Universidade Federal de Goiás
Instituto de Matemática e Estatística
Programa de Mestrado Profissional em
Matemática em Rede Nacional

Uma Aplicação da Congruência na Determinação de Critérios de Divisibilidade

Luis Henrique Pereira da Silva

Goiânia

2015

sistema de bibliotecas ufg

UFG

TERMO DE CIÊNCIA E DE AUTORIZAÇÃO PARA DISPONIBILIZAR AS TESES E DISSERTAÇÕES ELETRÔNICAS (TEDE) NA BIBLIOTECA DIGITAL DA UFG

Na qualidade de titular dos direitos de autor, autorizo a Universidade Federal de Goiás (UFG) a disponibilizar, gratuitamente, por meio da Biblioteca Digital de Teses e Dissertações (BDTD/UFG), sem ressarcimento dos direitos autorais, de acordo com a Lei nº 9610/98, o documento conforme permissões assinaladas abaixo, para fins de leitura, impressão e/ou *download*, a título de divulgação da produção científica brasileira, a partir desta data.

1. Identificação do material bibliográfico: **[x] Dissertação** **[ ] Tese**

2. Identificação da Tese ou Dissertação

Autor (a):	Luis Henrique Pereira da Silva					
E-mail:	luis-leidy@hotmail.com					
Seu e-mail pode ser disponibilizado na página? [x]Sim [ ] Não						
Vínculo empregatício do autor	Secretária Municipal de Educação de Nerópolis-GO					
Agência de fomento:	Fundação Coordenação de Aperfeiçoamento de Pessoal de Nível Superior			Sigla:	CAPES	
País:	Brasil	UF:	GO	CNPJ:	**00.889.834/0001-08**	
Título:	Uma Aplicação da Congruência na Determinação de Critérios de Divisibilidade					
Palavras-chave:	Critérios de divisibilidade para números inteiros, multiplicação e divisão Egípcia, máximo divisor comum, números primos, decomposição em fatores primos e congruência.					
Título em outra língua:	A Matching of Application for the Determination of Criteria Divisibility					
Palavras-chave em outra língua:	Divisibility criteria to whole numbers, multiplication and division Egyptian, greatest common divisor, prime numbers, decomposition in prime factors and matching.					
Área de concentração:	Matemática do Ensino Básico					
Data defesa: (27/03/2015)						
Programa de Pós-Graduação:	Mestrado Profissional em Matemática em Rede Nacional					
Orientador (a):	Dr. Mário José de Souza					
E-mail:						
Co-orientador (a):*						
E-mail:						

*Necessita do CPF quando não constar no SisPG

3. Informações de acesso ao documento:

Concorda com a liberação total do documento [x] SIM [ ] NÃO[1]

Havendo concordância com a disponibilização eletrônica, torna-se imprescindível o envio do(s) arquivo(s) em formato digital PDF ou DOC da tese ou dissertação.

O sistema da Biblioteca Digital de Teses e Dissertações garante aos autores, que os arquivos contendo eletronicamente as teses e ou dissertações, antes de sua disponibilização, receberão procedimentos de segurança, criptografia (para não permitir cópia e extração de conteúdo, permitindo apenas impressão fraca) usando o padrão do Acrobat.

Luis Henrique Pereira da Silva

Assinatura do (a) autor (a)

Data: 27 / 03 / 2015

[1] Neste caso o documento será embargado por até um ano a partir da data de defesa. A extensão deste prazo suscita justificativa junto à coordenação do curso. Os dados do documento não serão disponibilizados durante o período de embargo.

Luis Henrique Pereira da Silva

Uma Aplicação da Congruência na Determinação de Critérios de Divisibilidade

Trabalho de Conclusão de Curso apresentado ao Instituto de Matemática e Estatística da Universidade Federal de Goiás, como parte dos requisitos para obtenção do grau de Mestre em Matemática.

Área de Concentração: Matemática do Ensino Básico

Orientador: Prof. Dr. MÁRIO JOSÉ DE SOUZA

Goiânia

2015

Ficha catalográfica elaborada automaticamente
com os dados fornecidos pelo(a) autor(a), sob orientação do Sibi/UFG.

Pereira da Silva, Luis Henrique
Uma Aplicação da Congruência na Determinação de Critérios de Divisibilidade [manuscrito] / Luis Henrique Pereira da Silva. - 2015.
52 f.

Orientador: Prof. Dr. Mário José de Souza.
Dissertação (Mestrado) - Universidade Federal de Goiás, Instituto de Matemática e Estatística (IME) , Programa de Pós-Graduação em Ensino na Educação Básica (Profissional), Goiânia, 2015.
Bibliografia.

1. Critérios de divisibilidade para números inteiros. 2. multiplicação e divisão Egípcia. 3. máximo divisor comum. 4. números primos. 5. decomposição em fatores primos e congruência. I. de Souza, Mário José, orient. II. Título.

Luis Henrique Pereira da Silva

Uma Aplicação da Congruência na Determinação de Critérios de Divisibilidade

Trabalho de Conclusão de Curso defendido no Programa de Mestrado Profissional em Matemática em Rede Nacional – PROFMAT/UFG, do Instituto de Matemática e Estatística da Universidade Federal de Goiás, como requisito parcial para obtenção do título de Mestre em Matemática, área de concentração Matemática do Ensino Básico, aprovado no dia 27 de março de 2015, pela Banca Examinadora constituída pelos professores:

Prof. Dr. Mário José de Souza
Instituto de Matemática e Estatística-UFG
Presidente da Banca

Prof. Dr. Moiseis dos Santos Cecconello
ICET/UFMT

Profª. Drª. Lidiane dos Santos Monteiro Lima
Instituto de Matemática e Estatística-UFG

Luis Henrique Pereira da Silva graduou-se em Matemática pela Universidade Estadual de Goiás (UEG) 2003, obtendo o título de licenciado em matemática.

Dedico este trabalho a minha amada esposa Leidy e aos meus filhos Henrique e Arthur minhas Vidas.

Agradecimentos

Agradeço primeiramente a Deus, que é criador de todas as coisas e o maior idealizador dos meus sonhos.

À minha esposa, que está sempre ao meu lado e aos meus filhos pela compreensão nesse período, que por muitas das vezes abriram mão de suas vontades para me satisfazer.

Aos Professores que contribuíram para minha formação acadêmica.

Aos amigos que formamos pelas trocas de experiências, sugestões e companheirismo no curso.

Ao meu orientador o Professor Doutor Mário José de Souza, por acreditar em minha capacidade e incentivo em desenvolver este trabalho.

À CAPES pelo suporte financeiro, com bolsa de estudos que foi fundamental nesses dois anos.

Resumo

Este trabalho tem como objetivo demonstrar de modo prático os critérios de divisibilidade de 2 a 97 no crivo de Eratóstenes com os corte a direita e a esquerda, baseando-se no método de multiplicação e divisão egípcia. Todo processo é demostrado utilizando a divisibilidade para números inteiros, máximo divisor comum, números primos, decomposição em fatores primos e congruência.

Palavras-chave

Critérios de divisibilidade para números inteiros, multiplicação e divisão Egípcia, máximo divisor comum, números primos, decomposição em fatores primos e congruência.

Abstract

This work aims to demonstrate in a practical way the divisibility criteria 2-97 in sieve Eratostenes with cutting the right and the left, based on the method of multiplication and division Egyptian. The entire process is demonstrated using the divisibility to whole numbers, greatest common divisor, prime numbers, decomposition in prime factors and matching.

Keywords

Divisibility criteria to whole numbers, multiplication and division Egyptian, greatest common divisor, prime numbers, decomposition in prime factors and matching.

Sumário

1 Introdução

O foco deste trabalho são os critérios de divisibilidade de números inteiros positivos. Os conteúdos matemáticos que serão apresentados estão ligados a estes critérios. Esta introdução descreve as aflições pela quais passam alguns professores, em sala de aula, quando buscam responder como os números chegaram até nós e como os egípcios efetuavam multiplicações e divisões utilizando apenas sucessões de duplicações, servindo de fundamento aos critérios que serão desenvolvidos.

A Grande Invenção

Frequentemente sou indagado pelos meus alunos, com perguntas, talvez inocentes, mas de relevância para o processo de ensino aprendizagem. Perguntas como "Quem inventou os números? Para quê? Onde? Como eles calculavam?". Estas perguntas se bem trabalhadas e vivenciadas, dão uma melhor percepção da matemática permitindo aprendê-la e descobrí-la.

É interessante observar que as histórias da matemática e da humanidade fundem-se uma na outra quando afirmam que a invenção dos números deve ter correspondido as preocupações de ordem prática e utilitária, assim como o fogo e a roda. Em suas buscas, homens distantes no espaço e no tempo, postos em condições idênticas, alcançaram resultados inteiramente análogos. Os algarismos 0, 1, 2, 3, 4, 5, 6, 7, 8 e 9 descrevem todos os números que a mente humana pode imaginar de modo que tornou-se uma linguagem universal entre os povos e nações do mundo atual.

Com a necessidade de efetuar contagens cada vez mais extensas, o processo de contar foi sistematizado. Isso foi feito por meio dos algarismos acima mencionados colocando os números em grupos básicos convenientes, representando assim uma correspondência com os elementos de um outro conjunto. Em [4] o autor descreve que o método consiste em escolher um certo número b como base e atribuir nomes aos $1, 2, 3, \ldots, b$. Para os números maiores do que b os nomes eram essencialmente combinações dos nomes dos números já escolhidos.

Pensar que as quatro operações de aritmética, que hoje parece elementares, representou durante alguns séculos, para milhares de homens, uma arte complexa, reservada para poucos, geralmente sacerdotes. Que os cálculos eram em sua maioria realizados com os dedos da mão ou por fichas, e que contabilizavam-se com entalhes em madeiras ou ossos de animais. Em [6] vê-se que para dominar os mistérios da multiplicação e da divisão, o filho de um rico comerciante da Idade Média necessitava de vários anos de estudo e passava pelas vicissitudes de uma viagem por toda a Europa.

Para os Egípcios a operação aritmética fundamental era a adição, e as operações de multiplicação e divisão eram em geral efetuadas por uma sucessão de duplicações com base no fato de que todo número pode ser representado por uma soma de potências de 2. Como exemplo de multiplicação o produto de 29 por 35 pode ser encontrado, dobrando o 1 até que o próximo dobro exceda o multiplicando 29. O trabalho pode ser disposto como se segue:

$*$	1	35
	2	70
$*$	4	140
$*$	8	280
$*$	16	560

Como $29 = 16 + 8 + 4 + 1$, somando-se os múltiplos adequados de 35, isto é, aqueles indicados por $(*)$ chega-se à resposta $35 + 140 + 280 + 560 = 1015$. E para, digamos, dividir 814 por 31, dobra-se sucessivamente o divisor 31 até o ponto em que o próximo dobro exceda o dividendo 814. O procedimento está exposto abaixo:

	1	31
$*$	2	62
	4	124
$*$	8	248
$*$	16	496

Como

$$\begin{aligned} 814 &= 496 + 318 \\ &= 496 + 248 + 70 \\ &= 496 + 248 + 62 + 8 \end{aligned}$$

vemos, observando as linhas com $(*)$ na coluna acima, que o quociente é $16+8+2 = 26$ e que o resto é 8. Para [4] o processo egípcio de multiplicação e divisão não só elimina a necessidade de aprender uma tábua de multiplicação, como também se amolda tanto ao ábaco que perdurou enquanto esse instrumento esteve em uso e mesmo depois.

A seguir é apresentada, uma breve descrição de cada capítulo.

No Capítulo 2, são estudadas propriedades elementares sobre divisibilidade no conjunto dos números inteiros, sendo que o Algoritmo da Divisão (Teorema 2.4) apresenta-se como o resultado mais importante. As noções de máximo divisor comum e de números primos com um método prático para os determinar, também são enfatizadas.

