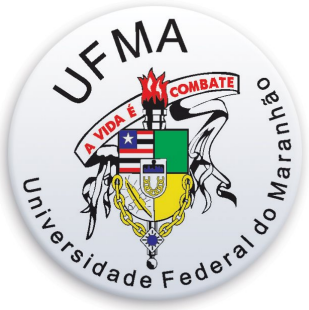

UNIVERSIDADE FEDERAL DO MARANHÃO
CENTRO DE CIÊNCIAS EXATAS E TECNOLOGIA
Programa de Pós-graduação em Rede - Matemática em Rede Nacional/CCET

Derivaldo Barros Gomes

CRITÉRIOS DE DIVISIBILIDADE: provas aritméticas das regras tratadas no ensino de matemática da educação básica

São Luís - MA
2024

Derivaldo Barros Gomes

CRITÉRIOS DE DIVISIBILIDADE: provas aritméticas das regras tratadas no ensino de matemática da educação básica

Dissertação apresentada como requisito parcial para obtenção do título de Mestre em Matemática, ao Programa de Mestrado Profissional em Matemática em Rede Nacional, da Universidade Federal do Maranhão.

Orientador: Prof. Dr. José Santana Campos Costa

São Luís - MA

2024

Ficha gerada por meio do SIGAA/Biblioteca com dados fornecidos pelo(a) autor(a).
Diretoria Integrada de Bibliotecas/UFMA

Barros gomes, Derivaldo.
Critérios de divisibilidade: provas aritméticas das regras tratadas no ensino de matemática da educação básica / Derivaldo Barros gomes. - 2024.
66 p.

Orientador(a): José santana Campos costa.
Dissertação (Mestrado) - Programa de Pós-graduação em Rede - Matemática em Rede Nacional/ccet, Universidade Federal do Maranhão, São luís, 2024.

1. Divisibilidade. 2. Aritmética. 3. Critérios. 4. . 5. . I. Campos costa, José santana. II. Título.

Derivaldo Barros Gomes

CRITÉRIOS DE DIVISIBILIDADE: provas aritméticas das regras tratadas no ensino de matemática da educação básica

Dissertação apresentada como requisito parcial para obtenção do título de Mestre em Matemática, ao Programa de Mestrado Profissional em Matemática em Rede Nacional, da Universidade Federal do Maranhão.

Dissertação de Mestrado. São Luís - MA, 09 de maio de 2024.

Prof. Dr. José Santana Campos Costa
Orientador
Universidade Federal do Maranhão - UFMA

Prof. Dr.Gerar John Alva Morales
Universidade Federal do Maranhão -UFMA

Prof. Dr. José Eduardo Milton de Santana
Universidade Federal de Alagoas - UFAL - Penedo

São Luís - MA
2024

Agradecimentos

Agradeço, primeiramente a Deus, por esta dádiva chamada vida, por todas as oportunidades e por mais esta conquista.. Como católico, que sou, também presto minhas homenagens a São José de Ribamar, padroeiro, e a virgem Santíssima.

Aos meus pais, Rosélia e Raimundo, aos meus irmãos Radson, Paulo e Jackson; ao Rodolfo pela companhia, parceria e paciência nesta jornada.Pois como membros de minha familia, são um porto para repousar sempre nas minhas inquietações e angústias.

Ao meu orientador professor Dr José Santana, que desde quando iniciei meus estudos no mestrado, identifiquei-me de maneira carismática e profissional, pelo compromisso e zelo no que faz, além das fascinantes aulas.

Aos meus amigos do mestrado, o Roger, João, Eudes, Mauro, Willamys, Ezequiel e Luís, que nesta jornada foram companheiros, nas aflições e nos estudos. Sendo bastante unidos e perseverantes nesta jornada.

A todos os professores do programa, em especial ao prof. Dr Anselmo, profa. Dra. Valdiane, profa. Dra. Valeska, e ao coordenador Dr João de Deus, pelas orientações valiosas nas aulas de cada disciplina e aos direcionamentos dados. Aqueles que direta ou indiretamente contribuíram para que pudesse alcançar mais esta conquista em minha vida e de meus companheiros de turma.

Resumo

Este trabalho objetiva mostrar as técnicas utilizadas nos critérios de divisibilidade, tratadas na educação básica, em especial no sexto ano do ensino fundamental, a exemplo do critério por dois, por três, por quatro, por cinco, por seis, por sete, por oito, por nove, por dez e por onze, sendo este último acrescido aqui neste trabalho, como fonte de curiosidade. Tais técnicas foram demonstradas fazendo uso de definições, teoremas e corolários extraídas do arcabouço da aritmética e tratadas com bastante rigor na mesma; para tal, foi utilizado, tópicos como o teorema fundamental da aritmética, congruência, máximo divisor comum e mínimo múltiplo comum, a divisão Euclidiana, princípio da boa ordenação e indução.

Palavras-chave: divisibilidade; aritmética; critérios.

Abstract

This work aims to show the techniques used in the divisibility criteria, treated in basic education, especially in the sixth year of elementary school, such as the criteria for two, for three, for four, for five, for six, for seven, for eight, for nine, by ten and by eleven, the latter being added here in this work, as a source of curiosity. Such techniques were demonstrated using definitions, theorems and corollaries extracted from the arithmetic framework and treated with great rigor; To this end, topics such as the fundamental theorem of arithmetic, congruence, greatest common divisor and least common multiple, Euclidean division, principle of good ordering and induction were used.

Keywords: divisibility; arithmetic; criteria.

Sumário

1 INTRODUÇÃO 8

2 CONCEITOS PRELIMINARES 10
2.1 Axiomas de Peano e o método da Indução 10
2.2 Os números inteiros e o Princípio da Boa Ordenação 12
2.2.1 Adição e Multiplicação 13
2.2.2 Ordenação dos Inteiros 14
2.2.3 Princípio da Boa Ordenação 17

3 DIVISIBILIDADE 19
3.1 Divisibilidade 19
3.2 O sistema de numeração decimal 23
3.3 Divisão envolvendo números inteiros 26
3.3.1 O algoritmo da divisão 27
3.4 O máximo divisor comum 29
3.5 O algoritmo de Euclides 34
3.6 O mínimo múltiplo comum 36
3.7 Os números primos 37

4 CONGRUÊNCIA 40

5 CRITÉRIOS DE DIVISIBILIDADE 45
5.1 Critério de divisibilidade por 2 45
5.2 Critério de divisibilidade por 3 e por 9 46
5.3 Critério de divisibilidade por 4 48
5.4 Critério de divisibilidade por 5 e por 10 49
5.5 Critério de divisibilidade por 6 49
5.6 Critério de divisibilidade por 7 51
5.7 Critério de divisibilidade por 8 53
5.8 Critério de divisibilidade por 11 55

6 CURIOSIDADES E MACETES 58
6.1 A prova dos nove 59
6.2 O Calendário 59
6.3 Macetes 64

7 CONSIDERAÇÕES FINAIS 65

REFERÊNCIAS 66

1 Introdução

Problemas que envolvem divisibilidade são tratadas na educação básica nas séries intermediárias, precisamente no sexto ano do Ensino Fundamental. Nesta série os critérios de divisibilidade são tratados como técnicas, dispensada de suas provas. Sendo abordada através de exemplos de sua utilidade e funcionalidade. Deste modo, este texto pode ser util como uma sequência didática a este conteúdo. Esse tema também é mencionado na Base Nacional Comum Curricular e destacamos a habilidade EF06MA05:

> 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. (BRASIL, 2018)

Vale ressaltar que tais critérios são aplicados, na educação básica, a números naturais e não a números inteiros como ensinadas no Ensino Superior. Tais "técnicas" ensinadas com números naturais, são assim aplicadas, não porque este fosse o único conjunto que apresentasse funcionalidade para tais métodos, mas porque justamente no quinto e sexto ano do ensino fundamental, muitos problemas de matemática estivessem relacionados a esse conjunto, os naturais. Nessas mesmas séries já são apresentados aos jovens estudantes, números decimais, números fracionários, que são características de números racionais. Mas tal menção nessas séries não é dada com devido mérito, porque os livros didáticos o fazem tratando de forma paralela ao conjunto dos números naturais e não como um conjunto dos quais os naturais fizessem parte.

Entretanto, muito do que está colocado neste trabalho, tem como conjunto base o conjunto dos números inteiros,como por exemplo, teoremas, corlários e exemplos, dos conceitos básicos para embasar o desenvolvimento do tema deste trabalho. No tópico critérios de divisibilidade, muito do que está exposto, tem como conjunto numérico de abordagem, o conjunto dos números naturais. É importante salientar que os elementos numéricos utilizados nas técnicas que serão apresentadas, são elementos escritos na base dez. Como base para técnicas de critérios de divisibilidade, é utilizado como base teórica, O princípio da boa ordenação, importante princípio que caracteriza bem o conjunto dos números inteiros; o método da indução, as noções de divisibilidade e a divisão euclidiana, o máximo divisor comum e o mínimo múltiplo comum. De maneira sucinta é apresentado o estudo de números primos, uma vez que estas teorias são importantes na teoria dos números. E por fim, de forma também abreviada, é destacado alguns pontos importantes em congruência, para assim, em seguida, realizar abordagem em critérios de divisibilidade.

Os critérios de divisibilidade apresentados aqui, são aqueles que são ensinados aos

estudantes da educação básica, como mencionado em momento anterior, em sua grande maioria são apresentados como "macetes" para identificar quando um dado número natural é ou não divisível por outro. No caso, critério de divisibilidade por dois, por três, por quatro, por cinco, por seis, por oito, por nove e por dez. Foi acrescentado o critério do sete e do onze, pois com a experiência como professor de matemática para turmas de sexto ano, muitos alunos e alunas interrogavam o porque do salto do seis para o oito e se não havia critério por sete. E sempre propunha para que realizassem pesquisas para que na aula seguinte houvesse possibilidade de discutir os critérios descobertos; isso era feito para que percebessem como a matemática tem tantas outras preciosidades que nem sempre são apresentadas de forma imediata. Outros critérios existem, mas estão fora do escopo deste trabalho, pois o objetivo principal é apresentar os critérios não apenas como macetes, mas evidenciando que a base construída para a técnica em si, já é a engenhosidade que justifica o que tantos professores de matemática precisam apresentar aos estudantes, sem deixar de lado a elegância e beleza que a matemática possui quando é preciso justificar o porque de determinado assunto ser apresentado daquela forma.

No Capítulo dois é apresentado os conceitos fundamentais para dar base ao tema e que são extremamente importantes para realizar boa parte das demonstrações apresentadas neste trabalho, tais como o Axioma de Peano, o Método da Indução, o Principio da Boa Ordenação e, de forma abreviada, os números inteiros e algumas propriedades.

O Capítulo três apresenta uma abordagem mais criteriosa sobre divisibilidade com algumas proposições importantes para justificar determinadas passagens, tais como, garantia de divisibilidade ou não de certos números naturais. Nesse mesmo capítulo é também apresentado, de forma resumida, o sistema de numeração decimal e o teorema chave para escrita de um dado número por meio de sua base numérica.Tópicos como o algoritmo de Euclides, o Máximo Divisor Comum, o Mínimo Múltiplo Comum e Números Primos são pontos importantes, pois possuem teoremas e proposições fortes que dão maior segurança matemática no que será desenvolvido no capítulo cinco.

O Capítulo quatro, apesar de curto, mostra o assunto de Congruência apresentando algumas proposições, teoremas e corolários utilizados justamente nas demonstrações dos critérios de divisibilidade que são apresentados no capítulo cinco. Sendo que é no capítulo cinco que se apresenta o assunto tema, trazendo os critérios com provas, de dois a onze, seguindo uma ordem numérica, justamente, como uma forma didática de apresentar tais critérios.

No capítulo seis foi colocado algumas curisoidades, como a prova dos nove e o calendário, com o intuito de aguçar a curiosidade do leitor sobre a aplicação dos critérios de divisibilidade e também da congruência. E neste mesmo capítulo os macetes fazem o encerramento do trabalho, fornecendo ao leitor as técnicas, de forma abreviada, dos critérios colocados no capítulo cinco.

2 CONCEITOS PRELIMINARES

Neste capítulo será apresentado alguns conceitos fundamentais para o desenvolvimento deste trabalho, tais como os axiomas de Peano, o Método da Indução e o Princípio da Boa Ordenação.

2.1 Axiomas de Peano e o método da Indução

Os Axiomas de Peano são os seguintes:

(A) Todo número natural n tem um sucessor, representado por $n+1$.

(B) Se $m+1 = n+1$, então $m = n$.

(C) Existe um único número natural, designado por 1, tal que $n+1 \neq 1$, para todo n natural.

(D) (Axioma de Indução) Seja X um conjunto de números naturais (isto é, $X \subset \mathbb{N}$). Se $1 \in X$ e se, além disso $n+1 \in X$, para cada $n \in X$, então $X = \mathbb{N}$.

Aqui $\mathbb{N}$ é o conjunto dos números naturais. É importante salientar que em muitas obras da literatura acadêmica de matemática o conjunto dos naturais $\mathbb{N} = \{1, 2, 3, 4, ...\}$, tendo como ponto de partida o 1 e em outros, o conjunto dos naturais $\mathbb{N} = \{0, 1, 2, 3, ...\}$, tendo como ponto de partida o 0 (zero). Em muitas demosntrações de indução será utilizado a primeira forma do conjunto dos naturais. Quando for conveniente a segunda notação será utilizada com a devida menção.

O método da indução (ou Axioma de Indução) como ilustram, no livro matemática discreta dos professores Augusto Morgado e Paulo Cezar (MORGADO; CARVALHO, 2015), "não é somente um método de demonstração: ele é também um método para construir definições." Tal método será bastante útil para realizarmos nas demonstrações de muitas proposições e teoremas deste trabalho. O Teorema abaixo é uma versão um pouco mais geral que o Axima (D) citado acima.

Teorema 1. *Seja $P(n)$ uma propriedade relativa ao número natural n e seja k um número natural.*

Suponhamos que

i) $P(k)$ é válida;

ii) Para $n \geq k$, a validez de $P(n)$ implica a validez de $P(n+1)$.

Então $P(n)$ é válida para todo $n \geq k$.

Demonstração. O Axioma da Indução é um caso particular do acima, para $k = 1$. Mas para demonstrar essa versão um pouco mais geral, recorremos ao Axioma de Indução. Tomando

$$X = \{n \text{ natural } |(k + n - 1) \text{ é válida}\}$$

Então, $1 \in X$, já que por (i), $P(k + 1 - 1) = P(k)$ é válida. Além disso, por (ii), se $n \in X$, então $n + 1 \in X$. Logo, pelo Axioma da Indução, X é o conjunto dos números naturais. Isto significa que $P(k + n - 1)$ é válida para todo n natural, ou seja, que $P(n)$ é válida para todo $n \geq k$. □

Exemplo 1. *Prove que, para qualquer número natural* n, $n^3 + (n+1)^3 + (n+2)^3$ *é divisível por 9.*

Demonstração. Consideremos $P(n) : n^3 + (n + 1)^3 + (n + 2)^3$. Para $P(n)$ ser divisível por 9 é preciso que:

$$P(n) : n^3 + (n + 1)^3 + (n + 2)^3 = 9\text{k para } k \text{ natural}$$

Para $n = 1$, temos:

$P(1) : 1^3 + 2^3 + 3^3 = 36$ que é divisível por 9.

Suponhamos $P(n)$ válida, ou seja que $P(n)$ seja divisível por 9.

Façamos a verificação para $P(n + 1)$.

$$P(n + 1) : (n + 1)^3 + (n + 2)^3 + (n + 3)^3$$

Como $(n + 1)^3 + (n + 2)^3 = 9k - n^3$, temos ainda que $P(n + 1)$ é:

$$\begin{aligned}(n + 1)^3 + (n + 2)^3 + (n + 3)^3 &= 9k - n^3 + (n + 3)^3 \\ &= 9k + 9n^2 + 27n + 27 \\ &= 9(k + n^2 + 3n + 3) \text{ que é divisível por 9}\end{aligned}$$

Como $P(n)$ implica em $P(n + 1)$, logo $P(n)$ é válida para n natural. □

Teorema 2. *Principio da Indução Completa ou da Indução Forte*

Seja $P(n)$ uma propriedade relativa ao número natural n. Suponhamos que:

i) $P(1)$ é válida

ii) Para todo n natural, a validez de $P(k)$, para todo $k \leq n$, implica a validez de $P(n+1)$. Então $P(n)$ é válida para todo n natural.

Demonstração. Consideremos a sentença aberta $Q(n) : P(k)$ é válida, para todo natural $k \leq n$ Como, por (i) $P(1)$ é válida, $Q(1)$ também é. Suponhamos agora que $Q(n)$ seja válida. Isto quer dizer que $P(k)$ é válida, para todo $k \leq n$. Mas por (ii), isto implica a validez de $P(n+1)$, que por sua vez implica em $P(k)$ seja válida para todo $k \leq n+1$. Logo, $Q(n+1)$ também é válida. Portanto, pelo Axioma de Indução, $Q(n)$ é válida para todo n natural, de onde decorre a validez de $P(n)$ para todo n natural. □

Os assuntos que serão aqui apresentados possuem como conjunto de referência o conjunto dos números inteiros. Quando for conveniente é que será utilizado o conjunto dos números naturais.

