

PLANO DE DESENVOLVIMENTO DE DISCIPLINA (PDD)

MA553 - Teoria Aritmética dos Números

2º semestre de 2026

Docente responsável	Prof. Dr. Saeed Tafazolian
Horários	Terça-feira, 08:00-10:00; Quinta-feira, 08:00-10:00
Sala	PB11
Contato	tafazolian@ime.unicamp.br
Página da disciplina	https://www.ime.unicamp.br/~tafazolian/node/43

1. 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.

2. Desenvolvimento das atividades teóricas e práticas

A disciplina será desenvolvida em aulas presenciais, às terças e quintas-feiras, com acompanhamento dos conteúdos por notas de aula disponibilizadas na página da disciplina. Serão abordados os tópicos do programa abaixo, incluindo exemplos e exercícios associados aos conteúdos apresentados.

3. Programa

1. Números inteiros, divisibilidade e congruências.
2. Sistemas completos e reduzidos dos restos.
3. Congruências de grau um.
4. Teorema de Fermat, de Euler e aplicações.
5. Sistemas lineares de congruências, teorema chinês dos restos e aplicações.
6. Estruturas algébricas.
7. Equações diofantinas elementares, ternas de Pitágoras e a equação diofantina $x^4 + y^4 = z^4$.
8. Representação de números naturais como soma de quatro quadrados.
9. Congruências de grau dois e símbolo de Legendre.
10. Lei da reciprocidade quadrática e aplicações.
11. Raiz primitiva.

4. Critérios de avaliação

Serão realizadas duas provas obrigatórias, P1 e P2. A média parcial será calculada por:

$$N = (P1 + P2) / 2$$

O critério de avaliação será aplicado da seguinte forma:

- Se $N \geq 5,0$, não haverá necessidade de Exame Final.
- Se $2,5 \leq N < 5,0$, o estudante poderá realizar o Exame Final (P3), abrangendo toda a matéria do curso.
- Para o estudante que realizar P3, define-se $F = (N + P3) / 2$, e a nota final será $NF = \max\{N, F\}$.
- Se $N < 2,5$, o estudante não estará habilitado ao Exame Final, conforme o critério estabelecido para a disciplina.

5. Calendário das avaliações e datas acadêmicas relevantes

Atividade	Data / horário	Observação
P1	29/09/2026 (terça-feira), 08:00-10:00	Conteúdo: pontos 1, 2, 3, 4, 5 e 9 do programa.
Último dia para desistência de matrícula em disciplina	02/10/2026	Data institucional informada pela Graduação.
Avaliação e Discussão de Cursos	20/10/2026 (terça-feira)	Não haverá aula; atividades voltadas à avaliação dos cursos.
P2	26/11/2026 (quinta-feira), 08:00-10:00	Segunda prova obrigatória.
Exame Final (P3)	10/12/2026 (quinta-feira), 08:00-10:00	Conteúdo: toda a matéria do curso.

6. Notas de aula já disponibilizadas

- 11/08: Divisibilidade
- 13/08: O Algoritmo da Divisão
- 18/08: Mínimo Múltiplo Comum e Máximo Divisor Comum
- 20/08: Números Primos e Compostos

7. Hipóteses de substituição de avaliação

O Exame Final ou outra atividade avaliativa poderá, a critério do docente e desde que previsto neste PDD, substituir a avaliação aplicada no dia da ausência do estudante, nas hipóteses indicadas nas orientações da Graduação:

- Abono de faltas previsto no Regimento Geral de Graduação da UNICAMP.
- Atividade de trabalho de campo ou atividade acadêmica obrigatória, mediante documento comprobatório assinado pela Coordenação de Graduação do curso do(a) estudante.
- Apresentação de atestado médico.

A solicitação e a documentação comprobatória deverão observar os procedimentos e prazos institucionais aplicáveis.

8. Cláusula de Honestidade e Lisura Acadêmica

Todas as atividades relacionadas às disciplinas devem ser realizadas em conformidade com as orientações fornecidas pelos docentes e com o devido rigor ético.

Caso o(a) docente responsável, no exercício de sua liberdade de cátedra, forme convicção acerca da ausência de lisura ou de condições adequadas para a realização da atividade avaliativa, poderá atribuir nota zero, seja para a atividade única ou, conforme o caso, para o conjunto de atividades do semestre. A ocorrência deverá ser fundamentada e comunicada à Coordenação de Curso de Graduação, podendo o(a) estudante estar sujeito a processo administrativo.

9. Atendimento extra-classe

O atendimento extra-classe será realizado pelo docente responsável mediante agendamento prévio. Para solicitação de atendimento e esclarecimento de dúvidas, utilizar o e-mail institucional: tafazolian@ime.unicamp.br.

10. Programa de Atendimento Educacional Especializado (PAEE)

Estudantes com deficiência ou transtornos de aprendizagem que necessitem de adaptações didático-pedagógicas podem solicitar apoio por meio do Programa de Atendimento Educacional Especializado (PAEE), em parceria com a DEAPE. Para informações e orientações: pae@unicamp.br.

11. Bibliografia

- José P. de Oliveira Santos, Introdução à Teoria dos Números, Coleção Matemática Universitária, IMPA, 2003.
- Abramo Hefez, Elementos de Aritmética, Textos Universitários, SBM, 2006.
- S. C. Coutinho, Números Inteiros e Criptografia RSA, Série de Computação e Matemática, IMPA, 1997.
- G. E. Andrews, Number Theory, Dover Publications, 1971.

- S. Y. Kim, "An Elementary Proof of the Quadratic Reciprocity Law", American Mathematical Monthly 111, January 2004.
- N. Koblitz, A Course in Number Theory and Cryptography, Springer-Verlag, 1987.
- I. Niven, H. S. Zuckerman e H. L. Montgomery, An Introduction to the Theory of Numbers, 5th ed., Wiley, 1991.
- O. Ore, Number Theory and its History, McGraw-Hill Book Company, Inc., 1948.
- J. P. Serre, A Course in Arithmetic, Springer-Verlag, 1973.
- I. M. Vinogradov, Fundamentos de la Teoría de los Números, Editorial MIR, 1977.
- A. Weil, Number Theory for Beginners, Springer-Verlag, 1979.

12. Informações adicionais

As notas de aula e demais informações da disciplina são disponibilizadas na página do docente indicada no início deste PDD. Alterações estritamente necessárias no cronograma serão comunicadas aos estudantes, respeitando as normas institucionais aplicáveis e os elementos vinculantes deste Plano de Desenvolvimento de Disciplina.

Documento preparado a partir das informações publicadas na página da disciplina MA553 e das orientações institucionais de PDD/Graduação para o 2º semestre de 2026.