No Capítulo 3, o conceito de congruência é introduzido e são apresentadas as propriedades que são utilizadas para demonstrar os critérios de divisibilidade com a ideia de corte a direita (Teorema 3.7, Corolários 3.8 e 3.9) e do corte a esquerda (Teorema 3.10). Este último fornece o resto quando um dado número não é divisível (Observação 3.16). Alguns exemplos mostram o funcionamento dos critérios.

No Capítulo 4 algumas aplicações dos critérios de divisibilidade são apresentados com o intuito de motivar o professor e desmistificar aqueles livros didáticos de matemática que colocam alguns critérios de divisibilidade como inúteis.

No último Capítulo as considerações finais desse trabalho são feitas.

2 Divisibilidade

Neste capítulo serão apresentados vários resultados básicos relacionadas a divisibilidade no conjunto dos números inteiros. Serão enfatizados o algoritmo da divisão, a noção do máximo divisor comum e o papel fundamental desempenhado pelos números primos. Para mais detalhes sobre o assunto as referências [3], [5], [8] e [11] são indicadas.

2.1 Divisibilidade

Definição 2.1. *Dados $a, b \in \mathbb{Z}$, com $a \neq 0$, dizemos que a divide b, denotamos por $a \mid b$, se existir um $k \in \mathbb{Z}$ tal que $b = a \cdot k$. Caso a não divida b, escrevemos $a \nmid b$.*

Proposição 2.2. *Se a, b e $c \in \mathbb{Z}$, $a \mid b$ e $b \mid c$, então $a \mid c$, com a e $b \neq 0$.*

Demonstração: Por hipótese $a \mid b$ e $b \mid c$, então pela Definição 2.1 existem $k_1, k_2 \in \mathbb{Z}$ tal que $b = a \cdot k_1$ e $c = b \cdot k_2$. Substituindo o valor de b na equação $c = b \cdot k_2$ teremos $c = a \cdot k_1 \cdot k_2$ como $k_1, k_2 \in \mathbb{Z}$ implica que $a \mid c$. ■

Proposição 2.3. *Se a, b, c, m e $n \in \mathbb{Z}$, $c \mid a$ e $c \mid b$, então $c \mid (m \cdot a \pm n \cdot b)$.*

Demonstração: Por hipótese $c \mid a$ e $c \mid b$, então pela Definição 2.1 existem $k_1, k_2 \in \mathbb{Z}$ tal que $a = c \cdot k_1$ e $b = c \cdot k_2$. Multiplicando-se estas duas equações respectivamente por m e n teremos $m \cdot a = m \cdot c \cdot k_1$ e $n \cdot b = n \cdot c \cdot k_2$. Somando-se membro a membro obtemos $m \cdot a + n \cdot b = m \cdot c \cdot k_1 + n \cdot c \cdot k_2$, o que implica
$m \cdot a + n \cdot b = c \cdot \underbrace{(m \cdot k_1 + n \cdot k_2)}_{\in \mathbb{Z}}$, ou seja, $c \mid (m \cdot a + n \cdot b)$. De maneira análoga provamos que $c \mid (m \cdot a - n \cdot b)$. ■

Teorema 2.4 (algoritmo da divisão). *Dados a e $b \in \mathbb{Z}$, com $b \neq 0$, existem únicos q e $r \in \mathbb{Z}$ tais que $a = b \cdot q + r$, com $0 \leq r < |b|$, $(r = 0 \Leftrightarrow b \mid a)$. Tais inteiros q e r são, respectivamente, o quociente e o resto da divisão de a por b.*

Demonstração: Suponha primeiro que $b > 0$, e seja q o maior inteiro tal que $b \cdot q \leq a$. Então $b \cdot q \leq a < b \cdot (q + 1) = b \cdot q + b$, de modo que $0 \leq a - b \cdot q < b$ e basta definir $r = a - b \cdot q$. Se $b < 0$, então $-b > 0$, donde existem $q, r \in \mathbb{Z}$ tais que $a = (-b) \cdot q + r$, com $0 \leq r < -b$. Daí, $a = b \cdot (-q) + r$, com $0 \leq r < -b = |b|$. Desta

forma, teremos garantida, a existência de q e r. A fim de mostrarmos a unicidade, suponha a existência de outro par q' e $r' \in \mathbb{Z}$, verificando:
$a = b \cdot q + r = b \cdot q' + r'$, com $0 \leq r' < |b|$.
Disto tem-se $(b \cdot q + r) - (b \cdot q' + r') = 0 \Rightarrow b \cdot (q - q') = r' - r$, ou seja, $b \mid (r' - r)$.
Mas, como $r' < b$ e $r < b$, tem-se $|r' - r| < b$ e, como $b \mid (r' - r)$ deve-se ter $r' - r = 0$ o que implica $r = r'$. Logo $q' \cdot b = q \cdot b \Rightarrow q = q'$, uma vez que $b \neq 0$. ■

Observação 2.5. *O resto da divisão de a por b é zero se, e somente se, $b \mid a$.*

Observação 2.6. *A demonstração do Teorema 2.4 fornece um algoritmo (isto é, um procedimento executável) para calcular o quociente e o resto da divisão de um número por outro, por subtrações sucessivas.*

Exemplo 2.7. *Calculemos a divisão de 23 por 5:* $23 - 3 \cdot 5 = 8$*;* $23 - 4 \cdot 5 = 3 < 5$*, sendo* $q = 4$ *e* $r = 3$*.*

2.2 Máximo Divisor Comum

Nesta seção será apresentado um algoritmo prático para encontrar o máximo divisor comum entre dois números inteiros, bem como vários resultados do máximo divisor comum que facilitam o processo de divisibilidade entre esses dois números.

Máximo Divisor Comum

Definição 2.8. *O máximo divisor comum de dois inteiros positivos a e b, não simultaneamente nulos, denotado por (a, b), é o maior inteiro positivo que divide a e b.*

Algoritmo de Euclides: Segundo [5] o método, chamado de Algoritmo de Euclides, é um primor do ponto de vista computacional e pouco conseguiu-se aperfeiçoá-lo em mais de dois milênios. O algoritmo pode ser sintetizado e realizado na prática.
Inicialmente, efetuamos a divisão $a = b \cdot q_1 + r_1$ e colocamos os números envolvidos no seguinte diagrama:

	q_1	
a	b	
r_1		

A seguir, continuamos efetuando a divisão $b = r_1 \cdot q_2 + r_2$ e colocamos os números envolvidos no diagrama:

	q_1	q_2	
a	b	r_1	
r_1	r_2		

Prosseguimos, enquanto for possível, até obtermos:

	q_1	q_2	q_3	$\ldots$	q_{n-1}	q_n	q_{n+1}
a	b	r_1	r_2	$\ldots$	r_{n-2}	r_{n-1}	$r_n = (a, b)$
r_1	r_2	r_3	r_4	$\ldots$	r_n	0	

Exemplo 2.9. *Calcule o máximo divisor comum de 168 e 49.*

	3	2	3
168	49	21	$7 = (168, 49)$
$168 - 147 = 21$	$49 - 42 = 7$	$21 - 21 = 0$	

Observação 2.10. *Note que o quociente não interessa neste algoritmo. Basta o resto.*

Definição 2.11. *Os inteiros a e b são relativamente primos quando $(a, b) = 1$.*

Teorema 2.12. *Seja $d \in \mathbb{Z}$ o máximo divisor comum de a e $b \in \mathbb{Z}$, então existem inteiros n_0 e m_0 tais que $d = n_0 \cdot a + m_0 \cdot b$.*

Demonstração: Seja B o conjunto de todas as combinações lineares $n \cdot a + m \cdot b$ onde n e $m \in \mathbb{Z}$. Este conjunto contém claramente, números negativos, positivos e também o zero. Sejam n_0 e m_0 tais que $c = n_0 \cdot a + m_0 \cdot b$ seja o menor inteiro positivo pertencente ao conjunto B. Mostremos que $c \mid a$ e $c \mid b$. Suponhamos que $c \nmid a$. Neste caso, pelo Teorema 2.4, existem q e r tais que: $a = q \cdot c + r$ com $0 < r < c$. Portanto, $r = a - q \cdot c = a - q \cdot (n_0 \cdot a + m_0 \cdot b) = a \cdot (1 - q \cdot n_0) + (-q \cdot m_0) \cdot b$. Isto mostra que

$r \in B$, pois $(1 - q \cdot n_0)$ e $(-q \cdot m_0) \in \mathbb{Z}$, o que é uma contradição, uma vez que $0 < r < c$ e c é o menor elemento positivo de B. Logo, $c \mid a$ e de forma análoga se prova que $c \mid b$.
Como d é um divisor comum de a e b, existem k_1 e $k_2 \in \mathbb{Z}$, tais que $a = k_1 \cdot d$ e $b = k_2 \cdot d$ e, portanto, $c = n_0 \cdot a + m_0 \cdot b = n_0 \cdot k_1 \cdot d + m_0 \cdot k_2 \cdot d = d \cdot \underbrace{(n_0 \cdot k_1 + m_0 \cdot k_2)}_{\in \mathbb{Z}}$
o que implica $d \mid c$ e como $d < c$ não é possível, uma vez que d é o maior divisor comum, concluimos que $d = n_0 \cdot a + m_0 \cdot b$. ■

Teorema 2.13. *Dados d, m e $n \in \mathbb{Z}$, tal que $d = m \cdot n$ e $(m, n) = 1$, então $d \mid a$, $a \in \mathbb{Z}$, se, e somente se, $m \mid a$ e $n \mid a$.*

Demostração: $\Rightarrow$) Como $d \mid a$, pela Definição 2.1, existe $r \in \mathbb{Z}$ tal que $a = d \cdot r$, mas por hipótese $d = m \cdot n$, donde $a = m \cdot n \cdot r$ o que implica $m \mid a$ e $n \mid a$.
$\Leftarrow$) Como $m \mid a$ e $n \mid a$, pela Definição 2.1, existem r_1 e $r_2 \in \mathbb{Z}$, tal que ($a = m \cdot r_1$ e $a = n \cdot r_2$) (I), como por hipótese $(m, n) = 1$ e $d = m \cdot n$, segue-se do Teorema 2.12 que:
$m \cdot b + n \cdot c = 1$ (Multiplicando ambos os lados da igualdade por a)
$m \cdot b \cdot a + n \cdot c \cdot a = a$ (Substituindo (I) na parte esquerda da igualdade)
$m \cdot b \cdot n \cdot r_2 + n \cdot c \cdot m \cdot r_1 = a$
$m \cdot n \cdot \underbrace{(b \cdot r_2 + c \cdot r_1)}_{\in \mathbb{Z}} = a \Rightarrow m \cdot n \mid a \Rightarrow d \mid a$. ■

Teorema 2.14. *Sejam a, b e $c \in \mathbb{Z}$. Se $a \mid b \cdot c$ e $(a, b) = 1$, então $a \mid c$.*

Demostração: Como $(a, b) = 1$ pelo Teorema 2.12 existem inteiros n e m tais que $n \cdot a + m \cdot b = 1$. Multiplicando-se os dois lados desta igualdade por c temos: $n \cdot (a \cdot c) + m \cdot (b \cdot c) = c$. Como $a \mid a \cdot c$ e, por hipótese, $a \mid b \cdot c$ então, pela Proposição 2.3, $a \mid c$. ■

Teorema 2.15. *Dados $a, b \in \mathbb{Z}, a \mid b \Leftrightarrow (a, b) = a$*

Demostração: $\Rightarrow$) Se $a \mid b$, então pela Definição 2.1 existe $k \in \mathbb{Z}$ tal que $b = a \cdot k$, donde $(a, b) = (a, a \cdot k) = a \cdot (1, k) = a$, pois $(1, k) = 1$
$\Leftarrow$) Se $(a, b) = a \Rightarrow a \mid a$ e $a \mid b$. ■

2.3 Números Primos

Nesta seção iniciaremos o estudo dos números primos, um dos conceitos mais importantes da Matemática, e apresentamos um método prático para determinar números primos.

