a-esonerate}\} \cup \{Ris(C, D) | C, D \in S \ \textit{t.c.}\ a \in C \wedge \neg a \in D\}\}$$

Se $C \in S$ clausola a-esonerata, $C \in S'$ e $v(C) = 1$. Considero $Ris_a(C, D) \in S'$ con $C, D \in S$, $a \in C$ e $\neg a \in D$. Poiché $v(S) = 1$ in parte $v(C) = 1 = v(D)$. Siano

$$C = \{x_1, \dots, x_k, a\} \quad D = \{y_1, \dots, y_h, \neg a\} \quad x_i, y_j \neq a, \neg a$$

allora

$$Ris_a(C, D) = \{x_1, \dots, x_k, y_1, \dots, y_h\}$$

1. Se $v(a) = 0$ allora esiste i tale che $v(x_i) = 1$ con $1 \leq i \leq k$ perchè $v(C) = 1$. Dunque
$$v(Ris_a(C, D)) = 1$$
2. Se $v(a) = 1$ allora esiste j tale che $v(y_j) = 1$ con $1 \leq j \leq h$ perché $v(D) = 1$, ma $v(\neg a) = 0$. Segue che
$$v(Ris_a(C, D)) = 1$$

Quindi $v(S') = 1$.

$\Leftarrow$ Suppongo che S' sia soddisfacibile e provo che S è soddisfacibile. Sia v valutazione tale che $v(S') = 1$, ossia v soddisfa tutte le clausole in S'.

– Siano $C_1, \ldots, C_n \in S$ le clausole contenenti il pivot a quindi $C_i = C_i \cup \{a\}$
– Siano $D_1, \ldots, D_m \in S$ le clausole contenenti il pivot $\neg a$ quindi $D_j = D_j \cup \{\neg a\}$

Distinguo due casi:

1. Suppongo che esista un $1 \leq i \leq n$ tale che $v(C'_i) = 0$. Allora dato che

$$Ris_a(C, D) = C'_i \cup D'_d$$

è soddisfatto da v, e $v(C'_i) = 0$ segue che $v(D'_j) = 1 \Rightarrow v(D_j) = 1$. Pongo

$$\hat{v} = \begin{cases} v(x) \text{ se } x \neq a \\ 1 \text{ se } x = a \end{cases}$$

ovvero $\hat{v}(a) = 1$. Dunque $\hat{v}(D'_j) = v(D_j) = 1$ per ogni $1 \leq j \leq m$. Inoltre $\hat{v}(C_i) = 1$ per ogni $1 \leq i \leq n$ poiché $a \in C_i$ e $\hat{v}(a) = 1$. Segue che

$$\hat{v}(S) = 1$$

2. Suppongo che $v(C'_i) = 1$ per ogni $1 \leq i \leq n$. Definisco $\tilde{v}$ valutazione

$$\tilde{v} = \begin{cases} v(x) \text{ se } x \neq a \\ 0 \text{ se x=a} \end{cases}$$

Quindi $\tilde{v}(a) = 0$ e osservo che $\tilde{v}(C_i) = 1$ per ogni $1 \leq i \leq n$ perchè $\tilde{v}(C'_i) = 1$. Inoltre $\tilde{v}(D_j) = 1$ per ogni $1 \leq j \leq m$ perchè $\tilde{v}(\neg a) = 1$. Segue che

$$\tilde{v}(S) = 1$$

□

6.4 Logica dei Predicati

Definisco l'alfabeto

$$A = X \cup C \cup P \cup F \cup \{\forall, \exists\} \cup \{\neg, \wedge, \vee, \rightarrow, \longleftarrow\} \cup \{(,)\}$$

dove:

- X è l'insieme dei simboli di predicati $\{x_1, y_1, x_3, \ldots, x_n\}$
- C è l'insieme dei simboli di costanti $\{c, d, e, \ldots\}$
- P è l'insieme dei simboli di predicati, ognuno con la sua arietà.
- F è l'insieme dei simboli di funzione $\{F_1, F_2, \ldots, G_1, \ldots\}$

Per arietà si intende il numero di argomenti che prende il predicato.

Definizione 14 (Termine)**.** *Ogni simbolo di variabile o di costante è un termine. Se F è un simbolo di funzione di arietà n e $t_1, t_2, \ldots, t_n$ sono termini. Allora $F(t_1, t_2, \ldots, t_n)$ è un termine.*

Osservazione 5. *Un termine si dice chiuso se non contiene simboli di variabile.*

Definizione 15 (Formula atomica)**.** *Dati $t_1, t_2, \ldots, t_n$ termini e P simbolo di predicato di arietà n. Allora $P(t_1, t_2, \ldots, t_n)$ è una formula atomica.*

Definizione 16 (Struttura adeguata ad A)**.** *Definita come*

$$\Sigma = (\mathcal{S}, \mathcal{C}, \mathcal{P}, \mathcal{F})$$

dove

- $\mathcal{S}$ *è un insieme non vuoto, detto supporto di* Σ
- $\mathcal{C} \subseteq S$ *formato da* k *elementi, detti costanti*
- $\mathcal{F}$ *insieme di funzioni di arietà* n $f = \underbrace{S \times S \times \cdots \times S}_{n \text{ volte}} \to S$
- $\mathcal{P}$ *insieme di relazioni su* S

