Corso LMM- C. Anno 2005-2006

Argomenti trattati a lezione.

- Prima lezione (28-9-2005).
  Cosa sono le proposizioni e i predicati. Negazione di una proposizione. I connettivi "o" ed "e". Tabelle di verità. Implicazioni. Metodi di dimostrazione: dimostrazione diretta e per assurdo (compreso l'uso della contronominale). Fra gli esempi, abbiamo dimostrato che $\sqrt{2}$ è un numero irrazionale e che i numeri primi sono infiniti.

- Seconda lezione (30-09-2005).
  Definizione di insieme come collezione (non ordinata) di oggetti. Notazioni e prime proprietà degli insiemi. Il paradosso di Russel e l'introduzione dell'insieme universo. Operazioni sugli insiemi: intersezione, unione, differenza, complementare. Uso delle tabelle di verità per dimostrare uguaglianze fra insiemi. Regole associativa, commutativa, distributiva e di De Morgan per intersezione, unione e complementare. Analogia di tali regole con le regole per "and", "or" e "not" fra proposizioni.
  Definizione di prodotto cartesiano fra due insiemi.

- Terza lezione (7-10-2005).
  I quantificatori "esiste" e "per ogni" e la loro interpretazione tramite l'insieme di verità di un predicato. Dimostrazioni di esistenza costruttive e non costruttive. Negazione di proposizioni miste che comprendono "per ogni" ed "esiste". Esempio di interpretazione insiemistica (con il prodotto catesiano) di una proposizione mista che comprende un "per ogni" ed un "esiste".
  Il principio di induzione. Esempi di dimostrazioni per induzione: formula per la somma dei primi n numeri naturali e disuguaglianza di Bernoulli.

- Quarta lezione (21-10-2004).
  Il principio di induzione: enunciati equivalenti (induzione "forte" e buon ordinamento). Esempi di applicazione dell'induzione forte.
  Funzioni: definizione, grafico di una funzione, insieme immagine. Funzioni iniettive, surgettive, bigettive. Composizione di funzioni. Teorema: una funzione è invertibile se e solo se è bigettiva, e in tal caso la sua inversa è unica (traccia della dimostrazione in classe, la dimostrazione completa la trovate scritta negli appunti integrativi). Applicazione del teorema: come si può definire la cardinalità di un insieme ? Tentativo di definizione di "insieme con n elementi" con n numero naturale.

- Quinta lezione (26-10-2005).
  Dimostrazione (facoltativa) del fatto che se esiste una funzione iniettiva dall'insieme dei primi n numeri naturali positivi all'insieme dei primi m numeri naturali positivi allora $n \leq m$. Si dimostra in realtà la contronominale, che è nota come Lemma dei Cassetti. Questo permette di concludere che la definizione di cardinalità di un insieme data

nella quarta lezione è buona. Esempi di applicazione del lemma dei cassetti. Problemi importanti: contare le funzioni da un insieme finito X ad un insieme finito Y, contare le funzioni iniettive da un insieme finito X ad un insieme finito Y (in particolare, contare le funzioni bigettive fra due insiemi finiti con la stessa cardinalità). L'insieme delle parti $\mathcal{P}(A)$ di un insieme A; nel caso in cui A sia finito, abbiamo dimostrato che $|\mathcal{P}(A)| = 2^{|A|}$.

- Sesta lezione (11-11-2005).
  Le prime tecniche per contare: il principio di addizione (la cardinalità di una unione di insiemi finiti a due a due disgiunti), il principio di moltiplicazione (la cardinalità di un prodotto cartesiano di insiemi finiti). Introduciamo i coefficienti binomiali $\begin{pmatrix} n \\ r \end{pmatrix}$ come "il numero dei sottoinsiemi di cardinalità r in un insieme di cardinalità n". Prime proprietà dei coefficienti binomiali. Come costruirli ricorsivamente: la relazione fondamentale $\begin{pmatrix} n \\ r \end{pmatrix} = \begin{pmatrix} n-1 \\ r-1 \end{pmatrix} + \begin{pmatrix} n-1 \\ r \end{pmatrix}$ (con dimostrazione !) e il triangolo di Tartaglia-Pascal. Come esprimere i coefficienti binomiali con i fattoriali (con dimostrazione !). Il teorema del binomio di Newton (con dimostrazione !). Esempi e applicazioni.

