UNIVERSIDADE FEDERAL DE CAMPINA GRANDE
Programa de Pós-Graduação em Matemática
Mestrado Profissional - PROFMAT/CCT/UFCG

Renato Machado de Sousa

Produto Educacional

# UMA PROPOSTA DE ENSINO DA ARITMÉTICA POR MEIO DE SEQUÊNCIAS DIDÁTICAS

Campina Grande - PB
09/2024

UNIVERSIDADE FEDERAL DE CAMPINA GRANDE
Programa de Pós-Graduação em Matemática
Mestrado Profissional - PROFMAT/CCT/UFCG

Renato Machado de Sousa

# UMA PROPOSTA DE ENSINO DA ARITMÉTICA POR MEIO DE SEQUÊNCIAS DIDÁTICAS

Produto Educacional vinculado ao Trabalho de Conclusão de Curso apresentado ao Corpo Docente do Programa de Pós-Graduação em Matemática - CCT - UFCG, na modalidade Mestrado Profissional, como requisito parcial para obtenção do título de Mestre.

Orientador: Dr. José Fernando Leite Aires
Coorientador: Dr. Leomaques Francisco Silva Bernardo

Campina Grande - PB
09/2024

# Resumo

Este produto educacional propôs uma abordagem do ensino da Aritmética por meio de sequências didáticas, explorando conceitos, definições e propriedades relevantes para promover as aprendizagens essenciais, com o objetivo de desenvolver alternativas metodológicas e teóricas inovadoras para melhorar a compreensão e o engajamento dos alunos em relação aos tópicos da Aritmética. A metodologia adotada neste produto envolveu uma abordagem qualitativa e implementação de sequências didáticas. Os resultados demonstraram um aumento na participação dos alunos, melhor compreensão dos conceitos abordados e um ambiente de aprendizagem mais dinâmico e interativo. Este estudo procurou oferecer uma contribuição relevante ao processo de ensino e aprendizagem da Matemática, evidenciando a eficácia da integração de abordagens teóricas e práticas no ensino da Aritmética, promovendo um aprendizado mais envolvente e eficaz.

**Palavras-chave**: Produto Educacional. Sequência Didática. Metodologias. Aritmética.

# Sumário

# 1 Introdução

A sequência didática que será apresentada neste texto é fruto de uma pesquisa desenvolvida para o trabalho de conclusão de curso do Mestrado Profissional em Matemática - PROFMAT na Universidade Federal de Campina Grande. A sequência didática foi composta por sete encontros, ocorridos aos sábados das 9 h às 12 h, aplicado em uma turma do 3º ano do Ensino Médio da Escola Estadual de Ensino Fundamental e Médio Major Veneziano Vital do Rêgo na cidade de Campina Grande-PB, as quais planejamos os objetivos e procedimentos necessários para alcançá-los. Sendo assim, realizamos a exposição da unidade temática, modalidade/nível de Ensino, objetos de conhecimento, habilidades, objetivos/expectativas de Aprendizagem, estratégia de Ensino, materiais utilizados e a duração das atividades em cada encontro da sequência desenvolvida.

Visando contribuir com o ensino e aprendizado significativo da Aritmética, neste produto educacional recorremos à sequência didática. De acordo com (ARAÚJO, 2013) e (ZABALA, 1998), é necessário organizar as atividades de forma a incluir todos nossos alunos, cumprindo todas as etapas e objetivos que devem ser alcançados. Em nosso trabalho de conclusão de curso tivemos a oportunidade de aplicar e discutir alguns resultados da sequência didática que serão propostas aqui. Para mais detalhes, veja a dissertação intitulada, UMA PROPOSTA DE ENSINO DA ARIMÉTICA POR MEIO DE SEQUÊNCIAS DIDÁTICAS: UM PASSEIO PELA HISTÓRIA, CONCEITOS E APLICAÇÕES (SOUSA, 2024).

## 1.1 A relevância do tema e sua contextualização no Ensino Médio

A Aritmética é uma área da Matemática fundamental presente no currículo do Ensino Médio, e o estudo dos conceitos, definições, assim como das propriedades, pode desempenhar um papel na formação Matemática dos alunos, amplificando os conhecimentos preliminares estudados no Ensino Fundamental e estimulando novas aprendizagens. Esses conteúdos permitem a compreensão das definições e as relações entre as propriedades numéricas, desenvolvendo o raciocínio lógico e a capacidade de resolução de situações-problema. Além disso, essa abordagem específica destaca o compromisso do currículo em fornecer uma formação Matemática abrangente e relevante para os alunos, preparando-os para enfrentar os desafios acadêmicos e práticos que surgem no Ensino Médio.

# 2 Objetivos

## 2.1 Gerais

O objetivo geral deste produto educacional é promover aos alunos do Ensino Médio uma retomada sobre os conhecimentos aritméticos, definições e propriedades com o intuito de proporcionar um ensino de qualidade. Projeta-se que, ao final dos encontros, os alunos sejam capazes de tomar decisões independentes e sejam protagonistas do conhecimento aritmético. Além disso, oferecer o desenvolvimento das habilidades e competências matemáticas estabelecidas na Base Nacional Comum Curricular (BRASIL, 2018) e na Proposta Curricular do Novo Ensino Médio da Paraíba (PARAÍBA, 2021), colaborando, significativamente, para a formação dos alunos.

## 2.2 Específicos

Almeja-se que, os alunos desenvolvam as seguintes habilidades com o nosso produto educacional:

- Definir os números naturais em compostos e primos;
- Aplicar os critérios de divisibilidade ;
- Compreender e descrever os algoritmos da divisão e de Euclides para encontrar o (MDC);
- Resolver e explorar problemas contextualizados envolvendo os números inteiros;
- Investigar e aplicar algoritmos aritméticos envolvendo à linguagem de programação Python;
- Compreender e associar as ideias de matrizes, determinantes e Criptografia, no intuito de codificar e decodificar mensagens.
- Abordar os conceitos trabalhados durante os encontros por meio de um jogo intitulado “Trilha da Aritmética ”.

# 3 Referenciais Teóricos

Na Base Nacional Comum Curricular (BRASIL, 2018) para o Ensino Fundamental II e Médio e na Proposta Curricular do Novo Ensino Médio da Paraíba (PARAÍBA, 2021), a Matemática é vista como uma área do conhecimento que promove a compreensão da sociedade, a investigação de fenômenos do cotidiano e o desenvolvimento do raciocínio lógico. Com relação ao ramo da Aritmética, a BNCC destaca a importância de explorar e compreender as relações entre os conceitos, as propriedades e a aplicação dos números, o que contribui para a formação de alunos independentes, críticos e capazes de ser protagonistas do ensino e aprendizagem de qualidade.

## 3.1 Base Nacional Comum Curricular (BNCC) e Proposta Curricular do Novo Ensino Médio da Paraíba (PCEMPB)

A BNCC (BRASIL, 2018), enquanto um guia normativo, desempenha um papel crucial ao apontar-nos em direção a conteúdos essenciais para o sucesso no ambiente de trabalho e no cenário da produção científica do aluno. Este documento visa não apenas fornecer uma estrutura educacional consistente, mas também orientar o processo de aprendizagem em direção as habilidades e conhecimentos que são não apenas pertinentes ao contexto acadêmico, mas também fundamentais para o êxito no mundo profissional e na contribuição para avanços científicos. Dessa forma, a BNCC (BRASIL, 2018) se posiciona como uma ferramenta orientadora que busca alinhar a formação educacional às exigências da sociedade contemporânea, preparando os estudantes para os desafios e oportunidades do mundo do trabalho e da pesquisa científica.

As unidades temáticas que serão abordadas neste produto educacional são os números e a álgebra, e os objetos de conhecimento são operações tais como: adição, subtração, multiplicação e divisão euclidiana, a fim de auxiliar na resolução de problemas do dia a dia. Entendendo a Aritmética de forma eficiente podemos então trabalhar outros conteúdos de forma mais abrangente, e abordar consequentemente, os conteúdos de forma mais dinâmica.

A BNCC (BRASIL, 2018) estabelece que ao longo da Educação Básica, 10 competências gerais devem ser desenvolvidas e aprimoradas. Estas competências abrangem áreas como conhecimento, pensamento científico, crítico e criativo, repertório cultural, habilidades de comunicação, cultura digital, além de focar em aspectos como trabalho e projeto de vida, argumentação, autoconhecimento e autocuidado, empatia, operação, responsabilidade e cidadania. Também propõe uma abordagem holística e abrangente

para o desenvolvimento integral dos alunos ao longo de sua jornada educacional. Além das 10 competências, são necessárias habilidades que capacitam o aluno a ser independente na busca pelo conhecimento e a desempenhar um papel ativo como protagonista de sua própria trajetória.

As habilidades relacionadas à Aritmética, no âmbito da Proposta Curricular do Novo Ensino Médio da Paraíba (PARAÍBA, 2021), estão apresentadas no documento normativo. Estas habilidades delineiam os objetivos específicos e as competências que os alunos devem adquirir no que diz respeito à Aritmética, com o objetivo de desenvolver sua compreensão e a capacidade de aplicação desses conceitos.

Essa abordagem específica destaca o compromisso do currículo em fornecer uma formação Matemática abrangente e relevante para os alunos, preparando-os para enfrentar os desafios acadêmicos e práticos que surgem no Ensino Médio. Vale destacar que tais habilidades serão abordadas em virtude do estudo e aplicação da Criptografia por meio da Aritmética, matrizes e determinantes.

### 3.1.1 Competências específicas

- Admitir que a Matemática é uma ciência fundamental para as relações culturais e históricos, e uma ciência viva, que contribui significativamente, para resolver problemas do cotidiano e tecnológicos, inclusive com relação ao mundo do trabalho e ao acadêmico;

- Desenvolver a capacidade de investigação e do raciocínio lógico, produzindo argumentos técnicos e um conhecimento para compreender o mundo em que vivemos;

- Compreender as relações entre conceitos e propriedades na área da Matemática (Aritmética) e de outras áreas do conhecimento, no sentindo de promover um conhecimento matemático e desenvolver as habilidades de perseverança e autoestima dos alunos;

- Utilizar os processos matemáticos, com o uso de tecnologias digitais, para proporcionar a aplicação de algoritmos eficientes para resolver problemas do cotidiano;

- Propor estratégias, conceitos, definições e procedimentos matemáticos para interpretar, construir modelos e resolver problemas em diversos contextos no dia a dia dos alunos.