Definizione 17 (Interpretazione)**.** *Data Σ struttura adeguata ad A, un'interpretazione di A su Σ è una scelta di biezioni:*

$$\begin{cases} f_1 = C \to \mathcal{C} \\ f_2 = F \to \mathcal{F} \text{ rispettando l'arietà} \\ f_3 = P \to \mathcal{P} \text{ rispettando l'arietà} \end{cases}$$

Esempio. Sia $A = C \cup F \cup X \cup P \cup \{\forall, \exists\} \cup \{\neg, \wedge, \vee, \to, \leftarrow, \longleftrightarrow\}$ con

- $C = \{c_0, c_1\}$ simboli di costante
- $F = \{f, g\}$ simboli di funzione di arietà 2
- $P = \{p\}$ simbolo di predicato di arietà 2

e sia $t_1 = f(c_0, g(c_0, c_1))$ termine. Diamo due interpretazioni:

1. $\mathcal{S} = \mathbb{Z}, \mathcal{C} = \{0, 1\}, \mathcal{F} = \{+, \cdot\}, \mathcal{P} = \{\subset\}$. In questa interpretazione t_1 corrisponde a
$$+(0, \cdot(0, 1)) = 0 + (1 \cdot 0) = 0 \in \mathcal{S}$$
2. $\mathcal{S} = \mathbb{Z}, \mathcal{C} = \{3, 5\}, \mathcal{F} = \{MCD, mcm\}, \mathcal{P} = \{|\}$. In questa interpretazione t_1 corrisponde a
$$MCD(3, mcm(5, 3)) = 3$$

Osservazione 6. *Data un interpretazione di A su Σ ad ogni termine chiuso corrisponde uno e uno solo elemento del supporto S.*

Definizione 18 (Assegnazione)**.** *Dato alfabeto A=(X,C,F,P) e una struttura adeguata $\Sigma = (\mathcal{S}, \mathcal{C}, \mathcal{F}, \mathcal{P})$ ad A e un interpretazione i di A su Σ. Si dice assegnazione una funzione $a : X \to S$.*

Proposizione 3. *Ogni assegnazione $a : X \to S$ si estende in modo unico ad una funzione $\overline{a}$: $\{$termini su $A\} \to S$.*

Definizione 19 (Valutazione)**.** *Data Σ struttura, i interpretazione e a assegnazione. Ad ogni formula atomica $p(t_1, \dots, t_n)$ è associato un valore di verità*

$$v_a(p(t_1, \dots, t_n)) = \begin{cases} 1 & se\ (\mathcal{F}_1, \dots, \mathcal{F}_n) \in R \quad (\mathcal{F}_1, \dots, \mathcal{F}_n)\ soddisfa\ R \\ 0 & se\ (\mathcal{F}_1, \dots, \mathcal{F}_n) \notin R \end{cases}$$

al simbolo di predicato corrisponde una relazione R in S tramite l'interpretazione i. Si ha

$$v_a : \{formule\ atomiche\ su\ A\} \to \{0, 1\}$$

Definizione 20 (Formula)**.** *Dato A=(X,C,F,P) alfabeto. sono formule su A le seguenti:*

- *formule atomiche*
- *se α è una formula allora $\neg\alpha$ è una formula*
- *se α, β formule allora $(\alpha \wedge \beta), (\alpha \vee \beta), (\alpha \to \beta), (\alpha \longleftrightarrow \beta)$ sono formule*
- *se α formula e $x \in X$ simbolo di variabile allora $(\forall\, x\alpha), (\exists\, x\alpha)$ sono formule*

Definizione 21. *Sia α formula indico con $var(\alpha)$ =simboli di variabili in a. Ora, sia $x \in var(\alpha)$, x si dice vincolata se ricade nel campo di azione di un quantificatore $\forall\, \exists$. Altrimenti si dice libera.*

Definizione 22 (Enunciato)**.** *Formula priva di variabili libere.*

Osservazione 7. *Date un interpretazione e un assegnazione a ad ogni termine t su alfabeto A è associato un elemento $\overline{t^a} \in S$.*

Esempio. Dato $t : +(x, c)$, considero l'interpretazione $\Sigma = (\mathbb{Z}, 0, +, \emptyset)$, data l'assegnazione $a : x \to 1$, a t corrisponde

$$\overline{t^a} : +(1, 0) = 1$$

Quindi ad ogni formula atomica $\alpha = P(t_1, \dots, t_n)$ corrisponde un valore di verità

$$v_a(\alpha) = \begin{cases} 1\ se\ \overline{P}(\overline{t_1^a}, \dots, \overline{t_n^a}) \text{ è vera} \\ 0 \text{ altrimenti} \end{cases} \tag{6}$$

Esempio. Sia $\alpha : P(x, c)$ con $P \in \mathcal{P}$ e sia interpretazione $\mathcal{S} = \mathbb{Z}$, $P \to <$, $c \to 1$ e $a : x \to 0$ allora

$$v_a(\alpha) = <(0, 1) = 1 \text{ perché } 0 < 1$$

Definizione 23 (Istanziazione)**.** *Data $a : X \to \mathcal{S}$ assegnazione, $x \in X$ e $s \in \mathcal{S}$, definisco una nuova assegnazione $a(x \leftarrow s)$ tale che*

$$a(x \leftarrow s)(y) = \begin{cases} a(y)\ se\ y \neq x \\ a(x) = s \end{cases}$$

si chiama istanziazione.

