Programma di Matematica Discreta

Anno Accademico 2013-14

Prof. Stefano Capparelli

Elementi di teoria dei numeri I numeri naturali. Principio di induzione. Principio del buon ordinamento. Divisione con resto tra interi. Massimo comun divisore. Algoritmo di Euclide. Identità di Bézout. Teorema fondamentale dell'aritmetica. Numeri perfetti. Numeri primi. Frazioni continue. Congruenze. Piccolo teorema di Fermat. Teorema cinese dei resti. Congruenze lineari. Sistemi di congruenze. La funzione ϕ di Eulero. Proprietà di ϕ.

Elementi di algebra moderna Introduzione alla teoria dei gruppi. Teorema di Eulero. Gruppi di permutazioni. Gruppi diedrali. Teorema di Lagrange. Gruppi ciclici. Omomorfismi di gruppo. Nucleo e immagine. Anelli, campi e polinomi. Divisione tra polinomi. Campi finiti. Caratteristica di un campo. Teorema di classificazione dei campi finiti.

Alcune applicazioni Crittografia classica. Cifrari di Cesare. Cifrari con matrici. Sistemi a chiave pubblica.Protocollo Diffie-Hellmann. Autenticazione delle firme. Teoria dei codici. Codici correttori. Distanza minima. Codice di Hamming. Matrici generatrici e matrici di controllo di parità.

Leggi ricorsive Esempi. Numeri Fibonacci. Metodo dello spazio vettoriale.Metodo della matrice. Metodo della funzione generatrice. Numeri di Catalan. Ricorrenze lineari. Serie formali. Funzione generatrice della successione di Catalan.

Cenni di teoria delle partizioni di interi Definizioni. Diagrammi di Ferrers. Partizioni coniugate. Teorema delle partizioni di Eulero. Il problema degli spiccioli.

Combinatoria Regola del prodotto. Principio di inclusione-esclusione. Numero di Ramsey. Polinomi ortogonali. Successione dei momenti. Formula di ricorrenza. Coefficienti binomiali.Varie identità. Convoluzione di Vandermonde. Composizioni di interi.

Introduzione alla teoria dei grafi Definizioni ed esempi. Grafi semplici, multigrafi, pseduografi, grafi orientati. Handshaking lemma. Grafi semplici notevoli: grafi completi, cicli, ipercubi, grafo di Petersen. Grafi bipartiti. Rappresentazione attraverso matrici. Isomorfismi. Connettività. Cammini e circuiti di Eulero. Cammini e circuiti di Hamilton. Grafi planari, Teorema di Eulero sui grafi. Teorema di Kuratowski. Colorazione dei grafi.

Testi di riferimento.

- S. Capparelli, *Appunti di Matematica Discreta*, dispense del corso, 2014
- P. Maroscia, *Geometria e Algebra Lineare*, Zanichelli 2002.
- M. Cerasoli, F. Eugeni, M. Protasi, *Elementi di Matematica Discreta*, Zanichelli 1988.
- R.L. Graham, D.E. Knuth, O. Patashnik, *Concrete Mathematics: A foundation for Computer Science*, Addison-Wesley, Reading, MA, 1994.
- M. Aigner, G.M. Ziegler *Proofs from THE BOOK*, Springer, 2004
- M.W. Baldoni, C. Ciliberto, G. M. Piacentini Cattaneo, *Aritmetica, Crittografia e Codici*, Springer 2006