UAB
Universitat Autònoma de Barcelona

Aritmética

Código: 100113
Créditos ECTS: 6

2024/2025

Titulación	Tipo	Curso
2500149 Matemáticas	OT	4

Contacto

Nombre: Francesc Bars Cortina

Correo electrónico: francesc.bars@uab.cat

Idiomas de los grupos

Puede consultar esta información al final del documento.

Prerrequisitos

Es recomendable haber cursado todas las asignaturas obligatorias de álgebra. Concretamente, para que un alumno pueda entender mejor la asignatura es imprescindible tener asumidos los conocimientos propios de las asignaturas Estructuras Algebraicas y Teoría de Galois para extensiones finitas.

Objetivos y contextualización

(de Google Translate)

La asignatura tiene como objetivo ser una introducción a los problemas aritméticos y, a la vez, ofrecer una visión de los métodos que intervienen en el análisis y resolución de estos problemas. Dado que hay demasiados tipos de problemas en teoría de números como para ser cubiertos en un curso de estas características, el curso se basa principalmente en los problemas diofántico, y se introduce a partir de estos la teoría algebraica de números y la geometría aritmética.

El curso se divide en cuatro partes: (I) Congruencias y divisibilidad; (II) Curvas elípticas; (III) Ley de reciprocidad cuadrática; y (IV) primalidad y factorización. El nexo de unión de las cuatro partes, y que puede servir de motivación aunque no sea el objetivo del curso, es la aplicación que de ellos se ha hecho a la criptografía.

En la primera parte estudiaremos resultados básicos de congruencias, y veremos las primeras aplicaciones a la criptografía.

La segunda parte ladedicarem a las curvas elípticas, enfatizando las aplicaciones que se ha hecho a la factorización y la criptografía.

En la tercera parte introduciremos la ley de reciprocidad cuadrática y sus consecuencias.

La cuarta parte está dedicada al estudio de algoritmos para determinar la primalidad de enteros, y para encontrar factores no triviales de enteros compuestos.

Contrariamente a lo que algunos podrían creer, la teoría de números es una de las ramas de las matemáticas que más se parece a las ciencias experimentales: su principal objeto de estudio es algo tan concreto como los

números, que conocemos y usamos a diario. Es por ello que la experimentación es un rasgo básico de la teoría de números, y esto se refleja en el curso mediante el uso de herramientas informáticas (principalmente Sage) que permiten descubrir, entender y resolver muchos fenómenos aritméticos.

Competencias

- Asimilar la definición de objetos matemáticos nuevos, de relacionarlos con otros conocidos y de deducir sus propiedades.
- Demostrar de forma activa una elevada preocupación por la calidad en el momento de argumentar o hacer públicas las conclusiones de sus trabajos.
- Demostrar una elevada capacidad de abstracción.
- Desarrollar un pensamiento y un razonamiento crítico y saber comunicarlo de manera efectiva, tanto en las lenguas propias como en una tercera lengua.
- Que los estudiantes hayan desarrollado aquellas habilidades de aprendizaje necesarias para emprender estudios posteriores con un alto grado de autonomía.
- Que los estudiantes puedan transmitir información, ideas, problemas y soluciones a un público tanto especializado como no especializado.
- Que los estudiantes sepan aplicar sus conocimientos a su trabajo o vocación de una forma profesional y posean las competencias que suelen demostrarse por medio de la elaboración y defensa de argumentos y la resolución de problemas dentro de su área de estudio.
- Que los estudiantes tengan la capacidad de reunir e interpretar datos relevantes (normalmente dentro de su área de estudio) para emitir juicios que incluyan una reflexión sobre temas relevantes de índole social, científica o ética.
- Utilizar eficazmente bibliografía y recursos electrónicos para obtener información.

Resultados de aprendizaje

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. Demostrar de forma activa una elevada preocupación por la calidad en el momento de argumentar o hacer públicas las conclusiones de sus trabajos.
3. Desarrollar un pensamiento y un razonamiento crítico y saber comunicarlo de manera efectiva, tanto en las lenguas propias como en una tercera lengua.
4. Que los estudiantes hayan desarrollado aquellas habilidades de aprendizaje necesarias para emprender estudios posteriores con un alto grado de autonomía.
5. Que los estudiantes puedan transmitir información, ideas, problemas y soluciones a un público tanto especializado como no especializado.
6. Que los estudiantes sepan aplicar sus conocimientos a su trabajo o vocación de una forma profesional y posean las competencias que suelen demostrarse por medio de la elaboración y defensa de argumentos y la resolución de problemas dentro de su área de estudio.
7. Que los estudiantes tengan la capacidad de reunir e interpretar datos relevantes (normalmente dentro de su área de estudio) para emitir juicios que incluyan una reflexión sobre temas relevantes de índole social, científica o ética.
8. Utilizar eficazmente bibliografía y recursos electrónicos para obtener información.
9. Utilizar las herramientas algebraicas en distintos ámbitos.