2.2 Os números inteiros e o Princípio da Boa Ordenação

De acordo com o professor Abramo, no livro Aritmética, enuncia que o conceito de números inteiros teve origem de sua criação com o objetivo de resolver problemas de contagem. Os números negativos tem sido considerados esporadicamente na antiguidade, mas tratado com um olhar mais desconfiado por parte dos matemáticos até então; foi no final da idade média na Europa, com as atividades mercantis que esse receio fora diminuindo, pois foi sentido a necessidade de considerar os inteiros relativos e com eles realizar operações. Segundo ainda relata Abramo (HEFEZ, 2009), "o matemático de Bolonha, Rafael Bombelli (1526-1572), no seu livro l'Algebra, publicado em 1572, enuncia claramente as regras operatórias com números inteiros". A evolução da noção intuitiva de números inteiros para um conceito mais elaborado se deu a passos lentos, pois só no final do século XIX, quando os fundamentos de toda matemática foram questionados e intensamente repensados, é que a noção de número passou a ser baseada em conceitos da teoria dos conjuntos, considerados mais primitivos.

Não é o objetivo deste trabalho, aprofundar e apresentar a natureza dos números inteiros, elementos apresentados no rigor da matemática e da teoria dos números, mas apenas apresentar alguns elementos interessantes e importantes deste conjunto, uma vez que em grande parte do que será aqui exposto, os números inteiros são mencionados e utilizados em teoremas e proposições de divisibilidade.

Tomemos como ponto de partida o conjunto $\mathbb{Z}$ dos números inteiros, representado por

$$\mathbb{Z} = \{..., -3, -2, -1, 0, 1, 2, 3, ...\}$$

juntamente com as operações de adição $(a, b) \to a+b$ e de multiplicação $(a, b) \to a \cdot b$.

Assim como cita o professor Abramo (HEFEZ, 2009) "A lista de axiomas que adotaremos está longe de ser a menor possível, pois quanto menor for essa lista, mais

demorado será chegar aos aspectos mais interessantes da teoria, ônus que não desejamos ter aqui", será realizado aqui breve abordagem.

2.2.1 Adição e Multiplicação

A adição e multiplicação no conjunto dos números inteiros, possuem as seguintes propriedades:

1) são bem definidas:

   Para todos a, b, c, d inteiros, se $a = c$ e $b = d$, então $a + b = c + d$ e $a \cdot b = c \cdot d$.

2) são comutativas:

   Para todos a, b inteiros, $a + b = b + a$ e $a \cdot b = b \cdot a$.

3) são associativas:

   Para todos a, b, c inteiros, $(a + b) + c = a + (b + c)$ e $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.

4) ambas possuem elementos neutros:

   Para todo a inteiro, $a + 0 = a$ e $a \cdot 1 = a$

5) a adição possui elementos simétricos:

   Para todo a inteiro, existe $b = -a$ tal que $a + b = 0$.

6) a multiplicação é distributiva com relação à adição:

   Para todos a, b, c inteiros, tem-se $a \cdot (b + c) = a \cdot b + a \cdot c$. É pela propriedade 1 que nos é permitido somar um dado número (ou multiplicar um dado número) a ambos os lados de uma igualdade.

Observe que o conjunto dos números inteiros é particionado em dois subconjuntos:

$$\mathbb{Z} = \mathbb{N} \cup (-\mathbb{N})$$

Em que $\mathbb{N}$ é o conjunto dos números naturais e $-\mathbb{N}$ é o simétrico do conjunto $\mathbb{N}$.

Proposição 1. $a \cdot 0 = 0$ *para todo a inteiro.*

Demonstração. das propriedades 4 e 6, temos:

$$a.0 = a \cdot (0 + 0) = a \cdot 0 + a \cdot 0$$

Somando $-(a \cdot 0)$ a ambos os lados da igualdade e utilizando as propriedades já enunciadas, obtemos:

$$\begin{aligned} 0 &= -(a \cdot 0) + a \cdot 0 \\ &= -(a \cdot 0) + (a \cdot 0 + a \cdot 0) \\ &= (-(a \cdot 0) + a \cdot 0) + a \cdot 0 \\ &= 0 + a \cdot 0 \\ &= a \cdot 0 \end{aligned}$$

□

Proposição 2. *A adição é compatível e cancelativa com respeito a igualdade: Para todos a, b, c inteiros,*

$$a = b \Leftrightarrow a + c = b + c$$

Demonstração. A implicação $a = b \Rightarrow a + c = b + c$ é consequência da adição ser bem definida (propriedade 1). Supondo que $a + c = b + c$, somando $(-c)$ a ambos os lados, obtemos $a = b$. □

2.2.2 Ordenação dos Inteiros

Admitiremos que em $\mathbb{Z}$ também valem as seguintes propriedades:

7) Fechamento de $\mathbb{N}$:

O conjunto $\mathbb{N}$ é fechado para a adição e para a multiplicação, ou seja, para todos a, b naturais, tem-se que $a + b \in \mathbb{N}$ e $a \cdot b \in \mathbb{N}$.

8) Tricotomia:

Dados a, b inteiros, uma e apenas uma, das seguintes possibilidades é verificada:

i) $a = b$;

ii) $b - a \in \mathbb{N}$;

iii) $-(b - a) = a - b \in \mathbb{N}$

Diz-se que a é menor do que b, simbolizados por $a < b$, toda vez que a propriedade (ii) acima for verificada.

Como $a - 0 = a$, decorre da definição dada que $a > 0$ se, e somente se, $a \in \mathbb{N}$. Portanto,

$$\{x \in \mathbb{Z} | x > 0\} = \mathbb{N} \; e \; \{x \in Z | x < 0\} = -\mathbb{N}$$

Decorre daí que $a > 0$ se, e somente se, $-a < 0$.

Proposição 3. *A relação "menor que" é transitiva: para todos a, b, c inteiros, $a < b$ e $b < c$ implica que $a < c$.*

Demonstração. Supondo $a < b$ e $b < c$, temos que $b - a$ e $c - b$ são naturais. Como $\mathbb{N}$ é aditivamente fechado, temos que $c - a = (b - a) + (c - b) \in N$; logo, $a < c$. □

Proposição 4. *A adição é cancelativa com respeito à relação "menor que": para todos a, b, c inteiros, $a < b$ se, e somente se $a + c < b + c$.*

Demonstração. Suponha que $a <$b. Logo, $b - a \in \mathbb{N}$

Dessa forma,

$$(b + c) - (a + c) = b - a \in \mathbb{N}$$

O que implica que $a + c < b + c$.

De forma reciproca, suponha que $a + c < b + c$. Pela primeira parte da proposição, podemos somar $(-c)$ a ambos os lados da igualdade, o que nos conduz ao resultado que desejamos provar. □

Proposição 5. *A multiplicação por elementos de $\mathbb{N}$ é compatível e cancelativa com respeito à relação "menor que": para todos a, b inteiros e c natural, $a < b \Leftrightarrow a \cdot c < b \cdot c$.*

Demonstração. Suponha que $a < b$. Logo, $b - a \in \mathbb{N}$.

Assim, se $c \in \mathbb{N}$, pelo fato de $\mathbb{N}$ ser multiplicativamente fechado, temos $b \cdot c - a \cdot c = (b - a) \cdot c \in \mathbb{N}$; logo, $a \cdot c < b \cdot c$.

Reciprocamente, suponha que $a \cdot c < b \cdot c$, com $c \in \mathbb{N}$. Pela tricotomia temos três possibilidades a analisar:

i) $a = b$. Isso acarretaria $a \cdot c = b \cdot c$, o que é falso.

ii) $b < a$, isso acarretaria, pela primeira parte da demonstração, que $b \cdot c < a \cdot c$, o que também é falso.

iii) $a < b$. Esta é a única possibilidade válida.

□

Proposição 6. *A multiplicação é compatível e cancelativa com respeito a igualdade: para todos a, b inteiros e todo c inteiro não nulo* $a = b \Leftrightarrow a \cdot c = b \cdot c$.

Demonstração. A implicação $a = b \Rightarrow a \cdot c = b \cdot c$ vale também para $c = 0$ e decorre de maneira imediata do fato da multiplicação ser bem definida (Propriedade 1).

i) caso $c > 0$. Se $a < b$, pela Proposição 5, tem-se que $a \cdot c < b \cdot c$, o que é um absurdo. Se $b < a$, pelo mesmo argumento, $b \cdot c < a \cdot c$, o que é absurdo. Portanto, a única alternativa válida é a = b.

   Para $c > 0$, tem-se que

   $a = b \rightarrow$a - b = b - b$\rightarrow$(a - b).c = (b - b).c$\rightarrow$ac - bc = 0.

ii) caso $-c > 0$. A argumentação segue a mesma linha usada acima para o caso $c > 0$, levando em conta que $d < e$ se, e somente se, $-d > -e$ (que será provado logo a seguir).

   Prova-se que para d, e inteiros, temos $d < e$ se, e somente se, $-d > -e$.

   ($\Rightarrow$) considerando $d < e$, somando a ambos os lados $-(d + e)$, temos:

$$d - (d + e) < e - (d + e) \rightarrow -e < -d$$

   ($\Leftarrow$) considerando $-d > -e$, soma-se a ambos os lados $d + e$, temos:

$$-d + d + e > -e + d + e \rightarrow e > d.$$

□

Decorre do exposto até aqui que $\mathbb{Z}$ é um domínio de integridade[1], isto é, se a e b são inteiros tais que $a \cdot b = 0$, então $a = 0$ ou $b = 0$. De fato, se $a \neq 0$, então $ab = 0 = a \cdot 0$. Pelo cancelamento de $a \neq 0$, segue-se que $b = 0$.

Diremos que a é menor ou igual do que b, ou que b é maior ou igual do que a, escrevendo $a \leq b$ ou $b \geq a$, se $a <$b ou $a = b$.

Note que $a \leq b$ se, e somente se, $b - a \in \mathbb{N}$.Frisa-se que o conjunto dos naturais mencionado é aquele que inclui o zero. Com isso, verifica-se facilmente que essa nova relação é efetivamente uma relação de ordem, pois possui as seguintes propriedades:

[1] Conforme (GONÇALVES, 1999) um dominio de integridade é uma estrutura algebrica com duas operações: soma e multiplicação; comutativo, com unidade e sem divisores de zero.

1) é reflexiva: para todo a inteiro, $a \leq a$.

2) é antissimétrica: para todos a, b inteiros, $a \leq b$ e $b \leq a$ implica que $a = b$.

3) é transitiva: para todos a,b,c inteiros, $a \leq b$ e $b \leq c$ implica que $a \leq c$.

Definiremos a importante noção de valor absoluto.

Seja a inteiro, definimos:

$$|a| = \begin{cases} a, \text{ se } a \geq 0 \\ -a, \text{ se } a < 0 \end{cases}$$

2.2.3 Princípio da Boa Ordenação

Antes de enunciarmos esta propriedade, vejamos alguns pontos importantes.

- Um subconjunto S de $\mathbb{Z}$ é limitado inferiormente, se existir $c \in \mathbb{Z}$ tal que $c \leq x$ para todo $x \in S$.
- Diremos que $a \in S$ é um menor elemento de S se $a \leq x$, para todo $x \in S$.
- Apesar do conjunto vazio, ser aquele que não possui nenhum elemento, convencionamos que seja limitado inferiormente e, respectivamente, superiormente, tendo qualquer número como cota inferior e, respectivamente, cota superior. Ou seja, seja T um subconjunto de $\mathbb{Z}$, sendo T vazio. Se existisse $x \in T$, $c \leq x$, sendo c uma cota inferior e, $x \leq d$, sendo d uma cota supeiror.
- Um menor elemento de S, se existir, é único. Tal fato se justifica se considerarmos a e a', como os menores elementos de S, teremos então que $a \leq a'$ e $a' \leq a$ o que implica em $a = a'$.
- A exemplo, $\mathbb{Z}$ e $-\mathbb{N}$ não são limitados inferiormente e nem possuem um menor elemento. Mas $\mathbb{N}$ é limitado inferiormente e possui 0 como menor elemento (em alguns textos, o menor elemento natural é o 1. Tudo irá depender da conveniência do autor).

Princípio da Boa Ordenação (PBO). Se S é um subconjunto não vazio de $\mathbb{Z}$ e limitado inferiormente, então S possui um menor elemento.

Vejamos algumas ilustrações do uso do PBO.

Proposição 7. *Não existe nenhum número inteiro n tal que $0 < n < 1$.*

Demonstração. Provemos por absurdo. Suponhamos que exista n com essa propriedade. Dessa forma temos um conjunto não vazio $A = \{x \in \mathbb{Z}; 0 < x < 1\}$ que é limitado inferiormente.

Assim A, possui um menor elemento a, com $0 < a < 1$. Multiplicando esta última desigualdade por a (atenção para o fato de $a > 0$), temos:

$0 < a^2 < a$ que ainda é $0 < a^2 < a < 1$

Portanto $a^2 \in A$ e $a^2 < a$, que é uma contradição!

Logo A é vazio. □

Corolário 1. *Dado um número inteiro n qualquer, não existe nenhum número inteiro m tal que* $n < m < n + 1$.

Demonstração. Por absurdo, suponhamos que exista um número inteiro m satisfazendo as desigualdades $n < m < n + 1$.

Logo, $0 < m - n < 1$, o que contradiz a proposição anterior. □

Corolário 2 (Propriedade Arquimediana)**.** *Sejam* $a, b \in \mathbb{Z}$*, com* $b \neq 0$*. Então existe* $n \in \mathbb{Z}$ *tal que* $n \cdot b > a$.

Demonstração. Como $|b| \neq 0$, da Proposição 7, temos que $|b| \geq 1$.

Portanto,

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

Tomando $n = |a| + 1$, se $b > 0$ e $n = -(|a| + 1)$, para $b < 0$, o resultado segue na desigualdade acima. □

3 DIVISIBILIDADE

O processo de realizar a divisão de um número por outro, em grande maioria das vezes realizadas entre números inteiros, é uma das maiores engenhosidades já descobertas no mundo matemático. O engenhoso algoritmo enunciado por Euclides a séculos atrás, em sua grande obra, intitulada Os Elementos, mostra o quão grande foi esse homem em sua época. Claro que outros gigantes, que o antecederam e o sucederam merecem honras por tamanhas descobertas científicas; a obra de Euclides, quanto ao processo de divisão envolvendo dois números inteiros, é uma das maiores técnicas já reveladas para a sociedade. Conheçamos alguns pontos importantes.

3.1 Divisibilidade

Definição 1. *Dados dois números inteiros a e b, dizemos que a divide b, denotado por $a|b$, se existir um inteiro c tal que $b = ac$.*

Exemplo 2. *Tem-se como exemplo que* $3|12$ *pois* $12 = 3.4$

Exemplo 3. *Porém como não há inteiro c que satisfaça* $21 = 2.c$*, então* $2 \nmid 21$

Proposição 8. *Sejam a, b, c, d inteiros.*

Tem-se que:

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

ii) $0|a \Leftrightarrow a = 0$.

iii) a divide b se, e somente se, $|a|$ divide $|b|$.

iv) se $a|b$ e $b|c$, então $a|c$.

v) se $a|b$ e $c|d \Rightarrow ac|bc$.

vi) se $a|(b \pm c)$ então $a|b \Leftrightarrow a|c$.

vii) se $d|n$ e $n|d \Rightarrow |d| = |n|$ para n inteiro.

Demonstração. Sejam a, b, c, d inteiros, tem-se:

i) Decorre das igualdades $a = a \cdot 1$, $a = 1 \cdot a$ e $0 = 0 \cdot a$.

ii) ($\Rightarrow$) Suponha que $0|a$ dessa forma, existe c inteiro tal que $a = c \cdot 0$.

Decorre da Proposição 1 que $a \cdot 0 = 0$, daí conclui-se que $a = 0$.

($\Leftarrow$) para a recíproca temos que $0|0$, o que torna imediato a prova.

iii) ($\Rightarrow$)*se* a|b então existe k inteiro tal que $b = ak$.

Sendo assim $|b| = |ak| = |a|.|k|$ o que leva a concluir que $|a|$ divide $|b|$.

($\Leftarrow$)$|a|$ divide $|b|$, então $|b| = k.|a|$, para um determinado k inteiro. Tomando módulos, tem-se:

$|b| = |k| \cdot |a| \Rightarrow |b| = |k| \cdot |a| \Rightarrow |b| = |k \cdot a| \Rightarrow b = k \cdot a$ ou $b = -k \cdot a$

Dessa forma, tem-se que a divide b.

iv) Se $a|b$ tem-se $b = k_1 \cdot a$, para k_1 inteiro; e $b|c$, tem-se $c = k_2 \cdot b$.

