UNIVERSIDADE ESTADUAL DO CEARÁ

CENTRO DE CIÊNCIA E TECNOLOGIA

CURSO DE MESTRADO PROFISSIONAL EM ENSINO DE MATEMÁTICA

ALAN DÉRICK DE ARAUJO LIMA

ANÁLISE COMPARATIVA DE CRITÉRIOS DE DIVISIBILIDADE POR 7: TEORIA E TECNOLOGIA.

FORTALEZA – CEARÁ

2021

ALAN DERICK DE ARAUJO LIMA

ANÁLISE COMPARATIVA DE CRITÉRIOS DE DIVISIBILIDADE POR 7: TERORIA E TECNOLOGIA.

Dissertação apresentada ao Curso de Mestrado Profissional em Matemática em Rede Nacional do Programa de Pós-Graduação em Matemática do Centro de Ciências e Tecnologia da Universidade Estadual do Ceará, como requisito parcial para obtenção do Título de Mestre em Ensino de Matemática.

Orientador: Prof°. Dr. Daniel Brandão de Menezes.

FORTALEZA – CEARÁ

2021

Dados Internacionais de Catalogação na Publicação
Universidade Estadual do Ceará
Sistema de Bibliotecas

Lima, Alan Derick de Araujo.
Análise Comparativa de Critérios de Divisibilidade por 7: Teoria e Tecnologia [recurso eletrônico] / Alan Derick de Araujo Lima. - 2021.
88 f. : il.

Dissertação (MESTRADO PROFISSIONAL) - Universidade Estadual do Ceará, Centro de Ciências e Tecnologia, Curso de Mestrado Profissional Em Matemática Rede Nacional - Profissional, Fortaleza, 2021.
Orientação: Prof. Dr. Daniel Brandão de Menezes.
1. Aritmética. 2. Critérios de Divisibilidade. 3. Divisibilidade. 4. Números primos. 5. Linguagem Pascal.. I. Título.

ALAN DERICK DE ARAUJO LIMA

ANÁLISE COMPARATIVA DE CRITÉRIOS DE DIVISIBILIDADE POR 7: TEORIA E TECNOLOGIA.

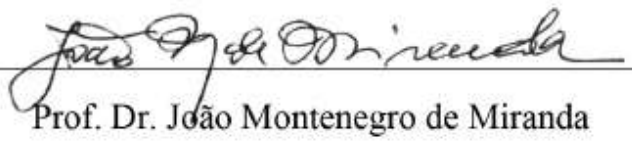
Dissertação apresentada ao Curso de Mestrado Profissional em Matemática do Programa de Pós-Graduação em Matemática em Rede Nacional do Centro de Ciências e Tecnologia da Universidade Estadual do Ceará, como requisito parcial para à obtenção do Título de Mestre em Matemática. Área de concentração: Matemática.

Aprovada em: 03 de maio de 2021.

BANCA EXAMINADORA:

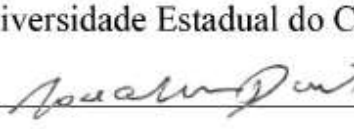
Prof. Dr. Daniel Brandão Menezes (Orientador)

Universidade Estadual Vale do Acaraú - UVA



Prof. Dr. João Montenegro de Miranda

Universidade Estadual do Ceará - UECE



Prof. Dr. José Othon Dantas Lopes - UFC

Universidade Federal do Ceará

Dedico este trabalho,

À minha companheira por sempre estar ao meu lado, aos meus filhos e à minha mãe.

AGRADECIMENTOS

À Deus por me encher de força e determinação para prosseguir em frente nesse árduo trabalho.

À minha companheira, por sempre estar ao meu lado, por ter me dado o melhor presente da vida, dois filhos, por dividir bons momentos, por me amar e acreditar em meus sonhos.

À minha mãe, por acreditar em meus sonhos. Por enxergar que, quanto melhor é adquirir a conhecimento do que o ouro, e quanto mais excelente é escolher o entendimento do que a prata.

Aos professores Claudemir Leandro, Leo Ivo, Manoel Pereira, Nicolas Alcântara e Tiago Caúla Ribeiro que foram os meus professores nas disciplinas do curso.

Ao professor João Montenegro que me orientou no trabalho e me ajudou a melhorá-lo com sugestões acerca do conteúdo.

Ao professor Daniel Brandão que, também, me orientou no trabalho e me ajudou a melhorá-lo com sugestões acerca do conteúdo.

“Os números governam o mundo”.

(Platão)

RESUMO

Critérios de divisibilidade são pouco ensinados na educação básica. Vê-se apenas no 6º ano do Ensino Fundamental e em provas olímpicas de matemática. Além disso, é um tema belo e muito vasto da teoria dos números, pois existem vários critérios de divisibilidade para um mesmo número. Por isso, faz-se necessária uma investigação sobre o critério que necessita de menos operações para verificar se um número é divisível por outro. O objetivo geral do presente trabalho é estabelecer comparações entre diferentes critérios de divisibilidade por 7. Os objetivos específicos do trabalho são: apresentar os critérios de divisibilidade por 2, 3, 4, 5, 6, 7, 8, 9 e 10, mostrar como construir um critério de divisibilidade e investigar uma ferramenta computacional para determinar se um número é primo. Primeiramente, foi feita uma pesquisa bibliográfica para desenvolver a fundamentação teórica e o capítulo Construindo Critérios de Divisibilidade. Para isso foram utilizados os livros de Hefez (2006), Oliveira (2010), Alencar (1987), Burton (1980) e Santos (1998), as dissertações de Shimokawa (2020) e Silva (2019) e o artigo de Ribeiro (2020). Em seguida, utilizou-se uma linguagem de programação (Pascal) para construir os algoritmos para mostrar os divisores de um número com o intuito de determinar se um número é primo e para gerar critérios de divisibilidade por um número primo. Posteriormente, é apresentado os critérios de divisibilidade de Pascal, de Zbikowski, de Chika Ofili e outros, e estabelecida uma comparação entre eles para observar qual necessita de menos operações e iterações na verificação. Por fim, foram apresentadas algumas considerações, mostrando, de forma breve, as dificuldades enfrentadas na pesquisa, as perspectivas futuras e uma reflexão sobre a metodologia empregada.

Palavras-chave: Aritmética. Critérios de divisibilidade. Divisibilidade. Números Primos Linguagem Pascal.

ABSTRACT

Divisibility criteria are poorly taught in basic education. It is only seen in the 6th year of elementary school and in Olympic mathematics tests. In addition, it is a beautiful and very vast theme of number theory, as there are several criteria of divisibility criteria the same number. For this reason it is necessary to investigate the criterion that requires fewer operations to verify whether a number is divisible by another or not. The general objective of the present work is to establish comparisons between different criteria of divisibility by 7. The specific objectives of the work are: to present the criteria of divisibility by 2, 3, 4, 5, 6, 7, 8, 9 and 10, to show how build a divisibility criterion and investigate a computational tool to determine whether a number is prime. First, a bibliographic search was carried out to develop the theoretical foundation and the chapter Constructing Divisibility Criteria. For this purpose, the books Hefez (2006), Oliveira (2010), Alencar (1987), Burton (1980) and Santos (1998), the dissertations of Shimokawa (2020) and Silva (2019) and the article by Ribeiro (2020). Then a programming language (Pascal) was used to build the algorithms to show the divisors of a number in order determine whether a number is prime and to generate criteria for divisibility by a prime number. Subsequently, the divisibility criteria of Pascal, Zbikowski, Chika Ofili and others are presented, and a comparison between them is established to see which one needs fewer operations and iterations in the verification. Finally, some considerations were presented showing, briefly, the difficulties faced in the research, the future perspectives and a reflection on the methodology employed.

Keywords: Arithmetic. Divisibility criteria. Divisibility. Prime numbers. Pascal language.

LISTA DE FIGURAS

Figura 1 - Regiões do Plano 19
Figura 2 - Exemplo de Fluxograma 53
Figura 3 - Principais formas de um fluxograma 54
Figura 4 - Forma geral de representação de um algoritmo em pseudocódigo 55
Figura 5 - Algoritmo Soma_dois_Numeros 56
Figura 6 - Professor Niklaus Wirth 56
Figura 7 - Instalando o Dev-Pascal - 1ª Janela 58
Figura 8 - Instalando o Dev-Pascal - 2ª Janela 58
Figura 9 - Instalando o Dev-Pascal - 3ª Janela 58
Figura 10 - Tela inicial 59
Figura 11 - Criando novo arquivo Dev Pascal 60
Figura 12 - Salvando o arquivo Dev Pascal 60
Figura 13 - Nomeando o arquivo Dev Pascal 61
Figura 14 - Algoritmo Soma_dois_Numeros em Pascal 62
Figura 15 - 2º Algoritmo Soma_dois_numeros em Pascal 63
Figura 16 - Algoritmo Média_02 em Pascal 64
Figura 17 - Algoritmo Quadrado_Perfeito em Pascal 65
Figura 18 - Algoritmo divisores de um número em Pascal 66
Figura 19 - Obtendo os divisores de 60 através do programa divisores 66
Figura 20 - Algoritmo para determinar se um número é primo em Pascal 68
Figura 21 - Verificando se o número 7 é primo através do programa Primo 68
Figura 22 - Verificando se o número 30 é primo através do programa Primo 69
Figura 23 - Algoritmo para gerar critérios de divisibilidade em Pascal 70
Figura 24 - Gerando os critérios de divisibilidade de Chika Ofili e Zbikowski 70

LISTA DE TABELAS

Tabela 1 - Crivo de Erastóstenes 31
Tabela 2 - Critérios de divisibilidade de alguns números primos 50
Tabela 3 - Critérios de divisibilidade por 7 utilizando a quebra na dezena 75
Tabela 4 - Critérios de divisibilidade por 7 utilizando a quebra na centena 77
Tabela 5 - Comparando alguns critérios de divisibilidade 7 83

SUMÁRIO

1 INTRODUÇÃO 13
2 FUNDAMENTAÇÃO TEÓRICA 16
2.1 Princípio de Indução 16
2.2 Divisibilidade 20
2.3 Sistema de numeração decimal 25
2.4 Números primos 28
2.5 Critério de divisibilidade por 2, 4 e 8 31
2.6 Critério de divisibilidade por 3 e 9 33
2.7 Critério de divisibilidade por 6 36
2.8 Critério de divisibilidade por 5 e 10 37

3 CONSTRUINDO CRITÉRIOS DE DIVISIBILIDADE 39
3.1 Congruência modular 39
3.2 Aplicações da congruência modular 41
3.3 Construção de critérios de divisibilidade 44
3.4 Critério de divisibilidade por 11 e 13 48
3.5 Critério de divisibilidade por 17 e 19 49
3.6 Tabela de critério de divisibilidade 50

4 A LINGUAGEM PASCAL 51
4.1 Introdução à lógica de programação 51
4.2 Um breve histórico sobre a linguagem Pascal 55
4.3 Ambiente de programação Dev Pascal 56
4.4 Estrutura de programação em Pascal 60
4.5 Algoritmo para determinar os divisores de um número 64
4.6 Algoritmo para determinar se um número é primo 66
4.7 Algoritmo para gerar critérios de divisibilidade 68

5 ALGUNS CRITÉRIOS DE DIVISIBILIDADE POR 7 71
5.1 Critério de divisibilidade por 7 de Blaise Pascal 71
5.2 Critério de divisibilidade por 7 de Zbikowski 72
5.3 Critério de divisibilidade por 7 de Chika Ofili 72
5.4 Critério de divisibilidade por 7 (Quebra na dezena) 73
5.5 Critério de divisibilidade por 7 (Quebra na centena) 74
5.6 Critério de divisibilidade por 7 (Das classes) 76
5.7 Mais um critério de divisibilidade por 7 77
5.8 Comparando os critérios de divisibilidade por 7 79

6 CONSIDERAÇÕES FINAIS..... 83
REFERÊNCIAS..... 84
ANEXOS..... 86

1 INTRODUÇÃO

A teoria dos números é a parte da matemática que estuda os enigmas dos números e teve sua origem na Grécia antiga. Os belos problemas ligados a esta área constituem, até hoje, uma das mais importantes fontes que inspiram os apreciadores da Matemática. Além disso, essa área possui diversas aplicações vantajosas à humanidade, como por exemplo, o processo de criptografia usado em transações pela internet. (OLIVEIRA, 2010).

Os critérios de divisibilidade aparecem da necessidade de saber se um certo número n é divisível por outro número b sem precisar usar o algoritmo da divisão euclidiana. Portanto, eles são muito importantes no que diz respeito a praticidade. Os critérios de divisibilidade são consequências do modo como representamos frequentemente os números naturais utilizando o sistema decimal (SILVA, 2019)

Em Brasil (2018, p. 301), na Base Nacional Comum Curricular (BNCC), no 6º ano do Ensino Fundamental traz na temática números a seguinte habilidade.

> (EF06MA05): Classificar números naturais em primos e compostos, 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, 8, 9, 10, 100 e 1000.

Critérios de divisibilidade são pouco ensinados no ensino básico, aparecem apenas no 6º ano do Ensino Fundamental. Além disso, é um assunto que aparece em prova de olimpíadas. Por isso, é necessário fazer um estudo mais detalhado do assunto uma vez que é cobrado de forma muito básica apenas no 6º ano e de maneira um pouco mais aprofundada em provas olímpicas.

Além disso, é um tema belo e muito vasto da teoria dos números. Existem vários critérios de divisibilidade para um mesmo número e surge daí a necessidade de utilizar o melhor para evitar perda de tempo nas verificações.

Em 2020, ao participar de um programa de aperfeiçoamento de professores (OBMEP na Escola) que possuía três módulos: aritmética, geometria e combinatória. No módulo de aritmética, foram apresentados alguns critérios de divisibilidade. Numa dessas apresentações foi comentado sobre a descoberta de um novo critério de divisibilidade por 7, feita por um jovem nigeriano de 12 anos.

Após esse critério de divisibilidade, foram pesquisados outros critérios de divisibilidade por 7, entre os quais, utilizando a quebra na dezena (remoção dos algarismos das

unidades e dezenas de um número) e a quebra na centena (remoção dos algarismos das unidades, dezenas e das centenas de um número). Daí surgiu a necessidade de saber qual desses critérios eram mais vantajosos computacionalmente.

Diante disto, o presente trabalho pretende responder a seguinte pergunta: qual é o critério de divisibilidade por 7 que necessita um menor número de operações na verificação de um número com 6 algarismos?

O objetivo geral do presente trabalho é:

- ✓ Estabelecer comparações entre diferentes critérios de divisibilidade por 7.

Os objetivos específicos são:

1. Apresentar os critérios de divisibilidade por 2, 3, 4, 5, 6, 7, 8, 9 e 10.
2. Mostrar como construir um critério de divisibilidade.
3. Investigar a ferramenta computacional Dev Pascal para determinar se um número é primo ou não.

A pesquisa do trabalho foi de caráter exploratória/bibliográfica. A pesquisa teve como fonte livros, artigos, monografias e dissertações. Os livros-texto utilizados foram Hefez (2006), Oliveira (2010), Alencar (1987), Burton (1980) e Santos (1998). Foram utilizadas as dissertações de Shimokawa (2020) e Silva (2019), também foi utilizado o artigo de Ribeiro (2020). Artigos, monografias, dissertações e outras referências foram acrescidas no decorrer da pesquisa.

O trabalho foi dividido em quatro capítulos: Fundamentação Teórica, Construindo Critérios de Divisibilidade, A Linguagem Pascal e Alguns Critérios de Divisibilidade por 7.

O segundo capítulo foi dedicado às bases fundamentais da aritmética. Foram apresentados o Princípio do Menor Elemento e o Princípio de Indução Finita. Depois foi apresentada a noção de divisibilidade e algumas de suas propriedades. Foi tratado, ainda, sobre a representação decimal de numeração e sobre os números primos. Por fim, foi feito um breve estudo sobre os critérios de divisibilidade comumente abordados nos livros de ensino básico.

Foi tratado, no terceiro capítulo, sobre congruência modular bem como algumas propriedades. Depois foram apresentados alguns exemplos em que podemos empregar a noção

de congruência modular. Foi apresentado, também, uma maneira de construir critérios de divisibilidade utilizando a quebra na unidade. Por fim, foi exibida uma tabela com alguns critérios de divisibilidade por alguns números primos.

No quarto capítulo, foi tratada sobre a linguagem Pascal. Foi feita uma introdução à lógica de programação, um breve histórico sobre a linguagem Pascal, uma apresentação do ambiente de programação Dev Pascal, uma apresentação da estrutura de programação em Pascal e foi apresentado alguns algoritmos utilizando a linguagem Pascal, dentre os quais: algoritmo para mostrar os divisores de um número, o algoritmo para determinar se um número é primo ou não e o algoritmo que gera critérios de divisibilidade por números primos.

Foi tratado, no quinto capítulo, sobre os critérios de divisibilidade por 7 de Pascal, de Zbikowski, de Chika Ofili, da quebra na dezena, da quebra na centena e outros. Depois foi verificado para um número de 6 dígitos cada critério de divisibilidade. Por fim, o número de operações e de iterações de cada critério de divisibilidade por 7 foi posto em uma tabela para observar qual necessitava de menos operações na verificação.

Nas considerações finais, foram apresentadas algumas considerações acerca do trabalho, mostrando as dificuldades enfrentadas na pesquisa, as perspectivas futuras e uma reflexão sobre a metodologia empregada.

2 FUNDAMENTAÇÃO TEÓRICA

Neste capítulo, tratamos de alguns resultados fundamentais para a compreensão e o desenvolvimento de assuntos posteriormente abordados. Para a demonstração de algumas proposições e de alguns teoremas são necessários alguns princípios fundamentais. Razão pela qual iniciamos o capítulo com esses princípios.

2.1 Princípio de indução finita

Utilizaremos neste capítulo e quando se fizer necessário as propriedades das operações e da ordem dos conjuntos dos números inteiros.

Definição: Seja $S \subset \mathbb{Z}$ e $a \in S$. Dizemos que a é o menor elemento de S se $a \leq x$, para todo $x \in S$. (ALENCAR FILHO, 1987)

Em outras palavras, um número a é o menor elemento de um conjunto dado se cada elemento desse conjunto for maior ou igual que a.

Definição: Seja $S \subset \mathbb{Z}$ e $c \in S$. Dizemos que S é limitado inferiormente se existir $c \in \mathbb{Z}$ tal que $c \leq x$ para todo $x \in S$. (HEFEZ, 2016)

O conjunto dos números naturais é limitado inferiormente e tem o número 1 como seu menor elemento. O conjunto dos inteiros negativos não é limitado inferiormente nem tem menor elemento.

Princípio da boa ordenação: Todo subconjunto não vazio de $\mathbb{N}$ possui um menor elemento. (ALENCAR FILHO, 1981)

Proposição: Não existe $n \in \mathbb{N}$ tal que $0 < n < 1$. (HEFEZ, 2016)

Demonstração: Suponha, que exista um número inteiro n tal que $0 < n < 1$. Seja $S = \{x \in \mathbb{N}; 0 < x < 1\}$. Então, o conjunto S não é vazio e é limitado inferiormente. Portanto, o conjunto S possui um menor elemento a. Como $0 < a < 1$, temos que:

$$0 < a^2 < a < 1$$

contrariando o fato de que a é o menor elemento de S. Consequentemente não existe inteiro entre 0 e 1.

Corolário: (Propriedade Arquimediana): Sejam $a, b \in \mathbb{Z}$, com $b \neq 0$. Então existe $n \in \mathbb{Z}$ tal que $nb > a$. (HEFEZ, 2016)

Demonstração: Como $|b| \neq 0$, da proposição anterior, temos que $|b| \geq 1$. Logo,

$$(|a| + 1)|b| \geq |a| + 1 > |a| \geq a$$

Portanto, existe $n = |a| + 1$ para $b > 0$ ou $n = -(|a| + 1)$ para $b < 0$ tal que $nb > a$.

O princípio abaixo é a primeira formulação do princípio de indução finita, para não haver confusão com a segunda formulação do mesmo princípio, chamamos de princípio de indução matemática.

Princípio de Indução Matemática: Sejam $S \subset \mathbb{N}$ tal que:

(i) $1 \in S$.
(ii) $n \in S \implies n + 1 \in S$
Então, $S = \mathbb{N}$. (HEFEZ, 2016).

Utilizaremos o seguinte princípio para demonstrar propriedades envolvendo números naturais. Esse é um dos princípios mais importantes da matemática, pois várias proposições precisam desse princípio para demonstrá-las.

Como consequência do Princípio da Indução Matemática enunciaremos a seguir o que chamamos de Princípio da Indução Finita.

Princípio de Indução Finita: Seja $a \in \mathbb{N}$ e seja $p(n)$ uma sentença aberta em $n \in \mathbb{N}$. Suponha que

(i) $p(a)$ é verdadeiro, e que
(ii) $\forall n \geq a$, $p(n)$ verdadeira $\Longrightarrow p(n+1)$ é verdadeira.
Então, $p(n)$ é verdadeira para todo $n \geq a$ (HEFEZ, 2016).

Exemplo: Mostre que $1 + 3 + 5 + \cdots + (2n-1) = n^2$, com $n \in \mathbb{N}$. (IEZZI, 2013)

A proposição é verdadeira para $n = 1$, pois $1 = 1^2$. Suponha a proposição seja verdadeira para um certo n, ou seja, $1 + 3 + 5 + \cdots + (2n-1) = n^2$, com $n \in \mathbb{N}$ e provemos que a mesma seja verdadeira para $n + 1$. Temos,

$$\underbrace{1 + 3 + 5 + \cdots + (2n-1)} + (2(n+1) - 1) = \underbrace{n^2} + (2(n+1) - 1) =$$
$$= n^2 + 2n + 1 =$$
$$= (n+1)^2.$$

Assim, a proposição é verdadeira para $n + 1$.

Pelo Princípio de Indução Finita, temos que $1 + 3 + 5 + \cdots + (2n-1) = n^2$, para todo $n \in \mathbb{N}$

Exemplo: Temos que $(1+x)^n \geq 1 + nx$, com $n \geq -1$ e $n \in \mathbb{N}$. (LIMA, 2006) Essa desigualdade é conhecida com Desigualdade de Jacques Bernoulli.

A proposição é verdadeira para $n = 1$, pois: $(1+x)^1 = 1 + 1 \cdot x$. Admitamos que a proposição seja verdadeira para um certo n e provemos que a mesma seja verdadeira para $n + 1$. Temos:

$$(1+x)^n \geq 1+nx \Longrightarrow (1+x)^n(1+x) \geq (1+nx)(1+x)$$
$$\Longrightarrow (1+x)^{n+1} \geq 1+x+nx+nx^2$$
$$\Longrightarrow (1+x)^{n+1} \geq 1+(n+1)x+nx^2$$

Como $nx^2 \geq 0$, segue-se que: $1+(n+1)x+nx^2 \geq 1+(n+1)x$.

Logo, $(1+x)^{n+1} \geq 1+(n+1)x$.