Definição 2.16. *Um inteiro $p > 1$ é primo se seus únicos divisores positivos forem 1 e p. Se o inteiro $n > 1$ não é primo dizemos que n é composto, ou seja, n pode ser sempre fatorado num produto $n = b \cdot c$, onde $b, c > 1$ são inteiros.*

Proposição 2.17. *Sejam a, b e $p \in \mathbb{Z}$. Se $p \mid a \cdot b$, p primo, então $p \mid a$ ou $p \mid b$.*

Demonstração: Se $p \nmid a$, então $(a, p) = 1$ o que implica, pelo Teorema 2.14, $p \mid b$. ■

Teorema 2.18 (Teorema Fundamental da Aritmética). *Todo inteiro $n > 1$ pode ser representado de maneira única (a menos da ordem) como um produto de fatores primos.*

Demonstração: Se n é primo não há nada a demonstrar. Suponhamos, pois n composto. Seja $p_1 > 1$ o menor divisor positivo de n. Afirmamos que p_1 é primo. Isto é verdade, pois, caso contrário existiria $p, 1 < p < p_1$ com $p \mid n$, contradizendo a escolha de p_1. Logo, $n = p_1 \cdot n_1$.
Se n_1 for primo a prova está completa. Caso contrário, tomamos p_2 como o menor fator de n_1. Pelo argumento anterior, p_2 é primo e temos que $n = p_1 \cdot p_2 \cdot n_2$.
Repetindo este procedimento, obtemos uma sequencia decrescente de inteiros positivos $n_1, n_2, \ldots, n_r$. Como todos eles são inteiros maiores do que 1, este processo deve terminar. Como os primos na sequencia $p_1, p_2, \ldots, p_k$ não são, necessariamente, distintos, n terá, em geral, a forma:

$$n = p_1^{a_1} p_2^{a_2} \ldots p_k^{a_k}.$$

Para mostrarmos a unicidade usamos indução em n. Para $n = 2$ a afirmação é verdadeira. Assumimos, então, que ela se verifica para todos os inteiros maiores do que 1 e menores que n. Vamos provar que ela também é verdadeira para n. Se n é primo, não há nada a provar. Vamos supor, então, que n seja composto e que tenha duas fatorações, isto é,

$$n = p_1 p_2 \cdots p_s = q_1 q_2 \cdots q_r.$$

Vamos provar que $s = r$ e que cada p_i é igual a algum q_j. Como p_1 divide o produto $q_1 q_2 \cdots q_r$ e portanto pela Proposição 2.12 ele divide pelo menos um de seus fatores q_j. Sendo apenas 1 e q_1 os divisores de q_1 e sendo $p_1 \neq 1$, então $p_1 = q_1$. Cancelando p_1 com q_1 na igualdade inicial, obtemos $p_2 p_3 \cdots p_s = q_2 q_3 \cdots q_r$. Repetindo essa argumentação o quanto for necessário, chegaremos à unicidade conforme o enunciado. É claro que não poderá ocorrer ao fim algo como $1 = q_{s+1} \cdots q_r$, pois isto implicaria $q_r \mid 1$, o que não é possível pois q_r é primo. ■

Lema 2.19 (Euclides). *Todo inteiro $n > 1$ pode ser expresso como o produto de um número finito de primos, não necessariamente distintos.*

Demonstração: Demonstração por indução. Se $n = 2$, nada há a fazer, pois 2 é primo. Suponhamos, que todo inteiro n tal que $2 \leq n < m$ pode ser escrito como o produto de um número finito de primos; provemos que este é também o caso para m: se m for primo, nada há a fazer. Senão, existem inteiros a e b tais que $m = a \cdot b$, com $1 < a, b < m$. Pela hipótese de indução, a e b podem ser escritos como produtos de números finitos de primos, digamos $a = p_1 p_2 \ldots p_k$, $b = q_1 q_2 \ldots q_l$, com $k, l \geq 1$ e $p_1, \cdots, p_k, q_1, \cdots, q_l$ primos. Logo, $m = a \cdot b = p_1 \cdots p_k q_1 \cdots q_l$, também o produto de um número finito de primos. ■

Exemplo 2.20. *O processo prático elementar usado para decompor um número em fatores primos é baseado nos resultados do Teorema 2.18 e Lema 2.19. Por exemplo, para $n = 84$, faz-se:*

84	2
42	2
21	3
7	7
1	

Assim, $84 = 2 \cdot 2 \cdot 3 \cdot 7 = 2^2 \cdot 3 \cdot 7$

Teorema 2.21 (Euclides). *A sequência dos números primos é infinita.*

Demonstração: Suponhamos que a sequência dos primos seja finita. Seja pois, $p_1, p_2, \ldots, p_n$ a lista de todos os primos. Consideremos o número $K = p_1 p_2 \cdots p_n + 1$. É claro que K não divisível por nenhum dos p_i. Mas, pelo Teorema 2.18, ou K é primo ou possui algum fator primo e isto implica a existência de um primo que não pertence à nossa lista. Portanto a sequência dos números primos não pode ser finita. ■

Proposição 2.22 (Eratóstenes). *Se um inteiro $n > 1$ for composto, então n possui um divisor primo p, tal que $p \leq \sqrt{n}$.*

Demonstração: Seja $n = a \cdot b$, com $1 < a \leq b$. Sendo p um divisor primo de a, segue que $p \mid n$ e $p^2 \leq a^2 \leq a \cdot b = n$, de modo que $p \leq \sqrt{n}$. ■

O Crivo de Eratóstenes: Como a multiplicação é a operação mais fácil de executar do que a divisão, Eratóstenes, sábio grego do século III a.C., teve a ideia de organizar os cálculos sob a forma do crivo bem conhecido, que leva seu nome. O crivo serve para determinar todos os números primos e também os fatores primos dos números compostos inferiores a um número n dado arbitrariamente.

Exemplo 2.23. *Vamos ilustrar o processo tomando como exemplo $n = 100$. Opera-se da seguinte maneira: escrevam-se todos os inteiros até 100; riscam-se todos os múltiplos de 2, superiores a 2; em cada nova etapa, são riscados todos os múltiplos do menor inteiro p ainda não riscado e que são maiores do que p. Basta chegar-se ao número p tal que p^2 já ultrapassa 100.*

	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~~

Assim, todos os múltiplos de $2, 3, 4, 5, 7, 8, 9, 10 < \sqrt{1}00$ *são crivados. O número 47 é primo porque não foi crivado. Então, os números primos inferiores ou iguais a 100 são 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89 e 97.*

O processo constitui a base da teoria do crivo, que foi desenvolvida com o objetivo de fornecer estimativas da quantidade de números primos satisfazendo dadas condições.

3 Congruência

Neste capítulo apresentaremos a noção de congruência e algumas propriedades que utilizaremos nas demonstrações de alguns critérios de divisibilidade.

3.1 Congruência

Definição 3.1. *Sejam a, b e m inteiros dados, sendo $m > 1$, dizemos que a é congruente a b, módulo m, denotamos $a \equiv b \pmod{m}$, se $m \mid (a-b)$. Se $m \nmid (a-b)$ dizemos que a é incongruente a b módulo m e denotamos $a \not\equiv b \pmod{m}$.*

Exemplo 3.2. $13 \equiv 5 \pmod{2}$ *pois* $2 \mid (13-5)$. *Como* $5 \nmid 6$ *e* $6 = 17 - 11$ *temos que* $17 \not\equiv 11 \pmod{5}$.

Teorema 3.3. *Se a, b, c, d e m são inteiros tais que $a \equiv b \pmod{m}$ e $c \equiv d \pmod{m}$, então:*

i) $a + c \equiv b + d \pmod{m}$

ii) $a - c \equiv b - d \pmod{m}$

iii) $a \cdot c \equiv b \cdot d \pmod{m}$

Demostração: i) De $a \equiv b \pmod{m}$ e $c \equiv d \pmod{m}$ temos $a - b = k \cdot m$ e $c - d = k_1 \cdot m$. Somando-se membro a membro obtemos $(a + c) - (b + d) = (k + k_1) \cdot m$ e isto implica $a + c \equiv b + d \pmod{m}$. ii) Basta subtrair membro a membro $a - b = k \cdot m$ e $c - d = k_1 \cdot m$ obtendo $(a - b) - (c - d) = (a - c) - (b - d) = (k - k_1) \cdot m$ o que implica $a - c \equiv b - d \pmod{m}$. iii) Multiplicamos ambos os lados de $a - b = k \cdot m$ por c e ambos os lados $c - d = k_1 \cdot m$ por b, obtendo $a \cdot c - b \cdot c = c \cdot k \cdot m$ e $b \cdot c - b \cdot d = b \cdot k_1 \cdot m$. Basta, agora, somarmos membro a membro estas últimas igualdades obtendo $a \cdot c - b \cdot c + b \cdot c - b \cdot d = a \cdot c - b \cdot d = (c \cdot k + b \cdot k_1) \cdot m$ o que implica $a \cdot c \equiv b \cdot d \pmod{m}$. ■

Proposição 3.4. *Se a, b, k e m são inteiros com $k > 0$ e $a \equiv b \pmod{m}$, então $a^k \equiv b^k \pmod{m}$.*

Demonstração: Como
$a^k - b^k = (a-b)\cdot(a^{k-1} + a^{k-2}\cdot b + a^{k-3}\cdot b^2 + \cdots + a\cdot b^{k-2} + b^{k-1})$ e $m \mid a-b$ segue-se então da Definição 2.1 o resultado. ■

Exemplo 3.5. *Vamos calcular o resto da divisão do número* 17^{2002} *por 13.*
Solução *Como* $17 \equiv 4 \pmod{13}$ *e* $16 \equiv 3 \pmod{13}$*, segue da Proposição 3.4 que,*

$$17^{2002} \equiv 4^{2002} = 16^{1001} \equiv 3^{1001}, \text{ módulo 13}$$

Notando, agora, que $3^3 \equiv 1 \pmod{13}$ *e aplicando o Teorema 3.3 e a Proposição 3.4, obtemos:*

$$3^{1001} = 3^2 \cdot 3^{999} = 9\cdot(3^3)^{333} \equiv 9\cdot 1^{333} = 9, \text{ módulo 13}$$

Então, $17^{2002} \equiv 9 \pmod{13}$*, ou seja,* 17^{2002} *deixa resto 9 na divisão por 13.*

3.2 Critérios De Divisibilidade

Nesta subseção demostraremos, utilizando congruência, os critérios de divisibilidade dos números de 2 a 11, além dos números primos do Exemplo do Crivo 2.23. Não demonstraremos os casos de números compostos maiores que 10, pois de posse dos Teoremas 2.13 e 2.18 e o Lema 2.19 eles recairão nos critérios já demonstrados. Apresentaremos também alguns resultados como o Corte a Direita e o Corte a Esquerda de números que facilitarão todo o processo para verificação dos critérios de divisibilidade.

Observação 3.6. *Para os testes de divisibilidade no sistema de numeração de base 10, um número* $n = n_k n_{k-1}\ldots n_1 n_0$ *lido da esquerda para a direita pode ser escrito como a soma* $n = 10^k\cdot n_k + 10^{k-1}\cdot n_{k-1} + \ldots + 10\cdot n_1 + n_0$ *o método para testar a divisibilidade de n por d é o de reduzir essa soma e ver as informações que temos. Para facilitar a notação, vamos escrever* $n = (n_k n_{k-1}\ldots n_1 n_0)_{10}$.

Corte a Direita

Teorema 3.7. *Seja* $d \in \mathbb{Z}$*. Se* $(d, 10) = 1$*, então existe um número* $u \in \mathbb{Z}$ *tal que* $10\cdot u \equiv 1 \pmod{d}$*. Tal número u é chamado o inverso de 10 modulo d e escrevemos* $u \equiv 10^{-1} \pmod{d}$.

