Corso di Laurea Triennale in **Informatica** - a.a. 2015/16

programma sintetico del corso di

MATEMATICA DISCRETA

(9 CFU)

prof. **Fabio Gavarini**

----- ------- ---------- ------- -----

INSIEMI, CORRISPONDENZE, RELAZIONI, OPERAZIONI

Insiemi; sottoinsiemi, sovrainsiemi, inclusione. L'insieme delle parti. Famiglie. Operazioni tra insiemi. Partizioni.

Corrispondenze tra insiemi. Immagine o controimmagine di sottoinsiemi; corrispondenza inversa; composizione.

Funzioni. Caratterizzazione delle famiglie come funzioni. Restrizione di una funzione. Funzioni iniettive, suriettive o biiettive; biiettività e corrispondenza inversa. Composizione di funzioni; funzioni invertibili. Funzioni caratteristiche in un insieme. La biiezione naturale tra l'insieme delle parti di un insieme A e l'insieme delle funzioni caratteristiche in A.

Relazioni in un insieme. Proprietà notevoli per una relazione. Relazioni di preordine; relazioni d'ordine. Relazioni di equivalenza. La congruenza modulo n tra interi. L'equivalenza associata a una funzione. Classi di equivalenza, rappresentanti; insieme quoziente. Biiezione tra equivalenze in X e partizioni di X. Decomposizione canonica di una funzione.

Operazioni; gruppoidi, semigruppi, monoidi, gruppi. Il monoide libero A^* su un insieme A. Permutazioni di un insieme; le permutazioni formano un gruppo per la composizione. Insiemi con due operazioni; semianelli, anelli, campi. L'insieme delle parti (di un insieme) è un anello commutativo unitario per differenza simmetrica e intersezione.

Bibliografia: [Ca] Capitolo I, paragrafi 1, 2, 3 e 4 - [G-P] files *Insiemi* , *Funzioni e cardinalità* , *Relazioni 1* , *Gruppi, anelli, campi* - [L-L] Chapters 1, 2 e 3; Appendix B - [PC] Capitolo 1, paragrafi 1, 2 e 3; Capitolo 4, paragrafo 1; Capitolo 5, paragrafi 1 e 2

Videolezioni: *Insiemi* , *Corrispondenze* , *Funzioni 1* , *Funzioni 2* , *Funzioni caratteristiche* , *Relazioni* , *Equivalenze 1* , *Equivalenze 2* , *Operazioni 1* , *Operazioni 2*

NUMERI NATURALI, CALCOLO COMBINATORIO

Il Sistema dei Numeri Naturali (=S.N.N.). Il Principio di Induzione Debole (=Pr.I.D.). Ordinamento, somma e prodotto tra naturali; i numeri formano un semianello in cui l'ordine è compatibile con le operazioni. Principio di Induzione Forte (=Pr.I.F.), Principio del Minimo (=Pr.M.): equivalenza tra Pr.I.D., Pr.I.F. e Pr. M. (cenni). Dimostrazioni per induzione.

Divisione con resto tra naturali. Numerazione in base arbitraria: scrittura posizionale (di un naturale) in base arbitraria.

Calcolo del numero di: *(1)* funzioni da un insieme finito ad un altro ("disposizioni con ripetizione"); *(2)* funzioni *iniettive* da un insieme finito ad un altro ("disposizioni senza ripetizione"); *(3)* permutazioni di un insieme finito in sé stesso: il *fattoriale* di *n; (4)* sottoinsiemi con k elementi in un insieme con n elementi ("combinazioni di k elementi scelti tra n"): *coefficienti binomiali*; *(5)* partizioni di un insieme con n elementi in sottoinsiemi con numero di elementi assegnato: *coefficienti multinomiali*. La formula di Newton per lo sviluppo delle potenze di un binomio e per lo sviluppo delle potenze di un multinomio. Il triangolo di Pascal-Tartaglia.

Bibliografia: [AaVv] file Numeri naturali *(D'Andrea)* - [Ca] Capitolo I, paragrafi 1 e 5 ; Capitolo II, paragrafo 2 - [G-P] files Induzione , Aritmetica sugli interi, etc. (complementi), paragrafo 1 - [L-L] Chapter 1, section 8; Chapter 5, sections 1 to 5; Chapter 6, sections 1 to 3; Chapter 11, sections 3 - [PC] Capitolo 1, paragrafi 4 e 6; Capitolo 2, paragrafo 10

Videolezioni: *Naturali* , *Induzione* , *Divisione* , *Numerazione*

CARDINALITÀ, NUMERI CARDINALI

Equipotenza tra insiemi: riflessività, simmetria, transitività. Cardinalità di un insieme, numeri cardinali. Insiemi finiti, o infiniti numerabili, o infiniti non numerabili. Ordinamento tra numeri cardinali; Teorema di Schroeder-Bernstein *(senza dimostrazione)*.

