UNIVERSITÀ
DEGLI STUDI DI MILANO-BICOCCA

SYLLABUS DEL CORSO

Metodi Algebrici per l'Informatica

2122-2-E3101Q129

Obiettivi

Lo studente sarà in grado di utilizzare alcuni strumenti dell'algebra astratta per risolvere ed analizzare alcuni problemi legati al mondo dell'informatica. Ad esempio, i fondamenti che permettono di utilizzare i codici per sistemi di auto correzione di errore, e i fondamenti che vengono utilizzate per garantire la sicurezza dei piu' diffusi sistemi crittografici moderni.

Contenuti sintetici

Introduzione alle strutture algebriche di base. Aritmetica modulare, campi finiti e gruppi di permutazioni. Breve introduzione alla crittografia. Teoria dei codici, codici lineari ed esempi classici di codici lineari.

Programma esteso

Richiami di base di aritmetica. Teorema fondamentale dell'aritmetica. Scomposizione in fattori primi. Algoritmo Euclideo delle divisioni successive per il calcolo del massimo comune divisore tra tue interi. Studio dei tempi di calcolo di questo algoritmo.

Richiami sulle relazioni di equivalenza. Congruenze modulo n. Insieme quoziente Z/nZ. Operazioni su un insieme numerico, strutture algebriche.

Strutture algebriche: gruppi e anelli. Gruppi di permutazioni: numero di permutazioni e proprieta' fondamentali del gruppo simmetrico.

Struttura di Z/nZ . Congruenze lineari. Teorema cinese del resto. Funzione phi di Eulero e il suo uso in problemi di fattorizzazione.

Teorema di Eulero generalizzato. Descrizione del sistema crittografico RSA. Test di primalita'.

Campi finiti: Z_p con p un numero primo. Anello dei polinomi su un campo. Costruzione dei campi finiti a partire dall'anello dei polinomi.

Introduzione ai codici correttori di errore e ai codici lineari.

Prerequisiti

Sono necessarie le conoscenze matematiche della scuola media superiore e i contenuti del corso di Fondamenti dell'Informatica.

Modalità didattica

Lezioni frontali, esercitazioni, studio individuale supportato da materiali didattici in e-learning. Il corso e' erogato in italiano. Nel periodo di **emergenza Covid-19** le lezioni si svolgeranno completamente da remoto sincrono e asincrono con alcuni eventi in presenza fisica.

Materiale didattico

Note del corso disponibili sulla piattaforma e-learning.

Testi di riferimento:

Elementi di Matematica Discreta e Algebra Lineare, Francesca Dalla Volta e Marco Rigoli, Pearson Education.

A Course in Number Theory and Cryptography, Neal Koblinz, Springer Verlag.

Periodo di erogazione dell'insegnamento

Primo semestre.

Modalità di verifica del profitto e valutazione

Esame scritto.

L'esame scritto consiste in

a) domande a risposta aperta di ragionamento e deduzione
b) nella risoluzione di esercizi che richiedono calcolo o sviluppo di una soluzione ad un problema assegnato.

Prove parziali

Sono previste verifiche parziali a meta' corso e a fine corso che consistono in

a) domande a risposta aperta di ragionamento e deduzione

b) nella risoluzione di esercizi che richiedono calcolo o sviluppo di una soluzione a un problema dato.

Il superamento delle prove parziali sostituisce l'esame scritto.

Esame orale: facoltativo

Nel periodo di **emergenza Covid-19** gli esami orali saranno solo telematici. Verranno svolti utilizzando la piattaforma WebEx e nella pagina e-learning dell'insegnamento verrà riportato un link pubblico per l'accesso all'esame di possibili spettatori virtuali.

Valutazione: voto finale

Orario di ricevimento

Su appuntamento.