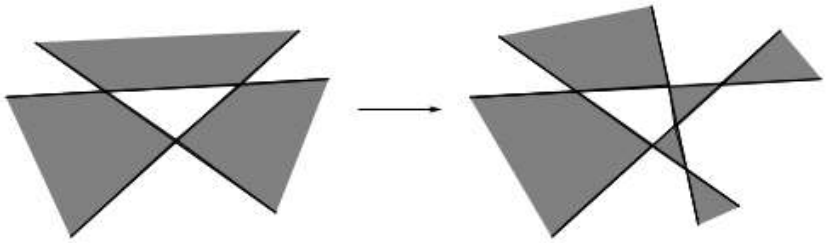
Portanto, $(1+x)^n \geq 1+nx$, para todo $n \in \mathbb{N}$.

Exemplo: Um número finito de linhas divide o plano em regiões. Mostre que essas regiões podem ser coloridas por duas cores, de forma que as regiões vizinhas tenham cores diferentes. (ANDREESCU, 2007).

Provamos essa proposição utilizando indução sobre n, onde n é o número de linhas. Para $n = 1$ temos que metade do plano será de uma cor e a outra metade de outra cor. Digamos cinza de um lado e branco do outro.

Suponha que sabemos como colorir um mapa definido por n linhas. Acrescentamos a $(n+1) -$ ésima linha à imagem e em seguida mantemos a cor da região de um lado dessa linha enquanto altera a cor das regiões do outro lado. Esta parte está ilustrada abaixo.

Figura 1: Regiões do Plano.



Fonte: ANDREESCU, 2007, p. 4.

Regiões que eram anteriormente adjacentes ainda têm cores diferentes. Regiões que compartilham um segmento da linha que antes faziam parte da mesma região, agora estão em lados opostos da linha. Logo, elas têm cores diferentes. Isso mostra que o novo mapa satisfaz a propriedade necessária.

Portanto, pelo Princípio de Indução Finita, essas regiões podem ser coloridas por duas cores, de forma que as regiões vizinhas tenham cores diferentes.

Utilizaremos o seguinte princípio para demonstrar um Teorema numa seção posterior. Daí a necessidade de enunciá-lo. É a terceira e última formulação do Princípio de Indução.

Princípio de Indução Completa: Seja $a \in \mathbb{Z}$ e seja $p(n)$ uma sentença aberta em $n \in \mathbb{Z}$. Suponha que

(i) $p(a)$ é verdadeiro, e que
(ii) $\forall n,\ p(a), p(a+1), \ldots,\ p(n)$ verdadeira $\Longrightarrow p(n+1)$ é verdadeira.
Então, $p(n)$ é verdadeira para todo $n \geq a$ (HEFEZ, 2016).

2.2 Divisibilidade

Definição: Um número inteiro a divide um número inteiro b se existir um número $q \in \mathbb{Z}$, tal que $b = aq$. (HEFEZ, 2016).

Usaremos a notação $a|b$ para representar o fato de que a divide b (OLIVEIRA, 2010). Essa noção será fundamental para as nossas demonstrações.

Proposição: Sejam $a, b\ e\ c \in \mathbb{Z}$. Tem-se que: (ALENCAR FILHO, 1981)

1) $1|a$, $a|a$ e $a|0$.

Demonstração: Temos que $a = a \cdot 1 \Longrightarrow 1|a$

$a = 1 \cdot a \Longrightarrow a|a$

$0 = 0 \cdot a \Longrightarrow a|0$

2) Se $a|b$ e $c|d$, então $ac|bd$.

Demonstração: Temos que $a|b \Longrightarrow b = a \cdot q,\ q \in \mathbb{Z}$

$c|d \Longrightarrow d = c \cdot s,\ s \in \mathbb{Z}$

Logo, $bd = (ac) \cdot (qs) \Longrightarrow ac|bd$.

3) Se $a|b$ e $b|c$, então $a|c$.

Demonstração: Temos que $a|b \Longrightarrow b = a \cdot q, \ \ q \in \mathbb{Z}$

$$b|c \Longrightarrow c = b \cdot s, \ \ s \in \mathbb{Z}$$

Logo, $c = bs = aqs \Longrightarrow a|c$.

O conjunto dos divisores inteiros de um número a é o conjunto formado por todos os divisores de a e será denotado por $D(a)$.

Exemplo: O conjunto dos divisores de 60 é o conjunto:

$$D(60) = \{\pm 1, \pm 2, \pm 3, \pm 4, \pm 5, \pm 6, \pm 12, \pm 15, \pm 20, \pm 30, \pm 60\}.$$

Proposição: Sejam $a, b \ \ e \ c \in \mathbb{Z}$. Se $a|b$ e $a|c$, então $a|(bx + cy)$, para todo $x, y \in \mathbb{Z}$. (HEFEZ, 2016).

Demonstração: Temos que:

$$a|b \Longrightarrow b = a \cdot q, \ \ q \in \mathbb{Z}$$

$$a|c \Longrightarrow c = a \cdot s, \ \ s \in \mathbb{Z}$$

Logo, $bx + cy = aqx + asy = a(qx + sy) \Longrightarrow a|(bx + cy)$.

Podemos utilizar a noção de divisibilidade juntamente com o Princípio de Indução Finita para demonstrar propriedades sobre números naturais.

Exemplo: Mostre que para qualquer $n \in \mathbb{N}$, $n^3 + 2n$ é sempre divisível por 3. (OLIVEIRA, 2010).

A proposição é verdadeira para $n = 1$, pois $1^3 + 2 \cdot 1 = 3$ é divisível por 3. Suponha a proposição seja verdadeira para um certo n, ou seja, $n^3 + 2n = 3q$, com $q \in \mathbb{N}$ e provemos que a mesma seja verdadeira para $n + 1$. Temos,

$$\begin{aligned}(n+1)^3+2(n+1) &= (n^3+3n^2+3n+1)+(2n+2)\\ &= (n^3+2n)+3(n^2+n+1)\\ &= 3q+3(n^2+n+1)\\ &= 3(q+n^2+n+1)\end{aligned}$$

Logo, $(n+1)^3+2(n+1)$ é divisível por 3.

Portanto, pelo Princípio de Indução Finita, temos que n^3+2n é divisível por 3 para todo $n \in \mathbb{N}$

Exemplo: Mostre que a soma dos cubos de três números naturais consecutivos é divisível por 9. (OLIVEIRA, 2010).

A proposição é verdadeira para $n=1$, pois $1^3+2^3+3^3 = 1+8+27 = 36 = 9 \cdot 4$ é divisível por 9.

Suponha a proposição seja verdadeira para um certo n, ou seja, $n^3+(n+1)^3+(n+2)^3 = 9q$, com $q \in \mathbb{N}$ e provemos que a mesma seja verdadeira para $n+1$. Temos,

$$\begin{aligned}(n+1)^3+(n+2)^3+(n+3)^3 &= (n+1)^3+(n+2)^3+n^3+9n^2+27n+27\\ &= \underbrace{n^3+(n+1)^3+(n+2)^3}+9(n^2+3n+3)\\ &= \quad 9q \quad + \quad 9(n^2+3n+3)\\ &= \quad 9(q+n^2+3n+3)\end{aligned}$$

Logo, $n^3+(n+1)^3+(n+2)^3$ é divisível por 9.

Portanto, pelo Princípio de Indução Finita, $n^3+(n+1)^3+(n+2)^3$ é divisível por 9 para todo $n \in \mathbb{N}$

Quando um número a não divide um número b fazemos uso de algoritmo conhecido como algoritmo da divisão, devido ao matemático grego Euclides de Alexandria.. Esse resultado é crucial para o desenvolvimento da teoria dos números.

Teorema (Algoritmo da Divisão): Sejam a e b dois números inteiros com $b \neq 0$. Existem dois únicos números inteiros q e r tais que:

$$b = aq + r,$$

com $0 \leq r < |a|$. (HEFEZ, 2016)

Demonstração: Provemos, primeiro, a existência dos números q e r.

Pela Propriedade Arquimediana existe $n \in \mathbb{Z}$ tal que, $n(-b) > -a$, logo $a - nb > 0$, isso mostra que $S = \{x = a - by; y \in \mathbb{Z}\} \cap (\mathbb{N} \cup \{0\})$ é não vazio e é limitado inferiormente por 0. Pelo Princípio da Boa Ordenação, temos que S possui um elemento $r = a - bq$ que é menor ou igual a todos os elementos de S, isto é, existem q e r inteiros tais que a = bq + r. Provemos que $r < |b|$. Suponhamos que $r \geq |b|$. Portanto, existe $s \in \mathbb{N} \cup \{0\}$ tal que $r = |b| + s$, então $0 \leq s < r$. Logo,

$$s = r - |b| = a - bq - |b| = a - b(q \pm 1) \in S,$$

com $s < r$. O que contradiz o fato de r ser o menor elemento S.

Vejamos, agora, a unicidade. Se $a = bq + r = bq' + r'$, onde q, q', r, r' são números inteiros, com $0 \leq r < |b|$ e $0 \leq r' < |b|$, então temos que $-|b| < r \leq r - r' \leq r' < |b|$. Portanto, $|r' - r| < |b|$. Temos, também, que $b(q - q') = r - r'$, o que implica em:

$$|b||q' - q| = |r' - r| < |b|$$

Isso só ocorre se $q' - q = 0$, ou seja, se $q = q'$. Decorre daí que $r = r'$. Assim, q e r são únicos.

Exemplo: Dividindo $a = 59$ por $b = 14$ obtemos o quociente $q = 4$ e o resto $r = 3$ que satisfazem as condições do algoritmo de Euclides. (ALENCAR FILHO, 1981)

$$59 = 14 \cdot 4 + 3 \text{ e } 0 \leq 3 < |14|.$$

Podemos, também, utilizar o Algoritmo da Divisão para demonstrar algumas propriedades sobre números inteiros.

Exemplo: O quadrado de um inteiro é da forma $5k$ ou $5k \pm 1$. (HEFEZ, 2016).

Seja n um inteiro qualquer. Pelo Algoritmo da Divisão, $n = 5q + r$, com $r \in \{0, 1, 2, 3, 4\}$. Assim, temos as seguintes possibilidades para n:

$$n = 5q, n = 5q + 1, n = 5q + 2, n = 5q + 3 \text{ e } n = 5q + 4$$

Elevando cada n ao expoente 2 temos:

para $n = 5q \Longrightarrow n^2 = (5q)^2 = 5 \cdot 5q^2 = 5 \cdot k$;

para $n = 5q + 1 \Longrightarrow n^2 = (5q + 1)^2 = 5 \cdot (5q^2 + 2q) + 1 = 5 \cdot k + 1$;

para $n = 5q + 2 \Longrightarrow n^2 = (5q + 2)^2 = 5 \cdot (5q^2 + 4q + 1) - 1 = 5 \cdot k - 1$;

para $n = 5q + 3 \Longrightarrow n^2 = (5q + 3)^2 = 5 \cdot (5q^2 + 6q + 2) - 1 = 5 \cdot k - 1$;

para $n = 5q + 4 \Longrightarrow n^2 = (5q + 4)^2 = 5 \cdot (5q^2 + 8q + 3) + 1 = 5 \cdot k + 1$.

Portanto, o quadrado de um inteiro é da forma $5k$ ou da forma $5k \pm 1$.

Definição: Chama-se divisor comum de dois inteiros a e b todo inteiro $d = 0$ tal que $d|a$ e $d\,|b$. (ALENCAR FILHO, 1981)

Exemplo: Sejam $a = 9$ e $b = 12$. Temos:

$$D(9) = \{\pm 1, \pm 3, \pm 9\}$$
$$D(12) = \{\pm 1, \pm 2, \pm 3, \pm 4, \pm 6, \pm 12\}$$

Os divisores comuns de 9 e 12 que denotaremos por $D(9,12)$ será o conjunto:

$$D(9,12) = \{\pm 1, \pm 3\}$$

Definição: Sejam a e b dois inteiros não nulos. Chama-se o máximo divisor comum de a e b o inteiro positivo d $(d > 0)$ que satisfaz as condições. (ALENCAR FILHO, 1981)

(1) $d|a$ e $d|b$
(2) Se $c|a$ e se $c|b$ então $c \leq d$.

Denotamos o máximo divisor comum de a e b por (a,b).

Exemplo: Sejam os inteiros $a = 16$ e $b = 24$. Os divisores comuns positivos de 16 e 24 são 1, 2, 4 e 8, e como 8 é o maior deles, segue-se que o máximo divisor comum de 16 e 24 é 8, ou seja, $(16, 24) = 8$.

Definição: Sejam a e b dois inteiros não nulos. Dizemos que a e b são primos entre si se, e somente se, $(a, b) = 1$. (ALENCAR FILHO, 1981)

Exemplo: Os números 2 e 5 são primos entre si, pois $(2, 5) = 1$.

Teorema: Dois números inteiros a e b não nulos, são primos entre si se, e somente se, existem inteiros x e y tais que $ax + by = 1$. (ALENCAR FILHO, 1981)

Demonstração: ($\Longrightarrow$) Se a e b são primos entre si, então $(a, b) = 1$ e portanto existem inteiros x e y tais que $ax + by = 1$.

($\Longleftarrow$) Se existem inteiros x e tais eu $ax + by = 1$ e se $(a, b) = d$, então da e $d|b$. logo, $d|(ax + by) = 1$ o que implica que $d = 1$ ou $(a, b) = 1$, isto é, a e b são primos ente si.

2.3 Sistema de numeração decimal

O sistema de numeração decimal, também conhecido como sistema de numeração na base 10, os números podem sem representados como uma sequência de 10 símbolos, constituídos pelos algarismos abaixo:

$$1, 2, 3, 4, 5, 6, 7, 8, 9, 0.$$

(OLIVEIRA, 2010)

Exemplo: O número 1.345 na base 10, é representação de

$$1 \cdot 10^3 + 3 \cdot 10^2 + 4 \cdot 10 + 5.$$

Cada algarismo de um número possui uma ordem que é contada da direita para a esquerda. Logo, o algarismo 5 pertence à 1ª ordem, o algarismo 4 pertence à 2ª ordem, o algarismo 3 pertence à 3ª ordem e o algarismo 1 pertence à quarta ordem.

Cada terna de ordens, que também são contadas da direita para esquerda recebe o nome de classe. As classes são separadas por um ponto. Em alguns países como Estados Unidos são separados por uma vírgula. (HEFEZ, 2016).

Temos a seguir os nomes das três primeiras classes juntamente com as suas ordens:

$$\textit{Classe das Unidades} \quad \begin{cases} \textit{unidades} & 1ª \text{ ordem} \\ \textit{dezenas} & 2ª \text{ ordem} \\ \textit{centenas} & 3ª \text{ ordem} \end{cases}$$

$$\textit{Classe do Milhar} \quad \begin{cases} \textit{unidades de milhar} & 4ª \text{ ordem} \\ \textit{dezenas de milhar} & 5ª \text{ ordem} \\ \textit{centenas de milhar} & 6ª \text{ ordem} \end{cases}$$

$$\textit{Classe do Milhão} \quad \begin{cases} \textit{unidades de milhão} & 7ª \text{ ordem} \\ \textit{dezenas de milhão} & 8ª \text{ ordem} \\ \textit{centenas de milhão} & 9ª \text{ ordem} \end{cases}$$

O sistema de numeração decimal surgiu e foi desenvolvido na China e na Índia, tem esse nome porque são utilizados 10 algarismos para representar os números. Além disso, esse sistema de numeração é posicional, ou seja, o algarismo possui um valor dependendo da posição que esteja no número. (HEFEZ, 2016).

Denotamos, de maneira geral, por $a = a_n a_{n-1} \dots a_1 a_0$ o número inteiro positivo. (OLIVEIRA, 2010)

$$a = a_n 10^n + a_{n-1} 10^{n-1} + \cdots + a_1 10 + a_0$$

O Teorema a seguir ilustra de uma maneira geral como os sistemas de numeração posicionais são organizados.

Teorema: Sejam dados os números inteiros a e b, com $a > 0$ e $b > 1$. Existem números inteiros $n \geq 0$ e $0 \leq r_0, r_1, \ldots, r_n < b$, com $r_n \neq 0$, univocamente determinados, tais que

$$a = r_0 + r_1 \cdot b + r_2 \cdot b^2 + \cdots + r_n \cdot b^n.$$

(HEFEZ, 2016).

Demonstração: Utilizaremos Indução Completa sobre a. Se $0 < a < b$ e tomando $n = 0$ e $r_0 = a$ temos que:

$$a = b^0 r_0 = r_0$$

Logo, a unicidade fica determinada.

Suponhamos que seja verdadeiro para um número menor do que a, em que $a \geq b$. Iremos mostrar que é verdadeira para a. Pelo Algoritmo da Divisão temos que existem q e r, únicos tais que:

$$a = bq + r, 0 \leq r < b. \quad (1)$$

Como $0 < q < a$, pela hipótese de indução, segue-se que existem números inteiros $k \geq 0$ e $0 \leq r_1, \ldots, r_{k+1} < b$, com $r_{k+1} \neq 0$ determinados de maneira única, tais que

$$q = r_1 + r_2 \cdot b + \cdots + r_{n'+1} \cdot b^k \quad (2)$$

Substituindo (2) em (1), temos:

$$a = bq + r = b(r_1 + r_2 \cdot b + \cdots + r_{n'+1} \cdot b^k) + r$$

Fazendo $r_0 = r$ e $n = k + 1$, segue-se o resultado.

2.4 Números primos

Numa seção posterior será tratado sobre a construção de critérios de divisibilidade por números primos, por isso se faz necessária uma breve abordagem sobre o assunto.

Definição: Número primo é todo número, maior do que 1, cujos únicos divisores positivos são a unidade e o próprio número. (ÁVILA, 2010)

Exemplo: Os números 2, 3, 5, 7, 11, 13, 17 e 19 são números primos, pois cada um deles possui apenas dois divisores positivos, 1 e ele próprio.

Definição: Número composto é todo número, maior do que 1, que não é primo. (ALENCAR FILHO, 1981)

Para saber se um número é composto basta verificar se o mesmo pode ser escrito como um produto de fatores primos. Veja o exemplo a seguir em que o número 60 é fatorado.

Exemplo: O números 60 é composto, pois pode ser escrito como o produto $2^2 \cdot 3 \cdot 5$, ou seja, além de si mesmo e 1 existem outros números que dividem 60.

Daí podemos concluir que um número inteiro positivo qualquer ou é primo ou é composto ou é 1.

Teorema Fundamental da Aritmética: Todo inteiro maior que 1 pode ser escrito como um produto de fatores primos. (HEFEZ, 2016)

Demonstração: Seja $S = \{n \in \mathbb{N}; n > 1$ e n não pode ser escrito como um produto de fatores primos$\}$. Basta mostrar que S é vazio. Por absurdo, suponha que S é diferente do vazio. Pelo Princípio da Boa Ordenação, S possui um menor elemento. Seja $a = \min S$. Temos que a não é primo. Portanto, $a = b \cdot c$, em que $1 < b < a$ e $1 < c < a$. Como b e c não pertencem ao conjunto S eles pdem ser escritos como um produto de números primos.

$$b = p_1 \cdot p_2 \cdot p_3 \cdot \ldots \cdot p_r$$
$$c = q_1 \cdot q_2 \cdot q_3 \cdot \ldots \cdot q_s$$

em que os números p_i e q_j são primos. Daí,

$$a = (p_1 \cdot p_2 \cdot p_3 \cdot \ldots \cdot p_r)(q_1 \cdot q_2 \cdot q_3 \cdot \ldots \cdot q_s) \Longrightarrow a \notin S$$

Logo, o conjunto S é vazio.

O Teorema a seguir decorre do Teorema Fundamental da Aritmética. Porém, não colocaremos aqui como um corolário, pois sua demonstração é considerada uma das mais belas da matemática. Além disso, se encontra num dos 13 livros de Euclides de Alexandria, mostrando daí a sua grande relevância na matemática.

Teorema: O conjunto dos números primos é infinito. (FERREIRA, 2014)

Demonstração: Suponha que existe uma quantidade finita de números primos e denotemos estes números por

$$p_1, p_2, p_3, \ldots, p_r,$$

Seja $n = p_1 \cdot p_2 \cdot p_3 \cdot \ldots \cdot p_r + 1 > 1$ um número inteiro. Logo, pelo Teorema Fundamental da Aritmética, existe um número primo p tal que $p|n$. Mas $p \nmid p_i$, com $i \in \{1, 2, 3, \ldots, r\}$, pois se p dividisse p_i então p dividiria 1, o que é impossível. Portanto, o conjunto dos números primos é infinito.

Proposição: Se $n \geq 2$, e nenhum primo p, com $2 \leq p \leq \sqrt{n}$, é um fator primo de n, então n é primo.

Demonstração: Seja n um número composto, temos pelo Teorema Fundamental da Aritmética que $n = p_1 \cdot p_2 \cdot p_3 \cdot \ldots \cdot p_r$, para fatores primos positivos $p_1, p_2, p_3, \ldots, p_r$, com $r \geq 2$ (pois se $r = 1$, n é um número primo). Daí temos que:

$p_1 \leq \sqrt{n}$ ou $p_2 \leq \sqrt{n}$, pois se $p_1 > \sqrt{n}$ e $p_2 > \sqrt{n}$, então

$$n = p_1 \cdot \ldots \cdot p_r \geq p_1 \cdot p_2 > \sqrt{n} \cdot \sqrt{n} = n.$$

o que é uma contradição.

Como p_1 e p_2 são fatores primos quaisquer de n, concluímos que, se $n \geq 2$ é um inteiro composto, n não pode ter dois fatores primos maiores que $\sqrt{n}$, ou seja, todos os fatores primos de n (com possível exceção de apenas um) são menores do que $\sqrt{n}$

Exemplo: Para testar se o número 137 é primo observamos, como o uso da calculadora que $\sqrt{137} \approx 11{,}70$.

Os números primos p satisfazendo $p \leq \sqrt{137} \approx 11{,}70$ são $2,\ 3,\ 5,\ 7\,, 11$. Verifica-se que 137 não é divisível por nenhum desses fatores, e portanto é um número primo.

Essa proposição pode ser usada para listar os números primos menores que ou iguais a n, com $n \in \mathbb{N}$. O procedimento para tal listagem é chamado Crivo de Eratóstenes, e consiste em listar os números menores que ou iguais a n crivando (demarcando) os múltiplos dos números primos menores do que ou iguais a $\sqrt{n}$.

Mostraremos, agora, como encontrar os números primos menores do que 100. Consideramos como pontos de partida os números primos p satisfazendo $2 \leq p \leq \sqrt{100} = 10$, os quais são 2, 3, 5 e 7.

Primeiramente, descartamos o número 1, que não é número primo. Depois, demarcamos (crivamos) os múltiplos de 2 maiores do que 2. Em seguida, crivamos os múltiplos de 3 maiores do que 3. Repete-se o procedimento para os números primos 5 e 7.

Além dos números 2, 3, 5 e 7, todos os números menores do que 100 que não foram crivados serão números primos, pois se um número n, $2 \leq p \leq 100$, não for um número primo então ele deverá ter um fator primo p satisfazendo $p \leq \sqrt{n} \leq \sqrt{100}$.