### 3.1.2 Habilidades relacionadas a BNCC e ao PCEMPB

- **(EF06MA05)** Definir os números naturais em compostos e primos, estabelecer relações entre números, expressas pelos termos "é múltiplo de", " é divisor de", " é fator de " , e estabelecer, por meio de investigações critérios de divisibilidade por: 2, 3, 4, 5, 6, 7, 8, 9, 10, 100 e 1000;
- **(EF06MA06)** Resolver e elaborar problemas que envolvam as ideias de múltiplo e divisor;
- **(EF07MA01)** Resolver e elaborar problemas com números naturais, envolvendo as noções de divisor e de múltiplo, podendo incluir máximo divisor comum ou mínimo múltiplo comum, por meio de estratégias diversas, sem a aplicação de algoritmos;
- **(EF07MA04)** Resolver e elaborar problemas que envolvam operações com números inteiros;
- **(EM13MAT405)** Utilizar conceitos iniciais de uma linguagem de programação na implementação de algoritmos escritos em linguagem corrente e/ou matemática;
- **(EM13MAT410)** Associar o conceito de matrizes, determinantes e sistemas de equações lineares às situações nas quais são utilizadas planilhas eletrônicas;
- **(EM13MAT411)** Reconhecer um sistema de equações associado a uma matriz com o intuito de resolver situações problemas.

# 4 Desenvolvimento da sequência didática

Neste capítulo, apresentamos como foi organizada nossa sequência didática, a qual foi dividida em sete encontros envolvendo conteúdos da Aritmética, onde abordamos um breve contexto histórico da temática assim como algumas aplicações relacionadas com o tema. O principal objetivo em uma sala de aula é agregar novos conhecimentos aos alunos.

> Por educar entendemos atuar junto ao sujeito visando seu integral desenvolvimento; já ensinar para nós é agir de forma a possibilitar ao educando o acesso ao conhecimento, intermediando sua busca por novos horizontes em direção à cidadania.(BALESTRA, 2012, p.24)

De acordo com (ARAÚJO, 2013), as Sequências Didáticas são modos do professor organizar suas atividades educacionais por meio de temas e procedimentos a serem aplicados. Dessa forma, o professor precisa buscar formas de incluir os alunos em todos os âmbitos da aprendizagem, desde a elaboração de uma aula até o seu resultado, que é o aprendizado do conteúdo estudado. O aluno precisa enxergar o que aquele aprendizado terá de útil em sua vida, pois assim terá cada vez mais interesse em aprender. Com isso, é muito importante que o professor ouça os seus educandos, e assim busque alternativas para estimular o interesse e a busca por conhecimento.

Corroborando com esse pensamento, (ZABALA, 1998, p.18) afirma que sequência didática é "um conjunto de atividades ordenadas, estruturadas e articuladas para a realização de certos objetivos educacionais, que têm um princípio e um fim conhecido tanto pelos professores como pelos alunos". Assim, compreendemos que a sequência didática se refere à organização de atividades bem planejadas com o intuito de tornar as aulas mais atraentes para os alunos e assim instiguem-os a vivenciar essas práticas no seu próprio cotidiano.

A sequência didática aplicada foi organizada da seguinte forma: nos sábados das 9 h às 12 h, com tempo estimado de cada encontro de 3 h, planejada para ser executada em 7 encontros. Vale ressaltar que o tempo pedagógico pode ser ajustado de acordo com a necessidade e o nível de cada turma.

**Sequência Didática I – Encontro 01**

Neste primeiro momento, introduzimos a História da Aritmética, mas especificamente, na Pré-História em que o homem passar a ter contato com a ideia de contagem, e consequentemente, passando a associar número com objetos, a fim de promover uma sociedade mais desenvolvida.

A ideia de números remonta a aproximadamente 30.000 anos atrás com a preocupação de registrar a quantidade de familiares, de animais e de objetos importantes para uma determinada comunidade tribal (HYGINO, 1991).

Um dos principais recursos para a contagem eram pedras, galhos, dedos das mãos, e as vezes até dos pés, para indicar a quantidade de elementos e posteriormente veio uma escrita rudimentar em paredes associando números com objetos. Este fato foi muito relevante para que estas informações fossem armazenadas e transmitidas para as gerações seguintes.

Mas o avanço do conceito de contagem de número ocorreu de forma lenta e em etapas difíceis de estipular. Por exemplo, o símbolo ou o som que foi empregado primeiro? Segundo (HYGINO, 1991), provavelmente, os símbolos surgiram primeiro com a intenção de representar os objetos, pessoas e animais para depois os sons serem utilizados e abordados para cada situação.

A primeira civilização a aplicar estes símbolos foram as pessoas que viviam nos vales dos Rio Nilo, Tigres e Eufrades. Mas temos registros também nos vales Indo e Yangtse Kiang na China a cerca de 6000 anos.

Podemos observar que estes símbolos foram fundamentais para a criação dos números naturais, inteiros, operações e suas propriedades.

Figura 1 – Rio Nilo


Fonte:<https://escolakids.uol.com.br/geografia/rio-nilo.htm>

Figura 2 – Rio Indo


Fonte:<https://blogcatedranaval.com/tag/rio-indo>

Figura 3 – Rio Yangtse


Fonte:<https://kids.britannica.com/kids/article/Yangtze-River/353943>.

Os números naturais foram representados ao longo da história de diversas formas diferentes. Mas, para este trabalho, convencionaremos o conjunto dos números naturais da seguinte forma:

$\mathbb{N} = \{0, 1, 2, \cdots\}$.

Já o conjunto dos números inteiros da seguinte maneira:

$\mathbb{Z} = \{\cdots, -2, -1, 0, 1, 2, \cdots\}$.

As definições apresentadas a seguir estão baseadas nos livros Programa de Iniciação Científica da OBMEP e o Livro de Aritmética utilizado no programa PROFMAT. Para maiores detalhes veja (HEFEZ, 2009) e (HEFEZ; ARITMÉTICA, 2009).

**Definição de múltiplo de um número natural:**

Dado um número natural $a$, consideremos o conjunto dos múltiplos naturais de $a$:

$$a\mathbb{N} = \{a \cdot d \mid d \in \mathbb{N}\}.$$

**Múltiplos Comuns:**

Considere o conjunto dos múltiplos de $3 = \{0, 3, 6, 9, 12, \cdots\}$ e o conjunto dos múltiplos $5 = \{0, 5, 10, 15, 20, \cdots\}$.

Portanto, o conjunto que representa os múltiplos comuns de 3 e 5 é mostrado abaixo: $\{0, 15, 30, 45, 60, \cdots\}$.

**Definição de Múltiplos Comuns:**

Os números que pertencem simultaneamente ao conjunto dos múltiplos de dois ou mais números dados será chamado de múltiplos comuns destes números.

**Observação:** Se $a$ e $b$ são números naturais não nulos, sabemos que o número $a \cdot b$ é um múltiplo de $a$; por outro lado, pela propriedade comutativa da multiplicação, tem-se que ele também um múltiplo de $b$. Assim, o conjunto dos múltiplos comuns de $a$ e $b$, além de conter o número 0, contém também o número $a \cdot b \neq 0$.

**Exercício 01:** Determine os múltiplos comuns de 3 e 4.

**Definição de divisores de um número natural:**

Diremos que um número natural $d$ é um divisor de outro natural $a$, se $a$ é múltiplo de $d$, ou seja, se $a = d \cdot c$, para algum natural $a$. Representamos o conjunto dos divisores de um número natural $n$ por $D(n)$.

**Exercício 02:** Determinar todos os divisores de 20.

**Definição de divisores comuns:**

São números que são divisores simultaneamente de dois ou mais números dados.

**Exercício 03:** Determine os divisores naturais comuns dos números 18 e 3.

## Sequência Didática I – Encontro 02

Neste encontro, abordamos os conceitos de Divisão euclidiana, Critérios de Divisibilidades, Crivo de Eratóstenes e Números Primos de Mersenne.

### Algoritmo da Divisão

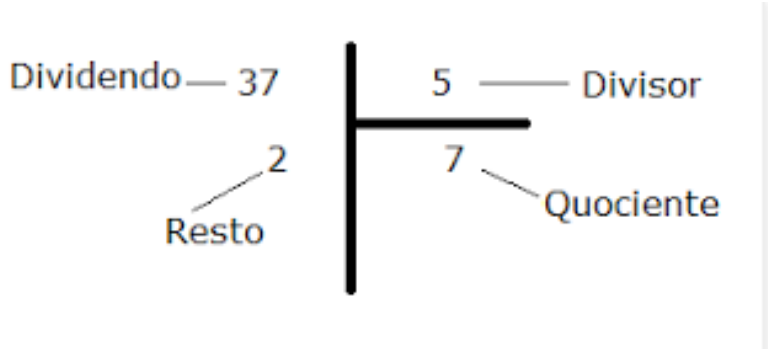
Uma das propriedades mais importantes dos números naturais é a possibilidade de dividir um número por outro. Essa divisão é a chamada divisão euclidiana. Dados dois números naturais $a$ e $b$, com $b \neq 0$, existem números naturais $q$ e $r$ tais que

$a = b \cdot q + r$, onde $0 \leq r < b$. Chamamos $a$, $b$, $q$ e $r$ de dividendo, divisor, quociente e resto, respectivamente.

$$\begin{array}{c|c} a & b \\ \hline r & q \end{array}$$

Vamos verificar como funciona o algoritmo da divisão euclidiana em um caso particular.

Figura 4 – Divisão de 37 por 5




Fonte:<https://sempreamathematicarcommusica.blogspot.com/2011/01/identidade-fundamental-da-divisao.html>

Temos, $37 = 5 \cdot 7 + 2$, portanto a divisão foi efetuada de forma correta.

**Exercício 04:** Usando o Algoritmo da Divisão efetue a divisão de 1436 por 7.

A seguir relembraremos alguns critérios importantes de divisibilidade que foram estudados em séries anteriores.

**Critério de divisibilidade por 2**

Um número N é divisível por 2 quando seu algarismo das unidades for divisível por 2.

**Critério de divisibilidade por 3**

Um número N é divisível por 3 se a soma dos seus algarismos for um número divisível por 3.

**Critério de divisibilidade por 4**

Um número N é divisível por 4 quando seus dois últimos algarismos formam um número divisível por 4, ou seja, quando o número formado pelos algarismos das dezenas e das unidades de N é divisível por 4.

**Critério de divisibilidade por 5**

Um número é divisível por 5 se seu algarismo das unidades é 0 ou 5.

**Critério de divisibilidade por 6**

Um número N é divisível por 6 quando N é divisível por 3 e por 2.

**Critério de divisibilidade por 7**

Dado um número natural $N$, considere $N = 10 \cdot b + a$, onde $a$ é o algarismo das unidades de $N$. Se $b - 2 \cdot a$ é divisível por 7, então $N$ é divisível por 7.

**Exemplo 01:** Para decidir se o número $N = 86415$ é divisível por 7, devemos aplicar o critério de divisibilidade por 7 diversas vezes até percebemos que o número é divisível por 7 ou não.

86415 $\rightarrow$ 8641 - $2 \cdot 5 = 8631 \rightarrow$ 863 - $2 \cdot 1 = 861 \rightarrow$ 86 - $2 \cdot 1 = 84 \rightarrow$ 8 - $2 \cdot 4 = 0$.

Usando o critério, temos:

0 é múltiplo de 7 $\rightarrow$ 84 é múltiplo de 7 $\rightarrow$ 861 é múltiplo de 7 $\rightarrow$ 8631 é múltiplo de 7 $\rightarrow$ 86415 é múltiplo de 7.

**Critério de divisibilidade por 9**

Um número N é divisível por 9 se a soma dos seus algarismos for um número divisível por 9.

