



UNIVERSIDADE FEDERAL DA BAHIA
PRÓ-REITORIA DE ENSINO DE GRADUAÇÃO

PLANO DE ENSINO-
APRENDIZAGEM DO COMPONENTE
CURRICULAR
Semestre 2023.1

DADOS DE IDENTIFICAÇÃO E ATRIBUTOS¹

CÓDIGO		NOME					DEPARTAMENTO OU EQUIVALENTE					
MATB32		INTRODUÇÃO À TEORIA DOS NÚMEROS					DEPARTAMENTO DE MATEMÁTICA					
CARGA HORÁRIA (estudante)							MODALIDADE/ SUBMODALIDADE			PRÉ-REQUISITO (POR CURSO)		
T	T/P	P	PP	Ext	E	TOTAL	DISCIPLINA/TEÓRICA			SEM PRÉ-REQUISITO		
60	-	-	-	-	-	60						
CARGA HORÁRIA (docente/turma)							MÓDULO			SEMESTRE DE INÍCIO DA VIGÊNCIA		
T	T/P	P	PP	Ext	E	TOTAL	T	T/ P	P	PP	Ex t	E
60	-	-	-	-	-	60	45	-	-	-	-	-
										2023.1		

EMENTA

Números naturais. Números inteiros. Divisibilidade nos inteiros e algoritmo da divisão de Euclides. Máximo divisor comum. Mínimo divisor comum. Equações diofantinas lineares. Números primos e o Teorema Fundamental da Aritmética. O Pequeno Teorema de Fermat. Primos de Fermat e de Mersenne. Congruências. Teoremas de Euler e de Wilson. Teorema chinês do resto. Criptografia RSA.

OBJETIVOS

OBJETIVO GERAL

Introduzir os principais tópicos de aritmética e teoria elementar dos números.

OBJETIVOS ESPECÍFICOS

- Estudar as principais propriedades dos números naturais, tais como os axiomas de Peano, princípios de indução, sistema posicional e o Teorema Fundamental da Aritmética.
- Compreender as propriedades dos números inteiros relacionadas à divisibilidade, tais como algoritmo da divisão de Euclides, máximo divisor comum e mínimo múltiplo comum.
- Resolver equações diofantinas lineares.
- Estudar os teoremas clássicos da aritmética dos números inteiros, relacionados a números primos e divisibilidade, tais como Teorema de Fermat, Teorema de Euler e Teorema de Wilson.
- Aplicar o teorema chinês do resto para resolver sistemas de congruências lineares.
- Introduzir noções de criptografia RSA.

¹ Os "dados de identificação e atributos" devem estar registrados conforme especificado no Programa do Componente Curricular e disponível no site da Superintendência Acadêmica (SUPAC)SIAC. O único campo a ser preenchido nesse tópico do formulário é o que diz respeito ao módulo de vagas ofertadas.

CONTEÚDO PROGRAMÁTICO

1. Números naturais:

- 1.1. Números naturais como cardinais de conjuntos finitos.
 - 1.1.1. Operações aritméticas.
- 1.2. Axiomas de Peano.
- 1.3. Relação de ordem.
- 1.4. Princípio da boa ordem.
- 1.5. Princípio de indução finita.
- 1.6. Representação numérica dos números naturais:
 - 1.6.1. O sistema romano.
 - 1.6.2. O sistema babilônico.
 - 1.6.3. O sistema egípcio.
 - 1.6.4. O sistema decimal.

2. Números inteiros:

- 2.1. A construção dos números inteiros.
- 2.2. Princípio da boa ordem.
- 2.3. Ordem.
- 2.4. Princípio de indução matemática.
- 2.5. Operações aritméticas e propriedades básicas:
 - 2.5.1. Adição, subtração, multiplicação, divisão e potenciação.
 - 2.5.2. Valor absoluto.

3. Divisibilidade nos inteiros e algoritmo da divisão de Euclides:

- 3.1. Propriedades da divisibilidade.
- 3.2. Algoritmo da divisão de Euclides.
- 3.3. Bases e representação numérica.

4. Máximo Divisor Comum (MDC):

- 4.1. Lema de Euclides.
- 4.2. Teorema de Bézout.
- 4.3. Algoritmo de Euclides para o cálculo de MDC.
- 4.4. MDC e os números de Fibonacci.

5. Mínimo Múltiplo Comum (MMC):

- 5.1. Propriedades do MMC.
- 5.2. Relação entre MDC e MMC.

