

Aritmètica

Codi: 100113
Crèdits: 6

Titulació	Tipus	Curs	Semestre
2500149 Matemàtiques	OT	4	0

Professor de contacte

Nom: Francesc Xavier Xarles Ribas

Correu electrònic: Xavier.Xarles@uab.cat

Utilització d'idiomes a l'assignatura

Llengua vehicular majoritària: català (cat)

Grup íntegre en anglès: No

Grup íntegre en català: Sí

Grup íntegre en espanyol: No

Equip docent

Marc Masdeu Sabate

Prerequisits

És recomanable haver cursat totes les assignatures obligatòries d'àlgebra; concretament, per tal que un alumne pugui superar l'assignatura serà imprescindible tenir assumits els coneixements propis de l'assignatura Estructures Algebraiques.

Objectius

L'assignatura té com a objectiu ser un introducció als problemes aritmètics i, a la vegada, oferir una visió dels mètodes que intervenen en l'anàlisi i resolució d'aquests problemes. Donat que hi ha massa tipus de problemes en teoria de nombres com per a ser coberts en un curs d'aquestes característiques, el curs es basa principalment en els problemes diofàntics, i s'introdueixen a partir d'aquests la teoria algebraica de nombres en el sentit clàssic.

El curs es divideix en tres parts: divisibilitat, restes quadràtics, cossos p -àdics. El nexa que els uneix és la resolució d'equacions diofàntiques i l'estudi dels nombres primers.

En la primera part estudiarem resultats bàsics de nombres primers, factorització i congruències.

L'objectiu principal de la segona part és la llei de reciprocitat quadràtica, després d'una introducció a les equacions diofàntiques.

En la tercera part introduïrem els nombres p -àdics des de diferents punts de vista. També parlarem de cossos no arquimedians més generals.

Durant tot el curs s'intentarà posar l'èmfasi també en les aplicacions a la criptografia dels resultats obtinguts. També s'introduiran les eines informàtiques que permeten resoldre molts d'aquests problemes: per exemple SAGE, PARI, MAPLE i MAGMA.

Competències

- Demostrar de forma activa una elevada preocupació per la qualitat en el moment d'argumentar o exposar les conclusions dels seus treballs
- Desenvolupar un pensament i un raonament crític i saber comunicar-ho de manera efectiva, tant en les llengües pròpies com en una tercera llengua
- Que els estudiants hagin desenvolupat les habilitats d'aprenentatge necessàries per a emprendre estudis posteriors amb un alt grau d'autonomia.
- Que els estudiants tinguin la capacitat de reunir i interpretar dades rellevants (normalment dins de la seva àrea d'estudi) per emetre judicis que incloguin una reflexió sobre temes rellevants d'índole social, científica o ètica.
- Utilitzar eficaçment bibliografia i recursos electrònics per obtenir informació

Resultats d'aprenentatge

1. Demostrar de forma activa una elevada preocupació per la qualitat en el moment d'argumentar o exposar les conclusions dels seus treballs
2. Desenvolupar un pensament i un raonament crític i saber comunicar-ho de manera efectiva, tant en les llengües pròpies com en una tercera llengua
3. Que els estudiants hagin desenvolupat les habilitats d'aprenentatge necessàries per a emprendre estudis posteriors amb un alt grau d'autonomia.
4. Que els estudiants tinguin la capacitat de reunir i interpretar dades rellevants (normalment dins de la seva àrea d'estudi) per emetre judicis que incloguin una reflexió sobre temes rellevants d'índole social, científica o ètica.
5. Utilitzar eficaçment bibliografia i recursos electrònics per obtenir informació

Continguts

Programa

1. Primers

- (a) Com trobar nombres primers grans?
- (b) Alguns resultats de cossos finits.
- (c) Tests de primalitat.
- (d) Factorització.

