UNIDAD CUAJ	IMALPA DIVISION CIENCIAS NATURALES	S E INGENIERIA 1 / 3
NOMBRE DEL P	LAN LICENCIATURA EN MATEMATICAS APLICAI	DAS
CLAVE UNIDAD DE ENSEÑANZA-APRENDIZAJE		CRED. 8
460089	ALGEBRA COMPUTACIONAL	TIPO OPT.
H.TEOR. 3.0 H.PRAC. 2.0	SERIACION AUTORIZACION	TRIM. VIII al XI

## OBJETIVO(S):

Objetivos Generales:

Que al final del curso el alumno sea capaz de:

- 1. Plantear y resolver tanto manualmente como computacionalmente problemas que se pueden modelar mediante ecuaciones diofantinas.
- 2. Programar los algoritmos que se desarrollan durante el trimestre.
- 3. Conocer técnicas para la factorización de polinomios en Zp.

## CONTENIDO SINTETICO:

- 1. Introducción al álgebra computacional. Algunas aplicaciones representativas.
- 2. Teoría de números en los enteros. Congruencias, ecuaciones diofantinas, Teorema Chino del residuo. Raíces primitivas módulo m, raíces n-ésimas de la unidad de Zp, campos finitos. Primos, Teorema pequeño de Fermat, Teorema de Fermat, Teorema de Euler, criterios de primalidad. Sistema RSA de criptografía.
- 3. Anillo de polinomios. Evaluación e interpolación modular, transformada rápida de Fourier, factorización de polinomio en Zp. Factorización libre de cuadrados. Algoritmo de Berlekamp. Aplicación a la teoría de códigos.

MODALIDADES DE CONDUCCION DEL PROCESO ENSEÑANZA-APRENDIZAJE:

Es recomendable:



UNIVERSIDAD AUTONOMA METROPOLITANA

APROBADO PODEL COLEGIO ACADEMICO EN SU SESION NUM. 315

EL SECRETARIO DEL COLEGIO

CLAVE 460089

ALGEBRA COMPUTACIONAL

Exponer la teoría e introducir los conceptos mediante ejemplos tomados de problemas tanto matemáticos como de otras disciplinas, resaltando los aspectos conceptuales en forma intuitiva.

Promover entre los alumnos la discusión, planteamiento y solución de problemas de aplicación a diferentes disciplinas.

Solicitar tareas tipo proyecto en las cuales se desarrollen las ideas tanto rigurosas como los algoritmos que involucre el álgebra computacional. Realizar prácticas en el aula de cómputo para la implementación de los algoritmos que se desarrollan durante el trimestre.

Constituir en el aula una cultura de enseñanza-aprendizaje que valore la argumentación, la elaboración y prueba de modelos y la exploración de los conceptos matemáticos del curso, así como su relevancia en la respuesta a problemas prácticos en ciencias naturales e ingeniería.

Trabajar por problemas tanto teóricos como de aplicación en donde el profesor conduce el proceso y los alumnos participan activamente, fomentando el trabajo en equipo.

Sostener reuniones periódicas de los profesores de los diversos grupos de este curso a lo largo del trimestre, con el fin de discutir el desarrollo del curso, evaluando y mejorando el proceso de conducción del aprendizaje, concebir los ejemplos y ejercicios presentados, así como elaborar las tareas y notas de clase, las evaluaciones periódicas y la evaluación terminal.

## MODALIDADES DE EVALUACION:

Evaluación Global:

Se ponderarán las siguientes actividades a criterio del profesor.

- Entrega de ejercicios y proyectos.
- Evaluaciones periódicas de los temas del curso.
- Participación en los procesos de planteamiento y solución de problemas tanto en las sesiones teóricas como en las prácticas computacionales.
- Evaluación terminal.

Evaluación de Recuperación:

- El alumno deberá presentar una evaluación crítica que contemple todos los



UNIVERSIDAD AUTONOMA METROPOLITANA

APROBADO POR EL COLEGIO ACADEMICO EN SU SESION NUM. \_\_3/5\_\_

LSECRETARIO DEL COLEGIO

NOMBRE DEL	PLAN LICENCIATURA	. EN MATEMATICAS	APLICADAS	3/3
CLAVE 4600	39 ALGEBRA COMP	UTACIONAL		

contenidos de la unidad de enseñanza-aprendizaje y no se requiere inscripción previa a la UEA.

## BIBLIOGRAFIA NECESARIA O RECOMENDABLE:

- 1. Akritas, A. G., Elements of computer. Algebra with applications; John Wiley & Son, USA, 1989.
- 2. Cohen, A. M., Cuypers, H. y Sterk, H., Algebra interactive!, Learning algebra in an exiting way; Springer, Alemania, 1999.
- 3. Gathern, J., Zur, V. y Jürgen, G.; Modern computer algebra; Cambridge University, Inglaterra, 2003.
- 4. Gill, A., Applied algebra for computer science; Prentice Hall, USA, 1976.
- 5. Koblitz, N., Algebraic aspects of cryptography; Springer, USA, 1999.
- 6. Mignotte, M., Mathematics for computer algebra; Springer-Verlag, USA, 1992.
- 7. Niederreiter L. R., Finite fields; Cambridge University Press, Inglaterra, 1997.



UNIVERSIDAD AUTONOMA METROPOLITANA

APROBADO POR EL COLEGIO ACADEMICO EN SU SESION NUM. 315

SECRETARIO DEL COLEGIO