

Anno Accademico 2006-2007, ciclo 2.

Programma del Corso: ELEMENTI DI ALGEBRA E LOGICA

Prima settimana: Insiemi e operazioni sugli insiemi. Funzioni iniettive, suriettive, invertibili. Cardinalità. Induzione matematica. Funzioni ricorsive.

L&L., Cap I, Sez.1,2,3,4,5,6,7,8,9,10. Cap III: Sez.1,2,3,5,6,7, Foglio di Esercizi 1.

Seconda settimana: Relazioni. Relazioni di equivalenza su un insieme, classi di equivalenza, insieme quoziente. Relazioni di ordine parziale, elementi massimali e minimali, massimo e minimo, insiemi totalmente ordinati, insiemi bene ordinati, diagramma di Hasse di un insieme finito parzialmente ordinato. Grafo associato ad una relazione, matrice associata ad una relazione, chiusure di relazioni.

L&L., Cap.II: Sez.1,2,3,4,6,8,9, Cap.XIV: Sez.3,5,7, Foglio di Esercizi 2.

Terza settimana: Aritmetica sui numeri interi: divisione con resto, divisibilità, massimo comun divisore, numeri primi, Teorema fondamentale dell'aritmetica, algoritmo euclideo e applicazioni. La relazione di congruenza modulo n . Congruenze e sistemi di congruenze. Teorema cinese del resto.

L&L., Cap.XI: Sez.4,5,6,7,8,9.
Appunti 1. Foglio di Esercizi 3.

Quarta settimana: Gruppi, anelli, campi. Il teorema di Lagrange, il Piccolo teorema di Fermat.

L&L., Cap.XII: Sez.2,4,6(cenni).
Appunti 2. Foglio di Esercizi 4.

Quinta/sesta settimana: Il criptosistema RSA. Test di primalità. Reticoli: assiomi di definizione, ordinamento parziale su un reticolo, isomorfismi di reticoli. Reticoli limitati.

Appunti 2.
R. Schoof, Fattorizzazione e criptosistemi a chiave pubblica.
L&L., Cap.XIV: Sez.8 (no dualità, no teorema 14.2), esercizio 14.34, Sez. 14.9. Fogli di Esercizi 6 e 7.

Settima settimana: Reticoli distributivi, reticoli complementati, reticoli booleani. Algebre di Boole. Calcolo proposizionale.

L&L., Cap.XIV: Sez.10,11. Cap.XV: Sez.1,2,4,5,6. Cap.IV: Sez.1,2,3,4,5,6,7,8. Foglio di Esercizi 7.

Ottava settimana: L'algebra di Boole della logica proposizionale. Espressioni Booleane: forma normale disgiuntiva, forma normale disgiuntiva completa, implicanti primi e forme minimali. Metodo del consenso per la determinazione di tutti gli implicanti primi. Predicati e quantificatori.

L&L., Cap.XV: Sez.7,8,9. Cap.IV: Sez.11. Foglio di Esercizi 8.