

Aritmètica**2012/2013**

Codi: 100113

Crèdits ECTS: 6

Titulació	Pla	Tipus	Curs	Semestre
2500149 Graduat en Matemàtiques	777 Graduat en Matemàtiques	OT	0	0

Professor de contacte

Nom: Francesc Bars Cortina

Correu electrònic: Francesc.Bars@uab.cat

Utilització d'idiomes

Llengua vehicular majoritària: català (cat)

Algun grup íntegre en anglès: No

Algun grup íntegre en català: Sí

Algun grup íntegre en espanyol: No

Prerequisits

Coneixements que ja s'han vist durant la titulació d'Anàlisi, Àlgebra i Geometria i Topologia.

Objectius

Aritmètica té els seus orígens amb l'inici de la humanitat. És molt conegut les ternes pitagòriques per exemple.

Un podria pensar en aritmètica com una assignatura poc profunda i la realitat és tot el contrari. Karl Friedrich Gauss va transformar l'aritmètica amb el que avui

es coneix com "Teoria de Nombres" i va excriure que aquesta disciplina és la reina de les matemàtiques. Per tant el contingut del curs es fonamenta en justificar

i que veieu el motiu per què aritmètica o teoria de nombres és la reina de les matemàtiques. Explicitar també que l'Aritmètica també es clau per aplicacions en criptografia, per exemple

el sistema de clau pública potser més interessant en l'actualitat és usant corbes el·líptiques, on en el passaport alemà està implementat, el mètode més simple de clau pública, però usat

enormement encara és el RSA.

Els problemes en Aritmètica són senzills d'enunciat, però per resoldre'ls cal usar totes les rames de la matemàtica fonamental, és dir Àlgebra, Anàlisi i Geometria i Topologia.

Aquest curs tractarem diversos aspectes i per exemple esperem fer un petit esboç de les idees de Kummer per a poder atacar parcialment el últim teorema de Fermat al final del s.XIX,

recordeu que l'últim teorema de Fermat ha estat demostrat

per Andrew Wiles (1995) amb tècniques molt més sofisticades que segurament ni comentarem. Per tant en el curs aprofundirem fortament els continguts 3(a) i 3(b) dels continguts del curs

on hi ha part de la base necessària d'Àlgebra per a transformar Aritmètica en "la reina de la Matemàtiques".

L'objectiu del curs consistirà doncs en relacionar qüestions d'Aritmètica amb Àlgebra, Geometria, Topologia i Anàlisi, (i en la part d'anàlisi, potser explicitem l'enfoc de Manin respecte si la

física és adèlica o no).

Els continguts del temari són grans línies (on algun subapartat dóna per un curs sencer), per tant molts d'ells no es faran o tan sols es comentaran en forma d'exposició divulgativa.

Competències

- Demostrar de forma activa una elevada preocupació per la qualitat en el moment d'argumentar o exposar les conclusions dels seus treballs
- Assimilar la definició d'objectes matemàtics nous, de relacionar-los amb altres coneguts i de deduir les seves propietats
- Demostrar una elevada capacitat d'abstracció.
- Hauran desenvolupat aquelles habilitats d'aprenentatge necessàries per emprendre estudis posteriors amb un alt grau d'autonomia
- Identificar les idees essencials de les demostracions d'alguns teoremes bàsics i saber-les adaptar per obtenir altres resultats
- Seran capaços de transmetre coneixements, procediments, resultats i idees matemàtiques.
- Utilitzar eficaçment bibliografia i recursos electrònics per obtenir informació

Resultats d'aprenentatge

1. Conocer demostraciones rigurosas de algunos teoremas de álgebra avanzada y asimilar la definición de nuevas estructuras y construcciones algebraicas, de relacionarlos con otros conocidos y deducir sus propiedades.
2. Utilizar las herramientas algebraicas en distintos ámbitos

Continguts

1. Introducció a l'Aritmètica.

(a) Els inicis i planteig d'equacions diofantines. Equació de Pell, equació de Fermat,...

(b) Ternes pitagòriques. Resolució d'equacions diofantines quadràtiques.

(c) Perquè els canvis de variable trigonomètrics per fer integració? Parametritzem un projectiu!!! esteu fent geometria i teoria

de cossos!