Caratterizzazione degli insiemi infiniti (per un insieme X): *(1)* X è infinito, *(2)* esiste una funzione iniettiva dall'insieme dei numeri naturali ad X, *(3)* esiste un sottoinsieme proprio di X che è equipotente ad X stesso.

1° Teorema di Cantor: L'unione di una famiglia finita (non vuota) o numerabile di insiemi numerabili è numerabile.

Esempi di applicazione del 1° Teorema di Cantor.

2° Teorema di Cantor: La cardinalità dell'insieme delle parti di X è strettamente maggiore della cardinalità di X.

I cardinali infiniti superiori $\aleph_n$. La cardinalità del continuo: $|\mathbf{R}| = |\mathscr{P}(\mathbf{N})|$; l'ipotesi del continuo generalizzata (cenni).

Bibliografia: [AaVv] file Cardinalità *(D'Andrea)* - [Ca] Capitolo I, paragrafo 6 - [G-P] file Funzioni e cardinalità, paragrafo 5 - [L-L] Chapter 3, section 7 - [PC] Capitolo 1, paragrafo 5

Videolezioni: *Cardinalità 1* , *Cardinalità 2*

NUMERI INTERI, CONGRUENZE, ARITMETICA MODULARE

Richiami sui numeri interi: operazioni, ordine, valore assoluto. Costruzione degli interi a partire dai naturali, come "naturali + i negativi". Fattorizzazione in un monoide. Divisibilità; elementi invertibili, elementi associati. Elementi riducibili, elementi irriducibili, elementi primi; ogni primo è irriducibile. Fattorizzazioni banali, fattorizzazioni equivalenti.

Massimo comun divisore (=*MCD*) e minimo comun multiplo (=*mcm*). Elementi coprimi (=primi tra loro).

Divisione con resto tra interi: esistenza e unicità di quoziente e resto (positivo). Esistenza del *MCD* in **Z**, e identità di Bézout per esso: calcolo con l'algoritmo euclideo delle divisioni successive. Tra i numeri interi, ogni irriducibile è primo.

Teorema Fondamentale dell'Aritmetica: esistenza e unicità di una fattorizzazione in irriducibili per interi non nulli e non invertibili. *Teorema di Euclide:* Esistono infiniti interi irriducibili (a due a due non associati).

Forma esplicita di $MCD(a,b)$ e di $mcm(a,b)$; la relazione $MCD(a,b)\ mcm(a,b) = a\ b$.

Equazioni diofantee: definizione, criterio di esistenza di soluzioni, algoritmo per il calcolo di una soluzione.

Congruenze in **Z** (modulo n). Ogni congruenza è una equivalenza; descrizione delle classi di congruenza e dell'insieme quoziente $\mathbf{Z}_n$. Somma e prodotto in $\mathbf{Z}_n$. *Teorema*: $\mathbf{Z}_n$ è un anello commutativo unitario *(senza dimostrazione)*. Criteri di divisibilità in **Z**. *Proposizione*: $\mathbf{Z}_n$ è un dominio $\Leftrightarrow$ n è irriducibile (=primo) $\Leftrightarrow$ $\mathbf{Z}_n$ è un campo.

Equazioni congruenziali in **Z**: risolubilità, algoritmo risolutivo. Elementi invertibili in $\mathbf{Z}_n$; criterio di invertibilità, calcolo dell'inverso. Il gruppo moltiplicativo $U(\mathbf{Z}_n)$ degli elementi invertibili di $\mathbf{Z}_n$; la funzione di Eulero. Ripetitività delle potenze in $\mathbf{Z}_n$. Il *Piccolo Teorema di Fermat*, il *Teorema di Eulero (senza dimostrazione)*; calcolo di potenze in $\mathbf{Z}_n$.

Il *metodo crittografico RSA*. Sistemi di equazioni congruenziali; il *Teorema Cinese del Resto (senza dimostrazione)*.

Bibliografia: [AaVv] files Numeri interi *(D'Andrea)*, paragrafo 4 , Congruenze, aritmetica modulare*(D'Andrea)*, paragrafi 1 e 2 - [Ca] Capitolo II, paragrafi da 1 a 6 - [G-P] files Aritmetica sugli interi, congruenze, Teorema Cinese del Resto , Aritmetica sugli interi, etc. (complementi) - [L-L] Chapter 11, sections 1 to 9 - [PC] Capitolo 2, paragrafi da 1, 2, 3, 6, 7, 8 e 9

RETICOLI, ALGEBRE DI BOOLE, FUNZIONI BOOLEANE

Relazioni d'ordine. Diagramma di Hasse. Sottoinsiemi ordinati, ordine prodotto. *Principio di Dualità* per insiemi ordinati. Elementi minimali (o massimali), minimo (o massimo), estremo inferiore (o estremo superiore) per un sottoinsieme in un insieme ordinato *E*.

