LABORATORIO DI ALGORITMI
PROGRAMMA

Premessa
Durante il laboratorio, oltre alla presentazione di alcuni argomenti prerequisito indispensabile per la comprensione del corso, verranno, a titolo di esercizio, implementati alcuni tra gli algoritmi esposti a lezione.
Inoltre, verranno esposti e implementati alcuni algoritmi di teoria dei numeri, con particolare riferimento alla fattorizzazione dei numeri interi.

Per partecipare al laboratorio è indispensabile conoscere i rudimenti del linguaggio di programmazione C++

Bibliografia
Il materiale presentato verrà estratto dai seguenti testi:

- Thomas H. Cormen, Charles E. Leiserson, Ronald L. Rivest, Clifford Stein - Introduction to Algorithms - Mc Graw Hill Book Company - 2003
- Robert Sedgewick - Algorithms - Addison Wesley Publishing Company - 1984
- Alan Parker - Algorithms and Data Structures in C++ - CRC Press - 1993
- David Bressoud, Stan Wagon - Computational Number Theory - Key College Publishing - 2000

Links

Maurizio Dini:
maurizioudini@katamail.com
http://web.freepass.it/maurizioudini

Davide Mognaschi:
http://www.cdmp.it/algoritmi

PRIMA PARTE

Introduzione
Definizione di algoritmo
Progettazione e analisi di algoritmi. Input, output, istanze.
Efficienza degli algoritmi
Dimensione dell'input (input size)
Tempi di elaborazione (running time)
Tasso di crescita dei tempi di elaborazione (order of growth)
Classificazione della complessità. Caso peggiore, caso medio
Richiami di analisi
Ordine di infinito e di infinitesimo. Simboli di Landau
Funzioni monotone
Parte intera e intero successivo
Classi di resto modulo n
Polinomi
Potenze
Logaritmi
Fattoriale e Stirling
Il logaritmo iterato

Pseudocodice
Definizione e convenzioni

Progettazione di algoritmi
"Forza bruta" (approccio incrementale) vs "Divide et impera" (approccio ricorsivo)
Un primo esempio. I due approcci a confronto: l'algoritmo Insertion Sort e l'algoritmo Merge Sort
Algoritmi probabilistici

Rappresentazione dei dati
interi
virgola mobile
alfanumerici
conversione dati
Operazioni sui dati
Porte logiche
Grafi

Funzioni ricorsive
Definizione ed esempi: fattoriale, la successione di Fibonacci
Relazioni ricorsive del 2° ordine
Funzioni Booleane

SECONDA PARTE

Algoritmi di teoria dei numeri
L’algoritmo euclideo diretto, inverso ed esteso
La tripla pitagorica
Aritmetica modulare
Fast exponentiation
Potenze di matrici
Il teorema cinese del resto
Piccolo teorema di Fermat
Numeri primi
Quanti sono?
Il metodo di Eratostene
Certificazione e tests di primalità
Una dozzina di congetture sui primi
Numeri primi e crittografia: l’algoritmo RSA
La funzione di Eulero
Algoritmi di fattorizzazione
Frazioni continue e fattorizzazione
Generazione di numeri casuali e test di casualità
Trasformata di Fourier discreta DFT
Computazione quantistica
I postulati della meccanica quantistica: una diversa logica di calcolo
Il modello di rappresentazione
Spazi di Hilbert
Prodotto tensore
Basi computazionali
Porte logiche
Algoritmo quantistico di Shor per la fattorizzazione dei numeri interi