2. Teoria de congruències.

- (a) Equacions diofàntiques de grau 2.
- (b) Teorema dels restes.
- (c) Solucions projectives d'equacions mòdul n .
- (d) Restes quadràtics i símbol de Legendre.
- (e) La llei de reciprocitat quadràtica.
- (f) Aplicacions criptogràfiques.

2. Cossos p -àdics.

- (a) Solucions mòdul p versus solucions mòdul p .
- (b) Enters p -àdics
- (c) Topologia p -àdica i valoracions.
- (d) Resolució d'equacions en els p -àdics.
- (e) El principi de Hasse, i el símbol de Hilbert.
- (f) Series de potències i convergència.

Metodologia

Aquesta assignatura té dues hores setmanals de teoria. Encara que no s'ha fixat prèviament un conjunt d'apunts, hi ha una varietat interessant de referències bibliogràfiques; en certs moments del curs caldrà

completar el contingut de les explicacions de classe amb consultes a bibliografia o a material proporcionat pel professor.

Hi haurà sessions dedicades a resoldre problemes. Cada alumne haurà de presentar un dels problemes de la llista resolt, per escrit i entregat al professor. Els dubtes que sorgeixin es poden preguntar durant la classe o a les hores de consulta dels professors. El treball sobre aquests problemes es recolza en els conceptes introduïts a classe de teoria, els enuncis dels teoremes, i les seves demostracions, ja que molt sovint les tècniques seran semblants.

En els seminaris es practicarà l'ús de SAGE per a resoldre un projecte.

A més, l'assignatura disposa d'una pàgina al "campus virtual" on s'aniran penjant les llistes de problemes, material addicional i qualsevol informació relacionada amb l'assignatura.

Activitats formatives

Títol	Hores	ECTS	Resultats d'aprenentatge
Tipus: Dirigides			
Classes de Teoria	30	1,2	1, 2, 3, 4
Tipus: Supervisades			
Classes de Problemes	14	0,56	1, 2, 3, 5
Pràctiques	6	0,24	2, 5
Tipus: Autònomes			
Estudi de la teoria	37	1,48	1, 4, 5
Realització de problemes i pràctiques d'ordinador	60	2,4	1, 2, 3, 4, 5

Avaluació

Durant el curs s'hauran d'entregar algun problema comú i un d'individualitzat, que contarán un 50% (40%+10%) de la nota final. El estudiant haurà de fer un programa d'ordinador en SAGE que apliqui alguna tècnica explicada a classe, d'entre una serie de propostes fetes al primer més de començar el curs, valen el 20% de la nota. La resta de la nota (30%) s'obtindrà d'un examen final on s'haurà de resoldre algun problema amb uns quants apartats.

Activitats d'avaluació

Títol	Pes	Hores	ECTS	Resultats d'aprenentatge
Entrega de Problemes	50%	0	0	1, 2, 3, 4, 5
Examen	30%	3	0,12	1, 2
Treball o Programa	20%	0	0	1, 2, 3, 4, 5

Bibliografia

Principal

Richard Crandall and Carl B. Pomerance, Prime Numbers: A Computational Perspective 2nd Edition, Springer-Verlag New York

J.-P. Serre Cours d'Arithmétique, Presses universitaires de France, Dunod, Paris, 1967.

F. Gouvêa, p-adic Numbers: an introduction Springer-Verlag, Berlin, 1997.

N.Koblitz, A Course in Number Theory and Cryptography', GTM114, Springer, 1994.

Complementaria

P. Samuel, Teoría algebraica de los números, Ediciones Omega, 1972.

I.N. Stewart, D.O. Tall, Algebraic Number Theory, Chapman and Hall, 1979.

Z.I. Borevich y I.R. Shafarevich, Number Theory, Academic Press, 1966.

J. Cilleruelo, A. Cordoba. La teoría de los numeros. Editorial Mondadori, 1992.

L.J. Mordell, Diophantine Equations Academic Press, 1969.

J. Neukirch, Algebraic number theory Springer-Verlag 1999.