(d) Alguns tècniques bàsiques amb equacions diofantines als enters, resolució mòdul p . Criptografia bàsica: RSA.

2. Anàlisi als nombres racionals.

(a) Us han enganyat? Als nombres racionals, $\mathbb{Q}$, hi ha un nombre infinit de valors absoluts no equivalents, i per tant diferents anàlisis

i la completació de $\mathbb{Q}$ per aquests nous valors absoluts no és $\mathbb{R}$ és un altre cos complet molt diferent, els cossos p -àdics. Inmersions de cossos de nombres: les valoracions arquimedianes.

(b) Anells de valoració discreta i completacions. Filtracions i definir una topologia en objectes algebraics.

(c) Aplicacions a l'Aritmètica: el principi de Hasse.

(d) La física és adèlica? Física usant anàlisi no arquimediana. (Recordeu que a la carrera sol veieu anàlisi arquimedià).

3. Aritmètica i Geometria.

(a) Anells de Dedekind. Topologies no equivalents en un anell de Dedekind: valoracions arquimedianes i no-arquimedianes.

(Un exemple bàsic és $\mathbb{Z}$ i relaciona amb 2(a)). Aplicació: idees de Kummer per atacar l'últim teorema de Fermat.

(b) Llenguatge en termes de geometria en busca solucions d'equacions diofantines. Teorema dels zeros de Hilbert.

(c) El gènere d'una corba algebraica. El Teorema de Faltings.

(d) Corbes el·líptiques (corbes de gènere 1 amb un punt). Aplicacions a criptografia.

(e) Galois i cohomologia. Una aplicació: en busca de trobar una obstrucció més fina quant el principi de Hasse no ens funciona.

(f) Representacions de grups de Galois, modularitat i el teorema de Wiles per la demostració del teorema de Fermat.

Metodologia

En les classes de teoria s'exposarà la matèria i en les classes de problemes es treballaran usualment exercicis que exemplifiquen els continguts teòrics. Potser en alguna classe de problemes es podrà exposar algun tema que ha treballat alguns alumnes en tota la classe.

Activitats formatives

Títol	Hores	ECTS	Resultats d'aprenentatge
Tipus: Dirigides			
Classes teoria	30	1,2	1, 2
Resolució de problemes	35	1,4	1, 2
Tipus: Supervisades			
Una línia de treball per treball individual de l'assignatura.	30	1,2	1, 2
Tipus: Autònomes			
Preparació de treballs senzills	18	0,72	1, 2
Resolució de problemes	35	1,4	1, 2

Avaluació

Durant el curs s'hauran d'entregar de forma individual dos problemes comuns (es dir el mateix problema per tota la classe) que contarán un màxim del 6 punts sobre 10 de la nota final del curs, aquest valor s'obtindrà si l'alumne asisteix usualment a les classes de teoria i problemes i fa correctament els dos problemes. També els alumnes que assisteixen a classe poden fer un breu treball (màxim 4 fulles) que compta fins 2 punts sobre 10 de l'assignatura, aquest treball consistirà en explicar un resultat no fet directament a classe (aquest treball pot fer-se en grups de com a molt 2 persones).

Un alumne que tingui una nota superior o igual a 5 ja aprova l'assignatura i a l'expedient li constarà aquella

nota.

Als alumnes que aprovin i vulguin millorar la nota (dels dos punts sobre 10 que falten) hauran de parlar amb el professor

de teoria durant el curs per tal que els hi possi un treball que hauran de presentar davant el professor a final de curs de forma individualitzada o fer un examen final de l'assignatura.

Els alumnes que no assisteixin a classe (o no aprovin amb l'entrega individual de dos problemes comuns i el treball de 4 fulles, que espero que aquest cas sigui el conjunt buit) hauran de fer un examen final que contarà el 100 % de la nota del curs.

Activitats d'avaluació

Títol	Pes	Hores	ECTS	Resultats d'aprenentatge
Entrega exercicis	60%	0	0	1
Entrega treball	20%	1	0,04	1, 2
Examen/Treball individual i exposició	20%	1	0,04	1, 2

Bibliografia

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

-D.Lorenzini "An invitation to Arithmetic Geometry".

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

-J. Neukirch "Algebraic Number Theory", Springer, 1999.

-J.P.Serre "A Course in Arithmetic", GTM 7, Springer, 1966.