Universidad Zaragoza

Curso Académico: 2023/24

27045 - Álgebra aplicada y computacional

Información del Plan Docente

Año académico: 2023/24
Asignatura: 27045 - Álgebra aplicada y computacional
Centro académico: 100 - Facultad de Ciencias
Titulación: 453 - Graduado en Matemáticas
Créditos: 6.0
Curso: 4
Periodo de impartición: Segundo semestre
Clase de asignatura: Optativa
Materia:

1. Información básica de la asignatura

Se han seleccionado tres aplicaciones del álgebra. Bases de Groebner que resuelven problemas relacionados con polinomios en varias variables. Criptografía actual, RSA y métodos relacionados con el problema del logaritmo discreto, en particular basados en curvas elípticas. Teoría de códigos correctores de errores que se producen en las trasmisiones de datos basados en álgebra lineal y cuerpos finitos.

Los planteamientos y objetivos de la asignatura están alineados con los Objetivos de Desarrollo Sostenible (ODS) de la Agenda 2030 de Naciones Unidas; en concreto, las actividades de aprendizaje previstas en esta asignatura contribuirán en alguna medida al logro de los objetivos 4 (educación de calidad), 5 (igualdad de género), 8 (trabajo decente y crecimiento económico) y 10 (reducción de las desigualdades).

2. Resultados de aprendizaje

- Desarrollar y aplicar algoritmos.
- Apreciar la aplicación de temas del álgebra en problemas de interés social y tecnológico.
- Conocer en profundidad los mecanismos matemáticos que resuelven problemas de seguridad y autenticidad en trasmisiones de datos.
- Conocer la potencia de los algoritmos derivados de las bases de Gröbner.

3. Programa de la asignatura

I. Bases de Gröbner.
   1. Órdenes monomiales.
   2. Ideales monomiales. Lema de Dickson.
   3. El teorema de la base de Hilbert.
   4. Propiedades de las bases de Gröbner.
   5. Aplicaciones de las bases de Gröbner.

II. Criptografía.
   6. Principios de criptografía.
   7. El sistema estándar de encriptación avanzada (AES).
   8. Criptografía de clave pública. Método RSA.
   9. Criptosistemas basados en el problema del logoritmo discreto.
   10. Tendencias actuales: criptografía de curvas elípticas.
   11. Firma electrónica. El DNIe.
   12. Funciones Hash.

III. Códigos correctores de errores.
   13. Códigos detectores de errores.
   14. Códigos lineales. Corrección de errores.
   15. Códigos de Hamming.
   16. Códigos multicorrectores: BCH.

17. Códigos correctores de errores a ráfagas, códigos RS.

4. Actividades académicas

Clases magistrales: 45 horas.
Prácticas informatizadas: 15 horas.
Estudio: 85 horas.
Pruebas de evaluación: 5 horas.

5. Sistema de evaluación

- Participación durante el desarrollo de las clases, tanto en las de carácter teórico, como práctico como de ordenador.
- Resolución de algunos problemas propuestos para exponer en clase.
- Elaboración de programas de ordenador, en los que se materialicen algunos de los algoritmos presentados en clase, y su aplicación a casos concretos.
- Exámenes escritos de las distintas partes de la asignatura.

Cada una de las tres partes de la asignatura tendrá una calificación independiente que supondrá 1/3 de la calificación global. Para cada parte habrá al menos una practica de ordenador y un máximo de tres. Para cada parte habrá al menos un examen antes de la prueba global que supondrá el 90% de la calificación de esa parte. Para aprobar será necesario haber hecho todas las prácticas de ordenador propuestas y haber aprobado los exámenes correspondientes a las tres partes de la asignatura. El examen global podrá servir para aprobar o para subir nota en todas o en alguna de las tres partes de la asignatura.

Se valorarán las presentaciones en LaTeX de algunos de los ejercicios que se propongan.

Sin menoscabo del derecho que, según la normativa vigente, asiste al estudiante para presentarse y, en su caso, superar la asignatura mediante la realización de una prueba global.