Corso di Laurea Triennale in **Ingegneria Informatica** - a.a. 2016/17

programma sintetico del corso di

ALGEBRA e LOGICA

(6 CFU)

prof. **Fabio Gavarini**

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

INSIEMI, CORRISPONDENZE, RELAZIONI, OPERAZIONI

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

Corrispondenze tra insiemi; immagine o controimmagine di sottoinsiemi; corrispondenza inversa. Composizione.

Funzioni. Restrizione di una funzione. Famiglie, comparazione con gli insiemi. Funzioni iniettive, suriettive o biiettive; biiettività e corrispondenza inversa. Composizione di funzioni; funzioni invertibili. Funzioni caratteristiche in un insieme. 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: riflessiva, simmetrica, antisimmetrica, transitiva. Relazioni di preordine, relazioni dí ordine, relazioni di equivalenza. L'equivalenza associata a una funzione. La congruenza modulo *n* tra numeri interi è una equivalenza. Classi di equivalenza, rappresentanti; insieme quoziente, proiezione canonica. Partizioni di un insieme. Biiezione naturale tra equivalenze in *X* e partizioni di *X*.

Operazioni; proprietà speciali, elementi neutri, inversi. Monoidi, gruppi; il gruppo degli invertibili in un monoide.

Insiemi con due operazioni; anelli, campi. L'insieme delle parti di un insieme è anello commutativo unitario (non campo) per le operazioni di 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, par. 1 e 2

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

NUMERI NATURALI

Il Sistema dei Numeri Naturali (=S.N.N.). Il Principio di Induzione Debole (=Pr.I.D.). Ordinamento, somma e prodotto tra naturali; proprietà notevoli. Il Principio di Induzione Forte (=Pr.I.F.), il 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; conversione da una base a un'altra.

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 11, section 3 - [PC] Capitolo 1, paragrafo 4; 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 numerabili o infiniti non numerabili. Ordinamento tra cardinali; Teorema di Schroeder-Bernstein *(senza dimostrazione)*.

La cardinalità del numerabile è il minimo tra i cardinali infiniti. 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^o Teorema di Cantor: L'unione di una famiglia finita (non vuota) o numerabile di insiemi numerabili è numerabile.

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

I numeri cardinali infiniti $\aleph_n$. L'ipotesi del continuo generalizzata (cenni). La cardinalità del continuo: $|\mathbf{R}| = |\mathscr{P}(\mathbf{N})|$ *(senza dimostrazione)*.

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

Numeri interi, relazione coi naturali. Divisibilità, divisori, multipli; elementi invertibili, elementi associati. Elementi riducibili, elementi irriducibili. Il problema generale della fattorizzazione in un monoide. Fattorizzazioni banali, fattorizzazioni equivalenti. Massimo comun divisore (=*MCD*) e minimo comun multiplo (=*mcm*). Elementi coprimi.

Divisione con resto tra interi: esistenza e unicità di quoziente e resto (positivo). Esistenza di *MCD* in **Z**, e identità di Bézout: algoritmo euclideo. Elementi primi; ogni primo è irriducibile. 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: criterio di esistenza di soluzioni, algoritmo per il calcolo di una soluzione.

Congruenze in **Z** (modulo n). Ogni congruenza è una relazione di 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 *(cenni)*. 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 della classe inversa; la funzione di Eulero. Calcolo di potenze in $\mathbf{Z}_n$: generalità, il *Teorema di Fermat (senza dimostrazione)*, il *Teorema di Eulero (senza dimostrazione)*. Applicazione: *il metodo crittografico R.S.A.*

Sistemi di equazioni congruenziali: discussione, risoluzione tramite il *Teorema Cinese del Resto* o per sostituzioni.

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 di un (sotto)insieme ordinato. Minoranti, maggioranti, estremo inferiore e estremo superiore per un sottoinsieme ordinato. Insiemi (semi)limitati.

Reticoli. *Principio di Dualità* per reticoli. Limiti, complementi, distributività in un reticolo. Elementi ∨-riducibili o ∨-irriducibili; atomi. *Teorema di ∨-Fattorizzazione (in ∨-irriducibili)* per reticoli finiti; *unicità della ∨-fattorizzazione* nel caso distributivo. *Teorema di ∨-Fattorizzazione Unica (in atomi)* per reticoli finiti distributivi complementati (=alg. di Boole finite). Isomorfismi tra reticoli, reticoli isomorfi; sottoreticoli. *Criterio di distributività (senza dimostrazione)*.

Algebre di Boole. Il *Principio di Dualità* per algebre di Boole. Isomorfismi tra algebre di Boole, algebre di Boole isomorfe. *Teorema (Stone - caso finito):* Ogni algebra di Boole finita è isomorfa all'insieme delle parti dell'insieme dei suoi atomi. In particolare, la cardinalità di un'algebra di Boole finita è sempre una potenza di 2.

Funzioni booleane, polinomi booleani (in n variabili). Equivalenza tra polinomi. Prodotti, prodotti fondamentali, prodotti completi. Somme di prodotti; ridondanza e non-ridondanza. *Forma Normale Disgiuntiva* di un polinomio booleano: esistenza e unicità, calcolo tramite *(1)* tramite "tavole di verità", oppure *(2)* manipolazioni successive. *Corollario:* Ogni funzione booleana sull'algebra di Boole 2 è polinomiale.

Forme minimali di un polinomio booleano. Gli implicanti primi di un polinomio booleano. *Proposizione:* Ogni polinomio è equivalente alla somma di tutti i suoi implicanti primi *(=:s.t.i.p. - senza dimostrazione)*. *Proposizione:* Ogni forma minimale di un polinomio booleano f è somma non ridondante di implicanti primi di f dalla quale non si possa cancellare nessun termine. Il *consenso* di due prodotti. Il *Metodo del Consenso* per il calcolo della s.t.i.p. di un polinomio booleano *(senza dimostrazione)*. Procedura di calcolo di una forma minimale di un polinomio booleano.

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*

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)/AL_2016-17.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