Demostração: De $(d, 10) = 1$, segue-se do Teorema 2.12 que existem k e $u \in \mathbb{Z}$ tal que $1 = k \cdot d + u \cdot 10 \Rightarrow \underbrace{(-k)}_{\in \mathbb{Z}} \cdot d = 10 \cdot u - 1 \Rightarrow d \mid 10 \cdot u - 1 \Rightarrow 10 \cdot u \equiv 1 \pmod{d}$. ■

Corolário 3.8. *Se* $u \equiv 10^{-1} \pmod{d}$, *escrevemos* $n = (n_k n_{k-1} \dots n_1 n_0)_{10}$ *e* $n' = (n_k n_{k-1} \dots n_1)_{10} + u \cdot (n_0)$. *Temos que* n *é divisível por* d *se, e somente se,* n' *é divisível por* d.

Demostração: Seja $n = (n_k n_{k-1} \dots n_1 n_0)_{10}$ tal que $d \mid n$. Logo:

$$\begin{aligned} & (n_k n_{k-1} \dots n_1 n_0)_{10} \equiv 0 \pmod{d} \\ \Leftrightarrow \quad & 10 \cdot (n_k n_{k-1} \dots n_1)_{10} + (n_0) \equiv 0 \pmod{d} \\ \Leftrightarrow \quad & 10 \cdot u \cdot (n_k n_{k-1} \dots n_1)_{10} + u \cdot (n_0) \equiv 0 \pmod{d} \\ \Leftrightarrow \quad & (n_k n_{k-1} \dots n_1)_{10} + u \cdot (n_0) \equiv 0 \pmod{d}. \blacksquare \end{aligned}$$

Corolário 3.9. *Se* $v \equiv 100^{-1} \pmod{d}$, *escrevemos* $n = (n_k n_{k-1} \dots n_2 n_1 n_0)_{10}$ *e* $n'' = (n_k n_{k-1} \dots n_2)_{10} + v \cdot (n_1 n_0)$. *Temos que* n *é divisível por* d *se, e somente se,* n'' *é divisível por* d.

Demostração: Seja $n = (n_k n_{k-1} \dots n_2 n_1 n_0)_{10}$ tal que $d \mid n$. Logo:

$$\begin{aligned} & (n_k n_{k-1} \dots n_2 n_1 n_0)_{10} \equiv 0 \pmod{d} \\ \Leftrightarrow \quad & 100 \cdot (n_k n_{k-1} \dots n_2)_{10} + (n_1 n_0) \equiv 0 \pmod{d} \\ \Leftrightarrow \quad & 100 \cdot v \cdot (n_k n_{k-1} \dots n_2)_{10} + v \cdot (n_1 n_0) \equiv 0 \pmod{d} \\ \Leftrightarrow \quad & (n_k n_{k-1} \dots n_2)_{10} + v \cdot (n_1 n_0) \equiv 0 \pmod{d}. \blacksquare \end{aligned}$$

Corte a Esquerda

Teorema 3.10. *Dado* $d \in \mathbb{Z}$, *com* $100 \equiv h \pmod{d}, h \in \mathbb{Z}$, *seja* $n = (n_k n_{k-1} \dots n_0)_{10}$, $n' = n_k \cdot h + (n_{k-1} \dots n_0)_{10}$, *e* $n_k \cdot h$ *somado ao digito* n_{k-2}. *Então* $n \equiv n' \pmod{d}$; *em particular,* n *é divisível por* d *se, e somente se,* n' *é divisível por* d.

Demostração: Seja $n = (n_k n_{k-1} \dots n_0)_{10}$, assumindo $k \geqslant 2$. Se $100 \equiv h \pmod{d}$, teremos:

$$\begin{aligned} n = (n_k n_{k-1} \dots n_0)_{10} &= n_k \cdot 10^k + (n_{k-1} \dots n_0)_{10} \\ &= n_k \cdot 100 \cdot 10^{k-2} + (n_{k-1} \dots n_0)_{10} \\ &\equiv n_k \cdot h \cdot 10^{k-2} + (n_{k-1} \dots n_0)_{10} \pmod{d}. \end{aligned}$$

Donde, $d \mid n \Leftrightarrow d \mid n'$.
O efeito da adição de $n_k \cdot h \cdot 10^{k-2}$ com $(n_{k-1} \ldots n_0)_{10}$ é o mesmo que a adição de $n_k \cdot h$ a $(n_{k-1} \ldots n_0)_{10}$. ■

Critério de divisibilidade por 2. Um número inteiro n é divisível por 2 se, e somente se, n termina em 0, 2, 4, 6, 8.
Demonstração: Como $10 \equiv 0 \pmod 2$, segue-se do Teorema 3.3 item iii) e Proposição 3.4 que $n_i \cdot 10^i \equiv 0 \pmod 2$. Portanto, dado um número $n = (n_r n_{r-1} \cdots n_0)_{10} = 10^r \cdot n_r + 10^{r-1} \cdot n_{r-1} + \ldots + 10^1 \cdot n_1 + n_0$, temos que: $n \equiv n_0 \pmod 2$. ■

Critérios de divisibilidade por 3.
1°) **Critério:** Um número n é divisível por 3 se, e somente se, a soma dos algarismos de n é divisível por 3.
Demonstração: Como $10 \equiv 1 \pmod 3$, pelo Teorema 3.3 e Proposição 3.4 segue $n_i \cdot 10^i \equiv n_i \pmod 3$. Isto mostra que, se $n = (n_r n_{r-1} \cdots n_0)_{10} = 10^r \cdot n_r + 10^{r-1} \cdot n_{r-1} + \ldots + 10^1 \cdot n_1 + n_0$, então:

$$n \equiv n_r + n_{r-1} + \ldots + n_1 + n_0 \pmod 3. \blacksquare$$

2°) **Critério:** Dado um número n, quando adicionamos o primeiro algarismo n_k de n ao resultado do número inicial a partir da posição n_{k-2} pela supressão do primeiro algarismo n_k, se o resultado for múltiplo de 3, o número original será múltiplo de 3. Se o número obtido ainda for grande, repete-se o processo até que se possa verificar a divisão por 3.
Demonstração: Seja $n = (n_k n_{k-1} n_{k-2} \cdots n_0)_{10}$, como $100 \equiv 1 \pmod 3$, segue-se do Teorema 3.10 que:

$$\begin{aligned} n = (n_k n_{k-1} \ldots n_0)_{10} &= n_k \cdot 10^k + (n_{k-1} \ldots n_0)_{10} \\ &\equiv n_k \cdot 1 \cdot 10^{k-2} + (n_{k-1} \ldots n_0)_{10} \pmod 3, k \geq 2. \blacksquare \end{aligned}$$

Critério de divisibilidade por 4. Um número n é divisível por 4 se, e somente se, os dois últimos algarismos de n formarem um número divisível por 4.
Demonstração: Como $10 \equiv 2 \pmod 4$ e pela Proposição 3.4, teremos $10^2 \equiv 2^2 = 4 = 0 \pmod 4$, segue do Teorema 3.3 que $n_i \cdot 10^i \equiv 0 \pmod 4$, para $i \geqslant 2$. Isto mostra que, se

$n = (n_r n_{r-1} \cdots n_0)_{10} = 10^r \cdot n_r + 10^{r-1} \cdot n_{r-1} + \ldots + 10^2 \cdot n_2 + 10^1 \cdot n_1 + n_0$, então:

$$\begin{aligned} n &\equiv 10^i \cdot n_i + 10 \cdot n_1 + n_0 \pmod 4 \\ n &\equiv 10 \cdot n_1 + n_0 \pmod 4 \\ n &\equiv (n_1 n_0)_{10} \pmod 4. \blacksquare \end{aligned}$$

Critério de divisibilidade por 5. Um número n é divisível por 5 se, e somente se, o último algarismo de n é 0 ou 5.
Demonstração: Como $10 \equiv 0 \pmod 5$, pelo Teorema 3.3 e Proposição 3.4 segue $n_i \cdot 10^i \equiv 0 \pmod 5$. Isto mostra que, se
$n = (n_r n_{r-1} \cdots n_0)_{10} = 10^r \cdot n_r + 10^{r-1} \cdot n_{r-1} + \ldots + 10^1 \cdot n_1 + n_0$, então:

$$n \equiv n_0 \pmod 5. \blacksquare$$

Critério de divisibilidade por 6. Um número n é divisível por 6 se, e somente se, n é divisível por 2 e 3.
Demonstração: Como podemos decompor $6 = 2 \cdot 3$ e $(2, 3) = 1$, segue do Teorema 2.13 que $2 \mid n$ e $3 \mid n$. $\blacksquare$

Critérios de divisibilidade por 7.
1°) **Critério:** Dado um número n, quando multiplicamos o último algarismo de n por 2 e subtraímos o resultado do número obtido do número inicial pela supressão do último algarismo, se o resultado for múltiplo de 7, o número original será múltiplo de 7. Se o número obtido ainda for grande, repete-se o processo até que se possa verificar a divisão por 7. (Obs: segundo [12] esse critério já era conhecido pelos Babilônicos.)
Demonstração: Como $(7, 10) = 1$, segue-se pelo Teorema 3.7 que existe $u \in \mathbb{Z}$, onde $u = -2$, tal que $10 \cdot (-2) \equiv 1 \pmod 7 \Rightarrow -20 \equiv 1 \pmod 7 \Rightarrow 7 \mid -20 - 1 = -21$.
Portanto, sendo $n = (n_r n_{r-1} \cdots n_0)_{10}$, segue-se, então do Corolário 3.8 que;
$(n_k n_{k-1} \ldots n_1)_{10} - 2 \cdot (n_0) \equiv 0 \pmod 7$. $\blacksquare$

2°) **Critério:** Dado um número n, quando multiplicamos o primeiro algarismo n_k de n por 2 e adicionamos ao resultado do número inicial a partir da posição n_{k-2} pela supressão do primeiro algarismo n_k, se o resultado for múltiplo de 7, o número original será múltiplo de 7. Se o número obtido ainda for grande, repete-se o processo até que se possa verificar a divisão por 7.

Demonstração: Seja $n = (n_k n_{k-1} n_{k-2} \cdots n_0)_{10}$, como $100 \equiv 2 \pmod 7$, segue-se do Teorema 3.10 que:

$$\begin{aligned} n = (n_k n_{k-1} \ldots n_0)_{10} &= n_k \cdot 10^k + (n_{k-1} \ldots n_0)_{10} \\ &\equiv n_k \cdot 2 \cdot 10^{k-2} + (n_{k-1} \ldots n_0)_{10} \pmod 7, k \geq 2. \blacksquare \end{aligned}$$

Exemplo 3.11. *Verificar se o número 248738 é divisível por 7:*
Pelo 1°) *critério de divisibilidade de 7, teremos:*

$$\begin{array}{r} 248738 \\ -\quad 16 \\ \hline 24857 \\ -\quad 14 \\ \hline 2471 \\ -\quad 2 \\ \hline 245 \\ -\quad 10 \\ \hline 14 \end{array}$$

Donde, temos que 14 é múltiplo de 7, ou seja, 248738 é divisível por 7. ■
Verificando pelo 2°) *critério de divisíbilidade de 7, temos:*

$$
\begin{array}{rr}
 & \not{2}48738 \\
+ & 4 \\
\hline
 & \not{5}2738 \\
+ & 10 \\
\hline
 & \not{3}738 \\
+ & 6 \\
\hline
 & \not{7}98 \\
+ & 14 \\
\hline
 & \not{1}12 \\
+ & 2 \\
\hline
 & 14
\end{array}
$$

Donde, vemos claramente que $2487738 \equiv 0 \pmod 7$. ■

Critérios de divisibilidade por 8.

1°) **Critério:** Um número n é divisível por 8 se, e somente se, os três últimos algarismos de n formarem um número divisível por 8.

