Fondamenti matematici per l'informatica

Giacomo Fantoni

4 dicembre 2019

Indice

Capitolo 1

Insiemi e operazioni su insiemi

1.1 Concetti primitivi

- Insieme
- Elemento di un insieme

1.2 Teoria degli insiemi

1.2.1 Concetto di appartenenza

Considerando un insieme come una collezione di oggetti detti elementi è necessario affinchè un oggetto sia un insiem che si possa sempre stabilire se qualcosa è un suo elemento ($x \in A$) o no ($x \notin A$).

1.2.1.1 Paradosso di Russell

Si consideri l'oggetto $A = \{x | x \notin x\}$. Si supponga che A così definito sia un insieme, ovvero A è l'insieme degli elementi x tali che x non è un elemento di x. Provando a stabilire se $A \in A$ si ottiene:

- Se $A \in A$ dalla definizione di A segue $A \notin A$.
- Se $A \notin A$ allora per definizione di A segue $A \in A$

Da queste considerazioni deriva che A non è un insieme in quanto non si può decidere se un elemento appartiene o no.

1.3 Assiomi

1.3.1 Estesionabilità

Dati due insiemi A e B si dice che $A = B \Leftrightarrow (\forall x : x \in A \Leftrightarrow x \in B)$

1.3.2 Esistenza del vuoto ($\exists\emptyset$)

Esiste un insieme $\emptyset$, detto insieme vuoto, caratterizzato dal fatto di non contenere alcun elemento: $\exists\emptyset : \forall x, x \notin \emptyset$.

1.3.2.1 Osservazioni

- L'assioma di estensionalità garantisce l'unicità dell'insieme vuoto.
- Sia $P(x)$ una proprietà attribuile a x, allora $\forall x \;\; x \in \emptyset \Rightarrow P(x)$ è sempre vera.

1.3.3 Separazione

Sia X un'insieme e sia P una proprietà esprimibile in termini del linguaggio della teoria degli insiemi allora $\{x \in X | P(x)\}$ è un insieme

1.4 Sottoinsiemi

Siano A e B due isiemi, si dice che:

- si dice che A è contenuto in B, scritto $A \subset B$ (non si intende strettamente contenuto: $A \subset A$), se $\forall x : x \in A \Rightarrow x \in B$. Si dice che A è un sottoinsieme di B.
- A è un sottoinsieme proprio di B se A è strettamente contenuto in B, ovvero se $A \underset{\neq}{\subset} B \Leftrightarrow \forall x : x \in A \Rightarrow c \in B$ e $\exists y \in B : y \notin A$

1.4.0.1 Insieme universo

Se esistesse l'insieme Γ di tutti gli insiemi allora $\{x | x \notin X\} = \{x \in \Gamma | x \notin x\}$, che genera un paradosso di Russell.

1.5 Operazioni tra insiemi

- **Intersezione**: $X \cap Y := \{x | x \in X \wedge x \in Y\}$.
- **Differenza**: $X \backslash Y = \{x | x \in X \wedge x \notin Y$. Se $Y \subset X$ la differenza si dice il complementare di Y in X ($C_X(Y)$).

- **Unione**: $X \cup Y := \{x | x \in X \vee x \in Y\}$.
- **Prodotto cartesiano**: $X \times Y := \{(x, y) | x \in X, y \in Y\}$.
- **Insieme delle parti**: Insieme delle parti di X $2^X = B(X) = \{A | A \subset X\}$.
- Sia I un insieme non vuoto e $\forall i \in I$ è dato un insieme X_i si definiscono:
  - **Intersezione arbitraria**: $\bigcap_{i \in I} X_i = \{x | \forall i \in I, x \in X_i\}$
  - **Unione arbitraria**: $\bigcup_{i \in I} = \{x | \exists i \in I, x \in X_i\}$

Capitolo 2

Relazioni e funzioni

2.1 Relazione

Siano X e Y due insiemi. Un sotttoinsieme R di $X \times Y$ si dice relazione tra X e Y se $(x, y) \in R$ si scrive anche xRy: x è in R relazione con y.

2.2 Funzione

Sia f una relazione tra X e Y f si dice funzione da X in Y se $\forall x \in X \exists! y \in Y : (x, y) \in f), (xfy)$. $f : X \to Y$ è una funzione (X, Y, f).

- X è il doiminio di f.
- Y è il codominio.
- y si dice valore di f in x e si dice $f(x)$.

2.2.1 Osservazione

Sia $f : X \to Y$ una fuzione (vista come relazione). Si vuole definire f come concetto primitivo che associa ad ogni $x \in X$ un unico elemento $y \in Y$

2.2.2 Composizioni

Siano $f : X \to Y$ e $g : Y \to Z$ due funzioni. Si definisce composizione di f con g come la funzione $g \circ f = X \to Z$, con $(g \circ f)(x) := g(f(x)) \forall x \in X$.

2.2.3 Immagine

Sia $f : X \to Y$ una funzione e sia $A \subset X$. L'immagine di A tramite f è definita come: $f(A) := \{y \in Y | \exists x \in A, y = f(x)\} = \{f(x) \in Y | x \in A\}$. $f(X)$ si dice immagine di f.

2.2.4 Controimmagine

Sia $f : X \to Y$ una funzione e sia $B \subset Y$. L'immagine inversa (o controimmmagine) di B tramite f è definita come: $f^{-1}(B) := \{x \in X | f(x) \in B\}$.

2.2.4.1 Singoletti ($f^{-1}(y)$) o fibra di y sopra f

Se B è formato da un solo elemento ($B = \{y\}$) si ottiene $f^{-1}(\{y\}) = \{x \in X | f(x) = y\}$, si formalizza in questo modo il concetto di equazione.

2.2.5 Proprietà delle funzioni

Si $f : X \to Y$ f si dice:

- **Iniettiva**: se $\forall x_1, x_2 \in X$ con $x_1 \neq x_2$ allora $f(x_1) \neq f(x_2)$, equivalentemente se $\forall x_1, x_2 \in X$ tali che $f(x_1) = f(x_2)$, allora $x_1 = x_2$
- **Surgettiva (suriettiva)**: se $f(X) = Y$, equivalentemente $\forall y \in Y, \exists x \in X$ tale che $f(x) = y$.
- **Bigettiva (o biiettiva)**: se al contempo iniettiva e surgettiva.

2.2.6 Invertibilità

Sia $f : X \to Y$ una funzione. Allora le seguenti proposizioni sono equivalenti:

1. f è bigettiva.
2. Esiste ed è unica una funzione $g : Y \to Y$ tale che $g \circ f = Id_x(x)$ e $f \circ g = Id_y(y)$.

2.2.6.1 Dimostrazione

2 $\Rightarrow$ 1: f è iniettiva: siano $x_1, x_2 \in X$ tali che $f(x_1) = f(x_2)$, considero $g(f(x_1)) = g(f(x_2))$, $(g \circ f)(x_1) = (g \circ f)(x_2)$, $Id_x(x_1) = Id_x(x_2)$, $x_1 = x_2$, perciò f è iniettiva. f è surgettiva: sia $y \in Y$, allora $f(g(y)) = (f \circ g)(y) = Id_y(y) = y$, perciò la f è bigettiva.
1 $\Rightarrow$ 2: si supponga f bigettiva. Sia $y \in Y$ si osserva che $f^{-1}(y) \neq \emptyset$ per surgettività di f e $f^{-1}(y) = \{x_y\}$ per iniettività di f, ad ogni punto y si può perciò definire $g : Y \to X$ ponendo $g(y) := x_y$. Per costruzione $f(x_y) = y$, perciò $f(g(y)) = (f \circ g)(x_y) = Id_y$ e se $y = f(x)$ allora $f(x) = f(g(f(x)))$, perciò $x = g(f(x)) = (g \circ f)(x)$, ovvero $(g \circ f)(x) = Id_x$.

2.2.6.2 Definizione

Se g esiste allora è unica ed è detta inversa di f ($f^{-1} : Y \to X$).

2.3 Equipotenza di insieme

2.3.1 Definizione

Dati X e Y due insiemi questi sono equipotenti (o meglio X è equipotente a Y) indicato con $X \sim Y$ se esiste una bigezione $f : X \to Y$. In questo caso sii dice che X e Y hanno la stessa cardinalità.

2.3.2 Proprietà

Siano X, Y e Z tre insiemi, valgono le seguenti proprietà:

- X è equipotente a sè stesso: $X \sim X$.
- Se X è equipotente a Y allora Y è equipotente a X: $X \sim Y \Rightarrow Y \sim X$.
- Se X è equipotente a Y e Y è equipotente a Z, allora X è equipotente a Z: $(X \sim Y) \wedge_Y \sim Z) \Rightarrow X \sim Z$.

2.3.2.1 Dimostrazioni

- $X \sim X$: viene scelta l'identità.
- $X \sim Y \Rightarrow Y \sim X$: se $f : X \to Y$ è una bigezione, allora $f^{-1}Y \to X$ è una bigezione, inoltre $(f^{-1})^{-1} = f$.
- $(X \sim Y) \wedge_Y \sim Z) \Rightarrow X \sim Z$: $\exists X \underset{\sim}{\xrightarrow{f}} Y, Y \underset{\sim}{\xrightarrow{g}} Z \Rightarrow g \circ f : X \xrightarrow{\sim} Z$

Pur essendo riflessiva, commutativa e transitiva non è una relazione di equivalenza in quanto non esiste l'insieme universo.

2.3.2.2 Idea di cardinalità

Si può considerare una classe di insiemi detta cardinali caratterizzata dale seguenti proprietà:

- Comunque scelto un insieme $X, \exists$ un cardinale α tale che $X \sim \alpha$, ovvero ogni insieme X è equipotente ad uno e un solo cardinale, denotato con $|X|$.
- Se $\alpha \neq \beta$ sono due cardinali distinti, $\alpha \not\sim \beta$, ovvero due cardinali distinti non sono equipotenti tra loro.

2.4 Teorema

Siano X e Y due insiemi, allora $X \sim Y \Leftrightarrow |X| = |Y|$ (avere stessa cardinalità).

2.4.1 Dimostrazione

2.4.1.1 $\mathbf{X \sim Y \Rightarrow |X| = |Y|}$

Si supponga che $X \sim Y$, si osserva che esiste f tale che $X \xrightarrow[f]{\sim} Y$. Siano $k = |X|$ e $\lambda = |Y|$, e siano $g : X \to k$ e $h : Y \to \lambda$ delle bigezioni, allora $h^{-1} \circ f \circ g^{-1} : k \to \lambda$ è una bigezione e pertanto $k = \lambda$.

2.4.1.2 $\mathbf{|X| = |Y| \Rightarrow X \sim Y}$

Se $k = |X| = |Y|$ allora esistono due bigezioni $f : X \to k$ e $g : Y \to k$, è stato precedentemente dimostrato che $g^{-1} \circ f : X \to Y$ è una bigezione e perciò $X \sim Y$.

Capitolo 3

Numeri naturali, assiomi di Roano

Si definisca l'insieme $\mathbb{N}$ dei numeri naturali come l'insieme descritto dagli assiomi enunciati.

3.1 Assiomi di Peano

1. $0 \in \mathbb{N}$ detto zero.
2. $\exists succ : \mathbb{N} \to \mathbb{N}$ tale che sia iniettiva.
3. $succ(\mathbb{N} \subset \mathbb{N} \backslash \{0\}$.

3.2 Assioma di induzione

3.2.1 Enunciato

Sia $n \in \mathbb{N}$, $n \neq 0$, allora esiste un unico $m\mathbb{N}$ tale che $succ(m) = n$. Tale m viene chiamato predecessore di n.

3.2.2 Dimostrazione

Si supponga per assurdo che esista un $m \neq 0$ tale che $succ(n) \neq m \forall n$, allora sia $A = \mathbb{N} \backslash \{m\}$. Si nota che $0 \in A$ in quanto $m \neq 0$. Se $n \in A$, allora $succ(n) \neq m$, perciò $succ(n) \in A$, perciò $A = \mathbb{N}$, che è una contraddizione. È pertanto dimostrata l'esistenza di tale numero, la sua unicità deriva dall' iniettività della funzione $succ$. Sia $A \subset \mathbb{N}$, si supponga che $0 \in A$ (base dell'induzione) e $\forall n \in \mathbb{N} : n \in A \Rightarrow succ(n) \in A$, ovvero se $n \in A$ (ipotesi induttiva) allora si può dimostrare che $succ(n) \in A$ (passo induttivo).

