Programma del corso di
TEORIA DEI NUMERI
ALGEBRA SUPERIORE - I modulo
tenuto dalla Prof. Patrizia LONGOBARDI
nell'anno accademico 2002–2003

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.

Legami tra polinomi a coefficienti interi e polinomi a coefficienti in Z_n. Teorema di Lagrange.

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, condizioni necessarie e sufficienti perché esistano. La struttura del gruppo delle unità di Z_n. L'esponente universale.

Il gruppo dei residui quadratici, il simbolo di Legendre, Criterio di Eulero. Lemma di Gauss. La legge di reciprocità quadratica. Caratterizzazione dei residui quadratici.

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

Cenni sul metodo della "discesa infinita"di Fermat, sulle terne pitagoriche e sull'ultimo teorema di Fermat.

Cenni di crittografia, codici a chiave pubblica: il sistema di Diffie e Hellman, il sistema RSA.

Testi consigliati

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

e inoltre

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);

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