**Critério de divisibilidade por 10**

Um número é divisível por 10 se seu algarismo das unidades é 0.

**Critério de divisibilidade por 11**

Um número natural N é divisível por 11 quando a diferença não negativa entre a soma dos algarismos de ordem ímpar (Soi) e a soma dos algarismos de ordem par (Sop) for um número divisível por 11.

**Exemplo 02:** Considere o número $N = 3767632$. Temos:

| $7^a$ | $6^a$ | $5^a$ | $4^a$ | $3^a$ | $2^a$ | $1^a$ |
|---|---|---|---|---|---|---|
| 3 | 7 | 6 | 7 | 6 | 3 | 2 |

Assim, $S_{oi} = 2+6+6+3 = 17$ e $S_{op} = 3+7+7 = 17$. Agora observe que $S_{oi}$ -$S_{op}$ = 17-17= 0 é divisível por 11, o número $N$ é divisível por 11.Aqui, o significado de "diferença não negativa" é semelhante ao que aparece no primeiro critério de divisibilidade por 7. Lembrando que $S_{oi}$ é o somatório dos números das classes ímpares e $S_{op}$ é o somatório dos números das classes pares.

**Exercício 05:** Classifique as seguintes afirmações em verdadeira (V) ou falsa (F):

a) ( ) 2374160 é divisível por 2

b) ( ) 202428 é divisível por 3

c) ( ) 3263612 é divisível por 11

d) ( ) 14777 é divisível por 7

e) ( ) 20025 é divisível por 9

f) ( ) 20002 é divisível por 5

g) ( ) 32147800003 é divisível por 10

**Questão para pensar:** Em grupos estabeleçam um critério de divisibilidade por 16, isto é, quando um número é divisível por 16?

A seguir, apresentaremos um conceito de grande importância na Matemática: o fato de um número ser primo ou não. Esses números desempenham um papel fundamental e a eles estão associados muitos problemas famosos cujas soluções tem resistido aos esforços de várias gerações de matemáticos (HEFEZ; ARITMÉTICA, 2009).

**Definição de números primos:** Um número natural maior do que 1 que possui como divisores positivos 1 e ele próprio é chamado número primo.

**Exemplo 03:** São exemplos de números primos: 2, 3, 5, $\cdots$ .

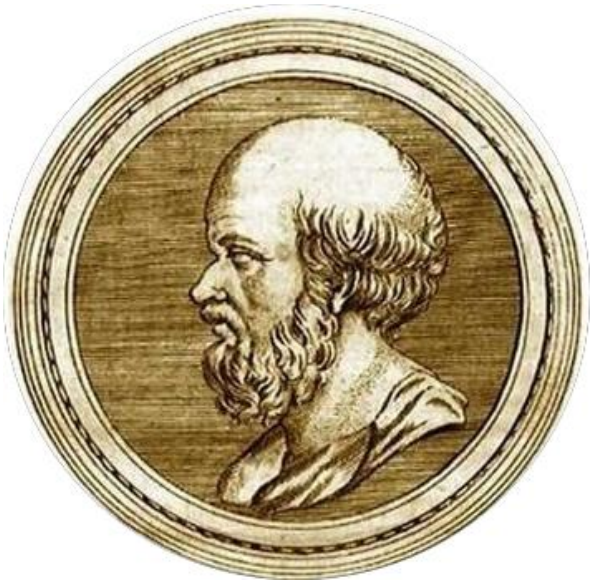
**Definição de números compostos:** Um número maior que 1 e que não é primo será dito composto.

**Exemplo 04:** São exemplos de números compostos: 4, 6, 9, 10, 12, $\cdots$ .

### Crivo de Eratóstenes

Eratóstenes foi um estudioso que viveu no século III a.C. Nasceu em Cirene, na África, e morreu em Alexandria, na Grécia. Teve um destaque muito grande na comunidade científica da época com diversos trabalhos em Matemática, Ciência, Filosofia, Geografia e em outras áreas.

Figura 5 – Eratóstenes



Fonte:<http://www.geografia.seed.pr.gov.br/modules/galeria/detalhe.php?foto=1063&evento=1>

Mas, o trabalho que mais teve destaque foi o Crivo de Eratóstenes, que explicaremos a seguir. Considere um número natural $n$. Por exemplo, $n = 32$. Agora, listamos todos os números de 1 a 32 em um quadro. Nosso objetivo é determinar quais são todos os números primos de 1 até 32.

Tabela 01 - Números de 1 até 32

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
| 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 |
| 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 |
| 25 | 26 | 27 | 28 | 29 | 30 | 31 | 32 |

Fonte: Elaborado pelo autor (2024)

A princípio poderíamos fazer uma varredura com todos os números, mas este processo seria muito exaustivo. Porém, graças ao Crivo de Eratóstenes, podemos realizar o processo de eliminação, onde em cada passo descartamos da tabela alguns números dos quais temos certeza de que são compostos. Fazemos isso várias vezes de um modo bem específico para que, ao final do processo, tenhamos certeza de que os números que sobrarem sejam todos primos (HEFEZ, 2009).

Iniciaremos o processo retirando os números 1 e os múltiplos de 2. Pois, por definição, os números primos são maiores do que 1 e o 2 é o único primo par. Já os múltiplos de 2 são compostos. Logo, eles não são primos e devemos descartá-los.

Tabela 02 - Etapa 2 do Crivo de Eratóstenes

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| ~~1~~ | 2 | 3 | ~~4~~ | 5 | ~~6~~ | 7 | ~~8~~ |
| 9 | ~~10~~ | 11 | ~~12~~ | 13 | ~~14~~ | 15 | ~~16~~ |
| 17 | ~~18~~ | 19 | ~~20~~ | 21 | ~~22~~ | 23 | ~~24~~ |
| 25 | ~~26~~ | 27 | ~~28~~ | 29 | ~~30~~ | 31 | ~~32~~ |

Fonte: Elaborado pelo autor (2024)

Continuando com este processo temos que o 3 é primo. Logo, todos os múltiplos de 3 são compostos e, portanto, riscamos todos. E ficamos fazendo este processo sucessivamente, até riscarmos todos os números compostos que desejamos 1 até $N$.

Tabela 03: - Etapa 3 do Crivo Eratóstenes

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| ~~1~~ | 2 | 3 | ~~4~~ | 5 | ~~6~~ | 7 | ~~8~~ |
| ~~9~~ | ~~10~~ | 11 | ~~12~~ | 13 | ~~14~~ | ~~15~~ | ~~16~~ |
| 17 | ~~18~~ | 19 | ~~20~~ | ~~21~~ | ~~22~~ | 23 | ~~24~~ |
| 25 | ~~26~~ | ~~27~~ | ~~28~~ | 29 | ~~30~~ | 31 | ~~32~~ |

Fonte: Elaborado pelo autor (2024)

Percebe-se que, no final deste processo, os números que não foram riscados são os números primos, como mostra a Tabela 04.

Tabela 04 - Etapa Final do Crivo Eratóstenes

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| ~~1~~ | 2 | 3 | ~~4~~ | 5 | ~~6~~ | 7 | ~~8~~ |
| ~~9~~ | ~~10~~ | 11 | ~~12~~ | 13 | ~~14~~ | ~~15~~ | ~~16~~ |
| 17 | ~~18~~ | 19 | ~~20~~ | ~~21~~ | ~~22~~ | 23 | ~~24~~ |
| ~~25~~ | ~~26~~ | ~~27~~ | ~~28~~ | 29 | ~~30~~ | 31 | ~~32~~ |

Fonte: Elaborado pelo autor (2024)

### Números Primos de Mersenne

Introduziremos, neste momento, alguns tipos de números primos especiais, que são denominados de números de Mersenne, uma homenagem a Marin Mersenne.

O projeto Great Internet Mersenne Prime Search (GIMPS) foi criado em 1996 por George Woltman, formado em Ciência da Computação pelo Instituto de Tecnologia de Massachusetts (MIT), é um projeto voluntário de computação distribuída, que como o próprio nome já indica, seu objetivo é encontrar números primos conhecidos como primos de Mersenne (WOLTMAN, 1996), isto é, conforme a **definição** de (HEFEZ; ARITMÉTICA, 2009), temos:

Os números de Mersenne são os números da forma

$$M_p = 2^p - 1,$$

para algum $p$ natural maior do que 1. Onde $p$ é um número primo.

**Curiosidade**: O GIMPS descobriu o maior número primo conhecido até o momento, $2^{82.589.933} - 1$ , com 24.862.048 dígitos. Um computador oferecido por Patrick Laroche de Ocala, Flórida, fez a descoberta em 7 de dezembro de 2018 (WOLTMAN, 1996). Essa descoberta encontra-se no site oficial do GIMPS.

### Sequência Didática I – Encontro 03

Neste terceiro encontro, trabalharemos o processo de fatoração, o Teorema Fundamental da Aritmética e suas aplicações. Fatorar um número significa transformá-lo em uma multiplicação (TELÁRIS, 2012). Também pode ser definido como decompor um número em um produto de fatores primos (DOLCE; IEZZI; MACHADO, 2009). O processo de fatoração é muito importante para a Matemática, pois através dele podemos simplificar e facilitar a resolução de situações-problema.

**Exemplo 1:** Escreva o número 1820 como um produto de números primos (CADAR; DUTENHEFNER, 2015). Pelo algoritmo da decomposição do número em fatores primos, temos:

Figura 6 – Decomposição do 1820 em fatores primos

| | |
|---|---|
| 1820 | 2 |
| 910 | 2 |
| 455 | 5 |
| 91 | 7 |
| 13 | 13 |
| 1 | |

Fonte: Elaborado pelo autor (2024)

Multiplicando os números do lado direito da barra vertical obtemos a fatoração de 1820 como produto de números primos: $1820 = 2^2 \cdot 5 \cdot 7 \cdot 13$

**Teorema Fundamental da Aritmética:** Todo número natural $a > 1$, ou é primo, ou se escreve como produto de números primos. E além disso, está escrita é única (HEFEZ; ARITMÉTICA, 2009).

**Exemplo 2:** $60 = 2^2 \cdot 3 \cdot 5$.

Quantidade de divisores: Vamos representar por $q(n)$ a quantidade de divisores do número natural $n$. E $n$ pode ser escrito da seguinte forma:

$$n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot p_3^{\alpha_3} \cdots p_r^{\alpha_r} .$$

Onde $p_1$, $p_2$, $p_3$, $\cdots$ , $p_r$ são primos e $\alpha_1$, $\alpha_2$, $\alpha_3$,$\cdots$, $\alpha_r$. São números naturais maiores que 1, então :

$q(n) = (\alpha_1 + 1) \cdot (\alpha_2 + 1) \cdot (\alpha_3 + 1) \cdots (\alpha_r + 1)$.

**Exemplo 3:** Determine a quantidade de divisores de 18.

Uma vez que $18 = 2^1.3^2$, tem-se $q(18) = (1+1) \cdot (1+2) = 2 \cdot 3 = 6$; portanto, existem 6 números que são divisores por 18.

