



---

Teoria Aritmética dos Números

MA553A, 3<sup>a</sup>/5<sup>a</sup>, 08:00–10:00

Plamen Kochloukov

---

Submetido em 13/08/22 19:09

## **Ementa**

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.

## **Teoria**

Nas aulas presenciais serão desenvolvidos os tópicos da ementa. Serão dadas as demonstrações das respectivas afirmações. Serão providenciados exemplos importantes que mostram por que os conceitos e os teoremas são importantes, e quais as aplicações.

## **Prática**

Resolveremos vários exercícios, pois aritmética sem exercícios não tem como fazer. Os alunos receberão listas com exercícios para resolução em casa, e para se prepararem para as avaliações.

## **Atendimento**

A matéria não conta com PAD nem PED. Fixaremos com os alunos dois horários por semana, às terças e quintas, 13:00-14:00 para atendimento. Este será realizado via google meet.

## **Avaliação**

Serão aplicadas três provas, nos dias 22/09, 01/11 e 06/12, com pesos iguais a 3. Serão avaliadas as soluções de exercícios selecionados das listas, estes com peso total 1. Para ser aprovado(a) na matéria, o(a) aluno(a) deverá alcançar média 5. Caso contrário, deverá fazer o exame final, no dia 20/12/2022. A nota final neste caso será a média simples da média final e da nota do exame final.

## **Referências**

1. José P. de Oliveira Santos, Introdução à Teoria de Números, Coleção Matemática Universitária, IMPA, 2003.
2. Abramo Hefez, Elementos de Aritmética, Textos Universitários, SBM, 2006.
3. S. C. Coutinho, Números Inteiros e Criptografia RSA, Série de Computação e Matemática,

IMPA, 1997.

4. G. E. Andrews, Number Theory, Dover Publications, 1971.

5. N. Koblitz, A Course in Number Theory and Cryptography, Springer-Verlag, 1987.

6. I. Niven, H.S. Zuckerman e H.L. Montgomery, An Introduction to the Theory of Numbers, 5th ed., Wiley, 1991.