3.3 Principio di induzione di prima forma

Il principio di induzione è una diretta conseguenza dell'assioma di induzione.

3.3.1 Enunciato

Sia $\{P(n)\}_{n\in\mathbb{N}}$ una famiglia di affermazioni $P(n)$ indicizzata su $n \in \mathbb{N}$ tale che:

- $P(0)$ è vera (base di induzione).
- $\forall n \in \mathbb{N}$, $P(n)$ vera $\Rightarrow P(succ(n))$ è vera (passo induttivo).

Allora $P(n)$ è vera $\forall n \in \mathbb{N}$.

3.3.2 Dimostrazione

Sia $A = \{n|P(n) \text{ è vera}\}$, allora $0 \in A$ e se $n \in A$ allora vale $P(n)$, pertanto vale $P(succ(n))$, ovvero $succ(n) \in A$, pertanto per l'assioma di induzione $A = \mathbb{N}$.

3.3.3 Principio di induzione "shiftato"

Del tutto analogo al principio enunciato precedentemente, l'unica differenza è che la prima affermazione vera non è $P(0)$ ma $P(n)$. Tale affermazione sarà conseguentemente vera $\forall m \in \mathbb{N} : m \geq n$.

3.4 Il teorema di ricorsione

Questo teorema è necessario per riuscire a definire somma, prodotto e relazione d'ordine tra naturali.

3.4.1 Enunciato

Sia X un insieme e $h : \mathbb{N} \times X \to \mathbb{N}$ una funzione e $c \in X$, allora $\exists! f : \mathbb{N} \to X$ tale che:

- $f(0) = c$
- $f(succ(n)) = h(n, f(n)) \ \ \forall n \in \mathbb{N}$

3.4.2 Dimostrazione

3.4.2.1 Unicità di f

Si supponga che esistono due funzioni f e g che dimostrano tale proposizione usando il principio di induzione: dal primo punto si verifica che per $n = 0$ $f(n) = c = g(n)$, mentre dal secondo si ottiene che $f(succ(n)) = h(n, f(n))$, mentre $g(succ(n)) = h(n, g(n))$, ma dato che $f(n) = g(n)$, si ottiene che $f(succ(n)) = h(n, f(n)) = h(n, g(n)) = g(succ(n))$.

3.4.2.2 Esistenza di f

Per la definizione di funzione, per provarne l'esistenza si deve trovare un insieme $f \subset \mathbb{N} \times X$ tale che $\forall n \in \mathbb{N} \exists! c \in X : (n, x) \in f$ e che, traducendo le richieste del teorema:

- $(0, c) \in f$
- $\forall n \in \mathbb{N}, (x, n) \in f \Rightarrow (succ(n), h(n, x)) \in f$

Sia $\Omega = \{Z \subset \mathbb{N} \times X | Z$ verifica i punti del teorema$\}$, si necessita di trovare un elemento di Ω che sia una funzione. Sia $f = \bigcap_{Z \in \Omega} Z$. Essendo f l'intersezione di tutti gli elementi di Ω, necessariamente $\forall Z \in \Omega \quad f \subset Z$. Si provi ora che $f \in \Omega$: infatti $(0, c) \in f$. Se $(n, x) \in f$, allora $(n, x) \in Z \quad \forall Z \in \Omega$. Si provi ora che $f \in \Omega$: $(o, c) \in Z \quad \forall Z \in \Omega$, pertanto $(0, c) \in f$. Se $(n, x) \in f$ allora $(n, x) \in Z \forall Z \in \Omega$, ma siccome $\forall Z \in \Omega$

3.5 Operazioni tra naturali

Il teorema di ricorsione permette di definire la somma e il prodotto tra numeri naturali.

3.5.1 Somma

Dato $n \in \mathbb{N}$ si definisce la somma $m \to m+n$ ricorsivamente nel seguente modo:

$$n + 0 = n$$
$$n + succ(m) = succ(n) + m$$

3.5.1.1 Osservazioni

Se si definisce 1 come $succ(0) = 1$, allora $\forall n \in \mathbb{N} \quad succ(n) = n + 1$

3.5.2 Prodotto

Dato $n \in \mathbb{N}$ si definisce il prodotto $m \to m \cdot n$ ricorsivamente nel seguente modo:

$$n \cdot 0 = 0 n \cdot (m + 1) = n \cdot m + n$$

Capitolo 4

Insiemi ordinati

Sia X un insieme e R una relazione binaria su X, R si dice ordinamento parziale o relazione d'ordine parziale se valgono le seguenti proprietà $\forall x, y, z \in X$:

- Riflessiva: xRx.
- Antisimmetrica: $(xRy \wedge yRx) \Rightarrow x = y$.
- Transitiva: $(xRy \wedge yRz) \Rightarrow xRz$.

Se inoltre vala la tricotomia: $xRy \vee yRx$ allora si dice ordinamento totale. Una coppia (X, R) in cui R è un ordinamento si dice insieme ordinato.

4.0.0.1 Osservazioni

- Le relazioni d'ordine si scrivono con simboli del tipo $\leq$ o $\preceq$. Con $x \succeq y$ si intende $y \preceq x$, mentre $x \prec y$ implica $x \preceq y \wedge x \neq y$.
- In questi termini $(\mathbb{N}, \leq)$ risulta un insieme totalmente ordinato.

4.1 Ordinamento dei naturali

Attraverso la somma è possibile definire la nozione di ordinamento dei naturali: siano $n, m \in \mathbb{N}$, si dirà che $n \leq m$ se $\exists k \in \mathbb{N} : m = n + k$

4.1.0.1 Osservazione

Si può vedere $\leq$ come un sottoinsieme di $\mathbb{N} \times \mathbb{N}$, più precisamente $\leq = \{(m, m) \in \mathbb{N} \times \mathbb{N} | \exists k \in \mathbb{N} : n + k = m\}$.

4.1.0.2 Proprietà

$\forall n, m, k, h \in \mathbb{N}$

- $n \leq n$
- $(n \leq m \wedge m \leq n) \Rightarrow m = n$
- $(n \leq m \wedge m \leq k) \Rightarrow n \leq k$
- $m \leq n \vee n \leq m$
- $n \leq m \Rightarrow n + k \leq m + k$
- $n \leq m \wedge k \geq 1 \Rightarrow nk \leq mk$
- $n \leq m \wedge k \leq h \Rightarrow n + k \leq m + h$
- $n \leq m \wedge k \leq h \Rightarrow nl \leq mh$

Capitolo 5

Insiemi Finiti

Dato un numero naturale $n \in \mathbb{N}$ e denotato $I_n = \{0, 1, \cdots, n-1\}$, si dice che un insieme X è finito se esiste $n \in \mathbb{N}$ tale che X è equipotente a I_n, ovvero $X \sim I_n$. Un insieme è detto infinito se non è finito.

5.1 Il lemma dei cassetti

Siano X e Y due insiemi aventi rispettivamente $X \sim I_n$ e $Y \sim I_m$ con $n < m$ allora ogni applicazione $f : Y \to X$ non è iniettiva.

5.1.0.1 Dimostrazione

Si proceda per induzione su n. Se $n = 0$ allora $X = \emptyset$ e $Y \neq \emptyset$, pertanto l'insieme X^Y delle applicazioni è vuoto e non cè nulla da dimostrare (dal falso segue ogni cosa). Ora si supponga che la tesi sia vera per n e la si provi per $n + 1$: sia $X \sim I_{n=1}$ e $Y \sim I_m$ con $m > n + 1$. Si supponga per assurdo che l'applicazione $f : Y \to X$ sia iniettiva. Per definizione esiste una bigezione $g : I_{n+1} \to X$, si ponga $x_n = g(n)$ e $X' = X - \{x_n\}$. Ovviamente X' è in bigezione con I_n. si hanno perciò due casi:

- $f^{-1}(x_n) = \emptyset$, ovvero che $\forall y \in Y, f(y) \neq x_n$.
- $f^{-1}(x_n) \neq \emptyset$, ovvero che $\exists y \in Y : f(y) = x_n$.

Nel primo caso $f(Y) \subset X'$, pertanto $f : Y \to X'$ sarebbe una funzione iniettiva da un insieme equipotente a I_m in un'insieme equipotente a I_n, dato che $m > n + 1 > n$ questo è assurdo per ipotesi di induzione. Nel secondo caso sia $y \in Y$ tale che $f(y) = x_n$ e $Y' = Y - \{y\}$. Dato che f è iniettiva, $f(Y') \subset X'$ perciò $f|Y' : Y' \to X'$ è un'applicazione iniettiva. Dato che $Y' \sim I_{m-1}$ e $X' \sim I_n$ e che $m - 1 > n$ si ottiene un assurdo per ipotesi di induzione.

5.2 Cardinalità degli insiemi finiti

5.2.0.1 Corollario del lemma dei Cassetti

Se $n, m \in \mathbb{N}$ sono due numeri naturali diversi e X, Y sono insiemi finiti con $|X| = |I_n|$ e $|Y| = |I_m|$ allora X e Y non sono equipotenti, in particolare se $|X| = |I_n|$ e $|X| = |I_m|$ allora $m = n$.

5.2.1 Cardinalità

Sia X un insieme finito, si dice cardinalità di X l'unico numero naturale n tale che $|X| = |I_n|$. Tale numero si indica con $|X|$.

5.2.1.1 Equipotenza e cardinalità

Due insiemi finiti sono equipotenti se e solo se $|X| = |Y|$. Infatti se $|X| = |Y|$ allora $\exists n \in \mathbb{N}$ tale che X è equipotente a I_n e Y è equipotente a I_n, ma allora X e Y sono equipotenti. Viceversa se sono equipotenti il corollario precedente mostra che hanno la stessa cardinalità.

5.3 Sottoinsiemi di un insieme finito

Sia X un insieme finito tale che $Y \subset X$ allora anche Y è finito e $|Y| \leq |X|$. Se Y è un sottoinsieme proprio allora $|Y| < |X|$.

5.3.0.1 Dimostrazione

Si proceda per induzione su $n = |X|$. Se $n = 0$ allora $X = \emptyset$ e anche $Y = \emptyset$ da cui si conclude. Si supponga ora che la tesi sia vera per n e la si provi per $n+1$: sia dato X con $|X| = n+1$. Sia $f : I_{n+1} \to X$ una bigezione, e si ponga $x_n = f(n)$ e $X' = X - \{x_n\}$. Ovviamente $f|_{I_n} : I_n \to X'$ è una bigezione, pertanto $|X'| = n$. Si considerano pertanto i due casi, in cui $x_n \in Y$ e $x_n \notin Y$. Nel primo caso $Y \subset X'$, pertanto per ipotesi di induzione $|Y| \leq |X'| = n < n + 1 = |X|$. Nel secondo caso, considerato $Y' = Y - \{x_n\}$ si ha che $Y' \subset X'$, pertato $|Y'| \leq |X'|$, ovvero $|Y| = |Y'| + 1 \leq |X'| = |X| + 1 = |X|$. SI osservi che in quest'ultimo caso che se $Y \neq X$ allora anche $Y' \neq X'$, pertanto per ipotesi di induzione si ha che $|Y'| < |X'|$ da cui $|Y| < |X|$.

5.3.1 Corollario

Un insieme finito non è equipotente ad alcun suo sottoinsieme proprio.

Capitolo 6

Insiemi infiniti

6.1 Assioma della scelta

Sia I un insieme e $\forall i \in I$ sia dato un insieme $A_i \neq \emptyset$, allora esiste una funzione, detta funzione di scelta:

$$\varphi : I \to \bigcup_{i \in I} A_i \tag{6.1}$$

Tale che $\forall i \in I \varphi(i) \in A_i$.

6.1.0.1 Osservazioni

- Questo assioma determina che quando si ha un insieme di insiemi non vuoti è possibile scegliere in un colpo solo un elemento da ciascuno di essi, senza determinare però quale sia tale funzione.

- Una formulazione simile all'assioma della scelta: si consideri un insieme X e come insieme di indici $2^X - \{\emptyset\}$ e per ogni $i \in I$ si ponga $A_i = i$. L'assioma della scelta determina l'esistenza della funzione $\varphi : 2^X - \{\emptyset\} \to X = \bigcup_{i \in 2^X - \{\emptyset\}} i$ tale che $\varphi(i) \in i \forall i \in 2^X - \{\emptyset\}$

6.2 Equipotenza ai numeri naturali

Se X è un insieme infinito allora contiene un sottoinsieme Y equipotente a $\mathbb{N}$.