Substituindo $b = k_1 \cdot a$ em $c = k_2 \cdot b$, tem-se $c = k_2 \cdot k_1 \cdot a$, o que prova que a divide c.

v) Se $a|b$ e $c|d$, então existem k_1 e k_2 inteiros, tal que $b = k_1 a$ e $d = k_2 c$. Dessa forma, $bd = k_1 k_2 ac$. Logo $ac|bd$.

vi) ($\Rightarrow$) Suponha que $a|(b + c)$. Dessa forma existe k_1 inteiro, tal que $b + c = k_1 a$.

Mas se $a|b$, então existe k_2 inteiro tal que $b = k_2 a$. Juntando as duas igualdades dadas, tem-se que

$$k_2 a + c = k_1 a$$

no que resulta em $c = k_1 a - k_2 a = (k_1 - k_2)a$. Então $a|c$.

($\Leftarrow$) supondo que $a|(b + c)$, donde $b + c = k_1 a$.

Mas se $a|c$, então existe k_3 inteiro tal que $c = k_3 a$. De forma análoga ao feito anteriormente, tem-se:

$$b + k_3 a = k_1 a \Rightarrow b = (k_1 - k_3)a$$

o que possibilita concluir que $a|b$.

Por outro lado, se $a|(b - c)$ e $a|b$, utilizando o caso já mostrado, tem-se $a| - c$, o que implica que $a|c$.

vii) considere d e n inteiros positivos, se $d|n$ e $n|d$ existem inteiros k_1 e k_2 tal que $d = k_1 n$ e $n = k_2 d$, o que leva a concluir que $d = n$.

Dessa forma se n e d forem inteiros quaisquer nas condições dadas, então $|d| = |n|$. □

Proposição 9. *Se a, b, c inteiros são tais que $a|b$ e $a|c$, então para todo x, y inteiros*

$$a|(xb + yc)$$

.

Demonstração. Tendo que $a|b$ e $a|c$ então existem k_1 e k_2 inteiros tais que $b = k_1 a$ e $c = k_2 a$.

Logo, para x, y inteiros

$$xb + yc = x(k_1 a) + y(k_2 a) = (xk_1 + yk_2)a$$

o que prova o resultado. □

Proposição 10. *Se a, b inteiros, onde b é não nulo, tem-se que $a|b$ implica que $|a| \leq |b|$.*

Demonstração. Se $a|b$, existe k_1 inteiro tal que $b = k_1 a$.

Tomando módulos, tem-se que

$|b| = |k_1||a|$. Como $b \neq 0$, tem-se que $k_1 \neq 0$; logo, $1 \leq |k_1|$ e, consequentemente, $|a| \leq |a||k_1| = |b|$. □

Em particular, se a inteiro e $a|1$, então $0 < |a| \leq 1$; então $|a| = 1$ e, portanto, $a = \pm 1$.

Para $b \neq 0$, tem-se que todo divisor a de b é tal que $|a| \leq |b|$. Segue-se que b tem um número finito de divisores que estão no intervalo $-|b| \leq a \leq |b|$.

Proposição 11. *Se a, b inteiros e n natural não nulo. Temos que $a - b$ divide $a^n - b^n$*

Demonstração. Prova-se usando indução sobre n.

Para $n = 1$, tem-se claramente que $a - b$ divide $a^1 - b^1$

$$a^{n+1} - b^{n+1} = aa^n - ba^n + ba^n - bb^n = (a - b)a^n + b(a^n - b^n)$$

Como $a - b|a - b$ e por hipótese $a - b|a^n - b^n$, pelo Princípio da Indução e pela Proposição 9, $a - b|a^{n+1} - b^{n+1}$, estabelecendo assim o resultado para todo n natural. □

Proposição 12. *Se a, b inteiros e n natural. Tem-se que $a+b$ divide $a^{2n+1}+b^{2n+1}$.*

Demonstração. Usando indução sobre n, assim como na proposição anterior, tem-se:

Para $n = 0$, tem-se de modo imediato que $a + b|a + b$.

Suponha que $a + b|a^{2n+1} + b^{2n+1}$. Então:

$$\begin{aligned} a^{2(n+1)+1} + b^{2(n+1)+1} &= a^2a^{2n+1} - b^2a^{2n+1} + b^2a^{2n+1} + b^2b^{2n+1} \\ &= (a^2 - b^2)a^{2n+1} + b^2(a^{2n+1} + b^{2n+1}) \end{aligned}$$

Como $a + b$ divide $a^2 - b^2$, pois $a^2 - b^2 = (a - b)(a + b)$ e, por hipótese $a + b$ divide $a^{2n+1}+b^{2n+1}$, decorre das igualdades acima e da Proposição 9, que $a+b|a^{2(n+1)+1}+b^{2(n+1)+1}$, estabelecendo assim o resultado para todo n natural. □

Proposição 13. *Se a, b inteiros e n natural não nulo. Tem-se que $a+b$ divide $a^{2n}-b^{2n}$.*

Demonstração. Novamente a prova será usando indução sobre n.

Para $n = 1$, tem-se $a + b$ divide $a^2 - b^2$ (foi mostrado na proposição anterior).

Suponha que $a + b|a^{2n} - b^{2n}$. Então:

$$\begin{aligned} a^{2(n+1)} - b^{2(n+1)} &= a^2a^{2n} - b^2a^{2n} + b^2a^{2n} - b^2b^{2n} \\ &= \left(a^2 - b^2\right) a^{2n} + b^2 \left(a^{2n} - b^{2n}\right). \end{aligned}$$

Como $a + b|a^2 - b^2$ e, por hipótese $a + b|a^{2n} - b^{2n}$, decorre das igualdades acima e da Proposição 9 que $a + b|a^{2(n+1)} + b^{2(n+1)}$, o que estabelece o resultado para todo n natural. □

Como forma de ilustrar as proposições demonstradas, apresenta-se alguns exemplos.

Exemplo 4. *Sejam a, b, c inteiros com c não nulo. Mostre que $a|b$ e $b|a$ se, e somente se,*

$$|a| = |b|$$

Demonstração. Se $b = 0$, como $a|b$ devemos ter $a = 0$, decorrente da Proposição 8 .

Assim, $|a| = 0 = |b|$.

Suponha b inteiro não-nulo, logo a também é inteiro não-nulo, pois $a|b$. Pela Proposição 10 , temos que $|a| \leq |b|$ e $|b| \leq |a|$, o que mostra que $|a| = |b|$. □

Exemplo 5. *Mostre que, para todo n natural,*

a) $10|11^n - 1$

b) $8|3^{2n}-1$

c) $13|9^{2n}-2^{4n}$

d) $6|5^{2n+1}+1$

Demonstração. a) Tem-se que, $10 = 11-1$ e $11^n - 1 = 11^n - 1^n$.

Segue da Proposição 11 , ou seja, $(a-b)|\,(a^n-b^n)$, que $10|11^n-1$, para todo n natural.

b) Tem-se que $8 = 9-1$; como $9 = 3^2$, segue-se que:

$$3^{2n}-1 = \left(3^2\right)^n - 1 = 9^n - 1^n$$

Da Proposição 11 , pode-se concluir que $8|3^{2n}-1$, para todo n natural.

c) Como $13 = 9+4 = 9+2^2$ e $9^{2n}-2^{4n} = 9^{2n}-\left(2^2\right)^{2n}$, da Proposição 13 , segue o que se deseja provar, para todo n natural.

d) Como $6 = 5+1$ e $5^{2n+1}+1 = 5^{2n+1}+1^{2n+1}$, segue da Proposição 12 o que se deseja provar, para todo n natural. □

Exemplo 6. *Para quais valores naturais de a, a* $-2|a^3+4$ *?*

Demonstração. Tem-se que $a^3+4 = a^3-8+12$.

Como $a-2$ divide a^3-8 (pela Proposição 11) então $a-2$ divide a^3+4 se, e somente se, $a-2$ divide 12 ; isso ocorre se, e somente assim se, $a \in \{1,3,4,5,6,8,14\}$. □

3.2 O sistema de numeração decimal

O homem desde os primórdios, quando ainda vivendo em cavernas, alguns deles usavam gravuras, para fazer representações das situações do dia-a-dia. Com certa evolução da humanidade, os povos foram construindo formas de fazer contagem e representação desse processo. O homem fazia contagem por meio de associação com outros objetos, mas ainda de forma rudimentar sem estabelecer signos para "suas contas". A humanidade foi evoluindo e daí civilizações foram construindo sistemas de numeração próprios. Tem-se como exemplos, os mais citados nos livros de matemática, tendo por exemplo a coleção de (JR, 2022) nos capítulos que se referem aos sistemas de numeração, cada qual utilizando simbologia especifica como forma de representar os signos numéricos, como o sistemas de numeração dos egípcios, dos babilônios e dos romanos.

Aqui será realizado estudo, abreviado, no sistema de numeração decimal posicional. Não porque este fosse o único sistema a ser utilizado no meio acadêmico, mas por questão de simplicidade e usualidade. Mas o sistema de numeração decimal, não foi aceito tão

facilmente pelo povo europeu, como informa o professor Abramo, no livro de Aritmética, página 46:

> Esse sistema de numeração, que é uma variante do sistema sexagesimal utilizado pelos babilônios 1700 anos de Cristo, foi desenvolvido na China e na Índia. Existem documentos do século VI comprovando a utilização desse sistema. Posteriormente, foi se espalhando pelo Oriente Médio, por meio das caravanas, tendo encontrado grande aceitação entre os povos árabes. A introdução dos sistema decimal na Europa foi tardia por causa dos preconceitos da Idade Média. Por exemplo, em um documento de 1299, os banqueiros de Florença condenavam o seu uso. O sistema começou a ter maior difusão na Europa a partir de 1202, quando da publicação do livro Liber Abacci, de Fibonacci. Vários séculos se passaram para que, finalmente, esse sistema fosse adotado sem restrições pelos europeus. (HEFEZ, 2009)

Como é sabido, o sistema é chamado de decimal, justamente porque há dez símbolos, que chamaremos de algarismos, que são:

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

para o qual o 0 (zero) é a representação da ausência de algarismo.

O sistema é também chamado de posicional. Justamente porque "a ordem" em que estão cada algarismo no símbolo, o faz ser único e diferente de outro número dado com os mesmos algarismos, colocados em posições diferentes, como por exemplo os números 123 e 312, apesar de possuírem os mesmos algarismo, representam números diferentes e quando associados a quantidade, representam quantias diferentes.

No sistema posicional, cada algarismo, além de seu valor intrínseco, possui um peso que lhe é atribuído em função da posição que ele ocupa no número. Esse peso, que corresponde a uma potência de dez, varia do seguinte modo:

1) O algarismo posicionado mais à direita tem peso um;

2) O seguinte, sempre da direita para a esquerda, tem peso dez;

3) O subsequente tem peso 100;

4) O seguinte tem peso 1000 e assim por diante.

Não é demais frisar, que o peso de cada algarismo no número indicado é sempre dado da direita para a esquerda.

Os números de um a nove são representados pelos algarismos, respectivamente, 1, 2, 3, 4, 5, 6, 7, 8 e 9, o número dez é representado por 10, o número cem por 100 e o número mil por 1000.

Considere como ilustração o número 34013, que na base 10 tem a representação dado a seguir:

$$3.10^4 + 4.10^3 + 0.10^2 + 1.10 + 3$$

Cada algarismo de um número possui uma ordem. Esta ordem é contada daquele que está na extrema direita para a esquerda. Dessa forma, no exemplo a cima, o primeiro 3 que aparece é de primeira ordem enquanto o segundo 3 é de quinta ordem.

Cada terna de ordens, também contadas da direita para a esquerda, forma uma classe. Ilustra-se a seguir os nomes das primeiras classes e ordens:

Classe do Milhão			Classe do Milhar			Classe das Unidades		
Centenas de milhão	Dezenas de milhão	Unidades de milhão	Centenas de milhares	Dezenas de milhares	Unidades de milhares	Centenas	Dezenas	Unidades
9^a ordem	8^a ordem	7^a ordem	6^a ordem	5^a ordem	4^a ordem	3^a ordem	2^a ordem	1^a ordem

Será enunciado um importante teorema, no qual os sistemas de numeração posicionais estão baseados, sendo uma aplicação da divisão euclidiana, que em momento oportuno será apresentado.

Teorema 3. *Sejam dados os números inteiros a e b, com $a > 0$ e $b > 1$. Existem números inteiros $n \geq 0$ e $0 \leq r_0, r_1, ..., r_n < b$, com $r_n \neq 0$, univocamente determinados, tais que*

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

Demonstração. Usando Indução Completa sobre a.

Se $0 < a < b$, basta tomar $n = 0$ e $r_0 = a$.

Supondo o resultado válido para todo natural menor do que a, onde a $\geq b$.

Prova-se para a. Utilizando a divisão euclidiana, existem q e r, únicos, tais que

$$a = bq + r, \text{com } 0 \leq r < b$$

Avalia-se o fato de que $0 < q < a$;

Se $q = 0$, a $= r$, porém $0 \leq r < b$ e a $< b$, o que seria um absurdo;

Se $q > 0$, como $a = bq + r$, então $a > q$, pois $a \geq b$;

O caso de $q < 0$ não poderia ocorrer, uma vez que $0 < a < b$. Daí, tem-se que $0 < q < a$.

Como $0 < q < a$, pela hipótese de indução, segue-se que existem números inteiros $k \geq 0$ e $0 \leq r_1, r_2, \ldots, r_{k+1} < b$, com $r_k \neq 0$, univocamente determinados, tais que

$$q = r_1 + r_2 b + \ldots + r_{k+1} b^k.$$

Levando em conta as igualdades dadas acima, tem-se que

$$a = bq + r = b\left(r_1 + r_2\ b + \ldots + r_{k+1}\ b^k\right) + r$$

donde o resultado segue pondo $r_0 = r$ e $n = k + 1$. □

Temos então, pelo teorema, a expansão relativa à base b. Se $b = 2$, temos a expansão binária; se $b = 10$, teremos a expansão decimal.

3.3 Divisão envolvendo números inteiros

Antes, apresenta-se o teorema de Eudoxius, presente na obra de José Plinio, Introdução à teoria dos números (página 4) (SANTOS, 2006), sem demonstração e, também a de Ulisses Parente em O Algoritmo de Euclides estendido (página 2) (PARENTE, 2022); chave para a demonstração da divisão euclidiana.

Teorema 4 (O teorema de Eudoxius)**.** *Dados a e b inteiros com b não nulo, então a é múltiplo de b ou se encontra entre dois múltiplos consecutivos de b, isto é, correspondendo a cada par de inteiros a e $b \neq 0$ existe um inteiro q tal que, para $b > 0$,*

$$qb \leq a < (q + 1)b$$

e para $b < 0$,

$$qb \leq a < (q - 1)b$$

Demonstração. Se $b|a$, tem-se que $a = bq$, para q inteiro e a prova conclui.

Suponha $a \geq 0$ (o caso $a < 0$ pode ser tratado de modo análogo) e considere o número racional $\dfrac{a}{b}$, com $b > 0$.

O fato do conjunto dos números naturais ser ilimitado superiormente garante a existência de um número natural maior do que $\frac{a}{b}$. Consideremos n, o menor possível maior do que $\frac{a}{b}$. Porém a minimalidade de n garante que $\frac{a}{b} < n-1$ é falso. Dessa forma

$$n-1 \leq \frac{a}{b} < n$$

Considerando $n-1 = q$, tem-se que $n = q+1$. Dessa forma:

$$n-1 \leq \frac{a}{b} < n \Rightarrow q \leq \frac{a}{b} < q+1 \Rightarrow qb \leq a < (q+1)b$$

Mas, se $b < 0$ com $a \geq 0$, tem-se o número racional $\frac{a}{b} < 0$.

Considere n inteiro, tal que $n \leq \frac{a}{b}$, sendo n o maior possível. Como n é negativo e pelo Principio da Boa Ordenação e Corolário 1 (adaptado), não existe nenhum inteiro entre n e $n-1$. Dessa forma $\frac{a}{b} < n-1$.

Assim,

$$n \leq \frac{a}{b} < n-1 \Rightarrow n.b \leq a < (n-1).b$$

Chamando n de q concluímos a prova.

Para $b < 0$ e $a \leq 0$ tem-se o número racional $\frac{a}{b} > 0$. E a prova é análoga a primeira parte da prova já demonstrada. □

Exemplo 7. *Se $a = 11$ e $b = 4$, deve-se tomar $q = 2$, pois $2 \times 4 \leq 11 \leq 3 \times 4$.*

Para $a = -11$ e $b = 4$, toma-se $q = -3$, pois $-3 \times 4 \leq 11 \leq (-3+1) \times 4$.

Para $a = -11$ e $b = -4$, toma-se $q = 3$, pois $3 \times (-4) \leq 11 \leq (3-1) \times (-4)$.

3.3.1 O algoritmo da divisão

O algoritmo da divisão ensinada na educação básica, nas séries intermediarias do Ensino Fundamental, será aqui apresentada, tendo como base o teorema de Eudoxius.

Teorema 5. *Dados dois números inteiros a e b, $b > 0$, existe um único par de inteiros q e r tais que*

$$a = qb + r, \text{com } 0 \leq r < b$$

(q é chamado de quociente e r de resto da divisão de a por b).

