Programma del corso di Matematica Discreta
Corso di Laurea in I.T.P.S. – A (Triennale)
A.A. 2020–2021
Dott. Vincenzo C. Nardozza

(1) **Concetti di base.**
   (a) **Logica**
   Proposizioni. Connettivi logici fondamentali e tavole di verità. Proposizioni equivalenti. Contraddizioni e tautologie. Implicazione logica e sue parafrasi. Formulazioni equivalenti della implicazione logica. Bicondizionale. Ordine di precedenza tra gli operatori logici. Regole di negazione (formule di De Morgan). Negazione dell'implicazione e della bicondizionale. Predicati e quantificatori. Regole per la negazione di una proposizione predicativa. Proposizioni dipendenti da più variabili logiche.
   (b) **Insiemistica**
   Insieme universo, insieme, appartenenza. Inclusione e uguaglianza insiemistica. Rappresentazione di un insieme e costruttore logico. Insieme vuoto; l'insieme vuoto è contenuto in ogni insieme; un insieme non cambia se si permutano i suoi elementi o se li si riportano più volte. Unione, intersezione e complementare. Proprietà elementari delle operazioni insiemistiche. Famiglia di insiemi. Leggi di De Morgan. Unione, intersezione e leggi di De Morgan per famiglie di insiemi. Insieme delle parti di un insieme.
   (c) **Relazioni**
   Prodotto cartesiano. **Funzioni:** Definizione di funzione; immagine e controimmagine di un elemento. Rappresentazione di una funzione con diagrammi di Venn, come array a due righe, come parola, tramite il modello d'occupazione. Uguaglianza tra funzioni. Composizione di funzioni. Funzione identità. Funzioni invertibili. Funzioni iniettive, suriettive e bigettive. Caratterizzazione delle funzioni invertibili. **Posets:** relazioni d'ordine parziale. Insiemi totalmente ordinati. Massimo e minimo di un sottinsieme di un poset. Insiemi ben ordinati. Prop: ogni insieme ben ordinato è totalmente ordinato. Diagramma di Hasse di un poset. **Relazioni di equivalenza:** relazione di equivalenza su un insieme. Classi di equivalenza. Insieme quoziente. Partizione di un insieme. Relazione tra partizione di un insieme e relazione di equivalenza su un insieme. Trasversale di una relazione. Proiezione canonica. Relazione di equivalenza indotta da una funzione.
   (d) **Principio di induzione e ricorsività**
   Successioni. Sommatorie. Principio di induzione matematica nelle sue formulazioni equivalenti: induzione semplice, induzione completa e principio del minimo. **Ricorsività:** Algoritmi ricorsivi. Successioni ricorsive. Ricorrenza lineare, ricorrenza omogenea. Forma chiusa di una successione ricorsiva. Progressioni aritmetiche e geometriche.

(2) **Interi**
   Gli interi come quoziente di $\mathbb{N}\times\mathbb{N}$. Richiami sulle operazioni tra interi, loro ordinamento e valore assoluto. Divisibilità tra interi. Algoritmo di divisione euclidea. Rappresentazione degli interi in un sistema posizionale in base $b>1$. Algoritmo di rappresentazione di un intero in base $b>1$. Numero delle cifre di un dato intero in una base b fissata. Massimo comun divisore tra interi. Proprietà elementari del MCD(a,b). Teorema di Bezout. Forma di Bezout per l'espressione del MCD(a,b). Numeri coprimi. Lemma di Euclide. Algoritmo euclideo per il calcolo del MCD. Calcolo dei coefficienti di Bezout. Minimo comune multiplo tra interi. Espressione del mcm tramite il MCD. Generalità e richiami sulle equazioni. Equazioni diofantee. Equazioni diofantee lineari. Metodo di risoluzione delle equazioni diofantee lineari.Numeri interi primi e numeri interi irriducibili. Teorema fondamentale dell'Aritmetica. Esistenza di infiniti interi primi. Esistenza di numeri irrazionali. Crivello di Eratostene.

