

Fonaments de matemàtica discreta

Codi	Tipus	Curs/Semestre	Crèdits
24969	Troncal Semestral	Primer / Segon	4,5

Objectius

Competències específiques

Coneixements

Aquesta assignatura està organitzada en tres parts:

1. Aritmètica.
2. L'anell de polinomis.
3. Cossos finits.

Els objectius per a cada una de les parts són els següents:

1. Aprendre les propietats de la divisibilitat dels nombres enters i com aquestes es poden aplicar a la criptografia.
2. Entendre les propietats de la divisibilitat a l'anell de polinomis sobre un cos.
3. Comprendre com són tots els cossos finits i com es calcula en ells. A més, un altre objectiu és que l'alumne aprengui alguna aplicació dels cossos finits a la teoria de la codificació.

Habilitats

Les habilitats que s'aniran desenvolupant al llarg de l'assignatura són:

- Saber calcular el m.c.d. i els coeficients de la identitat de Bézout en els enters i els polinomis.
- Saber resoldre equacions diofàntiques lineals i sistemes de congruències d'enters.
- Conèixer la base teòrica del criptosistema RSA.
- Saber resoldre problemes d'àlgebra lineal sobre cossos finits.

Competències genèriques

Les competències generals de la titulació que es pretén desenvolupar en aquesta assignatura són les següent:

- Capacitat d'anàlisi i síntesi.
- Comunicació oral i escrita.
- Resolució de problemes.
- Raonament crític.

Capacitats prèvies

És convenient que l'alumne tingui coneixements d'àlgebra lineal per a la tercera part del curs. Aquests coneixements es poden aprendre a l'assignatura d'àlgebra lineal del primer semestre de primer curs.

Continguts

Aritmètica	
<ol style="list-style-type: none"> 1. Anells. L'anell dels enters. 2. Divisió entera. 3. Màxim comú divisor. Algorisme d'Euclides. 4. Identitat de Bézout. Equacions diofàntiques lineals. 5. Nombres primers. 6. Congruències. 7. Aritmètica modular. L'anell Z_m 8. Teorema xinès de les restes. 9. Funció multiplicativa d'Euler. Teorema de Fermat i teorema d'Euler. 10. L'algorisme d'elevar i multiplicar. 11. Aplicació a la criptografia: criptografia RSA. 	
L'anell de polinomis	
<ol style="list-style-type: none"> 1. Divisió de polinomis. 2. Màxim comú divisor. Algorisme d'Euclides. Ident. de Bézout. 3. Polinomis irreductibles. 4. Zeros de polinomis. 5. Congruències mòdul un polinomi. 6. Els anells $K[x]/(m(x))$. 	
Cossos finits	
<ol style="list-style-type: none"> 1. Construcció explícita de cossos finits. 2. Característica i cos primer. Cardinal d'un cos finit. 3. Ordre d'un element. Elements primitius en un cos finit. 4. Representació vectorial i potencial dels elements d'un cos finit. 5. Polinomis mínims, polinomis primitius. 6. Descomposició $x^n - x$ en factors 7. Aplicació a la codificació: codis BCH. 	

Metodologia docent

La metodologia docent d'aquesta assignatura es basa en les classes magistrals on el professor exposa la teoria de l'assignatura acompanyada de la realització d'exercicis d'exemple. A més a més, hi ha també les classes de problemes en les que el professor resoldrà alguns problemes i ajudarà als alumnes a superar els dubtes que puguin tenir a l'hora de resoldre'ls. La llista dels problemes estarà penjada al Campus Virtual, que també s'usarà per mantenir informats als alumnes sobre dates de lliurament de problemes, examen parcial, i també

per subministrar als alumnes materials complementaris d'estudi.

Avaluació

1a convocatòria (febrer/juny)		2a convocatòria (juliol/setembre)
Avaluació en grups	Avaluació individual	
L'avaluació d'aquesta assignatura es realitza de forma individual.	<p>L'avaluació continuada consta de:</p> <ul style="list-style-type: none"> • Lliurament de problemes i una entrevista. Compta un 10% en la nota final. • Examen parcial sobre el primer tema. Compta un 30% de la nota final. En cas d'aprovar, elimina matèria de l'examen final. <p>A part de l'avaluació continuada s'haurà de realitzar l'examen final que tindrà una valoració del 60% de la nota final.</p>	La segona convocatòria de l'assignatura s'avaluarà únicament amb un examen de tota la matèria.

Bibliografia bàsica

- J.M. BASART, J. RIFÀ, M. VILLANUEVA (1997). Fonaments de matemàtica discreta. Elements de combinatòria i d'aritmètica. Col.lecció Materials de la UAB, n. 36, ISBN 84-490-0855-7.

Bibliografia complementària

- N.L. BIGGS (1985). Discrete Mathematics. Oxford University Press, ISBN 0-19-853426-4. (Edició en castellà: Matemàtica Discreta. Vicens Vives, 1994.)
- L. CHILDS (1992). A Concrete Introduction to Higher Algebra. UTM, Springer-Verlag, ISBN 0-387-90333-X.
- J. RIFÀ, L. HUGUET (1991). Comunicación digital. Masson, ISBN 84-311-0576-3.

Enllaços

<http://defalla.upc.es/~crsd/>

<http://www.utm.edu/research/primes/>

<http://primes.utm.edu/curios/includes/file.php?file=primetest.html>

Wiris, la teva calculadora

The prime page

A Primality test