6.4.1 Semantica per formule di logica proposizionale

Data α formula su A, Σ struttura adeguata, i interpretazione di A su Σ e $a : X \to S$ assegnazione, definisco $v_a(\alpha) \in \{0, 1\}$ nel modo seguente:

1. Se α formula atomica, vedi equazione (6).
2. $$v_a(\neg\alpha) = \begin{cases} 0 \text{ se } v_a(\alpha) = 1 \\ 1 \text{ se } v_a(\alpha) = 0 \end{cases}$$
3. $$v_a(\alpha_1 \wedge \alpha_2) = \begin{cases} 1 \text{ se } v_a(\alpha_1) = v_a(\alpha_2) = 1 \\ 0 \text{ altrimenti} \end{cases}$$
4. $$v_a(\alpha_1 \vee \alpha_2) = \begin{cases} 0 \text{ se } v_a(\alpha_1) = v_a(\alpha_2) = 0 \\ 1 \text{ altrimenti} \end{cases}$$
5. $$v_a(\alpha_1 \to \alpha_2) = \begin{cases} 0 \text{ se } v_a(\alpha_1) = 1 \text{ e } v_a(\alpha_2) = 0 \\ 1 \text{ altrimenti} \end{cases}$$
6. $$v_a(\alpha_1 \longleftrightarrow \alpha_2) = \begin{cases} 1 \text{ se } v_a(\alpha_1) = v_a(\alpha_2) \\ 0 \text{ altrimenti} \end{cases}$$
7. $$v_a(\forall\, x\alpha) = \begin{cases} 1 \text{ se per ogni } s \in S \text{ vale } v_{a(x \leftarrow s)}(\alpha) = 1 \\ 0 \text{ altrimenti} \end{cases}$$
8. $$v_a(\exists\ x\alpha) = \begin{cases} 1 \text{ se esiste } s \in S \text{ tale che } v_{a(x \leftarrow s)}(\alpha) = 1 \\ 0 \text{ altrimenti} \end{cases}$$

Se $v_a(\alpha) = 1$ scrivo $\Sigma \models_a \alpha$ e dico che α è vera in Σ sotto l'assegnazione a.

Definizione 24 (Logicamente valida)**.** *α formula su A, diciamo che α è logicamente valida se per ogni struttura adeguata Σ e per ogni interpretazione i di A in Σ per ogni assegnazione a vale $\Sigma \models_a \alpha$.*

Definizione 25 (Soddisfacibile)**.** *α è soddisfacibile se esiste una struttura adeguata Σ, una interpretazione i di A in Σ esiste a assegnazione tale che $\Sigma \models_a \alpha$.*

Definizione 26 (Insoddisfacibile)**.** *α è insoddisfacibile se per ogni struttura adeguata Σ, per ogni interpretazione i di a in Σ e per ogni assegnazione a, vale $\Sigma \not\models_a \alpha$.*

Esempio. Sia A simbolo di predicato allora:

- $\forall\, x(A(x) \wedge \neg A(x))$ è insoddisfacibile
- $\forall\, x(A(x) \vee \neg A(x))$ è logicamente valida

- $\exists\, x(A(x))$ è soddisfacibile ma non logicamente valida.

Definizione 27 (Logicamente equivalente)**.** *α, β formule, $\alpha \equiv \beta$, ossia α è logicamente equivalente a β, se per ogni struttura adeguata Σ, per ogni interpretazione i e per ogni assegnamento a, vale $\Sigma \models_a \alpha$ se e solo se $\Sigma \models_a \beta$.*

Definizione 28 (Conseguenza logica)**.** *α, β formule, $\alpha \models \beta$, ossia β è conseguenza logica di α, se per ogni Σ,i,a vale che se $\Sigma \models_a \alpha$ allora $\Sigma \models_a \beta$*

Osservazione 8. *$\alpha \equiv \beta$ è vera se e solo se $\alpha \models \beta$ e $\beta \models \alpha$.*

6.4.2 Forma normale prenessa

Una formula si dice in forma normale prenessa se essa è composta da una parte sinistra contenente solo quantificatori e variabili e una parte destra non contenente alcun quantificatore.
Esempio.