Reticoli. *Principio di Dualità* per reticoli. Limiti, complementi, distributività; elementi $\vee$-riducibili o $\vee$-irriducibili; atomi. *Teorema di $\vee$-Fattorizzazione Unica (in $\vee$-irriducibili)* per reticoli finiti distributivi. *Teorema di $\vee$-Fattorizzazione Unica (in atomi)* per reticoli finiti distributivi complementati (=algebre di Boole). Isomorfismi tra reticoli, reticoli isomorfi; sottoreticoli. *Teorema:* Un reticolo è distributivo $\Leftrightarrow$ non ha sottoreticoli isomorfi a $\boldsymbol{N}_5$ o a $\boldsymbol{M}_5$ *(senza dimostrazione)*.

Algebre di Boole. *Principio di Dualità* per algebre di Boole. Anelli booleani. *Teorema di Equivalenza:* "Algebra di Boole" e "anello booleano unitario" sono nozioni equivalenti *(soltanto la definizione delle corrispondenze)*. Isomorfismi tra algebre di Boole, algebre di Boole isomorfe. *Teorema (Stone - finito):* Ogni algebra di Boole finita è isomorfa all'insieme delle parti dell'insieme dei suoi atomi. Sottoalgebre di Boole. *Teorema (Stone - generale):* Ogni algebra di Boole è isomorfa ad una sottoalgebra di Boole dell'insieme delle parti di un opportuno insieme *(senza dimostrazione)*.

Funzioni booleane, polinomi booleani. Equivalenza tra polinomi booleani. Prodotti, prodotti fondamentali; somme di prodotti. Forma normale disgiuntiva di un polinomio; calcolo tramite *(1)* "tavole di verità", o *(2)* manipolazioni successive. Forme minimali di un polinomio booleano. Gli implicanti primi di un polinomio booleano. Somme di prodotti irridondanti. Il *Metodo del Consenso* per calcolare la somma degli implicanti primi di *f*, e una sua forma minimale.

Bibliografia: [Ca] Capitolo I, paragrafo 3(B) - [G-P] files Relazioni - 2 , Reticoli , Algebre di Boole , Funzioni booleane , Forme minimali di una funzione polinomiale - [L-L] Chapter 14, sections 1 to 5 and 7 to 11; Chapter 15, sections 1 to 9

Videolezioni: *Insiemi ordinati* , *Reticoli 1* , *Reticoli 2* , *Reticoli 3* , *Algebre di Boole 1* , *Algebre di Boole 2*

FUNZIONI RICORSIVE, EQUAZIONI ALLE DIFFERENZE

Funzioni (o "successioni") ricorsive; equazione ricorsiva, grado e dati iniziali. Casi particolari: lineari, lineari omogenee, lineari a coefficienti costanti, lineari omogenee a coefficienti costanti (=l.o.c.c).

Teorema di Ricorsione: Esiste un'unica funzione che soddisfa una data equazione ricorsiva e ha dati iniziali assegnati.

Proposizione: L'insieme *S* delle successioni soluzioni di un'equazione ricorsiva lineare omogenea di ordine *k* è chiuso per la somma e per il prodotto con uno scalare; inoltre, esistono *k* successioni $\underline{a}_1, \ldots, \underline{a}_k$ in *S* tali che ogni successione in *S* si possa scrivere in modo unico come combinazione lineare delle successioni $\underline{a}_1, \ldots, \underline{a}_k$ *(cenni di dimostrazione)*.

Strategia di calcolo di una funzione ricorsiva lineare omogenea. Metodo di calcolo esplicito per funzioni ricorsive l.o.c.c. nei casi: *(1)* di grado 1; *(2)* di grado 2, con due radici distinte; *(3)* di grado 2, con una sola radice (doppia).

Bibliografia: [G-P] file Equazioni alle differenze finite (cenni) - [L-L] Chapter 3, section 6; Chapter 6, sections 6, 7 and 8

Videolezioni: *Funzioni ricorsive 1* , *Funzioni ricorsive 2* , *Funzioni ricorsive 3.1*

(MULTI)GRAFI, (MULTI)DIGRAFI

Multidigrafi, multigrafi; la matrice di adiacenza. Sottomultigrafi e sottomultidigrafi. Unione di multidigrafi, o di multigrafi. Grado entrante, grado uscente, grado (totale) di un vertice in un multidigrafo; grado di un vertice in un multigrafo. Grafi regolari, grafi completi. Multidigrafi bipartiti, multigrafi bipartiti, digrafi bipartiti, digrafi funzionali.