6.2.0.1 Dimostrazione

Sia $\varphi : 2^X - \{\emptyset\} \to X$ una funzione di scelta e si denoti con 2^X_F l'insieme delle parti finite di X, ovvero $2^X_F = \{Z \subset X | Z \text{ è finito}\}$. Dato un elemento $x_0 \in X$ che esiste in quanto X è infinito si consideri la funzione $\psi : \mathbb{N} \to 2^X_F$ definita

ricorsivamente da:

$$\psi(0) = \{x_0\}$$
$$\psi(n+1) = \psi(n) + \cup\{\varphi(X - \psi(n))\}$$

E si definisca la funzione $f : \mathbb{N} \to Y$ ponendo $f(0) = x_0$ e per ogni $n > 0$ $f(n) = \varphi(X - \psi(n-1))$. Si osservi che dalla definizione di ψ deriva che $\forall n \in \mathbb{N}, f(n) \in \psi(n)$ e che $\psi(n) \subset \psi(n+1)$, da cui segue che se $n \leq m$ allora $\psi(n) \in \psi(m)$ e pertanto $f(n) \in \psi(m)$. Ne segue che se $n < m$, $f(n) \in \psi(m-1)$, mentre $f(m) = \varphi(X - \psi(m-1)) \in X - \psi(m-1)$ pertanto $f(n) \neq f(m)$, ovvero f è iniettiva. Per il lemma dei cassetti allora Y è equipotente a Y.

6.2.0.2 Osservazioni

- Nella dimostrazione del teorema si definisce ricorsivamente la funzione $\psi : \mathbb{N} \to 2^X_F$. La funzione $h : \mathbb{N} \times 2^X_F \to 2^X_F$ che in questa funzione ricorsiva è data da $h(n, Z) = Z \cup \{\varphi(X - Z)\}$. Dato che X è infinito e Z finito, allora $X - Z \neq \emptyset$ pertanto $\varphi(X - Z)$ ha senso ed è finito.
- Questo teorema dimostra che la cardinalità dei numeri naturali è la più piccola delle cardinalità degli insiemi infiniti.

6.3 Equipotenza di sottoinsiemi di insiemi finiti

Ogni insieme infinito è equipotente ad un suo sottoinsieme proprio.

6.3.0.1 Dimostrazione

Sia X un insieme finito e $Y \subseteq X$ un suo sottoinsieme equipotente a $\mathbb{N}$, si è già visto come $\mathbb{N}$ sia equipotente ad un suo sottoinsieme proprio, quindi se $|Y| = |\mathbb{N}|$, Y è equipotente ad un suo sottoinsieme proprio, in particolare esiste una bigezione $f : Y \to Y'$ essendo $Y' \underset{\neq}{\subset} Y$. Pertanto la funzione $g : X \to X$ è definita da:

$$x \text{ se } x \in X - Y$$
$$f(x) \text{ se } x \in Y$$

Dà una bigezione tra X e il suo sottoinsieme $(X - Y) \cup Y' \underset{\neq}{\subset} X$.

6.4 Definizione di insieme infinito

La proposizione dimostrata precedente e il corollario del teorema dei sottoinsiemi di un insieme finito determinanto questa definizione di insieme infinito.

6.4.0.1 Definizione

Un insieme è infinito se e solo se è equipotente ad un suo sottoinsieme proprio.

Capitolo 7

Insiemi numerabili

7.0.0.1 Definizione

Un insieme X si dice numerabile se $|X| = |\mathbb{N}|$. La cardinalità di $\mathbb{N}$ si indica con $\aleph_0$, è pertanto equivalente scrivere $|X| = \aleph_0$.

7.1 Unione di insiemi numerabili disgiunti

Se X e Y sono due insiemi numerabili disgiunti allora $X \cup Y$ è un insieme numerabile.

7.1.0.1 Dimostrazione

Siano $f : X \to \mathbb{N}$ e $g : Y \to \mathbb{N}$ due bigezioni e si definisca $h : X \cup Y \to \mathbb{N}$ come $h(x) = \begin{cases} 2f(x) & \text{se } x \in X \\ 2g(x)+1 & \text{se } x \in Y \end{cases}$. Si verifica facilmente che h è una bigezione.

7.2 Operazioni tra insiemi numerabili e finiti

7.2.1 Unione di un insieme numerabile e uno finito

Se X numerabile e Y finito sono disgiunti allora $X \cup Y$ è numerabile.

7.2.1.1 Dimostrazione

Siano $f : X \to \mathbb{N}$ e $g : Y \to \mathbb{N}$ due bigezioni e si definisca $h : X \cup Y \to \mathbb{N}$ come:$h(x) = \begin{cases} g(x) & x \in Y \\ f(x)+n & x \in X \end{cases}$ si verifica facilmente che h è una bigezione.

7.2.2 Sottoinsiemi di un insieme numberabile

Se X è un insieme numerabile e $Y \subset X$, allora Y è finito o numerabile.

7.2.2.1 Dimostrazione

Se Y non è finito allora contiene un sottoinsieme Z numerabile, da cui segue la tesi del lemma dimostrato successivamente.

7.2.3 Cardinalità dell'unione con insiemi infiniti

Se X è un insieme infinito e Y è un insieme finito o numerabile, allora $|X \cup Y| = |X|$.

7.2.3.1 Dimostrazione

Si supponga Y disgiunto da X, in quanto $X \cup Y = X \cup (Y - X)$ e per la proposizione precendente $(Y - X)$ è finito o numerabile. Sia $Z \subset X$ un insieme numerabile, per le proposizioni precedenti esiste una bigezione $f : Z \to Z \cup Y$, si definisca allora $g : X \to X \cup Y$ ponendo:$g(x) = \begin{cases} f(x) & x \in Z \\ x & x \in X - Z \end{cases}$. Si provi che è iniettiva: se $x_1, x_2 \in Z$ allora $f(x_1) \neq f(x_2)$, perciò $g(x_1) \neq g(x_2)$, se $x_1, x_2 \in X - Z$ evidentemente è iniettiva. Si provi ora che è surgettiva: nel primo caso dipende dalla surgettività di f, nel secondo è banale.

7.2.4 Unione di una famiglia di insiemi finiti

Sia $\{X_n | n \in \mathbb{N}\}$ è una famiglia di insiemi finiti a due a due disgiunti, allora $\bigcup_{i=0}^{\infty} X_i$ è numerabile.

7.2.4.1 Dimostrazione

Sia $m_n = |X_n|$ e $\forall n$ sia $f_n : I_n \to X_n$ una bigezione. Si considerino i numeri $M_n = \sum_{i=0}^{n} m_i$, $M_{-1} = 0$ e si definisca $f : \mathbb{N} \to \bigcup_{i=0}^{\infty} X_i$ e si ponga $f(k) = f_n(k - M_{n-1}$ se $M_{n-1} \leq k < M_n$. È banale mostrare come questa funzione sia bigettiva.

7.2.5 Prodotto di due insiemi numerabili

Essendo $\mathbb{N} \times \mathbb{N}$ numerabile, ogni prodotto di insiemi numerabili è numerabile.

7.2.5.1 Dimostrazione

Per ogni $m \in \mathbb{N}$ si consideri $X_m = \{(n_1, n_2) \in \mathbb{N} \times \mathbb{N} | n_1 + n_2 = m$, chiaramente $|X_m| = m+1$ per ogni m e $X_m \cap X_k = \emptyset$ se $m \neq k$, e infine $\bigcup_{m=0}^{\infty} X_m = \mathbb{N} \times \mathbb{N}$ (si noti che $(n_1, n_2) \in X_{n_1+n_2}$, la tesi segue pertanto dalla proposizione precedente. Si noti inoltre che se X e Y sono numerabili, allora $f : X \to \mathbb{N}$ e $g : Y \to \mathbb{N}$ sono bigezioni e pertanto la applicazione definita dal loro prodotto è una bigezione.

7.2.6 Unione di una famiglia di insiemi numerabili

Sia $\{X_n | n \in \mathbb{N}\}$ è una famiglia di insiemi numerabili a due a due disgiunti, allora $\bigcup_{i=0}^{\infty} X_i$ è numerabile.

7.2.6.1 Dimostrazione

Per ogni $n \in \mathbb{N}$ sia $f_n : \mathbb{N} \to X_n$ una bigezione e si definisca $f \ltimes \times \mathbb{N} \to \bigcup_{i=0}^{\infty} X_i$, ponendo $f(n, m) = f_n(m)$, è banale verificare come f sia una bigezione.

Capitolo 8

Cardinalità

8.1 Confronto di cardinalità

8.1.0.1 Definizione

Dati due insiemi X e Y si dirà che la cardinalità di X è minore della cardinalità di Y, scritto $|X| \leq |Y|$ se esiste una funzione iniettiva $f : X \to Y$. Si dirà che la cardinalità è strettamente minore, o $|X| < |Y|$ se $|X| \leq |Y|$ e $|X| \neq |Y|$. È immediato verificare che $|X| \leq |Y|$ se e solo se Y contiene un sottoinsieme equipotente a X.

8.1.0.2 Proprietà

$\forall X, Y, Z$

- Riflessiva: $|X| \leq |X|$.
- Transitiva: $|X| \leq |Y| \wedge |Y| \leq |Z| \Rightarrow |X| \leq |Z|$.
- Verrà successivamente verificata la proprietà antisimmetrica.

Per dimostrare queste proprietà basta dimostrare che l'identità e la composta di funzioni iniettive sono iniettive.

8.2 Cardinalità di sottoinsiemi

Sia $X \subset Y \subset Z$ e che $|X| = |Z|$, allora $|Y| = |Z|$.

8.2.0.1 Dimostrazione

Sia $f : Z \to X$ una bigezione e $A_0 = Z - Y$ e $A_{n+1} = f(A_n)$ e si ponga $A = \bigcup_n A_n$. Si osservi che $f(A) \subset A \cap Y$ e che f è una bigezione tra f e la

sua immagine. Si definisca pertanto $g(x) = \begin{cases} f(z) & z \in A \\ z & z \in Z - A \end{cases}$ e si provi che sia una bigezione: si hanno tre casi: $z_1, z_2 \in A$: esssendo f iniettiva $g(z_1) = f(z_1) \neq g(z_2) = f(z_2)$; $z_1, z_2 \in Z - a$, in questo caso $g(z_1) = z_1 \neq g(z_2) = z_2$; $z_1 \in A$ e $z_2 \in Z - A$, in tal caso $g(z_1) = f(z_1)$ mentre $g(z_2) = z_2$. Pertanto g è surgettiva. Sia ora $y \in Y$ pertanto o $y \in Y - A$e allora $g(y) = y$ o $y \in A$. In questo caso esiste $i \in \mathbb{N}$ tale che $y \in A_i$, inoltre, dato che $y \in Y$ e $A_0 = Z - Y$ allora $i > 0$. Perciò essendo $A_i = f(A_{i-1}$ esiste $z \in A_{i-1} : f(z) = y$, essendo $z \in A$ $g(z) = f(z) = y$.

8.3 Teorema di Cantor-Bernstein

Siano X e Y due insiemi e si suppongano $f : X \to Y$ e $g : Y \to X$ due funzioni iniettive, allora esiste una funzione bigettiva $h : X \to Y$.

8.3.0.1 Dimostrazione

Si osservi che $|X| = |f(X)|$ e che $|g(f(X))| = |f(X)|$, pertanto $|X| = |g(f(X))|$, inoltre $g(f(x)) \subset g(Y) \subset X$, pertanto per il lemma precedente $|X| = |g(Y)|$, dato che $|g(Y)| = |Y|$ segue la tesi.

8.4 Tricotomia dei cardinali

Per ogni coppia di insiemi X, Y, si ha $|X| \leq |Y| \vee |Y| \leq |X|$.

8.4.0.1 Osservazione

La relazione di avere cardinalità minore o uguale di gode di tutte le proprietà di un ordinamento totale.

8.5 Operazioni tra cardinali

1. $|X| + |Y| = |(X \times \{0\}) \cup (Y \times \{1\})|$.
2. $|X||Y| = |X \times Y|$.
3. $|X|^{|Y|} = |X^Y|$.
4. $2^{|X|} = |2^X|$.

E tutte le proprietà analoghe alle operazioni tra numerali.

8.6 L'assioma del buon ordinamento

8.6.1 Minimo

Sia X un insieme e $\leq$ un ordinamento su X e $A \subset X$, si definirà $z \in A$ come minimo se $\forall x \in A, z \leq x$. $(z = \min A)$.

8.6.2 Buon ordinamento

Un ordinamento totale su X si dice un buon ordinamento se ogni sottoinsieme non vuoto di X ha un minimo.

