Numeri Primi, Algebra Modulare e Crittografia

Professoressa Gloria **Rinaldi**

17 giugno 2013

L'attività prevede una parte introduttiva che affronta i concetti generali della crittografia e presenta la crittografia classica a chiave privata, attraverso cenni ai codici più noti (codice di Cesare, codice di Vigenère, macchina Enigma). Viene poi introdotta la crittografia a chiave pubblica ponendo l'accento sul problema dello scambio delle chiavi (protocollo del doppio lucchetto, idea di Diffide-Hellman).

La seconda parte, svolta in modalità laboratoriale ponendo l'accento più sugli esempi concreti che sulla parte dimostrativa, affronta le problematiche da un punto di vista matematico.

Si parla quindi di numeri primi, della loro distribuzione nell'insieme degli interi, di test di primalità e di problemi di fattorizzazione. Si introduce l'aritmetica modulare e si presentano i teoremi di Eulero-Fermat, utili alla costruzione dell'algoritmo RSA. Su questa parte gli studenti sono chiamati a interagire con il docente, attraverso soluzione di esercizi mirati.

L'attività si conclude con la presentazione dell'algoritmo RSA e vede gli studenti impegnati nella implementazione di un sistema RSA di tipo didattico, con esecuzione di tutti i passaggi (costruzione e scambio di chiavi, cifratura e firma, verifica della firma e decifratura).

Crittoanalisi e Statistica

Professor Luca **La Rocca**

18 giugno 2013

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 orientata alla risoluzione di problemi.

Gli studenti avranno modo di sperimentare il metodo di al-Kindi, avvalendosi di una breve introduzione dell'insegnante e di un opportuno software. 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).

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

Professor Riccardo **Martoglia**

19 giugno 2013

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, la parte iniziale dell'attività mostrerà dal vivo ai ragazzi, direttamente dalla collezione del dipartimento FIM, uno dei più importanti computer di quegli anni, vera pietra miliare della storia dell'informatica. Dopo aver imparato alcuni principi base, con piccoli esempi e un software di emulazione i ragazzi saranno invitati a toccare con mano come si sarebbe dovuti procedere per realizzare le basi del gioco su un tale dispositivo.

La parte principale dell'attività ci riporterà invece, 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 la loro fruizione (argomenti alla base dell'informatica e del mondo di internet). Ancora una volta, 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 informazioni, permettendo di compiere i primi passi nell'avventura.

Ma quante sono le geometrie?

Professoressa Paola **Bandieri**

20 giugno 2013

L’attività prevede un momento iniziale di introduzione all’argomento delle Geometrie non euclidee attraverso una “conferenza interattiva”. L’insegnante, cioè, introdurrà le motivazioni storico-filosofiche, i contenuti base, nonché i paralleli e le differenze tra la geometria euclidea e le geometrie non euclidee e ciò avverrà attraverso un costante confronto con i ragazzi e attività manipolative che stimolino la riflessione.

In un secondo momento, attraverso lo strumento del software Cinderella, che permette costruzioni geometriche in tutte le geometrie, i ragazzi saranno invitati ad analizzare alcuni classici teoremi della geometria euclidea e le loro dimostrazioni, soffermandosi in particolare sulla necessità o meno del quinto postulato.

In questo modo si distingueranno i teoremi della geometria assoluta da quelli della geometria euclidea e si analizzerà con Cinderella quale sia l’equivalente dei teoremi di geometria euclidea nelle altre geometrie. Non mancheranno, tra l’altro, scoperte sorprendenti sulle proprietà di certi oggetti matematici, divenuti familiari a tutti, quando li si esamini in ambiti non euclidei.

E’ assolutamente indispensabile che ogni partecipante si presenti munito di forbici (magari a punta arrotondata).