

UNIVERSIDADE FEDERAL DO PARANÁ

ANTONIO EVENCIO DE CARVALHO NETO

DESPERTANDO A CURIOSIDADE: DIVISIBILIDADE E NÚMEROS PRIMOS

CURITIBA

2024

ANTONIO EVENCIO DE CARVALHO NETO

DESPERTANDO A CURIOSIDADE: DIVISIBILIDADE E NÚMEROS PRIMOS

Dissertação apresentada ao Curso de Mestrado Profissional em Matemática em Rede Nacional, Setor de Ciências Exatas, UFPR, como requisito parcial para a obtenção do título de Mestre em Matemática.

Orientadora: Prof^a Adriana Luiza do Prado, DSc

CURITIBA

2024

Antonio Evencio de Carvalho Neto
Despertando a Curiosidade: Divisibilidade e Números Primos/ Antonio Evencio
de Carvalho Neto. – Curitiba, 2024-
70 p. : il. (algumas color.) ; 30 cm.

Orientadora: Prof^a Adriana Luiza do Prado, DSc

Dissertação – Universidade Federal do Paraná, 2024.

1. Números Naturais. Números Primos. Critérios de divisibilidade.

I. Orientadora: Prof^a Adriana Luiza do Prado, DSc.

II. Universidade Federal do Paraná

III.

IV. Despertando a Curiosidade: Divisibilidade e Números Primos

CDU 02:141:005.7



MINISTÉRIO DA EDUCAÇÃO
SETOR DE CIÊNCIAS EXATAS
UNIVERSIDADE FEDERAL DO PARANÁ
PRÓ-REITORIA DE PESQUISA E PÓS-GRADUAÇÃO
PROGRAMA DE PÓS-GRADUAÇÃO MATEMÁTICA EM REDE
NACIONAL - 31075010001P2

TERMO DE APROVAÇÃO

Os membros da Banca Examinadora designada pelo Colegiado do Programa de Pós-Graduação MATEMÁTICA EM REDE NACIONAL da Universidade Federal do Paraná foram convocados para realizar a arguição da Dissertação de Mestrado de **ANTONIO EVENCIO DE CARVALHO NETO** intitulada: **DESPERTANDO A CURIOSIDADE: DIVISIBILIDADE E NÚMEROS PRIMOS.**, sob orientação da Profa. Dra. ADRIANA LUIZA DO PRADO, que após terem inquirido o aluno e realizada a avaliação do trabalho, são de parecer pela sua Aprovação no rito de defesa.

A outorga do título de mestre está sujeita à homologação pelo colegiado, ao atendimento de todas as indicações e correções solicitadas pela banca e ao pleno atendimento das demandas regimentais do Programa de Pós-Graduação.

CURITIBA, 10 de Dezembro de 2024.

ADRIANA LUIZA DO PRADO

Presidente da Banca Examinadora

Documento assinado digitalmente



CAMILA ISOTON

Data: 10/12/2024 19:30:45-0300

Verifique em <https://validar.iti.gov.br>

Avaliador Externo (UNIVERSIDADE FEDERAL DA GRANDE DOURADOS)

LUCELINA BATISTA DOS SANTOS

Avaliador Interno (UNIVERSIDADE FEDERAL DO PARANÁ)

Documento assinado digitalmente



LUCELINA BATISTA DOS SANTOS

Data: 10/12/2024 20:09:35-0300

Verifique em <https://validar.iti.gov.br>

AGRADECIMENTOS

Dedico a Deus, em primeiro lugar, aos meus pais José e Rachel que desde sempre me estimularam a estudar, ao meu avô Antônio e Tia Lúcia professores de Matemática que deram bons exemplos de dedicação e zelo pelo ensino da Matemática, aos meus irmãos e minha professora de Artes do ensino fundamental que me iniciou nos estudos de Geometria e a todos meus professores da Graduação e do Mestrado especialmente a professora Adriana e Aldemir que muito bem me orientaram nesse trabalho. Agradeço também por todos os meus alunos que são a razão deste.