A tabela a seguir mostra todos os números compostos crivados (marcados) e o número 1 que também foi crivado. Todos os números que não foram crivados são os números primos menores do que 100.

Tabela 1: 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~~	~~33~~	~~34~~	~~35~~	~~36~~	37	~~38~~	~~39~~	~~40~~
41	~~42~~	43	~~44~~	~~45~~	~~46~~	47	~~48~~	~~49~~	~~50~~
~~51~~	~~52~~	53	~~54~~	~~55~~	~~56~~	~~57~~	~~58~~	59	~~60~~
61	~~62~~	~~63~~	~~64~~	~~65~~	~~66~~	67	~~68~~	~~69~~	~~70~~
71	~~72~~	73	~~74~~	~~75~~	~~76~~	~~77~~	~~78~~	79	~~80~~
~~81~~	~~82~~	83	~~84~~	~~85~~	~~86~~	~~87~~	~~88~~	89	~~90~~
~~91~~	~~92~~	~~93~~	~~94~~	~~95~~	~~96~~	97	~~98~~	~~99~~	~~100~~

Fonte: BURTON, 1980, p. 54.

2.5 Critérios de divisibilidade por 2, 4 e 8.

Deixamos reservada esta e as próximas subseções para alguns critérios de divisibilidade da habilidade EF06MA05 da Base Nacional Comum Curricular do Ensino Fundamental.

Um número é divisível por 2 quando seu último algarismo for divisível por 2, isto é, se o algarismo da unidade for divisível por 2, ou seja, forem 0, 2, 4, 6 ou 8. (SHIMOKAWA, 2020)

De outra maneira, temos a proposição seguinte:

Proposição: Um número da forma $N = 10a + b$ é divisível por 2 se, e somente se, b é divisível por 2. Sendo $N = ab = 10a + b$.

Demonstração: ($\Longrightarrow$) Temos, pela definição de divisibilidade, que $N = 10a + b$ é divisível por 2 quando existe $q \in \mathbb{Z}$ tal que $10a + b = 2q$. Logo,

$$10a + b = 2q \Longrightarrow b = 2q - 10a$$
$$\Longrightarrow b = 2q - 10a$$

$$\Longrightarrow b = 2(q - 5a)$$

Portanto, 2 divide b.

($\Longleftarrow$) Temos, pela definição de divisibilidade, que b é divisível por 2 quando existe $q \in \mathbb{Z}$ tal que $b = 2q$. Logo,

$$b = 2q \Longrightarrow b + 10a = 2q + 10a$$
$$\Longrightarrow b + 10a = 2(q + 5a)$$

Portanto, 2 divide $N = 10a + b$.

Exemplo: O número 1024 é divisível por 2 pois o algarismo da unidade é 4 e é divisível por 2.

Proposição: Um número da forma N = 100k + ab é divisível por 4 se, e somente se, ab é divisível por 4. Sendo $N = a_n \dots a_2 a_1 a_0 = a_n \dots a_2 ab = kab = 100k + ab$. (SANTOS, 1998).

Demonstração: ($\Longrightarrow$) Temos, pela definição de divisibilidade, que N = 100k + ab é divisível por 4 quando existe $q \in \mathbb{Z}$ tal que $100k + ab = 4q$. Logo,

$$100k + ab = 4q \Longrightarrow ab = 4q - 100k$$
$$\Longrightarrow ab = 4q - 100k$$
$$\Longrightarrow ab = 4(q - 25k)$$

Portanto, 4 divide ab.

($\Longleftarrow$) Temos, pela definição de divisibilidade, que ab é divisível por 4 quando existe $q \in \mathbb{Z}$ tal que $ab = 4q$. Logo,

$$ab = 4q \Longrightarrow ab + 100k = 4q + 100k$$

$$\Longrightarrow ab + 100k = 4(q + 25k)$$

Portanto, 4 divide $N = 100k + ab$.

Exemplo: O número 640 é divisível por 4 pois o número formado pelos dois últimos algarismos, 40 é divisível por 4.

Proposição: Um número da forma N = 1000k + abc é divisível por 8 se, e somente se, abc é divisível por 8. Sendo $N = a_n \dots a_3 a_2 a_1 a_0 = a_n \dots a_3 abc = kabc = 1000k + abc$.

Demonstração: ($\Longrightarrow$) Temos, pela definição de divisibilidade, que N = 1000k + abc é divisível por 8 quando existe $q \in \mathbb{Z}$ tal que $1000k + abc = 8q$. Logo,

$$1000k + abc = 8q \Longrightarrow abc = 8q - 1000k$$
$$\Longrightarrow abc = 8q - 1000k$$
$$\Longrightarrow abc = 8(q - 125k)$$

Portanto, 8 divide abc.

($\Longleftarrow$) Temos, pela definição de divisibilidade, que abc é divisível por 8 quando existe $q \in \mathbb{Z}$ tal que $abc = 8q$. Logo,

$$abc = 8q \Longrightarrow abc + 1000k = 8q + 1000k$$
$$\Longrightarrow abc + 1000k = 8(q + 125k)$$

Portanto, 8 divide $N = 1000k + abc$.

Exemplo: O número 1240 é divisível por 8 pois o número formado pelos três últimos algarismos, 240 é divisível por 8.

2.6 Critérios de divisibilidade por 3 e 9

Lema: Tem-se que 3 divide $10^n - 1$ para todo $n \in \mathbb{N}$. (CAMINHA, 2013).

Demonstração: Utilizaremos o princípio de indução.

(Caso base) Para n = 1 temos que

$$3|(10^1 - 1) = 10 - 1 = 9$$

(Passo indutivo) Suponha que a proposição seja verdadeira para um certo n, provemos que a mesma seja verdadeira para n+1. Temos,

$$\begin{aligned} 3|(10^n - 1) &\Longrightarrow 10^n - 1 = 3q \\ &\Longrightarrow 10(10^n - 1) = 30q \\ &\Longrightarrow 10^{n+1} - 10 = 30q \\ &\Longrightarrow 10^{n+1} - 1 - 9 = 30q \\ &\Longrightarrow 10^{n+1} - 1 = 9 + 30q \\ &\Longrightarrow 10^{n+1} - 1 = 3(3 + 10q) \end{aligned}$$

Portanto, pelo princípio da Indução Finita, temos que 3 divide $10^n - 1$ para todo $n \in \mathbb{N}$.

Proposição: Um número $N = a_n \ldots a_1 a_0$ é divisível por 3 se, e somente se, $a_0 + a_1 + \cdots + a_n$ é divisível por 3.

Demonstração: Temos que $N = 10^n a_n + \cdots + 10^1 a_1 + 10^0 a_0$ é divisível por 3 quando existe $q \in \mathbb{Z}$ tal que $10^n a_n + \cdots + 10^1 a_1 + 10^0 a_0 = 3q$. Logo,

$$\begin{aligned} &10^n a_n + \cdots + 10^1 a_1 + 10^0 a_0 = 3q \Leftrightarrow \\ \Leftrightarrow\ &(10^n - 1 + 1)a_n + \cdots + (10^1 - 1 + 1)a_1 + 1a_0 = 3\text{q} \\ \Leftrightarrow\ &\underbrace{(10^n - 1)a_n + \cdots + (10^1 - 1)a_1}_{S_1} + \underbrace{a_n + \cdots + a_1 + a_0}_{S_2} = 3q \end{aligned}$$

Pelo Lema $3|(10^n - 1)$ para todo $n \in \mathbb{N}$, logo

$3|(10^n - 1)a_n + \cdots + (10^1 - 1)a_1 = S_1$ e $S_1 = 3r$.

Assim,

$$(10^n - 1)a_n + \cdots + (10^1 - 1)a_1 + a_n + \cdots + a_1 + a_0 = 3q \Leftrightarrow$$
$$\Leftrightarrow S_2 = a_0 + a_1 + \cdots + a_n = 3q - 3r = 3(q - r)$$
$$\Leftrightarrow 3|a_0 + a_1 + \cdots + a_n$$

Exemplo: O número 135 é divisível por 3, pois 3 | (1+3+5) = 9.

Lema: 9 divide $10^n - 1$ para todo $n \in \mathbb{N}$.

Demonstração: Utilizaremos o princípio de indução.

(Caso base) Para n = 1 temos que

$$9|(10^1 - 1) = 10 - 1 = 9$$

(Passo indutivo) Suponha que a proposição seja verdadeira para um certo n, provemos que a mesma seja verdadeira para n+1. Temos,

$$\begin{aligned} 9|(10^n - 1) &\Longrightarrow 10^n - 1 = 9q \\ &\Longrightarrow 10(10^n - 1) = 90q \\ &\Longrightarrow 10^{n+1} - 10 = 90q \\ &\Longrightarrow 10^{n+1} - 1 - 9 = 90q \\ &\Longrightarrow 10^{n+1} - 1 = 9 + 90q \\ &\Longrightarrow 10^{n+1} - 1 = 9(1 + 10q) \end{aligned}$$

Portanto, pelo princípio da Indução Finita, temos que 9 divide $10^n - 1$ para todo $n \in \mathbb{N}$.

Proposição: Um número $N = a_n \dots a_1 a_0$ é divisível por 9 se, e somente se, $a_0 + a_1 + \cdots + a_n$ é divisível por 9. A demonstração é análoga à do critério anterior.

Demonstração: Temos que $N = 10^n a_n + \cdots + 10^1 a_1 + 10^0 a_0$ é divisível por 9 quando existe $q \in \mathbb{Z}$ tal que $10^n a_n + \cdots + 10^1 a_1 + 10^0 a_0 = 9q$. Logo,

$$10^n a_n + \cdots + 10^1 a_1 + 10^0 a_0 = 3q \Leftrightarrow$$
$$\Leftrightarrow (10^n - 1 + 1)a_n + \cdots + (10^1 - 1 + 1)a_1 + 1a_0 = 9q$$
$$\Leftrightarrow \underbrace{(10^n - 1)a_n + \cdots + (10^1 - 1)a_1}_{S_1} + \underbrace{a_n + \cdots + a_1 + a_0}_{S_2} = 9q$$

Pelo Lema, $9|(10^n - 1)$ para todo $n \in \mathbb{N}$, logo

$9|(10^n - 1)a_n + \cdots + (10^1 - 1)a_1 = S_1$ e $S_1 = 9r$.

Assim,

$$(10^n - 1)a_n + \cdots + (10^1 - 1)a_1 + a_n + \cdots + a_1 + a_0 = 9q \Leftrightarrow$$
$$\Leftrightarrow S_2 = a_0 + a_1 + \cdots + a_n = 9q - 9r = 9(q - r)$$
$$\Leftrightarrow 9|(a_0 + a_1 + \cdots + a_n)$$

Exemplo: O número 2493 é divisível por 9, pois 9 | (2+4+9+3) = 18.

2.7 Critério de divisibilidade por 6

Proposição: Um número $n = a_r \dots a_1 a_0$ é divisível por 6 se, e somente se, é divisível por 2 e por 3. (SILVA, 2019)

Demonstração: ($\Longrightarrow$) Seja $n \in \mathbb{N}$. Como $6|n$ então existe $q \in \mathbb{N}$ tal que $n = 6q$. Então, temos que $n = 2 \cdot 3q = 3 \cdot 2q \Longrightarrow n = 2r = 3s$, com r e s números inteiros. Consequentemente, pela definição de divisibilidade, $2|n$ e $3|n$. Logo, se n é divisível por 6 então n é divisível por 2 e 3.

($\Longleftarrow$) Suponhamos que $2|n$ e $3|n$. Logo, existem $k, l \in \mathbb{N}$ tais que $n = 2 \cdot k$ e $n = 3 \cdot l$. Temos que:

$$3 - 2 = 1 \Longrightarrow 3n - 2n = n \Longrightarrow 3 \cdot 2 \cdot k \ - 2 \cdot 3 \cdot l = n \Longrightarrow 2 \cdot 3 \cdot (k - l) = n$$
$$\Longrightarrow 6 \cdot (k - l) = n$$

Logo, pela definição de divisibilidade, $6|n$.

Portanto, n é divisível por 6 se, e somente se, n é divisível por 2 e por 3.

Exemplo: O número 132 é divisível por 6, pois é divisível por 2 (é par) e é divisível por 3 (1 + 2 + 3 = 6 é divisível por 3).

2.8 Critério de divisibilidade por 5 e 10

Proposição: Um número $N = a_n \ldots a_1 a_0$ é divisível por 5 se, e somente se, $a_0 = 0$ ou $a_0 = 5$. (SILVA, 2019)

Demonstração: Como $N = 10^k a_k + \cdots + 10a_1 + a_0$, então colocando 10 em evidência, temos:

$$N = 10(10^{k-1} a_k + \cdots + a_1) + a_0$$

Como 10 é divisível por 5, então N é divisível por 5 se, e somente se, a_0 for divisível por 5, ou seja, $a_0 = 0$ ou $a_0 = 5$.

Exemplo: O número 125 é divisível por 5, pois o algarismo da unidade é 5.

Proposição: Um número $N = a_n \ldots a_1 a_0$ é divisível por 10 se, e somente se, $a_0 = 0$. (SILVA, 2019)

Demonstração: Como $N = 10^k a_k + \cdots + 10a_1 + a_0$, então colocando 10 em evidência, temos:

$$N = 10(10^{k-1}a_k + \cdots + a_1) + a_0$$

Como 10 é divisível por 10, então N é divisível por 10 se, e somente se, a_0 for divisível por 10, ou seja, $a_0 = 0$.

Exemplo: O número 240 é divisível por 10, pois o algarismo da unidade é 0.

3 CONSTRUINDO CRITÉRIOS DE DIVISIBILIDADE

Neste capítulo trataremos de congruência modular e suas aplicações. Mostraremos como construir alguns critérios de divisibilidade, faremos a construção dos critérios de divisibilidade por 11, 13, 17 e 19 e mostraremos uma tabela com os critérios de divisibilidade por um número primo p menor que 100.

3.1 Congruência modular

Mostraremos, agora, algumas definições e proposições importantes sobre aritmética modular.

Definição: Seja m um número inteiro não nulo, positivo. Dois inteiros a e b serão ditos congruentes módulo m se os restos da divisão de a e b por m forem iguais. Quando a e b são congruentes módulo m, escrevemos

$$a \equiv b \ (mod\ m)$$

Caso os números não sejam congruentes, utiliza-se a notação $a \not\equiv b \ (mod\ m)$. (RIBEIRO, 2020)

Exemplo: Temos que $26 \equiv 11 \ (mod\ 5)$, pois se dividirmos 26 por 5 teremos resto 1 e se dividirmos 11 por 5 também teremos resto 1, ou seja, 26 e 11 deixam mesmo resto na divisão por 5.

Proposição: Se $a, b, m \in \mathbb{N}$, tem-se que $a \equiv b \ (mod\ m)$ se, e somente se, $m|(a - b)$. (RIBEIRO, 2020).

Demonstração: Sejam $a = mq + r$, com $0 \leq r < m$ e $b = mk + s$, com $0 \leq s < m$, as divisões euclidianas de a e b por m. Logo,

$$a - b = m(q - k) + (r - s)$$

Se $a \equiv b\ (mod\ m)$ então $r = s$ o que implica que $m|(a - b)$. Reciprocamente, se $m|(a - b)$ então $r - s = 0 \Longrightarrow r = s$, pois $|r - s| < m$.

Exemplo: Temos que $17 \equiv 1\ (mod\ 4)$, pois 4|(17 – 1) = 16.

Proposição (Propriedades da congruência)**:** Sejam a, b, c, d, m e $n \in \mathbb{Z}$, $n \geq 1$. Temos que:

1. Se $a \equiv b\ (mod\ m)$ e $c \equiv d\ (mod\ m)$ então $a + c \equiv b + d\ (mod\ m)$;

Demonstração: Temos que, se $a \equiv b\ (mod\ m)$ *e* $c \equiv d\ (mod\ m)$, então existem inteiros q e r tais que $a - b = qm$ e $c - d = rm$. Logo, $(a + c) - (b + d) = (a - b) + (c - d) = qm + rm = (q + r)m$, o que implica que $a + c \equiv b + d\ (mod\ m)$.

2. Se $a \equiv b\ (mod\ m)$ e $c \equiv d\ (mod\ m)$ então $ac \equiv bd\ (mod\ m)$;

Demonstração: Temos que, se $a \equiv b\ (mod\ m)$ *e* $c \equiv d\ (mod\ m)$, então existem inteiros q e r tais que $a - b = qm$ e $c - d = rm$.

Logo,

$$\begin{aligned} ac - bd &= (b + qm)(d + rm) - bd \\ &= bd + brm + dqm + qrm^2 - bd \\ &= (br + dq + qrm)m \end{aligned}$$

o que implica que $ac \equiv bd\ (mod\ m)$.

3. Se $a \equiv b\ (mod\ m)$ então $a^n \equiv b^n\ (mod\ m)$;

Demonstração: A proposição é verdadeira para $n = 1$ (por hipótese). Suponha que seja verdadeira para n e provemos que seja verdadeira para $n + 1$.

Temos:

$$a^n \equiv b^n\ (mod\ m)\ e\ a \equiv b\ (mod\ m).$$

Pela propriedade 2, temos:

$$a^n a \equiv b^n \, b(mod\ m) \implies a^{n+1} \equiv b^{n+1} \, (mod\ m),$$

Logo, a proposição é verdadeira para $n + 1$. Portanto, a proposição é verdadeira para todo $n \in \mathbb{N}$.

4. Se $a \equiv b \ (mod\ m)$ e $b \equiv c \ (mod\ m)$ então $a \equiv c \ (mod\ m)$.

Demonstração: Temos que, se $a \equiv b \ (mod\ m)$ *e* $b \equiv c \ (mod\ m)$, então existem inteiros q e r tais que $a - b = qm$ e $b - c = rm$.

Logo,

$$\begin{aligned} a - c &= (a - b) + (b - c) \\ &= qm + rm \\ &= (q + r)m \end{aligned}$$

o que implica que $a \equiv c \ (mod\ m)$.

3.2 Aplicações da congruência modular

Exemplo: Mostre que $41|(2^{20} - 1)$. (BURTON, 1980)

Começamos notando que $2^5 \equiv -9 \ (mod\ 41)$. Logo, pelo item 3 das Propriedades da congruência, temos que $(2^5)^4 \equiv (-9)^4 \ (mod\ 41) \implies 2^{20} \equiv 81 \cdot 81 \ (mod\ 41)$. Mas $81 \equiv -1 \ (mod\ 41)$, logo $81 \cdot 81 \equiv 1 \ (mod\ 41)$. Pela Propriedade 4 da congruência, temos

$$2^{20} \equiv 81 \cdot 81 \equiv 1 \ (mod\ 41)$$

Portanto, $41|(2^{20} - 1)$.

Exemplo: Mostre que $31|(20^{15} - 1)$. (MARTINEZ, 2018)

Equivalentemente, precisamos mostrar que $20^{15} \equiv 1 \ (mod\ 31)$ Começamos notando que $20 \equiv -11 \ (mod\ 31)$. Logo, pela parte 3 da Proposição, temos que $20^2 \equiv$

$(-11)^2\ (mod\ 31) \Longrightarrow 20^2 \equiv 121\ (mod\ 31)$. Mas $121 \equiv -3\ (mod\ 31)$, logo $20^2 \equiv -3\ (mod\ 31)$. Pela Propriedade 2 da congruência temos

$$20 \cdot 20^2 \equiv (-11) \cdot (-3)(mod\ 31) \Longrightarrow 20^3 \equiv 33\ (mod\ 31)$$

Como $33 \equiv 2\ (mod\ 31)$ então $20^3 \equiv 2\ (mod\ 31)$. Elevando a 5, temos que:

$$20^{15} \equiv 32\ (mod\ 31)$$

Como $32 \equiv 1\ (mod\ 31)$ então $20^{15} \equiv 1\ (mod\ 31)$. Portanto, $31|20^{15} - 1$.

Além de verificar se um número é divisível por outro utilizamos a congruência modular para descobrir o resto da divisão de um número.

Exemplo: Qual é o resto da divisão de 2^{45} ao ser dividido por 7 ? (DOMINGUES, 1991)

Começamos notando que $2^3 \equiv 1\ (mod\ 7)$. Logo, pela Propriedade 3 da congruência, temos que:

$$(2^3)^{15} \equiv 1^{15}\ (mod\ 7) \Longrightarrow 2^{45} \equiv 1(mod\ 7).$$

Portanto, o resto da divisão de de 2^{45} ao ser dividido por 7 é 1.

Exemplo: Determine o resto da divisão da soma $1! + 2! + 3! + 4! + \cdots + 99! + 100!$ por 12. (BURTON, 1980)

Observamos, primeiro, que $4! \equiv 24 \equiv 0\ (mod\ 12)$. Assim, para $k \geq 4$ temos que:

$$k! \equiv 4! \cdot 5 \cdot 6 \cdots k \equiv 0 \cdot 5 \cdot 6 \cdots k \equiv 0\ (mod\ 12)$$

Dessa forma, temos que:

$$1! + 2! + 3! + 4! + \cdots + 99! + 100! \equiv 1! + 2! + 3! + 0 + \cdots + 0 + 0 \equiv 9\ (mod\ 12)$$

Consequentemente, a soma em questão deixa resto 9 quando dividido por 12.

Podemos, também, utilizar congruência para demonstrar os critérios de divisibilidade. Seguem alguns critérios de divisibilidade e suas demonstrações utilizando congruência.

Proposição: Um número N é divisível por 9 se, e somente se, a soma de seus algarismos é divisível por 9.

Demonstração: Digamos que $N = a_n a_{n-1} \ldots a_1 a_0$. Como $10 \equiv 1\ (mod\ 9)$ então $10^n \equiv 1\ (mod\ 9)$. Assim,

$$\begin{aligned} a_0 &\equiv a_0\ (mod\ 9) \\ 10 \cdot a_1 &\equiv a_1\ (mod\ 9) \\ 10^2 \cdot a_2 &\equiv a_2\ (mod\ 9) \\ &\vdots \\ 10^n \cdot a_n &\equiv a_n\ (mod\ 9) \end{aligned}$$

Logo,

$$N = a_0 + 10 \cdot a_1 + 10^2 \cdot a_2 + \cdots + 10^n \cdot a_n \equiv a_0 + a_1 + a_2 + \cdots + a_n\ (mod\ 9)$$

Portanto, $N = a_n \ldots a_1 a_0$ é divisível por 9 se, e somente se, $a_0 + a_1 + \cdots + a_n$ é divisível por 9.