Demonstração: Como $10 \equiv 2 \pmod 8$ e pela Proposição 3.4, teremos $10^3 \equiv 2^3 = 8 = 0 \pmod 8$, segue do Teorema 3.3 que $n_i \cdot 10^i \equiv 0 \pmod 8$, para $i \geq 3$. Isto mostra que, se

$n = (n_r n_{r-1} \cdots n_0)_{10} = 10^r \cdot n_r + 10^{r-1} \cdot n_{r-1} + \ldots + 10^3 \cdot n_3 + 10^2 \cdot n_2 + 10^1 \cdot n_1 + n_0$, então:

$$n \equiv 10^i \cdot n_i + 10^2 \cdot n_2 + 10 \cdot n_1 + n_0 \pmod 8$$
$$n \equiv (n_2 n_1 n_0)_{10} \pmod 8. \blacksquare$$

2°) **Critério:** Dado um número n, quando multiplicamos o primeiro algarismo n_k de n por 4 e adicionamos ao resultado do número inicial a partir da posição n_{k-2} pela supressão do primeiro algarismo n_k, se o resultado for múltiplo de 8, o número original será múltiplo de 8. Se o número obtido ainda for grande, repete-se o processo até que se possa verificar a divisão por 8.

Demonstração: Seja $n = (n_k n_{k-1} n_{k-2} \cdots n_0)_{10}$, como $100 \equiv 4 \pmod 8$, segue-se do Teorema 3.10 que:

$$\begin{aligned} n = (n_k n_{k-1} \ldots n_0)_{10} &= n_k \cdot 10^k + (n_{k-1} \ldots n_0)_{10} \\ &\equiv n_k \cdot 4 \cdot 10^{k-2} + (n_{k-1} \ldots n_0)_{10} \pmod 8, k \geq 2. \blacksquare \end{aligned}$$

Critérios de divisibilidade por 9.

1°) **Critério:** Um número n é divisível por 9 se, e somente se, a soma dos algarismos de n é divisível por 9.

Demonstração: Como $10 \equiv 1 \pmod 9$ e pelo Teorema 3.3 e Proposição 3.4 segue-se $n_i \cdot 10^i \equiv n_i \pmod 9$. Isto mostra que, se
$n = (n_r n_{r-1} \cdots n_0)_{10} = 10^r \cdot n_r + 10^{r-1} \cdot n_{r-1} + \ldots + 10^1 \cdot n_1 + n_0$, então:

$$n \equiv n_r + n_{r-1} + \ldots + n_1 + n_0 \pmod 9. \blacksquare$$

2°) **Critério:** Dado um número n, quando adicionamos o primeiro algarismo n_k de n ao resultado do número inicial a partir da posição n_{k-2} pela supressão do primeiro algarismo n_k, se o resultado for múltiplo de 9, o número original será múltiplo de 9. Se o número obtido ainda for grande, repete-se o processo até que se possa verificar a divisão por 9.

Demonstração: Seja $n = (n_k n_{k-1} n_{k-2} \cdots n_0)_{10}$, como $100 \equiv 1 \pmod 9$, segue-se do Teorema 3.10 que:

$$\begin{aligned} n = (n_k n_{k-1} \ldots n_0)_{10} &= n_k \cdot 10^k + (n_{k-1} \ldots n_0)_{10} \\ &\equiv n_k \cdot 1 \cdot 10^{k-2} + (n_{k-1} \ldots n_0)_{10} \pmod 9, k \geq 2. \blacksquare \end{aligned}$$

Exemplo 3.12. *Vamos verificar se o número 174321 é divisível por 9:*
Pelo 1°) *critério de divisibilidade de 9, teremos:* $1+7+4+3+2+1 = 18$ *que é múltiplo de 9. Logo, o número 174321 é divisível por 9.* ■
Verificando pelo 2°) *critério de divisibilidade de 9, temos:*

$$
\begin{array}{rr}
 & \not{1}74321 \\
+ & 1 \\
\hline
 & \not{7}5321 \\
+ & 7 \\
\hline
 & \not{6}021 \\
+ & 6 \\
\hline
 & \not{8}1 \\
+ & 8 \\
\hline
 & 9
\end{array}
$$

Donde, vemos claramente que $174321 \equiv 0 \pmod 9$. ■

Critério de divisibilidade por 10. Um número n é divisível por 10 se, e somente se, o último algarismo de n termina em 0.
Demonstração: Como $10 \equiv 0 \pmod{10}$ e pelo Teorema 3.3 e Proposição 3.4 segue-se $n_i \cdot 10^i \equiv 0 \pmod{10}$. Isto mostra que, se
$n = (n_r n_{r-1} \cdots n_0)_{10} = 10^r \cdot n_r + 10^{r-1} \cdot n_{r-1} + \ldots + 10^1 \cdot n_1 + n_0$, então:

$$n \equiv n_0 \pmod{10}. \blacksquare$$

Critérios de divisibilidade por 11.
1°) **Critério:** Dado um número inteiro n, sejam P e I as somas dos algarismos de ordem par e ímpar de n, respectivamente. Se $P - I$ é múltiplo de 11, então n é múltiplo de 11.
Demonstração: Como $10 \equiv -1 \pmod{11}$ e pelo Teorema 3.3 e Proposição 3.4 segue-se $10^i \equiv -1 \pmod{11}$ se i é impar e $10^i \equiv 1 \pmod{11}$ se i é par. Isto mostra que, se $n = (n_r n_{r-1} \cdots n_0)_{10} = 10^r \cdot n_r + 10^{r-1} \cdot n_{r-1} + \ldots + 10^1 \cdot n_1 + n_0$, então:

$$
\begin{aligned}
n_0 &\equiv n_0 \pmod{11} \\
10 \cdot n_1 &\equiv -n_1 \pmod{11} \\
10^2 \cdot n_2 &\equiv n_2 \pmod{11} \\
&\vdots \\
10^r \cdot a_r &\equiv (-1)^r \cdot a_r \pmod{11}
\end{aligned}
$$

Logo:
$n = 10^r \cdot n_r + 10^{r-1} \cdot n_{r-1} + \ldots + 10^1 \cdot n_1 + n_0 \equiv n_0 - n_1 + n_2 - \ldots + (-1)^r \pmod{11}$ ■

2°) **Critério:** Dado um número n, quando subtraímos o último algarismo de n ao resultado do número obtido do número inicial pela supressão do último algarismo, se o resultado for múltiplo de 11, o número original será múltiplo de 11. Se o número obtido ainda for grande, repete-se o processo até que se possa verificar a divisão por 11.

Demonstração: Como $(11, 10) = 1$, segue-se do Teorema 3.7 que existe $u \in \mathbb{Z}$, onde $u = -1$, tal que $10 \cdot (-1) \equiv 1 \pmod{11} \Rightarrow -10 \equiv 1 \pmod{11} \Rightarrow 11 \mid -10 - 1 = -11$. Portanto, sendo $n = (n_r n_{r-1} \cdots n_0)_{10}$, segue-se do Corolário 3.8 que;
$(n_k n_{k-1} \ldots n_1)_{10} - 1 \cdot (n_0) \equiv 0 \pmod{11}$. ■

3°) **Critério:** Dado um número n, quando adicionamos o primeiro algarismo n_k de n ao resultado do número inicial a partir da posição n_{k-2} pela supressão do primeiro algarismo n_k, se o resultado for múltiplo de 11, o número original será múltiplo de 11. Se o número obtido ainda for grande, repete-se o processo até que se possa verificar a divisão por 11.

Demonstração: Seja $n = (n_k n_{k-1} n_{k-2} \cdots n_0)_{10}$, como $100 \equiv 1 \pmod{11}$, segue-se do Teorema 3.10 que:

$$\begin{aligned} n = (n_k n_{k-1} \ldots n_0)_{10} &= n_k \cdot 10^k + (n_{k-1} \ldots n_0)_{10} \\ &\equiv n_k \cdot 1 \cdot 10^{k-2} + (n_{k-1} \ldots n_0)_{10} \pmod{11}, k \geq 2. \blacksquare \end{aligned}$$

Exemplo 3.13. *Verificar se o número 4520835 é divisível por 11:*
Pelo 1°) *critério de divisibilidade de 11, teremos:* $5 - 3 + 8 - 0 + 2 - 5 + 4 = 11$ *que é múltiplo de 11. Logo, o número 4520835 é divisível por 11.* ■
Verificando pelo 2°) *critério de divisibilidade de 11, temos:*

$$
\begin{array}{rr}
 & 4520835 \\
- & \quad 5 \\
\hline
 & 452078 \\
- & \quad 8 \\
\hline
 & 45199 \\
- & \quad 9 \\
\hline
 & 4510 \\
- & \quad 0 \\
\hline
 & 451 \\
- & \quad 1 \\
\hline
 & 44 \\
- & \quad 4 \\
\hline
 & \quad 0
\end{array}
$$

Donde, vemos que 0 é múltiplo de 11,ou seja, 4520835 é divisível por 11. ■

Pelo $3°$*) critério de divisibilidade de 11, temos:*

$$
\begin{array}{rr}
 & \not{4}520835 \\
+ & 4 \\
\hline
 & \not{5}60835 \\
+ & 5 \\
\hline
 & \not{6}5835 \\
+ & 6 \\
\hline
 & \not{6}435 \\
+ & 6 \\
\hline
 & \not{4}95 \\
+ & 4 \\
\hline
 & 99
\end{array}
$$

Donde, vemos 99 é múltiplo de 11, ou seja, $4520835 \equiv 0 \pmod{11}$.■

Critérios de divisibilidade por 13.

1°) **Critério:** Dado um número n, quando multiplicamos o último algarismo de n por 4 e somamos ao resultado do número obtido do número inicial pela supressão do último algarismo, se o resultado for múltiplo de 13, o número original será múltiplo de 13. Se o número obtido ainda for grande, repete-se o processo até que se possa verificar a divisão por 13.

Demonstração: Como $(13, 10) = 1$, segue-se do Teorema 3.7 que existe $u \in \mathbb{Z}$, onde $u = 4$, tal que $10 \cdot 4 \equiv 1 \pmod{13} \Rightarrow 40 \equiv 1 \pmod{13} \Rightarrow 13 \mid 40 - 1 = 39$. Portanto, sendo $n = (n_r n_{r-1} \cdots n_0)_{10}$, segue-se do Corolário 3.8 que;
$(n_k n_{k-1} \ldots n_1)_{10} + 4 \cdot (n_0) \equiv 0 \pmod{13}$. ■

2°) **Critério:** Dado um número n, quando multiplicamos o primeiro algarismo n_k de n por 4 e subtraímos o resultado do número inicial a partir da posição n_{k-2} pela supressão do primeiro algarismo n_k, se o resultado for múltiplo de 13, o número original será múltiplo de 13. Se o número obtido ainda for grande, repete-se o processo até que se possa verificar a divisão por 13.

