

INFORMAÇÕES SOBRE TEORIA ARITMÉTICA DOS NÚMEROS- II S/2023

1. INFORMAÇÕES GERAIS

1.1. Pessoas.

- Professor Responsável: Ethan Cotterill (contato: ethan@unicamp.br)
- PAD: A ser determinado

1.2. Aulas e atendimentos.

- Horário de oferecimento: Segundas 21-23, Quartas 19-21
- Horário de Atendimento PAD: a ser determinado
- Atendimento do Prof. Ethan: a ser determinado
- Observação: Notas serão disponibilizadas no Google Classroom.

2. DAS PROVAS

As provas acontecem durante o horário das aulas. Segue um cronograma provisório.

- P1: 13/09/2023
- P2: 01/11/2023
- P3: 04/12/2023
- Exame (E): 13/12/2023

2.1. **Da avaliação final.** A avaliação desta disciplina será baseada nos resultados das provas P1, P2, P3 e (eventualmente) do exame final, onde as notas serão ponderadas como descrito a seguir. Média semestral $MS = 0.2 \cdot P1 + 0.4 \cdot P2 + 0.4 \cdot P3 + A$, onde $0 \leq A \leq 0.3$. O aluno que obtiver $MS \geq 6.0$ estará aprovado e dispensado do exame final. Caso sua MS seja menor que 6,0 sua média será $MF = \min\{6, 0.5 \cdot MS + 0.5 \cdot E\}$, sendo a condição necessária e suficiente para a aprovação $MF \geq 5.0$. Havendo justificativa, uma prova substitutiva será aplicada no dia do exame.

3. EMENTA DO CURSO

Estruturas algébricas (operações binárias, grupos, anéis e corpos).
Axiomas de Peano e construção do anel dos números inteiros e racionais.
Outros exemplos de anéis e corpos (polinômios, corpos quadráticos, inteiros de Gauss, $\mathbb{Z}_m$).
Domínios euclidianos.
Representação de números inteiros em bases diversas.
Máximo divisor comum, mínimo múltiplo comum e o Algoritmo de Euclides.
Elementos irredutíveis e primos e critérios de divisibilidade.

Domínios principais, fatoriais e o teorema fundamental da aritmética.

Equações diofantinas de grau um. Sistemas residuais, congruências lineares e o teorema chinês do resto.

Os teoremas de Euler e Wilson.

Congruências de grau dois, símbolos de Legendre e Jacobi e Lei da Reciprocidade Quadrática.

Ternas pitagóricas e números que podem ser escritos como soma de dois quadrados.

Equações diofantinas notáveis. Ordem multiplicativa e raízes primitivas. Noções de criptografia.

REFERÊNCIAS

- [1] M. Artin, *Algebra*, 2ª edição, Pearson 2010.
- [2] I. Niven, H. Zuckerman, H. Montgomery, *An introduction to the theory of numbers*, 5th Ed., Wiley & Sons, 1991.
- [3] J. Plínio de Oliveira Santos, *Introdução à teoria dos números*, 3ª edição, IMPA 2012.