8.6.3 Il buon ordinamento dei numeri naturali

L'ordinamento dei numeri naturali è un buon ordinamento.

8.6.3.1 Dimostrazione

Si supponga che l'insieme $A \subset \mathbb{N}$ non possegga minimo e si provi che $A = \emptyset$. Si costruisca B come il complementare di A e si dimostri per induzione che $\forall n \in \mathbb{N}, \{0, 1, 2, \cdots, n\} \subset B$. $0 \notin A$ se no sarebbe il suo minimo. Ora assumendo $\{0, 1, 2, \cdots, n\} \subset B$, allora $0, 1, 2, \cdots, n \notin A$ e se $n+1 \in A$ ne sarebbe il minimo, pertanto $n + 1 \in B$, pertanto $B = \mathbb{N}$ e $A = \emptyset$.

8.7 Il principio di induzione di seconda forma

Sia $P(n)$ una famiglia di affermazioni indicizzata su $\mathbb{N}$ e si supponga che:

1. $P(0)$ sia vera.
2. $\forall n > 0$, $P(k)$ vera $\forall k < n \Rightarrow P(n)$.

8.7.0.1 Dimostrazione

Sia $A = \{n \in \mathbb{N} | P(n) \text{ non è vera}\}$ e si supponga per assurdo che $A \neq \emptyset$, allora per la proprietà del buon ordinamento A ha un minimo $n \neq 0$ in quanto $P(0)$ è vera. Inoltre se $k < n$ allora $k \notin A$ in quanto $n = \min A$, pertanto dalla due segue che $P(n)$ è vera, pertanto $n \notin A$, che è una contraddizione.

Capitolo 9

La divisione euclidea

Supposta nota la definizione di $\mathbb{Z}$ come insieme dei numeri interi.

9.0.0.1 Definizione

Siano $n, m \in \mathbb{Z}$ con $m \neq 0$, allora esistono unici $q, r \in \mathbb{Z}$ tali che:

$$n = mq + r$$
$$0 \leq r < |m|$$

9.0.1 Dimostrazione

9.0.1.1 Esistenza

Si supponga che $n, m \in \mathbb{N}$ e si utilizzi il principio di induzione. Se $n = 0$ basta considerare $q = r = 0$. Si supponga $n > 0$ e che la tesi sia vera $\forall k < n$. Se $n < m$ basta prendere $q = 0$ e $r = n$, altrimenti sia $k = n - m$, dato che $m \neq 0$, $0 \leq k < n$, pertanto per ipotesi di induzione esistono $q, r \in \mathbb{N}$ tali che $k = mq + r$ e $0 \leq r < m$, ma allora $n = k + m = mq + r + m = (q + 1)m + r$. Si supponga ora $n < 0$ e $m > 0$, allora $-n > 0$, pertanto per il caso precedente si ha che esistono $q, r \in \mathbb{Z}$ tali che $-n = qm + r$ e $0 \leq r < m = |m|$, pertanto $n = m(-q) - r = m(-q) + m - m - r = m(-1 - q) + (m - r)$. Si consideri infine $m < 0$, allora $-m > 0$, pertanto per i due casi precedenti esistono $q, r \in \mathbb{Z}$ tali che $n = (-m)q + r = m(-q) + r$ e $0 \leq r < -m = |m|$.

9.0.1.2 Unicità

Si supponga che $n = mq + r$ e $n = mq' + r'$, con $0 \leq r, r' < m$. Si supponga ora $r' > r$, allora $m(q - q') = r' - r$, passando ai moduli $|m||q - q'| = |r - r'| < |m|$, da cui $0 \leq |q - q'| < 1$, pertanto $|q - q'| = 0$, ovvero $q = q'$, allora dalla supposizione precedente si ottiene $r = r'$.

Capitolo 10

Scrittura dei naturali in base arbitraria

Sia $b \in \mathbb{N}$ si dice che $n \in \mathbb{N}$ è rappresentabile in base b se esistono $k \in \mathbb{N} \wedge \varepsilon_0, \varepsilon_1, \cdots, \varepsilon_k \in I_b = \{0, 1, \cdots, b-1\}$ tali che $n = \varepsilon_0 + \varepsilon_1 b + \varepsilon_2 b^2 + \cdots + \varepsilon_k b^k \in \mathbb{N}$, che se eisstono si può scrivere $n = (\varepsilon_k \varepsilon_{k-1} \cdots \varepsilon_1 \varepsilon_0)_b$. Equivalentemente n è rappresentabile in base b se $\exists \{\varepsilon_i\}_{i \in \mathbb{N}}$ con $\varepsilon_i \in I_b$ tale che $\{\varepsilon_i\}_{i \in I}$ tale che $\varepsilon_n = 0 \; \forall n \geq k$ e $n = \sum_{i=0}^{k} \varepsilon_i b^i$.

10.1 Casi particolari

10.1.1 b = 0

$n = \sum_{i \in 0}^{\infty} \varepsilon_i b^i$, $\varepsilon_i \in I_0 = \emptyset$, pertanto nessun naturale si può scrivere in tale modo.

10.1.2 b = 1

$n = \sum_{i \in 0}^{\infty} \varepsilon_i b^i$, $\varepsilon_i \in I_1 = \{0\}$, pertanto si può rappresentare solo lo zero.

10.2 Teorema

Sia $b \geq 2$ allora ogni numero naturale $n \in \mathbb{N}$ è rappresentabile in modo unico in base b, ovvero $\exists! \{\varepsilon_i\}_{i \in \mathbb{N}} : \varepsilon_i \in I_b \; \forall i \in \mathbb{N}$ tale che la successione è definita nulla e vale $n = \sum_{i=0}^{k} \varepsilon_i b^i$.

10.2.1 Dimostrazione

10.2.1.1 Esistenza

Si provi per induzione di seconda forma su n. Per $n = 0$, si pone $\varepsilon_i = 0\ \forall i \in \mathbb{N}$, pertanto la successione è nulla e $\varepsilon_i = 0 \in I_b$ è vero e $n = 0 = \sum_{i=0}^{k} 0b^i$. Si supponga ora $n > 0$ e che la tesi sia vera $\forall k < n$. Siano q, r tali che $n = bq + r$ con $0 \leq r < b$, dato che $b >\geq 2$ si ha che $0 \leq q < bq \leq bq + r = n$, quindi per ipotesi esiste una successione definitivamente nulla $\{\delta_i\}$ costituita di interi tali che $0 \leq \delta_i < b$ per ogni i e tale che $q = \sum_{i=0}^{\infty} \delta_i b^i$. Pertanto $n = bq + r = b\sum_{i=0}^{\infty} \delta_i b^i + r = \sum_{i=1}^{\infty} \delta_{i-1} b^i + r = \sum_{i=0}^{\infty} \varepsilon_i b^i$, dove si è posto $\varepsilon_0 = r$ e $\varepsilon_i = \delta_{i-1}$. La successione $\{\varepsilon_i\}$ è definitivamente nulla ed inoltre $0 \leq \varepsilon_i = \delta_{i-1} < b\ \ \forall i$ e $0 \leq \varepsilon_0 = r < b$.

10.2.1.2 Unicità

Si proceda per induzione su n. Se $n = 0 = \sum_i \varepsilon_i b^i$ allora $\varepsilon_i = 0\ \ \forall i$. Si supponga ora $n > 0$ e che l'espressione in base b sia unica per tutti i numeri $k < n$, sia ora $n = \sum_{i=0}^{\infty} \varepsilon_i b^i = \sum_{i=0}^{\infty} \varepsilon'_i b^i$, allora si può scrivere: $n = b\sum_{i=1}^{\infty} \varepsilon_i b^{i-1} + \varepsilon_0 = b\sum_{i=1}^{\infty} \varepsilon_i b^{i-1} + \varepsilon'_0$. Ora, per l'unicità della divisione euclidea si ha che $\varepsilon_0 = \varepsilon'_0$ e $q = \sum_{i=1}^{\infty} \varepsilon_i b^{i-1} = \sum_{i=1}^{\infty} \varepsilon'_i b^{i-1} + \varepsilon_0$. Come prima $q < n$ e pertanto per ipotesi di induzione si ha che $\varepsilon_i = \varepsilon'_i\ \ \forall i \geq 1$.

Capitolo 11

Divisibilità

11.0.0.1 Definizione

Dati due interi n, m si dice che n è un divisore di m (o che m è un multiplo di n) se $\exists k \in \mathbb{Z} : m = nk$. Si indica con $n|m$.

11.0.0.2 Numeri primi

Il numeri n si dice primo se i suoi unici divisori sono $\pm 1, \pm n$.

11.1 Proprietà

1. $n|m \wedge m|q \Rightarrow n|q$.
2. $n|m \wedge m|n \Rightarrow n0 \pm m$.

11.1.0.1 Dimostrazione

1. Se $m = kn$ e $q = hm$ allora $q = hkm = (hk)m$, ossia $n|q$.
2. Se $n = mk$ e $m = nh$ allora $m = hkm$, quindu $m(1 - hk) = 0$, perciò $m = n = 0$, oppure $1 - hk = 0$, allora $h = k = \pm 1$, pertanto $n = \pm m$.

11.2 Massimo comune divisore

11.2.0.1 Definizione

Dati due interi ne m entrambi non nulli, si dice che d è un massimo comune divisore tra n e m se:

1. $d|n \wedge d|m$.
2. $c|n \wedge c|m \Rightarrow c|d$.

SI dirà che d è il massimo comune divisore di n e m se è un massimo comune divisore positivo, viene indicato con (n, m).

11.2.1 Unicità del massimo comune divisore

Se d e d' sono due massimi comunei divisori tra n e m allora $d' = \pm d$.

11.2.1.1 Dimostrazione

Essendo d è un divisore comune di n, m e d' il massimo comune divisoresi ha che $d|d'$, scambiando i ruoli di d e d' si ottiene $d'|d$, pertanto per le proprietà della divisibilità $d' = \pm d$.

11.2.2 Esistenza del massimo comune divisore

Dati due numeri $n, m \in \mathbb{Z}$ non entrambi nulli esiste ilmassimo comune divisore di n e m.

11.2.2.1 Dimostrazione

Si consideri l'insieme $S = \{s \in \mathbb{Z} | s > 0, \exists x, y \in \mathbb{Z} : s = nx + my\}$. $S \neq \emptyset$ dato che $nm + mm > 0$ (dato che m e n sono entrambi non nulli). Sia $d = nx + my = \min S$, si dimostri che d è il massimo comune divisore. Se $c|n \wedge c|m$ allora $n = ck$ e $m = ch$, perciò $d = nx + my = xkx + chy = c(kx + hy)$, ossia $c|d$. Si dimostri ora che $d|n$. Si consideri ora la divisione euclidea tra n e d, ovvero $n = dq + r$ con $0 \leq r < d$, se $r > 0$ allora $r = n - dq = n - (nx + my)q = n(1 - qx) + (-m)y$ è un elemento di S. Questo è assurdo perchè $r < d$ e $d = \min S$, pertanto $r = 0$, ossia $d|n$. Si prova in modo analogo che $d|m$.

11.2.3 Numeri coprimi

$n, m \in \mathbb{Z}$ non entrambi nulli si dicono comprimi se $(n, m) = 1$.

11.2.3.1 Osservazione

$(n, m) = 1 \Leftrightarrow \exists x, y \in \mathbb{Z} : nx + my = 1$, in particolare $(n, n + 1) = 1 \forall n$, infatti $1 = (n + 1)1 + n(-1)$.

11.2.4 Massimo comune divisore e numeri coprimi

Sia $d = (n, m)$, allora $(\frac{n}{d}, \frac{m}{d}) = 1$.

11.2.4.1 Dimostrazione

$d = nx + my$, perciò $1 = \frac{n}{d}x + \frac{m}{d}y$.

11.3 Algoritmo di Euclide

Siano $n, m \in \mathbb{Z}, m \neq 0$. Sia $n = mq + r$ e la divisione euclidea di n per m allora $\{c \in \mathbb{Z} | c|n \wedge c|m\} = \{c \in \mathbb{Z} | c|m \wedge c|r\}$, in particolare quindi $(n, m) = (m, r)$.

11.3.0.1 Dimostrazione

Se $c|n$ e $c|m$ allora $n = ch$ e $m = ck$, perciò $r = n - mq = ch - ckq = c(h - kq)$, ossia $x|r$ e $c|m$, viceversa se $x|r$ e $c|m$ allora $m?ch$ e $r = ck$, pertanto $n = mq + r = chq + ck = c(hq + r)$, ossia $c|n$ e $c|m$.

