UNIVERSITÀ
DEGLI STUDI DI MILANO-BICOCCA

SYLLABUS DEL CORSO

Metodi Algebrici per l'Informatica

2526-2-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 autocorrezione di errore, e i fondamenti che vengono utilizzate per garantire la sicurezza dei piu' diffusi sistemi crittografici moderni.

1. Conoscenza e capacità di comprensione
   Al termine del corso, lo studente avrà acquisito una comprensione di base della matematica discreta, con particolare riferimento a: aritmetica modulare, congruenze, classi di resto, elementi introduttivi di teoria dei gruppi,
   nozioni fondamentali di crittografia classica e teoria dei codici correttori d'errore.

2. Capacità di applicare conoscenza e comprensione
   Lo studente sarà in grado di applicare i concetti e le tecniche apprese per risolvere problemi concreti e formulare soluzioni in ambiti legati all'informatica, come la sicurezza dei dati e la trasmissione affidabile delle informazioni.

3. Autonomia di giudizio
   Lo studente svilupperà la capacità di ragionare in modo critico e autonomo sui concetti teorici appresi, analizzando la correttezza e l'efficacia di metodi matematici in contesti informatici.

4. Abilità comunicative
   Lo studente sarà in grado di esporre in modo chiaro e rigoroso i concetti matematici studiati, utilizzando il linguaggio simbolico e tecnico appropriato, sia in forma scritta che orale.

5. Capacità di apprendere
   Lo studente acquisirà strumenti logico-matematici che gli permetteranno di affrontare autonomamente l'apprendimento di contenuti più avanzati nell'ambito della matematica e dell'informatica teorica.

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. Codici ciclici. Breve Introduzione ad alcuni sistemi CAS (Computer Algebra System) e.g. Magma, GAP, gp/pari o Sagemath.

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. Sottogruppi normali, ideali di un anello, morfismi. 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: F_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.
Le attività previste sono: 48 ore di lezione frontale in modalità erogativa e 20 ore di esercitazione frontale in modalità erogativa.

Materiale didattico

Note del corso disponibili sulla piattaforma e-learning.
Testi di riferimento:
Childs, Lindsay N. "A concrete introduction to higher algebra. Second edition". Undergraduate Texts in Mathematics. Springer-Verlag, New York, 1995.
Koblitz, Neal "A course in number theory and cryptography". Graduate Texts in Mathematics, 114. Springer-Verlag,

New York, 1987.
Craven, David "Computing with Magma", https://web.mat.bham.ac.uk/D.A.Craven/docs/lectures/magma.pdf

Periodo di erogazione dell'insegnamento

Primo semestre.

Modalità di verifica del profitto e valutazione

L'accesso all'esame scritto richiede il superamento di una prova informatizzata.

Per accedere a tale prova e' necessario iscriversi al portale di WIMS https://wims.matapp.unimib.it/
Su tale portale sono disponibili 10 test di autovalutazione (uno per settimana di corso) che verranno gradualmente attivati.

Siete caldamente esortati a risolverli poiche' parte dell'esame consistera' in esercizi selezionati tra quelli dei test.
Non si effettueranno prove in itinere.

Al termine del corso verra' attribuito un bonus di xx punti se conseguito un punteggio yy ove

- xx=2 per 27<yy?30;
- xx=1.5 per 22<yy?27;
- xx=1 per 18?yy<22.

Il bonus resta valido fino all'inizio del corso dell'anno successivo.

L'esame è suddiviso in cinque fasi:

1. Test a scelta multipla per accertarsi che i concetti base siano stati acquisiti. Qui viene valutata l'esattezza delle risposte (max. 10 punti)
2. Se sufficiente tale test dà accesso alla prova scritta consistente nella risoluzione di alcuni esercizi di routine (max. 10 punti)
3. Assegnazione di un esercizio in cui si valuta la capacita' di rielaborare ed utilizzare la teoria ai fini del problem-solving (max. 6 punti)
4. Richiesta di delineare uno dei Teoremi cardine del corso fornendo cenni di dimostrazione ed esempi (max. 4 punti)
5. Prova orale richiede l'esposizione di asserti e dimostrazioni di teoremi, le definizioni, gli esempi/controesempi e le tecniche di calcolo.
   E' obbligatoria per chi consegue nelle precedenti fasi un punteggio inferiore a 21, facoltativa altrimenti;
   a chi consegue voto >= 27 e non sostiene l'orale verrà verbalizzato 27.

Non viene attribuito a priori nessun peso relativo alla prova orale rispetto alle precedenti prove.

Le prime due fasi vengono svolte accedendo alla piattaforma WIMS https://wims.matapp.unimib.it/

Orario di ricevimento

Su appuntamento.

Sustainable Development Goals

ISTRUZIONE DI QUALITÁ