FITXA IDENTIFICATIVA

Dades de l'Assignatura

Codi	44085
Nom	Mètodes algebraics i les seues aplicacions
Cicle	Màster
Crèdits ECTS	3.0
Curs acadèmic	2024 - 2025

Titulació/titulacions

Titulació	Centre	Curs	Període
2183 - M.U.Invest.Matemàtica	Facultat de Ciències Matemàtiques	1	Segon quadrimestre

Matèries

Titulació	Matèria	Caràcter
2183 - M.U.Invest.Matemàtica	4 - Intensificació matemàtica fonamental	Optativa

RESUM

Aquesta assignatura permet a l'alumne adquirir unes competències relatives a l'aplicació de l'Àlgebra abstracta tant dins la matemàtica pura i aplicada com en altres àmbits interdisciplinaris: enginyeria, informàtica, ciberseguretat, tractament de la informació, etc.

Els continguts de l'assignatura fan referència a l'aplicació d'estructures algebraiques bàsiques (semigrups, grups, anells, cossos, algebres, etc.) en criptografia, teoria de codis correctors d'errors, geometria algebraica, esquemes de repartiment de secrets, resolució de sistemes d'equacions diferencials lineals, factorització de nombres enters, tests de primalidad, signatura digital, resolució de puzles i sudokus, programació lineal sencera, i altres àrees.

CONEIXEMENTS PREVIS

Relació amb altres assignatures de la mateixa titulació

No heu especificat les restriccions de matrícula amb altres assignatures del pla d'estudis.

Altres tipus de requisits

Es recomanen nocions bàsiques de les següents estructures algebraiques: grups, anells, cossos i espais vectorials.

2183 - M.U.Invest.Matemàtica

- Que els estudiants comprenguen els conceptes i les demostracions rigoroses de teoremes fonamentals d'alguna de les àrees específiques de les Matemàtiques.
  ?
- Que els estudiants siguen capaços d'aplicar els resultats i tècniques apreses per a la resolució de problemes complexos d'alguna de les àrees de les Matemàtiques, en contextos acadèmics o professionals.
  ?
- Que els estudiants posseïsquen la capacitat per a enunciar i verificar proposicions en alguna de les àrees de les Matemàtiques i per a transmetre els coneixements matemàtics adquirits, oralment i per escrit.
- Que els estudiants sàpien triar i utilitzar ferramentes informàtiques adequades per a abordar problemes relacionats amb les Matemàtiques i les seues aplicacions.
  ?

Les activitats a desenvolupar per part de l'alumne són un portafoli (resolució de problemes) i un treball grupal amb els quals es valora la capacitat comunicativa en àmbit de l'assignatura tant a nivell escrit com oral. Es realitzaran exposicions orals dels treballs realitzats de manera individual i/o grupal per a avaluar la competència transversal

DESCRIPCIÓ DE CONTINGUTS

1. Aritmètica modular i aplicacions.

- Conceptes bàsics d'aritmètica modular.
- Aplicacions de l'aritmètica modular en criptografia i altres camps.
- Introducció al sistema d'àlgebra computacional GAP.

2. Teoria de grups i aplicacions.

- Revisió de conceptes bàsics en Teoria de grups.
- Teoria de grups amb GAP. El graf de Cayley.
- Aplicacions a la resolució de puzles, geometria i altres àrees.

3. Teoria d'anells i cossos. Aplicacions.

- Revisió dels conceptes bàsics de la Teoria d'anells i cossos.
- Introducció a la geometria algebraica.
- Cossos finits. Tractament amb GAP.
- Criptografia basada en el problema del logaritme discret: ElGamal i criptografia el·líptica. Tractament amb el sistema computacional Sage.
- Aplicacions: factorització de nombres enters, esquemes de repartiment de secrets, tests de primalidad i algorismes de signatura digital.

4. Introducció a la Teoria de codis correctors d'errors.

- Conceptes bàsics: transmissió de la informació, codi corrector, paràmetres.
- Codis lineals. Codificació. Descodificació amb síndromes. Tractament amb GAP.
- Cotes dels paràmetres.
- Codis de Reed-Solomon.

5. Anells de polinomis. Bases de Groebner i aplicacions.

- Resultats bàsics. Ordres monomiales. Algorisme de la divisió.
- Bases de Groebner.
- Utilització del sistema d'àlgebra computacional Singular per al càlcul i maneig de les bases de Groebner.
- Aplicacions: Geometria algebraica, àlgebra commutativa, resolució d'equacions en derivades parcials, programació lineal sencera, demostració automàtica de teoremes geomètrics, resolució de sudokus, etc.

VOLUM DE TREBALL

ACTIVITAT	Hores	% Presencial
Classes de teoria	30,00	100
Elaboració de treballs en grup	20,00	0
Elaboració de treballs individuals	20,00	0
Estudi i treball autònom	5,00	0
TOTAL	**75,00**	

METODOLOGIA DOCENT

Es realitzarà una breu introducció teòrica al començament de cada tema de l'assignatura i posteriorment s'analitzaran els mètodes necessaris per a la resolució de les diferents aplicacions plantejades relacionades amb els continguts exposats en el tema. Es farà ús de diferents sistemes computacionals algebraics que ajuden en la resolució dels exercicis pràctics plantejats.

AVALUACIÓ

L'avaluació de l'alumne serà contínua i estarà basada principalment en el lliurament de problemes senzills mitjançant l'elaboració del portafoli i la realització d'un treball acadèmic. Es realitzarà un examen oral per a valorar el coneixement adquirit tant en el portafoli com en el treball acadèmic. Als alumnes que tinguen la dispensa d'assistir a classe se'ls plantejaran qüestions senzilles de seguiment. S'avaluaran amb un 80% els treballs acadèmics i el portafoli i amb 20% l'exposició oral i escrita del treball realitzat.

REFERÈNCIES

Bàsiques

- Applied abstract algebra (Lidl, Rudolf ; Pilz, Günter)
- Modern algebra with applications (Gilbert, William J.)
- Finite group theory (Isaacs, I. Martin)
- Álgebra : a graduate course (Isaacs, I. Martin)
- Applied modern algebra (Larry L. Dornhoff, Franz E. Hohn)
- Applied abstract algebra (Kim, Ki Hang)
- The theory of finite groups : an introduction (Kurzweil, Hans)
- Modern computer algebra (Gathen, Joachim von zur)
- A Singular Introduction to Commutative Algebra [electronic resource] (Greuel, GM ; Pfister, G.)
- Ideals, varieties, and algorithms : an introduction to computational algebraic geometry and commutative algebra (Cox, David A. et al.)

Complementàries

- Codificación de la información(Munuera Gómez, Juan - Tena Ayuso, Juan - Universidad de Valladolid)