Universitat Autònoma de Barcelona

2019/2020

Aritmética

Código: 100113
Créditos ECTS: 6

Titulación	Tipo	Curso	Semestre
2500149 Matemáticas	OT	4	0

Contacto

Nombre: Marc Masdeu Sabate
Correo electrónico: Marc.Masdeu@uab.cat

Uso de idiomas

Lengua vehicular mayoritaria: catalán (cat)
Algún grupo íntegramente en inglés: No
Algún grupo íntegramente en catalán: Sí
Algún grupo íntegramente en español: No

Otras observaciones sobre los idiomas

La bibliografia es en catalán e inglés

Equipo docente

Francesc Xavier Xarles Ribas

Prerequisitos

Es recomendable haber cursado todas las asignaturas obligatorias de álgebra; concretamente, para que un alumno pueda superar la asignatura será imprescindible tener asumidos los conocimientos propios de la asignatura Estructuras Algebraicas.

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

- Demostrar de forma activa una elevada preocupación por la calidad en el momento de argumentar o hacer públicas las conclusiones de sus trabajos.
- 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 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. Demostrar de forma activa una elevada preocupación por la calidad en el momento de argumentar o hacer públicas las conclusiones de sus trabajos.
2. Desarrollar un pensamiento y un razonamiento crítico y saber comunicarlo de manera efectiva, tanto en las lenguas propias como en una tercera lengua.
3. Que los estudiantes hayan desarrollado aquellas habilidades de aprendizaje necesarias para emprender estudios posteriores con un alto grado de autonomía.
4. 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.
5. Utilizar eficazmente bibliografía y recursos electrónicos para obtener información.

Contenido

(de Google Translate)

I. Primeros y congruencias divisibilidad

- Factorización de enteros
- Los enteros módulo n
- Métodos efectivos para inversos y exponenciación
- Diffie-Hellman y RSA

II. Curvas elípticas

- Definición y ley de grupo
- Puntos de torsión, puntos racionales
- Curvas sobre cuerpos finitos
- Criptografía con curvas elípticas
- Conteo de puntos

III. La ley de reciprocidad cuadrática

- Residuos cuadráticos y el símbolo de Legendre
- LRQ y demostración
- El símbolo de Jacobi
- Aplicación: raíces cuadradas módulo p

IV. Primalidad y factorización

- Primalidad
- Algoritmos de factorización
- Rho de Pollard
- Bases de factores
- Fracciones continuadas
- Algoritmos por logaritmo discreto

Metodología

(de Google Translate)

Esta asignatura tiene dos horas semanales de teoría. Aunque no se ha fijado previamente un conjunto de apuntes, hay una variedad interesante de referencias bibliográficas; en ciertos momentos del curso 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 resuelto, por escrito y entregado al profesor. Las dudas que surjan se pueden preguntar 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, ya que muy a menudo las técnicas serán similares.

En los seminarios se practicará el uso de SAGE para resolver un proyecto.

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.

Actividades

Título	Horas	ECTS	Resultados de aprendizaje
Tipo: Dirigidas			
Clases de Teoría	30	1,2	1, 2, 3, 4
Tipo: Supervisadas			
Clases de Problemas	14	0,56	1, 2, 3, 5
Prácticas	6	0,24	2, 5
Tipo: Autónomas			
Estudio de la teoría	37	1,48	1, 4, 5
Realización de problemas y prácticas de ordenador	60	2,4	1, 2, 3, 4, 5

Evaluación

(de Google Translate)

Durante el curso se deberán entregar algún problema, que contará un 25% de la nota final. El estudiante deberá hacer un programa de ordenador en Sage que aplique alguna técnica explicada en clase, de entre una serie de propuestas hechas al primer mes de empezar el curso, y que valdrá el 20% de la nota. Se hará también un trabajo y / o presentación oral, que contribuirá un 25% de la nota. El resto de la nota (30%) se obtendrá de un examen final donde se deberá resolver algún problema con varios apartados.

Sólo se podrá recuperar el examen final y / o el programa, 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.

Actividades de evaluación

Título	Peso	Horas	ECTS	Resultados de aprendizaje
Entrega de problemas	25%	0	0	1, 2, 3, 4, 5
Examen final	30%	3	0,12	1, 2
Presentación oral	25%	0	0	1, 2, 3, 4, 5
Programa	20%	0	0	1, 2, 3, 4, 5

Bibliografía

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.

Complementaria

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.