Grado en Matemáticas
27045 - Álgebra aplicada y computacional

Guía docente para el curso 2013 - 2014

Curso: 4, Semestre: 2, Créditos: 6.0

Información básica

Profesores

- **Manuel Vázquez Lapuente** vazquez@unizar.es

Recomendaciones para cursar esta asignatura

Haber adquirido competencias de Álgebra Lineal y Geometría y de Estructuras Algebraicas

asistencia a clasesy participación activa en las mismas

resoluciones de ejercicios y problemas

trabajar los programas de ordenador que se propongan

Actividades y fechas clave de la asignatura

la resolución de ejercicios se realizará semanalmente

las prácticas de ordenador tendrán carácter quincenal

las fechas de la evaluación final se indicarán en la web

Inicio

Resultados de aprendizaje que definen la asignatura

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

1:

- 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.

Introducción

Breve presentación de la asignatura

Desarrollo de temas que conectan directamente el álgebra con el mundo “real”, con especial énfasis en criptografía (teoría de números, números primos, curvas elípticas) y en la teoría de códigos correctores de errores (álgebra lineal, polinomios, cuerpos finitos, combinatoria).

Contexto y competencias

Sentido, contexto, relevancia y objetivos generales 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.

Contexto y sentido de la asignatura en la titulación

Se recomienda haber cursado las asignaturas de Conjuntos y números, Algebra lineal, y Estructuras algebraicas.

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

1:
Desenvolverse en el manejo de los objetivos descritos (ver apartado “Resultados de Aprendizaje”)

CG2. 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.

CG3. 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.

CG4. Poder comunicar, de forma oral y escrita, información, ideas, problemas y soluciones del ámbito matemático a un público tanto especializado como no especializado.

CT1. Saber expresar con claridad, tanto por escrito como de forma oral, razonamientos, problemas, informes, etc.

CE4. Utilizar aplicaciones informáticas con distintos tipos de software científico para experimentar en Matemáticas y resolver problemas.

CE5. Desarrollar algoritmos y programas que resuelvan problemas matemáticos, utilizando para cada caso el entorno computacional adecuado.

Importancia de los resultados de aprendizaje que se obtienen en la asignatura:

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

Evaluación

Actividades de evaluación

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

1:

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

b) Resolución de ejercicios y su presentación oral.

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) Actividades complementarias: tests, presentaciones orales de temas relacionados con el programa, resoluciones de criptogramas, etc.

e) Examen escrito sobre algunas partes de la asignatura.

La calificación constará de dos partes. la primera se realizará en función de las habilidades mostradas en las actividades a), b), c) y d) anteriores, y supondrá el 60% de la nota final. La segunda se referirá a la actividad e) anterior, y su peso será del 40% sobre la calificación final. No obstante, las actividades ab) y c) tienen el carácter de obligatorias.

--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.

Actividades y recursos

Presentación metodológica general

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

Las clases de teoría (dos 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 resolución de ejercicios se realizará en clase semanal, y la de elaboración de programas de ordenador 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.

Actividades de aprendizaje programadas (Se incluye programa)

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

1: *Parte I. Criptografía*

- 1. Principios de criptografía
- 2. El sistema estándar de encriptación avanzada (AES)
- 3. Criptografía de clave pública. Método RSA
- 4. Criptosistemas basados en el problema del algoritmo discreto.
- 5. Tendencias actuales: criptografía de curvas elípticas.
- 6. Firma electrónica. El DNIe.
- 7. Funciones hash.

Parte II. Códigos correctores de errores

- 8. Códigos detectores de errores.
- 9. Códigos lineales.
- 10. Corrección de errores.
- 11. Códigos perfectos.
- 12. Códigos multicorrectores: BCH.
- 13. Códigos correctores de errores a ráfagas.
- 14. Corrección de errores en códigos RS.
- 15. Aplicaciones de códigos.

Parte III. Álgebra computacional

- 16. Bases de Gröbner

2:

Principales referencias

- Hardy-Richman-Walker, *Applied Algebra: codes, ciphers and discrete algorithms*, CRC Press, 2009
- Klima-Sigmon-Stitzinger, *Applications of Abstract Algebra*, CRC Press, 2000.
- Joyner-Kreminski-Turisco, *Applied Abstract Algebra*, Hopkins UP, 2004.
- Vaudenay, *A Classical, Introduction to Cryptography*, Springer, 2006.
- Paar-Pelzl, *Understanding Cryptography*, Springer, 2010.
- Pastor-Sarasa-Salazar, *Criptografía digital*, Prensas Universitarias de Zaragoza, 2ª ed, 2001.
- Durán-Hernández-Muñoz, *El criptosistema RSA*, RA-MA, 2005.
- Huppert-Willems, *Lineare Algebra*, Teubner, 2006.
- Stein, W, Elementary Number Theory: Primes, Congruences, and Secrets, 2011, http://wstein.org/ent/ent.pdf

Planificación y calendario

Calendario de sesiones presenciales y presentación de trabajos

Ver “fechas clave e hitos clave”. Más información se colgará en el Add.

Referencias bibliográficas de la bibliografía recomendada

- Durán Díaz, Raúl. El criptosistema RSA / Raúl Durán Díaz, Luis Hernández Encinas, Jaime Muñoz Masqué Madrid : Ra-Ma, D.L. 2005
- 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
- Huppert, Bertram. Lineare Algebra. 2ª ed. Vieweg+teubner Verlag. 2010
- Joyner, David. Applied Abstract Algebra. Johns Hopkins. 2004
- Klima, Richard. E. [et al.]. Applications of abstract algebra. With Maple and MATLAB . 2nd. Ed. Taylor & Francis. 2006
- Paar, Christof. Understanding Cryptography. Springer. 2010
- 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
- Vaudenay, Serge. A Classical Introduction To Cryptography. reprint of 1st ed. 2006 Springer. 2010