Teorema ("Lemma delle Strette di Mano"): (1) In ogni multigrafo finito, la somma dei gradi di tutti i vertici è uguale al doppio del numero degli spigoli del multigrafo. *(2)* In ogni multidigrafo finito, la somma dei gradi entranti di tutti i vertici e la somma dei gradi uscenti di tutti i vertici sono entrambe uguali al numero degli archi del multidigrafo.

Cammini, circuiti, connessione in multigrafi e in multidigrafi. Componenti connesse, ponti in un multigrafo.

Proposizione: Ogni multigrafo finito è l'unione delle sue componenti connesse.

Cammini euleriani in un multi(di)grafo; multi(di)grafi euleriani o semieuleriani. *Teorema* di caratterizzazione dei multigrafi e multidigrafi euleriani o semieuleriani. L'*Algoritmo di Fleury* per il calcolo di un cammino euleriano.

Alberi (non orientati), foreste: definizione ed esempi. Foglie in un multigrafo.

Teorema (caratterizzazione degli alberi): Per un grafo G le seguenti quattro proprietà sono equivalenti:

(a) G è un albero; *(b)* G è aciclico, ma se si aggiunge un qualsiasi nuovo spigolo si ottiene un grafo ciclico;

(c) per ogni scelta di vertici u e v in G esiste uno ed un solo percorso da u a v in G; *(d)* G è connesso, ma se si toglie un qualsiasi spigolo si ottiene un sottografo sconnesso (in altre parole, ogni spigolo in G è un ponte).

Teorema (caratterizzazione degli alberi finiti): Per ogni multigrafo $G:=(V,E)$ con numero finito $|V|=n$ di vertici, le seguenti proprietà sono equivalenti: *(a)* G è un albero; *(b)* G è aciclico e $|E|=n-1$ $(=|V|-1)$; *(c)* G è connesso e $|E|=n-1$ $(=|V|-1)$.

Proposizione: Ogni albero finito con almeno due vertici ha almeno due foglie.

Albero generatore o *foresta generatrice* di un multigrafo: definizione, esistenza, algoritmi per calcolare un albero generatore in un multigrafo connesso.

Bibliografia: [L-L] Chapter 8, sections 1, 2, 3, 4, 5, 7, 8 and 11; Chapter 9, sections 1, 2, 3 and 5 - [Qua] Breve Introduzione alla Teoria dei Grafi, Capitoli 1, 2, 4 e 6

• • • ☼ ☼ ☼ • • •

TESTI (libri, dispense, videolezioni, ecc.) consigliati:

[AaVv] - Autori Varî, *Materiale vario disponibile in rete* (per gentile concessione degli autori) - - alla pagina http://www.mat.uniroma2.it/~gavarini/page-web_files/mat-didat.html#Mat-Dis_altro-mat

[Ca] - G. Campanella, *Appunti di Algebra 1* (per gentile concessione dell'autore) - alla pagina http://www.mat.uniroma2.it/~gavarini/page-web_files/mat-didat_data/dispense-ecc/Algebra_1_-_dispense_di_Campanella.rar

[Ga] - F. Gavarini, *Videolezioni varie* - alla pagina http://didattica.uniroma2.it/files/index/insegnamento/144372

[G-P] - L. Geatti, G. Pareschi, *Appunti varî* (per gentile concessione degli autori) - - alla pagina http://www.mat.uniroma2.it/~gavarini/page-web_files/mat-didat_data/Algebra-Logica_(ING-INF)/Pagina_Web_Algebra-Logica_2012-13/AL_2012-13.html#app_alg-log

[L-L] - S. Lipschutz, M. Lipson, *Discrete Mathematics*, 3rd Edition, Schaum's Outlines, McGraw-Hill, 2007

[PC] - G. M. Piacentini Cattaneo, *Algebra - un approccio algoritmico*, ed. Decibel/Zanichelli, Padova, 1996

[Qua] - G. Quattrocchi, *Breve Introduzione alla Teoria dei Grafi* (per gentile concessione dell'autore) - - alla pagina http://www.mat.uniroma2.it/~gavarini/page-web_files/mat-didat_data/dispense-ecc/Quattrocchi_G._-_Breve_Introduzione_alla_Teoria_dei_Grafi.pdf