MATEMATICA DISCRETA

1. DESCRITTORI

1.1 *Settore scientifico-disciplinare*: <MAT 03>
1.2 *Crediti formativi universitari*: <6-CFU>
1.3 *Docente*: <Stefano Capparelli>
1.4 *Contatti docente*: <0649766682-capparelli@member.ams.org>
1.5 *Offerto ai corsi di studio*: <corso di laurea 3 anno>
1.6 *Calendarizzazione*: < secondo semestre>
1.7 *Tipologia di valutazione*: <esame con votazione in trentesimi >
1.8 *Anni accademici di riferimento*: <2013-14>

2. OBIETTIVI DEL MODULO E CAPACITÀ ACQUISITE DALLO STUDENTE

ITALIANO

Lo scopo principale del corso è quello di illustrare nozioni, metodi e risultati fondamentali nel settore della Matematica Discreta, riguardanti in particolare la teoria dei numeri, la combinatoria, la teoria dei gruppi, la teoria dei campi finiti, la teoria dei grafi e i codici lineari.

INGLESE

The principal aim of the course is to present basic ideas, methods and results of Discrete Mathematics, with particular regard to number theory, combinatorics, group theory, finite fields theory, graph theory and linear codes.

3. RISULTATI DI APPRENDIMENTO ATTESI

ITALIANO

Gli studenti che abbiano superato l'esame avranno buona padronanza di metodi e risultati nell'ambito della Matematica Discreta, utili per impostare e risolvere vari problemi, soprattutto di carattere applicativo. Ciò come conseguenza di un approccio concreto allo studio, sviluppato durante il corso, e all'impegno sistematico rivolto all'attività di "problem solving".

INGLESE

First of all, a successful student will be able to have a direct approach to the study of concrete problems, as a result of a long training specifically oriented to "problem solving". Moreover, he will master techniques and results of Discrete Mathematics, useful for the study of relevant applied problems.

4. PROGRAMMA

ITALIANO

Numeri interi. Numeri primi. Numeri di Fibonacci. Il teorema fondamentale dell'Aritmetica e alcune sue conseguenze. La funzione di Eulero. La congruenza modulo n . Sistemi di congruenze. Il teorema cinese dei resti. Gruppi. Gruppi ciclici. Gruppi finiti. Il teorema di Lagrange. Il teorema di Cauchy. Il piccolo teorema di Fermat. Il teorema di Eulero. Anelli e campi. Campi finiti. Polinomi, matrici e spazi vettoriali su un campo finito. Introduzione ai codici lineari. Teoria delle partizioni di interi. Funzioni generatrici, trasformata zeta. Successioni definite per ricorrenza. Polinomi ortogonali. Identita' soddisfatte da coefficienti binomiali. Formula di Vandermonde. Grafi finiti. Grafi connessi. Alberi. Il teorema di Cayley. Grafi piani. La formula di Eulero. Il teorema di Kuratowski. Grafi euleriani. Grafi hamiltoniani. La matrice di adiacenza di un grafo finito e le sue potenze. Il polinomio caratteristico di un grafo. Autovalori di un grafo.
Alcuni risultati generali sugli insiemi finiti. I numeri di Bell e la formula di Aitken. Il teorema di Pick. Introduzione alla teoria di Ramsey. Crittografia a chiave pubblica. Funzioni aritmetiche unidirezionali. Il metodo di Diffie e Hellman. Il protocollo RSA.

INGLESE

Integers. Prime numbers. Fibonacci's numbers. The fundamental theorem of Arithmetic and some of its consequences. The Euler function. The congruence modulo n . Systems of congruences. The Chinese remainder theorem. Groups. Cyclic groups. Finite groups. Lagrange's theorem. Cauchy's theorem. Fermat's little theorem. Euler's theorem. Rings and fields. Finite fields. Polynomials, matrices and vector spaces over

a finite field. Introduction to linear codes. Partitions of integers. Generating functions. z-transform. Binomial coefficients. Vandermonde identity. Finite graphs. Connected graphs. Trees. Cayley's theorem. Planar graphs. Euler's formula. Kuratowski's theorem. Eulerian graphs. Hamiltonian graphs. The adjacency matrix of a finite graph and its powers. The characteristic polynomial of a graph. Eigenvalues of a graph. Some general results on finite sets. The Bell numbers and Aitken's formula. Pick's theorem. Introduction to Ramsey's theory. Public-key cryptography. Unidirectional arithmetical functions. The method of Diffie and Hellman. The RSA protocol.

5. MATERIALE DIDATTICO

- S. Capparelli, Lezioni di Matematica Discreta, Appunti del corso , 2013
- P. Maroscia, Geometria e Algebra lineare, Zanichelli, 2002
- M. Cerasoli - F. Eugeni - M. Protasi, Elementi di matematica discreta, Zanichelli, 1988
- R.L. Graham - D.E. Knuth - O. Patashnik, Matematica discreta, Hoepli, 1996
- M. Aigner - G.M. Ziegler, Proofs from THE BOOK, Springer, 2004

6. SITO WEB DI RIFERIMENTO

http://www.dmmm.uniroma1.it/~stefano.capparelli/