RESUMO

O propósito deste trabalho é reunir informações sobre os conteúdos de Matemática dos últimos anos do Ensino Fundamental e do Ensino Médio para aprofundar o conhecimento sobre os números, sua história e construção no sentido de despertar a curiosidade nos alunos.

O uso de princípios e formas de trabalho (construção da tabela direta com números primos e apresentar a matemática com suas regras e teoremas, e a partir deles resolver situações problemas).

Este propósito teve início a partir das aulas no Ensino Fundamental e trabalho com a Olimpíada Brasileira de Matemática das Escolas Públicas (OBMEP). Percebemos que a Matemática, além das aplicações práticas, possui encanto próprio e mesmo quando vemos que a Matemática está em todas as coisas ela pode existir em si mesma.

Palavras-chaves: Números Naturais. Números Primos. Critérios de divisibilidade.

ABSTRACT

The purpose of this work is to gather information about the Mathematics content of the last years of Elementary School and High School to deepen the knowledge about numbers, their history and construction in order to arouse curiosity in students.

The use of principles and ways of working (building a direct table with prime numbers and presenting mathematics with its rules and theorems, and from them solving problem situations).

This purpose began with classes in Elementary School and work with the Brazilian Mathematics Olympiad for Public Schools (OBMEP). We realized that Mathematics, in addition to its practical applications, has its own charm and even when we see that Mathematics is in everything, it can exist in itself.

Key-words: Natural Numbers. Prime numbers. Divisibility criteria.

LISTA DE ILUSTRAÇÕES

FIGURA 1 – Data com números primos	12
FIGURA 2 – Carl Boyer	13
FIGURA 3 – Francesco Maurolycus	15
FIGURA 4 – Abramo Hefez	15
FIGURA 5 – Euclides	17
FIGURA 6 – Erastóstenes	19
FIGURA 7 – Ábaco escolar	24
FIGURA 8 – Material dourado	24
FIGURA 9 – Tabela com os intervalos de números compostos entre os primos com Excel	37
FIGURA 10 – Fonte: Próprio autor	53

LISTA DE TABELAS

TABELA 1 – Fonte: Próprio autor	19
TABELA 2 – Fonte: Próprio autor	20
TABELA 3 – Fonte: Próprio autor	20
TABELA 4 – Fonte: Próprio autor	21
TABELA 5 – Fonte: Próprio autor	28
TABELA 6 – Fonte: Próprio autor	32
TABELA 7 – Fonte: Próprio autor	32
TABELA 8 – Tabela 1a	54
TABELA 9 – Tabela 1b	55
TABELA 10 – Tabela 2a	55
TABELA 11 – Tabela 2b	55
TABELA 12 – Tabela 3a	55
TABELA 13 – Tabela 3b	56
TABELA 14 – Tabela 4a	56
TABELA 15 – Tabela 4b	56

LISTA DE ABREVIATURAS E DE SIGLAS

ABNT Associação Brasileira de Normas Técnicas

BNCC Base Nacional Comum Curricular

EF06MA01 Ensino Fundamental 6o. ano Matemática conteúdo 01

EF06MA02 Ensino Fundamental 6o. ano Matemática conteúdo 02

EF06MA05 Ensino Fundamental 6o. ano Matemática conteúdo 05

EF07MA01 Ensino Fundamental 7o. ano Matemática conteúdo 01

EF07MA03 Ensino Fundamental 7o. ano Matemática conteúdo 03

EF07MA04 Ensino Fundamental 7o. ano Matemática conteúdo 04

EF07MA05 Ensino Fundamental 7o. ano Matemática conteúdo 05

OBMEP Olimpíada Brasileira de Matemática das Escolas Públicas

PCN Parâmetros Curriculares Nacionais

LISTA DE SÍMBOLOS

$\mathbb{N}$	Conjunto dos números naturais
$\mathbb{Z}$	Conjunto dos números inteiros
$\rightarrow$	Implicação
(a, b)	Máximo divisor comum de a e b
$mmc(a, b)$	Mínimo múltiplo comum de a e b