O Mínimo Múltiplo Comum (MMC) de dois ou mais números naturais é o menor número, excluindo o zero, que é múltiplo desses números (DOLCE; IEZZI; MACHADO, 2009).

O MMC é o produto dos fatores primos comuns e não comuns, cada um com o maior expoente que apresenta nas formas fatoradas dos números dados (DOLCE; IEZZI; MACHADO, 2009).

**Exemplo 4:** Vamos calcular o MMC de 10, 15 e 21, para a resolução desta questão podemos usar três métodos distintos.

**Primeiro método: listagem de múltiplos.** Esse método é o que utilizaremos no **Exemplo 4**. Listamos os múltiplos de cada um dos números dados e procuramos identificar o menor número que é múltiplo de todos, isto é, que pertence a todas as listas de múltiplos. O MMC de uma lista de números naturais não nulos existe e é único. No entanto, esse método pode ser muito trabalhoso se tivermos que lidar com números grandes.

Sejam $M(10)$, $M(15)$ e $M(21)$ os conjuntos dos múltiplos, respectivamente, de 10, 15, 21.

$M(10) = \{0, 10, 20, 30, 40, 50, 60, 70, 80, 90, 100, \cdots, 160, 170, 180, 190, 200, 210, \cdots\}$.

$M(15) = \{0, 15, 30, 45, 60, 75, 90, 105, 120, 135, 150, 165, 180, 195, 210, \cdots\}$.

$M(21) = \{0, 21, 42, 63, 84, 105, 126, 147, 168, 189, 210, \cdots\}$.

Com exceção do zero, o menor múltiplo comum de 10, 15 e 21 é exatamente 210. Logo, $\text{MMC}(10, 15, 21) = 210$.

**Segundo método: decomposição simultânea.** Como o próprio nome já diz, esse método consiste em decompor simultaneamente, como produtos de fatores primos, os números dos quais queremos calcular o MMC.

Figura 7 – Decomposição simultaneamente dos números 10 , 15 e 21

| 10 | 15 | 21 | 2 |
|---|---|---|---|
| 5 | 15 | 21 | 3 |
| 5 | 5 | 7 | 5 |
| 1 | 1 | 7 | 7 |
| 1 | 1 | 1 | 2.3.5.7=210 |

Fonte: Elaborado pelo autor (2024)

**Terceiro método: decomposição de fatores primos.**

$10 = 2 \cdot 5$

$15 = 3 \cdot 5$

$21 = 3 \cdot 7$

Vamos retirar todos os números primos da decomposição de cada número em fatores primos e considerar os maiores expoentes de cada número primo. Logo, teremos:

MMC(10, 15,21) $= 2 \cdot 3 \cdot 5 \cdot 7 = 210$.

**Exercício 1 (PUC MG/2001):** O Mínimo Múltiplo Comum dos números $2^3$, $3^n$ e 7 é 1512. O valor de n é:

A) 3

B) 4

C) 5

D) 6

E) 7

**Exercício 2 (IFCE 2020):** Um relógio A bate a cada 15 minutos, outro relógio B bate a cada 20 minutos, e um terceiro relógio C, a cada 25 minutos. O menor intervalo de tempo decorrido entre duas batidas simultâneas dos três relógios, em horas, é igual:

A) 3

B) 4

C) 5

D) 6

E) 7

O Máximo Divisor Comum de dois ou mais números naturais é o maior número que é divisor de todos esses números (DOLCE; IEZZI; MACHADO, 2009).

O MDC é o produto dos fatores primos comuns, cada um com o menor expoente que apresenta nas fatorações dos números dados (DOLCE; IEZZI; MACHADO, 2009) .

**Exemplo 5:** Os números 12, 18 e 30 têm conjuntos de divisores, respectivamente, dados por:

$D(12) = \{1, 2, 3, 4, 6, 12\}$;

$D(18) = \{1, 2, 3, 6, 9, 18\}$;

$D(30) = \{1, 2, 3, 5, 6, 10, 15, 30\}$.

O maior número divisor comum entre 12, 18 e 30 é exatamente 6.

Portanto, MDC(12,18,30)= 6.

**Primeiro método: listagem de divisores.** Consiste no que já foi feito no **Exemplo 5.** Listamos os divisores de cada número e procuramos o maior dentre os divisores comuns a todos. Esse método não será eficaz se os números dados tiverem muitos divisores.

**Segundo método: divisões sucessivas).** Esse método, também conhecido como algoritmo de Euclides, pode ser aplicado para o cálculo do MDC entre dois números naturais. Mais adiante veremos que, aplicando-o várias vezes, também é possível usá-lo para o cálculo do MDC de mais de dois números. O método se baseia nas duas observações a seguir.

O método consiste nos seguintes passos:

1. 1. Se os dois números são iguais a zero, o MDC não existe.
2. Se um dos números for igual a zero, o MDC será o outro número.
3. Se os dois números são diferentes de zero, mas são iguais, o MDC será qualquer um dos dois.
4. Se os dois números são diferentes de zero e diferentes um do outro, divida o maior pelo menor.
5. Se o resto da divisão for igual a zero, o MDC é o menor dos números.
6. Se o resto da divisão for diferente de zero, retorne ao passo 4, substituindo o maior número pelo menor e o menor número pelo resto.
7. Repita os passos 4, 5 e 6 até o resto da divisão ser igual a zero.

Geralmente, usamos uma grade para facilitar a compreensão, um bom exemplo, esta na Figura 11.

**Exemplo 6:** Usando agora o algoritmo de Euclides calcularemos o MDC(124, 48). De início, colocamos os dois números na linha do meio da grade, sendo o maior número (124) colocado na primeira casa à esquerda e o menor número (48) colocado na segunda casa, ao lado do maior número.

Figura 8 – Algoritmo de Euclides (MDC)

| Quocientes: | 2 | 1 | 1 | 2 | 2 |
|---|---|---|---|---|---|
| 124 | 48 | 28 | 20 | 8 | 4 |
| Restos: 28 | 20 | 8 | 4 | 0 | |

Fonte: Elaborado pelo autor (2024)

O algoritmo de Euclides é uma ferramenta muito eficiente para encontrar o máximo divisor comum de dois números quaisquer diferente de zero de maneira rápida e objetiva.

O método consiste em efetuar sucessivas divisões entre os dois números seguidos que constam na segunda linha, da seguinte forma. Neste processo colocamos o quociente de cada divisão na primeira linha, acima do divisor, e o resto correspondente na terceira linha abaixo do dividendo.

Inicialmente dividimos 124 por 48, obtendo quociente 2 e resto 28. Uma vez que o resto da divisão é não-nula, adicionamos o resto 28 após o 48 na segunda linha. Agora dividimos 48 por 28, obtendo quociente 1 e resto 20, como mostra a Figura 8. Continuamos este processo até que o resto da divisão seja iguala zero. Neste caso, o máximo divisor comum será o último resto não nulo da terceira linha, ou seja, MDC(124,48)= 4.

**Terceiro método: decomposição em fatores primos.** Sejam $a_1$, $a_2$, $\cdots$, $a_n$ números naturais diferentes de zero. Se um deles for igual a 1, o (MDC) de todos esses números também será igual a 1. Caso contrário, podemos escrever cada um deles como produto de números primos e em seguida considerar o produto dos primos em comum nas fatorações, com os maiores expoentes de cada número primo comum.

Exemplo 7: Determine o máximo divisor comum MDC(12, 18, 30) fatorando os três números.

$12 = 2^2 \cdot 3$.

$18 = 2 \cdot 3^2$.

$30 = 2 \cdot 3 \cdot 5$.

Para encontrar o máximo divisor comum de três números quaisquer basta observarmos os primos que dividem simultaneamente, os três números fatorados dados, logo sao 2 e 3. O primo 2 aparece com expoente 1 na decomposição de 12, 18 e 30 e o número primo 3 aparece com expoente 1 na decomposição de 12, 18 e 30. Devemos escolher o menor expoente e os números primos que dividem simultaneamente os três número, para enfim encontrar o (MDC).

Portanto, o máximo divisor comum dos três números será $2 \cdot 3 = 6$.

Este recurso pode se realizar com dois ou mais números, tornando-se um artifício muito eficiente e utilizado.

**Exercício 3 (Vunesp 2023):** Um ajudante de uma loja de ferragens precisa distribuir, em saquinhos de plásticos, três tipos diferentes de parafusos, de agora em diante identificados com tipo A, B e C. Todos os saquinhos devem conter a mesma quantidade de parafusos e sempre parafusos de um mesmo tipo. Também foi pedido ao ajudante que cada saquinho tivesse a maior quantidade possível de parafusos. Sabendo que são 132 parafusos do tipo A, 180 parafusos do tipo B e 228 parafusos do tipo C, o número de saquinhos necessários para cumprir essa tarefa é:

A) 30

B) 34

C) 42

D) 45

E) 48

**Observação:** Podemos também relacionar o Máximo Divisor Comum com o Mínimo Múltiplo Comum. Esta relação é muito fácil, mas o aluno não deve ter a ilusão de que este recurso pode ser utilizado com números grandes, pois teremos um trabalho muito desgastante. Para estes números grandes é mais eficiente utilizarmos o algoritmo de Euclides (HEFEZ, 2009).

| Sejam $a$ e $b$ dois números naturais não nulos. Então: |
|---|
| MMC $(a, b)\cdot$ MDC $(a, b) = a \cdot b$. |

**Exercício 4 (Aprendiz de Marinheiro - 2016):** Sejam $A = 120$, $B = 160$, $x$=MMC $(A, B)$ e $y$=MDC $(A, B)$, então o valor de $x + y$ é igual a:

A) 460

B) 480

C) 500

D) 520

E) 540

### Sequência Didática I – Encontro 04

Uma das ideias mais importantes e fortes na Teoria dos Números é a de congruência que foi introduzida por Karl Friedrich Gauss (1777 − 1855) (HYGINO, 1991).

Neste encontro trabalharemos a aritmética dos fenômenos periódicos e a ideia de congruência, recurso importante para resolução de problemas envolvendo estes eventos, ou seja, aquelas situações em que há uma repetição regular de intervalos.

Estes fenômenos acontecem, diariamente, quando precisamos tomar um medicamento no horário regular, quando olhamos o relógio e percebemos que os dias são obtidos através dos segundos, minutos e horas. Que as semanas são formadas por 7 dias, os meses por 28, 29, 30 ou 31 dias, e os anos são formados por 365 dias e 6 horas aproximadamente ou 366 dias quando são bissextos.

Movimentos periódicos ocorrem em diversas situações do nosso cotidiano, por exemplo, o movimento que a Terra leva para dar uma volta em torno de si, representa 24h (movimento de rotação), já o movimento que a terra dá em torno do sol corresponde a 365 dias e 6 horas aproximadamente (movimento de translação) (COUTINHO, 2015).