11.4 Proprietà dei numeri coprimi

1. $(n, m) = 1 \wedge n|mq \Rightarrow n|q$.
2. $(n, m) = 1 \wedge n|q \wedge m|q \Rightarrow nm|q$.

11.4.0.1 Dimostrazione

1. Se $(n, m) = 1$ allora esistono $x, y \in \mathbb{Z}$ tali che $1 = nx + my$, perciò $q = nqx + mqy$. Pertanto se $n|mp$, esiste h tale che $mq = nh$, pertanto $q = nqx + nhy = n(qx + hy)$.
2. $n|q$, pertanto $q = nh$, dato che $m|q = nh$ e $(n, m) = 1$, allora per la prima si ha che $m|h$, ovvero $h = km$, perciò $q = nh = nmk$, ossia $nm|q$.

11.4.1 Corollario

p è primo se e solo se $\forall n, m \in \mathbb{Z}$ si ha che $p|nm \Rightarrow p|n$ oppure $p|m$.

11.4.1.1 Dimostrazione

Si supponga che $p|nm$, dato che p è primo, allora $(p, n) = 1$ e per la proposizione precedente si ha che $p|m$. Viceversa si supponga che $\forall n, m \in \mathbb{Z}$ si ha che $p|nm \Rightarrow p|n$ oppure $p|m$ allora se $p = dh$ allora $p|dh$, pertanto $p|d$, pertanto, come visto precendentemente $d = \pm p$ e $h = \pm 1$ oppure $p|h$, quindi $h = \pm p$ e $d = \pm 1$.

11.5 Minimo comune multiplo

11.5.0.1 Definizione

Dati due interi $n, m \in \mathbb{Z}$ si dice che M è un minimo comune multiplo di n e m se:

1. $n|M$ e $m|M$.

2. Se $n|c$ e $m|c$ allora $M|c$.

Come nel caso del massimo comune divisore si dimostra che due minimi comuni multipli sono uguali a meno del segno, pertanto si chiama minimo comune multiplo quello positivo e viene indicato con $[n, m]$.

11.5.1 Esistenza

Siano $n, m \in \mathbb{Z}$ non entrambi nulli allora esiste il minimo comune multiplo tra n e m.

11.5.1.1 Dimostrazione

Sia $M = \frac{nm}{(n,m)} = n'm'(n, m)$ dive si è posto $n = n'(n, m)$ e $m = m'(n, m)$. Chiaramente allora $M = nm' = n'm$, pertanto $n|M$ e $m|M$. Se $n|c$ e $m|c$ allora $(n, m)|c$, pertanto posto $c = c'(n, m)$ si ha che $n'|c'$ e $m'|c'$. Dato che $(n', m') = 1$, come visto precedentemente si ha che $n'm'|c'$ perciò che $M = n'm'(n, m)|c'(n, m) = c$.

11.6 Teorema fondamentale dell'algebra

$\forall n \in \mathbb{Z}, n \geq 2$ esistono numeri primi $p_1, p_2, \cdots, p_k > 0$ tali che $n = p_1 p_2 \cdots p_k$. Se anche $q_1, \cdots, q_h$ esiste una bigezione $\sigma : \{1, 2, \cdots, h\} \to \{1, 2, \cdots k\}$ tale che $q_i = p_{\sigma(i)}$. Ovvero ogni intero maggiore di 1 si scrive in modo unico, a meno dell'ordine, come prodotto di numeri interi positivi.

11.6.1 Dimostrazione

Si proceda per induzione si n. Se $n = 2$ non c'è nulla da dimostrare in quanto primo. Si supponga $n > 2$ e che la tesi sia vera $\forall k < n$. Se n è primo non c'è nulla da dimostrare, se n non è primo allora esistono due numeri $d_1 d_2$ con $1 < d_1, d_2 < n$ tali che $n = d_1 d_2$. Per ipotesi di induzione esistono dei primi positivi p_i e q_j tali che $d_1 = p_1 \cdots p_{k_1}$ e $d_2 = q_1 \cdots q_{k_2}$, allora $n = p_1 \cdots p_{k_1} q_1 \cdots q_{k_2}$ è prodotto di primi positivi.

11.6.1.1 Unicità

Sia $n = p_1 \cdots p_k = q_1 \cdots q_h$ con p_i e q_j primi positivi e $k \leq h$. Si proceda per induzione su k. Se $k = 1$ allora $n = p_1 = q_1 \cdots q_h$, quindi $q_j | p_1 \forall j$ e dato che p_1 è primo ogni $q_j = 1 \vee q_j = p_1$. Poichè per ipotesi ogni $q_j > 1$ allora $q_j = p_1$ per ogni j. Se ora fosse $h > 1$ si avrebbe $n = q_1 \cdots q_h \geq q_1 q_2 = p_1^2 > p_1 = n$, che sarebbe assurdo, quindi $h = 1$ e $q_1 = p_1$. Sia ora $k > 1$, allora $p_k | n = q_1 \cdots q_h$, pertanto come visto precedentemente esiste un j tale che $p_k | q_j$. Dato che sia p_k che q_j sono primi positivi, allora $p_k = q_j$. Ora si ottiene che $p_1 \cdots p_{k-1} = q_1 \cdots q_{j-1} q_{j+1} \cdots q_h$, pertanto per ipotesi di induzione si può dire che le due fattorizzazioni hanno lo stesso numero di elementi, ossia $k - 1 = h - 1$

e che esiste una bigezione $\delta : \{1, \cdots, j-1, j+1, \cdots, k\} \to \{1, \cdots, k-1\}$ tale che $q_i = p_{\delta(i)} \forall i$. Si definisca ora $\sigma : \{1, 2, \cdots, n\} \to \{1, 2, \cdots n\}$ tale che $\sigma(i) = \begin{cases} k & i = j \\ \delta(i) & i \neq j \end{cases}$. Si ottiene una bigezione tale che $q_i = p_{\sigma(i)} \forall i$.

11.6.2 Esistenza di infiniti numeri primi

I numeri primi sono infiniti.

11.6.2.1 Dimostrazione

Si supponga per assurdo che $p_1, \cdots, p_n$ siano tutti primi. Si consideri $n = p_1 \cdots p_n + 1$. Si nota che $n > 1$ e non è divisibile per nessun p_i e quindi n sarebbe un numero maggiore di 1 che non è divisibile per nessun primo e ciò contraddice il teorema fondamentale dell'algebra.

Capitolo 12

Congruenza

12.0.0.1 Definizione

Siano $a, b \in \mathbb{Z}$, si dice che a è congruo a b modulo n , ovvero $a \equiv b \mod n$ se $n|a-b$.

12.0.1 Proprietà

Valgono le seguenti proprietà $\forall a, b, c, n \in \mathbb{Z}$:

1. Riflessiva: $a \equiv a \mod n$.
2. Simmetrica: $a \equiv b \mod n \Rightarrow b \equiv a \mod n$.
3. Transitiva: $a \equiv b \mod n b \equiv c \mod n \Rightarrow a \equiv c \mod n$.

12.0.1.1 Dimostrazione

1: $n|0 = a - a$.
2: $n|a-b \Rightarrow a-b = kn$, pertanto $b-a = (-k)n$, perciò $n|b-a$, ovvero $b \equiv a \mod n$.
3: $a-b = kn$ e $b-c = hn$, allora $a-c = a-b+b-c = kn+hn = (k+h)n$, pertanto $a \equiv c \mod n$.

12.0.1.2 Osservazioni

Si ricordi la definizione di relazione di equivalenza: una relazione si dice di equivalenza se valgono le proprietà riflessiva, simmetrica e transitiva.

1. È prassi denotare le relazioni di equivalenza con $\sim, \equiv, \approx$.
2. La definizione di congruenza in modulo n può essere allora rienunciato dicendo che la relazione di congruenza in modulo n è una relazione d'equivalenza su $\mathbb{Z}$

12.1 Classi di equivalenza

Siano X un insieme non vuoto e sia $\sim$ una relazione di equivalenza su X. La classe di equivalenza di $x \in X$ rispetto a $\sim$ è l'insieme: $[x]_\sim := \{y \in X | y \sim x\}$. Il simbolo della relazione può essere omessso.

12.1.1 Insieme quoziente

Si definisce l'inseme quoziente di X modulo $\sim$ come l'insieme costituito da tutte le classi di equivalenza: $X/_\sim := \{[x]_\sim \in P(X) | x \in X\}$.

12.1.2 Proprietà

Sia X un insieme e $\sim$ una relazione di equivalenza su X, allora $\forall x, y, z \in X$:

1. $x \in [x]_\sim$.
2. $[x]_\sim = [y]_\sim \Leftrightarrow x \sim y$.
3. $[x]_\sim \cap [y]_\sim \neq \emptyset \Leftrightarrow [x]_\sim = [y]_\sim$.

12.1.2.1 Dimostrazione

1: Si ottiene dalla proprietà riflessiva delle operazioni di equivalenza.
2: si supponga che $[x]_\sim = [y]_\sim$ vale $x \in [x]_\sim = [y]_\sim \Leftrightarrow x \sim y$. Si verifichi l'implicazione inversa considerando $z \in [x]$, allora $z \sim x$ e per la proprietà transitiva delle relazioni di equivalenza $z \equiv y$, ovvero $z \sim y$, ossia $[x] \subset [y]$, scambiando i ruoli di x e y si ottiene la relazione inversa e pertanto $[x] = [y]$.
3: Se $z \in [x] \cap [y]$ allora $z \sim x$ e $z \sim y$, che per la proprietà transitiva e simmetrica verifica che $x \sim y$, pertanto $[x] = [y]$.

12.1.2.2 Osservazione

Le proprietà descritte sopra garantiscono che l'insieme delle classi di equivalenza di un insieme rispetto ad una relazione d'equivalenza costituisce una partizione dell'insieme, ovvero sono una collezione $\mathcal{P}$ di sottoinsiemi di X tali che:

- $\forall A \in \mathcal{P}, A \neq \emptyset$.
- $\bigcup_{A \in \mathcal{P}} A = X$.
- $\forall A, b \in \mathcal{P}, A \neq B \Rightarrow A \cap B = \emptyset$.

12.2 Classi di congruenza

12.2.0.1 Definizione

Siano $a, n \in \mathbb{Z}$, si chiama classe di congruenza di a modulo n l'insieme $[a]_n = \{x \in \mathbb{Z} | x \equiv a \mod n\}$. Verrà indicato $\mathbb{Z}_{/n\mathbb{Z}} = \{[a]_n | a \in \mathbb{Z}\}$.

12.2.0.2 Osservazioni

1. $x \equiv a \mod n \Leftrightarrow n|(x-a) \Leftrightarrow \exists k \in \mathbb{Z} : x - a = kn \Leftrightarrow \exists k \in \mathbb{Z} : x = kn + a$, pertanto $[a]_n = \{a + kn | z \in \mathbb{Z}\}$.
2. La classe di congruenza di a modulo n non è altro che la classe di equivalenza di a rispetto alla relazione di equivalenza $\equiv \mod n$. $\mathbb{Z}_{/n\mathbb{Z}}$ è pertanto l'insieme quoziente. di $\mathbb{Z}$ rispetto a tale operazione.

12.2.1 Proprietà

$\forall a, b \in \mathbb{Z}$:

1. $a \in [a]_n$.
2. $[a]_n = [b]_n \Leftrightarrow a \equiv b \mod n$.
3. $[a]_n \cap [b]_n \neq \emptyset \Leftrightarrow [a]_n = [b]_n$.

12.2.2 Le classi modulo n sono esattamente n

Se $n > 0$ e r è il resto della divisione euclidea di a per n allora $a \equiv r \mod n$.

12.2.2.1 Dimostrazione

$a = nq + r$, pertanto $n|nq = a - r$.

12.2.3 Corollario

Se $n > 0$ allora $\mathbb{Z}_{/n\mathbb{Z}}$ ha n elementi.

12.2.3.1 Dimostrazione

Dalla proposizione dimostrata precedentemente e dalla seconda proprietà delle classi di congruenza segue immediatamente che l'insieme ha al più n elementi, più precisamente $[0]_n, [1]_n, \cdots, [n-1]_n$. D'altronde se $0 \leq h < k < n$ allora $0 < k - h < n$, pertanto $n \not| (k-h)$, pertanto $[h]_n \neq [k]_m$.

12.2.3.2 Osservazione

È facile notare come mai le classi di congruenza modulo n vengono anche chiamate classi di resto modulo n.

