UNIVERSIDAD DE ANTIOQUIA
FACULTAD DE CIENCIAS EXACTAS Y NATURALES
ÁREA DE PREGRADO EN MATEMÁTICAS

Código: CNM-482
Nombre: ÁLGEBRA COMPUTACIONAL **I**
Prerrequisito: CNM-355, CNM-356, CNM-360
Duración del semestre: 16 semanas
Intensidad semanal: 4 horas
Número de créditos: 4
Campo de formación: Profesional
Tipo de curso: Teórico
Este curso es validable y habilitable.

1. Objetivos

1.1. Objetivos generales

1.1.1. Los tres cursos de Álgebra computacional pretenden dar al estudiante una visión general de esta nueva área de la matemática y dotarlo de las herramientas básicas para resolver problemas con la ayuda del computador.

1.2. Objetivo específico

1.2.1. Adquirir destrezas para el manejo de enteros grandes.

1.2.2. Conocer los problemas de la factorización y primalidad de enteros.Adquirir destrezas para el manejo de enteros grandes.

1.2.2. Conocer los problemas de la factorización y primalidad de enteros.

2. Contenido

Unidad 1: ARITMÉTICA COMPUTACIONAL. (Duración: 10 horas**)**

2.1.1. Aritmética de enteros grandes : Suma, resta, multiplicación y división.
2.1.2. Algorítmo extendido de Euclides. Complejidad computacional de estos algorítmos.

Unidad 2: SEUDOPRIMOS. (Duración: 10 horas**)**

2.2.1. Congruencias.
2.2.2. Cálculo de a^n mod m.
2.2.3. Teorema chino del residuo.
2.2.4. Pequeño teorema de Fermat.
2.2.5. Seudoprimos.
2.2.6. Números fuertemente seudoprimos.
2.2.7. Bases para las que un entero es seudoprimo y para las que es fuertemente seudoprimo.

Unidad 3: NÚMEROS DE CARMICHAEL. (Duración:10 horas**)**

2.3.1. Números de Carmichael.
2.3.2. Números de Carmichael de rango 3.

Unidad 4: PRIMALIDAD. (Duración:16 horas**)**

2.4.1. Criterios determinísticos de primalidad.
2.4.2. Teorema de Lucas.
2.4.3. Teorema de Pepin.
2.4.4. Teorema de Lehmer.
2.4.5. Teorema de Proth.

Unidad 5: FACTORIZACIÓN DE ENTEROS. (Duración: 16 horas**)**

2.5.1. Algorítmos de factorización de enteros.
2.5.2. División-ensayo.
2.5.3. Algorítmo de Fermat.
2.5.4. Algorítmo Rho.
2.5.5. Algorítmo p-1 de Pollard.
2.5.6. Curvas Elípticas.
2.5.7. Fracciones Continuadas.

Nota : A lo largo del curso se estudiará y utilizará el sistema de Álgebra computacional **MUPAD.**

3. Metodología

- Exposición magistral del profesor.
- Discusión con los alumnos de lecturas asignadas.
- Sesiones de problemas.

4. Evaluación

La que defina el consejo de Facultad.

5. Bibliografía.

Akritas, A.G. Elements of computer algebra with applications. John Wiley and sons, New York, 1989.

Bressoud, D. M. Factorization and primality testing. Springer-Verlag, New York, 1989.

Cohen, H. A course in computational algebraic number theory. Springer-Verlag, New York, 1993.

Dixon, J. D. Factorization and primality test. Amer. Math. Monthly 91 (1984) 333-352.

Koblitz, N. A course in number theory and cryptography. Springer-Verlag, New York, 1987.

Ribenboin, P. The book of prime number records. Springer- Verlag, New York, 1988.

Actualizado por: Gilberto García Pulgarín