Um outro exemplo que podemos introduzir é referente ao calendário escolar, suponhamos que um pai pergunte ao filho: filho dia 23 vai ter aula de Física? O filho verifica que hoje é dia 11 (segunda-feira), utilizando a tabela abaixo:

Figura 9 – Dias da semana

| Restos | 0 | 1 | 2 | 3 | 4 | 5 | 6 |
|---|---|---|---|---|---|---|---|
| Dia | Segunda | Terça | Quarta | Quinta | Sexta | Sábado | Domingo |

Fonte: (COUTINHO, 2015)

Sabe-se que hoje é dia 11 e que o dia que se deseja saber é dia 23, portanto, a diferença do dia que se quer e hoje é dado por $23 - 11 = 12$, podemos rescrever o 12 da seguinte forma: $12 = 7 + 5$, onde este 5 seria o resto da divisão de 12 por 7. Portanto, o dia 23 vai cair em um sábado, conforme a Figura 21. Logo, sábado não tem aula.

**Exercício 01:** O ano de 2019 começou em um terça-feira, em que dia da semana caíra o último dia do ano de 2019 ?

**Exercício 02:** O ano de 2023 começou em um domingo, em que dia da semana caíra o $1^o$ dia de 2026?

É importante salientar que nos calendários existem anos que são bissextos. Há alguns critérios que precisamos identificar para que seja classificado um ano bissexto.

Se o ano for um múltiplo de 4, o ano é bissexto, mas se o ano for múltiplo de 4 e múltiplo de 100 simultaneamente o ano não será bissexto e por fim se o ano for múltiplo de 4, múltiplo de 100 e múltiplo de 400 teremos um ano bissexto, é relevante saber

destas informações para que haja uma classificação do ano de forma adequada. Fonte: <https://www.youtube.com/watch?v=Gj5uopyMoKc>.

**Exercício 03:** Quantos calendários anuais diferentes existem?

Em algum momento nos deparamos com a seguinte situação: "$7 + 8 = 3$". Para que esta situação tenha sentido é necessário contextualizarmos. Um relógio seria um exemplo significativo, pois 15 horas representa 3 horas da tarde. Como isso temos a ideia da aritmética dos restos. Que podemos representar da seguinte forma:

$7 + 8 \equiv 3 \pmod{12}$ (lê-se: sete mais oito é congruente a três módulo doze).

A seguir iremos explicar de forma mais detalhada essa operação. Antes disso, definiremos formalmente a ideia de congruência módulo m. A definição apresentada a seguir consta em (HEFEZ; ARITMÉTICA, 2009).

Seja $m$ um número natural. Diremos que dois números inteiros $a$ e $b$ são congruentes módulo $m$ se os restos de sua divisão euclidiana por $m$ são iguais. Quando os inteiros $a$ e $b$ são congruentes módulo $m$, escreve-se: $a \equiv b \pmod{m}$

Quando a relação $a \equiv b \pmod{m}$ for falsa, diremos que $a$ e $b$ não são congruentes, ou que são incongruentes, módulo $m$. Escreveremos, nesse caso:

**Exercício 04:** Vamos verificar se são verdadeiras $(V)$ ou falsas $(F)$ as seguintes congruências:

a) $11 + 2 \equiv 1 \pmod{12}$ ( )

b) $10 + 10 \equiv 8 \pmod{12}$( )

c) $20 \equiv 0 \pmod{4}$ ( )

d) $21 \equiv 9 \pmod{12}$ ( )

e) $8 \equiv 2 \pmod{3}$( )

A ideia primária da aritmética modular é bem simples. Fixado um inteiro $m$, todos os demais números inteiros a são substituídos pelo resto de sua divisão euclidiana por $m$. Desse modo, o conjunto $\mathbb{Z}$ dos números inteiros se transforma no conjunto $\mathbb{Z}_m = \{0, 1, 2, \ldots, m-1\}$ , denominado conjunto dos inteiros módulo $m$ (cujos elementos são os restos possíveis da divisão de um inteiro qualquer por $m$).

Fonte: <https://sca.profmatsbm.org.br/profmat_tcc.php?id1=6047&id2=171053443>.

No conjunto $\mathbb{Z}$ apresentado anteriormente definiremos duas operações: adição e multiplicação, as quais serão detalhadas a seguir. A soma será denotada pelo símbolo $\oplus$ e o produto será denotado pelo símbolo $\odot$ .

$$a \oplus b = \text{resto da divisão de } a + b \text{ por } m.$$
$$a \odot b = \text{resto da divisão de } a \cdot b \text{ por } m.$$

**Exemplo 01:** Observe que em $\mathbb{Z}_4$ temos as seguintes operaçãos.

$2 \oplus 3 =$ resto da divisão de $2 + 3$ por $4 =$ resto da divisão de 5 por $4 = 1$.

$2 \odot 3 =$ resto da divisão de $2 \cdot 3$ por $4 =$ resto da divisão de 6 por $4 = 2$.

As tabelas apresentadas a seguir representam as tábuas das operações de adição e multiplicação em $\mathbb{Z}_4$ .

Tabela 05 -Tábua de operação $\oplus$ em $\mathbb{Z}_4$

| $\oplus$ | 0 | 1 | 2 | 3 |
|---|---|---|---|---|
| 0 | 0 | 1 | 2 | 3 |
| 1 | 1 | 2 | 3 | 0 |
| 2 | 2 | 3 | 0 | 1 |
| 3 | 3 | 0 | 1 | 2 |

Fonte: Elaborado pelo autor (2024)

Tabela 06 -Tábua de operação $\odot$ em $\mathbb{Z}_4$

| $\odot$ | 0 | 1 | 2 | 3 |
|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 |
| 1 | 0 | 1 | 2 | 3 |
| 2 | 0 | 2 | 0 | 2 |
| 3 | 0 | 3 | 2 | 1 |

Fonte: Elaborado pelo autor (2024)

**Exercício 05:** Construa as tábuas das operações de adição e multiplicação em $\mathbb{Z}_7$.

### Sequência Didática I - Encontro 05

Neste encontro, faremos uma abordagem relembrando alguns conceitos fundamentais de matrizes, suas operações e determinantes, pois esses conteúdos serão importantes para o Encontro 06, no qual trabalharemos a Criptografia e as Cifras de Hill.

Uma matriz nada mais é do que uma tabela disposta em linhas e colunas, e é bastante usada para organizar dados em empresas, jornais, calendários e planilhas. Historicamente, o surgimento de tabelas para resolver situações-problema tem indícios na China por volta de 2500 a.C., apresentados em um dos capítulos do livro chinês "Chui-Chang Suan-Shu". Mas quem introduziu a ideia de configurar dados em tabelas foi o matemático francês Augustin-Louis Cauchy (1789-1857), como é mostrado no livro (DANTE, 2013).

Vamos definir as matrizes conforme (IEZZI; HAZZAN, 2004). Dados dois números $m$ e $n$ naturais não-nulos, chama-se matriz $m$ por n (indica-se $m$ x $n$) toda tabela $M$ formada por números reais distribuídos em $m$ linhas e $n$ colunas.

Em uma matriz $M$ qualquer, cada elemento é indicado por $a_{ij}$. O índice $i$ indica a linha e o índice $j$ indica a coluna. Por convenção $i = 1,\cdots, m$ e $j = 1,\cdots, n$.

**Exemplo 01:**

$$M = (a_{ij})_{m\times n} = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ a_{31} & a_{32} & \cdots & a_{3n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix}$$

Após relembrarmos a definição de matriz, vamos abordar a operação de multiplicação de matrizes, que será de extrema importância para o próximo encontro. Uma condição para que o produto $A \cdot B$ seja definido é que o número de colunas de $A$ seja igual ao número de linhas de $B$ (IEZZI et al., 2001).

A matriz produto $C = A\cdot B$ é uma matriz cujo o número de linhas é igual ao número de linhas de $A$ e o número de colunas é igual ao número de colunas de $B$. Observemos o esquema abaixo:

$$A_{m\times n} \cdot B_{n\times p} = C_{m\times p}$$

Podemos observar que a condição de existência do produto é válida, pois o número de colunas da matriz $A$ é igual ao número de linhas da matriz $B$. Logo, este produto existe e o resultado do mesmo é uma matriz cujo número de linhas corresponde ao mesmo da matriz $A$ e o número de colunas corresponde ao mesmo da matriz $B$.

**Exemplo 02:**

$$\begin{pmatrix} 1 & 4 & 0 \\ \text{-}2 & 4 & 3 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 \\ 0 & 2 \\ \text{-}3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 10 \\ \text{-}11 & 7 \end{pmatrix}$$

Como a condição de existência para a multiplicação de matrizes é válida, ou seja, o número de colunas da primeira matriz é igual ao número de linhas da segunda matriz, logo o resultado desta multiplicação de matrizes será uma matriz de ordem 2.

Vejamos o processo: Sejam $C = A\cdot B$, onde A é representada pela primeira matriz, $B$ a segunda matriz e $C$ a matriz resultado do produto de $A$ por $B$. A seguir ilustraremos como calcular os elementos da matriz produto $C$. Percebe-se que as letras minúsculas representam os elementos de cada matriz e suas respectivas posições; por exemplo, $a_{11}$ seria o elemento da matriz A na primeira linha e primeira coluna. O elemento $c_{11}$ da matriz $C$ é obtido pela soma dos produtos dos elementos correspondentes da primeira linha da matriz $A$ pelos elementos da primeira coluna de $B$.

$c_{11} = a_{11} \cdot b_{11} + a_{12} \cdot b_{21} + a_{13} \cdot b_{31} \Rightarrow c_{11} = 1 \cdot 1 + 4 \cdot 0 + 0 \cdot (-3) = 1.$

$c_{12} = a_{11} \cdot b_{12} + a_{12} \cdot b_{22} + a_{13} \cdot b_{32} \Rightarrow c_{12} = 1 \cdot 2 + 4 \cdot 2 + 0 \cdot 1 = 10.$

$c_{21} = a_{21} \cdot b_{11} + a_{22} \cdot b_{21} + a_{23} \cdot b_{31} \Rightarrow c_{21} = (-2) \cdot 1 + 4 \cdot 0 + 3 \cdot (-3) = -11.$

$c_{22} = a_{21} \cdot b_{12} + a_{22} \cdot b_{22} + a_{23} \cdot b_{32} \Rightarrow c_{22} = (-2) \cdot 2 + 4 \cdot 2 + 3 \cdot 1 = 7.$

Vale salientar que esses conceitos já foram abordados no $2^o$ ano do Ensino Médio, mas é importante relembrá-los para garantir uma aprendizagem significativa quando forem apresentados a Criptografia e as Cifras de Hill.

**Exercício 01:** Dadas as matrizes:

$$D_2 = (d_{ij})_{2\times 2} = \begin{pmatrix} 1 & -2 \\ 3 & 4 \end{pmatrix}$$

$$B = (b_{ij})_{2\times 2} = \begin{pmatrix} -1 & 2 \\ 1 & 3 \end{pmatrix}$$

Verifique se a propriedade comutativa é válida, ou seja, se $D_2 \cdot B = B \cdot D_2$.