Contenido

(de Google Translate)

I. Cónicas y números p-adicos Cónicas y ley de residuo cuadrático. Números p-ádicos. Puntos racionales Análisis no arquimediano. Completación de cuerpos.II. Curvas elípticas Definición y ley de grupo Puntos de

torsión, puntos racionales Teorema de Mordell. III. Teoría de Números Algebraica Dominios de Dedekind. El grupo de clases de un cuerpo. Kummer atacando el último teorema de Fermat. IV. Una pincelada en Geometría Aritmética. *Curvas planas no-singulares *Puntos y valores absolutos no-arquimedianos. *Dominios de Dedekind y no-singularidad.

Actividades formativas y Metodología

Título	Horas	ECTS	Resultados de aprendizaje
Tipo: Dirigidas			
Clases de Teoría	30	1,2	2, 3, 4, 7
Tipo: Supervisadas			
Clases de Problemas	14	0,56	2, 3, 4, 8
Prácticas	6	0,24	3, 8
Tipo: Autónomas			
Estudio de la teoría	37	1,48	2, 7, 8
Realizaci?n de problemas y trabajo sobre alguna equaci?n diofantina.	60	2,4	2, 3, 4, 7, 8

(de Google Translate)

Esta asignatura tiene dos horas semanales de teoría. Además de los apuntes del curso, en ciertos momentos será necesario completar el contenido de las explicaciones de clase con consultas a bibliografía o material proporcionado por el profesor. Habrá sesiones dedicadas a resolver problemas. Cada alumno deberá presentar uno de los problemas de la lista resuelta, por escrito y entregado al profesor. Las dudas que surjan pueden preguntarse durante la clase o en las horas de consulta de los profesores. El trabajo sobre estos problemas se apoya en los conceptos introducidos en clase de teoría, los enunciados de los teoremas y sus demostraciones. En los seminarios se practicará una aplicación concreta para resolver ciertas ecuaciones diofantinas. Habrá una entrega de problemas por grupos donde será de algún problema similar a los seminarios. Habrá una lista de trabajos, donde el alumno puede elegir uno, o proponerlo propiamente para realizar un pequeño trabajo sobre ese tema. Además, la asignatura dispone de una página en el "campus virtual" donde se irán colgando las listas de problemas, material adicional y cualquier información relacionada con la asignatura. Nota: se reservarán 15 minutos de una clase, dentro del calendario establecido por el centro/titulación, para que el alumnado rellene las encuestas de evaluación de la actuación del profesorado y de evaluación de la asignatura/módulo.

Nota: se reservarán 15 minutos de una clase dentro del calendario establecido por el centro o por la titulación para que el alumnado rellene las encuestas de evaluación de la actuación del profesorado y de evaluación de la asignatura o módulo.

Evaluación

Actividades de evaluación continuada

	Resultados de

Título	Peso	Horas	ECTS	aprendizaje
Entrega de problemas	30%	0	0	2, 3, 4, 6, 7, 8
Entrega de un problema conjunto.	25%	0	0	2, 3, 4, 7, 8, 9
Examen final	15%	3	0,12	1, 2, 3
Trabajo individual de un trabajo no estudiado y presentación oral con un vídeo	30%	0	0	2, 3, 4, 5, 7, 8

(de Google Translate)

Durante el curso se asignarán ejercicios de una lista diferentes que cada alumno puede entregar individualmente, que contará con un 30% de la nota final. También habrá un problema específico conjunto en el que cada alumno deberá presentar individualmente y contará un 25% de la nota del curso. Cada alumno tendrá asignado un trabajo de una lista (pero que puede proponer al profesor otro, siempre y cuando el profesor de teoría lo acepte) donde deberá realizar una exposición oral con un vídeo de a lo sumo 10 minutos, este trabajo corresponderá a un 30% de la nota del curso. El resto de la nota (15%) se obtendrá de un examen final en el que se deberá resolver algún problema con varios apartados. Sólo podrá recuperarse el examen final. Es importante remarcar que, en caso de presentarse a mejorar nota, el estudiante renuncia a la nota previa. Un alumno puede renunciar a hacer las entregas de problemas y/o trabajo, comunicándolo antes al profesor de teoría y ese % iría al examen final de la asignatura.

Sólo se podrá recuperar el examen final, siempre y cuando la nota en cada parte a recuperar haya superado el 3,5 sobre 10. Es importante destacar que, en caso de presentarse a mejorar nota, el estudiante renuncia a la nota previa.

Alumnos con evaluación única de Aritmética, y que lo hayan solicitado oficialmente, harán tan sólo el examen final de la asignatura directamente debiendo obtener una nota igual o superior a 5 sobre 10 para poder superar la asignatura. En caso de no superarlo, tendrán el examen de recuperación.

Bibliografía

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.

Suplementaria

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

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

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

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

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.

Software

Podría usarse Sagemath (sagemath.org) o bién Magma durante el curso.

Lista de idiomas

Nombre	Grupo	Idioma	Semestre	Turno
(PAUL) Prácticas de aula	1	Catalán	segundo cuatrimestre	manaña-mixto
(SEM) Seminarios	1	Catalán	segundo cuatrimestre	tarde
(TE) Teoría	1	Catalán	segundo cuatrimestre	manaña-mixto