Información del curso del primer semestre 2018

Programa:

1. **Teoría Elemental de Número**s. Divisibilidad, máximo común divisor y mínimo común múltiplo. Números primos, descomposición factorial. Algoritmo de Euclides extendido, ecuaciones diofánticas lineales, congruencias. Teorema chino del resto. Teorema de Fermat-Euler, primos de Charmichael. Sistemas de numeración.
2. **Teoría de Grupos**. Definición y ejemplos, subgrupos, grupos cíclicos, enteros módulo n, invertibles módulo n. Orden de un elemento, orden de un grupo. Clases laterales, Teorema de Lagrange, subgrupos normales, grupo cociente. Homomorfismos. Primer teorema de isomorfismo.
3. **Raíces primitivas**. Existencia y unicidad para primos y potencias de primos. Cantidad de raíces primitivas, logaritmo discreto, test de Lucas, test de primalidad.
4. **Criptografía**. Criptosistemas clásicos (César, RSA, Vigenere), Diffie-Hellman (intercambio de clave), RSA, cifrado de bloques, método de factorización de Fermat.

Última modificación: jueves, 22 de febrero de 2018, 13:38