Corso di Laurea Triennale in **Ingegneria Informatica** - a.a. 2025/2026

programma del corso di

ALGEBRA e LOGICA

(6 CFU)

(canale M-Z) prof. Fabio Gavarini

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

INSIEMI, CORRISPONDENZE, RELAZIONI, OPERAZIONI

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

Corrispondenze tra insiemi; operazioni sulle corrispondenze, composizione tra corrispondenze.

Funzioni. Famiglie, comparazione con gli insiemi. Funzioni iniettive, suriettive o biiettive; biiettività e corrispondenza inversa. Composizione di funzioni. Funzioni invertibili e loro caratterizzazioni. Permutazioni in un insieme. Funzioni caratteristiche in un insieme. Biiezione canonica 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. Rela-zioni di preordine, relazioni dí ordine, relazioni di equivalenza. L'equivalenza associata a una funzione. La relazione di divisibilità tra interi e tra naturali. La congruenza modulo n tra numeri interi. Classi di equivalenza, rappresentanti; in-sieme quoziente, proiezione canonica. Partizioni di un insieme. Biiezione naturale tra equivalenze in X e quozienti di X.

Operazioni in un insieme; proprietà speciali, elementi neutri, inversi. Casi speciali: monoidi, gruppi; il gruppo degli invertibili in un monoide. Insiemi con due operazioni; anelli, campi.

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). Il metodo di dimostrazione per induzione.

Divisione con resto tra numeri 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.

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

2º 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: $|\mathbf{R}| = |\mathcal{P}(\mathbf{N})|$.

Elementi di calcolo combinatorio. Calcolo del numero di: *(1)* funzioni da un insieme finito ad un altro; *(2)* funzioni *iniettive* da un insieme finito ad un altro; *(3)* biiezioni tra due insiemi finiti (o permutazioni di un insieme finito in sé stesso) con n elementi: la funzione *fattoriale* di n; *(4)* sottoinsiemi con k elementi in un insieme con n elementi: i *coefficienti binomiali; (5)* partizioni di un insieme con n elementi in k sottoinsiemi: i *coefficienti multinomiali*. La formula di Newton per lo sviluppo delle potenze di un binomio e per lo sviluppo delle potenze di un multinomio. Proprietà notevoli dei coefficienti binomiali, e casi speciali. Il triangolo di Pascal-Tartaglia.

Bibliografia: [AaVv] file Cardinalità *(D'Andrea)* - [Ca] Capitolo I, paragrafi 2 e 6 - [G-P] file Funzioni e cardinalità, paragrafo 5 - [L-L] Chapter 3, section 7 - [PC] Capitolo 1, paragrafi 5 e 6

Videolezioni: *Cardinalità 1* , *Cardinalità 2*

NUMERI INTERI, CONGRUENZE, ARITMETICA MODULARE

Insiemi con due operazioni (binarie): anelli, anelli commutativi unitari, campi. L'anello commutativo unitario dei numeri interi, relazione coi numeri naturali, ordinamento, valore assoluto. Divisibilità, divisori, multipli; elementi invertibili, elementi associati. Elementi riducibili, elementi irriducibili. Fattorizzazioni banali, fattorizzazioni equivalenti. Massimo comun divisore (=*MCD*) e minimo comun multiplo (=*mcm*) tra due interi. Interi coprimi (o "primi tra loro").

La divisione con resto tra due numeri interi. Esistenza di *MCD* in **Z**, e identità di Bézout: algoritmo euclideo delle divisioni successive. Elementi primi; ogni primo è irriducibile; tra i numeri interi, ogni irriducibile è primo *(senza dimostrazione)*.

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 tra loro.

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)*. Divisori dello zero in un anello.

Proposizione: $\mathbf{Z}_n$ è un dominio $\Leftrightarrow$ n è irriducibile (=primo) $\Leftrightarrow$ $\mathbf{Z}_n$ è un campo. Criteri di divisibilità in **Z**.

Equazioni congruenziali in **Z**, equazioni modulari in $\mathbf{Z}_n$: discussione e risoluzione. Definizione di gruppo. Il gruppo degli elementi invertibili in $\mathbf{Z}_n$; criterio di invertibilità, calcolo della classe inversa; la funzione di Eulero. Il *Teorema cinese del resto:* per r, s numeri naturali coprimi, gli anelli commutativi unitari $\mathbf{Z}_{rs}$ e $\mathbf{Z}_r \times \mathbf{Z}_s$ sono isomorfi. Calcolo di potenze in $\mathbf{Z}_n$: generalità, il *Teorema di Eulero (senza dimostrazione)*. L'algoritmo di riduzione dell'esponente di una potenza in $\mathbf{Z}_n$.

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

Insiemi ordinati; diagramma di Hasse. Sottoinsiemi ordinati, intervalli. Ordine prodotto, ordine lessicografico, ordine funzionale. *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; definizione come insiemi ordinati e definizione come insiemi con due operazioni binarie. Il *Teorema di Corrispondenza (per reticoli):* Le due definizioni di reticolo sono equivalenti *(con passi principali della dimostrazione)*. *Principio di Dualità* per reticoli. Esempi e controesempi di reticoli. Limiti, complementi, distributività in un reticolo. *Proposizione:* In un reticolo distributivo, il complemento - se esiste - è unico, e valgono le *Leggi di De Morgan.* Elementi $\vee$-riducibili o $\vee$-irriducibili; atomi. *Proposizione:* In un reticolo finito, *(a)* un elemento è $\vee$ -irriducibile $\Leftrightarrow$ copre al più un elemento, e *(b)* ogni atomo è $\vee$-irriducibile. *Teorema di $\vee$-Fattorizzazione (in $\vee$-irriducibili)* per reticoli finiti; *unicità della $\vee$-fattorizzazione* nel caso distributivo. *Teorema di $\vee$-Fattorizzazione Unica (in atomi)* per reticoli finiti distributivi complementati (=algebre di Boole finite). Isomorfismi tra reticoli, reticoli isomorfi; sottoreticoli. *Caratterizzazione dei reticoli distributivi (senza dimostrazione)*.

Algebre di Boole; definizione come reticolo e come anello booleano unitario. Il *Principio di Dualità* per algebre di Boole. Isomorfismi tra algebre di Boole. *Teorema (Stone - caso finito):* Ogni algebra di Boole finita è isomorfa all'insieme delle parti dell'insieme dei suoi atomi. Sottoalgebre di Boole. *Teorema (Stone - caso generale):* Ogni algebra di Boole è isomorfa a una sottoalgebra di Boole di un insieme delle parti *(senza dimostrazione)*.

Funzioni booleane, polinomi booleani, funzioni booleane polinomiali. Relazione di equivalenza tra polinomi booleani.

Prodotti, prodotti fondamentali, prodotti completi. Somme di prodotti; ridondanza e non-ridondanza. *Forma Normale Disgiuntiva* di un polinomio booleano: esistenza e unicità, calcolo. *Corollario:* Ogni funzione booleana sull'algebra di Boole 2 è polinomiale.

Grandezza di una somma di prodotti. *Forme minimali* di un polinomio booleano. Implicazione tra polinomi; implicanti primi di un polinomio booleano. *Proposizione:* Ogni polinomio è equivalente alla somma di tutti i suoi implicanti primi *(=:s.t.i.p. – cenni della dimostrazione)*. *Proposizione:* Ogni forma minimale di un polinomio booleano f è somma di implicanti primi di f dalla quale non si possa cancellare nessun termine. Il *consenso* tra 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*

BIBLIOGRAFIA (libri, dispense, videolezioni, ecc.) consigliata:

[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