Internet e il Web: cosa c'è sotto?

Paolo BURGIO

Lunedì 15 giugno: 9.30 – 12.30

Tutti usiamo internet, ma veramente sappiamo cosa succede ad ogni click del mouse? In poco meno di due ore ripercorreremo le origini di internet e del web (che non sono la stessa cosa): da semplice rete per la trasmissione dei dati, ad Arpanet (ministero della difesa USA … perché i militari ci son sempre di mezzo), al World Wide Web, al Web 2.0. Verranno spiegate le problematiche di base per la trasmissione di pacchetti sul web, introdotti i protocolli principali (TCP/IP, HTTP(S), ecc ecc) alla base di internet, e le tecnologie coinvolte: da HTML a javascript, dai server web ai browser, da facebook a …

In piedi sulle spalle dei giganti.

Marko BERTOGNA

Lunedì 15 giugno: 14.00 – 17.00

La lezione fornirà alcune modalità di base per la realizzazione di software che utilizzino librerie esistenti. Verranno illustrati i passi principali del processo di compilazione/collegamento, distinguendo tra collegamento statico e dinamico delle librerie. Durante la lezione verranno forniti esempi di applicazioni software a giochi realizzati dagli studenti del corso di Programmazione II.

Esplorazioni numeriche, congetture e dimostrazioni

Nicolina MALARA

Martedì 16 giugno: 9.30 – 12.30

L'attività si propone l'esplorazione guidata di una serie di situazioni numeriche finalizzata alla formulazione e risoluzione di problemi dimostrativi. Si parlerà anche del principio di induzione e si proporrà la sua applicazione come metodo dimostrativo in casi semplici. Si parlerà, inoltre, delle funzioni della dimostrazione e del suo ruolo nello sviluppo delle teorie matematiche.
Si studieranno classici problemi aritmetici attraverso i quali si porteranno gli studenti a sviluppare dimostrazioni, a riflettere sul ruolo del linguaggio algebrico nella produzione di pensiero e sul significato del principio di induzione.
Lo scopo è portare gli studenti a misurarsi con le modalità tipiche di lavoro matematico, giungendo a formulare congetture sulla base di regolarità osservate, ad argomentare ed a produrre la costruzione di semplici dimostrazioni.

Come fanno le calcolatrici tascabili a calcolare seno e coseno?

Carlo BENASSI

16 giugno 2015, ore 14.00 – 17.00

Il CORDIC (COordinate Rotation Digital Computer) è l'algoritmo che viene generalmente usato dalle calcolatrici tascabili per calcolare pressoché istantaneamente il valore delle funzioni trigonometriche senza per questo aver bisogno di grandi risorse hardware. Il CORDIC è stato introdotto nel 1959 per permettere ai computer di allora di calcolare velocemente il seno ed il coseno di un angolo, ma presto si scoprì che con poche modifiche esso poteva essere utilizzato per calcolare anche tutte le altre funzioni elementari: le funzioni trigonometriche inverse, esponenziali e logaritmi, perfino le radici. Sebbene sia molto ingegnoso, il CORDIC fa uso di strumenti matematici tutto sommato elementari, cioè di quelli che si incontrano nella scuola superiore.
In questa attività vedremo come funziona il CORDIC e cercheremo di apprezzarne l'efficacia aiutandoci anche con qualche semplice simulazione numerica.

Crittoanalisi e Statistica

Luca LA ROCCA

17 giugno 2015, ore 10.00 – 16.30

Nel IX secolo d.C., mentre l'Europa si culla nel medioevo, lo studioso arabo al-Kindi descrive per la prima volta come l'analisi delle frequenze permetta di decrittare un testo cifrato per sostituzione monoalfabetica (la tecnica di cui la cifratura di Cesare è il primo esempio documentato di impiego militare). La sostituzione monoalfabetica è destinata a diventare un argomento di enigmistica, mentre la statistica muove i primi passi come disciplina che studia l'estrazione di segnali da dati rumorosi.

Gli studenti avranno modo di sperimentare il metodo di al-Kindi, avvalendosi di una breve introduzione dell'insegnante e del software statistico R (liberamente disponibile in rete). Verranno affrontati testi in cifra di difficoltà crescente, con l'obiettivo di arrivare a decrittare testi cifrati per sostituzione polialfabetica. In particolare, si cercherà di far breccia nella cifratura di Vigenère mediante il test di Kasinski, ideato in prima battuta da quel Charles Babbage meglio noto come "padre del computer".

