

**Aritmètica**

Codi: 100113  
Crèdits: 6

Titulació	Tipus	Curs	Semestre
2500149 Matemàtiques	OT	4	2

**Professor/a de contacte**

Nom: Francesc Bars Cortina

Correu electrònic: francesc.bars@uab.cat

**Idiomes dels grups**

Podeu accedir-hi des d'aquest [enllaç](#). Per consultar l'idioma us caldrà introduir el CODI de l'assignatura. Tingueu en compte que la informació és provisional fins a 30 de novembre de 2023.

**Equip docent**

Eloi Torrents Juste

**Prerequisits**

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

**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) Nocions bàsiques. Còniques i nombres  $p$ -àdics; (II) Corbes el·líptiques (III) Teoria de Nombres Algebraica; (IV) Una introducció a la geometria aritmètica. El nexa d'unió de les quatre parts, és la diferent resolució d'equacions diofantines que son varietats topològiques amb el seu gènere.

En la primera part estudiarem còniques, i veurem l'anàlisi  $p$ -àdic, corresponent a valors absoluts als racionals on està acotat els valor absolut en els enters.

La segona part l'adedicarem a les corbes el·líptiques, treballant l'estructura de grup dels seus punts en aritmètica.

En la tercera part introduïrem anells dins cossos, tal que es pot fer un estudi dels seus ideals primers (o valors absoluts) via una extensió finita de Galois.

La quarta part està dedicada a l'estudi de cossos de transcendència 1 sobre un cos i la seva interrelació amb l'estudi de corbes, corresponent a anells dins cossos estudiat en el capítol anterior.

## 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 informació 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 algebraïques, 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 informació 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 algebraïques en diferents àmbits

## Continguts

I. Còniques i nombres  $\mathbb{p}$ -àdics

- Còniques i llei de residu quadràtic. Nombres p-àdics. Punts racionals
- Anàlisi no arquimedià. Completació de cossos.

## II. Corbes el·líptiques

- Definició i llei de grup
- Punts de torsió, punts racionals
- Teorema de Mordell.

## III. Teoria de Nombres Algebraica

- Dominis de Dedekind.
- El grup de classes d'un cos.
- Kummer atacant l'últim teorema de Fermat.

## IV. Una pinzellada a Geometria Aritmètica.

\*Corbes planes no-singulars

\*Punts i valors absoluts no-arquimedians.

\*Dominis de Dedekind i no-singularitat.

## 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.

En els seminaris es practicarà una aplicació concreta per resoldre certes equacions diofantines. Hi haurà una entrega de problemes per grups on serà d'algun problema similar als seminaris.

Hi haurà una llista de treballs, on l'alumne pot triar-ne un, o proposar-ne ell pròpiament per realitzar un petit treball sobre aquell tema.

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.

Nota: es reservaran 15 minuts d'una classe, dins del calendari establert pel centre/titulació, per a la complementació per part de l'alumnat de les enquestes d'avaluació de l'actuació del professorat i d'avaluació de l'assignatura/mòdul.

## 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
Realitzaci'o de problemes i treball sobre alguna equaci? diofantina.	60	2,4	2, 3, 4, 7, 8

## Avaluació

Durant el curs s'assignaran exercicis d'una llista diferents que cada alumne pot entregar individualment, que comptarà un 30% de la nota final. També hi haurà un problema específic conjunt on cada alumne haurà de presentar individualment i comptarà un 25 % de la nota del curs.

Cada alumne tindrà assignat un treball d'una llista (però que pot proposar-ne al professor altre, sempre i quant el professor de teoria ho accepti) on haurà de fer una exposició oral amb un vídeo de com a molt 10 minuts, aquest treball correspondrà a un 30% de la nota del curs.

La resta de la nota (15%) s'obtindrà d'un examen final on s'haurà de resoldre alguns problemes amb uns quants apartats.

Només es podrà recuperar l'examen final. És important remarcar que, en cas de presentar-se a millorar nota, l'estudiant renuncia a la nota prèvia.

Un alumne amb avaluació continuada pot renunciar a fer les entregues de problemes i/o treball, comunicant-ho abans al professor de teoria i aquell % aniria a l'examen final de l'assignatura.

Alumnes amb avaluació única d'Aritmètica, i que ho hagin demanat oficialment, faran tan sols l'examen final de l'assignatura directament havent d'obtenir una nota igual o superior a 5 sobre 10 per a poder superar l'assignatura. En cas de no superar, tindrán l'examen de recuperació.

## Activitats d'avaluació continuada

Títol	Pes	Hores	ECTS	Resultats d'aprenentatge
Entrega de problemes	30%	0	0	2, 3, 4, 6, 7, 8
Entrega problema conjunt.	25%	0	0	2, 3, 4, 7, 8, 9
Examen final	15%	3	0,12	1, 2, 3
Treball individual d'un tema no tractat al curs i presentació oral amb un vídeo	30%	0	0	2, 3, 4, 5, 7, 8

## Bibliografia

Principal

K.Kato, N.Kurokawa, T.Saito, Number Theory 1, Fermat's Dram. Translation of Mathematical Monographs, vol. 186, 1996, AMS.

D. Lorenzini. An invitation to Arithmetic Geometry. Graduate Studies in Mathematics, vol 9, 1996, AMS.

#### Complementària

A.R. Omondi. Criptography arithmetic: algorithms and hardware architectures, Advances in Information Security (vol.77), 2020. <https://link.springer.com/book/10.1007/978-3-030-34142-8>

A. Granville, Number Theory Revealed: a Masterclass. AMS, 2019.

S. Lang: Cyclotomic Fields I and II. GTM121, Springer, 1990, ISBN: 0-387-96671-4

A. Lozano-Robledo: Elliptic Curves, modular forms and their L-functions. Student Mathematical Library, vol. 58. AMS (2011).

M.Papikian: Drinfeld modules. Graduate Texts in Mathematics, 296. Springer, Cham, 2023. xxi+526 pp. ISBN: 978-3-031-19706-2

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.

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

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

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

K.Kato, N.Kurokawa, T.Saito, Number Theory 2, introduction to Class Field Theory. Translations of Mathematical Monographs, vol.240, AMS (1998).

N.Kurokawa, M.Kurihara, T.Saito, Number Theory 3, Iwasawa Theory and modular forms. Translations of Mathematical Monographs, vol.242, AMS (2012).

J.J.Silverman, The arithmetic of Elliptic Curves, GTM 106, Springer.

J.J. Silverman, The arithmetic of Dynamical Systems, GTM 241, Springer.

J.J. Silverman, A friendly introduction to Number Theory, Pearson Modern Classics series.

M.Hindry, J.J.Silverman, Diophantine Geometry: an introduction. GTM 201, Springer.

J.Hoffstein, J.Pipher, J.J.Silverman, An introduction to mathematical cryptography, Springer Verlag.

## Programari

L'alumne que ho vulgui pot fer un treball usant un programari matemàtic, i/o complimentar les entregues amb què pot fer un programari matemàtic.

L'alumne podrà usar Sage Math, o Magma online computation. Magma és un programari específic per Àlgebra on hi ha moltes funcions introduïdes, i un programa senzill que duri menys de 2 minuts es pot fer en línia via web de forma gratuïta.