SUMÁRIO

1	INTRODUÇÃO	12
1.1	OBJETIVO GERAL	12
1.2	OBJETIVOS ESPECÍFICOS	12
2	CONJUNTOS NUMÉRICOS	13
2.1	NÚMEROS NATURAIS	13
2.2	NÚMEROS PRIMOS	17
2.2.1	INTERVALOS DE NÚMEROS COMPOSTOS EM SEQUENCIA	32
2.3	NÚMEROS INTEIROS	38
2.3.1	DIVISIBILIDADE	42
2.4	DIVISÃO EUCLIDIANA	42
3	CRITÉRIOS UNIVERSAIS DE DIVISIBILIDADE	48
3.1	O SISTEMA DE NUMERAÇÃO DECIMAL	48
3.2	CRITÉRIO DE DIVISIBILIDADE DE UM NÚMERO POR 2	50
3.3	CRITÉRIO DE DIVISIBILIDADE DE UM NÚMERO POR 5	51
3.4	CRITÉRIO DE DIVISIBILIDADE DE NÚMEROS PRIMOS COM 10	52
3.5	ARITMÉTICA DOS RESTOS	56
4	CONCLUSÃO	60
	Referências	69

1 INTRODUÇÃO

Este trabalho teve início a partir das aulas no Ensino Fundamental e estudos com a Olimpíada Brasileira de Matemática das Escolas Públicas (OBMEP). Percebemos que a Matemática, além das aplicações práticas, possui encanto próprio e mesmo quando vemos que a Matemática está em todas as coisas ela pode existir em si mesma.

Começamos o dia colocando a data e uma provocação aos alunos.

Data 10 / 12 / 2024 ou $2.5 / 2^2.3 / 2^3.11.23$

FIGURA 1 – Data com números primos

Estes detalhes podem mostrar a Matemática como arte. Por exemplo, ninguém questiona para que serve uma música que é fantástica ou um quadro de um pintor que permanece por séculos como objeto de admiração.

Por vezes, caímos na tentação de rotular a Matemática como um remédio amargo a ser tomado, que resolve todos os problemas do mundo e acabamos achando aplicações, às vezes desnecessárias, que mais afastam o estudante da disciplina e não levam a lugar algum.

Por outro lado, podemos perceber que pesquisadores ao longo da história fizeram pesquisas que não havia como utilizar na prática e depois foram encontradas muitas aplicações. Quando estas teorias foram estudadas despertaram um encanto que as levaram para frente como um quadro de um pintor famoso. Mais tarde descobrem-se aplicações. Dentro desta perspectiva podemos trabalhar conceitos de Matemática nos anos finais do Ensino Fundamental.

1.1 OBJETIVO GERAL

Nosso objetivo geral é trabalhar de uma forma simples a introdução dos conceitos da reta numérica e de forma concreta os princípios algébricos.

1.2 OBJETIVOS ESPECÍFICOS

1. Estudar os conjuntos numéricos começando com os naturais, sua história e conceitos.
2. Estudar os números primos e suas características.
3. Introdução dos números inteiros e divisão euclidiana.

2 CONJUNTOS NUMÉRICOS

2.1 NÚMEROS NATURAIS

Sabemos que a noção de contagem é inerente ao ser humano e até algumas formas de vida apresentam padrões Matemáticos. Observando a natureza vemos estes padrões em toda a parte e que, segundo Boyer (BOYER, 1974) em certa época pensou-se que a Matemática se ocupava do mundo que nossos sentidos percebem, e foi somente no século dezanove que a Matemática Pura se libertou das limitações impostas pela natureza.

Em relação a esta percepção, Boyer (2) comenta:



FIGURA 2 – Carl Boyer

“Essa percepção abstrata que nós chamamos número, representa um grande passo no caminho para a Matemática moderna. É improvável que isso tenha sido a descoberta de um indivíduo ou de uma dada tribo: é mais provável que a percepção tenha sido gradual e pode ter se desenvolvido tão cedo no desenvolvimento cultural do homem quanto o uso do fogo, talvez a 300.000 anos”. (BOYER, 1974)

Com a evolução das civilizações estes conceitos foram sendo aprimorados até chegarmos no nível de sofisticação atual. No livro (BOYER, 1974), temos a informação que o homem difere dos outros animais de modo mais acentuado pela sua linguagem e cujo desenvolvimento foi essencial para que surgisse o pensamento abstrato.