Demonstração. Utilizando o teorema de Eudoxius, com $b > 0$, existe q satisfazendo:

$$qb \leq a < (q+1)b$$

somando - qb em todas as partes da desigualdade, tem-se:

$$0 \leq a - qb < b.$$

Desta forma, define-se $r = a - qb$, tem-se garantida a existência de q e r.

Afim de mostrar a unicidade, suponha-se a existência de outro par q_1 e r_1 verificando:

$$a = q_1\ b + r_1 \,\text{com}\, 0 \leq r_1 < b$$

tem-se que:

$$\begin{gathered}(qb + r) - (q_1\ b + r_1) = 0 \\ b\,(q - q_1) + (r - r_1) = 0 \\ b\,(q - q_1) = r_1 - r\end{gathered}$$

Isto mostra que $b \mid (r_1 - r)$.

Como $r_1 <$ b e $r < b$, tem-se então $|r_1 - r| < b$.

Mas $b \mid (r_1 - r)$, então se deve ter $r_1 - r = 0$, o que implica $r_1 = r$. Logo $q_1 b = qb$, portanto $q_1 = q$, uma vez que b é não nulo. □

Exemplo 8. *Dados a, n naturais, com $a > 2$ e ímpar, determinar a paridade de* $\dfrac{a^n - 1}{2}$.

Demonstração. Fazendo a prova, por indução de que $a^n - 1$ é par para a é ímpar. Consideremos k natural, temos que a ímpar é da forma $a = 4k + 1$. Para $n = 1$, tem-se que

$a^1 - 1 = 4k$.

Suponha que para a ímpar se tenha $a^n - 1$ par.

Dessa forma,

$a^{n+1} - 1 = a^{n+1} - a + a - 1 = a.(a^n - 1) + a - 1$ é par.

Portando, pelo Principio de indução, para a ímpar $a^n - 1$ é par.

Como a é ímpar, tem-se que $a^n - 1$ é par e, portanto $\dfrac{a^n - 1}{2}$ é um número natural.

$$\frac{a^n - 1}{2} = \frac{a - 1}{2}\left(a^{n-1} + \ldots + a + 1\right)$$

Sendo a ímpar, tem-se $a^{n-1} + \ldots + a + 1$ é par ou ímpar, segundo n par ou ímpar.

Dessa forma a analise reduz-se a identificar a paridade de $\frac{(a-1)}{2}$.

Sendo a ímpar, ele é da forma $4k+1$ ou $4k+3$. Se $a = 4k+1$, então $\frac{(a-1)}{2}$ é par, enquanto que, se $a = 4k+3$, $\frac{(a-1)}{2}$ é ímpar.

Assim, tem-se que $\frac{a^n - 1}{2}$ é par se, e somente se, n é par ou a é da forma $4k+1$. □

Exemplo 9. *Achar os múltiplos de 5 que se encontram entre 1 e 253.*

Solução:

Pelo algoritmo da divisão, tem-se que $253 = 5.50 + 3$, onde 50 é o quociente da divisão de 253 por 5. Daí, nota-se que os múltiplos de 5 que cabem em 253 totalizam 50 números.

A saber,

$$1 \cdot 5, 2 \cdot 5, 3 \cdot 5, \ldots, 50 \cdot 5$$

Exemplo 10. *Ache o quociente e o resto da divisão de 38 por 7.*

Solução : Sabendo que $35 = 7 \cdot 5$, então o quociente de 38 por 7 será 5 e o resto será 3 .

3.4 O máximo divisor comum

O máximo divisor comum de dois números inteiros a e b (a ou b diferente de zero), denotado por

$$(a, b)$$

é o maior inteiro d que divide a e b.

Segundo relata o professor Abramo, no seu livro de Aritmética na página 58, a definição dada é essencialmente a definição dada por Euclides nos Elementos e constitui-se em um dos pilares da sua aritmética.

Propriedades de $(a, b) = d$, para um número inteiro $d \geq 0$:

I) d é um divisor comum de a e b, e

II) d é divisível por todo divisor comum de a e b.

Teorema 6. *Seja d o máximo divisor comum de a e b, então existem inteiros n e m tais que $d = na + mb$.*

Demonstração. Considere S o conjunto de todas as combinações lineares $\{xa + yb\}$, onde x e y são inteiros. Escolha n e m, tais que $c = na + mb$ seja o menor inteiro positivo pertencente a S (notemos que S possui tanto números negativos, positivos como o zero). Prova-se que $c|a$ e $c|b$. Como as demonstrações são análogas, mostra-se apenas $c|a$. A prova será por contradição. Suponha-se que c não divida a. Neste caso, pelo teorema do algoritmo da divisão, existem q e r tais que $a = qc + r$ com $0 < r < c$. Portanto $r = a - qc = a - q(na + mb) = (1 - qn)a + (-qm)b$.

Isto mostra que r pertence ao conjunto S, pois $(1 - qn)$ e $(-qm)$ são inteiros, o que é uma contradição, uma vez que $0 < r < c$ e c é o menor elemento positivo de S. Logo $c|a$ e de forma análoga se prova que $c|b$.

Como d é um divisor comum de a e b, existem inteiros k_1 e k_2 tais que $a = k_1 d$ e $b = k_2 d$ e, portanto, $c = na + mb = nk_1 d + mk_2 d = (nk_1 + mk_2)d$ o que implica que $d|c$. Como d e c são ambos positivos, tem-se que $d \leq c$ e como $d < c$ não é possível, uma vez que d é o máximo divisor comum, concluí-se que $d = na + mb$. □

Teorema 7. *O máximo divisor comum d de a e b é o divisor positivo de a e b o qual é divisível por todo divisor comum.*

Demonstração. Do teorema anterior e pela Proposição 9, concluí-se que d_1 é divisor comum de a e b, então $d_1 \mid d$. Portanto não pode existir dois números tendo cada um a propriedade de ser divisível por todo divisor comum. Isto por causa do teorema anterior e da Proposição 8 (item vii), no caso dos números positivos d_1 e d, nos diz que d_1 deve ser igual a d. □

Lema 1. *Sejam a, b, n inteiros. Se existe $(a, b - na)$, então, (a, b) existe e*

$$(a, b) = (a, b - na)$$

Demonstração. Seja $d = (a, b-na)$. Como $d|a$ e $d|(b-na)$, segue que d divide $b = b-na+na$. Assim, d é um divisor comum de a e b. Supondo que c seja um divisor comum de a e b, então c será um divisor comum de a e $b - na$ e, portanto, c divide d. Logo $d = (a, b)$. □

Proposição 14. *Para todo inteiro positivo t, $(ta, tb) = t(a, b)$.*

Demonstração. Pelo Teorema 5, (ta, tb) é o menor valor positivo de $mta + ntb$, para m, n inteiros, que é igual a t vezes o menor valor positivo de $ma + nb = t \cdot (a, b)$. □

Corolário 3. *Dados a, b inteiros não ambos nulos, tem-se que*

$$\left(\frac{a}{(a,b)}, \frac{b}{(a,b)}\right) = 1$$

Demonstração. Pela proposição anterior (Proposição 14), tem-se que

$$\text{(a, b)} \left(\frac{a}{(a,b)}, \frac{b}{(a,b)}\right) = \left((a,b)\frac{a}{(a,b)}, (a,b)\frac{b}{(a,b)}\right) = (a,b)$$

O que prova o resultado. □

Enuncia-se a definição de números primos (que será realizado apresentação de maneira suscinta e melhorada em momento oportuno).

Definição 2. *Dois números inteiros, a e b, são ditos primos entre si, ou coprimos, se $(a,b) = 1$.*

Proposição 15. *Dois números inteiros a e b são primos entre si se, e somente se, existem números inteiros m e n tais que $ma + nb = 1$.*

Demonstração. Suponha que a e b sejam coprimos. Tem-se então que $(a,b) = 1$. De posse do Teorema 5, existem números inteiros m e n tais que,

$$ma + nb = (a,b) = 1$$

Reciprocamente, suponha que existam números inteiros m, n tais que

$$ma + nb = 1$$

Se $d = (a,b)$, tem-se que $d \mid (ma + nb)$, o que mostra que $d \mid 1$ e, portanto, $d = 1$. □

Teorema 8. *(Lema de Gaus) Sejam a, b e c números inteiros. Se $a|bc$ e $(a,b) = 1$, então $a|c$.*

Demonstração. Se $a \mid bc$, então existe um inteiro k tal que $bc = ka$.

Se $(a,b) = 1$, então pela Proposição 15, tem-se que existem m, n inteiros, tais que $ma + nb = 1$.

Multiplicando por c ambos os membros da igualdade dada acima, tem-se:

$$(ma + nb)c = 1 \cdot c$$
$$mac + nbc = c$$

Substituindo bc por ak, tem-se

$$mac + nak = (mc + nk)a = c$$

e, portanto $a|c$. □

Teorema 9. *Se a e b são inteiros e $a = bq + r$, onde q e r são inteiros, então*

$$(a, b) = (b, r).$$

Demonstração. Da relação $a = bq + r$, tem-se que todo divisor de b e r é também um divisor de a (Proposição 3).

Essa mesma relação, escrita na forma $r = a - qb$, diz que todo divisor de a e b é um divisor de r. Portanto o conjunto dos divisores comuns de a e b é igual ao conjunto dos divisores comuns de b e r, o que nos dá o resultado $(a, b) = (b, r)$. □

Proposição 16. *Dados números inteiros $a_1, \ldots, a_n$, não todos nulos, existe o seu mdc e*

$$(a_1, \ldots, a_n) = (a_1, \ldots, (a_{n-1}, a_n)).$$

Demonstração. Usando indução sobre n, para $n > 1$.

Para $n = 2$, nada se tem a provar.

Suponha o resultado válido para n. Provar para $n + 1$, basta mostrar que se d é o mdc de $a_1, \ldots, (a_n, a_{n+1})$, então d é o mdc de $a_1, \ldots, a_n, a_{n+1}$, pois isso provará também a existência.

Seja d o mdc de $a_1, \ldots, (a_n, a_{n+1})$. Logo, $d1$, ..., $d|a_{n-1}$ e $d|(a_n, a_{n+1})$. Portanto, $d|a_1$, ..., $d|a_{n-1}$, $d|a_n$ e $d|a_{n+1}$.

Por outro lado, seja c um divisor comum de $a_1, ..., a_n, a_{n+1}$. Logo, c é um divisor comum de $a_1, \ldots, a_{n-1}$ e (a_n, a_{n+1}) e portanto $c|d$. □

Proposição 17. *Seja a inteiro diferente de 1 e m natural não nulo, tem-se que*

$$\left(\frac{a^m - 1}{a - 1}, a - 1\right) = (a - 1,\ m)$$

Para $m = 1$, temos $\left(\frac{a^1 - 1}{a - 1}, a - 1\right) = (1, a - 1)$.

Demonstração. Suponha $m > 1$. Chamando d o primeiro membro da igualdade, e fazendo uso da relação

$$\frac{a^n - b^n}{a - b} = a^{n-1} + a^{n-2}b + \ldots. + ab^{n-2} + b^{n-1},$$

tem-se:

$$\begin{aligned} d &= \left(a^{m-1} + a^{m-2} + \ldots + a + 1, a - 1\right) \\ &= \left(\left(a^{m-1} - 1\right) + \left(a^{m-2} - 1\right) + \ldots + (a-1) + m, a - 1\right) \end{aligned}$$

Pela Proposição 11, tem-se ainda que:

$$a - 1 \mid \left(\left(a^{m-1} - 1\right) + \ldots + (a-1)\right)$$

Segue-se que $(a^{m-1} - 1) + (a^{m-2} - 1) + \ldots + (a-1) = n(a-1)$, para algum n natural naõ nulo e pelo Lema 1, tem-se que:

$$d = (n(a-1) + m, a - 1) = (a - 1, n(a-1) + m) = (a - 1, m)$$

□

Será realizado algumas aplicações das proposições e teoremas apresentados neste capítulo.

Exemplo 11. $(3, 15) = (3, 15 - 8 \times 3) = (3, 15 - 4 \times 3) = (3, 15 + 7 \times 3) = (3, 15 + 8 \times 3)$, *pelo uso do Lema 1.*

Exemplo 12. $4|(27 \times 20), logo 4 \mid 20$ *uma vez que* $(4, 27) = 1$*, uso do Teorema 7 (o Lema de Gauss).*

Exemplo 13. *Como* $(14, 35) = 7$*, tem-se que* $(14/7, 35/7) = 1$ *pelo Corolário 3*

.

Exemplo 14. *Seja* n *um número natural não nulo, mostre que* $(n, 2n + 1) = 1$*.*

Demonstração. Utilizando o Lema 1, tem-se para qualquer n natural não nulo que

$$(n, 2n + 1) = (n, 1) = 1$$

□

Exemplo 15. *Mostre que* $(a, a^2 + na + b) \mid b$*, quaisquer que sejam* a*,* b*,* n *naturais não nulos.*

Demonstração. De posse do Lema 1, observa-se que

$$\left(a, a^2 + na + b\right) = (a, a(a + n) + b) = (a, b)$$

e que $(a, b)|b$ pela definição de mdc. □

Exemplo 16. *Calcule* $\left(\frac{3^{40}-1}{3^5-1}, 3^5-1\right)$

Solução : Por simplicidade, coloca-se $x = 3^5$.

Usando a Proposição 17, tem-se:

$$\left(\frac{3^{40}-1}{3^5-1}, 3^5-1\right) = \left(\frac{x^8-1}{x-1}, x-1\right) = (x-1, 8) = (242, 8) = 2$$

3.5 O algoritmo de Euclides

Como enuncia o professor Abramo, no livro de Aritmética, na página 60, "O método, chamado de Algoritmo de Euclides, é um primor do ponto de vista computacional e pouco conseguiu-se aperfeiçoa-lo em mais de dois milênios". De fato o algoritmo de Euclides, entre tantas maravilhas do universo da matemática é de uma tamanha engenhosidade e elegância, que mesmo após séculos, o processo é ensinado de geração a geração, sem sofrer grandes mudanças.

Teorema 10. *Sejam $r_0 = a$ e $r_1 = b$ inteiros não negativos, com b não-nulo. Se o algoritmo da divisão for aplicado sucessivamente para se obter*

$$r_j = q_{j+1}r_{j+1} + r_{j+2}, 0 \leq r_{j+2} < r_{j+1}$$

para $j = 0, 1, 2, \ldots, n-1$ e $r_{n+1} = 0$, então $(a, b) = r_n$, o último resto não-nulo.

Demonstração. Aplicando o Teorema 5, do algoritmo da divisão, para dividir $r_0 =$ a por $r_1 = b$, obtendo $r_0 = q_1r_1 + r_2$. Em seguida, divide-se r_1 por r_2, obtendo $r_1 = q_2r_2 + r_3$.

Faz-se este procedimento, sucessivamente, até obter o resto $r_{n+1} = 0$.

Observa-se que em cada passo, o resto é sempre menor do que o anterior e como está se utilizando números inteiros positivos, após um número finito de aplicações do Teorema 5, tem-se resto nulo.

Assim, tem-se a seguinte sequência de equações:

$$\begin{aligned}
r_0 &= q_1r_1 + r_2, 0 < r_2 < r_1 \\
r_1 &= q_2r_2 + r_3, 0 < r_3 < r_2 \\
r_2 &= q_3r_3 + r_4, 0 < r_4 < r_3 \\
&\vdots \\
r_{n-2} &= q_{n-1}r_{n-1} + r_n, 0 < r_n < r_{n-1} \\
r_{n-1} &= q_nr_n + 0
\end{aligned}$$

A última equação listada diz, pelo Teorema 9, que o máximo divisor comum de r_n e r_{n-1} é r_n. A penúltima equação, que este número é igual (r_{n-1}, r_{n-2}). Prosseguindo desta maneira, fazendo aplicação repetida do Teorema 8 , tem-se a sequência:

$$r_n = (r_{n-1}, r_n) = (r_{n-2}, r_{n-1}) = \ldots = (r_1, r_2) = (r_0, r_1) = (a, b)$$

Dessa forma, o máximo divisor comum de a e b é o último resto não nulo da sequência de divisões descrita.

Faz-se a seguir a sistematização do algoritmo descrito no teorema acima, colocando os números num diagrama.

Tabela 1 – Divisão sucessiva

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

Fonte: Produção do próprio autor.

□

Exemplo 17. *Calcule o mdc de 250 por 112.*

Tabela 2 – Divisão

	2	4	3	4
250	112	26	8	2
26	8	2		

Fonte: Produção do próprio autor.

$2 = 26 - 8 \cdot 3$

$8 = 112 - 26 \cdot 4$

$26 = 250 - 112 \cdot 2$

Segue-se que

$$\begin{aligned} 2 &= 26 - (112 - 26 \cdot 4) \cdot 3 \\ &= 26.13 - 112 \cdot 3 \\ &= (250 - 112 \cdot 2) \cdot 13 - 112 \cdot 3 \\ &= 250.13 - 112 \cdot 29 \end{aligned}$$

Tem-se então que $(250, 112) = 2 = 250 \cdot 13 + (-29) \cdot 112$

Observa-se que através do algoritmo de Euclides de trás pra frente, pode-se escrever $2 = (250, 112)$ como múltiplo de 250 mais um múltiplo de 112.