1. $\forall x \exists\, y(A(x,y) \wedge B(x))$ è in FNP
2. $\forall x(\exists\, yA(x,y) \wedge B(x))$ non è FNP

Teorema 1. *Per ogni formula α esiste α_1 formula in forma normale prenessa tale che $\alpha \equiv \alpha_1$.*

Valgono le seguenti equivalenze logiche:

1. $\neg\forall\, x\alpha \equiv \exists\, x\neg\alpha$
   $\neg\exists\, x\alpha \equiv \forall\, x\neg\alpha$
2. $\forall\, x\alpha \wedge \forall\, x\beta \equiv \forall\, x(\alpha \wedge \beta$
   $\exists\, x\alpha \vee \exists\, x\beta \equiv \exists\, x(\alpha \vee \beta$
   Attenzione: $\forall\, x\alpha \vee \forall\, x\beta \not\equiv \forall\, x(\alpha \vee \beta)$
3. Se $x \notin var(\beta)$, allora:
   - $\forall\, x\alpha \vee \beta \equiv \forall\, x(\alpha \vee \beta)$
   - $\exists\, x\alpha \wedge \beta \equiv \exists\, x(\alpha \wedge \beta)$
   - $\forall\, x\alpha \wedge \beta \equiv \forall\, x(\alpha \wedge \beta)$
   - $\exists\, x\alpha \vee \beta \equiv \exists\, x(\alpha \vee \beta)$
4. $\forall\, x\forall\, y\alpha \equiv \forall\, y\forall\, x\alpha$
   $\exists\, x\exists\, y\alpha \equiv \exists\, y\exists\, x\alpha$

Esempio.

$$\forall\, xP(x) \to \forall\, xQ(x) \equiv \neg\forall\, xP(x) \vee \forall\, xQ(x) \equiv \exists\, x\neg P(x) \vee \forall\, xQ(x) \equiv$$
$$\exists\, x\neg P(x) \vee \forall\, yQ(y) \equiv \forall\, y\exists\, x(\neg P(x) \vee Q(y))$$

Esempio.

$$\exists\, x(\exists\, xQ(x,z) \vee \exists\, x(P(x)) \to \neg(\neg\exists\, xP(x) \wedge \forall\, x\exists\, zQ(z,x)) \equiv \text{ De Morgan}$$

$$\neg\exists\, z(\exists\, xQ(x,z) \vee \exists\, xP(x)) \vee (\exists\, xP(x) \vee \neg\forall\, x\exists\, zQ(z,x)) \equiv \text{ 1 + De Morgan}$$

$$\forall\, z(\neg\exists\, xQ(x,z) \wedge \neg\exists\, xP(x)) \vee (\exists\, xP(x) \vee \exists\, x\forall\, z\neg Q(z,x)) \equiv$$

$$\forall z(\forall x\neg Q(x,z) \wedge \forall x\neg P(x)) \vee (\exists\, xP(x) \vee \exists\, x\forall z\neg Q(z,x)) \equiv$$
$$\forall z\forall x(\neg Q(x,z) \wedge \neg P(x)) \vee \exists\, x(P(x) \vee \forall z\neg Q(z,x)) \equiv$$
$$\forall z\forall x(\neg Q(x,z) \wedge \neg P(x))) \vee \exists\, \forall z(P(x) \vee \neg Q(z,x)) \equiv$$

Rinomino x con y e z con w:

$$\forall z\forall x(\neg Q(x,z) \wedge \neg P(x)) \vee \exists\, y\forall w(P(y) \vee \neg Q(w,y)) \equiv \text{ Uso 3}$$

$$\forall z\forall x((\neg Q(x,z) \wedge \neg P(x)) \vee \exists\, y\forall w(P(y) \vee \neg Q(w,y)) \equiv \text{ Uso 3}$$
$$\forall z\forall x\exists\, y\forall w((\neg Q(x,z) \wedge \neg P(x)) \vee (P(y) \vee \neg Q(w,y)) \equiv$$
$$\forall z\forall x\exists\, y\forall w((\neg Q(x,z) \vee P(y) \vee \neg Q(w,y)) \wedge (\neg P(x) \vee P(y) \vee \neg Q(w,y)) \tag{7}$$

Infine ottengo una FNPC ossia una FNP congiuntiva.

Definizione 29 (Skolem)**.** *La forma di Skolem è una FNP senza quantificatori esistenziali.*

Proposizione 4. *Ogni formula α è equisoddisfacibile ad una formula α_1 in forma di Skolem. α_1 è una skolemizzazione di α.*

Esempio.

1. $\alpha = \exists\, x\forall\, y(A(x,y) \wedge Q(x))$ con c simbolo di costante diventa $\alpha_1 = \forall\, y(A(c,y) \wedge Q(c))$
2. $\alpha = \exists\, x\forall\, y\exists\, z(P(x,y) \to Q(x,z))$ sostituisco x con c costante, z con $f(y)$ con f simbolo di funzione che non compariva già, diventa $\alpha_1 = \forall\, y(P(c.y) \to Q(x,f(y)))$
3. (4) diventa $\forall\, z\forall\, x\forall\, w((\neg Q(x,z)\vee P(f(z,x))\vee\neg Q(w,f(z,x))\wedge(\neg P(x)\vee P(f(z,x))\vee\neg Q(w,f(z,x))$
4. $\forall\, x\exists\, y\forall\, z\exists\, wA(x,y,z,w)$ diventa $\forall\, x\forall\, zA(x,f(x),z,g(x,z))$

Definizione 30. *Sia α formula, definisco H_α = universo di Herbrand di α = {costanti c_i che sono in α e ne aggiungo una se non ce ne sono e tutti i termini ottenibili applicando i simboli di funzione in α a termini di H_α}.*

Esempio.