Existem matrizes que são especiais e importantes para efetuar operações; uma delas é a matriz unidade (ou matriz identidade) de ordem $n$ (indicada por $I_n$). Tal matriz é toda matriz diagonal em que os elementos da diagonal principal são iguais a 1, e o restante dos elementos que fazem parte da matriz são iguais a zero (IEZZI; HAZZAN, 2004).

$$I_2 = (i_{ij})_{2\times 2} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

$$I_3 = (i_{ij})_{3\times 3} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

$$\vdots$$

$$I_{\mathrm{n}} = (i_{ij})_{n\times n} = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix}$$

Outro conceito importante na teoria de matrizes é o de matriz inversível. Por definição, uma matriz quadrada $A$ de ordem $n$ é inversível se existir uma matriz $B$ tal que $A \cdot B = B \cdot A = I_n$ ($I_n$ é a matriz identidade). Se A não é inversível, então dizemos que A é uma matriz singular (IEZZI; HAZZAN, 2004).

**Exercício 02:** Considere a matriz

$$A_1 = \begin{pmatrix} 1 & 2 \\ 1 & 3 \end{pmatrix}$$

Determine a inversa de $A_1$.

Com relação à teoria dos determinantes, sua origem remonta por volta do século XVII, quando eram estudados os processos de resolução de sistemas lineares. Embora não seja um método muito prático, era possível resolver alguns sistemas através do Teorema de Cramer (IEZZI; HAZZAN, 2004) .

Vamos relembrar agora a definição de determinantes para os casos $n = 1, 2, 3$. Consideremos o conjunto de matrizes quadradas de elementos reais. Seja $M$ uma matriz de ordem $n$ desse conjunto. Chamamos de determinante da matriz $M$ (e indicamos por det $M$) o número obtido operando com os elementos de $M$ da seguinte forma:

1º Caso: Se $M$ é de ordem $n = 1$, então det$M_1$ é o único elemento de $M_1$.

$$M_1 = (a_{ij})_{1\times 1} = \begin{pmatrix} a_{11} \end{pmatrix}$$

Portanto, o determinante de $M_1$, Det $M_1 = a_{11}$.

2º Caso: Se $M$ é de ordem $n = 2$, então o determinante de $M_2$ é o produto dos elementos da diagonal principal menos o produto dos elementos da diagonal secundária.

$$M_2 = (a_{ij})_{2\times 2} = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$$

Portanto, o determinante de $M_2$, pode ser calculado da seguinte forma:

Det $M_2 = a_{11} \cdot a_{22} - a_{21} \cdot a_{12}$.

3º Caso: Se $M$ é de ordem $n = 3$, isto é :

$$M_3 = (a_{ij})_{3\times 3} = \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix}$$

Definimos,

Det $M_3 = a_{11}\cdot a_{22}\cdot a_{33} + a_{12}\cdot a_{23}\cdot a_{31} + a_{13}\cdot a_{21}\cdot a_{32} - a_{13}\cdot a_{22}\cdot a_{31} - a_{11}\cdot a_{23}\cdot a_{32} - a_{12}\cdot a_{21}\cdot a_{33}$.

Podemos memorizar este cálculo da seguinte forma:

$$M_3 = \begin{vmatrix} a_{11} & a_{12} & a_{13} & a_{11} & a_{12} \\ a_{21} & a_{22} & a_{23} & a_{21} & a_{22} \\ a_{31} & a_{32} & a_{33} & a_{31} & a_{32} \end{vmatrix}$$

a) Repetimos ao lado da matriz as duas primeiras colunas;

b) Os termos precedidos pelo sinal + são obtidos multiplicando-se os elementos segundo na direção das diagonais principais, isto é, são os termos:

$a_{11} \cdot a_{22} \cdot a_{33}$, $a_{12} \cdot a_{23} \cdot a_{31}$ e $a_{13} \cdot a_{21} \cdot a_{32}$.

c) Os termos precedidos pelo sinal $-$ são obtidos multiplicando-se os elementos segundo na direção das diagonais secundárias:

$-a_{13} \cdot a_{22} \cdot a_{31}$, $-a_{11} \cdot a_{23} \cdot a_{32}$ e $-a_{12} \cdot a_{21} \cdot a_{33}$.

Este método pode ser visto com mais detalhes no livro "Fundamentos de Matemática Elementar", volume 4 (IEZZI; HAZZAN, 2004).

**Exercício 03:** Calcule o determinante das seguintes matrizes.

$$a) P_1 = (p_{ij})_{1\times 1} = \begin{pmatrix} 2 \end{pmatrix}$$

$$b) P_2 = (p_{ij})_{2\times 2} = \begin{pmatrix} 1 & 2 \\ 1 & 3 \end{pmatrix}$$

$$c) P_3 = (p_{ij})_{3\times 3} = \begin{pmatrix} 1 & 0 & 3 \\ 0 & 1 & 2 \\ 4 & 1 & 2 \end{pmatrix}$$

**Observação:** É possível verificar que uma matriz admite inversa somente quando ela for quadrada e o seu determinante for não nulo.

Método para o Cálculo do Inverso de uma Matriz de ordem 2.

A seguir, descrevemos um método para o cálculo da inversa de uma matriz A de ordem 2. Tal método encontra-se em (BOLDRINI et al., 1980). Em primeiro lugar, precisamos entender o que é uma matriz adjunta Observação: É possível verificar que uma matriz admite inversa somente quando ela for quadrada e o seu determinante for não nulo.

Método para o Cálculo do Inverso de uma Matriz de ordem 2.

A seguir, descrevemos um método para o cálculo da inversa de uma matriz $A$ de ordem 2. Tal método encontra-se em (BOLDRINI et al., 1980). Em primeiro lugar, precisamos entender o que é uma matriz adjunta (PACCOLA, 1995).

A matriz adjunta de uma matriz quadrada $M$ é a transposta da matriz dos cofatores de $A$. Indicamos a matriz adjunta de $M$ por:

$$\text{Adj } M = (cofM)^t.$$

Vamos obter a matriz dos cofatores de M.

$$M_2 = (a_{ij})_{2\times 2} = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$$

O elemento $c_{ij}$ da matriz dos cofatores de $M_2$ é calculo por $(-1)^{i+j}$ vezes o determinante da matriz obtida após eliminarmos a linha $i$ e a coluna $j$ de $M_2$. Vamos

determinar os elementos da matriz dos cofatores da matriz $M_2$ de ordem 2, conforme descrito acima.

$c_{11} = (-1)^{1+1} \cdot a_{22} = a_{22}$.

$c_{12} = (-1)^{1+2} \cdot a_{21} = -a_{21}$.

$c_{21} = (-1)^{2+1} \cdot a_{12} = -a_{12}$.

$c_{22} = (-1)^{2+2} \cdot a_{11} = a_{11}$.

Logo, a matriz dos cofatores de $M_2$, isto é, Cof $M_2$ é :

$$CofM_2 = (a_{ij})_{2\times 2} = \begin{pmatrix} a_{22} & -a_{21} \\ -a_{12} & a_{11} \end{pmatrix}$$

Portanto, de acordo com a definição da matriz Adj $M_2 = (CofM_2)^t$:

$$AdjM_2 = (a_{ij})_{2\times 2} = \begin{pmatrix} a_{22} & -a_{12} \\ -a_{21} & a_{11} \end{pmatrix}$$

Por fim, podemos calcular a matriz inversa como sendo a fórmula:

$$A^{-1} = \frac{1}{DetM_2} \cdot (AdjM_2) = \frac{1}{DetM_2} \cdot \begin{pmatrix} a_{22} & -a_{12} \\ -a_{21} & a_{11} \end{pmatrix}$$

Iremos considerar esta fórmula como verdadeira sem demonstração.

**Exercício 04:** Calcule, se existir, a inversa da matriz $R_2$.

$$R_2 = (r_{ij})_{2\times 2} = \begin{pmatrix} 1 & 2 \\ 1 & 3 \end{pmatrix}$$

**Sequência Didática I - Encontro 06**

Nesta sequência didática vamos abordar um assunto de extrema relevância para o mundo moderno, a Criptografia, a qual pode ser implementada em diversos contextos tanto no Ensino Fundamental quanto no Ensino Médio. Nossa abordagem será voltada para o Ensino Médio e requer conhecimentos de Aritmética, bem como ideias envolvendo matrizes e determinantes, que foram apresentados em encontros anteriores.

Em grego, cryptos significa secreto, oculto. A Criptografia estuda os métodos para codificar uma mensagem de modo que seu destinatário legítimo consiga interpretá-la. É a arte dos "códigos secretos", que todos já praticamos quando criança. O mais simples desses códigos consiste em substituir uma letra para a seguinte, isto é, transladar o alfabeto uma casa para diante. Um código semelhante foi usado por César para comunicar-se com legiões em combate pela Europa. Este parece ter sido o primeiro exemplo de um código secreto de que se tem notícia (COUTINHO, 2015).

Nota-se que para um sistema criptográfico funcionar é preciso cumprir duas condições,o primeiro que ele seja reversível,ou seja ,que a mensagem possa ser codificada e

decodificada com precisão e o segundo, o receptor tenha uma chave para realizar esta codificação e decodificação com eficiência. Fonte: <https://www.youtube.com/watch?v=pgEV9XjOQ6I&t=134s>.

Atualmente, a Criptografia é uma ferramenta muito importante para sociedade moderna, utilizamos em trocas de e-mails, transações bancárias, compra e venda de produtos na internet, permitindo que estas informações sejam transmitidas de acordo com os três pilares da segurança da informação: confidencialidade, integridade e disponibilidade (KIM; SOLOMON, 2014).

Antes de apresentar o método de Criptografia que será estudado, faremos uma retomada ao conjunto $\mathbb{Z}_m$, por ser importante para identificar o inverso multiplicativo de um conjunto. Vamos utilizar um exemplo prático para discutir essa ideia. Considere a seguir a tábua de multiplicação em $\mathbb{Z}_5$.

Tabela 07 -Tábua de operação $\odot$ em $\mathbb{Z}_5$

| $\odot$ | 0 | 1 | 2 | 3 | 4 |
|---|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 | 0 |
| 1 | 0 | 1 | 2 | 3 | 4 |
| 2 | 0 | 2 | 4 | 1 | 3 |
| 3 | 0 | 3 | 1 | 4 | 2 |
| 4 | 0 | 4 | 3 | 2 | 1 |

Fonte: Elaborado pelo autor (2024)

Percebe-se que 1 funciona como elemento neutro da multiplicação em $\mathbb{Z}_5$. Observe, que:

$2 \odot 3 =$ resto da divisão de $2 \cdot 3$ por $5 =$ resto da divisão de 6 por $5 = 1$.

Por isso, dizemos que 2 é o inverso multiplicativo de 3 módulo 5.

**Exemplo 01:** Qual o inverso multiplicativo em $\mathbb{Z}_5$.

a) 1;

b) 2;

c) 2;

d) 3;

e) 0 tem inverso multiplicativo?

Uma das ferramentas importantes que temos para associar os estudos de matrizes e determinantes com a Criptografia são as Cifras de Hill que é um sistema poligráfico,

ou seja, cada letra é representada por um número módulo 26. Inventado por Lester S.Hill, matemático americano em 1929 (ROSSETO, 2018).