3.6 O mínimo múltiplo comum

Um número inteiro é chamado de múltiplo comum de dois números inteiros dados se ele é múltiplo simultaneamente de ambos os números.

Os números $a.b$ e 0 sempre serão múltiplos comuns de a e b.

Um número inteiro não negativo m é um mínimo múltiplo comum (mmc) dos números inteiros a e b, desde que possua as seguintes propriedades:

(i) m é um múltiplo comum de a e b;

(ii) se c é um múltiplo comum de a e b, então $m|c$.

Se m e m' são dois múltiplos comuns de a e b, de acordo com o item (ii) da definição dada, tem-se que $m = m'$, o que mostra que o mínimo múltiplo comum, se existe, é único.

Mas, se m é o mmc de a e b e, c é um múltiplo comum de a e b, então $m|c$. Portanto, se c é positivo, tem-se que $m \leq c$, mostrando que m é o menor dos múltiplos comuns positivos de a e b.

Denota-se por $[a, b]$ o mínimo múltiplo comum de dois números inteiros positivos a e b.

Proposição 18. *Dados dois números inteiros não negativos a e b, temos que $[a, b]$ existe e $[a, b](a, b) = |ab|$.*

Demonstração. Se $a = 0$ ou $b = 0$, tem-se facilmente que $|ab| = 0$, uma vez que $[a, b] = 0$.

Pondo $m = \frac{ab}{(a,b)}$, tem-se ainda que:

$$m = a\frac{b}{(a,b)} = b\frac{a}{(a,b)}$$

tem-se que $a|m$ e $b|m$. Dessa forma m é um múltiplo comum de a e b.

Considere c um múltiplo comum de a e b; dessa forma, $c = na = n'b$. Segue daí que

$$n\frac{a}{(a,b)} = n'\frac{b}{(a,b)}$$

Pelo Corolário 3, $\dfrac{a}{(a,b)}$ e $\dfrac{b}{(a,b)}$ são coprimos. Segue do Teorema 7, que

$\dfrac{a}{(a,b)}$ divide n', e portanto $m = \frac{a}{(a,b)}b$ divide $n'b$ que é igual a c. □

Corolário 4. *Se a e b são números inteiros primos entre si, então $[a, b] = |ab|$.*

Demonstração. Se a e b são primos entre si, tem-se que $(a, b) = 1$. Da Proposição 18, tem-se trivialmente que $[a, b] = |ab|$. □

Exemplo 18. *o* $[3, 5] = 15$*, uma vez que* $(3, 5) = 1$*.*

Exemplo 19. *Determinar o mmc de 250 e 112.*

Tem-se que $(250, 112) = 2$ e como $|250 \cdot 112| = 28000$

Da Proposição 18, pode-se determinar

$$[250, 112]$$

.

Assim $[250, 112] = \dfrac{28000}{2} = 14000.$

3.7 Os números primos

Nesta seção será feito uma abordagem sucinta sobre números primos, chegando no ponto crucial da aritmética que é o Teorema Fundamental da Aritmética. Até porque os números primos desempenham papel importante na teoria dos números, estando a eles associados inúmeros problemas cujas soluções ainda estão em aberto, mesmo após séculos que foram propostas, fazendo com que esses números sejam enigmáticos.

Definição 3. *Um número natural não nulo que possui como divisores positivos apenas o 1 e a si próprio é chamado de número primo.*

Dados dois números primos p e q e um número inteiro a qualquer, decorre da definição acima os seguintes fatos:

i) se $p|q$, então $p = q$

De fato, como $p \mid q$ e sendo q primo, tem-se $p = 1$ ou $p = q$. Sendo p primo, tem-se que $p > 1$, o que acarreta $p = q$.

ii) se p não divide a, então $(p, a) = 1$.

De fato, se $(p, a) = d$, tem-se que $d \mid p$ e d $\mid a$. Portanto, $d = p$ ou $d = 1$. Mas $d \neq p$, pois p não divide a e, consequentemente, $d = 1$.

Proposição 19. *(Lema de Euclides) Sejam a, b, p inteiros, com p primo. Se* $p|ab$*, então* $p|a$ *ou* $p|b$*.*

Demonstração. Se $p|ab$ e p não divide a, então $p|b$. Mas se p não divide a, tem-se que $(p, a) = 1$ e o resultado segue do Lema de Gauss (Teorema 7). □

Teorema 11. *(Teorema Fundamental da Aritmética) Todo número natural maior do que 1 ou é primo ou se escreve de modo único (a menos da ordem dos fatores) como um produto de números primos.*

Demonstração. Se n é primo não tem o que demonstrar.

Suponha que n seja composto. Seja p_1 ($p_1 > 1$) o menor dos divisores positivos de n. Afirma-se que p_1 é primo. Isto é verdadeiro, pois, caso contrário existiria $p, 1 < p < p_1$ com $p \mid n$, contradizendo a escolha de p_1. Sendo assim, $n = p_1 n_1$.

Se n_1 for primo a prova está completa. Caso contrário, toma-se p_2 como o menor fator de n_1. Pelo argumento anterior, p_2 é primo e, tem-se que $n = p_1 p_2 n_2$.

Repetindo este procedimento, obtem-se uma sequência 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 sequência $p_1, p_2, ..., p_k$ 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 mostrar a unicidade, usa-se indução em n. Para $n = 2$ a afirmação é verdadeira. Assumimdo, então, que ele se verifica para todos os inteiros maiores do que 1 e menores do que n. Prova-se que ela também é verdadeira para n. Se n é primo, não há nada a provar. Supondo, então, que n seja composto e que tenha duas fatorações, isto é,

$$n = p_1 p_2 \ldots p_s = q_1 q_2 \ldots q_r$$

Prova-se então que $s = r$ e que cada p_i é igual a algum q_j. Como p_1 divide o produto $q_1 q_2 \ldots q_r$ ele divide pelo menos um dos fatores q_j. Sem perda de generalidade, supondo que $p_1 \mid q_1$. Assim sendo $\frac{n}{p_1} = p_2 \ldots p_s = q_2 \ldots q_r$. Como $1 < \frac{n}{p_1} < n$, a Hipótese de Indução diz que as duas fatorações são idênticas, isto é, $s = r$ e, a menos da ordem, as fatorações $p_1 p_2 \ldots p_s$ e $q_1 q_2 \ldots q_s$ são iguais. □

Teorema 12. *Se* $n = \prod_{i=1}^{r} p_i^{a_i}$, *o conjunto dos divisores positivos de* n *é o conjunto de todos os números da forma* $\prod_{i=1}^{r} p_i^{c_i}, 0 \leq c_i \leq a_i, i = 1, 2, 3, \ldots, r$.

Demonstração. É de observação imediata que se c_i não estiver no intervalo mencionado, o produto acima não será um divisor de n.

É interessante observar que se denotar a sequência de primos em ordem crescente por $p_1 = 2, p_2 = 3, p_3 = 5, \ldots, p_n =$ enésimo primo, então todo inteiro positivo pode ser escrito na forma

$$n = \prod_{i=1}^{\infty} p_i^{a_i}, a_i \geq 0$$

Os divisores positivos de n são todos os números da forma $\prod_{i=1}^{\infty} p_i^{c_i}, 0 \leq c_i \leq a_i$.

Todos estes produtos são finitos, pois o número de fatores primos de qualquer inteiro é sempre finito. □

Teorema 13. *Se dois inteiros positivos a e b possuem as fatorações*

$$a = \prod_{i=1}^{\infty} p_i^{a_i},\ b = \prod_{i=1}^{\infty} p_i^{b_i}$$

então o máximo divisor comum de a e b é igual a :

$$(a, b) = \prod_{i=1}^{\infty} p_i^{c_i}$$

Onde $c_i = \min\{a_i, b_i\}$.

Demonstração. Para que um produto de fatores primos seja um divisor comum, nenhum expoente c_i de p_i poderá ser maior do que a_i e b_i.

Como se está interessado no maior dos divisores positivos, basta tomar para c_i o menor desses dois. □

4 CONGRUÊNCIA

Um dos assuntos mais férteis da aritmética foi introduzido pelo grande gênio Gauss (1777 - 1825) quando tinha apenas 24 anos de idade no seu livro Disquisitiones Arithmeticae, publicado em 1801. Carl Friedrich Gauss desde criança fora uma criança prodígio. Nasceu em Brunsk em 1777, filho de um trabalhador braçal, que não compreendia muito bem os anseios intelectuais do próprio filho. Conta a história, relatada por Gilberto Garbi, em seu livro O Romance das Equações Algébricas, na página 112,

> Aos 3 anos de idade já corrigira as desastradas contas feitas pelo pai.Aos 9, tendo o professor ordenado à classe que somasse os números de 1 a 100, observou que 1+ 100, 2 + 99, 3 + 98, etc, totalizavam sempre 101. Como o número de tais pares era 50 (com 100 números, formam-se 50 pares), a soma procurada era 101 x 50 = 5050 produto que, aliás, calculou de cabeça. Aos 12 anos discutia os axiomas dos Elementos, aos 13 questionou-se sobre a independência do postulado das paralelas em relação aos demais. Aos 15 percebeu que o postulado das paralelas poderia ser formulado diferentemente do que fizera Euclides, o que daria origem a outros tipos de geometria. Também aos 15 anos elaborou a primeira demonstração rigorosa do teorema geral das potências binomiais, coisa que Newton descobrira indutivamente mas não provara. Estas proezas não tardaram a chegar aos ouvidos do Duque de Brunswick, Ferdinad, que passou a custear os estudos de Gauss nas melhores escolas até seu doutoramento, gesto pelo qual o matemático demonstrou sempre a maior gratidão. (GARBI, 2007)

Com este trecho, pode-se notar o quão brilhante foi Gauss. Inclusive é ainda relatado por Garbi que o tema preferido de Gauss era a Teoria dos Números, inclusive é dele a frase “A Matemática é a Rainha das Ciências e a Teoria dos Números é a Rainha da Matemática”.

Apresenta-se os tópicos relevantes a este capítulo.

Definição 4. *Se a e b são inteiros, diz-se que a é congruente a b módulo m $(m > 0)$ se $m|(a - b)$. Denota-se isto por $a \equiv b \pmod{m}$. Se m não divide $a - b$, dizemos que a é incongruente a b módulo m.*

Exemplo 20. $11 \equiv 3 \pmod{2}$ *pois* $2|(11 - 3)$.

Proposição 20. *Se a e b são inteiros, temos que $a \equiv b \pmod{m}$ se, e somente se, existir um inteiro k tal que $a = b + km$.*

Demonstração. Por definição se $a \equiv b \pmod{m}$, então $m|(a - b)$, o que implica na existência de um inteiro k tal que $a - b = km$, isto é, $a = b + km$.

De forma recíproca, se $a = b + km$ (somando - b em ambos os membros) para algum k inteiro, implica em $a - b = km$, o que evidencia que $m|(a - b)$. Assim $a \equiv b \pmod{m}$. □

Proposição 21. *Se a, b, m e c são inteiros, $m > 0$, as seguintes sentenças são verdadeiras:*

1) $a \equiv a \pmod{m}$

2) Se $a \equiv b \pmod{m}$*, então* $b \equiv a \pmod{m}$

3) Se $a \equiv b \pmod{m}$ *e* $b \equiv c \pmod{m}$*, então* $a \equiv c \pmod{m}$

Demonstração.

1) Como $m|0$, então $m|(a - a)$, o que implica, pela Proposição 16, que $a \equiv a \pmod{m}$.

2) Se $a \equiv b \pmod{m}$, então existe algum inteiro k_1 tal que $a = b + k_1 m$. Dessa forma, tem-se ainda que $b = a - k_1 m$, o que implica pela Proposição 16 que $b \equiv a \pmod{m}$.

3) Se $a \equiv b \pmod{m}$ e $b \equiv c \pmod{m}$, então existem inteiros k_1 e k_2 tais que $a - b = k_1 m$ e $b - c = k_2 m$. Somando membro a membro estas ultimas igualdades, obtem-se:

$a - c = (k_1 - k_2)m$, o que implica $a \equiv c \pmod{m}$. □

Teorema 14. *Se a, b, c e m são inteiros tais que* $a \equiv b \pmod{m}$*, então*

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

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

3) $ac \equiv bc \pmod{m}$

Demonstração. Segue que:

1) Como $a \equiv b \pmod{m}$, temos que $a - b = km$ e, portanto, como $a - b = (a + c) - (b + c)$ temos $a + c \equiv b + c \pmod{m}$.

2) Como $(a - c) - (b - c) = a - b$ e, por hipótese, $a - b = km$ tem-se que

$$a - c \equiv b - c \pmod{m}$$

3) Como $a - b = km$ então $ac - bc = ckm$ o que implica $m|(ac - bc)$ e, portanto,

$$ac \equiv bc \pmod{m}$$

□

Corolário 5. *Para todo n natural, a, b inteiros, se* $a \equiv b \pmod{m}$*, então, tem-se*

$$a^n \equiv b^n \pmod{m}.$$

Demonstração. Usando prova indução em n, tem-se:

Como $a \equiv b \pmod{m}$, tem-se então que $m \mid (a-b)$.

Para $n = 1$, nada a provar.

Considere $n = k$, k natural maior do que 1 . Por hipótese de indução, considere válida $a^k \equiv b^k \pmod{m}$, ou seja, $m \mid \left(a^k - b^k\right)$.

Prova-se para $n = k+1$. Assim:

$$a^{k+1} - b^{k+1} = a^k \cdot a - b^k \cdot b = a^k \cdot a - a^k \cdot a + a^k \cdot a - b^k \cdot b = a^k \cdot (a-b) + b \cdot \left(a^k - b^k\right)$$

Como $m \mid (a-b)$ e, por hipótese de indução, $m \mid \left(a^k - b^k\right)$, então $m \mid \left(a^{k+1} - b^{k+1}\right)$, ou seja, por indução, $a^n \equiv b^n \pmod{m}$ é verdadeira para todo n natural. □

É interessante observar que o Pequeno Teorema de Fermat enuncia-se a seguir, podendo ser provado usando o Corolário 5 apresentado.

"Se p é um número primo e a inteiro, então $a^p \equiv a \pmod{p}$. Além disso, se p não divide a, então $a^{p-1} \equiv 1 \pmod{p}$".

Teorema 15. *Se a, b, c e m são inteiros e* $ac \equiv bc \pmod{m}$*, então* $a \equiv b \pmod{m/d}$*, onde d = (c, m).*

Demonstração. Usando o teorema anterior, tem-se que se $ac \equiv bc \pmod{m}$, implica em $ac - bc = c(a-b) = km$. Dividindo os dois membros por d, temos $(\frac{c}{d})(a-b) = k(\frac{m}{d})$.

Logo,

$$(\frac{m}{d}) | (\frac{c}{d})(a-b)$$

e como $(\frac{m}{d}, \frac{c}{d}) = 1$ tem-se então que

$$(\frac{m}{d}) \mid (a-b)$$

o que implica $a \equiv b \pmod{\frac{m}{d}}$. □

Definição 5. *Se h e k são dois inteiros com* $h \equiv k \pmod{m}$*, diz-se que k é um resíduo de h módulo m.*

Corolário 6. *Sejam a, b, c, m inteiros, com $m > 1$ e $(c, m) = 1$. Tem-se que $ac \equiv bc \pmod{m}$ se, e somente se, $a \equiv b \pmod{m}$.*

Proposição 22. *Sejam a, k, m inteiros, com $m > 1$ e $(k, m) = 1$. Se $a_1, \ldots, a_m$ é um sistema completo de resíduos módulo m, então $a + ka_1, \ldots, a + ka_m$ também é um sistema completo de resíduos módulo m.*

Demonstração. Usando do Corolário 5, para $i, j = 0, \ldots, m-1$, tem-se que:

$$a + ka_i \equiv a + ka_j \pmod{m} \leftrightarrow ka_i \equiv kaa_j \pmod{m} \leftrightarrow a_i \equiv a_j \pmod{m} \leftrightarrow i = j$$

Dessa forma, tem-se que a $+k_1, \ldots, a + ka_m$ são, dois a dois, não congruentes módulo m e, portanto, formam um sistema completo de resíduos módulo m. □

Proposição 23. *Sejam a, b inteiros e $m, n, m_1, \ldots m_r$ inteiros maiores do que 1.*

Tem-se que:

i) se $a \equiv b \pmod{m}$ e $n \mid m$, então $a \equiv b \pmod{n}$;

ii) $a \equiv b \pmod{m}_i$ para qualquer $i \in \{1, 2, \ldots, r\} \leftrightarrow a \equiv b \pmod{\ }[m_1, \ldots, m_r]$;

iii) se $a \equiv b \pmod{m}$, então $(a, m) = (b, m)$.