Demonstração: Seja $n = (n_k n_{k-1} n_{k-2} \cdots n_0)_{10}$, como $100 \equiv (-4) \pmod{13}$, segue-se do Teorema 3.10 que:

$$\begin{aligned} n = (n_k n_{k-1} \ldots n_0)_{10} &= n_k \cdot 10^k + (n_{k-1} \ldots n_0)_{10} \\ &\equiv n_k \cdot (-4) \cdot 10^{k-2} + (n_{k-1} \ldots n_0)_{10} \pmod{13}, k \geq 2. \blacksquare \end{aligned}$$

Exemplo 3.14. *Verificar se o número 221 é divisível por 13:*
Pelo 1°) *critério de divisibilidade de 13, teremos:*

$$\begin{array}{r} 22\not{1} \\ +\quad 4 \\ \hline 26 \end{array}$$

Donde, temos que 26 é múltiplo de 13, ou seja, $221 \equiv 0 \pmod{13}$. ■
Verificando pelo 2°) *critério de divisíbilidade de 13, temos:*

$$\begin{array}{r} \not{2}21 \\ -\quad 8 \\ \hline 13 \end{array}$$

Donde, vemos claramente que $13 \equiv 0 \pmod{13}$. ■

Exemplo 3.15. *Verificar se o número 283757 é divisível por 13:*
Pelo 1°) *critério de divisibilidade de 13, teremos:*

$$
\begin{array}{rr}
 & 283757 \\
+ & 28 \\
\hline
 & 28403 \\
+ & 12 \\
\hline
 & 2852 \\
+ & 8 \\
\hline
 & 293 \\
- & 12 \\
\hline
 & 41
\end{array}
$$

Donde, vemos que 41 não é divisível por 13, pois $41 = 13 \cdot 3 + 2$*, mas* $283757 \not\equiv 2 \pmod{13}$*; portanto, 283757 não é divisível por 13.* ■

Pelo 2°) *critério de divisibilidade de 13, temos:*

$$
\begin{array}{rr}
 & 283757 \\
- & 8 \\
\hline
 & 75757 \\
- & 28 \\
\hline
 & 2957 \\
- & 8 \\
\hline
 & 877 \\
- & 32 \\
\hline
 & 45
\end{array}
$$

Donde, vemos que 45 não é divisível por 13, pois $45 = 13 \cdot 3 + 6$*, ou seja,* $283757 \equiv 6 \pmod{13}$*; portanto 283757 não é divisível por 13, mas deixa resto 6 na divisão.*■

Observação 3.16. *A escolha do critério dependerá da capacidade de interpretação e da utilização que cada um propõe a fazer. Como visto no exemplo anterior, o critério de divisibilidade do corte a esquerda nos fornece o resto, se um dado número não é divisível por um outro.*

Critérios de divisibilidade por 17.

1°) **Critério:** Dado um número n, quando multiplicamos o último algarismo de n por 5 e subtraímos o resultado do número obtido do número inicial pela supressão do último algarismo, se o resultado for múltiplo de 17, o número original será múltiplo de 17. Se o número obtido ainda for grande, repete-se o processo até que se possa verificar a divisão por 17.

Demonstração: Como $(17, 10) = 1$, segue-se do Teorema 3.7 que existe $u \in \mathbb{Z}$, onde $u = -5$, tal que $10 \cdot (-5) \equiv 1 \pmod{17} \Rightarrow -50 \equiv 1 \pmod{17} \Rightarrow 17 \mid -50 - 1 = -51$. Portanto, sendo $n = (n_r n_{r-1} \cdots n_0)_{10}$, segue-se do Corolário 3.8 que;
$(n_k n_{k-1} \ldots n_1)_{10} - 5 \cdot (n_0) \equiv 0 \pmod{17}$. ■

2°) **Critério:** Dado um número n, quando multiplicamos o primeiro algarismo n_k de n por 2 e subtraímos o resultado do número inicial a partir da posição n_{k-2} pela supressão do primeiro algarismo n_k, se o resultado for múltiplo de 17, o número original será múltiplo de 17. Se o número obtido ainda for grande, repete-se o processo até que se possa verificar a divisão por 17.

Demonstração: Seja $n = (n_k n_{k-1} n_{k-2} \cdots n_0)_{10}$, como $100 \equiv (-2) \pmod{17}$, segue-se do Teorema 3.10 que:

$$\begin{aligned} n = (n_k n_{k-1} \ldots n_0)_{10} &= n_k \cdot 10^k + (n_{k-1} \ldots n_0)_{10} \\ &\equiv n_k \cdot (-2) \cdot 10^{k-2} + (n_{k-1} \ldots n_0)_{10} \pmod{17}, k \geq 2. \blacksquare \end{aligned}$$

Exemplo 3.17. *Verificar se o número 25428 é divisível por 17:*
Pelo 1°) *critério de divisibilidade de 17, teremos:*

$$
\begin{array}{rr}
 & 25428\not{8} \\
- & 40 \\
\hline
 & 2502\not{2} \\
- & 10 \\
\hline
 & 240\not{0} \\
- & 0 \\
\hline
 & 24
\end{array}
$$

Donde, vemos que 24 não é divisível por 17, pois $24 = 17 \cdot 1 + 7$*, mas* $25428 \not\equiv 7 \pmod{17}$*; portanto, 25428 não é divisível por 17.* ■
Pelo 2°) *critério de divisibilidade de 17, temos:*

$$
\begin{array}{rr}
 & \not{2}5428 \\
- & 4 \\
\hline
 & \not{5}028 \\
- & 10 \\
\hline
- & 72
\end{array}
$$

Donde, vemos que -72 não é divisível por 17, pois $-72 = 17 \cdot (-5) + 13$*, ou seja,* $25428 \equiv 13 \pmod{17}$*; portanto 25428 não é divisível por 17, mas deixa resto 13 na divisão.*■

Critério de divisibilidade por 19.

1°) **Critério:** Dado um número n, quando multiplicamos o último algarismo de n por 2 e somamos ao resultado do número obtido do número inicial pela supressão do último algarismo, se o resultado for múltiplo de 19, o número original será múltiplo de 19. Se o número obtido ainda for grande, repete-se o processo até que se possa verificar a divisão por 19.

Demonstração: Como $(19, 10) = 1$, segue-se do Teorema 3.7 que existe $u \in \mathbb{Z}$, onde $u = 2$, tal que $10 \cdot 2 \equiv 1 \pmod{7} \Rightarrow 20 \equiv 1 \pmod{19} \Rightarrow 19 \mid 20 - 1 = 19$. Portanto,

sendo $n = (n_r n_{r-1} \cdots n_0)_{10}$, segue-se do Corolário 3.8 que;
$(n_k n_{k-1} \ldots n_1)_{10} + 2 \cdot (n_0) \equiv 0 \pmod{19}$. ■

2°) **Critério:** Dado um número n, quando multiplicamos o primeiro algarismo n_k de n por 5 e adicionamos ao resultado do número inicial a partir da posição n_{k-2} pela supressão do primeiro algarismo n_k, se o resultado for múltiplo de 19, o número original será múltiplo de 19. Se o número obtido ainda for grande, repete-se o processo até que se possa verificar a divisão por 19.

Demonstração: Seja $n = (n_k n_{k-1} n_{k-2} \cdots n_0)_{10}$, como $100 \equiv 5 \pmod{19}$, segue-se do Teorema 3.10 que:

$$\begin{aligned} n = (n_k n_{k-1} \ldots n_0)_{10} &= n_k \cdot 10^k + (n_{k-1} \ldots n_0)_{10} \\ &\equiv n_k \cdot 5 \cdot 10^{k-2} + (n_{k-1} \ldots n_0)_{10} \pmod{19}, k \geq 2. \blacksquare \end{aligned}$$

Critério de divisibilidade por 23. Dado um número n, quando multiplicamos o último algarismo de n por 7 e somamos ao resultado do número obtido do número inicial pela supressão do último algarismo, se o resultado for múltiplo de 23, o número original será múltiplo de 23. Se o número obtido ainda for grande, repete-se o processo até que se possa verificar a divisão por 23.

Demonstração: Como $(23, 10) = 1$, segue-se do Teorema 3.7 que existe $u \in \mathbb{Z}$, onde $u = 7$, tal que $10 \cdot 7 \equiv 1 \pmod{23} \Rightarrow 70 \equiv 1 \pmod{23} \Rightarrow 23 \mid 70 - 1 = 69$. Portanto, sendo $n = (n_r n_{r-1} \cdots n_0)_{10}$, segue-se do Corolário 3.8 que;
$(n_k n_{k-1} \ldots n_1)_{10} + 7 \cdot (n_0) \equiv 0 \pmod{23}$. ■

Critério de divisibilidade por 29. Dado um número n, quando multiplicamos o último algarismo de n por 3 e somamos ao resultado do número obtido do número inicial pela supressão do último algarismo, se o resultado for múltiplo de 29, o número original será múltiplo de 29. Se o número obtido ainda for grande, repete-se o processo até que se possa verificar a divisão por 29.

Demonstração: Como $(29, 10) = 1$, segue-se do Teorema 3.7 que existe $u \in \mathbb{Z}$, onde $u = 3$, tal que $10 \cdot 3 \equiv 1 \pmod{29} \Rightarrow 30 \equiv 1 \pmod{29} \Rightarrow 29 \mid 30 - 1 = 29$. Portanto, sendo $n = (n_r n_{r-1} \cdots n_0)_{10}$, segue-se do Corolário 3.8 que;
$(n_k n_{k-1} \ldots n_1)_{10} + 3 \cdot (n_0) \equiv 0 \pmod{29}$. ■

Critério de divisibilidade por 31. Dado um número n, quando multiplicamos o último algarismo de n por 3 e subtraíndo o resultado do número obtido do número inicial pela supressão do último algarismo, se o resultado for múltiplo de 31, o número

original será múltiplo de 31. Se o número obtido ainda for grande, repete-se o processo até que se possa verificar a divisão por 31.
Demonstração: Como $(31, 10) = 1$, segue-se do Teorema 3.7 que existe $u \in \mathbb{Z}$, onde $u = -3$, tal que $10 \cdot (-3) \equiv 1 \pmod{31} \Rightarrow -30 \equiv 1 \pmod{31} \Rightarrow 31 \mid -30 - 1 = -31$. Portanto, sendo $n = (n_r n_{r-1} \cdots n_0)_{10}$, segue-se do Corolário 3.8 que;
$(n_k n_{k-1} \ldots n_1)_{10} - 3 \cdot (n_0) \equiv 0 \pmod{31}$. ■

Critério de divisibilidade por 37. Dado um número n, quando multiplicamos o último algarismo de n por 26 e somamos ao resultado do número obtido do número inicial pela supressão do último algarismo, se o resultado for múltiplo de 37, o número original será múltiplo de 37. Se o número obtido ainda for grande, repete-se o processo até que se possa verificar a divisão por 37.
Demonstração: Como $(37, 10) = 1$, segue-se do Teorema 3.7 que existe $u \in \mathbb{Z}$, onde $u = 26$, tal que $10 \cdot 26 \equiv 1 \pmod{37} \Rightarrow 260 \equiv 1 \pmod{37} \Rightarrow 37 \mid 260 - 1 = 259$. Portanto, sendo $n = (n_r n_{r-1} \cdots n_0)_{10}$, segue-se do Corolário 3.8 que;
$(n_k n_{k-1} \ldots n_1)_{10} + 26 \cdot (n_0) \equiv 0 \pmod{37}$. ■

Critério de divisibilidade por 41. Dado um número n, quando multiplicamos o último algarismo de n por 4 e subtraímos o resultado do número obtido do número inicial pela supressão do último algarismo, se o resultado for múltiplo de 41, o número original será múltiplo de 41. Se o número obtido ainda for grande, repete-se o processo até que se possa verificar a divisão por 41.
Demonstração: Como $(41, 10) = 1$, segue-se do Teorema 3.7 que existe $u \in \mathbb{Z}$, onde $u = -4$, tal que $10 \cdot (-4) \equiv 1 \pmod{41} \Rightarrow -40 \equiv 1 \pmod{41} \Rightarrow 41 \mid -40 - 1 = -41$. Portanto, sendo $n = (n_r n_{r-1} \cdots n_0)_{10}$, segue-se do Corolário 3.8 que;
$(n_k n_{k-1} \ldots n_1)_{10} - 4 \cdot (n_0) \equiv 0 \pmod{41}$. ■

Critério de divisibilidade por 43. Dado um número n, quando multiplicamos o último algarismo de n por 13 e somamos ao resultado do número obtido do número inicial pela supressão do último algarismo, se o resultado for múltiplo de 43, o número original será múltiplo de 43. Se o número obtido ainda for grande, repete-se o processo até que se possa verificar a divisão por 43.
Demonstração: Como $(43, 10) = 1$, segue-se do Teorema 3.7 que existe $u \in \mathbb{Z}$, onde $u = 13$, tal que $10 \cdot 13 \equiv 1 \pmod{43} \Rightarrow 130 \equiv 1 \pmod{43} \Rightarrow 43 \mid 130 - 1 = 129$. Portanto, sendo $n = (n_r n_{r-1} \cdots n_0)_{10}$, segue-se do Corolário 3.8 que;
$(n_k n_{k-1} \ldots n_1)_{10} + 13 \cdot (n_0) \equiv 0 \pmod{43}$. ■