As ideias contidas aqui constam em (ROSSETO, 2018). A princípio utilizaremos o alfabeto com as 26 letras, onde cada letra estará associada a um valor numérico: por exemplo A está associado a 1, B está associado a 2 e assim sucessivamente, até chegarmos ao Z que será associado a 0 (pois, Z corresponde a última letra do nosso alfabeto (posição 26) e quando dividimos o número 26 por 26 obtemos o resto 0). A princípio vamos atribuir um número a cada letra como podemos observar abaixo:

Figura 10 – Blocos de substituição de letras por números e vice-versa

| A | B | C | D | E | F | G | H | I | J | K | L | M |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 |
| N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
| 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 0 |

(ROSSETO, 2018)

Em seguida, dividiremos em blocos a palavra ou frase a ser decifrada. Cada bloco é formado por duas letras, logo estas letras serão associadas a dois números formando um vetor, com 2 linhas e 1 coluna. Pois este vetor é que vai garantir a condição de multiplicação de matrizes. Criamos uma matriz de ordem 2 para facilitar os cálculos, desde que esta matriz seja inversível, pois para codificar precisamos da matriz criada e para decodificar precisamos da matriz inversa. Lembrando que para termos uma matriz inversa é necessário que o determinante seja diferente de zero. Para entendermos melhor vejamos a seguinte situação.

Para criptografar uma mensagem, cada bloco de duas letras, considerando como vetor de dois componentes, é multiplicado por uma matriz de ordem 2 invertível módulo 26. Para descriptografar a mensagem, cada bloco é multiplicado pela inversa da matriz usada no processo de codificação.

A matriz utilizada para criptografia é a chave de cifra, e deve ser escolhida aleatoriamente do conjunto de matrizes de ordem 2 invertíveis módulo 26. A cifra pode, é claro, ser adaptada a um alfabeto com qualquer número de letras; toda aritmética só precisa ser feita módulo o número de letras em vez de módulo 26 (ROSSETO, 2018).

Sejam $A$ uma matriz de ordem 2, $A^{-1}$ a matriz inversa de ordem 2 de $A$, $V$ a matriz que representa vetor coluna a ser codificado, $M_c$ a matriz de codificação e $M_d$ a matriz de decodificação. Então:

Processo de codificação

$$\boxed{A_{2\times2} \cdot V_{2\times1} = M_c(_{2\times1})}$$

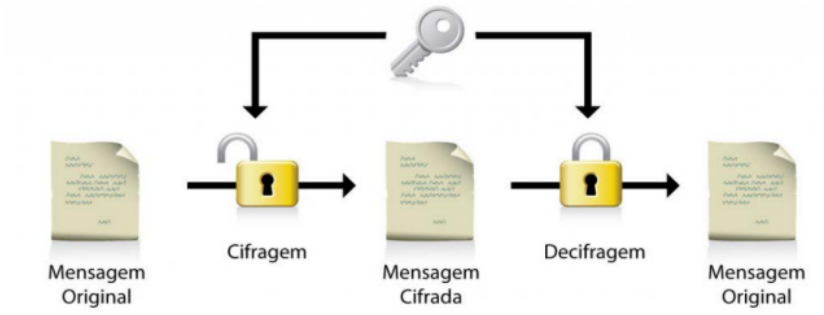
Fonte: Elaborado pelo autor (2024)

Processo de decodificação

$$\boxed{A^{-1}_{2\times2} \cdot (A_{2\times2} \cdot V_{2\times1}) = A^{-1}_{2\times2} \cdot M_c(_{2\times1}) = M_d(_{2\times1})}$$

Fonte: Elaborado pelo autor (2024)

Figura 11 – Esquema de ciframento e decifamento




Fonte:<https://www.cin.ufpe.br/~flash/ais98/cripto/criptografia.htm>

Codificaremos a seguir a palavra GALO.

A princípio colocaremos a palavra GALO em blocos, ou seja, separemos em sílabas e em seguida colocaremos seus respectivos valores.

Figura 12 – Bloco de vetores

| G | A | L | O |
|---|---|---|---|
| 7 | 1 | 12 | 15 |

Fonte: Elaborado pelo autor (2024)

Logo, em seguida escolhemos uma matriz quadrada de ordem 2 e inversível para facilitar os cálculos. Para que ela seja inversível, uma condição necessária é que ela seja não-singular, ou seja, o determinante da mesma tem de ser diferente zero.

$$A_2 = (a_{ij})_{2\times2} = \begin{pmatrix} 4 & 3 \\ 1 & 1 \end{pmatrix}$$

Observe que o determinante da matriz A é que é inversível módulo 26.

Vamos converter cada bloco em um vetor-coluna, pois assim podemos multiplicar a matriz pelo vetor de modo que a condição de existência de multiplicação de matrizes seja válida. Condição esta que trabalhamos no **Encontro 5**. Vamos cifrar o par G A da seguinte maneira ,segundo o Processo de Codificação apresentado anteriormente:

$$\begin{pmatrix} 4 & 3 \\ 1 & 1 \end{pmatrix} \cdot \begin{pmatrix} 7 \\ 1 \end{pmatrix} = \begin{pmatrix} 31 \\ 8 \end{pmatrix}$$

Sempre que ocorrer um número inteiro maior que 25, ele será substituído pelo resto da divisão deste inteiro por 26. Faremos sempre isso, pois estamos trabalhando com a aritmética dos inteiros módulo 26, uma vez que estamos considerando o alfabeto constituído de 26 letras. No cálculo anterior substituiremos 31 por 5, pois o resto da divisão de 31 por 26 é 5.

Assim,

$$\begin{pmatrix} 4 & 3 \\ 1 & 1 \end{pmatrix} \cdot \begin{pmatrix} 7 \\ 1 \end{pmatrix} = \begin{pmatrix} 31 \\ 8 \end{pmatrix} \equiv \begin{pmatrix} 5 \\ 8 \end{pmatrix} \pmod{26}$$

Portanto, o bloco G A cifrado será E H, pois o 5 está associado a letra E e o 8 está associado a letra H.

Por fim, vamos cifrar o último bloco, o par L O da seguinte maneira:

$$\begin{pmatrix} 4 & 3 \\ 1 & 1 \end{pmatrix} \cdot \begin{pmatrix} 12 \\ 15 \end{pmatrix} = \begin{pmatrix} 93 \\ 27 \end{pmatrix}$$

Como 93 e o 27 são maiores que 25, vamos substituir 93 pelo resto da divisão deste inteiro por 26, no caso 93 dividido por 26 deixa resto 15. E substituir o 27 pelo resto da divisão deste número inteiro por 26, logo 27 dividido por 26 deixa resto 1.

Assim,

$$\begin{pmatrix} 4 & 3 \\ 1 & 1 \end{pmatrix} \cdot \begin{pmatrix} 12 \\ 15 \end{pmatrix} = \begin{pmatrix} 93 \\ 27 \end{pmatrix} \equiv \begin{pmatrix} 15 \\ 1 \end{pmatrix} \pmod{26}$$

Logo, o bloco L O cifrado será O A. Percebe-se que a mensagem codificada será EHOA. Para decodificar esta mensagem, precisaremos encontrar a matriz inversa de A e multiplicar pelos vetores que formam o bloco codificado. Relembrando o **Encontro 5** que a inversa da matriz A pode ser calculada da seguinte forma:

$$A^{-1} = \frac{1}{DetM_2} \cdot (AdjM_2) = \frac{1}{DetM_2} \cdot \begin{pmatrix} a_{22} & -a_{12} \\ -a_{21} & a_{11} \end{pmatrix}$$

$$A_2 = (a_{ij})_{2\times 2} = \begin{pmatrix} 4 & 3 \\ 1 & 1 \end{pmatrix}$$

$$\text{Det } A_2 = a_{11} \cdot a_{22} - a_{21} \cdot a_{12} = 4 \cdot 1 - 1 \cdot 3 = 1.$$

$$A_2{}^{-1} = \tfrac{1}{1} \cdot \begin{pmatrix} 1 & -3 \\ -1 & 4 \end{pmatrix} = \begin{pmatrix} 1 & -3 \\ -1 & 4 \end{pmatrix}$$

Figura 13 – Bloco de vetores da mensagem codificada

| E | H | O | A |
|---|---|---|---|
| 5 | 8 | 15 | 1 |

Fonte: Elaborado pelo autor (2024)

Vamos converter cada bloco em vetor coluna, pois assim podemos multiplicar a matriz inversa pelo vetor de modo que a condição de existência de multiplicação de matrizes seja válida.

Vamos decodificar o par E H efetuando os seguintes cálculos, segundo o Processo de Decodificação apresentado anteriormente:

$$\begin{pmatrix} 1 & -3 \\ -1 & 4 \end{pmatrix} \cdot \begin{pmatrix} 5 \\ 8 \end{pmatrix} = \begin{pmatrix} -19 \\ 27 \end{pmatrix}$$

Sempre que ocorrer um número inteiro negativo, vamos realizar a seguinte operação $26 - 9 = 7$, portanto o resto da divisão de $-19$ por 26 será 7. No caso de 27 dividimos o mesmo por 26, teremos o resto 1. Como mostra o cálculo abaixo:

$$\begin{pmatrix} 1 & -3 \\ -1 & 4 \end{pmatrix} \cdot \begin{pmatrix} 5 \\ 8 \end{pmatrix} = \begin{pmatrix} -19 \\ 27 \end{pmatrix} \equiv \begin{pmatrix} 7 \\ 1 \end{pmatrix} \pmod{26}$$

Portanto, o bloco E H decodificado será G A.

Vamos decodificar o par O A da seguinte maneira:

$$\begin{pmatrix} 1 & -3 \\ -1 & 4 \end{pmatrix} \cdot \begin{pmatrix} 15 \\ 1 \end{pmatrix} = \begin{pmatrix} 12 \\ -11 \end{pmatrix}$$

Percebe-se que novamente o número negativo apareceu, logo basta subtrairmos 26 de 11: obtendo 15 como resultado. Logo, teremos a seguinte conclusão.

$$\begin{pmatrix} 1 & -3 \\ -1 & 4 \end{pmatrix} \cdot \begin{pmatrix} 15 \\ 1 \end{pmatrix} = \begin{pmatrix} 12 \\ -11 \end{pmatrix} \equiv \begin{pmatrix} 12 \\ 15 \end{pmatrix} \pmod{26}$$

Por fim, o bloco O A decodificado será L O. Portanto, quando juntamos a decodificação dos dois blocos obtemos a palavra G A L O.

Vale salientar que $\frac{1}{DetA}$ é o inverso multiplicativo de Det A $\pmod{26}$. A tabela seguir mostra o inverso multiplicativo para alguns valores de a $\pmod{26}$:

Figura 14 – Elementos inversos multiplicativo (mod 26)

| a | 1 | 3 | 5 | 7 | 9 | 15 | 17 | 19 | 21 | 23 | 25 |
|---|---|---|---|---|---|---|---|---|---|---|---|
| $a^{-1}$ | 1 | 9 | 21 | 15 | 3 | 7 | 23 | 11 | 5 | 17 | 25 |

Fonte: (ROSSETO, 2018)

**EXERCÍCIO 02:** Dada a matriz utilizada para codificar e decodificar a palavra galo, encontre a codificação e decodificação da palavra EU.