Demonstração. i) Se $a \equiv b \pmod{m}$, então $m \mid (b - a)$. Como $n \mid m$, segue-se que $n \mid (b - a)$. Dessa forma $a \equiv b \pmod{n}$.

ii) Se $a \equiv b \pmod{m}_i$, para $i = 1, \ldots, r$, então $m_i \mid (b - a)$, para todo i. Sendo $b - a$ um múltiplo de cada m_i segue-se que $[m_1, \ldots, m_r]\,(b - a)$, o que prova que

$$a \equiv b \pmod{\ }[m_1, \ldots, m_r]$$

A reciproca decorre do item i.

iii) Se $a \equiv b \pmod{m}$, então $m \mid (b - a)$ e, portanto $b = a + tm$, com t inteiro. Assim

$$(a, m) = (a + tm, m) = (b, m).$$ □

Será realizado a ilustração com alguns exemplos.

Exemplo 21. *Sejam a, p naturais, com p primo. Mostre que, se $a^2 \equiv 1 \pmod{p}$, então $a \equiv 1 \pmod{p}$ ou $a \equiv -1 \pmod{p}$.*

Demonstração. Tem-se que $a^2 - 1 = (a + 1)(a - 1)$. Se $a^2 \equiv 1 \pmod{p}$, então $a^2 - 1 \equiv 0 \pmod{p}$, o que implica que $p \mid (a^2 - 1)$.

Dessa forma $p \mid (a + 1)$ ou $p \mid (a - 1)$. □

Exemplo 22. *Ache o resto da divisão:*

a) de 7^{10} por 51 ; b) de 2^{100} por 11 ;

Solução :

a) Como $49 \equiv -2 \pmod{51}$. Pois $49 = 7^2$, tem-se ainda que $7^2 \equiv -2 \pmod{51}$.

Dessa forma $7^{10} \equiv (-2)^5 \equiv -32 \equiv 19 \pmod{51}$

Logo o resto da divisão é 19.

b) Tem-se que $2^5 = 32 \equiv -1 \pmod{11}$. Então $2^{100} \equiv (-1)^{20} \equiv 1 \pmod{11}$.

Logo o resto da divisão é 1.

Exemplo 23. *(ENC 98) O resto da divisão de* 12^{12} *por 5 é:*

(A) 0

(B) 1

(C) 2

(D) 3

(E) 4

Solução : Tem-se que $6 \equiv 1 \pmod{5}$ e $4 \equiv -1 \pmod{5}$. Daí então $6^{12} \equiv 1 \pmod{5}$

$2^{12}6^{12} = 12^{12} \equiv 2^{12} \equiv 4^6 \equiv (-1)^6 \equiv 1 \pmod{5}$

Logo, a resposta é a alternativa (B).

5 CRITÉRIOS DE DIVISIBILIDADE

No ensino de matemática do sexto ano do Ensino Fundamental, os critérios de divisibilidade são apresentados como mecanismos simples para identificar quando um número é ou não divisível por outro sem precisar de fato utilizar o algoritmo da divisão. Está previsto na BNCC, como habilidade EF06MA05, já citado na introdução. Tais critérios, de 2 até 10, são explicitados nos mais diversos materiais de apoio didático,inclusive nos livros da coleção (JR, 2022), como macetes simples. Não são apresentados, nos livros didáticos destinados ao público do Ensino Fundamental, provas matemáticas de tais critérios, até mesmo porque o objetivo do presente objeto de conhecimento é apenas apresentar aos estudantes estes critérios, que escondem grandes provas matemáticas, com foco em apenas mostrar resultado de aplicação. O objetivo deste capítulo é apresentar provas aritméticas dos critérios de divisibilidade apresentadas nos materiais didáticos dos livros da Educação Básica.

É importante frisar aqui, que todos os critérios que serão apresentados, o número n natural indicado está escrito na base decimal.

Os enunciados e demonstrações dos critérios que aqui estão tiveram como base de inspiração nas produções de Talyson Paulo da Silva (dissertação)(SILVA, 2019), do José Plinio de Oliveira (Introdução a teoria dos números) (SANTOS, 2006) e do Abramo Hefez (Aritmética)(HEFEZ, 2009).

Definição 6. *Fixado um número natural não nulo d, um critério de divisibilidade é uma condição P necessária e suficiente para que um número natural seja divisível por d, ou seja, um número natural n é divisível por d se, e somente se, a condição P é satisfeita.*

5.1 Critério de divisibilidade por 2

Um número natural $n = a_k a_{k-1} \dots a_2 a_1 a_0$ é divisível por 2 se, e somente se, seu último algarismo pertence ao conjunto $\{0, 2, 4, 6, 8\}$.

Demonstração. Escrevendo o número natural n, na base 10, tem-se:

$$n = a_k \cdot 10^k + a_{k-1} \cdot 10^{k-1} + \ldots + a_2 \cdot 10^2 + a_1 \cdot 10 + a_0$$

pode-se reescrever n como $n = 10.m + a_0$, com m natural, onde $m = a_k \cdot 10^{k-1} + a_{k-1} \cdot 10^{k-2} + \ldots + a_2 \cdot 10 + a_1$

Como 10 é divisível por 2 (o que indica que $10 \cdot m$ será divisível por 2), então n só será divisível por 2 se, e somente se, a_0 for divisível por 2, ou seja, $a_0 \in \{0, 2, 4, 6, 8\}$.

Fazendo a prova, alternativa, utilizando congruência.

Considerando n natural, tal que $n = a_k \cdot 10^k + a_{k-1} \cdot 10^{k-1} + \ldots + a_2 \cdot 10^2 + a_1 \cdot 10 + a_0$, pode-se observar que:

$10 \equiv 0 \pmod 2$, utilizando o Corolário 5 , tem-se que $10^k \equiv 0 \pmod 2$, para k natural.

Dessa forma, tem-se que

$2 \mid n$ se $a_k \cdot 10^k + a_{k-1} \cdot 10^{k-1} + \ldots + a_2 \cdot 10^2 + a_1 \cdot 10 + a_0 \equiv 0 \pmod 2$

isto só ocorre se $2|a_0$. □

Exemplo 24. *O diâmetro da Terra é de 12756 quilômetros, 12756 é divisível por 2?*

Este exemplo ilustra o aspecto dos jovens do sexto ano do Ensino Fundamental, poder a partir do número dado e com as informações do critério de divisibilidade, saber se o dado número é ou não divisível por 2. Como o citado número tem como último algarismo o 6, pelo critério de divisibilidade, o número 12756 é divisível por 2.

Exemplo 25. *O número $n = 123456789$ é divisível por 2?*

A resposta é não. Uma vez que o número n tem como último algarismo o 9, este não é divisível por 2, o que faz com que o dado número n não seja múltiplo de 2.

Exemplo 26. *Considere o número natural $n = 1023456d$. Qual o menor número natural não nulo d podemos ter para que n seja divisível por 2?*

A resposta, de acordo com o critério de divisibilidade por 2 é $d = 2$.

5.2 Critério de divisibilidade por 3 e por 9

O número $n = a_k a_{k-1 \ldots} a_2 a_1 a_0$ é divisível por 3 , respectivamente divisível por 9 , se, e somente se, $a_k + a_{k-1} + \ldots + a_2 + a_1 + a_0$ seja divisível por 3 , respectivamente por 9 .

Demonstração. Considerando o número n dado por

$$n = a_k \cdot 10^k + a_{k-1} \cdot 10^{k-1} + \ldots + a_2 \cdot 10^2 + a_1 \cdot 10 + a_0$$

subtraindo $(a_k + a_{k-1} + \ldots + a_2 + a_1 + a_0)$ dos dois lados da igualdade dada a cima, tem-se:

$n-(a_k+a_{k-1}+\ldots+a_2+a_1+a_0)=a_k\cdot 10^k+a_{k-1}\cdot 10^{k-1}+\ldots+a_2\cdot 10^2+a_1\cdot 10+a_0-(a_k+\ a_{k-1}+\ldots+a_2+a_1+a_0)$

Da Proposição 11, tem-se que $9|(10^k-1)$. Então:

$$n=(a_k+a_{k-1}+\ldots+a_2+a_1+a_0)+9\ m$$

Em que $9m=a_k\cdot\left(10^k-1\right)+\ldots+a_1\cdot(10-1)$. Então n só será divisível por 3 , respectivamente por 9 , se , e somente se, $(a_k+a_{k-1}+\ldots+a_2+a_1+a_0)$ for divisível por 3 , respectivamente por 9.

Usando a linguagem de congruência, como forma alternativa, para demonstração, faz-se observação, inicialmente, dos restos das potências de 10 por 3 e por 9 .

$$\begin{aligned}10^0&\equiv 1 \pmod 3 \text{ ou } \pmod 9\\ 10^1&\equiv 1 \pmod 3 \text{ ou } \pmod 9\\ 10^2&\equiv 1 \pmod 3 \text{ ou } \pmod 9\end{aligned}$$

ou seja, para todo i natural, tem-se

$$10^i\equiv 1 \pmod 3 \text{ ou } \pmod 9$$

Assim, tem-se:

$n=a_k\cdot 10^k+a_{k-1}\cdot 10^{k-1}+\ldots+a_2\cdot 10^2+a_1\cdot 10+a_0\equiv a_k+a_{k-1}+\ldots+a_2+a_1+a_0$ (mod 3) ou (mod 9). □

Exemplo 27. *O diâmetro da Terra é de 12756 quilômetros.12756 é divisível por 3? E por 9?*

Tem-se que $1+2+7+5+6=21$. Como $3|21$, então $3|12756$. Porém 21 não é divisível por 9, logo 12756 não é divisível por 9.

Exemplo 28. *Qual o menor valor d natural se deve ter para que o número $n=1023456d$ possa ser divisível por 3?*

Somando os algarismos de n (a priori não considerando ainda o desconhecido d) tem-se: $1+0+2+3+4+5+6=21$ e $3\mid 21$. Então o menor d natural que se pode ter é $d=0$.

Exemplo 29. *Qual o menor valor d natural se pode ter para que o número $n=1023456\ d$ possa ser divisível por 9 ?*

Observando pelo exemplo anterior, tem-se que $1+0+2+3+4+5+6=21$. Dessa forma o menor natural d somado a 21 para que o número n seja divisível por 9 é $d=6$, uma vez que $21+6=27$ e $9 \mid 27$.

5.3 Critério de divisibilidade por 4

Um número natural $n = a_k a_{k-1} \ldots a_2 a_1 a_0$, com dois ou mais algarismos, é divisível por 4 se, e somente se, o número formado por seus dois últimos algarismos for divisível por 4 ou for 00 .

Demonstração. Conside $n = a_k \cdot 10^k + a_{k-1} \cdot 10^{k-1} + \ldots + a_2 \cdot 10^2 + a_1 \cdot 10 + a_0$.

Reescrevendo n na forma $n = 100m + (10.a_1 + a_0)$, com m natural (m $= a_k.10^{k-2} +$ ... $+ a_2$). Temos que 4|100, dessa forma, n será divisível por 4 se, e somente se $10.a_1 + a_0$ for divisível por 4 , ou seja, 4|n se, e somente se $a_1 a_0$ também for divisível por 4 .

Usando congruência para fazer a demonstração alternativa, tem-se:

$a_k \cdot 10^k + a_{k-1} \cdot 10^{k-1} + \ldots + a_2 \cdot 10^2 = \left(a_k \cdot 10^{k-2} + a_{k-1} \cdot 10^{k-3} + \ldots + a_2\right) \cdot 100$

Como $100 \equiv 0 \pmod 4$ e $10 \equiv 2 \pmod 4$, tem-se pelo Teorema 13, item 1, que:

$$\left(a_k \cdot 10^{k-2} + a_{k-1} \cdot 10^{k-3} + \ldots + a_2\right) \cdot 100 + 10 \cdot a_1 + a_0 \equiv 2a_1 + a_0 \pmod 4$$

Assim, um número n é divisível por 4 se o dobro do algarismo da dezena somado ao algarismo da unidade também for divisível por 4. □

Exemplo 30. *O diâmetro da Terra é de 12756 quilômetros.12756 é divisível por 4?*

Observe que os dois últimos algarismos do número 12756 forma o número 56. E 4|56. Dessa forma o número que representa o diâmetro da Terra é divisível por 4.

De maneira alternativa, temos que o algarismo da ordem das dezenas é o 5 e, como o dobro do algarismo da dezena somado ao algarismo da unidade resulta em 16 (2.5 + 6), podemos concluir que o número 12756 é divisivel por 4.

Exemplo 31. *Qual o menor valor d natural se pode ter para que o número* $n = 1023456d$ *possa ser divisível por 4 ?*

Observe que os dois últimos algarismos do número natural n formam o número $6d$. Como 4|60, logo o menor valor natural de d é zero.

5.4 Critério de divisibilidade por 5 e por 10

Seja $n = a_k a_{k-1...} a_2 a_1 a_0$, um número natural, uma condição necessária e suficiente para que n seja divisível por 5 é que a_o seja 0 ou 5 e para ser divisível por 10 é que a_0 seja 0.

Demonstração. Escrevendo n da seguinte forma:

$$n = a_k \cdot 10^k + a_{k-1} \cdot 10^{k-1} + \ldots + a_2 \cdot 10^2 + a_1 \cdot 10 + a_0$$

Colocando 10 como fator comum, tem-se ainda que:

$$n = 10 \cdot \left(a_k \cdot 10^{k-1} + a_{k-1} \cdot 10^{k-2} + \ldots + a_2 \cdot 10 + a_1\right) + a_0$$

Como 5|10, tem-se que n é divisível por 5 se, e somente se, a_0 é divisível por 5 , ou seja, $a_0 = 0$ ou $a_0 = 5$. Tem-se n divisível por 10 se, e somente se, $a_0 = 0$.

De maneira alternativa, faça-se a prova utilizando congruência.

Tem-se que $10 \equiv 0 \pmod 5$ ou $\pmod{10}$, dessa forma se tem que $a_i \cdot 10^i \equiv 0 \pmod 5$ ou $\pmod{10}$, para todo i natural. Assim

$n = a_k \ldots a_2 a_1 a_0 = a_k \cdot 10^k + a_{k-1} \cdot 10^{k-1} + \ldots + a_2 \cdot 10^2 + a_1 \cdot 10 + a_0 \equiv a_0 \pmod 5$ ou $\pmod{10}$. Logo 5|n ou 10|n se, e somente se, a_o é divisível por 5 ou, respectivamente, por 10.

□

Exemplo 32. *O diâmetro da Terra é de 12756 quilômetros.12756 é divisível por 5? É também divisível por 10 ?*

Percebe-se pelo exposto no critério que o número 12576 não é divisível por 5 e nem por 10, pois o último algarismo do número dado é o 6 .

Exemplo 33. *Qual o menor valor d natural se pode ter para que o número $n = 1023456d$ possa ser divisível por 5? E por 10?*

Observa-se que o menor d natural para que n seja divisível por 5 e por 10 é $d = 0$.

5.5 Critério de divisibilidade por 6

O número natural $n = a_k a_{k-1} \ldots a_2 a_1 a_0$, será divisível por 6 se, e somente se, n for divisível simultaneamente por 2 e por 3.

Demonstração. Considere n natural da forma $n = 6\ m$, com m inteiro. Decorre do Teorema Fundamental da Aritmética que $6 = 2 \cdot 3$ (produto de fatores primos).

Dessa forma:

$$n = 6\ m = 2 \cdot (3\ m)$$

Fazendo com que $3\ m = x$, tem-se ainda que $n = 2x$, para x natural; então $2|n$. De forma análoga

$$n = 6\ m = 3 \cdot (2\ m)$$

Fazendo com que $2\ m = y$, então $n = 3y$, para y natural; então $3|n$.

Dessa forma, se n é divisível por 6, então n será divisível simultaneamente por 2 e por 3.

De outra forma, suponha que n seja divisível simultaneamente por 2 e por 3. Para o caso de $2 \mid n$, então existe x_1 natural tal que $n = 2x_1$. Observe que $3-2 = 1$, multiplicando ambos os membros desta igualdade por x_1 tem-se:

$(3-2)x_1 = x_1 \rightarrow 3x_1 - 2x_1 = x_1 \rightarrow 3x_1 - n = x_1 (i)$

Como $3|n$, então existe x_2 natural tal que $n = 3x_2$ (ii).

Por (i) e (ii) tem-se que:

$$3x_1 - n = x_1$$
$$3x_1 - 3x_2 = x_1$$
$$3\,(x_1 - x_2) = x_1$$

Fazendo $y = x_1 - x_2$, com $x_1 - x_2 \geq 0$, então $x_1 = 3y$, para y natural.

Logo,

$$n = 2x_1 = 2.3y = 6y, \text{ com y natural}$$

o que garante que n é divisível por 6 . □

Usando congruência, apresenta-se o critério de divisibilidade por 6, com uma outra característica, a ser enunciado a seguir:

Um número natural $n = a_k \cdot 10^k + a_{k-1} \cdot 10^{k-1} + \ldots + a_2 \cdot 10^2 + a_1 \cdot 10 + a_0$

é divisível por 6 se, e somente se, a soma do algarismo da unidade com o quádruplo de cada um dos outros algarismos é divisível por 6.

