Matematica Discreta 2
(diario del corso)

Domenico Luminati

a.a. 2003/04

Questo è il diario in tempo reale degli argomenti svolti a lezione. Alla fine del corso servirà come programma d'esame.

- **Lezione del 16 febbraio 2004 - ore 10.30-12.30**
  - il paradosso di Russel
  - assiomi di estensionalità, separazione, coppia, parti.
  - definizione di contenuto e intersezione e loro proprietà.
  - definizione di relazione, funzione parziale e funzione
  - composizione di relazioni e di funzioni
  - la composizione di funzioni è una funzione
  - iniettività, suriettività, equipotenza
  - proprietà riflessiva, simmetrica e transitiva dell'equipotenza di insiemi
  - cenno sulla possibilità di definire i cardinali e sulle loro proprietà.
- **Lezione del 18 febbraio 2004 - ore 9.30-10.30**
  - gli assiomi di Peano dei numeri naturali
  - esistenza del predecessore
  - il principio di induzione (prima forma)
  - enunciato del teorema di ricorsione
  - alcuni esempi di definizione ricorsiva: l'esponenziale, il fattoriale
- **Lezione del 19 febbraio 2004 - ore 10.30-12.30**
  - la dimostrazione del teorema di ricorsione
  - definizione ricorsiva delle operazioni
  - definizione dell'ordinamento dei numeri naturali
  - definizione di ordinamento e ordinamento totale di un insieme. L'esempio della relazione $\subseteq$
  - definizione di insieme finito
  - il lemma dei cassetti
- **Lezione del 23 febbraio 2004 - ore 10.30-11.30**
  - definizione di cardinalità di un insieme finito
  - insiemi finiti sono equipootenti se e solo se hanno la stessa cardinalità
  - sottinsiemi finiti di un insieme finito

- un insieme finito non è equipotente a nessun sottinsieme proprio
- succ : $\mathbb{N} \to \mathbb{N}\setminus\{0\}$ è una bigezione, quindi l'insieme $\mathbb{N}$ dei numeri naturali non è finito

- **Lezione del 25 febbraio 2004 - ore 8.30-10.30**
  - assioma della scelta
  - ogni insieme infinito contiene un sottinsieme equipotente a $\mathbb{N}$
  - un insieme è infinito se e solo se è equipotente ad un suo sottinsieme proprio
  - calcolo del numero di funzioni iniettive tra due insiemi finiti (disposizioni semplici)
  - calcolo del numero di sottinsiemi con k elementi di un insieme con n elementi.(combinazioni semplici)

- **Lezione del 1 marzo 2004 - ore 10.30-11.30**
  - il teorema di Cantor
  - interpretazione nel caso di $2^{\mathbb{N}}$
  - i numeri reali non sono numerabili
  - calcolo del numero di funzioni iniettive tra due insiemi finiti (disposizioni semplici)$\mathbb{N}$ è equipotente a $\mathbb{N} \times \mathbb{N}$
  - il teorema di Cantor-Schroeder-Bernstein (senza dimostrazione)
  - i numeri razionali sono equipotenti ai naturali
  - unione numerabile di insiemi numerabili è numerabile (senza dimostrazione)

- **Lezione del 3 marzo 2004 - ore 8.30-10.30**
  - definizione di insieme bene ordinato
  - $\mathbb{N}$ è bene ordinato da $\leq$.
  - seconda forma del principio di induzione
  - divisione euclidea
  - divisibilità
  - la relazione di divisibilità è un ordinamento parziale si $\mathbb{N}$

- **Lezione del 4 marzo 2004 - ore 11.30-12.30**
  - reappresentazione in base fissata dei numeri naturali
  - definizione di MCD
  - unicità del MCD

- **Lezione del 8 marzo 2004 - ore 10.30-11.30**
  - esistenza del MCD
  - algoritmo di Euclide per il calcolo del MCD
  - proprietà dei numeri coprimi
  - definizione di numero primo
  - caratterizzazione dei numeri primi

- enunciato del teorema fondamentale dell'aritmetica
- esistenza di infiniti numeri primi

- **Lezione del 10 marzo 2004 - ore 8.30-10.30**
  - dimostrazione del teorema fondamentale dell'aritmetica
  - definizione del mcm
  - esistenza e unicità del mcm
  - definizione di congruenza
  - relazioni d'equivalenza
  - la congruenza è una relazione d'equivalenza
  - classi d'equivalenza e insieme quoziente

- **Lezione del 15 marzo 2004 - ore 10.30-11.30**
  - le classi di congruenza $\mod n$ sono esattamente n
  - somma e prodotto di classi di congruenza
  - proprietà delle operazioni tra classi di congruenza
  - teorema cinese del resto

- **Lezione del 17 marzo 2004 - ore 8.30-10.30**
  - equazioni lineari di congruenze
  - elementi invertibili $\mod n$
  - caratterizzazione degli invertibili $\mod n$
  - unicità dell'inverso
  - piccolo teorema di Fermat

- **Lezione del 18 marzo 2004 - ore 10.30-13.30**
  - applicazione del piccolo teorema di Fermat alla crittografia RSA
  - calcolo di $\Phi(pq)$ e di $\Phi(p^n)$ con p, q primi
  - definizione di grafo
  - relazione associata ad un grafo (equivalenza delle due definizioni di grafo)
  - definizione di grafo diretto
  - matrice di adiacenza di un grafo item definizione di grado di un vertice
  - la somma dei gradi è pari al doppio del numero dei vertici
  - definizione di isomorfismo di grafi
  - il grado è invariante per isomorfismo.
  - esempi di grafi notevoli, P_n, C_n, K_n.

- **Lezione del 20 marzo 2004 - ore 9.30-12.30**
  - Una stima del numero di grafi non isomorfi
  - sottografi e sottografi indotti
  - passeggiate, cammini e cicli.
  - la relazione di congiungibilità

- definizione di componenti connesse di un grafo e grafi connessi
- invarianza per isomorfismo delle componenti connesse di un grafo
- equivalenza di congiungibilità con passeggiate e congiungibilità con cammini
- matrice di adiacenza e significato di A_G^k.

- **Lezione del 22 marzo 2004 - ore 10.30-13.30** – tenuta da M. Pagliacci
  - definizione di albero e foresta
  - teorema di caratterizzazione degli alberi
  - teorema di caratterizzazione per gli alberi finiti (formula di Eulero)

- **Lezione del 27 marzo 2004 - ore 9.30-12.30**
  - definizione di score e invarianza per isomorfismo
  - teorema dello score
  - definizione di passeggiata euleriana
  - caratterizzazione dei grafi euleriani
  - definizione di grafo hamiltoniano
  - definizione di 2-connessione
  - ogni grafo hamiltoniano è 2-connesso

- **Lezione del 29 marzo 2004 - ore 10.30-11.30**
  - prima caratterizzazione dei grafi 2-connessi (congiungibilità con cicli)

- **Lezione del 31 marzo 2004 - ore 8.30-10.30**
  - definizione di aggiunzione ($G + e$) e suddivisione ($G\%e$) di lati
  - se un grafo è 2-connesso allora anche $G + e$ e $G\%e$ lo sono.
  - seconda caratterizzazione dei grafi 2-connessi (ottenuti da K_3 per suddivisione e aggiunzione di lati)
  - esercizi

- **Lezione del 1 aprile 2004 - ore 10.30-12.30**
  - definizione di albero di copertura
  - Esistenza dell'albero di copertura
  - esercizi