12.3 Somma e prodotto di classi di congruenza

Siano $a, b, a', b', n \in \mathbb{Z}$ e si supponga che $a \equiv a' \mod n$ e $b \equiv b' \mod n$, allora:

1. $a + b = a' + b' \mod n$.
2. $a \cdot b = a' \cdot b' \mod n$.

12.3.0.1 Dimostrazione

1: Se $n|(a-a')$ e $n|(b-b')$, allora $n|((a-a')+(b-b')) = ((a+b)-(a'+b'))$.
2: $\exists k, h \in \mathbb{Z}$ tali che $a = a' + kn$ e $b = b' + hn$, allora moltiplicando membro a membro si ottiene $ab = a'b' + a'hn + b'kn + hkn^2 = a'b' + n(a'h + b'k + hkn)$, da cui segue immediatamente la tesi.

12.3.1 Operazioni tra classi di modulo n

La proposizione precedente permette di ben definire le operazioni di somma e prodotto tra le classi modulo n ponendo: $[a]_n + [b]_n = [a+b]_n$ e $[a]_n[b]_n = [ab]_n$.

12.3.1.1 Dimostrazione

Se $[a]_n = [a']_n$ e $[b]_n = [b']_n$ allora per la seconda proprietà delle classi di congruenza segue che $a \equiv a' \mod n$ e $b \equiv b' \mod n$, pertanto dalla proposizione precedente $a + a' \equiv b + b' \mod n$ e $aa' \equiv bb' \mod n$, dalla stessa proprietà si ottiene perciò $[a+b]_n = [a'+b']_n$ e $[ab]_n = [a'b']_n$.

12.3.1.2 Osservazione

Le operazioni tra classi di congruenza godono delle stesse proprietà delle operazioni tra naturali con due importanti differenza:

- Ci possono essere classi diverse da 0 che moltiplicate tra loro danno 0.
- Se $n > 0$ allora $\sum_{i=1}^{n} 1 = 0 \in \mathbb{Z}_{/n\mathbb{Z}}$.

12.4 Teorema cinese del resto

Il sistema di congruenze:

$$\begin{cases} x \equiv a \mod n \\ x \equiv b \mod n \end{cases}$$

ha soluzione se e solo se $(n,m)|b-a$. Se c è una soluzione del sistema allora gli elementi di $[c]_{[n,m]}$ sono tutte e sole le soluzioni del sistema.

12.4.0.1 Dimostrazione

Sia c una soluzione del sistema , allora esistono $h, k \in \mathbb{Z}$, tali che $c = a + hn = b + km$, pertanto $a - b = km - hn$, dal fatto che $(n,m)|n$ e $(n,m)|m$ si ha che $(n,m)|a-b$. Viceversa si supponga che $(n,m)|a-b$ allora come visto precedentemente $\exists h, k \in \mathbb{Z}$ tali che $a-b = hn+km$, allora $a-hn = b-km$ e si ha evidentemente che c risolve entrambe le congruenze. Ora essendo $S = \{x \in \mathbb{Z} | x$ risolve il sistema$\}$, si deve provare che se c è una soluzione allora $S = [c]_{[n,m]}$. Si supponga $S \subset [c]_{[n,m]}$. Sia c' un'altra soluzione, allora $c = a + hn = b + km$

e $c' = a + h'n = bk'n$, pertanto sottraendo si ha $c - c' = a + hn - a' - h'n = (h - h')n \Rightarrow n|(c - c')$, inoltre $c - c' = b + km - b' - 'm = (k - k')m \Rightarrow m|(c - c')$, pertanto $[n, m]|c - c'$, ossia $c' = c \mod [n, m]$, ovvero $c' \in [c]_{[n,m]}$. Si consideri $[c]_{[n,m]} \subset S$. Sia $c' \in [c]_{[n,m]}$, ovvero $c' = c + h[n, m]$, dal fatto che $c \equiv a \mod n$ e che $h[n, m] \equiv 0 \mod n$ segue per una proposizione precedente che $c' = c + h[n, m] \equiv a \mod n$, in modo analogo si ha che $c' \equiv b \mod m$ perciò $c' \in S$.

Capitolo 13

Invertibilità in modulo n

13.0.0.1 Definizione

Sia $a \in \mathbb{Z}$, si dirà che a è invertibile modulo n se esiste $x \in \mathbb{Z}$ tale che $ax \equiv 1 \mod n$ in $\mathbb{Z}_{/n\mathbb{Z}}$. Il tale x si dice inverso di a modulo n.

13.0.1 Condizione di invertibilità

a è invertibile in modulo n se e solo se $(a, n) = 1$.

13.0.1.1 Dimostrazione

Se a è invertibile e x è il suo inverso allora $n|(ax - 1)$, pertanto esiste $k \in \mathbb{Z}$ tale che $nk = ax - 1$, pertanto $1 = nk - ax$, da cui, come visto precedentemente $1 = (a, n)$. Viceversa se $1 = (a, n)$ allora esistono $\alpha, \beta \in \mathbb{Z}$ tali che $1 = \alpha a + n\beta$, da cui $\alpha a \equiv 1 \mod n$.

13.0.2 Unicità dell'inverso

Siano x, y due inversi di a modulo n, allora $x = y$ in $\mathbb{Z}_{/n\mathbb{Z}}$.

13.0.2.1 Dimostrazione

Dal fatto che $ax = 1$ in $\mathbb{Z}_{/n\mathbb{Z}}$, moltiplicando entrambi i membri per y ed usando la proprietà associativa e commutativa si ottiene: $[y]_n = [1]_n[y]_n = ([a]_n[x]_n)[y]_n = [x]_n([a]_n[y]_n = [1]_n[x]_n = [x]_n$.

13.0.3 Unicità dell'invertibile

Sia a invertibile modulo n e sia $a' = a$ in $\mathbb{Z}_{/n\mathbb{Z}}$, allora anche a' è invertibile e ha lo stesso inverso di a.

13.0.3.1 Dimostrazione

Se $ax = 1$ in $\mathbb{Z}_{/n\mathbb{Z}}$ allora $m|(ax-1)$, se $a' = a$ in $\mathbb{Z}_{/n\mathbb{Z}}$ allora esiste k tale che $a' = a + kn$, allora $a'x - 1 = ax - 1 + knx$ è divisibile per n e $a'x = 1$ in $\mathbb{Z}_{/n\mathbb{Z}}$.

13.0.4 Osservazioni

1. Si osservi che le due proposizioni precedenti permettono di definire l'invertibilità e l'inverso di una classe di congruenza: data una classe $[a]_n$, se a è invertibile, per la seconda delle due proposizioni l'insieme dei suoi inversi costituisce una classe di congruenza che dipende da $[a]_n$ e non da a, la classe costituita dagli inversi di a viene chiamata inverso di $[a]_n$ e viene denotata come $[a]_n^{-1}$.

2. La definizione di inverso di una classe di congruenza ne garantisce l'unicità: è l'unica tale che $[a]_n[a]_n^{-1} = [1]_n$. Questo fatto può essere provato utilizzandole proprietà formali delle operazioni. Si supponga che $u \in \mathbb{Z}_{/n\mathbb{Z}}$ e che esistano v_1, v_2 tali che $uv_1 = v_1u = 1$ e $uv_2 = v_2u = 1$, allora $v_1 = 1v_1 = uv_2v_1 = 1v_2 = v_2$.

13.0.5 Condizione di invertibilità per classi di congruenza

$[a]_n$ è invertibile se e solo se $(a, n) = 1$.

13.0.6 Corollario

Se p è primo, ogni elemento non nullo di $\mathbb{Z}_{/p\mathbb{Z}}$ è invertibile.

13.0.6.1 Dimostrazione

Se $a \neq 0$ in $\mathbb{Z}_{/p\mathbb{Z}}$, allora $p \not| a$ e, dato che p è primo $(p, a) = 1$, da cui la tesi.

Capitolo 14

Equazioni lineari modulo n

14.0.0.1 Osservazione

Si osservi che se a è invertibile in $\mathbb{Z}_{/n\mathbb{Z}}$ e se $c, d \in \mathbb{Z}_{/n\mathbb{Z}}$ sono tali che $ac = ad \in \mathbb{Z}_{/n\mathbb{Z}}$ allora necessariamente $c = d \in \mathbb{Z}_{/n\mathbb{Z}}$, in quanto se x è tale che $ax = 1$, $ac = ad \Rightarrow axc = axd \Rightarrow 1c = 1d \Rightarrow c = d$. In particolare se a è invertibile allora da $ab = 0$ si deduce che $b = 0$. Se p è primo tutti gli elementi non nulli sono invertibili, pertanto se $a \neq 0 \in \mathbb{Z}_{/n\mathbb{Z}}$ allora $ac = ad \in \mathbb{Z}_{/p\mathbb{Z}}$ implica che $c = d \in \mathbb{Z}_{/p\mathbb{Z}}$, in particolare $ab = 0$ implica che $a = 0 \vee b = 0 \in \mathbb{Z}_{/p\mathbb{Z}}$.

14.1 Soluzioni di una congruenza

Siano $a, b \in \mathbb{Z}$, allora esiste un intero x tale che: $ax \equiv b \mod n$ se e solo se $(a, n)|b$. Se x_0 è una soluzione della congruenza, allora detto $n' = \frac{n}{(a,n)}$, l'insieme delle soluzioni è dato da $[x_0]_{n'} = \{x_0 + kn' | k \in \mathbb{Z}\}$.

14.1.0.1 Dimostrazione

Se $ax \equiv a \mod n$ allora $n|(ax - b)$, pertanto esiste k tale che $(ax - b) = kn$, ossia $b = ax - kn$, pertanto $(a, b)|b$. Viceversa si supponga che $(a, n)|b$. Siano α, β tali che $(a, n) = \alpha a + \beta n$ e sia k tale che $b = k(a, n)$, allora $b = k(\alpha a + \beta n)$, da cui $n|(a(k\alpha) - b)$, ossia $k\alpha$ è una soluzione della congruenza. Si provi ora che l'insieme delle soluzioni è $[x_0]_{n'}$. Si provi che se $x_1 \in [x_0]_{n'}$ è una soluzione: $x_1 = x_0 + kn'$, pertanto $ax_1 = ax_0 + \frac{kan}{(a,n)}$, da cui $ax_1 - x_0 = \frac{kan}{(a,n)}$, dato che $\frac{a}{(a,n)} \in \mathbb{Z}$, n è un multiplo di $\frac{kan}{(a,n)}$, ovvero $ax_1 \equiv ax_0 \mod n$. Dato che $ax_0 \equiv b \mod n$ anche $ax_1 \equiv b \mod n$. Viceversa se $ax_1 \equiv b \mod n$ allora $ax_1 \equiv ax_2 \mod n$ da cui si ricava che $a(x_1 - x_0) \equiv 0 \mod n$, ovvero $n|a(x_1 - x_0)$. Allora, dato che $n'|n$ anche $n'|a'(x_1 - x_0)$, essendo $a' = \frac{a}{(a,n)}$, come visto in precedenza $(n', a') = 1$, usando la proposizione precedente $n'|(x_1 - x_0)$.

14.1.0.2 Osservazione

Questa dimostrazione mostra un metodo operativo per trovare una soluzione di una congruenza: basta usare l'algoritmo di Euclide per trovare α e β tali che $(a, n) = \alpha a + \beta n$.

14.2 Congruenza e classi

Siano $a, b \in \mathbb{Z}$ e $n \in \mathbb{N}$ tale che $(a, n) = 1$, allora l'insieme degli x tali che $ax \equiv b \mod n$ sono una classe di congruenza modulo n.

14.2.0.1 Dimostrazione

La congruenza ha soluzioni per quanto visto sopra. Passando a considerare le classi di congruenza si ha che se x è una soluzione allora $[a]_n[x]_n = [b]_n$ e dato che $[a]_n$ è invertibile implica che, moltiplicando entrambi i membri per $[a]_n^{-1}$ che $[x]_n = [a]_n^{-1}[b]_n$, provando la tesi.

14.3 Il teorema di Fermat

14.3.1 Prodotto di elementi in un insieme quoziente

Siano $u, v \in \mathbb{Z}_{/n\mathbb{Z}^\star}$ allora $uv \in \mathbb{Z}_{/n\mathbb{Z}^\star}$.

14.3.1.1 Dimostrazione

$uv(v^{-1}u^{-1}) = (vv^{-1})(uu^{-1}) = 1$.