**EXERCÍCIO 03:** Dada a matriz utilizada para codificar e decodificar a palavra galo, encontre a codificação e decodificação da palavra SAPO.

### Sequência Didática I – Encontro 07

Nesta sequência didática, faremos uma reapresentação dos tópicos que foram abordados nos encontros anteriores, desde definições, propriedades e resultados importantes, através de um jogo lúdico, que será denominado de **"Trilha da Aritmética"**.

Vamos criar um tabuleiro com o propósito de tornar a Matemática mais atrativa e significativa para o aluno. Nossa intenção é mostrar de maneira clara e direta que por meio dos jogos podemos desenvolver um pensamento criativo e crítico (GRANDO, 2004).

É muito comum associarmos a ideia de jogo com o material concreto, que muitas vezes utilizamos em sala de aula, mas na verdade o jogo é mais do que isso, pode proporcionar uma interação social, um desenvolvimento maior cognitivo e estratégias lúdicas essenciais para processo de ensino/aprendizagem dos alunos.

Mas, é extremamente relevante o professor analisar as vantagens e desvantagens de um determinado jogo, de modo que as vantagens se sobressaiam mais que as desvantagens, o mediador deve organizar o trabalho pedagógico de forma que ele consiga transmitir os conceitos e definições de modo que alunos se sintam motivados e tenham o prazer de aprender (GRANDO, 2004).

Para elaborar a estratégia do jogo vamos definir quatro etapas, segundo (GRANDO, 2004):

- Familiarização com o jogo;
- Exploração inicial com objetivo de relembrar conceitos e definições já trabalhadas em aulas anteriores;
- Aplicação de uma estratégia vencedora, ou seja, trabalhar em equipe com o pensamento coletivo;
- Validar as concepções trabalhadas nos encontros anteriores.

Para isto, construímos uma trilha no tabuleiro enumerada de 1 até 30, onde o primeiro aluno ou equipe que alcançar a chegada da trilha será o vencedor. Cada aluno ou equipe participante da "Trilha da Aritmética" será representado por um peão. Será definido a ordem da largada do jogo que poderá ser através de um sorteio por meio dos dados ou de um acordo prévio entre os participantes. O primeiro jogador lançará o dado e o peão será movido no tabuleiro de acordo com o número sorteado.

Por exemplo, se o número sorteado no dado for o 4, o peão que corresponde o aluno ou equipe deverá ser movido no tabuleiro 4 casas. Quando ele chegar nessa casa haverá uma pergunta, caso o jogador acerte ele permanecerá na casa e caso ele erre ele voltará para a casa de onde ele partiu. O tabuleiro será composto também de **"casas surpresas"**: as quais podem apresentar um bônus ou um ônus. Na nossa Trilha essas casas serão identificadas com os números **2, 5, 8, 12, 16, 18, 24 e 29**. A casa de número 2 terá o seguinte bônus: "avance duas casas".

Já a casa 5 terá o seguinte ônus: **"volte ao início"**. Com relação a casa 8 teremos o seguinte ônus: "Volte uma casa". Já a casa 12 terá o seguinte bônus: "avance duas casas". Com relação a casa 16 teremos o seguinte ônus: **"Volte duas casas"**. Já a casa 18 terá o seguinte ônus **"Volte ao início"**.

Já na casa 24 teremos o seguinte bônus: **"Avance duas casas"** e Por fim, a última casa surpresa, a 29 terá o seguinte ônus: **"recue três casas"**. É importante destacar que o jogo aqui sugerido pode ser adaptado e modificado a depender da intenção de cada professor e de cada turma que irá participar da atividade. Destacamos ainda que esse jogo ele poderá ser adaptado para trabalhar diferentes conteúdos da Matemática. Acreditamos que essa experiência de atividade se bem planejada e organizada pode representar uma importante metodologia de ensino-aprendizagem para o ensino da Matemática.

# 5 Conclusões

A sequência didática aqui apresentada procurou mostrar a validade do uso de aspectos vivenciados no curso de Mestrado Profissional em Matemática em Rede Nacional (PROFMAT). Onde foram obtidos os conhecimentos preliminares necessários para sua realização e execução, e também pela experiência em sala de aula, retomando aos conceitos e propriedades da Aritmética na Escola Estadual de Ensino Fundamental e Médio Major Veneziano Vital do Rêgo, no município de Campina Grande-PB, para alunos da 3ª ano do Ensino Médio do turno matutino.

O objetivo deste trabalho foi de evidenciar a sequência didática, aos alunos, aos professores e futuros professores quanto a eficacia dessas ferramentas para as aulas de Aritmética.

Os encontros com os alunos, realizados aos sábados, mostrou o quanto é importante o professor conhecer a realidade e a estrutura da escola para que o ensino seja consistente.

Para nós professores é fundamental planejar, organizar e estruturar os encontros para que haja um aprendizagem e estratégia pedagógica eficiente.

Durante estes encontros obtivemos resultados positivos e também dificuldades, que tivemos que superar. Foi neste ambiente que sentimos a necessidade de colocar em prática nosso trabalho acadêmico e abordar alguns tópicos relevantes estudados na disciplina MA 14 - Aritmética do curso de Mestrado Profissional em Matemática (PROFMAT), na intenção de promover um ensino/aprendizagem de qualidade.

A proposta de fazer uma retomada dos conteúdos iniciais de Aritmética oferece a oportunidade especial para os alunos buscarem esses conceitos detalhadamente, melhorando e desenvolvendo suas habilidades e competências em diversas áreas da matemática.

Com isto, a nossa intenção é tornar o aluno protagonista do seu conhecimento, deixando o mesmo a vontade para esclarecer dúvidas e propor novos caminhos para responder uma determinada questão.

Vale ressaltar que propomos algumas atividades para escutar o aluno, deixando sempre a liberdade de opinar e discutir sobre suas inquietações, a fim de melhorar o processo de ensino/aprendizagem. Fizemos uma abordagem sobre o conhecimento aritmético do aluno deixando bem claro que não haveria a exposição da nota e nem críticas sobre o seu conhecimento.

Em seguida, nos encontros trabalhamos diversos conceitos retirados principalmente da página das Olimpíadas Brasileira de Matemática das Escolas Públicas (OBMEP), Programa de Iniciação Científica (PIC), Revista do Professor de Matemática (RPM)

e outras fontes que consideramos imprescindíveis para a formação do conhecimento matemático.

De maneira resumida, este produto educacional representa apenas uma pequena fração do que pode ser explorado em Aritmética. Sugestões, críticas, comentários e correções sempre serão bem-vindos para melhorar a qualidade deste trabalho.

# Referências


ARAÚJO, D. L. de. O que é (e como faz) sequência didática? *Entrepalavras*, v. 3, n. 1, p. 322–334, 2013. Citado 2 vezes nas páginas 4 e 9.

BALESTRA, M. M. M. *A psicopedagogia em Piaget: uma ponte para a educação da liberdade*. [S.l.]: Editora Ibpex, 2012. Citado na página 9.

BOLDRINI, J. L. et al. Álgebra linear, 3a edição. *Sao Paulo: Editora Harbra Ltda*, 1980. Citado na página 29.

BRASIL. *Base Nacional Comum Curricular*. 2018. <http://basenacionalcomum.mec.gov.br/images/BNCC_EI_EF_110518_versaofinal_site.pdf>. Acesso em: 12 jul. 2023. Citado 2 vezes nas páginas 5 e 6.

CADAR, L.; DUTENHEFNER, F. Encontros de aritmética. *Apostila do PICOBMEP*, 2015. Citado na página 17.

COUTINHO, S. C. Criptografia. *Rio de Janeiro, Programa de Iniciação Científica da OBMEP (PIC-OBMEP)*, 2015. Citado 2 vezes nas páginas 23 e 30.

DANTE, L. R. Matemática: contexto & aplicações. v. 2. *São Paulo: Ática*, 2013. Citado na página 25.

DOLCE, O.; IEZZI, G.; MACHADO, A. *Matemática e Realidade. 6º ao 9º ano*. [S.l.]: São Paulo: Atual, 2009. Citado 3 vezes nas páginas 17, 18 e 20.

GRANDO, R. C. O jogo e a matemática no contexto da sala de aula. *São Paulo: Paulus*, p. 07–38, 2004. Citado na página 36.

HEFEZ, A. Iniciação à aritmética. *Sociedade Brasileira de Matemática*, 2009. Citado 3 vezes nas páginas 11, 15 e 22.

HEFEZ, A.; ARITMÉTICA, C. P. Sociedade brasileira de matemática. 2009. Citado 5 vezes nas páginas 11, 14, 16, 18 e 24.

HYGINO, D. Fundamentos da aritmética. *S. Paulo: Atual*, 1991. Citado 2 vezes nas páginas 10 e 23.

IEZZI, G. et al. *Matemática: ciência e aplicações*. [S.l.]: Atual, 2001. Citado na página 26.

IEZZI, G.; HAZZAN, S. *Fundamentos de matemática elementar, 4: sequências, matrizes, determinantes, sistemas*. [S.l.]: Atual, 2004. Citado 4 vezes nas páginas 25, 27, 28 e 29.

KIM, D.; SOLOMON, M. G. Fundamentos de segurança de sistemas de informação. *Rio de Janeiro: LTC*, p. 653–659, 2014. Citado na página 31.

PACCOLA, E. B. e H. *Matemática*: Versão beta - 2 grau. [S.l.]: Moderna, 1995. ISBN 85-16-01359-6. Citado na página 29.

PARAÍBA. *Proposta Curricular do Novo Ensino Médio da Paraiba*. 2021. Diponível em <https://paraiba.pb.gov.br/arquivos/pdfs/PropostaCurriculardoEnsinoMdiodaParabaPCEMPB23.pdf>. Acesso em: 12 jul. 2023. Citado 3 vezes nas páginas 5, 6 e 7.

ROSSETO, C. K. Criptografia como recurso didático: uma proposta metodológica aos professores de matemática. Universidade Estadual Paulista (Unesp), 2018. Citado 3 vezes nas páginas 31, 32 e 36.

SOUSA, R. M. d. *Uma proposta de ensino da Aritmética por meio de sequências didáticas: um passeio pela história, conceitos e aplicações*. Dissertação (Mestrado) — Universidade Federal de Campina Grande - UFCG, 2024. Citado na página 4.

TELÁRIS, P. *Matemática/Luiz Roberto Dante.–*. [S.l.]: São Paulo, 2012. Citado na página 17.

WOLTMAN, G. *GIMPS: Great Internet Mersenne Primes Search.[S. l.]*. 1996. Diponível em <https://www.mersenne.org/>. Acesso em: 26 mar. 2023. Citado 2 vezes nas páginas 16 e 17.

ZABALA, A. *A prática educativa: como ensinar*. [S.l.]: Penso Editora, 1998. Citado 2 vezes nas páginas 4 e 9.