Demonstração. Consideremos o natural n dado por $n = a_k \cdot 10^k + a_{k-1} \cdot 10^{k-1} + \ldots + a_2 \cdot 10^2 + a_1 \cdot 10 + a_0$.

Observa-se que:

$$10 \equiv 4 \pmod 6$$
$$10^2 \equiv 4^2 \pmod 6 \equiv 4 \pmod 6$$
$$\vdots$$
$$10^k \equiv 4^k \pmod 6 \equiv 4 \pmod 6$$

Daí, tem-se ainda que:

$$n = a_k \cdot 10^k + a_{k-1} \cdot 10^{k-1} + \ldots + a_2 \cdot 10^2 + a_1 \cdot 10 + a_0 \equiv 4 \cdot (a_k + \ldots + a_2 + a_1) + a_0 \pmod 6$$

Então 6|n se, e somente se, 4. $(a_k + \ldots + a_2 + a_1) + a_0 \equiv 0 \pmod 6$. □

Exemplo 34. *O diâmetro da Terra é de 12756 quilômetros. 12756 é divisível por 6?*

Viu-se este exemplo nos critérios por 2 e por 3, e observou-se que o número 12756 é simultaneamente divisível por 2 e por 3, portanto este número é divisível por 6 . Utilizando o processo alternativo, demonstrado utilizando congruência, tem-se que: $4 \cdot (1 + 2 + 7 + 5) + 6 = 4 \cdot 15 + 6 = 66$ que é divisível por 6 , portanto 12756 é divisível por 6.

5.6 Critério de divisibilidade por 7

Apesar do critério de divisibilidade por 7 não ser explorado na maioria dos materiais didáticos destinado ao ensino de matemática no Ensino Fundamental, sempre que o assunto critério de divisibilidade é explorado, surgem as inquietações sobre a existência de critério de divisibilidade por 7. Nesta seção aborda-se tal critério, não apenas para dar continuidade a abordagem do tema na sequencia apresentada, mas também como um estimulo sobre um critério de divisibilidade não usual.

Apresenta-se o critério, com uma ilustração. Considere um número natural n dado por $n = 8652$. Separa-se o algarismo 2, das unidades, e do número restante 865 subtraí-se o dobro deste algarismo, ou seja,

$$865 - 4 = 861$$

Repete-se este procedimento, tantas vezes quando possível, de tal forma que se tenha um número que seja facilmente identificável sua divisibilidade (ou não) por 7.

$$86 - 2 = 84$$

Como $7|84$, pois $7 \cdot 12 = 84$, então o número $n = 8652$ é divisível por 7 .

Considere i o algarismo das unidades do número n, então n pode ser escrito como $10k + i$. (No exemplo citado tem-se $k = 865$ e $i = 2$). No procedimento descrito acima se obteve um número r como sendo $k - 2i$. Com base nestas observações, será suficiente provar que os números $10k + i$ e $k - 2i$ são tais que, se um deles é múltiplo de 7, o outro também é. Prova-se a equivalência:

$$10k + i \text{ é múltiplo de } 7 \Leftrightarrow k - 2i \text{ é múltiplo de } 7$$

Demonstração. ($\Rightarrow$) Se $10k+i$ é múltiplo de 7, então existe um inteiro m tal que $10k+i = 7m$ e, portanto, $k - 2i = k - 2(7m - 10k) = k - 14m + 20k = 21k - 14\ m = 7(3k - 2m)$, o que implica k - 2i ser múltiplo de 7.

($\Leftarrow$) Se $k-2i$ é múltiplo de 7 , então existe n inteiro, tal que $k-2i = 7n$ e portanto,

$$10k + i = 10(7n + 2i) + i = 70n + 20i + i = 70n + 21i = 7(10n + 3i)$$

O que implica $10k + i$ ser múltiplo de 7 .

□

No exemplo citado, como 84 é divisível por 7, então 861 também o é. Sendo 861 divisível por 7, então 8652 também é divisível por 7.

Exemplo 35. *O diâmetro da Terra é de 12756 quilômetros.12756 é divisível por 7?*

Utilizando o procedimento apresentado, tem-se que o algarismo das unidades é o 6 , como o dobro de 6 é 12, tem-se que:

$$1275 - 12 = 1263$$

Na operação obtida, tem-se que o algarismo das unidades é o 3, cujo dobro é 6. Dessa forma:

$$126 - 6 = 120$$

Usando novamente o procedimento supracitado, tem-se que o dobro de zero é zero. Assim:

$$12 - 0 = 12$$

Como 12 não é divisível por 7, então o número 12756 não é divisível por 7.

5.7 Critério de divisibilidade por 8

Um número natural $n = a_k..a_3a_2a_1a_0$, com mais de três algarismos, é divisível por 8 se, e somente se, o número formado por seus três últimos algarismos for divisível por 8 .

Demonstração. Consideremos $n = a_k \cdot 10^k + a_{k-1} \cdot 10^{k-1} + \ldots + a_2 \cdot 10^2 + a_1 \cdot 10 + a_0$, colocando 10^3 como fator comum, no número n decomposto, a partir do algarismo posicionado na quarta ordem, tem-se:

$n = 10^3 \cdot \left(a_k 10^{k-3} + \ldots + a_3\right) + a_2 \cdot 10^2 + a_1 \cdot 10 + a_0 = 10^3 \cdot x + a_2 \cdot 10^2 + a_1 \cdot 10 + a_0$

sendo $x = a_k \cdot 10^{k-3} + \ldots + a_3$, para x natural.

Como $10^3 < 10^4 < 10^5 < \ldots < 10^k$. Tem-se que $8 \mid 10^3$, segue então que n será divisível por 8 se, e somente se, $a_2 \cdot 10^2 + a_1 \cdot 10 + a_0$ for divisível por 8 , ou seja, se os últimos três algarismos for divisível por 8 .

Usando a congruência, pode-se demonstrar de forma alternativa, o critério de divisibilidade por 8 , como se vê a seguir.

$$\begin{aligned} 10^0 &\equiv 1 \pmod 8 \\ 10 &\equiv 2 \pmod 8 \\ 10^2 &\equiv 4 \pmod 8 \\ 10^3 &\equiv 0 \pmod 8 \\ 10^4 &\equiv 0 \pmod 8 \\ &\vdots \\ 10^k &\equiv 0 \pmod 8, \text{ para } k > 2. \end{aligned}$$

Assim sendo,

$$n = a_k \cdot 10^k + a_{k-1} \cdot 10^{k-1} + \ldots + a_2 \cdot 10^2 + a_1 \cdot 10 + a_0 \equiv 0 + \ldots + 0 + a_2a_1a_0 \pmod 8$$

Dessa forma $8|n$ se, e somente se, $a_2a_1a_0 \equiv 0 \pmod 8$.

Observando o número n dado na forma decomposta, pode-se ter ainda que:

$$a_k \cdot 10^k + a_{k-1} \cdot 10^{k-1} + \ldots + a_3 \cdot 10^3 = \left(a_k \cdot 10^{k-3} + \ldots + a_3\right) \cdot 10^3$$

Como $10^3 \equiv 0 \pmod 8, 10^2 \equiv 4 \pmod 8$ e $10 \equiv 2 \pmod 8$, tem-se que

$$\left(a_k \cdot 10^{k-3} + \ldots + a_3\right) \cdot 10^3 + a_2 10^2 + a_1 10 + a_0 \equiv 4a_2 + 2a_1 + a_0 \pmod 8$$

□

Conclui-se, por congruência, que um número n é divisível por 8 se a soma do quádruplo do algarismo da centena com o dobro do algarismo da dezena com o algarismo da unidade também o for.

Exemplo 36. *O diâmetro da Terra é de 12756 quilômetros.12756 é divisível por 8?*

Observa-se que os três últimos algarismos do número dado é 756. Utilizando o procedimento demonstrado usando congruência, tem-se ainda que:

$$4 \cdot 7 + 2 \cdot 5 + 6 = 28 + 10 + 6 = 44$$

Como 44 não é divisível por 8, então 12756 não é divisível por 8.

Exemplo 37. *Qual o menor valor d natural se pode ter para que o número* $n = 1023456d$ *possa ser divisível por 8?*

Observa-se que os três últimos algarismos do número n dado é 56d. Utilizando o procedimento abordado na prova usando congruência, tem-se que:

$$4 \cdot 5 + 2 \cdot 6 + d = 20 + 12 + d = 32 + d$$

Assim sendo, se $d = 0$, tem-se o resultado acima igual a 32 e $8|32$, logo $n = 10234560$ é divisível por 8.

Exemplo 38. *Verifique se o número 1234120 é divisível por 8.*

De fato, os três últimos algarismos do número dado forma o número 120, como $8|120$, então 1234120 é divisível por 8.

5.8 Critério de divisibilidade por 11

Para encerrar as provas aritméticas dos critérios de divisibilidade apresentados na grande maioria do material didático utilizado no ensino de matemática no Ensino Fundamental, será abordado o critério de divisibilidade por 11. Assim como o critério de divisibilidade por 7, o do 11 é também não usual.

Um número natural $n = a_k a_{k-1} \dots a_2 a_1 a_0$ é divisível por 11 se, e somente se, $a_0 - a_1 + a_2 - a_3 + ...$ for divisível por 11.

Demonstração. Usando congruência, tem-se que $10 \equiv -1 \pmod{11}$, pelo Corolário 5 , tem-se $10^{2i} \equiv 1 \pmod{11}$ e $10^{2i+1} \equiv -1 \pmod{11}$.

Assim, para $n = a_k a_{k-1} \dots a_4 a_3 a_2 a_1 a_0$, tem-se que:

$$\begin{gathered} a_0 \equiv a_0 \pmod{11} \\ a_1 \cdot 10 \equiv -a_1 \pmod{11} \\ a_2 \cdot 10^2 \equiv a_2 \pmod{11} \\ a_3 \cdot 10^3 \equiv -a_3 \pmod{11} \\ \vdots \\ a_k 10^k \equiv (-1)^k a_k \pmod{11} \end{gathered}$$

Dessa forma se encontra:

$$n = a_k \cdot 10^k + a_{k-1} \cdot 10^{k-1} + \ldots + a_2 \cdot 10^2 + a_1 \cdot 10 + a_0 \equiv (-1)^k a_k + \ldots - a_3 + a_2 - a_1 + a_0 \pmod{11}$$

Segue que,

$$(-1)^k a_k + \ldots - a_3 + a_2 - a_1 + a_0 \pmod{11} \equiv \sum_{i=0}^{k} (-1)^i a_i \pmod{11}$$

ou seja, $11|n$ se, e somente se, $a_0 - a_1 + a_2 - a_3 + ...$ for divisível por 11. □

Exemplo 39. *O diâmetro da Terra é de 12756 quilômetros.12756 é divisível por 11? Usando o critério de divisibilidade por 11, tem-se que:*

$$6 + 7 + 1 = 14 \ e \ 5 + 2 = 7$$

Como $14 - 7 = 7$, concluí-se que 12756 não é divisível por 11 .

Exemplo 40. *verifique se o número* $n = 52345678$ *é divisível por 11 .*

Como $8+6+4+2=20$ e $7+5+3+5=20$ e $20-20=0$, tem-se que 0 é divisível por 11, portanto o número $n=52345678$ é divisível por 11 .

Apresenta-se outras ilustrações que podem ser resolvidas com os assuntos abordados neste trabalho.

Exemplo 41. *Considere o número natural $n=2^{60}$. Verifique se n é divisível por 3, 5, 6, 7 e 8. E nos casos em que n não for divisível, identifique o resto da divisão.*

Solução : Verifica-se por 3. Como $2^2 \equiv 1 \pmod 3$, pelo Corolário 5 , tem-se que:

$$\left(2^2\right)^{30} \equiv 1^{30} \pmod 3 \rightarrow 2^{60} \equiv 1 \pmod 3$$

Logo 2^{60} não é divisível por 3 e o resto na divisão é 1 .

Faça-se a verificação por 5. Como $2^2 \equiv -1 \pmod 5$, pelo Corolário 5, tem-se que:

$$\left(2^2\right)^{30} \equiv (-1)^{30} \pmod 5 \rightarrow 2^{60} \equiv 1 \pmod 5.$$

Logo 2^{60} não é divisível por 5 e o resto na divisão é 1.

Testando por 7 , tem-se que $2^3 \equiv 1 \pmod 7$, pelo Corolário 5 , tem-se que:

$$\left(2^3\right)^{20} \equiv 1^{20} \pmod 7 \rightarrow 2^{60} \equiv 1 \pmod 7.$$

Logo 2^{60} não é divisível por 7 e o resto na divisão é 1 .

E por fim, verificando por 8, tem-se que $2^3 \equiv 0 \bmod 8$, pelo Corolário 5 , tem-se que:

$$\left(2^3\right)^{20} \equiv 0^{20} \pmod 8 \rightarrow 2^{60} \equiv 0 \pmod 8$$

Logo 2^{60} é divisível por 8.

Exemplo 42. *Mostre que $a^{13}-a$ é divisível por 2, 3, 5 e 7, para todo a inteiro.*

Demonstração. Tem-se que $a^{13}-a=a\left(a^{12}-1\right)$ é divisível por 2 pois possuem a mesma paridade.

Do Pequeno Teorema de Fermat, enunciado após prova do Corolário 5, tem-se que:

$$a^3 \equiv a \pmod 3 \rightarrow a^4 \equiv a^2 \pmod 3$$

Então

$$a^{13} = \left(a^4\right)^3 a \equiv \left(a^2\right)^3 a \equiv \left(a^3\right)^2 a \equiv a^3 \equiv a \pmod 3$$

Ainda pelo Pequeno Teorema de Fermat, tem-se que $a^5 \equiv a \bmod 5$. Dessa forma

$$a^{13} \equiv a^5 \cdot a^5 \cdot a^3 \equiv a \cdot a \cdot a^3 = a^5 \equiv a \pmod 5.$$

De forma semelhante pelo Pequeno Teorema de Fermat, tem-se $a^7 \equiv a \bmod 7$. Logo

$$a^{13} \equiv a^7 \cdot a^6 \equiv a \cdot a^6 = a^7 \equiv a \pmod 7$$

□

6 CURIOSIDADES E MACETES

Nesta seção será apresentado algumas curiosidades, tais como a prova dos nove e o calendário. Ambos utilizam conceitos desenvolvidos em criterio de divisibilidade e de congruência. Interessante observar que em ambos os temas elencados, o primeiro é abordado no ensino das quatros operações fundamentais enquanto o segundo nos assuntos de divisibilidade, ambos no Ensino Fundamental. A prova dos noves confere para o estudante como uma ferramenta adicional de testagem do resultado obitido no processo aritmético, ainda nos anos iniciais do Ensino Fundamental. Já o calendário, como uma questão curiosa para identificar, além de verificação se dado ano foi ou não bissexto, de saber qual dia da semana caiu determinada data.

Um fato histórico sobre o calendário, é que o formato que nós conhecemos, nem sempre foi assim. Segundo conta (HEFEZ, 2009) "Desde o tempo do imperador romano Júlio César até o ano de 1482 vigorava no mundo ocidental o calendário juliano, nome dado em homenagem ao imperador que o havia instituido, e que estimava a duração do ano em 365,25 dias, segundo as mediações realizadas pelos egípcios em cerca de 300 a.C". Utilizando métrica mais apurada na duração do ano, a diferença entre as duas medidas resultava em um dia a menos a cada 128 anos. O papa Gregorio XIII, no ano de 1482, publica uma bula no dia 24 de fevereiro do referido ano, instituindo um novo calendário,que passaria a vigorar a partir de 5 de outubro do mesmo ano, pois já havia uma diferença de 10 dias entre o calendário juliano e o ciclo solar.

Os pontos principais da bula papal eram:

a) O dia seguinte ao dia 4 de outubro (quinta-feira), do calendário juliano, no novo calendário, seria o dia 15 de outubro (sexta-feira).

b) A cada quatro anos, nos anos múltiplos de 4, haveria um ano bissexto, com excessão dos anos dos centenários (anos múltiplos de 100) que só seriam bissextos se fossem múltiplos de 400.

c) O início do ano passou a ser o primeiro de janeiro, os meses alternariam com 31 e 30 dias, a começar com janeiro com 31 dias, exceto fevereiro que teriam normalmente 28 dias e 29 dias nos anos bissextos. O mês de agosto teria 31 dias.

A diferença na contagem dos anos bissextos nos anos centenários foi introduzida para corrigir uma pequena diferença que ainda sobra após a introdução dos anos bissextos.

Será realizado a exploração desses dois pontos curiosos nas seções a seguir.No qual o segundo (o calendário) será apresentado algumas proposições que auxiliam na compreensão do assunto.