1. $\alpha = \forall\, x\exists\, yA(x,y) \Longrightarrow H_\alpha = \{c\}$
2. $\beta = \forall\, x\exists\, yA(f(x),y) \Longrightarrow H_\beta = \{c, f(c), f(f(c)), \dots\}$
3. $\gamma = \forall\, xA(f(x,y),c,g(z) \Longrightarrow H_\gamma = \{x, f(c,c), g(c), f(f(c,c),g(c)), \dots\}$

α formula sull'alfabeto A, definisco struttura di Herbrand

$$\Sigma_H = (H_\alpha, \mathcal{C}, \mathcal{F}, \mathcal{P})$$

Interpretazione di Herbrand. Per f simbolo di funzione in α di arietà n, definisco

$$\overline{f} : \underbrace{H_\alpha \times \cdots \times\ H_\alpha}_{\text{n volte}} \to H_\alpha$$

tale che $\overline{f}(t_1, \dots, t_n) = f(t_1, \dots, t_n)$

Teorema 2. *Sia α formula in forma di Skolem. Allora α è soddisfacibile se e solo se è soddisfacibile in una sua interpretazione di Herbrand.*

Esempio. Verificare la validità di $\exists\, x(A(x) \wedge B(x)) \wedge \neg(\exists\, x(c(x) \wedge A(x)) \models \exists\, (B(x) \wedge \neg C(x))$. Valida se e solo se è insoddisfacibile la formula:

$$\exists\, x(A(x) \wedge B(x)) \wedge \neg(\exists\, x(C(x) \wedge A(x)) \models \neg\exists\, x(B(x) \wedge \neg C(x)) \equiv$$

Skolemizzazione della formula:

$$\exists\, x \forall\, y(A(x) \wedge B(x) \wedge (\neg C(y) \vee \neg A(y)) \wedge (\neg B(y) \vee C(y))) \equiv$$

La metto in FNPC:

$$\forall\, y(A(c) \wedge B(c) \wedge (\neg(C(y) \vee \neg A(y)) \wedge (\neg B(y) \vee C(y)))$$

In clausole:

$$S = \{\{A(c)\}, \{B(c)\}, \{\neg C(y), \neg A(y)\}, \{\neg B(y), C(y)\}\}$$

$$H_s = \{c\}$$

Sostituisco y con c:

$$\overline{S} = \{\{A(c)\}, \{B(c)\}, \{\neg C(c), \neg A(c)\}, \{\neg B(c), C(c)\}\}$$

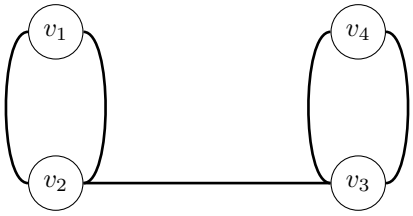
1. Pivot $A(c)$: $\overline{S}_1 = \{\{B(c)\}, \{\neg B(c), C(c)\}, \{\neg C(c)\}\}$
2. Pivot $B(c)$: $\overline{S}_2 = \{\{\neg C(c)\}, \{C(c)\}$
3. Pivot $C(c)$: $\overline{S}_3 = \{\square\}$ insoddisfacibile.

7 Teoria dei Grafi

Definizione 1 (Grafo)**.** *Si definisce grafo G la coppia G=(V,E), dove V è l'insieme dei vertici e $E \subseteq V^{[2]} = \{\{u, v\} | u, v \in V$ con $u \neq v\}$ insieme degli archi/lati.*

Definizione 2 (Grafo semplice)**.** *Un grafo senza cappi o archi paralleli.*

Definizione 3 (Multigrafo)**.** *G=(V,E,f) con $f : E \to V^{[2]}$*



Definizione 4 (Cammino)**.** *$v_0 l_0, v_1 l_1, \ldots, v_n l_n$,dove non si ripetono archi ma è accettabile la ripetizione di vertici, tale che $\forall\, i$ $v_i \in V$, $\forall\, i$ $l_i = \{v_{i-1}, v_i\} \in E$ con $l_i \neq l_j$ con $i \neq j$.*

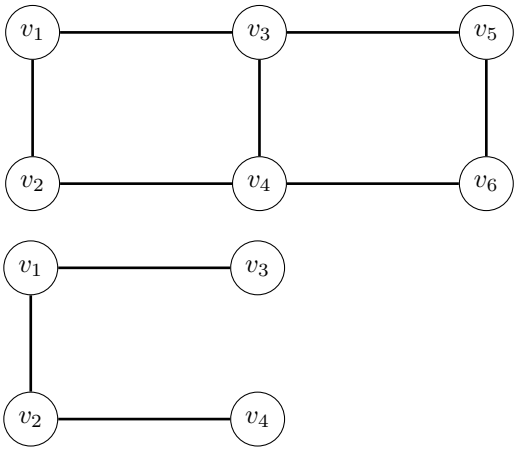
- *Se anche $v_i \neq v_j$ $\forall\, i \neq j$ con $1 \leq i, j \leq n-1$, allora si dice cammino semplice.*
- *Se $v_0 = v_n$ si dice cammino chiuso o circuito.*

- *La lunghezza di un cammino è il numero di archi da cui è composto.*
- *Un cammino semplice chiuso di lunghezza maggiore di due si dice* ***ciclo****.*

Definizione 5 (Grafo connesso)**.** *Un grafo G si dice connesso se* $\forall\, u, v \in V$ *esiste un cammino da u a v.*

Definizione 6 (Sottografo)**.** *G'=(V',E') sottografo di G=(V,E) se* $V' \subseteq V$ *e* $E' \subseteq E \cap V^{[2]}$

Esempio.



