

# PLANO DE ENSINO

## Aritmética – MA 14 (PROFMAT)

Prof. Ercílio Carvalho da Silva

2° Semestre – 2023

### Ementa

Os números inteiros. Aplicações da indução. Divisão nos inteiros. Representação dos números inteiros. Algoritmo de Euclides. Aplicações do máximo divisor comum. Números primos. Números especiais. Congruências. Os teoremas de Euler e Wilson. Congruências lineares e classes residuais. Congruências quadráticas. Noções de criptografia.

### Referência Bibliográfica

1. HEFEZ, A.; FERNANDEZ, C.S. **Introdução à álgebra linear**. SBM, 2016 (Coleção PROFMAT).
2. HEFEZ, A. **Exercícios resolvidos de Aritmética**. SBM, 2016 (Coleção PROFMAT).
3. PROFMAT, MA14 – **Aritmética**. Disponível em: . Acesso: 04 jan. 2017.

### Programa

1. Números inteiros: a adição e a multiplicação. Ordenação dos inteiros. Princípio da boa ordenação
2. Aplicação da indução: definição por recorrência. Binômio de Newton. Aplicações lúdicas
3. Divisão nos inteiros: divisibilidade. Divisão euclidiana. A aritmética na Magna Grécia
4. Representação dos números inteiros: sistema de numeração. Jogo de Nim
5. Algoritmo de Euclides: máximo divisor comum. Propriedades do MDC
6. Algoritmo de Euclides: algoritmo de Euclides estendido. Mínimo múltiplo comum. A equação pitagórica
7. Aplicações do máximo divisor comum: equações diofantinas lineares
8. Aplicações do máximo divisor comum: expressões binômias. Números de Fibonacci

9. Números primos: teorema fundamental da aritmética. Sobre a distribuição dos números primos
10. Números primos: pequeno teorema de Fermat
11. Números primos: o renascimento da Aritmética
12. Números especiais: primos de Fermat, de Mersenne e em PA
13. Números especiais: números perfeitos
14. Números especiais: decomposição do fatorial em primos. A equação  $E_p(x!) = \alpha$
15. Congruências: aritmética dos restos. aplicações
16. Congruências: congruências e números binomiais. O calendário
17. Os teoremas de Euler e de Wilson: teorema de Euler. Teorema de Wilson
18. Congruências lineares e classes residuais: resolução de congruências lineares. Teorema chinês dos restos
19. Congruências lineares e classes residuais: Classes residuais
20. Congruências quadráticas: congruências quadráticas. Resíduos quadráticos
21. Congruências quadráticas: somas de quadrados
22. Congruências quadráticas: lei da reciprocidade quadrática
23. Noções de criptografia: as origens da criptografia
24. Noções de criptografia: o advento dos computadores. A grande revolução: O sistema RSA

### Cronograma

Aula	Dia/Mês	Semana	Conteúdo
01	11/Ago	11 / Q2	Números inteiros Indução: 1° PIF
02	18/Ago	12 / Q2	Indução: 2° PIF e PMI (PBO) Divisibilidade
03	25/Ago	Recesso	Algoritmo da Divisão Sistemas de Numeração
04	01/Set	Recesso	MDC Identidade de Bezout Algoritmo de Euclides

05	08/Set	Recesso	Equações Diofantinas Lineares MMC
06	15/Set	Recesso	Teorema Fundamental da Aritmética Teste de primalidade
07	22/ Set	01 / Q3	Primos de Fermat e de Mersenne Infinitude dos primos Primos em uma PA
08	29/Set	02 / Q3	<b>Prova 1</b>
09	06/Out	03 / Q3	Congruências
10	13/Out	04 / Q3	FERIADO ( <i>Padroeira do Brasil - 12 a 14/Out</i> )
11	20/Out	05 / Q3	Pequeno Teorema de Fermat Teorema de Euler Teorema de Wilson
12	27/Out	06 / Q3	Congruências lineares Sistema de congruências Teorema Chinês de Restos
13	03/Nov	07 / Q3	FERIADO ( <i>Finados – 02 a 04/Nov</i> )
14	10/Nov	08 / Q3	Congruências quadráticas Resíduos quadráticos
15	17/Nov	09 / Q3	Soma de quadrados Lei da Reciprocidade (Feriado na 4 <sup>a</sup> -feira)
16	24/Nov	10 / Q3	Criptografia: fundamentos e o método RSA
17	01/Dez	11 / Q3	<b>Prova 2</b>
18	08/Dez	12 / Q3	<b>Prova de Recuperação</b>

**Observação:** Essa programação poderá sofrer alterações ao longo semestre!

### Sistema de Avaliação

- Será composto de **2 Provas** (presenciais) e alguns **Testes no Moodle**, com pesos de 80% e 20%, respectivamente.
- **Provas substitutivas** serão aplicadas apenas para quem perdeu e que tenha alguma justificativa legal (atestado). Será agendado uma data específica e poderá ocorrer fora do horário da aula.

## Notas e Conceitos

- $MF = 0,8 \times (\text{m\u00e9dia das Provas}) + 0,2 \times (\text{m\u00e9dia dos Testes})$

MF	Conceito
$0 \leq MF < 5$	F
$5 \leq MF < 7$	C
$7 \leq MF < 8,5$	B
$8,5 \leq MF \leq 10$	A

## Sobre a aprova\u00e7\u00e3o na disciplina

O aluno ser\u00e1 considerado aprovado se, **obrigatoriamente**, satisfizer as seguintes condi\u00e7\u00f5es:

- **A nota em cada uma das provas deve ser maior ou igual a 4**
- **$MF \geq 5$**

## Recupera\u00e7\u00e3o

Apenas para os alunos que ficaram com o Conceito F.

Nesse caso o aluno dever\u00e1 recuperar em pelo menos uma das provas, conforme for o caso e o conceito m\u00e1ximo atribuído ser\u00e1 C.