Ementa de Números Inteiros e Criptografia

Prof. Luis Menasché Schechter

Unidade 0: Introdução

1. Criptografia
2. Criptografia RSA
3. Noções de Algoritmos
4. Noções de Computação Algébrica

Unidade 1: Algoritmos Fundamentais

1. Algoritmo da Divisão
2. Algoritmo Euclidiano
3. Algoritmo Euclidiano Estendido
4. Resolução de Equações Diofantinas Lineares em 2 Variáveis

Unidade 2: Fatoração

1. Algoritmo Simples de Fatoração
2. Algoritmo de Fatoração de Fermat
3. Propriedade Fundamental dos Primos
4. Unicidade da Fatoração

Unidade 3: Números Primos

1. Fórmulas Polinomiais para Números Primos
2. Números de Mersenne e de Fermat
3. Infinidade dos Primos
4. Crivo de Eratóstenes

Unidade 4: Aritmética Modular

1. Relações de Equivalência
2. Inteiros Módulo n
3. Soma e Produto Modulares
4. Exponenciação Modular
5. Divisão Modular
6. Critérios de Divisibilidade
7. Pequeno Teorema de Fermat

Unidade 5: Pseudoprimos

1. Pseudoprimos de Fermat
2. Números de Carmichael
3. Teste de Miller e Pseudoprimos Fortes

Unidade 6: Sistemas de Congruências

1. Teorema Chinês do Resto
2. Algoritmo Chinês do Resto (ACR)
3. Uso do ACR para o Cálculo de Potências Módulo n

Unidade 7: Grupos

1. Definição
2. Grupos Aritméticos
3. Subgrupos
4. Subgrupos Cíclicos
5. Teorema de Lagrange
6. Lema Chave

Unidade 8: Fatoração de Números de Mersenne e de Fermat

1. Método de Fermat para Fatoração de Números de Mersenne
2. Método de Euler para Fatoração de Números de Fermat

Unidade 9: Testes de Primalidade

1. Teorema da Raiz Primitiva
2. Teste de Lucas
3. Teste de Pépin para Números de Fermat
4. Teste de Lucas Melhorado

Unidade 10: Criptografia RSA e El Gamal

1. Pré-Codificação
2. Codificação e Decodificação RSA
3. Segurança do RSA
4. Assinatura RSA
5. Codificação, Decodificação e Assinatura El Gamal