Universitat Autònoma de Barcelona

2020/2021

Aritmètica

Codi: 100113
Crèdits: 6

Titulació	Tipus	Curs	Semestre
2500149 Matemàtiques	OT	4	0

La metodologia docent i l'avaluació proposades a la guia poden experimentar alguna modificació en funció de les restriccions a la presencialitat que imposin les autoritats sanitàries.

Professor/a de contacte

Nom: Marc Masdeu Sabate

Correu electrònic: Marc.Masdeu@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

Altres indicacions sobre les llengües

Part de la bibliografia pot ser en anglès

Equip docent

Francesc Xavier Xarles Ribas

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 una 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'introdueix a partir d'aquests la teoria algebraica de nombres i la geometria aritmètica.

El curs es divideix en quatre parts: (I) Congruències i divisibilitat; (II) Corbes el·líptiques; (III) Llei de reciprocitat quadràtica; i (IV) Primalitat i factorització. El nexe d'unió de les quatre parts, i que pot servir de motivació encara que no sigui l'objectiu del curs, és l'aplicació que d'ells se n'ha fet a la criptografia.

En la primera part estudiarem resultats bàsics de congruències, i veurem les primeres aplicacions a la criptografia.

La segona part ladedicarem a les corbes el·líptiques, emfatitzant les aplicacions que s'ha fet a la factorització i

a la criptografia.

En la tercera part introduirem la llei de reciprocitat quadràtica i les seves conseqüències.

La quarta part està dedicada a l'estudi d'algoritmes per determinar la primalitat d'enters, i per trobar factors no trivials d'enters compostos.

Contràriament al que alguns podrien creure, la teoria de nombres és una de les branques de les matemàtiques que més s'assembla a les ciències experimentals: el seu principal objecte d'estudi és una cosa tan concreta com els nombres, que coneixem i fem servir a diari. És per això que l'experimentació és un tret bàsic de la teoria de nombres, i això es reflecteix en el curs mitjançant l'ús d'eines informàtiques (principalment Sage) que permeten descobrir, entendre i resoldre molts fenòmens aritmètics.

Competències

- Assimilar la definició d'objectes matemàtics nous, de relacionar-los amb altres coneguts i de deduir les seves propietats
- Demostrar de forma activa una elevada preocupació per la qualitat en el moment d'argumentar o exposar les conclusions dels seus treballs
- Demostrar una elevada capacitat d'abstracció.
- 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 puguin transmetre información idees, problemes i solucions a un públic tan especialitzat com no especialitzat
- Que els estudiants sàpiguen aplicar els seus coneixements al seu treball o vocació d'una forma professional i posseeixin les competències que solen demostrar-se per mitjà de l'elaboració i defensa d'arguments i la resolució de problemes dins de la seva àrea d'estudi.
- 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. Conèixer demostracions rigoroses d'alguns teoremes d'àlgebra avançada i assimilar la definició de noves estructures i construccions algebraiques, de relacionar-los amb altres coneguts i deduir les seves propietats.
2. Demostrar de forma activa una elevada preocupació per la qualitat en el moment d'argumentar o exposar les conclusions dels seus treballs
3. Desenvolupar un pensament i un raonament crític i saber comunicar-ho de manera efectiva, tant en les llengües pròpies com en una tercera llengua
4. Que els estudiants hagin desenvolupat les habilitats d'aprenentatge necessàries per a emprendre estudis posteriors amb un alt grau d'autonomia.
5. Que els estudiants puguin transmetre información idees, problemes i solucions a un públic tan especialitzat com no especialitzat
6. Que els estudiants sàpiguen aplicar els seus coneixements al seu treball o vocació d'una forma professional i posseeixin les competències que solen demostrar-se per mitjà de l'elaboració i defensa d'arguments i la resolució de problemes dins de la seva àrea d'estudi.
7. 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.
8. Utilitzar eficaçment bibliografia i recursos electrònics per obtenir informació.
9. Utilitzar les eines algebraiques en diferents àmbits

Continguts

I. Primers i congruències

- Divisibilitat
- Factorització d'enters
- Els enters mòdul n
- Mètodes efectius per inversos i exponenciació
- Diffie-Hellman i RSA

II. Corbes el·líptiques

- Definició i llei de grup
- Punts de torsió, punts racionals
- Corbes sobre cossos finits
- Criptografia amb corbes el·líptiques
- Comptatge de punts

III. La llei de reciprocitat quadràtica

- Residus quadràtics i el símbol de Legendre
- LRQ i demostració
- El símbol de Jacobi
- Aplicació: arrels quadrades mòdul p

IV. Primalitat i factorització

- Primalitat
- Algoritmes de factorització
- Rho de Pollard
- Bases de factors
- Fraccions continuades
- Algoritmes pel logaritme discret

Metodologia

Aquesta assignatura té dues hores setmanals de teoria. A més dels apunts del curs, en certs moments 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 enunciats 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	2, 3, 4, 7

Tipus: Supervisades			
Classes de Problemes	14	0,56	2, 3, 4, 8
Pràctiques	6	0,24	3, 8
Tipus: Autònomes			
Estudi de la teoria	37	1,48	2, 7, 8
Realització de problemes i pràctiques d'ordinador	60	2,4	2, 3, 4, 7, 8

Avaluació

Durant el curs s'hauran d'entregar algun problema, que comptarà un 25% de la nota final. L'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 mes de començar el curs, i que valdrà el 20% de la nota. Es farà també un treball i/o presentació oral, que contribuirà un 25% 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.

Només es podrà recuperar l'examen final i/o el programa, sempre i quan la nota en cada part a recuperar hagi superat el 3,5 sobre 10. És important remarcar que, en cas de presentar-se a millorar nota, l'estudiant renuncia a la nota prèvia.

Activitats d'avaluació

Títol	Pes	Hores	ECTS	Resultats d'aprenentatge
Entrega de problemes	25%	0	0	2, 3, 4, 6, 7, 8
Examen final	30%	3	0,12	1, 2, 3
Presentació oral	25%	0	0	2, 3, 4, 5, 7, 8
Programa	20%	0	0	2, 3, 4, 7, 8, 9

Bibliografia

Principal

W. Stein, Elementary Number Theory: Primes, Congruences, and Secrets, Springer-Verlag, Berlin, 2008.

J.-P. Serre, *A Course in Arithmetic,* GTM7, Springer, 1973.

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

Complementària

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.

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

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