G' è un sottografo di G.

Definizione 7 (Sottografo indotto)**.** *G' è un sottografo indotto da V' se oltre a* $V' \subseteq V$ *vale anche* $E' \subseteq E \cap V'^{[2]}$*.*

Definizione 8 (Cammino euleriano)**.** *Un cammino è euleriano se passa una e una sola volta per ogni arco del grafo.*

Definizione 9 (Grafo euleriano)**.** *Dato G multigrafo, questo si dice euleriano se ha un circuito euleriano.*

Definizione 10 (Grado di un vertice)**.** *Sia v vertice del multigrafo G, il grado di v è dato da*

$$d_G(v) = \textit{numero di archi incidenti su } v$$

Se $f_G(v) = 0$ *allora v si dice isolato.*

Lemma 1. *In G=(V,E) vale*

$$\sum_{v \in V} d_G(v) = 2|E|$$

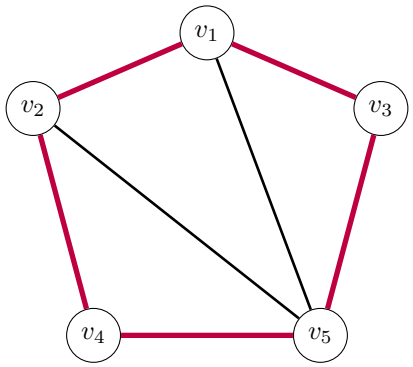
Corollario 1 (Strette di mano)**.** *Ogni grafo non orientato ha un numero pari di vertici con grado dispari.*

Teorema 1 (Eulero)**.** *Sia G grafo privo di vertici isolati, allora G è euleriano se e solo se è connesso ed ogni vertice ha grafo pari.*

Teorema 2. *Sia G grafo privo di vertici isolati, allora G ha un cammino non chiuso euleriano se e solo se è connesso ed h esattamente solo due vertici u e v di grado dispari. In questo caso il cammino euleriano inizierà da u e finirà in v.*

Definizione 11. *Sia G=(V,E) grafo, questo si dice hamiltoniano se ha un ciclo hamiltoniano, ossia un ciclo che passa una e una sola volta per ogni vertice $v \in V$.*

Esempio.



Ciclo hamiltoniano in viola

Definizione 12. *K_n grafo completo su n vertici $\{v_1, \dots, v_n\} = V$, $K_n = (V, V^{[2]})$ è hamiltoniano. Un grafo completo è sempre hamiltoniano.*

Teorema 3 (Teorema di Ore)**.** *Sia G=(V,E) con $|V| \geq 3$. Se per ogni $u, v \in V$ non adiacenti $d_G(u) + d_G(v) \geq |V|$ allora G è hamiltoniano.*

Dimostrazione. Si procede per induzione su k =numero di coppie di vertici non adiacenti di G.

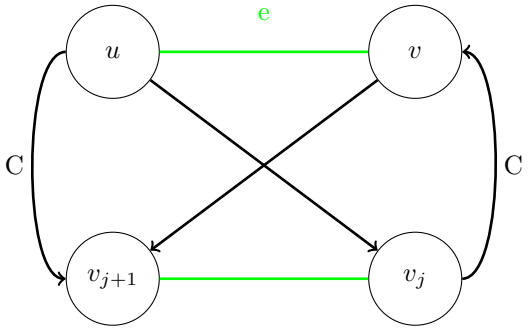
1. Caso base. Per $k = 0 \Rightarrow$ G è un grafo completo quindi hamiltoniano.
2. Passo induttivo. Supponiamo che $k \geq 1$ allora in G esistono $u, v \in V$ non adiacenti. Considero il grafo G' ottenuto da G aggiungendo l'arco $e = (u, v)$. Ora, G' continua a soddisfare le ipotesi del teorema perchè ho lo stesso numero di vertici e un arco in più. Inoltre, G' ha una coppia in meno di vertici adiacenti, quindi per ipotesi induttiva G' è hamiltoniano, ossia esiste un ciclo hamiltoniano C di G'. Quindi:
   - Se $e \notin C$ allora C è un ciclo hamiltoniano anche di G.
   - Se $e \in C$ allora:
     Scrivo $C - e = \{v = v_1, v_2, \dots, v_m\}$ dove $V = \{v_1, \dots, v_n\}$. Definisco

     $$U = \{v_i | (u, v_i) \in E\} = \{u \text{ è adiacente a } v_i \text{ in } G\}$$

     $$W = \{v_i | (v, v_{i+1} \in E\} = \{v \text{ è adiacente a } v_{i+1} \text{ in } G\}$$

     Quindi $|U| = d_G(u)$ e $|W| = d_G(v)$. Per ipotesi $|U| + |W| \geq n = |V|$. Ora $u \notin U \cup W$ perchè sennò u, v sarebbero adiacenti, quindi $|U \cup W| \leq n$.
     Quindi $U \cap W \neq 0$ perchè $|U \cup W| = |U| + |W| - |U \cap W|$. Sia $v_j \in U \cap W$, allora (u, v_j) e (v, v_{j+1}) sono archi di G. Allora parto da v seguo il lato (v, v_{j+1}), percorro il ciclo da v_{j+1} a u, seguo il lato (u, v_j) e infine da v_j a v, ottenendo un ciclo hamiltoniano.