Critério de divisibilidade por 47. Dado um número n, quando multiplicamos o primeiro algarismo n_k de n por 6 e adicionamos ao resultado do número inicial a partir da posição n_{k-2} pela supressão do primeiro algarismo n_k, se o resultado for múltiplo de 47, o número original será múltiplo de 47. Se o número obtido ainda for grande, repete-se o processo até que se possa verificar a divisão por 47.
Demonstração: Seja $n = (n_k n_{k-1} n_{k-2} \cdots n_0)_{10}$, como $100 \equiv 6 \pmod{47}$, segue-se do Teorema 3.10 que:

$$\begin{aligned} n = (n_k n_{k-1} \ldots n_0)_{10} &= n_k \cdot 10^k + (n_{k-1} \ldots n_0)_{10} \\ &\equiv n_k \cdot 6 \cdot 10^{k-2} + (n_{k-1} \ldots n_0)_{10} \pmod{47}, k \geq 2. \blacksquare \end{aligned}$$

Critérios de divisibilidade por 53.
1°) **Critério:** Dado um número n, quando multiplicamos os dois último algarismo de n por 9 e subtraímos o resultado do número obtido do número inicial pela supressão dos dois último algarismo, se o resultado for múltiplo de 53, o número original será múltiplo de 53. Se o número obtido ainda for grande, repete-se o processo até que se possa verificar a divisão por 53.
Demonstração: Como $(53, 10) = 1$, segue-se pelo Teorema 3.7 que existe $v \in \mathbb{Z}$, onde $v = -9$, tal que $100 \cdot (-9) \equiv 1 \pmod{53} \Rightarrow -900 \equiv 1 \pmod{53} \Rightarrow 53 \mid -900 - 1 = -900$. Portanto, sendo $n = (n_r n_{r-1} \cdots n_2 n_1 n_0)_{10}$, segue-se, então do Corolário 3.9 que; $(n_k n_{k-1} \ldots n_2)_{10} - 9 \cdot (n_1 n_0) \equiv 0 \pmod{53}$. $\blacksquare$

2°) **Critério:** Dado um número n, quando multiplicamos o primeiro algarismo n_k de n por 6 e subtraímos o resultado do número inicial a partir da posição n_{k-2} pela supressão do primeiro algarismo n_k, se o resultado for múltiplo de 53, o número original será múltiplo de 53. Se o número obtido ainda for grande, repete-se o processo até que se possa verificar a divisão por 53.
Demonstração: Seja $n = (n_k n_{k-1} n_{k-2} \cdots n_0)_{10}$, como $100 \equiv (-6) \pmod{53}$, segue-se do Teorema 3.10 que:

$$\begin{aligned} n = (n_k n_{k-1} \ldots n_0)_{10} &= n_k \cdot 10^k + (n_{k-1} \ldots n_0)_{10} \\ &\equiv n_k \cdot (-6) \cdot 10^{k-2} + (n_{k-1} \ldots n_0)_{10} \pmod{53}, k \geq 2. \blacksquare \end{aligned}$$

Critério de divisibilidade por 59. Dado um número, n quando multiplicamos o último algarismo de n por 6 e somamos ao resultado do número obtido do número inicial pela supressão do último algarismo, se o resultado for múltiplo de 59, o número

original será múltiplo de 59. Se o número obtido ainda for grande, repete-se o processo até que se possa verificar a divisão por 59.
Demonstração: Como $(59, 10) = 1$, segue-se do Teorema 3.7 que existe $u \in \mathbb{Z}$, onde $u = 6$, tal que $10 \cdot 6 \equiv 1 \pmod{59} \Rightarrow 60 \equiv 1 \pmod{59} \Rightarrow 59 \mid 60 - 1 = 59$. Portanto, sendo $n = (n_r n_{r-1} \cdots n_0)_{10}$, segue-se do Corolário 3.8 que;
$(n_k n_{k-1} \ldots n_1)_{10} + 6 \cdot (n_0) \equiv 0 \pmod{59}$. ■

Critério de divisibilidade por 61. Dado um número n, quando multiplicamos o último algarismo de n por 6 e subtraímos o resultado do número obtido do número inicial pela supressão do último algarismo, se o resultado for múltiplo de 61, o número original será múltiplo de 61. Se o número obtido ainda for grande, repete-se o processo até que se possa verificar a divisão por 61.
Demonstração: Como $(61, 10) = 1$, segue-se do Teorema 3.7 que existe $u \in \mathbb{Z}$, onde $u = -6$, tal que $10 \cdot (-6) \equiv 1 \pmod{61} \Rightarrow -60 \equiv 1 \pmod{61} \Rightarrow 61 \mid -60 - 1 = -61$. Portanto, sendo $n = (n_r n_{r-1} \cdots n_0)_{10}$, segue-se do Corolário 3.8 que;
$(n_k n_{k-1} \ldots n_1)_{10} - 6 \cdot (n_0) \equiv 0 \pmod{61}$. ■

Critério de divisibilidade por 67. Dado um número n, quando multiplicamos o último algarismo de n por 20 e subtraímos o resultado do número obtido do número inicial pela supressão do último algarismo, se o resultado for múltiplo de 67, o número original será múltiplo de 67. Se o número obtido ainda for grande, repete-se o processo até que se possa verificar a divisão por 67.
Demonstração: Como $(67, 10) = 1$, segue-se do Teorema 3.7 que existe $u \in \mathbb{Z}$, onde $u = -20$, tal que $10 \cdot (-20) \equiv 1 \pmod{67} \Rightarrow -200 \equiv 1 \pmod{67} \Rightarrow 67 \mid -200 - 1 = -201$. Portanto, sendo $n = (n_r n_{r-1} \cdots n_0)_{10}$, segue-se do Corolário 3.8 que; $(n_k n_{k-1} \ldots n_1)_{10} - 20 \cdot (n_0) \equiv 0 \pmod{67}$. ■

Critério de divisibilidade por 71. Dado um número n, quando multiplicamos o último algarismo de n por 7 e subtraímos o resultado do número obtido do número inicial pela supressão do último algarismo, se o resultado for múltiplo de 71, o número original será múltiplo de 71. Se o número obtido ainda for grande, repete-se o processo até que se possa verificar a divisão por 71.
Demonstração: Como $(71, 10) = 1$, segue-se do Teorema 3.7 que existe $u \in \mathbb{Z}$, onde $u = -7$, tal que $10 \cdot (-7) \equiv 1 \pmod{71} \Rightarrow -70 \equiv 1 \pmod{71} \Rightarrow 71 \mid -70 - 1 = -71$. Portanto, sendo $n = (n_r n_{r-1} \cdots n_0)_{10}$, segue-se do Corolário 3.8 que;
$(n_k n_{k-1} \ldots n_1)_{10} - 7 \cdot (n_0) \equiv 0 \pmod{71}$. ■

Critério de divisibilidade por 73. Dado um número n, quando multiplicamos o último algarismo de n por 22 e somamos ao resultado do número obtido do número inicial pela supressão do último algarismo, se o resultado for múltiplo de 73, o número original será múltiplo de 73. Se o número obtido ainda for grande, repete-se o processo até que se possa verificar a divisão por 73.
Demonstração: Como $(73, 10) = 1$, segue-se do Teorema 3.7 que existe $u \in \mathbb{Z}$, onde $u = 22$, tal que $10 \cdot 22 \equiv 1 \pmod{73} \Rightarrow 220 \equiv 1 \pmod{73} \Rightarrow 73 \mid 220 - 1 = 219$. Portanto, sendo $n = (n_r n_{r-1} \cdots n_0)_{10}$, segue-se do Corolário 3.8 que;
$(n_k n_{k-1} \ldots n_1)_{10} + 22 \cdot (n_0) \equiv 0 \pmod{73}$. ■

Critério de divisibilidade por 79. Dado um número n, quando multiplicamos o último algarismo de n por 8 e somamos ao resultado do número obtido do número inicial pela supressão do último algarismo, se o resultado for múltiplo de 79, o número original será múltiplo de 79. Se o número obtido ainda for grande, repete-se o processo até que se possa verificar a divisão por 79.
Demonstração: Como $(79, 10) = 1$, segue-se do Teorema 3.7 que existe $u \in \mathbb{Z}$, onde $u = 8$, tal que $10 \cdot 8 \equiv 1 \pmod{79} \Rightarrow 80 \equiv 1 \pmod{79} \Rightarrow 79 \mid 80 - 1 = 79$. Portanto, sendo $n = (n_r n_{r-1} \cdots n_0)_{10}$, segue-se do Corolário 3.8 que;
$(n_k n_{k-1} \ldots n_1)_{10} + 8 \cdot (n_0) \equiv 0 \pmod{79}$. ■

Critério de divisibilidade por 83. Dado um número n, quando multiplicamos o último algarismo de n por 25 e somamos ao resultado do número obtido do número inicial pela supressão do último algarismo, se o resultado for múltiplo de 83, o número original será múltiplo de 83. Se o número obtido ainda for grande, repete-se o processo até que se possa verificar a divisão por 83.
Demonstração: Como $(83, 10) = 1$, segue-se do Teorema 3.7 que existe $u \in \mathbb{Z}$, onde $u = 25$, tal que $10 \cdot 25 \equiv 1 \pmod{83} \Rightarrow 250 \equiv 1 \pmod{83} \Rightarrow 83 \mid 250 - 1 = 249$. Portanto, sendo $n = (n_r n_{r-1} \cdots n_0)_{10}$, segue-se do Corolário 3.8 que;
$(n_k n_{k-1} \ldots n_1)_{10} + 25 \cdot (n_0) \equiv 0 \pmod{83}$. ■

Critério de divisibilidade por 89. Dado um número n, quando multiplicamos o último algarismo de n por 9 e somamos ao resultado do número obtido do número inicial pela supressão do último algarismo, se o resultado for múltiplo de 89, o número original será múltiplo de 89. Se o número obtido ainda for grande, repete-se o processo até que se possa verificar a divisão por 89.
Demonstração: Como $(89, 10) = 1$, segue-se do Teorema 3.7 que existe $u \in \mathbb{Z}$, onde $u = 9$, tal que $10 \cdot 9 \equiv 1 \pmod{89} \Rightarrow 90 \equiv 1 \pmod{89} \Rightarrow 89 \mid 90 - 1 = 89$. Portanto,

sendo $n = (n_r n_{r-1} \cdots n_0)_{10}$, segue-se do Corolário 3.8 que;
$(n_k n_{k-1} \ldots n_1)_{10} + 9 \cdot (n_0) \equiv 0 \pmod{89}$. ■

Critério de divisibilidade por 97. Dado um número n, quando multiplicamos o primeiro algarismo n_k de n por 3 e adicionamos ao resultado do número inicial a partir da posição n_{k-2} pela supressão do primeiro algarismo n_k, se o resultado for múltiplo de 97, o número original será múltiplo de 97. Se o número obtido ainda for grande, repete-se o processo até que se possa verificar a divisão por 97.
Demonstração: Seja $n = (n_k n_{k-1} n_{k-2} \cdots n_0)_{10}$, como $100 \equiv 3 \pmod{97}$, segue-se do Teorema 3.10 que:

$$\begin{aligned} n = (n_k n_{k-1} \ldots n_0)_{10} &= n_k \cdot 10^k + (n_{k-1} \ldots n_0)_{10} \\ &\equiv n_k \cdot 3 \cdot 10^{k-2} + (n_{k-1} \ldots n_0)_{10} \pmod{97}, k \geq 2. \blacksquare \end{aligned}$$

Exemplo 3.18. *Verificar se o número 1288 é divisível por 56:*
Como podemos decompor $56 = 7 \cdot 8$, *e:*

	1	7
8	7	$1 = (7, 8)$
$8 - 7 = 1$	$7 - 7 = 0$	

segue-se que $(7, 8) = 1$, *e pelo Teorema 2.13 teremos que* $7 \mid 1288$ *e* $8 \mid 1288$
Verifiquemos se $7 \mid 1288$, *temos:*

$$\begin{array}{rr} & 1288 \not{8} \\ - & 16 \\ \hline & 112 \not{2} \\ - & 4 \\ \hline & 7 \end{array}$$

Verifiquemos se $8 \mid 1288$, *temos:*

$$
\begin{array}{rr}
 & \not{1}288 \\
+ & 4 \\
\hline
 & \not{3}28 \\
+ & 12 \\
\hline
 & \not{4}0 \\
+ & 8 \\
\hline
 & 8
\end{array}
$$

Como 7 é múltiplo de 7 e 8 é múltiplo de 8, segue-se que 1288 é divisível por 56. ■

4 Aplicações

Neste capítulo descrevemos o que entendemos sobre utilidade em matemática, e de como o professor poderá fazer a aplicação dos critérios de divisibilidade apresentado neste trabalho em sala de aula.