- Settima lezione (18-11-2005).
  Gli insiemi infiniti: come si può definire la loro cardinalità ? Definizione di equipotenza fra insiemi. Gli insiemi infiniti numerabili. Prime proprietà: l'unione di due insiemi infiniti numerabili è un insieme infinito numerabile, il prodotto cartesiano di due insiemi infiniti numerabili è un insieme infinito numerabile, un sottoinsieme infinito di un insieme numerabile è numerabile. Teorema (Cantor): l'insieme $\mathbb{Q}$ è numerabile. Teorema (Cantor): l'insieme $\mathbb{R}$ non è numerabile. Teorema: per ogni insieme X, vale che l'insieme delle parti di X ha cardinalità strettamente maggiore di X (dimostrazione facoltativa, vedere appunti integrativi). Teorema: $|\mathcal{P}(\mathbb{N})| = |\mathbb{R}|$ (dimostrazione facoltativa, vedere appunti integrativi). Cenni sull'ipotesi del continuo.

- Ottava lezione (30-11-2005).
  La divisione euclidea: dimostrazione del teorema di esistenza e unicità e prime applicazioni ed esempi. Il massimo comun divisore, definizione e prime proprietà. L'algoritmo di Euclide: perché funziona e come si usa per trovare $MCD\ (a, b)$.

- Nona lezione (2-12-2005).
  L'identità di Bezout: $MCD\ (a, b)$ si esprime come combinazione lineare a coefficienti interi di a e b. Metodo costruttivo (con l'algoritmo di Euclide) per trovare una tale combinazione lineare (un'altra dimostrazione, "esistenziale", dell'identità di Bezout si trova negli appunti integrativi e fa parte del programma del corso). Esempi. Il caso di due numeri a e b coprimi. Teorema: se $a \mid bc$ e a e b sono coprimi allora $a \mid c$. Equazioni diofantee lineari: abbiamo discusso come decidere se esiste una soluzione e come trovare tutte le infinite soluzioni di una equazione risolubile. Esempi.

- Decima lezione (9-12-2005).
  L'idea di congruenza modulo un intero positivo m. Definizione di quando "a è congruo a b modulo m". Prime proprietà. Regole per lavorare con le congruenze: somma, sottrazione, moltiplicazione di congruenze. Esempi, fra cui il criterio di divisibilità per 3. Regola per la divisione: $am \equiv an\ (t)$ è equivalente a $m \equiv n\ (\frac{t}{MCD(a,t)})$ (dimostrazione completa negli appunti integrativi).
  Teorema sulla risoluzione delle congruenze lineari (dimostrazione completa negli appunti integrativi). Esempi di risoluzione di congruenze lineari.

- Undicesima lezione (16-12-2005).
  Classi di congruenza modulo un intero positivo m. L'insieme $\mathbb{Z}_m$. Operazioni in $\mathbb{Z}_m$: addizione, moltiplicazione. Elementi invertibili in $\mathbb{Z}_m$: definizione e caratterizzazione. Se p è primo allora tutti gli elementi diversi da zero in $\mathbb{Z}_p$ sono invertibili.
  Il piccolo teorema di Fermat, con dimostrazione (facoltativa, raccomandata! Vedere le note integrative). Applicazioni ed esempi. Cenni sui numeri "falsi primi" di Carmichael.

  Parte finale facoltativa: sistemi di equazioni di congruenze. Esistenza delle soluzioni e algoritmo per trovarle. Il teorema cinese del resto. Esempi: dimostrazione che 561 è un "falso primo" e formula per la funzione ϕ di Eulero.

- Fanno parte del programma anche le seguenti osservazioni discusse a esercitazioni: le prime forme (con due e con tre insiemi) del principio di inclusione-esclusione. Applicazione: contare le funzioni surgettive da un insieme finito X ad un insieme finito Y di cardinalità 3. Il principio di inclusione-esclusione in generale (dimostrazione facoltativa, vedere le note integrative). Teorema di decomposizione unica di un numero intero > 1 in prodotto di primi. Come si trova, data la decomposizione in fattori primi di due numeri a e b, il $MCD(a, b)$.