UNIVERSIDADE FEDERAL DO ABC

Centro de Matemática, Computação e Cognição – CMCC

Plano de Ensino

Docente:

Felipe de Aguilar Franco
Sala 515-2 Bloco A – Campus Santo André
f.franco@ufabc.edu.br

Disciplina:

MCTB023-17 Teoria Aritmética dos Números.

Turma:

TNA1MCTB023-17SA

Quadrimestre:

Q3/2024

Horário e local das aulas:

Terças 19h–21h e Quintas 21h–23h na sala S-301-2 Bloco A – Campus Santo André

Atendimento:

Terças 16h–17h e Quintas 18h15–19h15 na sala 515-2 Bloco A – Campus Santo André

Objetivo:

Descrever o conjunto dos números inteiros com sua estrutura de ordem e suas operações aritméticas. Desenvolver a noção de divisibilidade e conceitos subjacentes: MDC, MMC, números primos. Deduzir e aplicar o Teorema Fundamental da Aritmética. Compreender a representação de inteiros numa base arbitrária. Classificar e resolver equações diofantinas lineares. Manipular congruências módulo m e operar em aritmética modular. Classificar e resolver congruências lineares e sistemas de congruências lineares. Explicar e aplicar teoremas clássicos envolvendo congruências.

Ementa:

Divisibilidade. O algoritmo da divisão. MDC e MMC. Teorema Fundamental da Aritmética. Sistemas de numeração. Representação de um número numa base arbitrária. Mudança de base. Equações diofantinas lineares. Ternos Pitagóricos.

Classes de congruência e sistemas completos de restos módulo m. Aplicações: critérios de divisibilidade. Congruências lineares: condições para existência e cálculo de soluções. Sistemas de congruências e o Teorema Chinês de Restos. A função phi de Euler, o Teorema de Euler e o Pequeno Teorema de Fermat. Teorema de Wilson.

Metodologia:

Aulas expositivas, listas de exercícios e solução de problemas em sala.

Avaliação:

Serão aplicadas três provas escritas, $P1$, $P2$ e $P3$, com duração de 1h40. Também serão disponibilizados três conjuntos de listas, $L1$, $L2$ e $L3$. Serão atribuídos conceitos aos conjuntos individuais $(Pi + Li)$ e ao conjunto de atividades $((P1 + L1)+(P2+L2)+(P3+L3))$ será atribuído um conceito em acordo com o estabelecido na Resolução ConsEPE n^o 147.

Caso a frequência tenha sido maior ou igual a 75%, o conceito atribuído ao conjunto $((P1 + L1) + (P2 + L2) + (P3 + L3))$ será o conceito obtido na disciplina; caso a frequência tenha sido inferior a 75%, será atribuído o conceito final O.

Provas Substitutiva:

No dia **19/12/24**, quinta-feira, serão aplicadas provas substitutivas a quem não pôde comparecer a alguma das provas $P1$, $P2$ ou $P3$, em virtude de circunstância contemplada no Art. 2o da Resolução ConsEPE no 227.

Exame de recuperação:

Na segunda semana do quadrimestre seguinte (em data, horário e local a serem divulgados), será realizado o *exame de recuperação*, uma prova escrita, com duração de 1h40min, que compreenderá todo o conteúdo da disciplina. A participação no exame de recuperação é facultativa; qualquer estudante que tiver atingido a frequência mínima de 75% poderá optar por fazer o exame de recuperação. Ao conjunto de avaliações $((P1 + L1) + (P2 + L2) + (P3 + L3) + R)$ juntamente com o exame de recuperação, será atribuído um conceito, sendo considerado prioritariamente o desempenho no exame de recuperação. Este será o conceito final obtido na disciplina, desde que superior ao conceito obtido anteriormente; caso contrário, o conceito original será mantido.

Cronograma Aproximado:

01/10 (Ter)	Apresentação do Curso; Números inteiros; Princípio da Boa Ordem
03/10 (Qui)	Indução Finita; Algoritmo da divisão
08/10 (Ter)	MDC e MMC; Algoritmo da divisão euclidiana
10/10 (Qui)	Divisibilidade
15/10 (Ter)	Equações diofantinas lineares
17/10 (Qui)	Aplicações
22/10 (Ter)	Revisão
24/10 (Qui)	***P*1**
29/10 (Ter)	Números Primos
31/10 (Qui)	Teorema fundamental da aritmética
05/11 (Ter)	Crivo de Erastóstenes
07/11 (Qui)	Congruências
12/11 (Ter)	Representações de números inteiros
14/11 (Qui)	Critérios de divisibilidade; Aplicações
19/11 (Ter)	***P*2**
21/11 (Qui)	Sistemas de congruências lineares
26/11 (Ter)	Teorema do Resto Chinês; Aplicações
28/11 (Qui)	A função ϕ de Euler e o Teorema de Euler
03/12 (Ter)	Teorema de Euler
05/12 (Qui)	Pequeno Teorema de Fermat
10/12 (Ter)	Teorema de Wilson
12/12 (Qui)	Revisão
17/12 (Ter)	***P*3**
19/12 (Qui)	**Prova Substitutiva**

Bibliografia Básica:

• BURTON, D. Elementary Number Theory. 7th ed. Boston: McGraw-Hill, 2011.
• POLCINO, C. M.; COELHO, S. P. Números: uma introdução à matemática. 3. ed. São Paulo: Edusp, 2001.
• HEFEZ, A. Elementos de Aritmética. 2. ed. Rio de Janeiro: SBM, 2006.

Bibliografia Complementar:

• SANTOS, J. P. O. Introdução à Teoria dos Números. 3. ed. Rio de Janeiro: IMPA, 1998.
• NIVEN, I. M.; ZUCKERMAN, H.S.; MONTGOMERY, H. L. An Introduction to the Theory of Numbers. 5th ed. New York: Wiley, 1991.
• COUTINHO, S. C. Números inteiros e criptografia RSA. Rio de Janeiro: IMPA, 2009.
• FIGUEIREDO, D. G. Números Irracionais e Transcendentes. Rio de Janeiro: SBM, 2003.

• ORE, O. Number Theory and its History. New York: Dover Publications, 1988.