Para [13] sobre utilidade há uma tendência comum em educação matemática para se concentrar em matemática aplicável, que está relacionada com a situações da vida real. A partir dessa perspectiva, há um perigo de regras de rotulagem de divisibilidade como inúteis. Acreditando que a utilidade, juntamente com a beleza matemática, está no olho de quem vê. Ainda para [13], um problema que atrai o interesse e a curiosidade dos alunos e geram neles uma investigação envolvente, convidando-os para fazerem conjecturas e testarem conjecturas é mais útil.

De acordo com os Parâmetros Curriculares Nacionais em seu papel formativo, a Matemática contribui para o desenvolvimento de processos de pensamentos e a aquisição de atitudes, cuja utilidade e alcance transcendem o âmbito da própria Matemática, podendo formar no aluno a capacidade de resolver problemas genuínos, gerando hábitos de investigação, proporcionando confiança e desprendimento para analisar e enfrentar situações novas, propiciando a formação de uma visão ampla e científica da realidade, a percepção da beleza e da harmonia, o desenvolvimento da criatividade e de outras capacidades pessoais.

É importante que o aluno perceba as definições, demonstrações, encadeamentos conceituais e lógicos, com a função de construir novos conceitos e estruturas. Partindo, assim para validar intuições e dar sentidos às técnicas aplicadas com o objetivo de elaborar conjecturas, de estimular a busca de regularidade e a generalização de padrões.

As competências e habilidades a serem desenvolvidas em matemática de acordo com os Parâmetros Curriculares Nacionais o aluno deve ser capaz de: Fazer e validar conjecturas, experimentando, recorrendo a modelos, esboços, fatos conhecidos, relações e propriedades; Relacionar etapas da história da matemática com a evolução da humanidade.

Fomos ensinados a acreditar e até mesmo apresentados a livros didáticos em que havia apenas algumas regras de divisibilidade para números como 2, 3, 5, 9, 10, 100, considerando-se o último dígito ou dígitos e alguns considerando a soma de dígitos. E também apenas de ouvir falar de regras de divisibilidade estranhas e totalmente inúteis para 7, 11 e talvez até 13, mencionadas brevemente, sem uma prova, ou omitidas por completo.

Levado pela curiosidade de uma aluna quando apresentava a turma os critérios de divisíbilidade e pela indicação do artigo [12] pelo meu orientador, gerou uma investigação interessante e envolvente, que cuminou nesse trabalho que serve tanto como material de pesquisa para professores quanto um argumento que pode ser também utilizado para desmistificar os critérios de divisibilidade como inúteis. Serve para envolver o aluno a testar e conjecturar os testes de divisibilidade com o corte a direita e o corte a esquerda, apresentados no Capítulo 3.

A seguir apresentaremos algumas sugestões de atividades com suas soluções que podem ser trabalhadas em sala, usando os critérios de divisibilidades propostos.

Exercício 4.1. *Admita dois números inteiros positivos, representados por a e b. Os restos da divisões de a e b por 17 são, respectivamente,14 e 16. Determine o resto da divisão do produto $a \cdot b$ por 17.*

Solução: *Pela Propriedade Restos do Produto ver [7], o resto da divisão $a \cdot b$ por 17 é o mesmo que o resto do produto dos restos, ou seja, resto de $a \cdot b$ por 17 é o mesmo resto de $14 \cdot 16 = 224$ por 17. Logo, pelo critério de divisibilidade de 17 com o Corte a Esquerda, teremos:*

$$\begin{array}{rr} & \not{2}24 \\ - & \quad 4 \\ \hline & 20 \end{array}$$

Donde, vemos que 224 não é divisível por 17, pois $224 = 17 \cdot 13 + 3$, ou seja, $224 \equiv 3 \pmod{17}$; portanto 224 não é divisível por 17, mas deixa resto 3 na divisão.■

Exercício 4.2. *(IFSP) Em uma empresa, $\frac{1}{7}$ dos funcionários são solteiros e $\frac{1}{13}$ dos solteiros pretendem casar em 2011. Analisando esses dados, podemos concluir que uma quantidade possível de funcionários é:*

a) 1300

b) 1000

c) 910

d) 500

Solução: *Seja X o número de funcionários da determinada empresa. Temos que o número de funcionários é divisível por 7 e 13, respectivamente, como $(7, 13) = 1$ segue-se do Teorema 2.13 que $7 \cdot 13 = 91$, ou seja, $91 \mid X$. Das respostas apresentadas, a única que é divisível por 91 é 910. Portanto, letra c) $X = 910$.*■

Exercício 4.3. *(OBMEP 2006) Uma professora distribui 286 bombons igualmente entre seus alunos da 6ª série. No dia seguinte, ela distribuiu outros 286 bombons, também igualmente, entre seus alunos da 7ª série. Os alunos da 7ª série reclamaram que cada um deles recebeu 2 bombons a menos que os alunos da 6ª série. Quantos alunos a professora tem na 7ª série?*

a) 11

b) 13

c) 22

d) 26

e) 30

Solução: *Seja X o número de bombons que cada aluno da 6ª série recebeu. Então cada aluno da 7ª série recebeu $X-2$. Como o número de alunos é um número inteiro segue que o número de bombons é divisível por X e $X-2$, respectivamente. Decompondo em fatores primos 286, termos:*

286	2
143	11
13	13
1	

Assim, $286 = 2 \cdot 11 \cdot 13$, como 11 e 13 diferem em duas unidades, temos que $X = 13$. Logo, cada aluno da 7ª série ganharam 11 bombons e a turma tem $2 \cdot 13 = 26$ alunos, portanto, a resposta correta é a letra d).■

Exercício 4.4. *Sabendo que o primeiro dia do ano de 2016 cairá em uma sexta-feira, e que por algum motivo todos os calendários desse ano desapareceram, e deseja-se saber em qual dia da semana cairá o dia 24 de outubro de 2016?*

Solução: *Primeiramente vamos verificar se 2016 será um ano bissexto, para isso, devemos verificar se $4 \mid 2016$ como $4 \mid 16$ segue-se do critério de divisibilidade por 4 que 2016 é múltiplo de 4, logo 2016 é um ano bissexto tendo o mês de Fevereiro 29 dias. Contando a quantidade de dias de Janeiro a 24 de Outubro teremos no total $31 + 29 + 31 + 30 + 31 + 30 + 31 + 31 + 30 + 24 = 298$ dias, como a semana tem 7 dias e nas condições do problema a semana inicia-se na sexta-feira, devemos verificar*

o resto da divisão de 298 por 7, assim pelo critério de divisibilidade de 7 com o Corte a Esquerda, teremos:

$$\begin{array}{rr} & \not{2}98 \\ + & 4 \\ \hline & \not{1}02 \\ + & 2 \\ \hline & 4 \end{array}$$

Donde, vemos que 298 não é divisível por 7, pois $298 = 7 \cdot 42 + 4$*, ou seja,* $298 \equiv 4 \pmod 7$*; portanto 298 não é divisível por 7, mas deixa resto 4 na divisão. Assim, passaram-se 42 semanas completas mais 4 dias, logo o dia 24 de outubro de 2016 cairá em uma segunda-feira.*■

Exercício 4.5. Sugestão de atividade em grupo: *Confecção do jogo de dominó utilizando os critérios de divisibilidade por 2, 3, 5, 9 e 10, com os números dispostos na Tabela 1 abaixo, recorte e cole seguindo os critérios de divisibilidade formando-se assim as peças para o jogo, segue-se as mesmas regras do jogo de dominó tradicional.*

Tabela 1: Dominó de Critério de Divisibilidade

2	267	3	355	5	332	2	340	10 ou 5	123
3	75	5	412	2	2538	9 ou 3	145	5	7060
10 ou 5	96	3	1002	2	735	5	80	10 ou 5	68
2	4932	3 ou 9	15	3	27	3 ou 9	115	5	310
5 ou 10	12	2 ou 3	35	5	18	2 ou 3	609	3	279
3 ou 9	24	2 ou 3	105	3 ou 5	405	3, 5 e 9	35	5	104

5 Considerações Finais

Consideramos que todos os processos dos critérios de divisibilidade apresentados não dependem de memorização, mas da compreensão do máximo divisor comum, da decomposição em fatores primos, do Teorema 2.13, do conceito de congruência assim como o entendimento de como funcionam o Teorema 3.7, Corolários 3.8 e 3.9 e o Teorema 3.10. Acreditamos ainda, que as ideias sobre os critérios de divisibilidade de números inteiros positivos, possam tornar-se material útil e fonte de inspiração para professores que interessem em incorporar os conceitos aqui desenvolvido em suas práticas de ensino e no direcionamentos de atividades que estímulem a descoberta aos estudantes interessados e curiosos.

Referências

[1] BRASIL, *Parâmetros Curriculares Nacionais: Matemática.* Secretária da Educação,MEC, 1998.

[2] Boyer, Carl Benjamin, *História da matemática: tradução: Elza F. Gomide.* São Paulo,Edgard Bluwcher, 1974.

[3] Domingues, Hygino H., *Fundamentos De Aritmética.* São Paulo,Atual, 1991.

[4] Eves, Howard, *Introdução à história da matemática /Howard Eves; tradução: Hygino H. Domingues.* Campinas-SP: Editora da Unicamp, 2004.

[5] Hefez, Abramo,*Elementos de Aritmética, Coleção Textos Universitários.* 2ª edição. Rio de Janeiro: SBM, 2006.

[6] Ifrah, Georges,*Os números: história de uma grande invenção O Georges Ifrah: tradução de Stella Maria de Freitas Senra: revisão técnica: Antônio José Lopes, Jorge José de oliveira.*11ª edição. São Paulo: Globo, 2005.

[7] Jurkiewicz, Samuel,*Divisibilidade e números inteiros.* Revista PIC OBMEP, Impa, 2007.

[8] Neto, Antonio Caminha Muniz,*Tópicos de Matemática Elementar: teoria dos números / Caminha Muniz.*2ª edição. Rio de Janeiro: SBM, 2012.

[9] Peterson, Ivars,*"Testing for Divisibility", Science News Online, vol. 162#7, (August 17, 2002).*
http://www.sciencenews.org/20020817/mathtrek.asp

[10] Ribenboim, Paulo,*Números Primos: Velhos Mistérios e Novos Recordes, Coleção Matemática Universitária* .1ª edição. Rio de Janeiro: IMPA,2012.

[11] Santos, José Plínio de Oliveira,*Introdução à teoria dos números.*3ª edição. Rio de Janeiro: IMPA,2012.

[12] Renault, Marc,*Stupid Divisibility Trichs, 2006*
http://webspace.ship.edu/msrenault/divisibility/

[13] Zazkis, Rina,*"Divisibility: A problem solving approach through generalizing and specializing", Humanistic Mathematics Network Journal 26 (June 2002), pp. 51-55.*
http://www2.hmc.edu/www_common/hmnj/index.html