Proposição: Um número $N = a_n \ldots a_1 a_0$ é divisível por 11 se, e somente se, $a_0 - a_1 + \cdots + (-1)^n a_n$ é divisível por 11. (DOMINGUES, 1991)

Demonstração: Temos que, $10 \equiv -1\ (mod\ 11)$ então $10^n \equiv -1\ (mod\ 11)$ se n for ímpar e $10^n \equiv 1\ (mod\ 11)$ se n for par. Assim,

$$\begin{aligned} a_0 &\equiv a_0 \ (mod\ 11) \\ 10 \cdot a_1 &\equiv -a_1 \ (mod\ 11) \\ 10^2 \cdot a_2 &\equiv a_2 \ (mod\ 11) \\ &\vdots \\ 10^n \cdot a_n &\equiv (-1)^n \cdot a_n \ (mod\ 11) \end{aligned}$$

Logo,

$$N = a_0 + 10 \cdot a_1 + 10^2 \cdot a_2 + \cdots + 10^n \cdot a_n \equiv a_0 - a_1 + a_2 - \cdots + (-1)^n \cdot a_n \ (mod\ 11)$$

Portanto, $N = a_n \ldots a_1 a_0$ é divisível por 11 se, e somente se, $a_0 - a_1 + \cdots + (-1)^n a_n$ é divisível por 11.

3.3 Construção de critérios de divisibilidade

Definição: Chamamos de congruência linear em uma variável a uma congruência da forma $ax \equiv b \ (mod\ m)$, onde a e b são inteiros quaisquer, m é um inteiro positivo e x é uma incógnita. (ALENCAR FILHO, 1981)

Dessa forma, todo número inteiro x_0 tal que $ax_0 \equiv b \ (mod\ m)$ é uma solução da congruência linear.

Definição: Dizemos que uma solução da congruência $ax \equiv b \ (mod\ m)$ é unica módulo m, se quaisquer duas soluções são congruentes módulo m.

Exemplo: A congruência linear $3x \equiv 9 \ (mod\ 12)$ tem como uma solução o valor $x_0 = 3$, pois $3 \cdot 3 \equiv 9 \ (mod\ 12)$.

Como $12|(3x - 9)$ então existe $k \in \mathbb{Z}$ tal que $12k = 3x - 9$. Assim, $3x = 9 + 12k$ e consequentemente $x = 3 + 4k$. Logo, todos os inteiros da forma $3 + 4k$ também será solução da congruência linear.

Definição: Seja m um inteiro não nulo, positivo e a um inteiro qualquer. Dizemos que x é um inverso multiplicativo de a módulo m se vale a igualdade:

$$ax \equiv 1\ (mod\ m)$$

(RIBEIRO, 2020).

Exemplo: Um inverso multiplicativo de 3 módulo 7 é 5, pois $3 \cdot 5 \equiv 1\ (mod\ 7\ )$.

Teorema: Se a e m são inteiros primos entre si e $m > 1$, então existe um inverso multiplicativo de a módulo m. (MARTINEZ, 2018)

Demonstração: Como $(a, m) = 1$, então $sa + tm = 1$. Assim $sa + tm = 1\ (mod\ m)$. Como $tm = 0\ (mod\ m)$ segue-se que $sa = 1\ (mod\ m)$. Logo, s é o inverso de a modulo m.

Teorema: O inverso multiplicativo único. (MARTINEZ, 2018)

Demonstração: Se $ax_0 \equiv ax_0{}' \equiv 1\ (mod\ m)$ temos:

$$x_0 \equiv x_0 \cdot 1 \equiv x_0(ax_0') \equiv (x_0 a)x_0' \equiv 1 \cdot x_0' \equiv x_0'(mod\ m)$$

Logo, $x_0 \equiv x_0'(mod\ m)$ e o inverso multiplicativo é único.

Proposição: Se p é primo e x_0 é solução de $ax \equiv 1\ (mod\ p)$ então $-(p - x_0)$ é também solução de $ax \equiv 1\ (mod\ p)$.

Demonstração: Note, primeiro que: $x_0 \equiv -(p - x_0)\ (mod\ p)$, pois

$$p\big|(x_0 - (-(p - x_0))) = x_0 + p - x_0 = p.$$

Pela Propriedade 3 da congruência temos que, $x_0 \equiv -(p - x_0)\ (mod\ p)$ e $a \equiv a\ (mod\ p)$, então $ax_0 \equiv -a(p - x_0)(mod\ p)$. Agora, pela Propriedade 4 da congruência temos que $-a(p - x_0) \equiv ax_0 \equiv 1\ (mod\ p)$ então $-a(p - x_0) \equiv 1\ (mod\ p)$.

Esta última proposição será muito útil para a construção de critérios de divisibilidade pelo método da quebra na unidade. E também será utilizada na construção do algoritmo computacional em linguagem Pascal na seção seguinte.

Quebrar um número na unidade significa remover os algarismos da unidade para manipulá-los algebricamente. Assim, por exemplo, o número 248 torna-se $248 = 240 + 8$ quando quebramos a sua unidade.

Teorema (Quebra na unidade): Sejam $n = a_r a_{r-1} a_{r-2} \ldots a_2 a_1 a_0$ um número natural, p um número primo (diferente de 2 e 5) e $x \in \mathbb{Z}$ tal que $10x \equiv 1\ (mod\ p)$. O critério de divisibilidade por p então é o seguinte: se $m = a_r a_{r-1} a_{r-2} \ldots a_2 a_1 + x a_0$ então p divide n, se e somente, se p divide m. (RIBEIRO, 2020).

Demonstração: Temos que

$$n = a_r 10^r + a_{r-1} 10^{r-1} + a_{r-2} 10^{r-2} + \cdots + a_2 10^2 + a_1 10 + a_0 \quad (4)$$
$$m = a_r 10^{r-1} + a_{r-1} 10^{r-2} + a_{r-2} 10^{r-3} + \cdots + a_2 10 + a_1 + x a_0 \quad (5)$$

Multiplicando a equação (2) por 10 temos:

$$10m = a_r 10^r + a_{r-1} 10^{r-1} + a_{r-2} 10^{r-2} + \cdots + a_2 10^2 + a_1 10 + 10 x a_0 \quad (6)$$

Subtraindo a equação (4) pela equação (6) temos:

$$n - 10m = a_0 - 10 x a_0$$
$$n = 10m + (1 - 10x) a_0$$

Como x é o inverso multiplicativo de 10 módulo p, então o termo $(1 - 10x)$ é divisível por p. Logo,

$$n - 10m = kp$$

Portanto,

$$n \equiv 10m\ (mod\ p)$$

Assim, $p|10m$, se e somente, se $p|n$. Como p é primo e não divide 10 (pois p não é igual a 2 nem a 5), então temos que p divide n se, e somente se, p divide m.

Fazendo $a = a_n \dots a_1$ e $b = a_0$, um número natural da forma $n = 10a + b$ e p um número primo (diferente de 2 e 5) então $p|(10a + b)$, se e somente, se $p|(a + xb)$. Dessa forma, podemos construir critérios de divisibilidade por qualquer número primo diferente de 2 e 5.

Pelo Teorema da Quebra na Unidade, para construir um critério de divisibilidade por 3 precisamos encontrar um inverso multiplicativo de 10 módulo 3, ou seja, encontrar um $x \in \mathbb{Z}$ tal que $10x \equiv 1\ (mod\ 3)$. Como $10 \cdot 1 \equiv 1\ (mod\ 3)$ então 1 é o inverso multiplicativo de 10 módulo 3.

Portanto, dado um número natural da forma $N = 10a + b$ e $p = 3$, tem-se que $3|(10a + b)$, se e somente, se $3|(a + b)$.

Podemos verificar que o critério de divisibilidade por 3 da seção anterior é equivalente a esse critério.

Proposição: Um número $N = a_n \dots a_1 a_0$ é divisível por 3 se, e somente se, $a_n + \cdots + a_1 + a_0$ é divisível por 3.

Demonstração: Temos que, $3|a_n \dots a_1 a_0$ se, e somente se, $a_n \dots a_1 + a_0$. Como, $3|a_n \dots a_1 + a_0$ se, e somente se, $3|(10^{n-1}a_n + 10^{n-2}a_{n-1} + \cdots + 10a_2 + a_1 + a_0)$ e como:

$$\begin{aligned} 10^{n-1} &\equiv 1\ (mod\ 3) \\ 10^{n-2} &\equiv 1\ (mod\ 3) \\ &\vdots \\ 10^{1} &\equiv 1\ (mod\ 3) \\ 10^{0} &\equiv 1\ (mod\ 3) \end{aligned}$$

Então,

$$10^{n-1} \cdot a_n + 10^{n-2} \cdot a_{n-1} + \cdots + 10 \cdot a_2 + a_1 + a_0 \equiv a_n + a_{n-1} + \cdots + a_1 + a_0 (mod\ 3)$$

Logo, $3|a_n \dots a_1 a_0$ se, e somente se, $3|(a_n + a_{n-1} + \cdots + a_2 + a_1 + a_0)$.

3.4 Critérios de divisibilidade por 11 e 13

Pelo Teorema da Quebra na Unidade, para construir um critério de divisibilidade por 11 precisamos encontrar um inverso multiplicativo de 10 módulo 11, ou seja, encontrar um $x \in \mathbb{Z}$ tal que $10x \equiv 1\ (mod\ 11)$. Como $10 \cdot (-1) \equiv 1\ (mod\ 11)$ então (-1) é o inverso multiplicativo de 10 módulo 11.

Portanto, dado um número natural da forma $N = 10a + b$. Logo, $11|(10a + b)$, se e somente, se $11|(a - b)$.

Exemplo: Aplicando esse critério para 154, obtemos:

$$15 - 4 = 11$$

Como $11|11$, então $11|\ 154$.

Para construir um critério de divisibilidade por 13 precisamos encontrar um inverso multiplicativo de 10 módulo 13. Como $10 \cdot 4 \equiv 1\ (mod\ 13)$ então 4 é o inverso multiplicativo de 10 módulo 13.

Portanto, dado um número natural da forma $N = 10a + b$. Logo, $13|(10a + b)$ se e somente, se $13|(a + 4b)$.

Exemplo: Aplicando esse critério para 169, obtemos:

$$16 + 4 \cdot 9 = 16 + 36 = 52$$

Como $13|\ 52$, então $13|\ 169$.

Como estamos utilizando o Teorema para construir esses critérios de divisibilidade não é necessário demonstrar esses critérios. O Teorema já garante que esses critérios são verdadeiros.

É importante notar que a partir desse Teorema podemos construir infinitos critérios de divisibilidade por um número primo, pois há infinitos inversos multiplicativos de 10 módulo

p. Porém, não faz sentido encontrar inversos multiplicativos maior do que p, pois deixaria o critério computacionalmente ruim. Por isso, estamos interessados em encontrar apenas inversos multiplicativos menores do que p.

3.5 Critérios de divisibilidade por 17 e 19

Prosseguindo as construções de critérios de divisibilidade temos que, para construir um critério de divisibilidade por 17 precisamos encontrar um inverso multiplicativo de 10 módulo 17. Como $10 \cdot (-5) \equiv 1\ (mod\ 17)$ então (-5) é o inverso multiplicativo de 10 módulo 17.

Portanto, dado um número natural da forma $N = 10a + b$. Logo, $17|(10a + b)$, se e somente, se $17|(a - 5b)$.

Exemplo: Aplicando esse critério para 272, obtemos:

$$27 - 5 \cdot 2 = 17$$

Como $17|17$, então $17|\ 272$.

Para construir um critério de divisibilidade por 19 precisamos encontrar um inverso multiplicativo de 10 módulo 19. Como $10 \cdot 2 \equiv 1\ (mod\ 19)$ então 2 é o inverso multiplicativo de 10 módulo 19.

Portanto, dado um número natural da forma $N = 10a + b$. Logo, $19|(10a + b)$, se e somente, se $19|(a + 2b)$.

Exemplo: Aplicando esse critério para 304, obtemos:

$$30 + 2 \cdot 4 = 30 + 8 = 38$$

Como $38 = 2 \cdot 19$, então $19|\ 38$. Daí, como $19|\ 38$, então $19|\ 304$.

3.6 Tabela de critérios de divisibilidade por alguns primos

Nessa seção iremos mostrar uma tabela com os critérios de divisibilidade por alguns primos. Nessa tabela temos a forma aditiva e subtrativa de cada número primo, ou seja, há dois critérios de divisibilidade para cada número primo dado.

Tabela 2: Critérios de divisibilidade de alguns números primos

Número Primo	Forma Aditiva	Forma Subtrativa
3	$a+b$	$a-2b$
7	$a+5b$	$a-2b$
11	$a+10b$	$a-b$
13	$a+4b$	$a-9b$
17	$a+12b$	$a-5b$
19	$a+2b$	$a-17b$
23	$a+7b$	$a-16b$
29	$a+3b$	$a-26b$
31	$a+28b$	$a-3b$
37	$a+26b$	$a-11b$
41	$a+37b$	$a-4b$
43	$a+13b$	$a-30b$
47	$a+33b$	$a-14b$
53	$a+16b$	$a-37b$
59	$a+6b$	$a-53b$
61	$a+55b$	$a-6b$
67	$a+47b$	$a-20b$
71	$a+64b$	$a-7b$
73	$a+22b$	$a-51b$
79	$a+8b$	$a-71b$
83	$a+25b$	$a-58b$
89	$a+9b$	$a-80b$
97	$a+68b$	$a-29b$

Fonte: GUEDES, 1988, p. 24.

Na seção posterior será construído um algoritmo para gerar esses critérios utilizando a linguagem de programação Pascal. Essa tabela servirá como uma fonte de consulta para verificar se os critérios gerados estão realmente corretos.

Os valores de a e b são os mesmos utilizados no Teorema da quebra da unidade onde $a = a_n a_{n-1} \ldots = a_0$ e $b = a_0$.

4 A LINGUAGEM PASCAL

O presente capítulo dá subsídios para uma iniciação à linguagem Pascal. Primeiro apresentamos uma introdução à lógica de programação, depois apresentamos rudimentos da linguagem Pascal e por fim apresentamos alguns algoritmos desenvolvidos utilizando a linguagem.

4.1 Introdução à lógica de programação

Primeiro devemos saber que a máquina (computador) não é um ser inteligente. O mesmo precisa de instruções para executar o que queremos. A diferença entre o ser humano e a máquina é que o computador executa algoritmos numa velocidade muito superior ao ser humano.

Mas o que seria algoritmo? De acordo com MATHIAS algoritmo é a especificação de uma sequência lógica ordenada de passos que deve ser seguida para a realização de uma tarefa garantindo a sua repetitividade. Portanto, algoritmo é um conjunto de passos para se resolver um determinado problema.

É importante notar que o termo algoritmo não é exclusivo da computação, sabemos que na matemática existe o algoritmo de Euclides por exemplo. Até mesmo no dia a dia usamos sem envolver os aspectos computacionais, tais como a receita de um bolo, a partitura de uma música, o manual de como montar um guarda-roupa, entre outros.

Veremos, agora, como os algoritmos podem ser representados, para depois serem codificados em uma linguagem de programação e por fim serem transformados em programas.

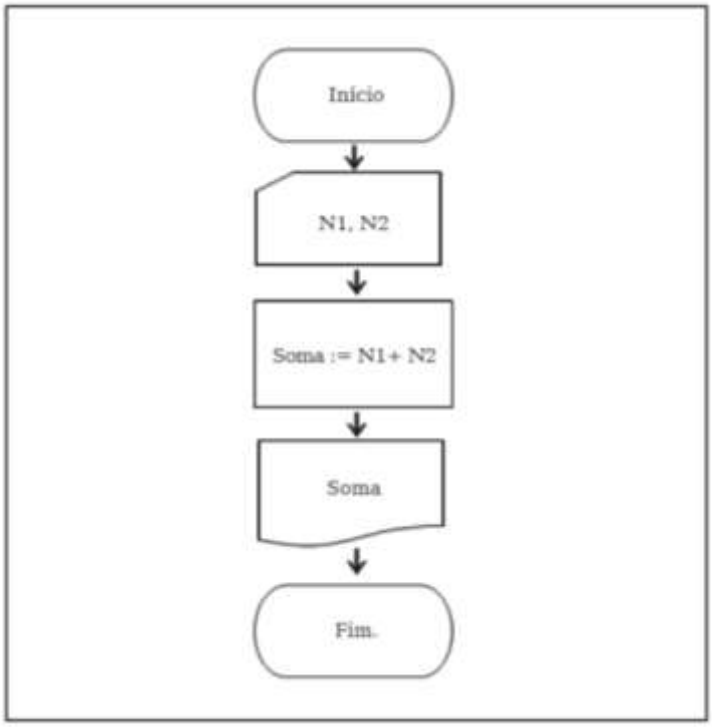
Uma maneira de representar os algoritmos é através de fluxogramas. Em Brasil (2018, p. 301), na Base Nacional Comum Curricular (BNCC) do Ensino Médio, na competência específica 3 traz a seguinte habilidade.

> (EM13MAT315): Reconhecer um problema algorítmico, enunciá-lo, procurar uma solução e expressá-la por meio de um algoritmo, com o respectivo fluxograma. (BRASIL, 2018, p. 529)

O que seriam fluxogramas então? De acordo com MATHIAS trata-se de uma representação gráfica de algoritmos, em que formas geométricas implicam ações (instruções, comandos) distintas. Em um fluxograma o mais importante é distinguir as etapas de construção

do algoritmo, onde fica a entrada de dados e onde fica a saída de dados. A figura abaixo ilustra um exemplo de fluxograma.

Figura 2: Exemplo de Fluxograma.

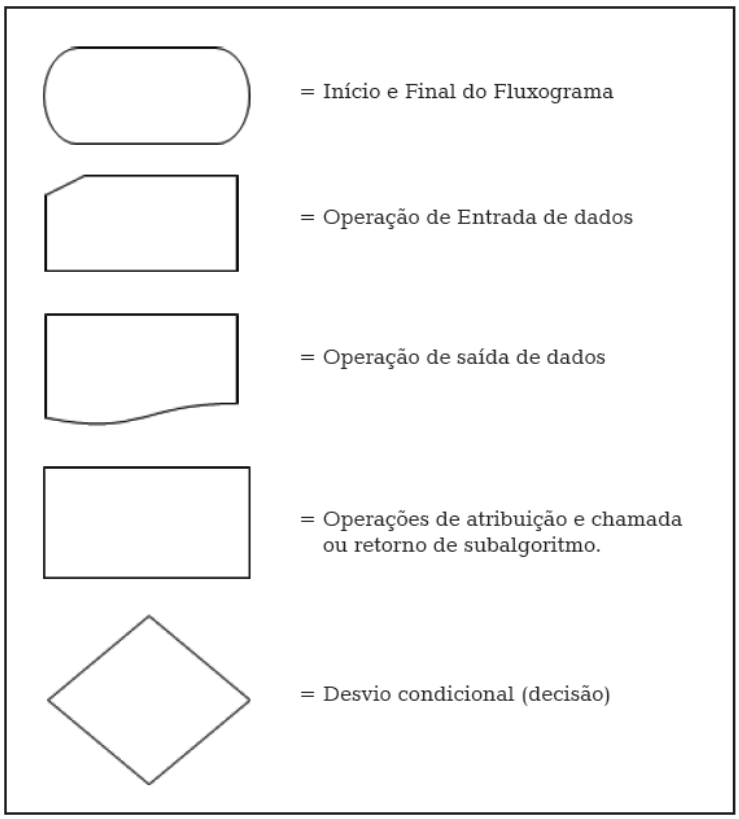


Fonte: MATHIAS, 2017, p. 33.

Observando a figura acima notamos que um algoritmo possui as seguintes etapas para a sua concepção: 1) Entradas: são as informações inseridas pelo usuário. 2) Processamento: são as manipulações e ou cálculos dos dados inseridos. 3) Saída: são os resultados obtidos do processamento dos dados. 4) Teste de mesa: Trata-se da execução das três fases anteriores, verificando o funcionamento das instruções executadas.

O uso de fluxograma é meramente didático pois as linguagens de programação atuais não os utilizam mais. A figura a seguir mostra o que cada figura representa na montagem de um fluxograma.

Figura 3: Principais formas de um fluxograma.



Fonte: MATHIAS, 2017, p. 33.

Em Brasil (2018, p. 301), na Base Nacional Comum Curricular (BNCC) do Ensino Médio, na competência específica 4 traz a seguinte habilidade.

> (EM13MAT406): Utilizar os conceitos de uma linguagem de programação na implementação de algoritmos escritos em linguagem corrente e/ou matemática. Portanto, é importante conhecer tais temas para serem implementados em sala de aula no ensino médio.

Antes de conhecer uma linguagem de programação costuma-se utilizar um pseudocódigo para representar os algoritmos, possuindo todos os requisitos que as linguagens de programação precisam, tais como, as declarações de variáveis com os respectivos tipos que são: inteiro, real, caractere, boolean, etc. Esses comandos e essas instruções são similares aos usados em linguagem de programação. (MATHIAS, 2017).

Como o pseudocódigo segue uma estrutura, ou seja, um padrão também é chamado de linguagem estruturada e possui um formato parecido com os das linguagens de programação, tornando fácil a codificação para qualquer linguagem que se queira usar. O modelo de algoritmo

que iremos utilizar será o Portugol, como o nome já sugere, a sua origem é a língua portuguesa. (MATHIAS, 2017).

A figura a seguir mostra uma forma de representação de um algoritmo em pseudocódigo.

Figura 4: Forma geral de representação de um algoritmo em pseudocódigo.

```
Algoritmo < nome_do_algoritmo >;
    Var
       < declaração_de_variáveis >;
    Início
       < corpo_do_algoritmo >;
    Fim.
```

Fonte: MATHIAS, 2017, p. 34.

A sequência é a seguinte: 1) escrevemos o nome algoritmo e damos o nome do algoritmo, 2) declaramos as variáveis que serão utilizadas, 3) damos início ao programa inserindo os comandos a serem executados, 4) encerramos o programa.

Iremos, agora, mostrar como é o algoritmo do programa soma de dois números exibido anteriormente no fluxograma. Primeiro, colocamos o nome Algoritmo e o nomeamos, depois declaramos as variáveis N1, N2, Soma de valores reais, o algoritmo é iniciado com o comando início, o comando Leia as notas N1 e N2 (entradas de dados) é inserido, os valores N1 e N2 são somados e guardados na variável Soma (processamento de dados), o valor da soma é escrito (saída de dados), por fim o algoritmo é encerrado com o comando fim. A figura a seguir ilustra toda essa sequência em Portugol.

Figura 5: Algoritmo Soma_dois_Numeros

```
Algoritmo Soma_dois_Numeros;

    Var
        N1, N2, Soma : real;

    Inicio
        Leia N1, N2;
        Soma := N1 + N2;
        Escreva Soma;
    Fim.
```

Fonte: MATHIAS, 2017, p. 36.

4.2 Um breve histórico sobre a linguagem Pascal

A linguagem de programação Pascal foi desenvolvida por Niklaus Wirth, professor do Departamento de Informática da Escola Politécnica da Universidade de Zurique na cidade de Genebra, Suíça. Foi desenvolvida por volta de 1968 à 1970. (MANZANO, 2001).

Em homenagem ao filósofo e matemático Blaise Pascal (1623 – 1662), inventor da primeira calculadora mecânica, a linguagem recebeu esse nome. Niklaus Wirth tinha o desejo de dispor, para o ensino de programação, uma nova linguagem que ao mesmo tempo fosse simples, coerente e capaz de incentivar a criação de programas claros e facilmente legíveis, favorecendo assim a utilização de boas técnicas de programação (MATHIAS, 2017).