6. Equações diofantinas lineares.

7. Números primos e o Teorema Fundamental da Aritmética:

- 7.1. Teorema Fundamental da Aritmética.
- 7.2. Crivo de Eratóstenes.

8. O Pequeno Teorema de Fermat (PTF).

9. Primos de Fermat e de Mersenne:

- 9.1. Números de Fermat.
- 9.2. Números de Mersenne.
- 9.3. Teorema de Dirichlet.
- 9.4. Números perfeitos.

10. Congruências:

- 10.1. As classes de restos módulo m .
- 10.2. Operações aritméticas com congruências.
- 10.3. Sistema reduzido de resíduos módulo m e sistema completo de resíduos módulo m .
- 10.4. Aplicações de congruência.
- 10.5. Critérios de divisibilidade.

11. Teoremas de Euler e de Wilson:

- 11.1. A função de Euler.
 - 11.2. Teorema de Euler.
 - 11.3. Teorema de Wilson.
-

12. Teorema chinês do resto:

- 12.1. Congruências lineares.
- 12.2. Sistemas de congruência lineares.
- 12.3. Teorema chinês do resto.

13. Criptografia RSA.

METODOLOGIA DE ENSINO-APRENDIZAGEM

Aulas expositivas e aulas de discussão.

AVALIAÇÃO DA APRENDIZAGEM

- $MF = \frac{N_1 + N_2 + N_3}{10}$, sendo MF (média final) é dada pela média aritmética das notas N_1, N_2, N_3 atribuídas às avaliações das 3 unidades, respectivamente.
Se $MF \geq 5,0$, o aluno está aprovado com essa média.
- A ausência em qualquer uma das avaliações será atribuída a nota ZERO.

REFERÊNCIAS

REFERÊNCIAS BÁSICAS

1. HEFEZ, Abramo. **Elementos de Aritmética**. 2. ed. Niterói, RJ: SBM, 2006.
2. MONTEIRO, Luiz Henrique Jacy. **Elementos de Álgebra**. Rio de Janeiro, RJ: Ao Livro Técnico, 1969.
3. SANTOS, José Plínio de Oliveira. **Introdução à Teoria dos Números**. 3. ed. Rio de Janeiro, RJ: IMPA, 2006.

REFERÊNCIAS COMPLEMENTARES

1. BURTON, David M. **Elementary Number Theory**. Boston, USA: Allyn and Bacon, 1980.
2. COUTINHO, Severino C. **Números Inteiros e Criptografia RSA**. 2. ed. Rio de Janeiro, RJ: IMPA, 2000.
3. DOMINGUES, Hygino Hugueros. **Fundamentos de Aritmética**. São Paulo, SP: Atual, 1991.
4. HEFEZ, Abramo. **Curso de Álgebra**. 2. ed. Rio de Janeiro, RJ: IMPA, 1997.
5. LANDAU, Edmund Georg Hermann. **Elementary Number Theory**. New York, USA: Chelsea, 1958.
6. MILIES, César Polcino; COELHO, Sônia Pitta. **Números: uma introdução à Matemática**. 3. ed. São Paulo, SP: EDUSP, 2013.
7. NIVEN, Ivan. **Números: racionais e irracionais**. Rio de Janeiro, RJ: SBM, 1984.

Aprovado em reunião de Departamento (ou equivalente): _____ em ____/____/____
Assinatura do Chefe do Departamento/ Coordenador Acadêmico

2 O plano de ensino-aprendizagem é um documento que tramita internamente na Unidade acadêmica (especificamente no departamento ou coordenação acadêmica), não sendo necessário encaminhá-lo à Prograd nem à Supac, após aprovação pela instância responsável.



Emitido em 23/05/2023

PROGRAMA E EMENTA Nº 1413/2023 - CAT/IME (12.01.17.14)

(Nº do Protocolo: NÃO PROTOCOLADO)

(Assinado eletronicamente em 23/05/2023 18:15)

JOILSON OLIVEIRA RIBEIRO

CHEFE - TITULAR

DM/IME (12.01.17.03)

Matrícula: ###656#0

(Assinado eletronicamente em 23/05/2023 15:39)

JOSEPH NEE ANYAH YARTEY

PROFESSOR DO MAGISTERIO SUPERIOR

DM/IME (12.01.17.03)

Matrícula: ###216#7

Para verificar a autenticidade deste documento entre em <https://sipac.ufba.br/public/documentos/> informando seu número: **1413**, ano: **2023**, tipo: **PROGRAMA E EMENTA**, data de emissão: **23/05/2023** e o código de verificação: **1d37a2729a**