□



Teorema 4. *Sia G=(V,E) e* $n = |V| \geq 3$ *e* $d_G(v) \geq \frac{n}{2}$ $\forall v \in V \Rightarrow G$ *è hamiltoniano.*

7.1 Criteri di Hamiltonianità

- Un eventuale ciclo hamiltoniano passa da ogni arco incidente su vertici di grado due.
- Se G è hamiltoniano, allora togliendo $k \geq 1$ vertici da G, insieme a tutti gli archi incidenti su di essi, ottengo al più k componenti connesse.

Definizione 13 (Distanza)**.** *Sia G=(V,E) grafo e* $u, v \in V$ *la distanza d(u,v) è il cammino di lunghezza minima tra u e v. Infinito se non esiste un cammino.*

Definizione 14 (Diametro)**.** *Il diametro diam(G) è la massima distanza tra vertici* $max\{d(u,v)|u,v \in V\}$.

Definizione 15 (Calibro)**.** *Il calibro g(G) di un grafo G è definito come la minima lunghezza di un ciclo in G. Infinito se G è aciclico, ossia non ha cicli.*

Definizione 16 (Circonferenza)**.** *La circonferenza è la massima lunghezza di un ciclo.*

Definizione 17 (Colorazione)**.** *Una funzione* $c : V \to C$*, dove C è l'insieme dei colori, è una colorazione di G se vale* $\forall (u,v) \in E$ $c(u) \neq c(v)$*. Se —C—=k allora G è k-colorabile. Il numero cromatico di G è definito come*

$$\mathcal{X}(G) = min\{k|G\ k - colorabile\}$$

Definizione 18 (Grafo bipartito)**.** *Sia G=(V,E) si dice bipartito se esiste una partizione di* $V = (X, \overline{X})$ *tale che* $X \cap \overline{X} = V$ *e* $X \cap \overline{X} = \emptyset$ *e per ogni* $(u,v) \in E$ *vale* $u \in X, v \in \overline{X}$ *oppure* $u \in \overline{X}, v \in X$*. Ovvero se l'insieme dei suoi vertici può essere partizionato in due sottoinsieme e ogni vertice di una di queste parti è collegato solo a vertici dell'altra parte.*

$$\mathcal{X}(G_{bipartito}) = 2$$

Osservazione 1. *Un grafo G è bipartito con* $|V| \geq 2$ *è bipartito se e solo se non contiene cicli dispari, ossia un ciclo con un numero dispari di vertici.*

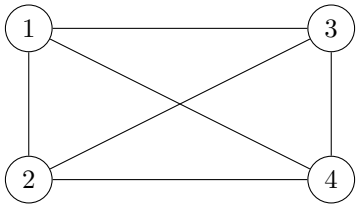
Definizione 19 (Isomorfismo)**.** *G=(V,E) e G'=(V',E') sono grafi isomorfi se esiste un isomorfismo, ossia una funzione* $f : V \to V'$ *biettiva tale che* $\forall u, v \in V$ *vale che* $(u,v) \in E$ *se e solo se* $(f(u), f(v)) \in E'$*. In pratica una funzione che mantiene l'adiacenza tra i vertici.*

Definizione 20 (Grafo piano)**.** *G=(V,E) si dice grafo piano se $V \subseteq \mathbb{R}^2$ e i lati sono curve semplici che si intersecano solo nei vertici.*

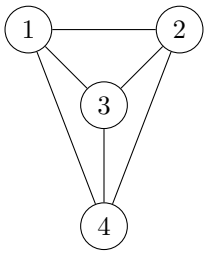
Definizione 21. *Una curva semplice è una funzione $\gamma : [0,1] \to \mathbb{R}^2$.*

Definizione 22. *G=(V,E) si dice planare se è isomorfo a un grafo piano.*

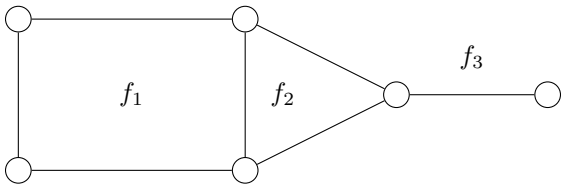
Esempio.



Non è piano ma è planare, infatti è isomorfo a:



Definizione 23. *Sia G=(V,E), definisco le facce di G:*



con f_3 la faccia infinita, ossia tutto il resto del piano.

Teorema 5 (Formula di Eulero)**.** *Sia G un grafo piano e connesso con n vertici, m archi e f facce, allora*

$$n - m + f = 2$$

Dimostrazione. Per induzione sul numero di archi m.