(3) **Combinatoria**
   Cardinalità e confronto di cardinalità. Insiemi finiti e infiniti. I naturali costituiscono un insieme infinito. Confronto tra le cardinalità degli insiemi numerici. Cardinalità degli insiemi finiti e significato del termine "contare". Principio di addizione. Principio di moltiplicazione. Cardinalità dell'insieme delle parti di un insieme finito. Numero di

divisori di un intero. Disposizioni con ripetizione. Numero di disposizioni con ripetizione di classe k su n oggetti. Disposizioni semplici. Numero di disposizioni semplici di classe k su n oggetti. Permutazioni. Fattoriale. Combinazioni semplici. Coefficiente binomiale. Proprietà elementari del coefficiente binomiale. Triangolo di Tartaglia. Sviluppo delle potenze di un binomio. La somma dei numeri del triangolo di Tartaglia lungo una una stessa riga è una potenza di 2. Formula chiusa del coefficiente binomiale. Combinazioni con ripetizioni di classe k su n oggetti. Numero di combinazioni con ripetizione di classe k su n oggetti. Multinsiemi. Principio di inclusione-esclusione. Principio dei cassetti.

(4) **Aritmetica Modulare**
Congruenza modulo n. La congruenza modulo n è una relazione di equivalenza. Caratterizzazione alternativa della congruenza modulo n. Descrizione delle classi di congruenza. Cardinalità dell'insieme quoziente. Compatibilità della congruenza con le operazioni tra interi. Inversi aritmetici e loro determinazione. Congruenze lineari. Risolubilità di una congruenza lineare. Soluzioni di una congruenza lineare risolubile. Metodi di risoluzione di una congruenza lineare. Ripartizione in classi delle soluzioni di una congruenza lineare. Sistemi di congruenze lineari. Normalizzazione di un sistema di congruenze lineari. Prima formulazione del Teorema Cinese dei Resti.

(5) **Gruppi**
Operazioni su un insieme. Proprietà dintintive di operazioni binarie: Associatività, commutatività, esistenza di un elemento neutro, esistenza del simmetrico. Definizione di gruppo. Esempi di gruppi. Ordine di un gruppo. Addizione tra classi di congruenza modulo n. Il gruppo $\mathbb{Z}_n$. Prodotti diretti di gruppi. Proprietà elementari di un gruppo: unicità dell'elemento neutro e del simmetrico di un elemento. Multipli e potenze di un elemento di un gruppo e loro proprietà. Sottogruppo di un gruppo. In un sottogruppo elemento neutro e inversi si conservano. Lemma di caratterizzazione dei sottogruppi. L'unione di sottogruppi non è un sottogruppo. Il prodotto di sottogruppi non è un sottogruppo. L'intersezione di sottogruppi è un sottogruppo. Sottogruppo generato da un sottinsieme di un gruppo. Sottogruppi ciclici di un gruppo. Gruppi ciclici. Elementi periodici e aperiodici di un gruppo. Periodo di un elemento periodico. Tutti gli elementi di un gruppo finito sono periodici. Proprietà di un elemento aperiodico. Proprietà del periodo di un elemento periodico. Relazione tra periodo di un elemento e ordine del sottogruppo ciclico da esso generato. Teorema di Lagrange per gruppi finiti. Se un gruppo è finito il periodo di un suo elemento divide l'ordine del gruppo. Numero di generatori di un gruppo ciclico finito. Funzione di Eulero. Isomorfismi e omomorfismi tra gruppi. Proprietà di un omomorfismo tra gruppi. Nucleo e immagine di un omomorfismo. Caratterizzazione dell'iniettività tramite il nucleo. Omomorfismo canonico tra $\mathbb{Z}$ e $\mathbb{Z}_n$. Classificazione dei gruppi ciclici. Proprietà dei gruppi ciclici. Reticolo dei sottogruppi di un gruppo ciclico. Teorema fondamentale sui gruppi abeliani finiti.

(6) **Gruppi simmetrici**
Inversa della composizione di due bigezioni. Supporto di una permutazione. Permutazioni a supporto disgiunto commutano. Cicli. Orbita di un elemento sotto una permutazione. Relazione di equivalenza indotta da una permutazione. Cicli associati alle orbite di una permutazione. Decomposizione di una permutazione in un prodotto di cicli disgiunti. Struttura ciclica di una permutazione. Periodo di una permutazione. Alcuni fatti di base sulle permutazioni. Permutazioni coniugate. Ogni permutazione è prodotto di trasposizioni. Parità di una permutazione e funzione segno. Gruppo alterno.