14.3.1.2 Osservazione

Immediata conseguenza della proposizione precedente è che se si fissa $u \in \mathbb{Z}_{/n\mathbb{Z}^\star}$ allora è possibile definire la funzione $L_u : \mathbb{Z}_{/n\mathbb{Z}^\star} \to \mathbb{Z}_{/n\mathbb{Z}^\star}$ ponendo $L_u(v) = uv$. Per quanto osservato sopra tale funzione risulta iniettiva, infatti $L_u(v_1) = L_u(V_2)$ vuol dire che $uv_1 = uv_2$ e dato che u è invertibile $v_1 = v_2$ e dato che $\mathbb{Z}_{/n\mathbb{Z}^\star}$ è finito, allora è bigettiva.

14.3.1.3 Funzione di Eulero

Dato un numero naturale n si indica con $\Phi(n)$ il numero di naturali minori o uguali a n e coprimi con n. Questa funzione si chiama funzione Φ di Eulero.

14.3.2 Cardinalità dell'insieme quoziente

$\forall n > 0, |\mathbb{Z}_{/n\mathbb{Z}^\star}| = \Phi(n)$.

14.4 Enunciato

Sia $u \in \mathbb{Z}_{/n\mathbb{Z}^\star}$, allora $u^{\Phi(n)} = 1 \in \mathbb{Z}_{/n\mathbb{Z}}$.

14.4.0.1 Dimostrazione

Sia $k = \Phi(n)$ e siano $x_1, \cdots, x_k$ tutti gli elementi di $\mathbb{Z}_{/n\mathbb{Z}^\star}$, dato che l'applicazione L_u è bigettiva $L_u(x_1), \cdots, L_u(x_k)$ sono ancora tutti gli insiemi di $\mathbb{Z}_{/n\mathbb{Z}^\star}$, pertanto per commutatività del prodotto $x_1 \cdot x_2 \cdot \cdots \cdot x_k = ux_1 \cdot ux_2 \cdot \cdots \cdot ux_k = u^k x_1 \cdot x_2 \cdot \cdots \cdot x_k$. Come dimostrato precedentemente $x_1 \cdot x_2 \cdot \cdots \cdot x_k$ è invertibile, pertanto $u^k = 1$.

14.4.1 Corollario

Se p è primo allora per ogni $x \neq 0$ in $\mathbb{Z}_{/p\mathbb{Z}}$ si ha che $x^{p-1} = 1 \in \mathbb{Z}_{/n\mathbb{Z}}$.

14.4.1.1 Dimostrazione

Segue direttamente dal teorema precedente in quanto se p è primo tutti i numeri minori di p sono coprimi con p, pertanto $\Phi(p) = p - 1$.

14.5 Crittografia RSA

14.5.1 Proposizione fondamentale della crittografia RSA

Sia c coprimo con $\Phi(n)$, allora l'applicazione $C : \mathbb{Z}_{/n\mathbb{Z}^\star} \to \mathbb{Z}_{/n\mathbb{Z}^\star}$ definita da $x \to x^c$ è invertibile e la sua inversa è data da $D(x) = x^d$ essendo $cd \equiv 1 \mod \Phi(n)$.

14.5.1.1 Dimostrazione

Se x è coprimo con $\Phi(n)$ allora esiste un d come nell'enunciato tale che $cd \equiv 1 \mod \Phi(n)$, allora $cd = k\Phi(n) + 1$, pertanto, utilizzando il teorema di Fermat si ottiene: $D(C(x)) = (x^c)^d = x^{cd} = x^{k\Phi(n)+1} = x(x^{\Phi(n)})^k = x1^k = x$. È del tutto analoga la prova di $C(D(x))\forall x$, da cui la tesi.

14.5.2 Metodo di crittografia RSA

La proposizione sopra dimostrata è alla base del metodo RSA di crittografia a chiave pubblica. Si supponga che A debba trasmettere un messaggio riservato a B, allora B rende noti due numeri m e c (modulo e chiave di codifica) tali che $(c, \Phi(m)) = 1$. L'alfabeto della trasmissione sarà allora costituito da $\mathbb{Z}_{/n\mathbb{Z}^\star}$ e durante la codifica la lettera x verrà sostituita con la lettera x^c modulo m. Il fatto che $(c, \Phi(m)) = 1$ garantisce che si possa determinare un numero d tale che $cd \equiv 1 \mod \Phi(m)$, ossia tale che $cd = k\Phi(m) + 1$. Per decodificare il messaggio basta ora elevare alla potenza d in quanto $(x^c)^d = x^{cd} = x^{k\Phi(m)+1} =$

$(x^{\Phi(m)})^k x = i^k x = x \in \mathbb{Z}_{/m\mathbb{Z}}$. Chiaramente chiunque conosca c e $\Phi(m)$ è in grado di determinare la chiave di codifica d, essendo per determinare $\Phi(m)$ necessario calcolare la scomposizione in fattori primi di m ed essendo questo un lavoro computazionalmente complesso, soltanto chi ha costruito m e c è in grado di determinare c facilmente. I numeri che vengono utilizzati sono del tipo $m = pq$ con p e q primi, per i quali si ha $\Phi(m) = (p-1)(q-1)$ e per i quali determinare $\Phi(m)$ è computazionalmente equivalente a trovare la fattorizzazione di m.

Capitolo 15

I grafi

Dato V un insieme e $k \in \mathbb{N}$, $\binom{V}{k} := \{A \in P(V) || A| = k\}$ che corrisponde esattamente: $|\binom{V}{k}| = \binom{|V|}{k}$.

15.0.0.1 Definizione

Un grafo G è una coppia (V, ε), dove V è un insieme non vuoto detto insieme dei vertici di G e ε è un sottoinsieme di $\binom{V}{2}$, detto insieme dei lati di G. Chiamando $\{v, w\}$ 2-sottoinsiemi di V, tale elemento si chiama lato di G, v e w si chiamano estremi di tale lato, inoltre se due vertici sono tali che $\{v, w\} \in \varepsilon$ si dice anche che v e w sono adiacenti.

15.1 Grafici notevoli

15.1.1 Cammino di lunghezza n

Si fissi un numero $n \in \mathbb{N}$, si definisce il cammino P_n di lunghezza n come $V(P_n) = \{0, 1, \cdots, n\}$. $\varepsilon(P_n) = \{\{i, i+1\} \in \binom{V(P_n)}{2} | i \in \{0, 1, \cdots, n-1\}\}$, dove $\varepsilon(P_0)$ ha un unico vertice ma non ci sono lati. n sarà il numero di lati.

15.1.1.1 Cammino di lunghezza infinita

Si definisce il cammino di lunghezza infinita P_∞ dove, dove $V(P_\infty) = \mathbb{N}$, e $\varepsilon(P_\infty) = \{\{i, i+1\} \in \binom{V(P_n)}{2} | i \in \mathbb{N}\}$. Un altro cammino infinito include $\mathbb{Z}$.

15.1.2 Ciclo

Sia $n \geq 3$, si definisce il ciclo C_n di lunghezza n, o n-ciclo, ponendo $C(C_n) = \{1, 2, \cdots, n\}$ e $\varepsilon(C_n) = \{\{i, i+1\} \in \binom{V(n)}{2} | i \in \{1, \cdots, n-1\}\} \cup \{\{1, n\}\}$.

15.1.3 Grafo completo

Sia $n \geq 1$ K_n un grafo completo su n vertici dove $V(K_n) = \{1, 2, \cdots, n\}$ e $\varepsilon(K_n) = \binom{V(K_n)}{2}$.

15.1.4 Grafo completo partito n e m vertici

Sia $K_{n,m}$, $V(K_{n,m}) = \{1, \cdots, n+m\}$, $\varepsilon(K_{n,m}) = \{\{i,j\} \in \binom{V(K_{n,m})}{2} | i \in \{1, \cdots, n\}, j \in \{n+1, \cdots, n+m\}\}$.

15.2 Sottografi e sottografi indotti

15.2.0.1 Definizione

Si supponga $G = (V, \varepsilon)$ e $G' = (V', \varepsilon')$ siano due grafi, si dice che G' è un sottografo di G se $V' \subset V$ e $\varepsilon' \subset \varepsilon$.

15.2.0.2 Osservazione

$G' < G \wedge G'' < G' \Rightarrow G'' < G$

15.2.1 Sottografo indotto da V'

Sia $G = (V, \varepsilon)$ un grafo e sia $V' \subset V$, $V' \neq \emptyset$. Il sottografo G' di G definito ponendo $G' = (V', \varepsilon \cap \binom{V'}{2})$, si indica con $G' = G[V']$

15.3 Morfismi dei grafi

15.3.0.1 Definizione

Siano $G = (V, \varepsilon)$ e $G' = (V', \varepsilon')$ due grafi. SIa $f : V \to V'$ una funzione iniettiva, si dice che f è un morfismo da G in G' se preserva l'adiacenza nel senso seguente; $\forall \epsilon = \{v, w\} \in \varepsilon, f(\epsilon) = \{f(v), f(w)\} \in \varepsilon'$, i questo caso si scrive $f : G \to G'$.

15.3.1 Isomorfismo

15.3.1.1 Definizione

Un morfismo $f : V \to V'$ si dice isomorfismo da G a G' se f è bigettiva e f^{-1} è un morfismo. Equivalentemente Se valgono le seguenti proprietà:

- f è una bigezione.
- $\forall e \in \varepsilon(G) : f(e) \in \varepsilon(G') \wedge e \in \binom{V(G)}{2}, f(e) \in \varepsilon(G') \Rightarrow e \in \varepsilon(G)$

La seconda proprietà può essere rienunciata come $\{f(e) \in \binom{V(G')}{2} | e \in \varepsilon(G)\} = \varepsilon(G')$, ovvero le immagini di tutti i lati sono tutti e soli i lati del grafo in arrivo.

15.3.1.2 Relazione di isomorfismo

Due grafi G e G' si dicono isomorfi se $\exists f : G \to G'$ isomorfismo. In questo caso si nota con $G \cong G'$. Dati tre grafi G, G', G'':

1. $G \cong G$ (si consideri l'identità dei vertici).
2. $G \cong G' \Rightarrow G' \cong G$ (si consideri la funzione isomorfica inversa).
3. $G \cong G' \wedge G' \cong G'' \Rightarrow G \cong G''$ (si consideri la composizione di isomorfismi).

15.4 Difficoltà della classificazione di grafi

Perchè due grafi siano isomorfi devono avere lo stesso numero di vertici e lati. Sia n il numero di vertici e l il numero di lati. Queste condizioni non sono sufficienti affinchè esista un isomorfismo. Fissato $n \geq 1$ e considerando l'insieme di tutti i grafi con n vertici, il massimo numero possibile di grafi che si possono scegliere che non sono due a due isomorfi (classi di isomorfismo distinte) sono circa $g_n \sim 2^{\frac{n^2}{2}}$.

15.5 Passeggiate, cammini e cicli

15.5.0.1 Definizione

Sia $G = (V, \varepsilon)$ un grafo e sia $(v_0, v_1, \cdots, v_k) \in V$ una successione ordinata finita di vertici di G. Si dice che:

1. $(v_0, v_1, \cdots, v_k)$ è una passeggiata in G se $\{v_i, v_{i+1}\} \in \varepsilon \forall i \in \{0, 1, \cdots, k-1\}$. Se $k = 0$ la successione (v_0).
2. $(v_0, v_1, \cdots, v_k)$ è un cammino in G se è una passeggiata e $v_i \neq v_j \forall i, j \in \{0, 1, \cdots, k\} \wedge i \neq j$, ovvero ogni vertice viene considerato una e una sola volta. (v_0) è un cammino.
3. $(v_0, v_1, \cdots, v_k)$ è un ciclo in G se $k \geq 3$, $v_0 = v_k$ e $(v_0, v_1, \cdots, v_{k-1})$ è un cammino.

15.6 Congiungibilità

15.6.0.1 Definizione

Sia $G = (V, \varepsilon)$ un grafo e siano $v, w \in V$, si dice che v e w sono congiungibili per passeggiata (o per cammino) in G se esiste una passeggiata (o un cammino) $(V_0, \cdots, v_k) \in G$ tale che $v_0 = v \wedge v_k = w$.

15.6.1 Condizione di congiungibilità

Sia $G = (V, \varepsilon)$ un grafo e siano $v, w \in V$. Allora v e w sono congiungibili per passeggiate in G se e soltato se lo sono per cammino.

