Programma del corso di
TEORIA DEI NUMERI E CRITTOGRAFIA
tenuto dalla Prof. Patrizia LONGOBARDI
nell'anno accademico 2011/2012

Richiami sulla divisibilità nell'insieme dei numeri naturali e dei numeri interi, teorema fondamentale dell'aritmetica, teorema di Bézout.

Numeri primi, osservazioni sulla loro distribuzione, crivello di Eratostene.

Numeri di Fermat, primi di Fermat. Numeri di Mersenne, primi di Mersenne.

Metodo di Fermat per la ricerca di divisori.

Richiami sulle congruenze nell'anello degli interi. L'anello $\mathbb{Z}_n$ $(n > 0)$. Insiemi completi di residui modulo un intero, di residui ridotti.

Criteri di divisibilità, prova del nove. Numeri palindromi, numeri triangolari.

Dimostrazioni del "piccolo teorema"di Fermat, del teorema di Wilson, del teorema di Eulero.

Equazioni diofantine lineari, condizioni necessarie e sufficienti perché esistano soluzioni e loro determinazione.

Il metodo "$p-1$"di Pollard per la ricerca di divisori di un intero.

Equazioni congruenziali lineari, condizioni necessarie e sufficienti perché esistano soluzioni e metodi per determinarle. Teorema cinese del resto, una sua generalizzazione. Pseudoprimi e numeri di Carmichael. Numeri che "passano il test"per un intero.

Legami tra polinomi a coefficienti interi e polinomi a coefficienti in Z_n. Teorema di Lagrange. Un criterio di primalità con i polinomi.

Funzioni aritmetiche, funzioni moltiplicative. La funzione "numero dei divisori"e la funzione "somma dei divisori". Numeri perfetti. La funzione di Eulero. La funzione di Möbius, la formula di inversione di Möbius. Il prodotto di Dirichlet.

Il gruppo delle unità di Z_n. Radici primitive. La struttura del gruppo delle unità di Z_n. L'esponente universale. Caratterizzazione dei numeri di Carmichael.

Congruenze quadratiche, il gruppo dei residui quadratici, il simbolo di Legendre, il criterio di Eulero, il lemma di Gauss. La legge di reciprocità quadratica. Residui quadratici per moduli arbitrari.

Cenni sulle somme di quadrati e sul problema di Waring, condizioni necessarie perché un numero sia somma di due o tre quadrati.

Metodo della "discesa infinita"di Fermat, cenni sulle terne pitagoriche e sull'ultimo teorema di Fermat.

Generalità sulla crittografia. Cifrari di Cesare, cifrari affini, cifrari con matrici (o di Hill), cifrari monoalfabetici e polialfabetici, il cifrario di Vigenère. Il logaritmo discreto, l'algoritmo baby step - giant step. Codici a chiave pubblica, il criptostema di Diffie-Hellman, la firma digitale, il metodo del doppio lucchetto, il criptosistema di Massey-Omura, il criptosistema di ElGamal. Il problema dello zaino, il problema supercrescente dello zaino, il cifrario a chiave pubblica di Merkle-Hellman. Il sistema RSA.

Testi consigliati

G. A. Jones, J. M. Jones, *Elementary Number Theory*, Springer, 1998 (rist. 2003);

e inoltre

M. W. Baldoni, C. Ciliberto, G. M. Piacentini Cattaneo, *Aritmetica, crittografia e codici*, Springer, 2006;

M. Curzio, P. Longobardi, M. Maj, *Lezioni di algebra*, Liguori, 1994 (II rist. 1996);

H. Davenport, *Aritmetica Superiore*, Zanichelli, 1994;

G. H. Hardy, E. M. Wright, *Introduction to the Theory of Numbers*, Oxford University Press, 1979;

K. Ireland, M. Rosen, *A Classical Introduction to Modern Number Theory*, II ed., Springer, 1992;

N. Koblitz, *A Course in Number Theory and Cryptography*, Springer, 1987 (II ed. 1994);

S. Leonesi, C. Toffalori, *Numeri e Crittografia*, Springer, 2006;

H. E. Rose, *Course in Number Theory*, Oxford University Press, 1988.