Figura 6: Professor Niklaus Wirth.

Fonte: http://people.inf.ethz.ch/wirth/

No Brasil, foi desenvolvido o compilador Pascalzim na Universidade de Brasília pelo Departamento de Ciências da Computação. Devido a sua facilidade de utilização a linguagem Pascal se tornou amplamente conhecida pelo mundo.

Atualmente encontra-se na internet mais de 300 compiladores ou interpretadores da linguagem (alguns pagos, outros gratuitos e muitos descontinuados, ou seja, não possuem mais suporte). As contribuições mais importantes para o desenvolvimento do Pascal foram feitas pela Borland (empresa americana de desenvolvimento de software) com a criação do Turbo Pascal e depois com a criação do Delphi Pascal. (PEREIRA, 2015)

Além desses compiladores temos também o ambiente de desenvolvimento integrado Lazarus que funciona nos sistemas operacionais Linux, FreeBSD, Win 32 e Win64 e o ambiente de desenvolvimento integrado Dev Pascal que funciona nos sistemas operacionais windows.

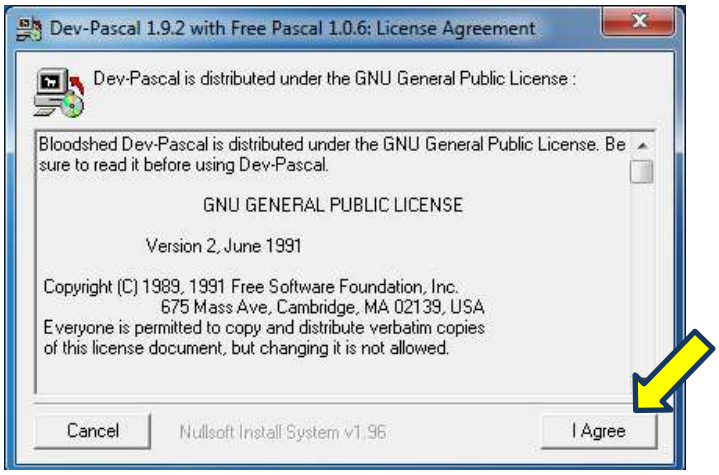
A linguagem Pascal é originalmente estruturada, ou seja, os programas são compostos de subprogramas menores que se conectam por chamadas (uma chamada de um determinado subprograma é a solicitação de execução de outros subprogramas a partir dele). A linguagem absorveu com o passar do tempo o modelo da orientação a objetos (que se baseia nos conceitos de classes e objetos) dando origem ao Object Pascal. (PEREIRA, 2015)

4.3 Ambiente de programação Dev Pascal.

Dev Pascal é um ambiente de desenvolvimento integrado (IDE) capaz de criar programas Windows ou baseados em console Pascal. Ele usa para tanto, os compiladores GNU Pascal ou Free Pascal. O Dev Pascal é encontrado no seguinte endereço eletrônico https://www.bloodshed.net/Dev-Pascal. Para fazer o download do arquivo executável clica-se no ícone em azul com o seguinte nome: Download Dev-Pascal 1.9.2 + Free Pascal Compiler.

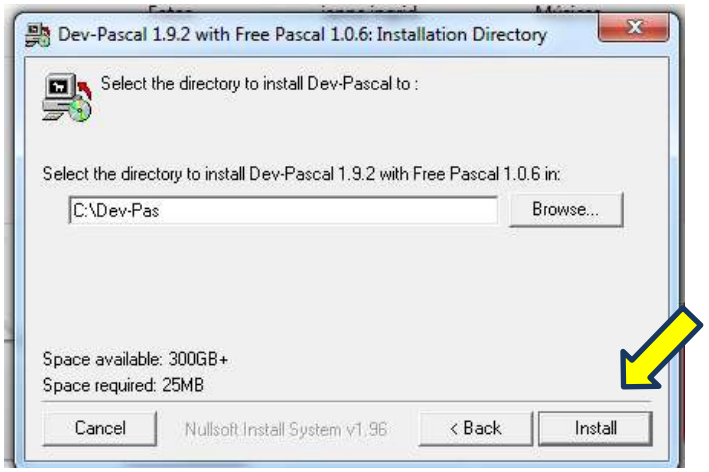
Depois de fazer download do arquivo clica-se duas vezes no arquivo executável de nome devpas192. Aparecerá uma janela e clica-se no botão agree (concorda). Aparecerá outra janela e clica-se em install (instalar). Aparecerá uma última janela e clica-se close (fechar). O Dev-Pascal está instalado no computador. As figuras a seguir ilustram esse procedimento descrito.

Figura 7: Instalando o Dev-Pascal - 1ª Janela.



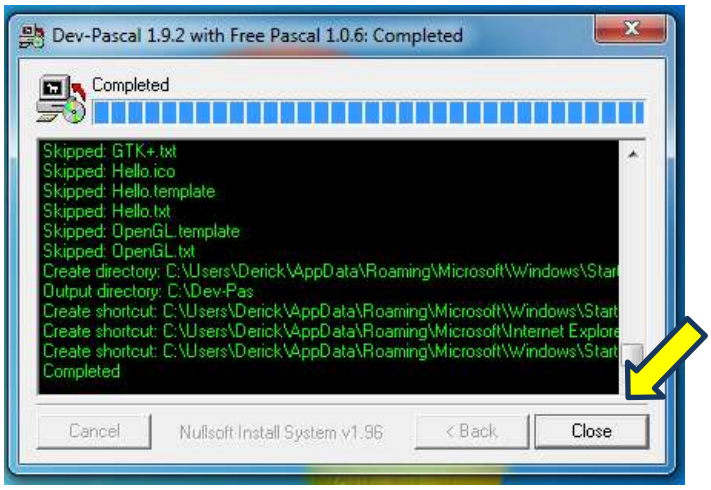
Fonte: Elaborado pelo autor.

Figura 8: Instalando o Dev-Pascal - 2ª Janela



Fonte: Elaborado pelo autor.

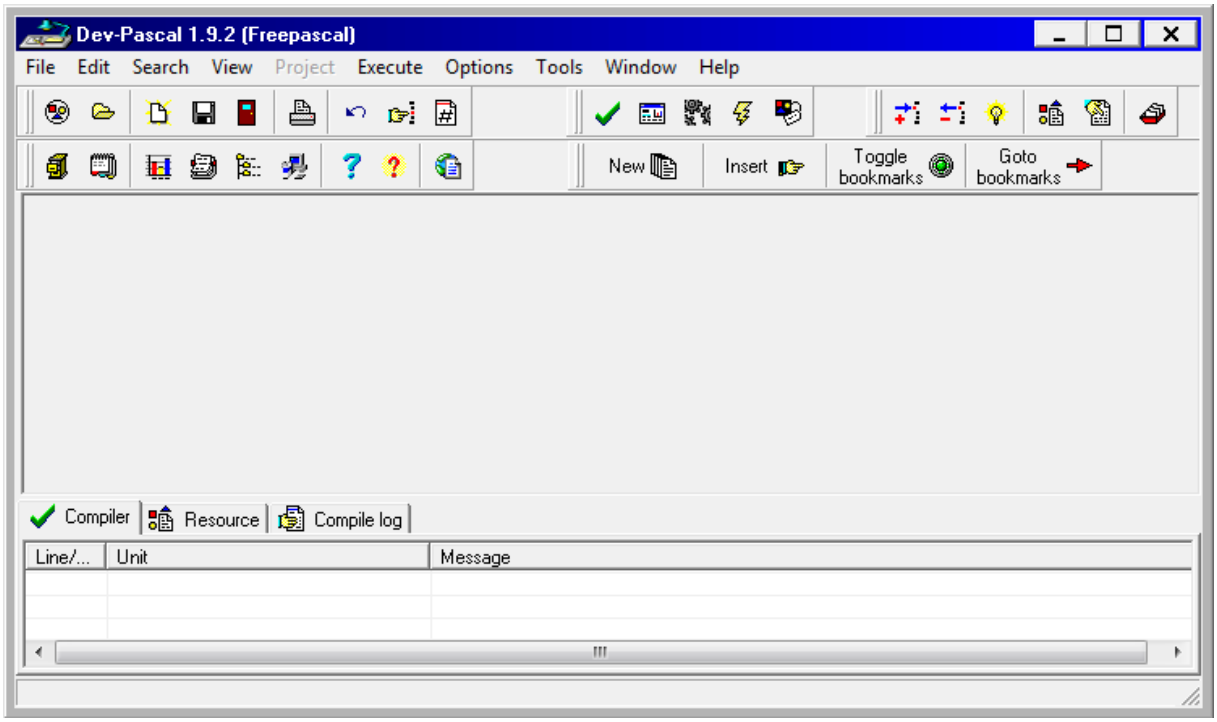
Figura 9: Instalando o Dev-Pascal - 3ª Janela.



Fonte: Elaborado pelo autor.

Assim que entrarmos no ambiente Dev pascal, a tela da Figura 9, será a primeira que teremos acesso.

Figura 10: Tela inicial

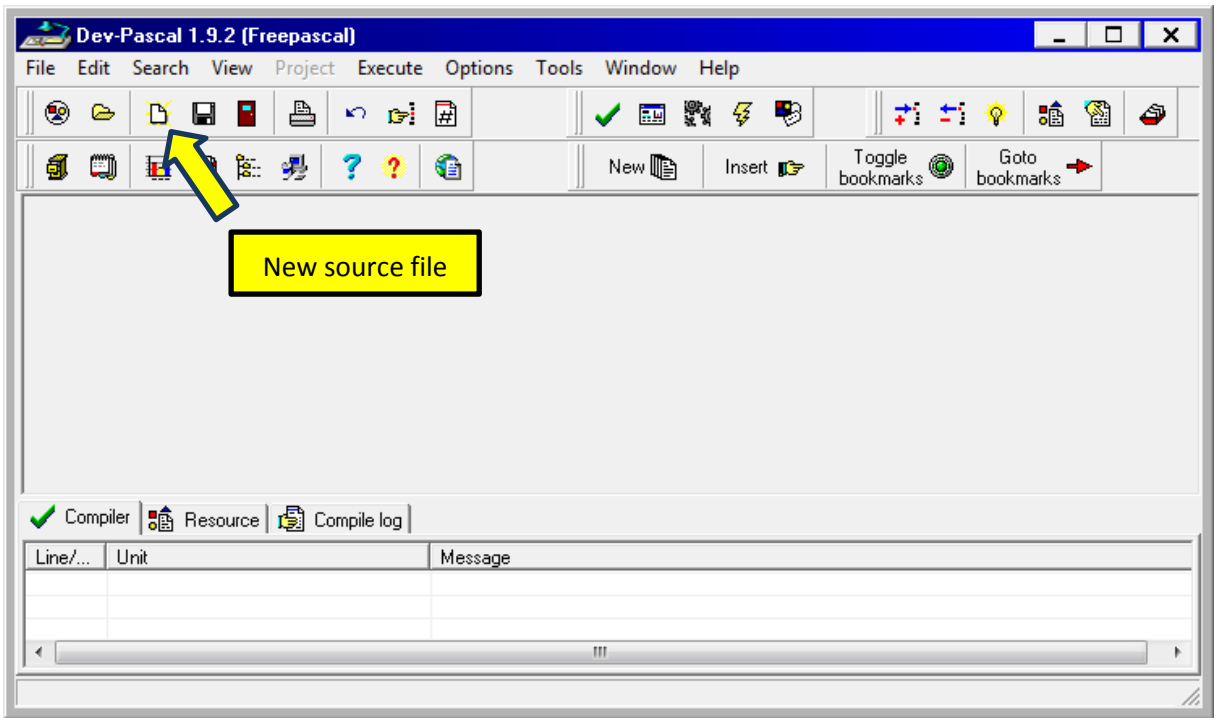


Fonte: Elaborado pelo autor.

Note que o IDE Dev Pascal possui na aba File (Arquivo), as opções necessárias para criar um novo programa, abrir , salvar e fechar programas . Abaixo das abas temos vários botões que podem ser utilizados no lugar das opções das abas, muito importante para dar celeridade às criações e às execuções dos programas.

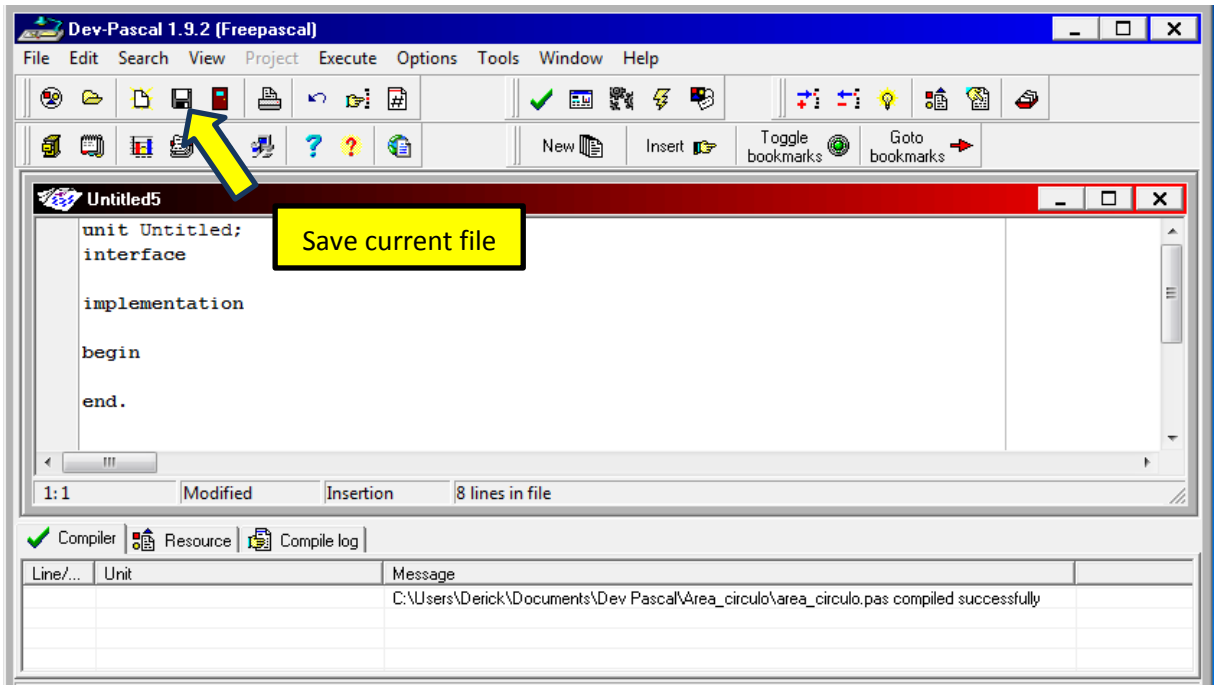
Para criar um program no Dev Pascal clica-se no botão New source file. Criamos um diretório (pasta) com o nome do programa e salvamos o arquivo no formato (.pas). Observe a sequência de figuras que mostra o passo a passo.

Figura 11: Criando novo arquivo Dev Pascal



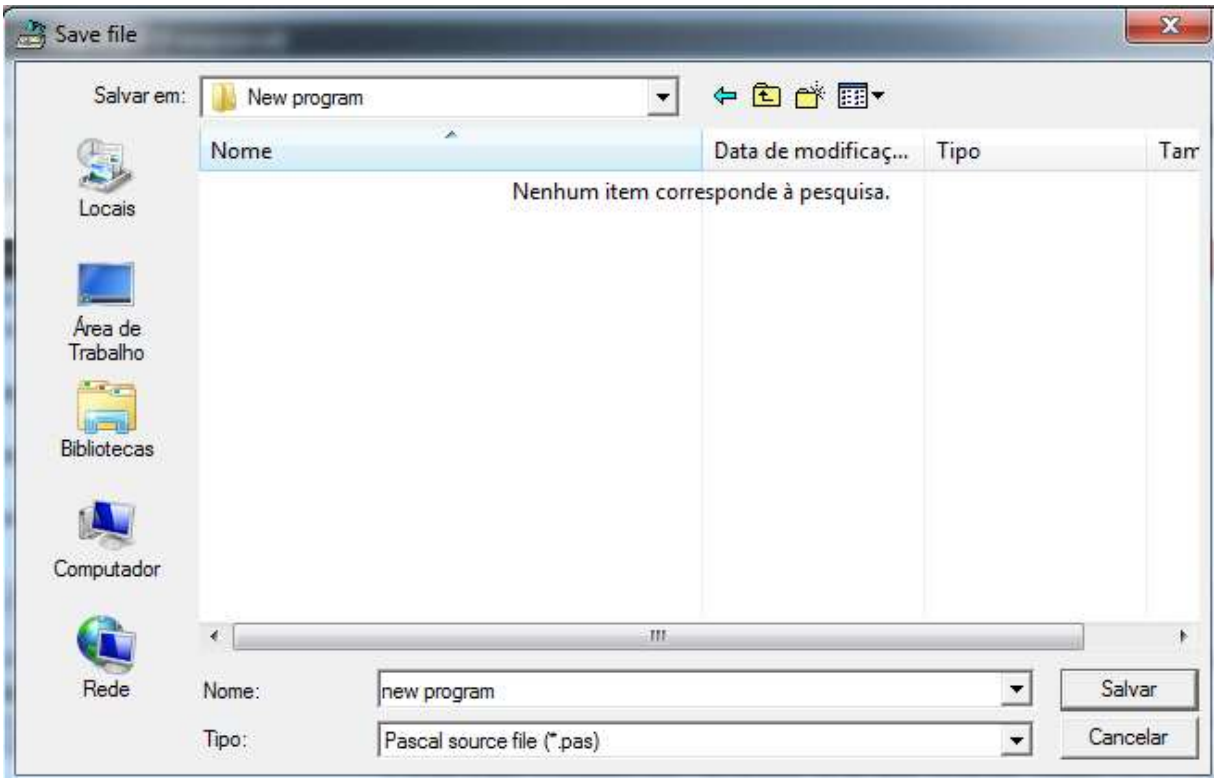
Fonte: Elaborado pelo autor.

Figura 12: Salvando o arquivo Dev Pascal



Fonte: Elaborado pelo autor.

Figura 13: Nomeando o arquivo Dev Pascal



Fonte: Elaborado pelo autor.

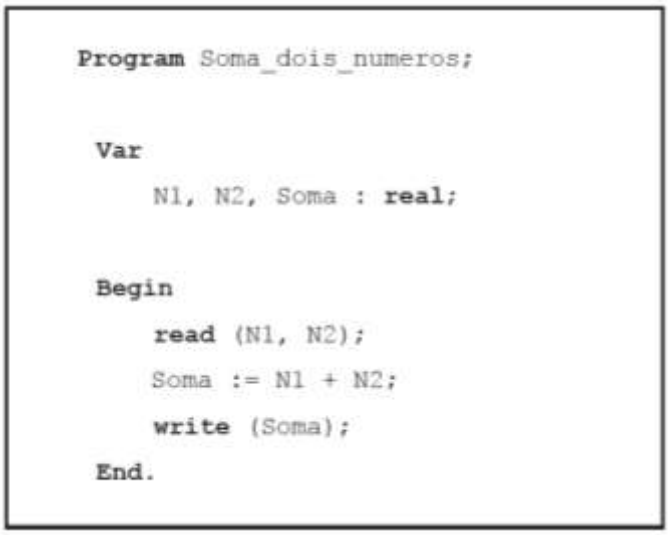
Nessa sequência de imagens criamos a pasta New program e salvamos o arquivo também com o nome new program no formato (.pas).

4.4 Estrutura de programação em Pascal

A linguagem de programação Pascal possui uma estrutura sequencial, ou seja, os comandos de um algoritmo são executados numa sequência preestabelecida. Cada comando é executado apenas após o término do comando anterior, ou seja, de forma sequencial, de cima para baixo e na ordem em que foram definidos. (MATHIAS, 2017).

Nessa linguagem primeiro começamos com o comando **Program** e o nome do programa. Depois são declaradas as variáveis com o comando **var**. Nessa parte temos as seguintes opções de variáveis: **integer** (inteiro), **real** (real), **char** (caractere), **string** (concatenação de caracteres) e **boolean** (recebe valor verdadeiro ou falso). Após a declaração das variáveis iniciamos o programa com o comando **begin** (inicio), escrevemos o código do programa e por fim encerramos com o comando **end** (fim). Na figura a seguir temos o algoritmo da Figura 4 decodificado em linguagem Pascal.

Figura 14: Algoritmo Soma_dois_mumeros em Pascal.



```
Program Soma_dois_numeros;

 Var
     N1, N2, Soma : real;

 Begin
     read (N1, N2);
     Soma := N1 + N2;
     write (Soma);
 End.
```

Fonte: MATHIAS, 2017, p. 105.

No algoritmo acima notamos que o mesmo tem uma estrutura sequencial, pois cada comando deve ser executado na ordem que está escrito, para que o algoritmo funcione, ou seja, some dois números e mostre o resultado da soma. Os valores N1, N2 e Soma são variáveis reais, o comando **read** significa leia, o símbolo **:=** (recebe) é chamado comando de atribuição e o comando **write** significa escreva.

Para uma melhor interface para o usuário pode-se fazer algumas alterações no algoritmo para torná-lo mais compreensível. Veja a seguir o mesmo programa com algumas alterações.

Figura 15: 2º Algoritmo Soma_dois_numeros em Pascal

```
Program Soma_dois_numeros;

  Var
    N1, N2, Soma : real;

  Begin
    writeln ('Programa que soma dois números');
    write ('Entre com o primeiro número: ');
    readln (N1);
    write ('Entre com o segundo número: ');
    readln (N2);
    Soma := N1 + N2;
    write ('A soma entre ', N1:5:2, ' mais ', N2:5:2, 'é igual a ', Soma:5:2);
  End.
```

Fonte: MATHIAS, 2017, p. 107.