1. Caso base. Se $m = 0$ allora G è costituito da un unico vertice, quindi $f = 1$ e 1+1-0=2 ossia la formula vale.
2. Passo induttivo. Studiamo due casi:
   (a) Supponiamo che esista $v \in V$ tale che $d_G(v) = 1$. Sia G' il grafo ottenuto togliendo v più l'arco su di esso incidente. G' è un grafo piano e connesso quindi le ipotesi continuano a valere. G' ha $m - 1$ lati quindi posso usare l'ipotesi induttiva $(n-1) - (m-1) + f = 2 \Rightarrow n - m + f = 2$.

(b) Ogni vertice ha grado maggiore o uguale a due. Quindi esiste C ciclo in G, per $e \in C$ arco del ciclo che separa due facce di G. Considero G_0 il grafo ottenuto togliendo l'arco e. Quindi G_0 ha n vertici, $m-1$ lati e $f-1$ facce. Allora per ipotesi induttiva $n-(m-1)+(f-1)=2$ e quindi $n-m+f=2$.

□

Proposizione 1. *Sia G=(V,E) grafo planare, scrivo $n=|V|$ e $m=|E|$, se $n \geq e$ allora:*

- $m \leq 3(n-2)$
- *Se G non è un albero, pongo g=g(G) calibro. Allora $m \leq \frac{g(n-2)}{g-2}$ con $g \geq 3$*

Dimostrazione. A meno di isomorfismo, suppongo G piano. Eventualmente aggiungendo dei lati, posso supporre G connesso.

- Se G è aciclico allora G è un albero, quindi $m=n-1$ e $n-1 \leq 3(n-2 \; \forall n \geq 3$.
- Se G non è un albero e $g=g(G) \geq 3$. Per α faccia di G indico $p(\alpha)$ il numero di archi del bordo di α ossia il perimetro. Osservo che ogni arco è al massimo nel bordo di due facce. Ora, sia F l'insieme delle facce di G, $|F|$ =numero di facce di G. Quindi

$$\sum_{\alpha \in F} p(\alpha) \leq 2m$$

Inoltre osservo che $p(\alpha) \geq g \; \forall \, \alpha \in F$. Quindi

$$2m \geq \sum_{\alpha \in F} p(\alpha) \geq |F| g = fg$$

ma per Formula di Eulero $f=m-n+2$ quindi

$$2m \geq (m-n+2)g$$

Quindi $gn-2g \geq gm-2m$ e allora

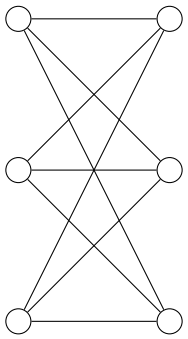
$$m \geq \frac{g(n-2)}{g-2}$$

□

Osservazione 2. *$A \to B$ equivale a $\neg B \to \neg A$, quindi se un grafo non rispetta $m \leq \frac{g(n-2)}{g-2}$ non è planare.*

Corollario 2. *$K_{3,3}$ non è planare.*

Infatti



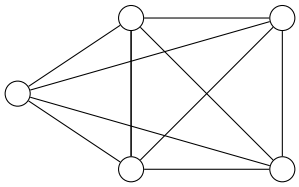
Segue che *n=6, m=9, g=4* e quindi

$$9 = m \not\leq \frac{g(n-2)}{g-2} = 8$$

Osservazione 3. *$K_{3,3}$ è un grafo bipartito.*

Corollario 3. *K_5 non è planare.*

Infatti



Segue che *n=5, m=10, g=3* e quindi

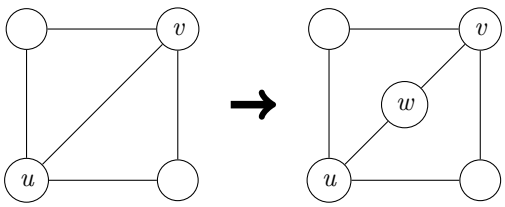
$$10 = m \not\leq 3(n-2) = 9$$

Osservazione 4. *Tutti i sottografi di un grafo planare sono planari.*

Corollario 4. *Se G=(V,E) planare allora esiste $v \in V$ tale che $d_G(v) \leq 5$.*

Dimostrazione. Se fosse $d_G(v) \geq 6$, $\forall\, v \in V$, $6n \leq \sum_{v \in V} d_G(v) = 2n$ quindi $n \geq 3n$ e questo è assurdo. □

Definizione 24 (Suddivisione elementare)**.** *Sia G=(V,E). Per suddivisione elementare di archi di un grafo si intende un'operazione che modifica un suo arco (u,v) in due spigoli (u,w) e (w,v) incidenti in un nuovo vertice w.*



Un grafo G'=(V',E') ottenuto da G con un numero finito di suddivisioni elementari è una suddivisione di G.

Teorema 6 (Teorema di Kuratowski)**.** *Un grafo G è planare se e solo se non ha sottografi isomorfi a suddivisioni di $k_{3,3}$ o k_5.*

Teorema 7 (Teorema dei quattro colori)**.** *Ogni grafo planare è 4-colorabile.*