Universidad Zaragoza

Curso Académico: 2021/22

27045 - Álgebra aplicada y computacional

Información del Plan Docente

Año académico: 2021/22
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

1.1. Objetivos de la asignatura

La asignatura y sus resultados previstos responden a los siguientes planteamientos y objetivos:

Se trata de una asignatura de formación optativa dentro del grado.

1.2. Contexto y sentido de la asignatura en la titulación

Se recomienda haber cursado las asignaturas de Números y conjuntos, Álgebra lineal, Estructuras algebraicas y Teoría de Galois.

1.3. Recomendaciones para cursar la asignatura

Haber adquirido competencias de álgebra lineal y geometría, estructuras algebraicas.

Asistencia a clases y participación activa en las mismas.

Resolución de ejercicios y problemas.

Trabajar los programas de ordenador que se propongan.

2. Competencias y resultados de aprendizaje

2.1. Competencias

Al superar la asignatura, el estudiante será más competente para:

- Desenvolverse en el manejo de los objetivos descritos (ver apartado Resultados de aprendizaje).
- Saber aplicar los conocimientos matemáticos a su trabajo de una forma profesional y poseer las competencias que se demuestran mediante la resolución de problemas en el área de las matemáticas y de sus aplicaciones.
- Tener la capacidad de reunir e interpretar datos relevantes, particularmente en el área de las matemáticas, para emitir juicios, usando la capacidad de análisis y abstracción, que incluyan una reflexión sobre temas relevantes de índole social, científica o ética.
- Poder comunicar, de forma oral y escrita, información, ideas, problemas y soluciones del ámbito matemático a un público tanto especializado como no especializado.
- Saber expresar con claridad, tanto por escrito como de forma oral, razonamientos, problemas, informes, etc.
- Utilizar aplicaciones informáticas con distintos tipos de software científico para experimentar en matemáticas y resolver problemas.
- Desarrollar algoritmos y programas que resuelvan problemas matemáticos, utilizando para cada caso el entorno computacional adecuado.

2.2. Resultados de aprendizaje

El estudiante, para superar esta asignatura, deberá demostrar los siguientes resultados:

- Desarrollo y aplicación de 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.

2.3. Importancia de los resultados de aprendizaje

Proporcionan una formación de carácter optativo dentro del grado (ver Contexto y sentido de la asignatura en la titulación).

3. Evaluación

3.1. Tipo de pruebas y su valor sobre la nota final y criterios de evaluación para cada prueba

El estudiante deberá demostrar que ha alcanzado los resultados de aprendizaje previstos mediante las siguientes actividades de evaluación:

a) Participación durante el desarrollo de las clases, tanto en las de carácter teórico, como práctico como de ordenador.

b) Resolución de algunos problemas propuestos para exponer en clase.

c) Elaboración de programas de ordenador, en los que se materialicen algunos de los algoritmos presentados en clase, y su aplicación a casos concretos.

d) 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.

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.

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

4. Metodología, actividades de aprendizaje, programa y recursos

4.1. Presentación metodológica general

El proceso de aprendizaje que se ha diseñado para esta asignatura se basa en lo siguiente:

Las clases de teoría y problemas (3 por semana) se utilizarán para la presentación y desarrollo de los distintos temas. Este desarrollo deberá ser posteriormente ampliado por el estudiante, con el uso de apuntes y bibliografía adecuada. La elaboración de programas de ordenador será mediante dos horas de periodicidad quincenal.

Se utilizará la herramienta Moodle y email como una forma de comunicación entre profesor y alumno. Para las clases de prácticas de ordenador se utilizará Sage. Se pondrá a disposición del estudiante textos y apuntes que ayuden en el seguimiento de la asignatura.

4.2. Actividades de aprendizaje

- Asistencia y participación en las clases.
- Se dedicará alguna clase a la resolución de ejercicios por parte de los estudiantes. Deberán mostrar sus dotes de comunicación y razonamiento, mediante expresión oral.
- Redacción de la resolución de ejercicios utilizando LaTeX.
- Resolución de problemas mediante uso de ordenador (programa SAGE), con periodicidad bisemanal.
- Consulta de procedimientos de resolución de las actividades anteriores en tutorías.
- Búsqueda de problemas de la vida real relacionados con los contenidos de la asignatura.

Las actividades docentes y de evaluación se llevarán a cabo de modo presencial salvo que, debido a la situación sanitaria, las disposiciones emitidas por las autoridades competentes y por la Universidad de Zaragoza dispongan realizarlas de forma

telemática o semitelemática con aforos reducidos rotatorios.

4.3. Programa

El programa que se ofrece al estudiante para ayudarle a lograr los resultados previstos comprende las siguientes actividades:

Parte 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 Gröebner.

Parte 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 algoritmo discreto
10. Tendencias actuales: criptografía de curvas elípticas.
11. Firma electrónica. El DNIe
12. Funciones hash.

Parte 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.

4.4. Planificación de las actividades de aprendizaje y calendario de fechas clave

Calendario de sesiones presenciales y presentación de trabajos:

Más información se colgará en el Add (Moodle).

Las fechas de los exámenes de cada parte se avisarán en el add.

Las prácticas de ordenador tendrán carácter quincenal.

Las fechas de la evaluación final se indicarán en la web.

4.5. Bibliografía y recursos recomendados

- Hardy, Darel W.. Applied algebra : codes, ciphers, and discrete algorithms / Darel W. Hardy, Fred Richman, Carol L. Walker . - 2nd ed. Boca Raton : Chapman & Hall/CRC, cop. 2009.
- Pastor Franco, José. Criptografía digital : fundamentos y aplicaciones / José Pastor Franco, Miguel Angel Sarasa López, José Luis Salazar Riaño . - 2a. ed. Zaragoza : Prensas Universitarias de Zaragoza, 2001.
- Durán Díaz, Raúl. El criptosistema RSA / Raúl Durán Díaz, Luis Hernández Encinas, Jaime Muñoz Masqué Madrid : Ra-Ma, D.L. 2005.
- Klima, Richard. E. [et al.]. Applications of abstract algebra. With Maple and MATLAB . 2nd. Ed. Taylor & Francis. 2006.
- Joyner, David. Applied Abstract Algebra. Johns Hopkins. 2004.
- Vaudenay, Serge. A Classical Introduction To Cryptography. reprint of 1st ed. 2006 Springer. 2010.
- Paar, Christof. Understanding Cryptography. Springer. 2010.
- Huppert, Bertram. Lineare Algebra. 2ª ed. Vieweg+teubner Verlag. 2010.

http://psfunizar10.unizar.es/br13/egAsignaturas.php?codigo=27045