Observamos mais dois comandos: o **writeln** e o **readln**. Estes comandos desempenham as mesmas funções dos comandos **write** e **read**, respectivamente. A única diferença é que, no primeiro caso, após a execução deles o cursor vai para a linha seguinte. (MATHIAS, 2017)

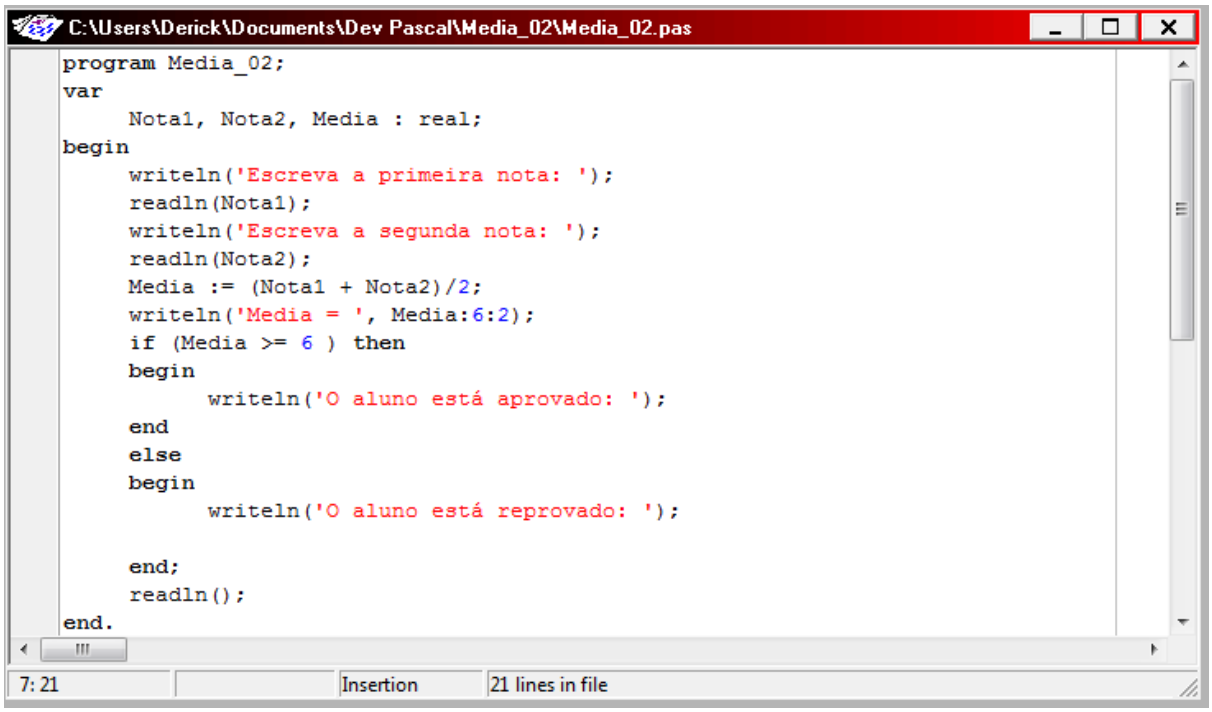
Os números 5 e 2 ao lado de N1, N2 e Soma tema finalidade de formatar a exibição do valor contido na variável, o 5 representa o número de dígitos antes do separador decimal e o 2 representa o número de dígitos após o separador decimal. (MATHIAS, 2017)

Nota-se que existem alguns recuos no código. Esses recuos definem a estrutura que o programa possui. Observe que os comandos **begin** e **end** têm o mesmo recuo e o restante do código tem outro recuo. O objetivo dessa indentação é organizar o código, de maneira que o programador possa identificar e entender a construção das diferentes estruturas de um programa. (MATHIAS, 2017)

Existe uma estrutura de decisão muito útil na construção de algoritmos mais elaborados. Esta estrutura se chama **if then** (se então), que avalia se a condição expressa no algoritmo é verdadeira. Se for verdadeira então um determinado comando é executado, caso contrário outro comando é executado. O algoritmo a seguir calcula a média aritmética de duas notas de um aluno. Se a média for maior ou igual à 6 então o comando que mostra a frase ‘O

aluno está aprovado' é executado, caso contrário outro comando que mostra a frase 'O aluno está reprovado' é executado.

Figura 16: Algoritmo Média_02 em Pascal

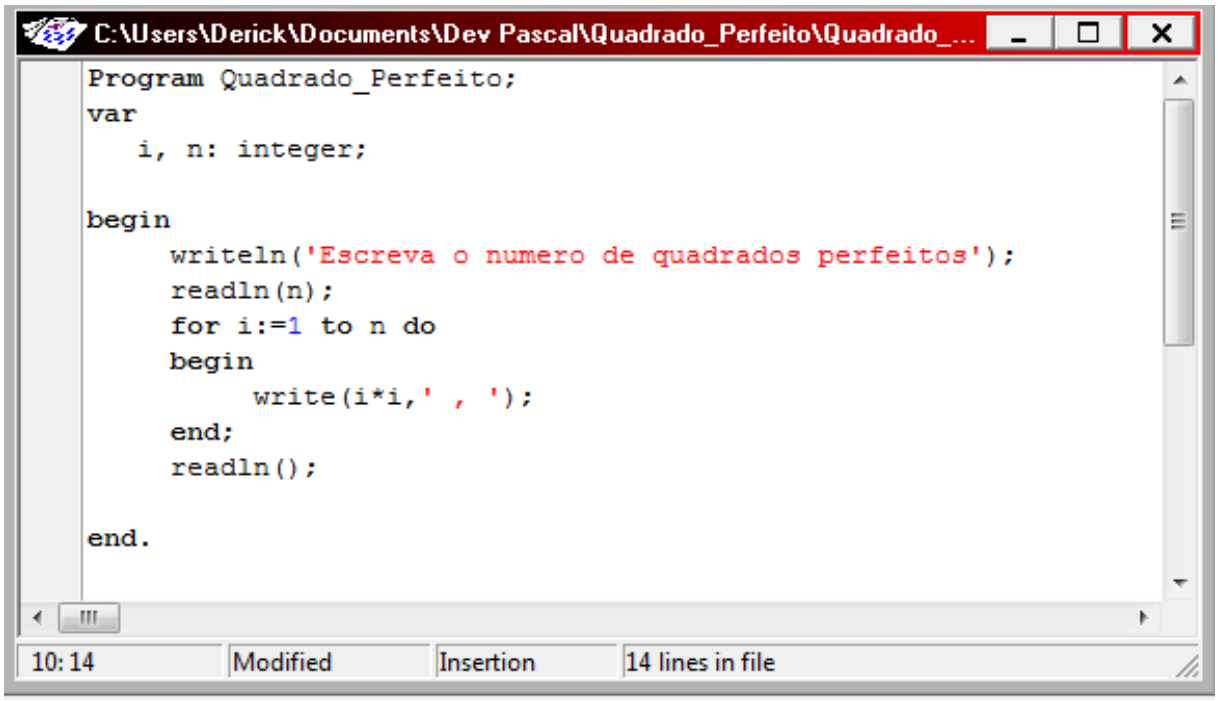


Fonte: Elaborado pelo autor.

Existe uma outra estrutura muito útil na construção de algoritmos mais elaborados. É uma estrutura de repetição e chama-se **for** (para) que tem a seguinte sintaxe **for i:= a to b do**, onde **a** é o limite inferior e **b** é o limite superior. A palavra **to** neste caso significa até e **do** significa faça. Explicitando melhor ficaria assim: para i recebe os valores de a até b faça. Portanto, serão repetidos comandos de a até b, por isso se chama de estrutura de repetição.

A figura a seguir mostra um algoritmo que utiliza a estrutura de repetição **for** para escrever uma sequência dos n primeiros números quadrados perfeitos.

Figura 17: Algoritmo Quadrado_Perfeito em Pascal



Fonte: Elaborado pelo autor.

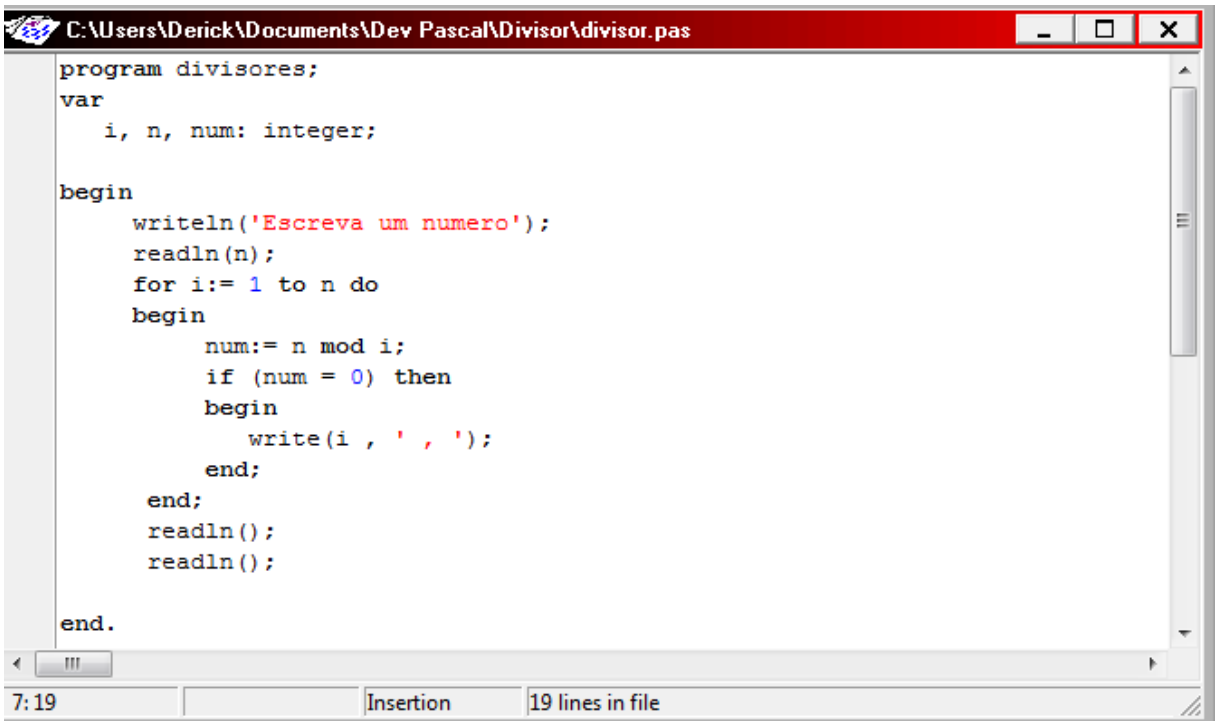
4.5 Algoritmo para determinar os divisores de um número

O algoritmo a seguir mostra como obtêm-se os divisores de um número inteiros positivo. Primeiro, nomeamos o programa com o nome divisores. Declaramos as variáveis que serão utilizadas: **i**, **n** e **num** de valores inteiros. Iniciamos o algoritmo e solicitamos que o usuário insira um número inteiro. Esse número é guardado na varável n.

Utilizando a estrutura de repetição **for** realizamos um procedimento que vai do número 1 até o número n inserido. O procedimento consiste em verificar se o resto da divisão do número **n** por **i** é 0. Fazendo uso do comando **n mod i** (que determina o resto da divisão de **n** por **i**), o resto da divisão de n por i é guardado na variável num.

Agora, fazendo uso da estrutura condicional **if** (se) o número i é escrito na tela do usuário caso **num** seja 0, ou seja, se **i** for divisor de **n**. Cada divisor **i** de **n** seja escrito na tela do usuário até **i** for igual à **n**. Segue abaixo o algoritmo para determinar os divisores de um número inteiro em Pascal.

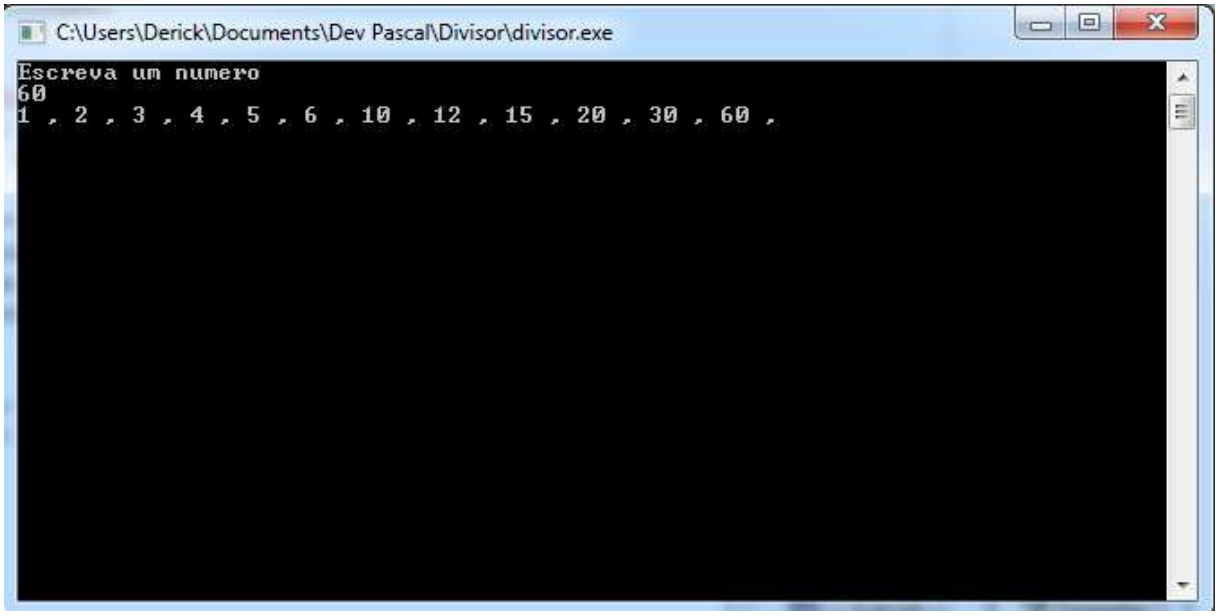
Figura 18: Algoritmo divisores de um número em Pascal



Fonte: Elaborado pelo autor.

Executamos o programa, inserimos o número 60 e verificamos os seus divisores. A figura a seguir ilustra isso.

Figura 19: Obtendo os divisores de 60 através do programa divisores



Fonte: Elaborado pelo autor.

4.6 Algoritmo para determinar se um número é primo

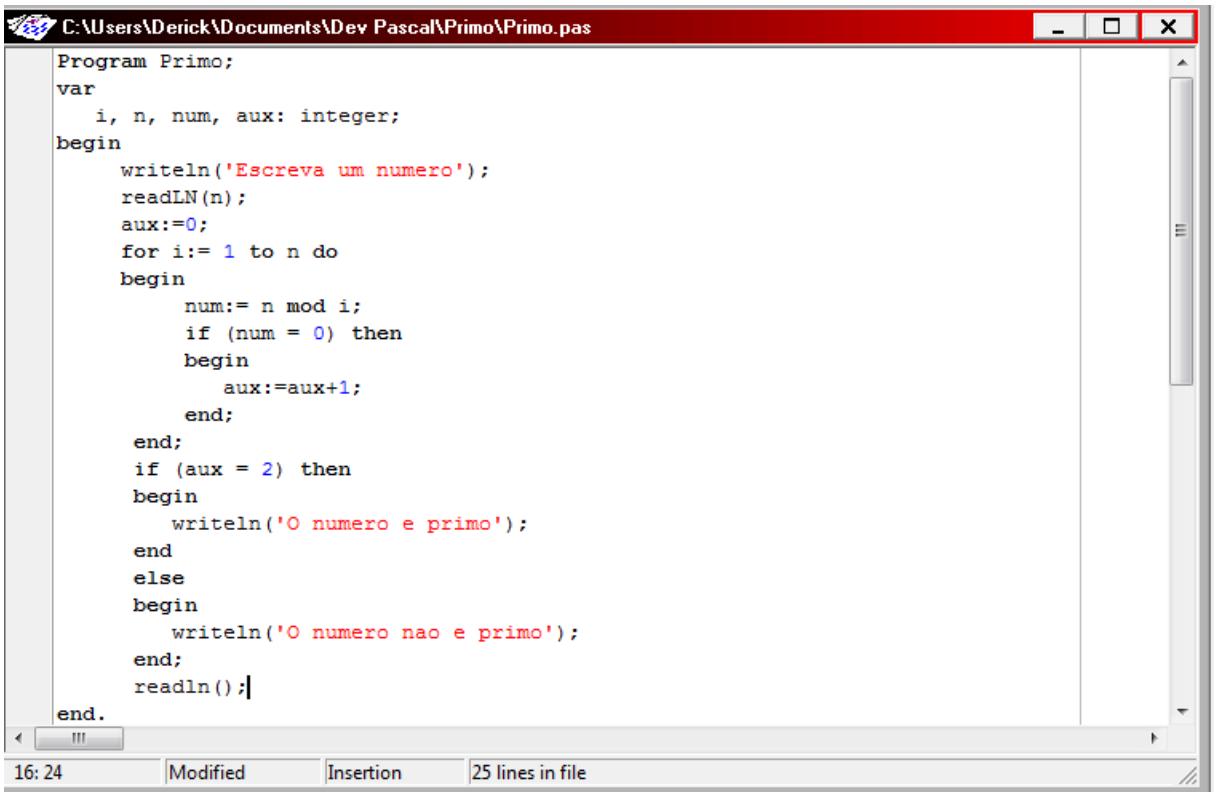
O algoritmo a seguir mostra como verificar se um número é primo ou não. Primeiro, nomeamos o programa com o nome Primo. Declaramos as variáveis que serão utilizadas: **i**, **n**, **num** e **aux** de valores inteiros. Iniciamos o algoritmo e solicitamos que o usuário insira um número inteiro. Esse número é guardado na varável n.

Utilizando a variável contadora **aux,** iremos contar quantos divisores tem um número **n**. Para isso, começamos atribuindo a variável **n** o valor 0. Fazendo uso da estrutura de repetição **for** realizamos um procedimento que vai do número 1 até o número n inserido. O procedimento consiste em verificar se o resto da divisão do número **n** por **i** é 0. Fazendo uso do comando **n mod i** (que determina o resto da divisão de **n** por **i**), o resto da divisão de n por i é guardado na variável num.

Fazendo uso da estrutura condicional **if** contamos quantos divisores tem o número **n**. Se **num** for 0 então a variável contadora **aux** tem uma unidade acrescida de seu valor. Após repetir n vezes a verificação do comando **n mod i**, o valor da variável **aux** é guardado.

Utilizando, novamente, a estrutura condicional **if** (se), fora da estrutura de repetição **for** (para) verificamos se o número n é primo ou não. Se **aux** for igual a 2 então o número será primo e será mostrado na tela do usuário: O número é primo. Senão, será mostrado na tela do usuário: O número não é primo. A figura a seguir mostra o algoritmo para determinar se um número é primo ou não.

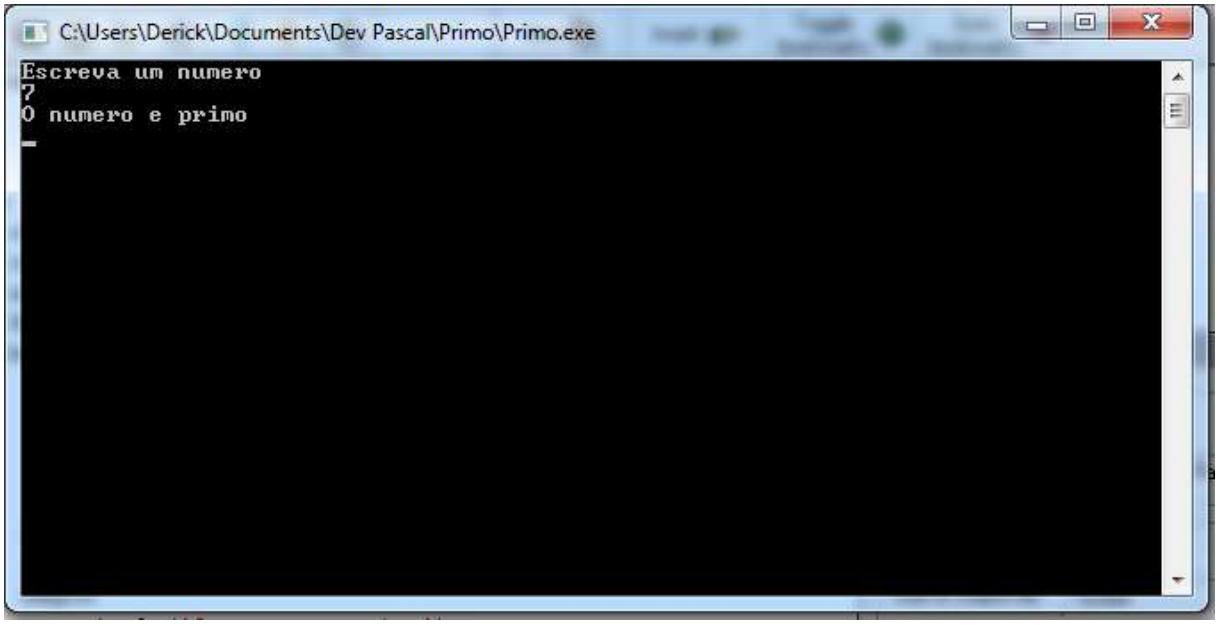
Figura 20: Algoritmo para determinar se um número é primo em Pascal



Fonte: Elaborado pelo autor.

Executamos o programa, inserimos o número 7 e verificamos que o mesmo é primo.

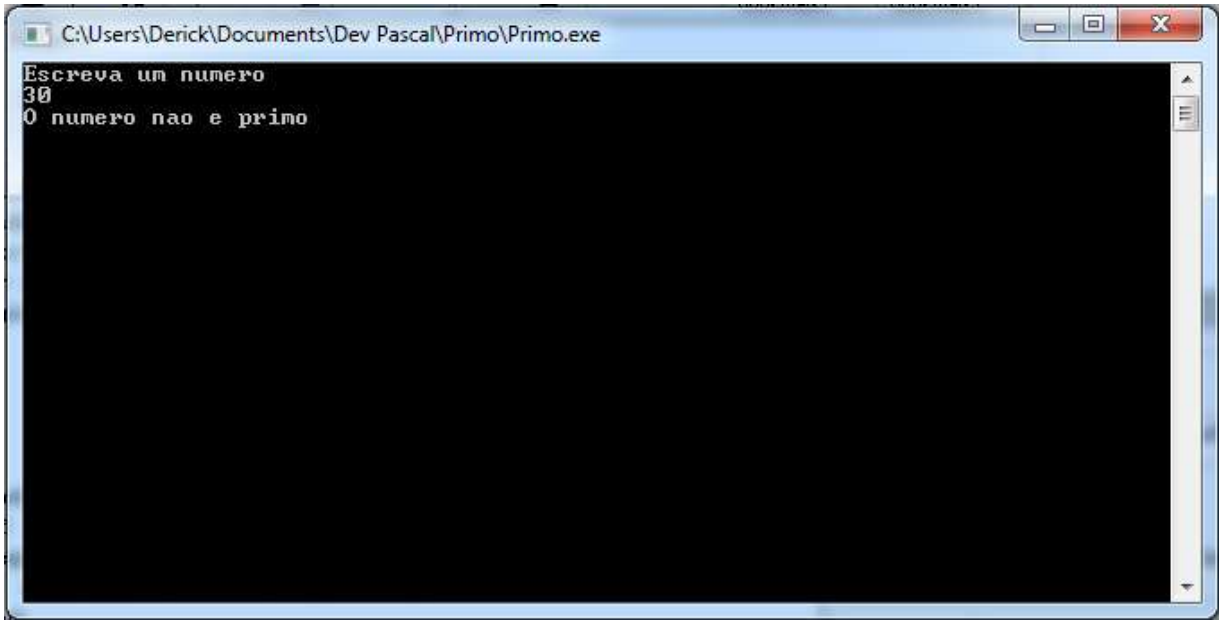
Figura 21: Verificando se o número 7 é primo utilizando o programa Primo



Fonte: Elaborado pelo autor.

Executamos o programa, novamente, inserimos o número 30 e verificamos que o mesmo não é primo. A figura a seguir ilustra isso.

Figura 22: Verificando se o número 30 é primo utilizando o programa Primo



Fonte: Elaborado pelo autor.