Infine, prendendo spunto dal fatto che il metodo di al-Kindi necessita di stimare le frequenze delle diverse lettere nella lingua di interesse, sulla base di un campione di parole, si discuterà l'incertezza associata a questa operazione e la sua possibile quantificazione (come per esempio nei sondaggi politico elettorali).

Dai Numeri Primi alla Crittografia Moderna

Gloria Rinaldi Giuseppe Mazzuoccolo

18 giugno 2015, ore 9:30-17

Per secoli il fascino dei numeri primi ha suscitato l'interesse e la curiosità di grandi matematici. I problemi ad essi connessi hanno una formulazione per lo più semplice e ciò ha creato grande

interesse da parte di molti, anche non esperti. Tuttavia, dietro alle facili formulazioni, si nascondono problematiche profonde che paiono ancora molto lontane da una soluzione.

Ciò ha fatto dei numeri primi un oggetto molto utile da utilizzare nelle moderne tecniche crittografiche.

Prima parte 9:30-12:30 Gloria Rinaldi:

Una prima parte introduttiva affronta i concetti generali della crittografia (riservatezza, autenticazione, canale sicuro) e presenta la crittografia classica a chiave privata attraverso cenni ai codici più noti (codice di Cesare, codice di Vigenere, macchina Enigma). Viene poi introdotto il problema dello scambio e distribuzione delle chiavi e il passaggio da crittografia a chiave privata a crittografia a chiave pubblica.

Si affronta quindi da un punto di vista teorico lo studio dei numeri primi quale strumento per la costruzione dell' algoritmo RSA di cifratura a chiave pubblica. Riguardo ai numeri primi vengono presentati il Teorema di Euclide sulla loro infinità, il Teorema fondamentale dell'Aritmetica, il Teorema di Hadamard e De la Vallée-Poussin. Si introduce l'aritmetica modulare e si presentano i Teoremi di Eulero Fermat e la costruzione teorica dell'algoritmo RSA, discutendone l'efficienza e la sicurezza in relazione ai problemi irrisolti sui numeri primi.

Seconda parte 14-17 Giuseppe Mazzuoccolo:

Attività in laboratorio di calcolo: Con l'utilizzo da parte degli studenti del calcolatore si mostrerà loro come il problema di stabilire la primalità di un numero sia un problema computazionalmente "economico", mentre determinare la decomposizione in fattori primi di un numero assegnato sia un problema generalmente "costoso". In particolare, si evidenzierà l'utilizzo di queste proprietà per il funzionamento del sistema crittografico RSA introdotto nella prima parte del corso. Sempre per sperimentazione diretta si introdurranno poi altri problemi aperti della Teoria dei Numeri legati alla distribuzione dei numeri primi (primi gemelli, primi repunit...).

"Ritorno al futuro: Un'avventura nel mondo dell'informatica"

Riccardo MARTOGLIA

19 giugno 2015, ore 10.00 – 16.30

L'attività condurrà per mano i ragazzi nella realizzazione di un piccolo videogioco del tipo "Scegli la tua avventura" (LibroGame), portandoli al contempo in una sorta di viaggio nel tempo nel mondo dell'informatica e della gestione dell'informazione al computer.

Dopo una piccola introduzione da parte del docente sui Libri-gioco, molto popolari negli anni '80, ed una dimostrazione di alcuni esempi liberamente fruibili, nella parte iniziale dell'attività i ragazzi saranno invitati, attraverso piccoli esempi e un software di emulazione, a toccare con mano come si sarebbe dovuti procedere per realizzare le basi del gioco su un dispositivo di quell'epoca.

La parte principale dell'attività ci riporterà poi, con un viaggio nel tempo di circa 30 anni, all'informatica dei giorni nostri e alla programmazione odierna. Il docente introdurrà, con opportune semplificazioni, alcune moderne tecniche per la memorizzazione dei dati e per la loro fruizione (argomenti alla base dell'informatica e del mondo di internet). I ragazzi potranno quindi immediatamente toccare con mano tali tecniche, progettando insieme al docente la parte dei dati (le

"stanze" del gioco) e costruendo una pagina web "intelligente" che accederà e visualizzerà tali dati, permettendo al giocatore di compiere i primi passi nell'avventura.