6.1 A prova dos nove

Este é um teste que pode ser realizado nas quatro operações fundamentais com o intuito de identificar erros nos processos operatórios. Por exemplo, o produto de 4.5 é 20. Com o objetivo de verificar a exatidão do resultado, questiona-se: e "os noves"fora? Nesse caso o objetivo dessa pergunta é tirar do número o maior multiplo de nove nele contido, ou basicamente identificar o resto da divisão do dado número por nove. Por simplicidade, aquele que está operando, pode "somar os algarismos"do número obtido como resultado da operação dada e em seguida retirar do resultado o maior múltiplo de nove. No exemplo $4.5 = 20$, podemos observar facilmente que o maior múltiplo de nove contido no resultado é o 18 ($= 2.9$) então "os noves"fora resulta em 2, pois $20 - 18 = 2$. De maneira alternativa, facilmente identificamos que no resultado 20, a soma dos algarismos resulta em 2 ($= 2 + 0$).

Com esta ilustração, utilizando a multiplicação como operação selecionada, considera-se:

Suponha efetuando a multiplicação $a.b$, obtendo o resultado c, cuja exatidão se quer verificar. Dessa forma, considerando os números naturais a e b, na base 10, tal que:

$a = a_k a_{k-1}...a_1 a_0$, $b = b_l b_{l-1}...b_1 b_0$, $c = c_m c_{m-1}...c_1 c_0$

Coolocando os noves fora em $a_0 + a_1 + ... + a_k$, obtem-se o algarismo, que chamaremos de a'. Procedendo da mesma forma para os números b e c, obtem-se os algarismos b' e c'. Efetuando a multiplicação $a'.b'$ e colocando os noves fora, obtem-se c". Se o resultado c" for diferente de c', então certamente, um erro na operação indicada foi cometido. Procede-se com a justificativa, por meio de congruência, a seguir:

$$c' \equiv c \equiv a.b \equiv a'.b' \equiv c" \pmod 9$$

com $0 \leq c' < 9$ e $0 \leq c'' < 9$. Caso $c' = c$", nada se pode afirmar quanto a exatidão da operação efetuada. Porém se passa a ter uma garantia de que a referida conta, tornou-se mais confiavel, justamente por ter passado por um teste.

Como ilustração temos que $9.5 = 45$ possui noves fora 0, pois 45 além de ser multiplo de 9, temos que $4+5 = 9$, no qual 9 - 9 = 0. Já para $7 + 8 = 15$, percebe-se que 15 - 9 = 6 (o noves fora), assim como $1 + 5 = 6$.

No caso de 100:10 = 10, tem-se noves fora 1; facilmente identificado na operação 10 - 9 quanto em $1 + 0 = 1$.

6.2 O Calendário

Nesta seção, apresenta-se uma fórmula para descobrir qual é o dia da semana correspondente a uma data determinada data passada ou futura. É interessante mencionar,

que devemos considerar dois fenômenos naturais cíclicos envolvendo o planeta Terra, os quais tem sido utilizados pela humanidade para se localizar no decorrer da historia. Esses fenômenos são o de rotação (movimento pelo qual a Terra faz em torno de seu próprio eixo) propiciando a humanidade identificar e diferenciar o dia da noite e, o movimento orbital elíptico em torno do Sol, responsável pelas estações. É nesses dois fenômenos que está baseado os calendários solares. Conforme cita o professor (HEFEZ, 2009) "Grosseiramente, a rotação completa da Terra em torno de seu eixo dá-nos uma unidade de tempo que é o dia, dividido em períodos iguais de 24 horas, subdivididas em minutos e segundos". Há também outra unidade de tempo, no qual a humanidade mensura o passar dos anos, que é o ano solar, neste caso, corresponde a rotação que a Terra faz de forma completa em torno do Sol.

É interessante observar que há alguns problemas na elaboração de um calendário. A começar pelo fato de que o ano solar não é um número exato de dias, tendo como resultado aproximado de 365,24219. Como relata (HEFEZ, 2009) "Este fato torna necessário que a cada tanto se deva corrigir o número de dias do ano, daí a razão da existência dos anos bissextos, que corrigem parcialmente esse defeito".

Para efeito de simplificação de contas, será estabelecida a fórmula com validade para valor anual a partir de 1601 (obedecendo critérios instituidos na bula papal de Gregório XIII). Por fevereiro ser irregular (com 28 ou 29 dias), para dar maior uniformidade à fórmula, este será colocado no final da contagem dos meses. Dessa forma o mês 1 de um ano será março, seguido de abril etc., até chegar aos meses 11 e 12, que são janeiro e fevereiro (do ano seguinte). Dessa forma, os meses de janeiro e fevereiro de um determinado ano serão considerados como os meses 11 e 12 do ano anterior.

Uma data (d, m, A) será constituída por três números, no qual d representa o dia, m o mês e A um ano posterior a 1600, ou seja $A \geq 1601$. Vale a pena frisar, que março será o mês 1, ou seja, m = 1. Como ilustração, 13 de janeiro de 1999 será representado por (13, 11, 1998) e 29 de fevereiro de 2016 por (29, 12, 2015).

Enumera-se os dias da semana por: domingo (1), segunda (2), terça (3), quarta (4), quinta (5), sexta (6) e sábado (7).

Para determinar o dia da semana $s\ (d, m, A)$, segue-se os passos:

a) Determina-se inicialmente uma fórmula para $s\ (1, 1, A)$ o dia da semana do primeiro dia do mês de março do ano A;

b) Acha-se a fórmula $s\ (1, m, A)$, o dia da semana do primeiro dia do mês m do ano A;

c) Determina-se a fórmula $s\ (d, m, A)$.

Proposição 24. *Seja $A > 1600$. Então, no intervalo (1600, A],*

i) o número de anos múltiplos de 4 é

$$[\tfrac{A}{4}] \text{ - } [\tfrac{1600}{4}] = [\tfrac{A}{4}] \text{ - } 400$$

ii) o número de anos centenários que não são bissextos é

$$[\tfrac{A}{100}] \text{ - } [\tfrac{A}{400}] \text{ - } 12$$

iii) o número de anos bissextos é

$$b = [\tfrac{A}{4}] \text{ - } [\tfrac{A}{100}] + [\tfrac{A}{400}] \text{ - } 388$$

Demonstração. i) É uma consequência direta da proposição citada a seguir, uma vez que o intervalo considerado é $(1600, A]$.

Tem-se que dados inteiros a, b e c tais que $0 < a < b < c$, então o número de múltiplos de a entre b e c é dado por: * $[\frac{c}{a}] - [\frac{b\text{ - }1}{a}]$, se b incluso na contagem. ** $[\frac{c}{a}] - [\frac{b}{a}]$, se b for excluído da contagem.

ii) O número de anos centenários desde o ano 1601 até o ano A é dado por:

$$[\tfrac{A}{100}] - [\tfrac{1600}{100}]$$

e o número de anos centenários bissextos do ano 1601, ao ano A é dado por:

$$[\tfrac{A}{400}] - [\tfrac{1600}{400}]$$

daí o resultado.

iii) Obtem-se o número desejado tomando (i) - (ii), ou seja,

$$\begin{aligned}&[\tfrac{A}{4}] \text{ - } 400 \text{ - } [\tfrac{A}{100}] + [\tfrac{A}{400}] + 12\\ &= [\tfrac{A}{4}] - [\tfrac{A}{100}] + [\tfrac{A}{400}] - 388\end{aligned}$$

□

Denota-se, provisoriamente, po s o dia da semana de primeiro de março de 1601, que irá ser determinado posteriormente.

Como 1602 não é bissexto, o dia primeiro de março de 1602 ocorrerá após 365 dias. Sendo $365 \equiv 1 \pmod 7$, segue-se que o dia 1 de março de 1602 ocorrerá em um dia da semana posterior a s, ou seja, cairá no dia $s + 1 \pmod 7$.

O mesmo argumento mostra que s (1, 1, 1603) $= s + 2 \pmod 7$. Para calcular s (1, 1, 1604), deve-se ter atenção, porque o mês de fevereiro do ano de 1604, considerado como mês 12 do ano anterior, tem 29 dias, logo a passagem de primeiro de março de 1603 para primeiro de março de 1604 ocorrerá 366 dias e, como $366 \equiv 2 \pmod 7$, tem-se que s (1, 1, 1604) $= s + 2 + 2 \pmod 7$. Vê-se então que cada ano bissexto que passa, deve-se somar $1 \pmod 7$ ao dia da semana anterior e a cada ano bissexto, deve-se somar 2.

Dessa forma, considerando o inicio da contagem no ano de 1601 e, sendo b o número de anos bissextos no intervalo $(1600, A]$, tem-se que

$$s(1, 1, A) = s + A - 1600 + b \pmod 7$$

. Consultando o calendário no dia que este trabalho foi escrito, verificou-se que o primeiro do março de 2024 foi uma sexta-feira; logo, $s(1, 1, 2024) = 6$. Fazendo a substituição desse valor na equação $s(1, 1, A) = s + A - 1600 + b \pmod 7$ e calculando b pela Proposição 24, obtemos $s \equiv 4 \pmod 7$; logo, s representa uma quarta-feira.

Proposição 25. *Tem-se que* $s(1, 1, A) = 4 + A + [\frac{A}{4}] - [\frac{A}{100}] + [\frac{A}{400}] \pmod 7$

Para passar de 1 de março para 1 de abril, deve-se somar 31 dias, e como $31 \equiv 3 \pmod 7$, tem-se que $s(1, 2, A) \equiv s(1, 1, A) + 3 \pmod 7$, logo a constante de $s(1, 2, A)$ é 7. Como $30 \equiv 2 \pmod 7$, tem-se que

$$s(1, 3, A) \equiv s(1, 2, A) + 2 \equiv s(1, 1, A) + 5 \pmod 7$$

logo, a constante de $s(1, 2, A)$ é 9, assim sucessivamente somando os números 2 ou 3 ao primeiro dia da semana do mês nterior para obter o primeiro dia da semana de um determinado mês, até chegarmos ao mês 12 (fevereiro). Assim, os termos constantes que devemos somar à expressão

$$A + [\tfrac{\mathrm{A}}{4}] \text{ - } [\tfrac{\mathrm{A}}{100}] + [\tfrac{\mathrm{A}}{400}] \pmod 7,$$

para obter o dia da semana de um determinado mês m de um ano A são:

$$4, 7, 9, 12, 14, 17, 20, 22, 25, 27, 30, 33,$$

ou seja,

$$4, 0, 2, 5, 0, 3, 6, 1, 4, 6, 2, 5 \pmod 7$$

Existe uma fórmula empírica em função de $m = 1, ..., 12$ que fornece esses valores $\pmod 7$:

$$2 + [\tfrac{13\text{m -1}}{5}].$$

Provando assim o resultado a seguir.

Proposição 26. *Tem-se que*

$$s(1, m, A) = 2 + [\tfrac{13m - 1}{5}] + A + [\tfrac{A}{4}] - [\tfrac{A}{100}] + [\tfrac{A}{400}] \pmod 7.$$

Como a cada dia do mês que passa devemos somar 1 módulo 7 ao dia da semana do dia anterior, obtem-se imediatamente o resultado a seguir.

Teorema 16. - *Zeller*

Tem-se a fórmula

$$s(d, m, A) = d + 1 + [\tfrac{13m - 1}{5}] + A + [\tfrac{A}{4}] - [\tfrac{A}{100}] + [\tfrac{A}{400}] \pmod 7.$$

A fórmula do teorema é conhecida como o Algoritmo de Zeller, em homenagem ao reverendo Christian Zeller, que a publicou em 1882.

Será feita a ilustração dessa seção com dois exemplos a seguir.

Exemplo 43. *Descubra qual foi o dia da semana:*

a) em que foi declarada a Independência do Brasil;

b) em que foi abolida a escravidão no Brasil.

Solução. *a) Sabe-se que a Independência do Brasil ocorreu no dia 07 de setembro de 1822. Pela convenção adotada, setembro é o mês 7 (atente para a condição de março ser o mês 1). Aplicando a fórmula de Zeller, obtem-se:*

$s(7, 7, 1822) = 7 + 1 + [\tfrac{13.7-1}{5}] + 1822 + [\tfrac{1822}{4}] - [\tfrac{1822}{100}] + [\tfrac{1822}{400}] \pmod 7.$

$s(7, 7, 1822) = 8 + 18 + 1822 + 455 - 18 + 4 \pmod 7 \equiv 2289 \equiv 0 \pmod 7$

O que resulta que a Independência do Brasil aconteceu num sábado.

b) A escravidão no Brasil foi abolida em 13 de maio de 1888. Pela convenção maio é o mês 3, ou seja m = 3. Aplicando a fórmula de Zeller, tem-se:

$s(13, 3, 1888) = 13 + 1 + [\tfrac{13.3-1}{5}] + 1888 + [\tfrac{1888}{4}] - [\tfrac{1888}{100}] + [\tfrac{1888}{400}] \pmod 7.$

$s(13, 3, 1888) = 14 + 7 + 1888 + 472 - 18 + 4 \equiv 2367 \equiv 1 \pmod 7$

O que resulta em um domingo.

Exemplo 44. *Descubra qual o dia da semana cairá o dia 7 de setembro de 2030?*

Solução. *Fazendo uso do mesmo procedimento adotado no exemplo anterior, temos:*

$s(7,7,2030) = 7 + 1 + [\frac{13.7-1}{5}] + 2030 + [\frac{2030}{4}] - [\frac{2030}{100}] + [\frac{2030}{400}] \pmod 7$.

$s(7,7,2030) = 8 + 18 + 2030 + 507 - 20 + 5 \pmod 7 \equiv 2548 \equiv 0 \pmod 7$

Dessa forma o dia 7 de setembro de 2030 cairá numa sábado.

6.3 Macetes

Nesta seção serão colocados alguns "macetes"da teoria colocada até aqui, com o intuito de simplificar e facilitar a identificação das técnicas por parte dos professores e dos estudantes da Educação Básica. Estes, macetes, estão embasados nos critérios apresentados no capitulo 5.

Apresenta-se:

Consideremos um número natural n, na base decimal. Este número será:

i) divisível por 2 se for par;

ii) divisível por 3 se a soma dos algarismos for múltiplo de 3;

iii) divisível por 4, se os dois ultimos algarismos do número for 00 ou for múltiplo de 4;

iv) divisível por 5, se o número termina em 0 ou 5;

v) divisível por 6, se o número for par e múltiplo de 3;

vii) divisível por 8, se os três últimos algarismos for 000 ou for múltiplo de 8;

viii) divisível por 9, se a soma dos algarismos for múltiplo de 9;

ix) divisível por 10, se o ultimo algarismo do número for 0.

7 Considerações finais

O presente trabalho teve como principal objetivo, apresentar provas aritméticas dos critérios de divisibilidade abordados no ensino de matemática no Ensino Fundamental. Muitos desses critérios são apresentados aos estudantes como técnicas, macetes, sem apresentar provas. Até porque, estas estão fora do escopo e objetivo do material didático destinado ao público alvo. Mas deixando para os professores de matemática a nobre tarefa de desvendar o que há por trás das técnicas que foram apresentadas.

Existem outros tantos critérios de divisibilidade que não foram abordados aqui; pois como o objetivo foi demonstrar aqueles que são tratados no ensino de matemática para os estudantes da Educação Básica, em geral, no sexto ano do Ensino Fundamental, foi citado apenas dois casos não usuais, simplesmente pela curiosidade que aqueles remeteram e também para deixar a sequência dos critérios apresentados de uma forma mais didática.

No último capitulo foi apresentado algumas curisoidades, como por exemplo a prova dos nove e o calendário, como forma de instigr professores de matemática na aplicação dos critérios e também de mostrar aos estudantes estas como elementos que fazem uso e aplicação da teoria, tanto de congruência quanto indiretamente de divisibilidade. No final, a presença dos macetes, direcionados aos leitores, foi uma síntese do que foi colocado no capítulo cinco e também como material consultivo para facilitar na identificação dos critérios; onde as provas já mostradas, remetem apenas ao interesse de observação de como os critérios à luz da aritmética podem ser provados.

Referências

BRASIL. *Ministério da Educação; Base Nacional Comum Curricular. Brasilia: MEC*, 2018. Citado na página 8.

GARBI, G. G. O romance das equações algébricas. Editoria Livraria da Física, 2007. Citado na página 40.

GONÇALVES, A. Introdução à Álgebra. Rio de Janeiro: IMPA., 1999. Citado na página 16.

HEFEZ, A. Aritmética. *Rio de janeiro: SBM*, 2009. Citado 5 vezes nas páginas 12, 24, 45, 58 e 60.

JR, J. R. G. A conquista da matemática. São Paulo: FTD, 2022. Citado 2 vezes nas páginas 23 e 45.

MORGADO, A. C.; CARVALHO, P. C. P. Matemática discreta: Rio de janeiro. SBM, 2015. Citado na página 10.

PARENTE, U. L. O algoritmo de euclides estendido. Portal da Matemática: OBMEP., 2022. Citado na página 26.

SANTOS, J. P. d. O. Introdução à teoria dos números. Rio de Janeiro, IMPA., 2006. Citado 2 vezes nas páginas 26 e 45.

SILVA, T. P. d. Critérios de divisibilidade: usuais, incomuns e curiosos. João Pessoa: UFPB., 2019. Citado na página 45.