4.7 Algoritmo para gerar critérios de divisibilidade

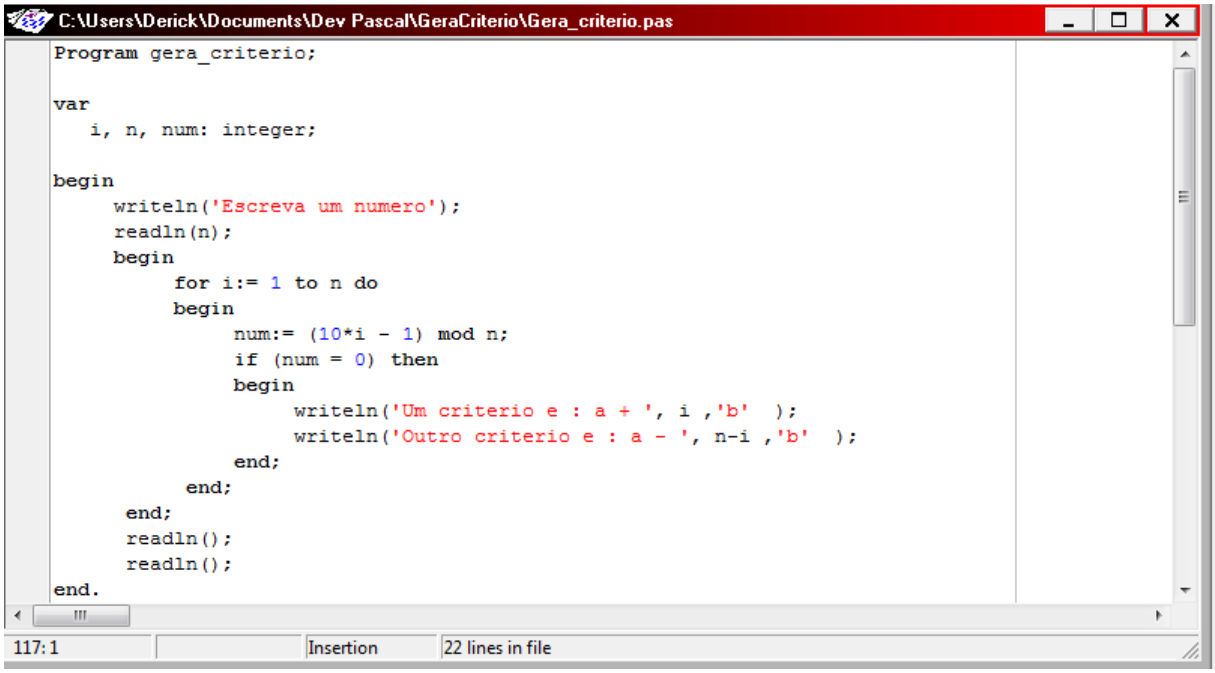
O algoritmo a seguir mostra como gerar critérios de divisibilidade. Primeiro, nomeamos o programa com o nome gera_criterio. Declaramos as variáveis que serão utilizadas: **i**, **n**, **num** de valores inteiros. Iniciamos o algoritmo e solicitamos que o usuário insira um número inteiro. Esse número é guardado na varável n.

Utilizando a estrutura de repetição **for** realizamos um procedimento que vai do número 1 até o número n inserido. O procedimento consiste em verificar se o resto da divisão do número **10i -1** por **n** é 0. Fazendo uso do comando **10i -1 mod n** (que determina o resto da divisão de **10i -1** por **n**), o resto da divisão de **10i -1** por **n** é guardado na variável **num**.

Fazendo uso da estrutura condicional **if** escreve-se o critério de divisibilidade por **n**. Se **num** for 0 então **i** é solução da congruência $\mathbf{10}\boldsymbol{i} \equiv \mathbf{1}\ (\boldsymbol{mod}\ \boldsymbol{n})$, logo pelo Teorema da Quebra na Unidade $\boldsymbol{n}$ divide $\boldsymbol{a} + \boldsymbol{ib}$, se e somente, se n divide $\boldsymbol{m} = \mathbf{10}\boldsymbol{a} + \boldsymbol{b}$, onde $\boldsymbol{m}$ é um número inteiro qualquer.

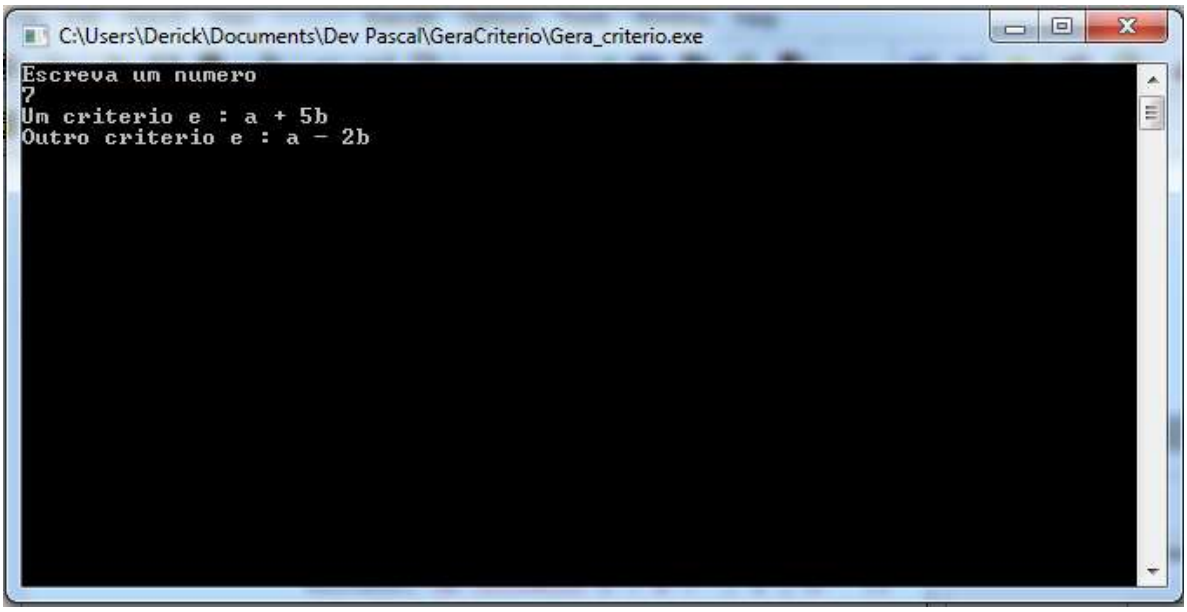
Como $\boldsymbol{n-i}$ também é solução da congruência $\boldsymbol{10i \equiv 1\ (mod\ n)}$, Teorema da Quebra na Unidade $\boldsymbol{n}$ divide $\boldsymbol{a-(n-i)b}$, se e somente, se $\boldsymbol{n}$ divide $\boldsymbol{m=10a+b}$, onde $\boldsymbol{m}$ é um número inteiro qualquer. Portanto, serão escritos esses dois critérios de divisibilidade na tela do usuário. Veja o algoritmo abaixo e os critérios de divisibilidade por 7 gerados.

Figura 23: Algoritmo para gerar critérios de divisibilidade em Pascal



Fonte: Elaborado pelo autor.

Figura 24: Gerando os critérios de divisibilidade de Chika Ofili e Zbikowski



Fonte: Elaborado pelo autor.

O primeiro critério de divisibilidade apresentado na Figura 24 é conhecido como critério de Chika Ofili e o segundo é o critério de Zbikowsky, mais comum nos livros de aritmética. Os dois critérios serão abordados na seção seguinte onde faremos uma comparação com outros critérios de divisibilidade por 7.

5 ALGUNS CRITÉRIOS DE DIVISIBILIDADE POR 7

Abordaremos, agora, alguns critérios de divisibilidade por 7. Primeiro será apresentado o critério de divisibilidade de Pascal. Depois, serão apresentados os critérios de divisibilidade de Zbikowski e Chika Ofili. Serão, ainda, apresentados outros critérios de divisibilidade por 7. Por fim, faremos uma verificação sobre qual é o critério que necessita de menos operações para um número de 6 dígitos.

5.1 Critério de divisibilidade por 7 de Blaise Pascal

Proposição: Dado o número natural $N = a_5a_4a_3a_2a_1a_0$, então $7|a_5a_4a_3a_2a_1a_0$ se, e somente se, $7|(5a_5 + 4a_4 + 6a_3 + 2a_2 + 3a_1 + a_0)$. (SHIMOKAWA, 2020).

Demonstração: Primeiramente, utilizando o item 3) das propriedades de congruência modular, observamos as seguintes congruências:

$$\begin{aligned} 10^0 &\equiv 1\ (mod\ 7) \\ 10^1 &\equiv 3\ (mod\ 7) \\ 10^2 &\equiv 2\ (mod\ 7) \\ 10^3 &\equiv 6\ (mod\ 7) \\ 10^4 &\equiv 4\ (mod\ 7) \\ 10^5 &\equiv 5(mod\ 7) \end{aligned}$$

Utilizando, agora, o item 2) das propriedades de congruência modular, temos que:

$$\begin{aligned} 10^0a_0 &\equiv a_0\ (mod\ 7) \\ 10^1a_1 &\equiv 3a_1\ (mod\ 7) \\ 10^2a_2 &\equiv 2a_2\ \ (mod\ 7) \\ 10^3a_3 &\equiv 6a_3\ (mod\ 7) \\ 10^4a_4 &\equiv 4a_4\ (mod\ 7) \\ 10^5a_5 &\equiv 5a_5\ (mod\ 7) \end{aligned}$$

Logo, utilizando o item 1) das propriedades de congruência modular, temos:

$$10^5a_5 + 10^4a_4 + 10^3a_3 + 10^2a_2 + 10^1a_1 + 10^0a_0 \equiv 5a_5 + 4a_4 + 6a_3 + 2a_2 + 3a_1 + a_0\ (mod\ 7)$$

Como $a_5a_4a_3a_2a_1a_0 = 10^5a_5 + 10^4a_4 + 10^3a_3 + 10^2a_2 + 10^1a_1 + 10^0a_0$, temos que $7|a_5a_4a_3a_2a_1a_0$ se, e somente se, $7|(5a_5 + 4a_4 + 6a_3 + 2a_2 + 3a_1 + a_0)$.

5.2 Critério de divisibilidade por 7 de Zbikowski

Proposição: O critério de divisibilidade de Zbikowski é o seguinte: dado o número natural N considere $N = 10a + b$ em que b é o algarismo das unidades de N. Tem-se que $7|(10a + b) = N$ se, e somente se, $7|(a - 2b)$.

Demonstração: Como $10 \cdot (-2) \equiv 1\ (mod\ 7)$, pois $7|(-20 - 1) = (-21)$. Logo, pelo Teorema da Quebra na Unidade, $7|(a - 2b) \Leftrightarrow 7|(10a + b)$..

Exemplo: Aplicando esse critério para 161, obtemos:

$$16 - 2 \cdot 1 = 14$$

Como $14 = 2 \cdot 7$ então $7|\ 14$, concluímos que $7|\ 161$.

5.3 Critério de divisibilidade por 7 de Chika Ofili

Proposição: O critério de divisibilidade por 7 de Chika Ofili é o seguinte: dado o número natural N considere $N = 10a + b$ em que b é o algarismo das unidades de N. Tem-se que $7|(10a + b) = N$) se, e somente se, $7|\ (a + 5b)$.

Demonstração: Como $10 \cdot 5 \equiv 1\ (mod\ 7)$, pois $7|(50 - 1) = 49$. Logo, pelo Teorema da Quebra na Unidade, $7|(a + 5b) \Leftrightarrow 7|(10a + b)$..

Embora Chika Ofili tenha descoberto este critério de divisibilidade por 7, já havia sido mencionado por GUEDES em seu artigo de 1988. Mesmo assim, foi um feito grande para um jovem de 12 anos, à época.

Exemplo: Aplicando esse critério para 112, obtemos:

$$11 + 5 \cdot 2 = 21$$

Como $21 = 3 \cdot 7$ então $7| 21$, daí concluímos que $7| 112$.

5.4 Critério de divisibilidade por 7 (Quebra na dezena)

Quebrar um número na dezena significa remover os algarismos da unidade e da dezena, para manipulá-los algebricamente. Assim, por exemplo, o numero 1243 torna-se $1243 = 1200 + 4 \cdot 10 + 3$ quando quebramos a sua dezena.

Teorema (Quebra na dezena)**:** Sejam $r \geq 2$, $n = a_r a_{r-1} a_{r-2} \ldots a_2 a_1 a_0$ um número natural e p um número primo (diferente de 2 e 5). Sejam x e y soluções inteiras das seguintes equações de congruências.

$$\begin{cases} 10y \equiv 1 \ (mod\ p) \\ 100x \equiv 1 \ (mod\ p) \end{cases}$$

Então p divide n se, e somente se, p divide $m = a_r a_{r-1} a_{r-2} \ldots a_2 + y a_1 + x a_0$ (RIBEIRO, 2020).

Demonstração: Temos que

$$n = a_r 10^r + a_{r-1} 10^{r-1} + a_{r-2} 10^{r-2} + \cdots + a_2 10^2 + a_1 10 + a_0 \quad (7)$$
$$m = a_r 10^{r-2} + a_{r-1} 10^{r-3} + a_{r-2} 10^{r-4} + \cdots + a_2 + y a_1 + x a_0 \quad (8)$$

Multiplicando a equação (8) por 100 temos:

$$100m = a_r 10^r + a_{r-1} 10^{r-1} + a_{r-2} 10^{r-2} + \cdots + a_2 10^2 + y a_1 100 + x a_0 100 \quad (9)$$

Subtraindo a equação (7) pela equação (9), temos:

$$n - 100m = \ a_1 10 - y a_1 100 + a_0 - x a_0 100$$

$$n = 100m + 10(1 - 10y)a_1 + (1 - 100x)a_0$$

Como $p|(1 - 10y)$ e $p|(1 - 100x)$ (Hipótese do Teorema), temos que:

$$n \equiv 100m \ (mod\ p)$$

Como p é diferente de 2 e 5, então p não divide 100. Logo, $p|100m$ se, e somente se, $p|n$. Portanto, p divide n se, e somente se, p divide $m = a_r a_{r-1} a_{r-2} \dots a_2 + ya_1 + xa_0$.

Para construir um critério de divisibilidade por 7 precisamos encontrar x e y tais que $100 \cdot x \equiv 1 \ (mod\ 7)$ e $10 \cdot y \equiv 1 \ (mod\ 7)$. Como $100 \cdot (-3) \equiv 1 \ (mod\ 7)$ e $10 \cdot 5 \equiv 1 \ (mod\ 7)$ então, pelo Teorema da quebra na dezena, 7 divide n se, e somente se, 7 divide $m = a_r a_{r-1} a_{r-2} \dots a_2 + 5a_1 - 3a_0$.

Exemplo: Utilizando este critério para 315, obtemos:

$$3 + 5 \cdot 1 - 3 \cdot 5 = 3 + 5 - 15 = 8 - 15 = -7$$

Como $7| -7$, daí concluímos que $7|\ 315$.

Fazendo $a = a_r a_{r-1} a_{r-2} \dots a_2$, $b = a_1$ e $c = a_0$, temos a seguinte tabela com 4 critérios de divisibilidade por 7 utilizando o Teorema 6 da quebra na dezena.

Tabela 3: Critérios de divisibilidade por 7 utilizando a quebra na dezena

	$\boldsymbol{x = 5}$	$\boldsymbol{y = -2}$
$\boldsymbol{y = 4}$	$a + 4b + 5c$	$a + 4b - 2b$
$\boldsymbol{y = -3}$	$a - 3b + 5c$	$a - 3b - 2c$

Fonte: Elaborado pelo autor.

5.5 Critério de divisibilidade por 7 (Quebra na Centena)

Quebrar um número na centena significa remover os algarismos da unidade, da dezena e da centena, para manipulá-los algebricamente. Assim, por exemplo, o número 1243 torna-se $1243 = 1000 + 2 \cdot 100 + 4 \cdot 10 + 3$ quando quebramos a sua centena.

Teorema (Quebra na centena)**:** Sejam $r \geq 3$, $n = a_r a_{r-1} a_{r-2} \ldots a_2 a_1 a_0$ um número natural e p um número primo (diferente de 2 e 5). Sejam x, y e z soluções inteiras das seguintes equações de congruências.

$$\begin{cases} 10z \equiv 1 \ (mod\ p) \\ 100y \equiv 1 \ (mod\ p) \\ 1000x \equiv 1 \ (mod\ p) \end{cases}$$

Então p divide n se, e somente se, p divide $m = a_r a_{r-1} a_{r-2} \ldots a_3 + za_2 + ya_1 + xa_0$ (RIBEIRO, 2020).

Demonstração: Temos que

$$n = a_r 10^r + a_{r-1} 10^{r-1} + a_{r-2} 10^{r-2} + \cdots + a_2 10^2 + a_1 10 + a_0 \quad (10)$$
$$m = a_r 10^{r-3} + a_{r-1} 10^{r-4} + a_{r-2} 10^{r-5} + \cdots + za_2 + ya_1 + xa_0 \quad (11)$$

Multiplicando a equação (11) por 1000, temos:

$$1000m = a_r 10^r + a_{r-1} 10^{r-1} + a_{r-2} 10^{r-2} + \cdots + za_2 1000 + ya_1 1000 + xa_0 1000 \ (12)$$

Subtraindo a equação (10) pela equação (12), temos:

$$n - 1000m = a_2 100 - za_2 1000 + a_1 10 - ya_1 1000 + a_0 - xa_0 1000$$
$$n = 100m + 10(1 - 10z)a_2 + 10(1 - 100y)a_1 + (1 - 1000x)a_0$$

Como $p|(1 - 10z)$, $p|(1 - 100y)$ e $p|(1 - 1000x)$ (Hipótese do Teorema), temos que:

$$n \equiv 1000m \ (mod\ p)$$

Como p é diferente de 2 e 5, então p não divide 1000. Logo, $p|1000m$ se, e somente se, $p|n$. Portanto, p divide n se, e somente se, p divide $m = a_r a_{r-1} a_{r-2} \ldots a_3 + za_2 + ya_1 + xa_0$.

Para construir um critério de divisibilidade por 7 precisamos encontrar x, y e z tais que $1000 \cdot x \equiv 1\ (mod\ 7)$, $100 \cdot y \equiv 1\ (mod\ 7)$ e $10 \cdot z \equiv 1\ (mod\ 7)$. Como $1000 \cdot (-1) \equiv 1\ (mod\ 7)$, $100 \cdot (-3) \equiv 1\ (mod\ 7)$ e $10 \cdot (-2) \equiv 1\ (mod\ 7)$ então, pelo Teorema da quebra na centena, 7 divide n, se e somente, se 7 divide $m = a_r a_{r-1} a_{r-2} \dots a_3 + 5a_2 - 3a_1 - a_0$.

Exemplo: Utilizando este critério para 2457, obtemos:

$$2 + 5 \cdot 4 - 3 \cdot 5 - 1 \cdot 7 = 2 + 20 - 15 - 7 = 22 - 22 = 0$$

Como $7|0$, daí concluímos que $7|\ 2457$.

Fazendo $a = a_r a_{r-1} a_{r-2} \dots a_3$, $b = a_2$, $c = a_1$ e $d = a_0$, temos a seguinte tabela com 8 critérios de divisibilidade por 7 utilizando o Teorema 7 da quebra na centena.

Tabela 4: Critérios de divisibilidade por 7 utilizando a quebra na centena

	$x = -1$	$x = 6$
$y = -3$ e $z = -2$	$a - 2b - 3c - d$	$a - 2b - 3c + 6d$
$y = -3$ e $z = 5$	$a + 5b - 3c - d$	$a + 5b - 3c + 6d$
$y = 4$ e $z = -2$	$a - 2b + 4c - d$	$a - 2b + 4c + 6d$
$y = 4$ e $z = 5$	$a + 5b + 4c - d$	$a + 5b + 4c + 6d$

Fonte: Elaborado pelo autor.

5.6 Critério de divisibilidade por 7 (Das classes)

Proposição: O número $N = a_r a_{r-1} a_{r-2} \dots a_2 a_1 a_0$ é divisível por 7 se, e somente se, o número $a_2 a_1 a_0 - a_5 a_4 a_3 + a_8 a_7 a_6 - \cdots$ é divisível por 7. (HEFEZ, 2015)

Demonstração: Primeiro, note que $7 \cdot 11 \cdot 13 = 1001$. Logo, $1000 \equiv -1\ (mod\ 7)$.

Assim, temos:

$$10^3 \equiv -1\ (mod\ 7)$$

$$10^6 \equiv (-1)^2\ (mod\ 7)$$

$$10^9 \equiv (-1)^3\ (mod\ 7)$$

$$10^3 \equiv (-1)^4\ (mod\ 7)$$

....

Temos então:

$$10^3 \equiv -1 \ (mod\ 7)$$
$$10^6 \equiv 1 \ (mod\ 7)$$
$$10^9 \equiv -1 \ (mod\ 7)$$
$$10^{12} \equiv 1 (mod\ 7)$$
....

Escrevendo, agora, um número N na representação decimal $N = a_r a_{r-1} a_{r-3} \dots a_2 a_1 a_0$ temos, módulo 7, que:

$$N = a_2 a_1 a_0 + a_5 a_4 a_3 \cdot 10^3 + a_8 a_7 a_6 \cdot 10^6 + \cdots$$
$$\equiv a_2 a_1 a_0 - a_5 a_4 a_3 + a_8 a_7 a_6 - \cdots$$

Dessa forma, o resto da divisão de N por 7 é igual ao resto da divisão de $a_2 a_1 a_0 - a_5 a_4 a_3 + a_8 a_7 a_6 - \cdots$por 7, ou seja, $7|N$ se, e somente se, $7|a_2 a_1 a_0 - a_5 a_4 a_3 + a_8 a_7 a_6 -$.

Exemplo: Verifique que o número 552.619.284 é divisível por 7.

Temos que: $284 - 619 + 552 = 217$. Como $217 = 7 \cdot 31$ então $7|284 - 619 + +552$. Portanto, $7|552.619.284$

5.7 Mais um critério de divisibilidade por 7

Proposição: Seja $N = 10a + b$ um número natural, em que a é o algarismo das unidades de N, $7|(10a + b) = N$ se, e somente se, $7|\ (2a + 3b)$.

Demonstração: Primeiro, mostraremos que se $7|\ 2a + 3b$ então $7|10a + b = N$.

Temos que:

$$7|2a + 3b \implies 2a + 3b = 7q, \text{ com } q \in \mathbb{N}.$$

$$\Longrightarrow 10a + b = 7q + 8a - 2b$$
$$\Longrightarrow 10a + b = 7q + 14a - 6a + 7b - 9b$$
$$\Longrightarrow 10a + b = 7(q + 2a + b) - 3(2a + 3b)$$
$$\Longrightarrow 10a + b = 7(q + 2a + b) - 3 \cdot 7q$$
$$\Longrightarrow 10a + b = 7(-2q + 2a + b)$$
$$\Longrightarrow 10a + b = 7k,$$

em que $(-2q + 2a + b) = k$. Logo, $7|(10a + b)$.

