CURSO: Graduação em Matemática – 2º semestre de 2023
DISCIPLINA: Álgebra e Criptografia
PROFESSOR(ES): Luciano Monteiro de Castro
CARGA HORÁRIA: 60h
PRÉ-REQUISITO: Fundamentos de Matemática e Matemática Discreta
HORÁRIO E SALA DE ATENDIMENTO: terças e quintas 9:30 a 10:30
SALA: 504

PLANO DE ENSINO

1. Ementa

Grupos, Teorema de Lagrange, Grupos Normais, Quociente e homomorfismos; Anéis e Domínios, Domínios euclidianos, Polinômios, Fatoração única, Ideais e Quociente; aplicações à Teoria dos Números, Primos, Pequeno teorema de Fermat, Pseudoprimos, Sistemas de Congruências; Polinômios Ciclotômicos, Raízes primitivas; Criptografia RSA.

2. Objetivos da disciplina

O objetivo da disciplina é ampliar, a partir do conhecimento e habilidades desenvolvidas em Fundamentos de Matemática e Matemática Discreta, a capacidade de aplicação de propriedades aritméticas e algébricas dos números inteiros em diversos processos envolvendo segurança na transmissão de dados. Em torno ao método de Criptografia RSA serão estudados conceitos e teoremas da matemática pura, em particular da Álgebra Abstrata, que encontram diversas aplicações também em outras áreas do conhecimento. Espera-se que os alunos obtenham um primeiro contato instrutivo com Teoria dos Números e Álgebra Abstrata, mas especificamente Anéis, Anéis Comutativos e Teoria dos Grupos, entendendo suas principais aplicações e permitindo o posterior aprofundamento conforme interesse e necessidade.

3. Procedimentos de ensino (metodologia)

Os conceitos e teoremas mais importantes serão comentados em aula, sendo recomendada a leitura prévia do material disponibilizado. Serão propostas abundantes listas de exercícios para trabalho individual e em grupo, com espaço na plataforma online (eclass) para postagem e discussão de

soluções. O foco do tempo de aula será a resolução de dúvidas. Serão aplicados testes regulares.

Haverá um trabalho final de implementação relacionado ao sistema de criptografia RSA.

4. Conteúdo programático detalhado

Datas	Tópico	Atividades
07 a 11/08	Introdução à Criptografia. Grupos	
14 a 18/08	Exemplos. Subgrupos	
21 a 25/08	Geradores, Diagramas de Cayley	
28 a 31/08	Ordem, Teorema de Lagrange	
04 a 14/09	Homomorfismos	
18 a 28/09	Grupo Quociente	
02 a 11/10	Semana da A1	
17 a 19/10	Ações de Grupos	
23 a 27/10	Anéis, Ideais	
30/10 a 03/11	Homomorfismos, Quocientes	
06 a 10/11	Teorema Chinês dos Restos	
13 a 17/11	Polinômios Ciclotômicos	
20 a 24/10	Raízes primitivas, Criptografia RSA	
27/11 a 04/12	Semana da A2	
14 a 20/12	Semana da AS	

5. Procedimentos de avaliação

A nota da A1será composta da seguinte maneira: Testes: 50% e Prova: 50%. A nota da A2 será composta da seguinte maneira: Prova: 50%, Testes: 25%, Trabalho computacional: 25%. A AS consistirá de uma prova única.

6. Bibliografia Obrigatória

Tengan, E. e Tadao Martins, S. “Álgebra Exemplar”. Projeto Euclides. IMPA.

Coutinho, S. Collier. Números Inteiros e Criptografia. Coleção Computação e Matemática. IMPA

Hefez, Abramo. Elementos de Aritmética. SBM.

Gonçalves, Adilson. Introdução a Álgebra. IMPA.

7. Bibliografia Complementar

Codes and Ciphers: Julius Caesar, the Enigma, and the Internet R. F. Churchhouse;

An Introduction to Cryptography Richard A. Mollin;

RSA and Public-Key Cryptography Richard A.

A Course in Number Theory and Cryptography NEAL Koblitz;

Algebraic Aspects of Cryptography NEAL Koblitz.

8. Minicurrículo do(s) Professor(s)

O professor Luciano Guimarães Monteiro de Castro Possui graduação em Ciencias Matemáticas pela Universidad de Valladolid (1995), e Mestrado em Modelagem Matemática da Informação pela EMAp – FGV. Atualmente é Professor da Fundação Getúlio Vargas e membro da Comissão Nacional de Olimpíadas de Matemática da SBM – IMPA. Tem experiência na área de Matemática, com ênfase em ensino.

9. Link para o Currículo Lattes

http://lattes.cnpq.br/0044915261354363