Teoria dei Numeri I : Programma del corso
(prof. Marilena Barnabei)

Partizioni di un intero. Diagrammi di Ferrers e proprietà relative. Il reticolo di Young.
Tabelle di Young. Algoritmo di Robinson-Schensted e sue proprietà. Teorema di Eulero: formula per la funzione generatrice della successione p(n)=numero di partizioni di n.
Dimostrazione del Teorema di Eulero. Funzione generatrice delle successioni di:

- numero di partizioni di n in parti dispari;
- numero di partizioni di n in parti dispari e distinte;
- numero di partizioni di n la cui parte maggiore è uguale a k.

Coefficienti binomiali Gaussiani: definizione, formula esplicita, proprietà. Interpretazione in termini di matrici a scala ridotta e di partizioni di interi. Partizioni di un intero contenute nella "scatola" hxk e loro legame con i coefficienti Gaussiani. Numeri pentagonali e formula di Eulero. Dimostrazione combinatoria del secondo Teorema di Eulero. Formula ricorsiva per la successione p(n).

Richiami su interi e congruenza. Sistema ridotto di residui modulo n. Funzione di Eulero: definizione e proprietà. Teorema: la funzione di Eulero è moltiplicativa. Teorema: la somma dei valori della funzione di Eulero su tutti i divisori di n è uguale ad n. Teorema di Eulero-Fermat e sue conseguenze. Piccolo Teorema di Fermat. Definizione della funzione di Moebius. Formula di inversione di Moebius. Applicazioni: il problema delle collane. Il metodo RSA.

Equazioni modulari: equazioni lineari. Condizione necessaria e sufficiente affinché un'equazione lineare abbia soluzione. Determinazione delle soluzioni. Equazioni modulari di grado superiore al primo. Il caso di modulo primo: Teorema di Lagrange. Teorema di Wilson.
Equazioni modulari di grado qualunque: caso generale e caso di modulo potenza di un primo.
Residui quadratici. Simbolo di Legendre (a|p). Criterio di Eulero. Moltiplicatività del simbolo di Legendre. Valutazione di (-1|p) e di (2|p). Legge di reciprocità quadratica: dimostrazione di Gauss.
Simbolo di Jacobi e proprietà relative: periodicità, moltiplicatività, reciprocità. Equazioni modulari di secondo grado.

Algoritmi di fattorizzazione: fattorizzazione per tentativi, metodo di Fermat, metodo "rho" di Pollard.
Test di primalità: test di Fermat e di Miller-Rabin. Teorema di Lucas-Lehmer.

Terne Pitagoriche. Terne primitive. Metodo di Euclide per determinare le terne primitive.

Funzioni aritmetiche: definizione e primi esempi.
Funzioni moltiplicative e completamente moltiplicative. Funzione somma di una funzione aritmetica data e sue proprietà. Esempi: le funzioni somma di potenze dei divisori.
Prodotto di Dirichlet per le funzioni aritmetiche e sue proprietà. L'algebra delle funzioni aritmetiche. Caratterizzazione delle funzioni invertibili. Funzione di von Mangoldt e sue proprietà. Il prodotto di funzioni moltiplicative è moltiplicativo. L'inversa di una funzione moltiplicativa è moltiplicativa.
Relazione tra la funzione di Moebius e le radici dell'unità. Caratterizzazione delle funzioni completamente moltiplicative tramite la loro inversa. Funzione di Liouville. Funzioni "potenza dei divisori" e loro proprietà.
Convoluzione generalizzata tra una funzione aritmetica ed una funzione di variabile reale. Proprietà. Funzione di distribuzione di una funzione aritmetica. Formula di inversione di Moebius generalizzata. Derivazione nell'algebra delle funzioni aritmetiche e proprietà relative. Identità di Selberg.

La distribuzione dei numeri primi: l'andamento asintotico della funzione \pi(x) è quello di x/logx (senza dimostrazione). Le funzioni \psi e \theta di Chebyshev e loro proprietà. Formulazioni equivalenti del teorema dei numeri primi. Serie di Dirichlet di una funzione aritmetica. L'algebra delle serie di Dirichlet. La funzione Zeta di Riemann e le sue proprietà elementari.

Testi consigliati:
Tom M. Apostol: Introduction to Analytic Number Theory – Springer, 2010
Marilena Barnabei, Flavio Bonetti: Elementi di Aritmetica Modulare – Esculapio, 2014