Demonstremos, agora, que se $7|\ (10a + b)$ então $7|(2a + 3b) = N$.

Temos que:

$$7|(10a + b) \Longrightarrow 10a + b = 7q \text{ com } q \in \mathbb{N}.$$
$$\Longrightarrow 10a + 2a + b + 3b - 7q = 2a + 3b$$
$$\Longrightarrow 12a + 4b - 7q = 2b + 3a$$
$$\Longrightarrow 42a - 30a + 7b - 3b - 7q = 2a + 3b$$
$$\Longrightarrow 7 \cdot 6a - 3 \cdot 10a + 7b - 3b - 7q = 2a + 3b$$
$$\Longrightarrow 7(6a + b) - 3(10a + b) - 7q = 2a + 3b$$
$$\Longrightarrow 7(6a + b) - 3 \cdot 7q - 7q = 2a + 3b$$
$$\Longrightarrow 7(6a + b - 3q - q) = 2a + 3b$$
$$\Longrightarrow 7(6a + b - 4q) = 2a + 3b$$
$$\Longrightarrow 7m = 2a + 3b,$$

em que $6a + b - 4q = m$. Logo, $7|(10a + b)$.

Portanto, $7|\ (10a + b) = N$ se, e somente se, $7|\ (2a + 3b)$.

Exemplo: Aplicando esse critério para 112, obtemos:

$$2 \cdot 11 + 3 \cdot 2 = 28$$

Como $28 = 4 \cdot 7$ então $7|\ 28$, daí concluímos que $7|\ 112$.

5.8 Comparando os critérios de divisibilidade por 7

Vamos, agora, comparar os critérios de divisibilidade por 7. Para isso, iremos verificar cada critério com um mesmo número de 6 dígitos. Depois, será analisado quantas iterações (uso do algoritmo) e quantas operações foram utilizadas em cada um para determinar qual é o melhor critério para o determinado número.

O critério que tiver menos operações será o melhor. Caso haja empate no número de operações, o melhor será o que tiver menos iterações. Para cada critério de divisibilidade iremos verificar se o número 143.549 é divisível por 7 e iremos contar quantas operações foram utilizadas e quantas iterações ocorreram.

Exemplo (Critério de Blaise Pascal) **:** Verifique o critério de divisibilidade por 7 de Pascal sobre o número 143.549.

$$\begin{aligned} 5 \cdot 1 + 4 \cdot 4 + 6 \cdot 3 + 2 \cdot 5 + 3 \cdot 4 + 9 &= 5 + 16 + 18 + 10 + 12 + 9 \\ &= 21 + 28 + 21 \\ &= 42 + 28 \\ &= 70 \end{aligned}$$

Como $70 = 7 \cdot 10$ então $7 \mid 70$, daí concluímos que $7 \mid 143.549$.

Nesse critério de divisibilidade por 7 foram necessárias 3 iterações e 6 operações para verificar se é divisível por 7.

Exemplo (Critério de Zbikowski)**:** Verifique o critério de divisibilidade por 7 convencional sobre o número 143.549.

$$14.354 - 2 \cdot 9 = 14.354 - 18 = 14.336$$
$$1.433 - 2 \cdot 6 = 1.433 - 12 = 1.421$$
$$142 - 2 \cdot 1 = 142 - 2 = 14$$

Como $14 = 2 \cdot 7$ então $7 \mid 14$, daí concluímos que $7 \mid 143.549$.

Nesse critério de divisibilidade por 7 foram necessárias 3 iterações e 6 operações para verificar se é divisível por 7.

Exemplo (Critério de Chika Ofili)**:** Verifique o critério de divisibilidade por 7 de Chika Ofili sobre o número 143.549.

$$14.354 + 5 \cdot 9 = 14.354 + 45 = 14.399$$
$$1.439 + 5 \cdot 9 = 1.439 + 45 = 1.484$$
$$148 + 5 \cdot 4 = 148 + 20 = 168$$
$$16 + 5 \cdot 8 = 16 + 40 = 56$$

Como $56 = 8 \cdot 7$ então $7 | 56$, daí concluímos que $7 | 143.549$.

Nesse critério de divisibilidade por 7 foram necessárias 4 iterações e 8 operações para verificar se é divisível por 7.

Exemplo (Critério da quebra na dezena)**:** Verifique o critério de divisibilidade por 7 da quebra na dezena sobre o número 143.549.

$$1.435 + 5 \cdot 4 - 3 \cdot 9 = 1.435 + 20 - 27 = 1.428$$
$$14 + 5 \cdot 2 - 3 \cdot 8 = 14 + 10 - 24 = 0$$

Como $0 = 0 \cdot 7$ então $7 | 0$, daí concluímos que $7 | 143.549$.

Nesse critério de divisibilidade por 7 foram necessárias 2 iterações e 8 operações para verificar se é divisível por 7.

Exemplo (Critério da quebra na centena)**:** Verifique o critério de divisibilidade por 7 da quebra na centena sobre o número 143.549.

$$143 + 5 \cdot 5 - 3 \cdot 4 - 1 \cdot 9 = 143 + 25 - 12 - 9 = 147$$

$$0 + 5 \cdot 1 - 3 \cdot 4 - 1 \cdot 7 = 0 + 5 - 12 - 7 = -14$$

Como $-14 = (-2) \cdot 7$ então $7| (-14)$, daí concluímos que $7| 143.549$.

Nesse critério de divisibilidade por 7 foram necessárias 2 iterações e 12 operações para verificar se é divisível por 7.

Exemplo (Critério das classes**):** Verifique o critério de divisibilidade por 7 da proposição sobre o número 143.549.

$$549 - 143 = 406$$

Agora temos que não podemos mais usar o mesmo critério pois esse critério só pode ser aplicado para número com mais de 3 algarismos. Logo, a melhor maneira para proceder é utilizar outro critério de divisibilidade para continuar a verificação. Utilizando o critério de divisibilidade por 7, temos:

$$40 - 2 \cdot 6 = 40 - 12 = 28$$

Como $28 = 4 \cdot 7$ então $7| 28$, daí concluímos que $7| 143.549$.

Nesse critério de divisibilidade por 7 foram necessárias 2 iterações e 3 operações para verificar se é divisível por 7.

Exemplo (Mais um Critério de divisibilidade por 7**):** Verifique o critério de divisibilidade por 7 da proposição sobre o número 143.549.

$$2 \cdot 14.354 + 3 \cdot 9 = 28.708 + 27 = 28.735$$

$$2 \cdot 2.873 + 3 \cdot 5 = 5.761$$

$$2 \cdot 576 + 3 \cdot 1 = 1.155$$

$$2 \cdot 115 + 3 \cdot 5 = 245$$

$$2 \cdot 24 + 3 \cdot 5 = 63$$

Como $63 = 9 \cdot 7$ então $7|63$ daí concluímos que $7|\ 143.549$.

Nesse critério de divisibilidade por 7 foram necessárias 5 iterações e 15 operações para verificar se é divisível por 7.

A tabela abaixo mostra o número de iterações e de operações para número de 6 dígitos 143.549.

Tabela 5: Comparando diferentes critérios de divisibilidade por 7

	Critério de divisibilidade	**Iterações**	**Operações**
1	Critério de Blaise Pascal	1	10
2	Critério de Zbikowski	3	6
3	Critério de Chika Ofili	4	8
4	Critério da quebra na dezena	2	8
5	Critério da quebra na centena	2	12
6	Critérios das Classes	2	3
7	Mais um critério de divisibilidade por 7	5	15

Fonte: Elaborado pelo autor.

Se estivermos procurando o critério com o menor número de iterações para 143.549, observamos que o critério de Pascal é o melhor com essa característica.

Se estivermos procurando o critério com o menor número de operações para 143.549, então o critério das classes combinado com o de Zbikowski será o melhor. Não foi utilizado apenas o critério das classes nessa verificação, pois não dava para utilizá-lo novamente no número remanescente.

Utilizando apenas um critério para verificar a divisibilidade por 7 observamos que o melhor é o de Zbikowski com 6 operações. Talvez, por esse motivo, seja o mais comentado nos livros.

6 CONSIDERAÇÕES FINAIS

No presente trabalho foi estabelecida uma comparação entre alguns critérios de divisibilidade por 7. Foi verificado que o critério de divisibilidade de Zbikowski é o que necessita um menor número de operações para a verificação de um número de 6 algarismos. Foi verificado, também, que o critério de divisibilidade de Pascal é o que necessita um menor número de iterações (uso do algoritmo) para a verificação do mesmo número.

Foram apresentados os critérios de divisibilidade por 2, 3, 4, 5, 6, 7, 8, 9 e 10. Foi mostrado como construir critérios de divisibilidade por números primos utilizando o Teorema da Quebra na Unidade. Também, foi apresentado o ambiente de programação Pascal e foi construído algoritmos para determinar os divisores de um número, para determinar se um número é primo ou não e para gerar critérios de divisibilidade por números primos.

Houve alguns obstáculos para a construção dos algoritmos, pois era necessário rever a linguagem de programação Pascal. Também houve dificuldade na construção do texto, pois não há muitos artigos e dissertações sobre a temática. Algumas dissertações e alguns artigos foram fundamentais para isso.

Muitas vezes o que se ensina é feito de maneira mecânica e os conteúdos são explicados sem mostrar como surgiu e o seu porquê. Daí a importância de se saber como os critérios de divisibilidade são construídos e como demonstrá-los. Também é importante mostrar vários critérios de divisibilidade para o aluno para o mesmo escolher aquele que considere mais fácil de utilizar. Além disso, a temática é pouco abordada no ensino básico, apenas no 6º ano do ensino fundamental e em turmas olímpicas. Daí a necessidade de tratar a temática com maior profundidade.

Os algoritmos para gerar critérios de divisibilidade utilizando a quebra a dezena e na centena não foi possível ser construído por questão de tempo e pela sua complexidade. Pretende-se construir tais algoritmos num trabalho futuro. Como o conteúdo algoritmo foi inserido na BNNC do ensino médio, o trabalho pode servir como guia para a apresentação do tema em turmas regulares e olímpicas do ensino médio.

É necessário que o professor esteja mais preparado tanto em conteúdo quanto em ferramentas computacionais para ministrar as aulas, pois é uma demanda crescente o conhecimento matemático e computacional na sociedade atual.

REFERÊNCIAS

ANDREESCU, Titu. GELCA, Razvan. **Putnam and Beyond**. New York: Springer, 2007.

ALENCAR FILHO, Edgard de. **Aritmética dos Inteiros**. São Paulo: Nobel, 1987.

ALENCAR FILHO, Edgard de. **Teoria Elementar dos Números**. São Paulo: Nobel, 1981.

ÁVILA, Geraldo Severo de Souza. **Várias faces da matemática:** tópicos para licenciatura e leitura geral. São Paulo: Blucher, 2010.

BRASIL. Ministério da Educação. Base Nacional Comum Curricular. Brasília, 2018. Disponível em http://base nacionalcomum.mmec.gov.br/images/BNCC_ELEF_110518_versa ofinal_site.pdf.

BRASIL. Ministério da Educação. Base Nacional Comum Curricular. Brasília, 2018. Disponível em http://portal.mec.gov.br/index.php?option=com_docman&view=download&ali as=85121-bncc-ensino-medio&category_slug=abril-2018-pdf&Itemid=30192.

CAMINHA, Antonio Muniz. **Tópicos de Matemática Elementar Volume 5:** Teoria dos Números. Rio de Janeiro: SBM, 2013.

BURTON, David. **Elementary Number Theory.** Massachusetts: Allyn and Bacon, 1980.

DOMINGUES, Hygino Hungueros. **Fundamentos de Aritmética.** São Paulo: Atual, 1991.

FERREIRA, Antonio Eudes. **Números primos e o postulado de Bertrand.** 44 f. Dissertação (Mestrado Profissional em Matemática em Rede Nacional) – Universidade Federal da Paraíba, João Pessoa, 2014.

GUEDES, Mário Gustavo Pinto.88). Outros critérios de divisibilidade. **Revista Professor de Matemática,** Rio de Janeiro, n2, 1988.

HEFEZ, Abramo. **Aritmética**. Rio de Janeiro: SBM, 2016.

HEFEZ, Abramo. **Iniciação a Aritmética**. Rio de Janeiro: IMPA, 2015.

IEZZI, Gelson. MURAKAMI, Carlos. **Fundamentos da Matemática Elementar vol. 1:** Conjuntos e Funções**.** São Paulo: Atual, 2013.

LIMA, Elon Lages. **Análise Real Volume 1:** Funções de uma variável**.** Rio de Janeiro: IMPA, 2006.

MANZANO, José Augusto Navarro Garcia. YAMATUMI, Wilson Yoshiteru. **Programando em Turbo Pascal 7.0:** Guia Prático de Orientação e Desenvolvimento. São Paulo: Érica, 2001.

MARTINEZ, Fábio Brochero. MOREIRA, Carlos Gustavo. SALDANHA, Nicolau. TENGAN, Eduardo. **Teoria dos Números:** um passeio com primos e outros números familiares pelo mundo inteiro. Rio de Janeiro: IMPA, 2018.

MATHIAS, Ivo Mario. **Algoritmos e programação I.** Ponta Grossa: UEPG, 2017.

OLIVEIRA, Krerley Irraciel Martins; FERNÁNDEZ, Adán José Corcho. **Iniciação à matemática:** um curso com problemas e soluções. Rio de Janeiro: SBM, 2010.

PEREIRA, Ricardo Reis. **Linguagem de Programação I.** Fortaleza: Editora UECE, 2015.

RIBEIRO, Bruno; SILVA, Talysson Paulo da. Montando critérios de divisibilidade diferentes. **Professor de matemática on-line**, Rio de Janeiro, v.8, n.2, abril de 2020. Disponível em: <https://doi.org/10.21711/2319023x2020/pmo813>.

SANTOS, José Plínio de Oliveira. **Introdução à Teoria dos Números.** Rio de Janeiro: SBM, 1998.

SILVA, Talysson Paulo da. **Critérios de divisibilidade: usuais, incomuns e curiosos.** 61 f. Dissertação (Mestrado Profissional em Matemática em Rede Nacional) – Universidade Federal da Paraíba, João Pessoa, 2019.

SHIMOKAWA, Edivaldo Yuzo. **Teste de Chika:** Um critério geral de divisibilidade**.** 2020. 34 f. Dissertação (Mestrado Profissional em Matemática em Rede Nacional) – Universidade Federal do Mato Grosso, Cuiabá, 2020.

ANEXO

Lista de Números Primos

Até 10:

2 3 5 7

Até 100:

11 13 17 19 23 29 31 37 41 43 47 53 59 61 67 71 73 79 83 89 97

Até 1000:

101 103 107 109 113 127 131 137 139 149 151 157 163 167 173 179 181 191 193 197
199 211 223 227 229 233 239 241 251 257 263 269 271 277 281 283 293 307 311 313
317 331 337 347 349 353 359 367 373 379 383 389 397 401 409 419 421 431 433 439
443 449 457 461 463 467 479 487 491 499 503 509 521 523 541 547 557 563 569 571
577 587 593 599 601 607 613 617 619 631 641 643 647 653 659 661 673 677 683 691
701 709 719 727 733 739 743 751 757 761 769 773 787 797 809 811 821 823 827 829
839 853 857 859 863 877 881 883 887 907 911 919 929 937 941 947 953 967 971 977
983 991 997

Até 10.000:

1009 1013 1019 1021 1031 1033 1039 1049 1051 1061 1063 1069 1087 1091 1093 1097
1103 1109 1117 1123 1129 1151 1153 1163 1171 1181 1187 1193 1201 1213 1217 1223
1229 1231 1237 1249 1259 1277 1279 1283 1289 1291 1297 1301 1303 1307 1319 1321
1327 1361 1367 1373 1381 1399 1409 1423 1427 1429 1433 1439 1447 1451 1453 1459
1471 1481 1483 1487 1489 1493 1499 1511 1523 1531 1543 1549 1553 1559 1567 1571
1579 1583 1597 1601 1607 1609 1613 1619 1621 1627 1637 1657 1663 1667 1669 1693
1697 1699 1709 1721 1723 1733 1741 1747 1753 1759 1777 1783 1787 1789 1801 1811
1823 1831 1847 1861 1867 1871 1873 1877 1879 1889 1901 1907 1913 1931 1933 1949
1951 1973 1979 1987 1993 1997 1999 2003 2011 2017 2027 2029 2039 2053 2063 2069
2081 2083 2087 2089 2099 2111 2113 2129 2131 2137 2141 2143 2153 2161 2179 2203
2207 2213 2221 2237 2239 2243 2251 2267 2269 2273 2281 2287 2293 2297 2309 2311
2333 2339 2341 2347 2351 2357 2371 2377 2381 2383 2389 2393 2399 2411 2417 2423
2437 2441 2447 2459 2467 2473 2477 2503 2521 2531 2539 2543 2549 2551 2557 2579
2591 2593 2609 2617 2621 2633 2647 2657 2659 2663 2671 2677 2683 2687 2689 2693
2699 2707 2711 2713 2719 2729 2731 2741 2749 2753 2767 2777 2789 2791 2797 2801
2803 2819 2833 2837 2843 2851 2857 2861 2879 2887 2897 2903 2909 2917 2927 2939
2953 2957 2963 2969 2971 2999 3001 3011 3019 3023 3037 3041 3049 3061 3067 3079
3083 3089 3109 3119 3121 3137 3163 3167 3169 3181 3187 3191 3203 3209 3217 3221
3229 3251 3253 3257 3259 3271 3299 3301 3307 3313 3319 3323 3329 3331 3343 3347
3359 3361 3371 3373 3389 3391 3407 3413 3433 3449 3457 3461 3463 3467 3469 3491
3499 3511 3517 3527 3529 3533 3539 3541 3547 3557 3559 3571 3581 3583 3593 3607
3613 3617 3623 3631 3637 3643 3659 3671 3673 3677 3691 3697 3701 3709 3719 3727
3733 3739 3761 3767 3769 3779 3793 3797 3803 3821 3823 3833 3847 3851 3853 3863

3877 3881 3889 3907 3911 3917 3919 3923 3929 3931 3943 3947 3967 3989 4001 4003
4007 4013 4019 4021 4027 4049 4051 4057 4073 4079 4091 4093 4099 4111 4127 4129
4133 4139 4153 4157 4159 4177 4201 4211 4217 4219 4229 4231 4241 4243 4253 4259
4261 4271 4273 4283 4289 4297 4327 4337 4339 4349 4357 4363 4373 4391 4397 4409
4421 4423 4441 4447 4451 4457 4463 4481 4483 4493 4507 4513 4517 4519 4523 4547
4549 4561 4567 4583 4591 4597 4603 4621 4637 4639 4643 4649 4651 4657 4663 4673
4679 4691 4703 4721 4723 4729 4733 4751 4759 4783 4787 4789 4793 4799 4801 4813
4817 4831 4861 4871 4877 4889 4903 4909 4919 4931 4933 4937 4943 4951 4957 4967
4969 4973 4987 4993 4999 5003 5009 5011 5021 5023 5039 5051 5059 5077 5081 5087
5099 5101 5107 5113 5119 5147 5153 5167 5171 5179 5189 5197 5209 5227 5231 5233
5237 5261 5273 5279 5281 5297 5303 5309 5323 5333 5347 5351 5381 5387 5393 5399
5407 5413 5417 5419 5431 5437 5441 5443 5449 5471 5477 5479 5483 5501 5503 5507
5519 5521 5527 5531 5557 5563 5569 5573 5581 5591 5623 5639 5641 5647 5651 5653
5657 5659 5669 5683 5689 5693 5701 5711 5717 5737 5741 5743 5749 5779 5783 5791
5801 5807 5813 5821 5827 5839 5843 5849 5851 5857 5861 5867 5869 5879 5881 5897
5903 5923 5927 5939 5953 5981 5987 6007 6011 6029 6037 6043 6047 6053 6067 6073
6079 6089 6091 6101 6113 6121 6131 6133 6143 6151 6163 6173 6197 6199 6203 6211
6217 6221 6229 6247 6257 6263 6269 6271 6277 6287 6299 6301 6311 6317 6323 6329
6337 6343 6353 6359 6361 6367 6373 6379 6389 6397 6421 6427 6449 6451 6469 6473
6481 6491 6521 6529 6547 6551 6553 6563 6569 6571 6577 6581 6599 6607 6619 6637
6653 6659 6661 6673 6679 6689 6691 6701 6703 6709 6719 6733 6737 6761 6763 6779
6781 6791 6793 6803 6823 6827 6829 6833 6841 6857 6863 6869 6871 6883 6899 6907
6911 6917 6947 6949 6959 6961 6967 6971 6977 6983 6991 6997 7001 7013 7019 7027
7039 7043 7057 7069 7079 7103 7109 7121 7127 7129 7151 7159 7177 7187 7193 7207
7211 7213 7219 7229 7237 7243 7247 7253 7283 7297 7307 7309 7321 7331 7333 7349
7351 7369 7393 7411 7417 7433 7451 7457 7459 7477 7481 7487 7489 7499 7507 7517
7523 7529 7537 7541 7547 7549 7559 7561 7573 7577 7583 7589 7591 7603 7607 7621
7639 7643 7649 7669 7673 7681 7687 7691 7699 7703 7717 7723 7727 7741 7753 7757
7759 7789 7793 7817 7823 7829 7841 7853 7867 7873 7877 7879 7883 7901 7907 7919
7927 7933 7937 7949 7951 7963 7993 8009 8011 8017 8039 8053 8059 8069 8081 8087
8089 8093 8101 8111 8117 8123 8147 8161 8167 8171 8179 8191 8209 8219 8221 8231
8233 8237 8243 8263 8269 8273 8287 8291 8293 8297 8311 8317 8329 8353 8363 8369
8377 8387 8389 8419 8423 8429 8431 8443 8447 8461 8467 8501 8513 8521 8527 8537
8539 8543 8563 8573 8581 8597 8599 8609 8623 8627 8629 8641 8647 8663 8669 8677
8681 8689 8693 8699 8707 8713 8719 8731 8737 8741 8747 8753 8761 8779 8783 8803
8807 8819 8821 8831 8837 8839 8849 8861 8863 8867 8887 8893 8923 8929 8933 8941
8951 8963 8969 8971 8999 9001 9007 9011 9013 9029 9041 9043 9049 9059 9067 9091
9103 9109 9127 9133 9137 9151 9157 9161 9173 9181 9187 9199 9203 9209 9221 9227
9239 9241 9257 9277 9281 9283 9293 9311 9319 9323 9337 9341 9343 9349 9371 9377
9391 9397 9403 9413 9419 9421 9431 9433 9437 9439 9461 9463 9467 9473 9479 9491
9497 9511 9521 9533 9539 9547 9551 9587 9601 9613 9619 9623 9629 9631 9643 9649
9661 9677 9679 9689 9697 9719 9721 9733 9739 9743 9749 9767 9769 9781 9787 9791
9803 9811 9817 9829 9833 9839 9851 9857 9859 9871 9883 9887 9901 9907 9923 9929
9931 9941 9949 9967 9973