15.6.1.1 Dimostrazione

Dalla congiungibilità per cammino la dimostrazione è banale in quanto un cammino è anche una passeggiata. Per dimostrare il viceversa si assuma l'esistenza di una passeggiata $P = (v_0, \cdots, v_k)$ tale che $v_0 = v$ e $v_k = w$. Si indichi con $\mathcal{P}$ l'insieme di tutte le passeggiate Q in G tali che $v_0 = v$ e $v_k = w$. Per ipotesi $p \in \mathcal{P} \neq \emptyset$. Dunque sia : $= \{l(Q) \in \mathbb{N} | Q \in \mathcal{P}\}$ con $l(Q)$ il numero di lati attraversati da Q o lunghezza della passeggiata. $\mathcal{A} \neq \emptyset$, poichè $\mathcal{A} \subset \mathbb{N}\ \exists \min \mathcal{A} = l(P_0)$, P_0 è la passeggiata con il numero minimo di lati. Sia pertanto $P_0 = (y_0, y_1, \cdots, y_h)$, se P_0 non fosse un cammino esisterebbero $i, j \in \{0, \cdots, h\} : i \neq j \wedge v_i = v_j$. Si può definire allora un'altra passeggiata $P_1 = (y_0, \cdots, y_i, y_{j+1}, \cdots, y_h)$, pertanto $l(P_q) = l(P_0) - (j-1) \leq l(P_0) < l(P_1)$, che è un assurdo, pertanto P_0 è un assurdo.

15.6.2 Congiungibilità ed equivalenza

La relazione di essere congiungibili per passeggio o per cammino è una relazione di equivalenza sui vertici.

15.6.2.1 Dimostrazione

$G = (V, \varepsilon)$ un grafo, dati $v, w \in V$, $v \sim w$ se v e w sono congiungibili in G. Siano $v, w, z \in V$.

- **Riflessività**: $v \sim v$ dal cammino (v).
- **Simmetria**: si supponga che $v \sim w$, ovvero $\exists (v_0, \cdots, v_k) \Rightarrow (v_k, \cdots, v_0)$, pertanto $w \sim v$.
- **Transitività**: $v \sim w \wedge w \sim z \Rightarrow v \sim z$, esistono pertanto due passeggiate $(v_0, \cdots, v_k) \wedge (w_0, w_h)$ tali che $v_0 = v$, $v_k = w$ e $w_0 = w$ e $w_h = z$. Si costruisca pertanto $(v_0 \cdots, v_k = w_0, \cdots, w_h)$ questo oggetto è una passeggiata in quanto i suoi elementi successivi sono adiacenti nelle passeggiate precedenti.

15.7 Componenti connesse

Dato $G = (V, \varepsilon)$ un grafo ed indicate con $V_1, \cdots, V_k$ le classi di equivalenza di V rispetto a $\sim$ i sottografi $G[V_1] \cdots G([V_k]$ di g indotti da $V_1, \cdots, V_k$ si dicono componenti connesse di G.

15.7.1 Componenti connesse e morfismi

Sia $f : G \to G'$ un morfismo di grafi. Se v e w sono congiungibili allora lo sono anche $f(v)$ e $f(w)$.

15.7.1.1 Dimostrazione

Se $(v = v_0, \cdots, v_k = w)$ è una passeggiata allora $(f(v) = f(v_0), \cdots, f(v_k) = f(w))$ è una passeggiata in g' per definizione di morfismo.

15.7.1.2 Componenti connesse e isomorfismi

Sia $f : G \to G'$ un isomorfismo di grafi. v e w sono congiungibili se e solo se lo sono anche $f(v)$ e $f(w)$. La dimostrazione segue immediatamente dalla precedente applicata a f e f^{-1}.

15.7.2 Isomorfismi di componenti connesse

Dati G e G' due grafi isomorfi questi hanno componenti connesse isomorfe, ovvero considerando $\{G_i\}_{i\in I}$ e $\{G'_j\}_{j\in J}$ gli insiemi delle componenti connesse dei due grafi allora esiste una bigezione $\phi : I \to J$ tale che $G_i \simeq G_{\phi(i)}$.

15.7.2.1 Dimostrazione

DA AGGIUNGERE vedi pag 45

15.8 Connessione

15.8.0.1 Definizione

Se G possiede una sola componente connessa allora è connesso, ovvero ogni coppia di vertici di G è congruente.

15.8.0.2 Osservazioni

Siano G eG' due grafi e sia $f : G \to G'$ un morfismo

- Un grafo è connesso solo se $\forall v, w \in V(G)$ v, w sono connessi da un cammino o da una passeggiata.
- Se f è un isomorfismo e G è connesso allora $\forall v', w' \in V' \Rightarrow \exists! f^{-1}(v')$ tale che $f(v) = v'$ e $w = f^{-1}(w')$ tale che $f(w) = w'$, poichè G è connesso la trasformazione della passeggiata è una passeggiata.

15.9 Grado di un vertice

Sia G un grafo e sia $v \in V(G)$, si definisce il grado di v in G come $deg_G(v) := |\{e \in \varepsilon(G) | v \in e\}|$, in particolare se G è finito allora $deg_G(v) \in \mathbb{N}$.

15.10 Relazione fondamentale tra grado dei vertici e numero dei lati di un grafo finito

Sia $G = (V, \varepsilon)$ un grafo finito, allora $\sum_{v \in V} deg(v) = 2|\varepsilon|$.

15.10.0.1 Dimostrazione

Siano $v_1, \cdots, v_n$ tutti i vertici di G e siano $e_1, \cdots, e_k$ i lati di G. Per ogni $i \in \{1, \cdot, n\}$ e per ogni $j \in \{1, cdots, k\}$, si definisca $m_{i,j} \in \{0, 1\} := \begin{cases} 0 & v_i \notin e_j \\ 1 & v_i \in e_j \end{cases}$. Allora per la proprietà commutativa della somma $\sum_{i=1}^{n} \sum_{j=1}^{k} m_{i,j} = \sum_{j=1}^{k} \sum_{i=1}^{n} m_{i,j}$. Per un i fissato il numero $\sum_{j=1}^{k} m_{i,j} = |\{j | v_i \in e_j\}|$, ovvero il numero di lati che contengono v_i, ovvero $\sum_{j=1}^{k} m_{i,j} = deg_G(v_i)$, pertanto il lato sinistro è uguale a $\sum_{i=1}^{n} deg_g(v_i)$, ovvero la somma dei gradi di tutti i vertici. Considerando ora la parte destra, per un j fissato si ha che $\sum_{i=1}^{n} m_{i,j} = |\{j | v_i \in e_j\}|$, che è uguale a due dato che ogni lato contiene due vertici. Si ha pertanto che la parte destra è $2k = 2|\varepsilon|$. Per concludere $\sum_{i=1}^{n} deg_G(V_i) = 2|\varepsilon|$.

15.11 Lemma delle strette di mano

In un grafo finito il numero di vertici con grado dispari è pari. Inoltre dati due grafi G e G' isomorfi di f, allora $deg_G(v) = deg_G(f(v))$.

15.12 Score di un grafo

15.12.0.1 Definizione

Sia G un grafo finito con vertici $v_1, \cdots, v_n$, si definisce lo score di G come la successione finita dei gradi dei suoi vertici, a meno di riordinamento. Equivalentemente $score(G) = (deg(v_1)_G, \cdots, deg_G(v_n))$. Lo score con i gradi crescenti è quello canonico.

15.12.0.2 Osservazioni

- Sia G un grafo finito e sia $V(G) = \{v_1, \cdots, v_n\}$, vale la relazione fondamentale; $2|\varepsilon(G)| = \sum_{i=1}^{n} deg_G(V_i)$, equivalentemente $score(G) = (d_1, \cdots, d_n)$, allora $\varepsilon(G) = \frac{1}{2}(\sum_{i=1}^{n} d_i)$.
- Siano G e G' due grafi finiti isomorfi, allora $scoreG) = score(G')$, ovvero $G \simeq G' \Rightarrow score(G) = score(G')$. Essedo la funzione un isomorfismo porta lati da $V(G)$ a lati di $V(G')$, pertanto se è isomorfismo $\forall v \in V(G), deg_G(V) = deg_{G'}(f(v)$. L'implicazione inversa è falsa.

15.12.1 Teorema dello score

Sia $d = (d_1, \cdots, d_n)$ una sequenza di numeri naturali, con $n > 1$ e sia $d_1 \leq \cdots \leq d_n$, e si denoti la sequenza $d' = (d'_1, \cdots, d'_n)$, dove $d'_i = \begin{cases} d_i & i < n - d_n \\ d_i - 1 & i \geq n - d_n \end{cases}$.
Allora d è lo score di un grafo se e solo se d' è lo score di un grafo.

15.13 Ostruzioni all'esistenza dei grafi

15.13.0.1 Grado e numero dei vertici

Se $G = (V, E)$ è un grafo $\forall v \in V, deg_G(v) \leq n - 1$

15.13.0.2 Numero di vertici con grado massimo

Se nello score di un grafo si trovano m vertici con grado massimo, lo score minimo dovrà essere m.

15.13.0.3 Lemma delle strette di mano

Il lemma delle strette di mano fornisce una condizione necessaria all'esistenza del grafo.

15.13.0.4 Vertici con grado massimo

Siano n vertici con grado massimo in uno score, allora il numero di vertici con $deg_G(v) \geq n$ devono essere la somma dei gradi massimi meno n.

15.13.0.5 Grafi con grado massimo 2

Sia $d = (d_1, \cdots, d_n) \in \mathbb{N}$ tali che $0 \leq d_1 \leq \cdots \leq d_n$ e che d soddisfi il lemma delle strette di mano, ovvero il numero di volte in cui compare 1 è pari, allora

1. Se non compare mai 1 è lo score di un grafo se $m \geq 3 \vee m = 0$, dove m è il numero di vertici con grado 2.

2. Tra i vertici del grafo ce ne sono ≥ 0 con grado 0, $2k+2 \geq 2$ con grado 1 e ≥ 0 con grado 2.

15.14 Grafi particolari

15.14.1 Grafo 2-connesso

15.14.1.1 Definizione

Sia G un grafo e sia $v \in V(G)$. Si supponga che $|V(G)| \geq 2$. Si definisca $G - v := (V(G) \backslash \{v\}, \{e \in \varepsilon(G) | v \notin e\})$. Un grafo $G = (V, \varepsilon(G))$ si dice 2-connesso se $|V| \geq 3$ e $\forall v \in V, G - v$ è connesso.

15.14.1.2 Osservazione

Un grafo 2-connesso $\Rightarrow$ grafo connesso. Sia G 2-connesso $\Rightarrow G - w$ è connesso.

15.14.1.3 Osservazione

Ogni ciclo è due connesso.

15.14.2 Vertici isolati e foglie

Sia G un grafo e $v \in V(G)$, se $deg_G(v) = 0$ v è un vertice isolato di G. Se $deg_G(v) = 1$ v si dirà foglia. Un grafo connesso non ha vertici isolati, un grafo due connesso non ha foglie. Tutte le entrate di uno score il cui valore minore maggiore di due.

15.14.3 Grafi hamiltoniani

15.14.3.1 Definizione

Un grafo con almeno tre vertici si dice hamiltoniano se esiste in ciclo del grafo che contiene tutti i vertici.

15.14.3.2 Osservazione

Un grafo hamiltoniano è sempre due connesso. Si consideri G un grafo hamiltoniano, pertanto esiste un sottografo H di G tale che $V(H) = V(G)$ e H è un ciclo. $\forall w \in V(G) = V(H)$, $G - w$ è connesso, essendo $H - w$ un cammino. L'implicazione inversa non è vera.

Capitolo 16

Gli alberi

16.0.0.1 Definizione

Si dice albero un grafo che sia connesso e senza cicli. Si dice foresta un grafo senza cicli.

16.0.1 Condizione necessaria per una foresta

Un grafo è una foresta se e soltanto se le sue componenti connesse sono alberi.

16.0.1.1 Dimostrazione

Si supponga di avere una foresta F e si consideri una delle sue componenti connesse F'. Se F' non fosse un albero dovrebbe contenere un ciclo, pertanto F non sarebbe una foresta in quanto un ciclo C , $C < F' < F \Rightarrow C < F$.

16.1 Teorema

Sia $T = (V, \varepsilon)$ un grafo anche infinito, allora le seguenti affermazioni sono equivalenti:

1. T è un albero.
2. $\forall v, v' \in V, \exists!$ cammino in T da v a v'.
3. T è connesso e $\forall e \in \varepsilon$, il grafo $T - e = G(V, \varepsilon \backslash \{w\}$ è sconnesso.
4. T non ha cicli e $\forall e \in \binom{V}{2} \backslash \varepsilon$, $T + e = (V, \varepsilon \cup \{e\})$ ha cicli.