

Programma definitivo di
MATEMATICA DISCRETA
Informatica (corso A)
a.a. 2019/20

1. Cenni di logica

Proposizioni atomiche. Simboli logici e quantificatori. Formule della logica proposizionale e tavole di verità. Tecniche di dimostrazione. Logica predicativa.

2. Richiami di teoria degli insiemi

L'insieme come concetto primitivo. Insieme vuoto. Unione, intersezione insieme delle parti di un insieme. Prodotto cartesiano.

3. Applicazioni

Applicazioni iniettive, surgettive e bigettive. Applicazioni invertibili e caratterizzazione. Insiemi infiniti ed insiemi finiti. Permutazioni.

4. Numeri naturali ed interi

L'insieme \mathbb{N} dei numeri naturali. L'insieme \mathbb{Z} dei numeri interi. Principio di induzione completa. Algoritmo della divisione. Massimo comune divisore e minimo comune multiplo. Numeri primi. Teorema fondamentale dell'aritmetica. Criteri di fattorizzazione di un intero: crivello di Eratostene e criterio di Fermat. Teorema di rappresentazione di un intero in base n . Criteri di divisibilità per 2, 5, 10, 3, 9, 11. Equazioni Diofantee.

5. Relazioni di ordine e di equivalenza.

Relazioni, relazioni riflessive, simmetriche, antisimmetriche e transitive. Relazioni d'ordine ed insiemi ordinati. Insiemi totalmente ordinati. Massimo e minimo. Relazioni di equivalenza. Classi di equivalenza e relative proprietà. Partizioni di un insieme. L'insieme quoziente di un insieme rispetto ad una relazione di equivalenza come partizione. La congruenza $(\text{mod } n)$ su \mathbb{Z} e la costruzione dell'insieme \mathbb{Z}_n delle classi dei resti $(\text{mod } n)$. Congruenze lineari su \mathbb{Z} . Teorema di compatibilità

di una congruenza lineare e soluzioni non congrue ($\text{mod } n$). La funzione di Eulero e le sue principali proprietà. Il piccolo Teorema di Fermat. Teorema di Eulero-Fermat. Soluzione dei sistemi di congruenze lineari; il Teorema cinese dei resti.

6. Cenni di combinatorica

Il numero delle applicazioni (disposizioni con ripetizioni), delle applicazioni ingettive (disposizioni semplici), surgettive e bigettive tra insiemi finiti. Numero delle combinazioni semplici e delle combinazioni con ripetizioni. Principio dei cassetti e principio di inclusione-esclusione. L'insieme S_n delle permutazioni su n oggetti. Permutazioni disgiunte. Cicli e scambi. Scomposizione in cicli disgiunti e quindi in scambi di una permutazione e classe di una permutazione.

7. Monoidi, gruppi, anelli e campi.

Leggi di composizione interne. Monoidi ed esempi. Esempi: il monoide delle parole, $(\mathbb{N}, +)$, (\mathbb{Z}, \cdot) .

Gruppi ed esempi fondamentali: $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, (\mathbb{Q}^*, \cdot) , (\mathbb{R}^*, \cdot) , (S_n, \circ) . Principali proprietà dei gruppi. Leggi di cancellazione. Compatibilità di una legge di composizione interna con una relazione di equivalenza e operazione indotta sul quoziente. Operazioni indotte su \mathbb{Z}_n : il gruppo $(\mathbb{Z}_n, +)$, il monoide (\mathbb{Z}_n, \cdot) . Caratterizzazione degli elementi invertibili di \mathbb{Z}_n . Il gruppo (\mathbb{Z}_p^*, \cdot) , con p primo. Sottogruppi e caratterizzazioni. Sottogruppo ciclico generato da un elemento. Gruppi ciclici ed esempi. Sottogruppi di un gruppo ciclico. Periodo di un elemento di un gruppo. Somma diretta di gruppi. Teorema di Lagrange e Teorema inverso per i gruppi ciclici.

Anelli e principali proprietà. Divisori dello zero, elementi unitari e proprietà relative. Gli anelli $(\mathbb{Z}, +, \cdot)$, $(\mathbb{Z}_n, +, \cdot)$. Definizione di campo ed esempi: $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, $(\mathbb{Z}_p, +, \cdot)$ (con p primo). Principali proprietà dei campi .

8. Matrici su un campo \mathbb{K}

Matrici di tipo (n, m) sul campo \mathbb{K} . L'insieme $M_{n,m}(\mathbb{K})$ delle matrici di tipo (n, m) sul campo \mathbb{K} . Matrici quadrate di ordine n : l'insieme $M_n(\mathbb{K})$ delle matrici quadrate di ordine n . Operazioni tra matrici: somma tra matrici dello stesso tipo; prodotto di un elemento di \mathbb{K} per una matrice; prodotto righe per colonne tra due matrici. Il gruppo

abeliano $(M_{n,m}(\mathbb{K}), +)$. Il monoide non commutativo $(M_n(\mathbb{K}), \cdot)$. Matrici invertibili rispetto al prodotto. Il gruppo $(GL(n, \mathbb{K}), \cdot)$ delle matrici invertibili. $M_{n,m}(\mathbb{K})$ come spazio vettoriale sul campo \mathbb{K} . Algoritmo di Gauss-Jordan per l'ottenimento di una matrice a scala e a scala ridotta a partire da una qualunque matrice. Pivot di una riga di una matrice e rango di una matrice. Caratterizzazione delle matrici quadrate invertibili tramite il rango. Calcolo della matrice inversa di una matrice invertibile tramite l'algoritmo di Gauss-Jordan, Algoritmo per il calcolo della matrice inversa.

9. Grafi

Grafi semplici e multigrafi, essenzialmente nel caso di grafi finiti. Grafi grafi regolari e grafi completi. Matrici di adiacenza e di incidenza di un grafo. Legame tra il numero dei lati e i gradi dei suoi vertici. Cammini e cicli. Cammini Euleriani e Hamiltoniani. Problema dei ponti di Königsberg e Teorema di Eulero. Grafi bipartiti. Grafi bipartiti completi. Grafi connessi e componenti connesse di un grafo. Alberi e loro caratterizzazioni. Grafi isomorfi. Grafi planari. Facce di un grafo planare. Formula di Eulero per i grafi planari. Teorema di Kuratowski.

Testi Consigliati:

A. FACCHINI: **ALGEBRA E MATEMATICA DISCRETA**,
ed. ZANICHELLI

G.M. PIACENTINI CATTANEO: **MATEMATICA DISCRETA**,
ed. ZANICHELLI

F. Dalla Volta, M. Rigoli: **ELEMENTI DI MATEMATICA DISCRETA E ALGEBRA LINEARE**,
ed. PEARSON Education

M.G. BIANCHI, A. GILLIO: **INTRODUZIONE ALLA MATEMATICA DISCRETA**, ed. McGRAW-HILL

L. DI MARTINO, M.C. TAMBURINI: **APPUNTI DI ALGEBRA**, ed. CLUED