(7) **Anelli**
Definizione di anello. Anelli commutativi e anelli unitari. Proprietà di 0 in un anello. Divisori di zero. Elementi invertibili in un anello. Terminologia: anelli integri, domini di integrità, corpi, campi. Sottoanelli e ideali di un anello. Omomorfismi tra anelli. Nucleo di un omomorfismo e caratterizzazione dell'iniettività di un omomorfismo tramite il suo nucleo. Studio dell'anello $\mathbb{Z}$ e dei suoi ideali. Somma diretta di anelli. Gruppo delle unità di una somma diretta di anelli. Ogni corpo, e in particolare ogni campo, non possiede ideali bilateri non banali. Divisori di zero e elementi invertibili formano insiemi disgiunti. Un ideale proprio non contiene elementi invertibili. Anelli quoziente. Il nucleo di un omomorfismo è un ideale e ogni ideale è il nucleo di un omomorfismo. Anello degli interi $\mathbb{Z}_n$ come anello quoziente. Elementi invertibili e divisori di zero in $\mathbb{Z}_n$. Epimorfismo canonico da $\mathbb{Z}$ a $\mathbb{Z}_n$. Piccolo Teorema di Fermat. Teorema di Eulero–Fermat. $\mathbb{Z}_n$ è un

campo se e solo se n è un primo. Ogni dominio d'integrità finito è un campo. Seconda formulazione del TCR. Moltiplicatività della funzione di Eulero e formula per il calcolo della φ. Criteri di divisibilità. Crittografia ed RSA.

(8) **Polinomi, funzioni polinomiali e campi finiti**
Polinomi a coefficienti in un anello commutativo con unità. Grado di un polinomio e sue proprietà. Divisione euclidea in $F[x]$. MCD e mcm tra polinomi e Teorema di Bezout. Ideali dell'anello $F[x]$. Polinomi irriducibili e polinomi primi. Congruenza modulo un polinomio. Anelli polinomiali. TCR per anelli polinomiali. Funzioni polinomiali. Radici di un polinomio. Polinomi irriducibili su $\mathbb{R}$ e $\mathbb{C}$. Teorema di Ruffini. Principio di identità dei polinomi a coefficienti in un campo infinito. Interpolazione di Lagrange per polinomi a coefficienti in un campo finito. Thm: ogni funzione da un campo finito in sè è polinomiale. Caratterizzazione dell'irriducibilità per polinomi di grado 2 e 3 tramite il Teorema di Ruffini. Ogni sottogruppo finito di F^* è ciclico. Campi finiti e loro classificazione. Aggiunzione di radici. Costruzione di $\mathbb{C}$ come anello polinomiale. Il campo $\mathbb{C}$ è algebricamente chiuso.

(9) **Anelli di matrici**
Matrici quadrate a coefficienti in un campo. Operazioni tra matrici quadrate. Anello delle matrici quadrate. Gruppo generale lineare $GL_n(F)$. Determinante di una matrice. Caratterizzazione delle matrici tramite il determinante. Formula di Binet. Inversa di una matrice 2×2 invertibile tramite il determinante. Operazioni elementari $R_{ij}(a)$, $\mu_i(\alpha)$ e T_{ij} sulle righe di una matrice. Invertibilità e calcolo dell'inversa di una matrice tramite le operazioni elementari sulle righe.

Testo adottato: G.M. Piacentini Cattaneo, *Matematica Discreta e applicazioni*, Zanichelli Editore (2008).

Integrazioni al testo adottato: appunti del docente.

Testi consigliati:

M. Bianchi, A. Gillio, *Introduzione alla Matematica Discreta*, McGraw–Hill Editore, Seconda Edizione (2005).

C. Delizia, P. Longobardi, M. Maj, C. Nicotera, *Matematica Discreta*, McGraw–Hill Editore, (2009).

K. H. Rosen, *Discrete Mathematics and Its Applications*, McGraw–Hill Editore, Settima Edizione (2012) (in Inglese).