

Matemática discreta 2 — Teórico 2

Gonzalo Tornaría

Enlace a los videos de las clases

- 01 - Introducción
- 02 - División entera
- 03 - Algoritmo de Euclides
- 04 - Identidad de Bézout
- 05 - Ecuaciones diofánticas
- 06 - El problema de los sellos
- 07 - Teorema fundamental de la aritmética
- 08 - Congruencias
- 09 - Ecuaciones con congruencias
- 10 - Inversos y teorema chino
- 11 - Teorema chino, exponenciación
- 12 - Teoremas de Fermat y de Euler
- 13 - Fórmula para la función de Euler, orden módulo m
- 14 - Grupos, definición y ejemplos
- 15 - Grupo dihedral, subgrupos
- 16 - grupo generado y orden de un elemento
- 17 - Teorema de Lagrange
- 18 - teorema de órdenes
- 19 - isomorfismos, raíces primitivas
- 20 - criterio para raíces primitivas, Hankeliana para \mathbb{Z}_p
- 21 - raíces primitivas modulo primo
- 22 - raíces primitivas módulo potencias de primo, cripto
- 23 - intercambio de claves Diffie-Hellmann, ataque de la persona en el medio
- 24 - criptosistemas de clave pública, RSA