No início da concepção dos sistemas de numeração podemos perceber que não foi algo linear e uniforme. Nos nossos dias temos diversos sistemas de numeração, por exemplo o sistema misto sexagesimal /decimal para indicarmos o tempo e ângulos em graus. Os povos que utilizam os calendários com diversos sistemas de numeração e orientados por razões religiosas, as unidades de medida que utilizam sistema de frações como a polegada e outras formas não decimais, além é claro dos sistemas utilizados para eletrônica digital que mistura vários tipos de sistemas, como binário e hexadecimal, por exemplo.

No nosso caso, vamos nos orientar pelo sistema decimal, sua história, conceitos e aplicações. Quando contemplamos no sistema decimal o conjunto dos Números Naturais já encontramos uma grande quantidade de detalhes curiosos. Podemos nos guiar por detalhes significativos que foram aparecendo. Para começar, podemos nos

questionar sobre a origem dos números conforme utilizamos hoje.

Quando observamos os números naturais, temos a impressão de que estamos diante de algo muito simples. Olhando um adulto ensinando uma criança a aprender a contar, vemos algo bastante elementar. Observando melhor, começamos a perceber alguns detalhes que nos indicam que não é tão elementar quanto aparenta ser.

Podemos iniciar uma reflexão mais profunda observando este pequeno gesto: pedimos para a criança mostrar um dedo e dizemos, um; e depois, dois dedos e dizemos, dois; e assim por diante. Neste ponto já percebemos que não ensinamos o zero como um número. Este fato traz à tona o conceito do zero ser ou não um número natural.

Guiseppe Peano (ALVARENGA, 2022) baseando-se na noção intuitiva de sucessor de um número propôs um lista de quatro axiomas, conhecidos como Axiomas de Peano, para caracterizar o conjunto dos números naturais, denotado por $\mathbb{N}$. Sendo eles:

1. Todo número natural tem um sucessor, que também é um número natural, e é único;
2. Os números naturais diferentes tem sucessores diferentes;
3. Existe um único natural que não é sucessor de nenhum outro e é indicado por 1;
4. Seja A um subconjunto de números naturais (isto é, $A \subset \mathbb{N}$). Se $1 \in A$ e se, o sucessor de cada elemento de A também pertence a A , então $A = \mathbb{N}$.

"O terceiro axioma estabelece 1 como sendo o único elemento natural que não é o sucessor de nenhum outro e que, portanto, representa o 'ponto de partida' no conjunto $\mathbb{N} = \{1, 2, 3, \dots\}$ dos números naturais. É comum, também, adotar-se 0 como ponto de partida, levando a $\mathbb{N} = \{0, 1, 2, 3, \dots\}$. A opção por uma ou outra alternativa é uma questão de gosto ou de conveniência."(MORGADO; CARVALHO, 2015)

Desta forma, percebemos que o zero muitas vezes fica como um incômodo necessário. Durante muito tempo, no desenvolvimento da história da Matemática o zero não apareceu como número, mas apenas como um espaço vazio entre os números. Sabemos que a Matemática, como vemos hoje precisa do zero, temos o sistema binário que utiliza o número zero e o número um e vemos que este sistema de numeração é bastante completo.

Assim, imagina-se um sistema de numeração com quantos símbolos desejarmos e percebemos que o zero deve ser um deles para que o sistema tenha algumas propriedades básicas.

Depois, conforme vamos trabalhando com estes números, aparecem seus muitos subconjuntos como conjunto dos números pares, conjunto dos números ímpares, conjunto dos números primos etc. e as suas operações. Assim, já podemos imaginar que o conjunto dos números naturais se torna interessante para uma reflexão mais profunda.

Na operação de adição percebemos que o conjunto dos Números Naturais é fechado para esta operação e que, ela não apresenta alguma dificuldade, por outro lado, as outras operações como subtração, multiplicação estão muito relacionadas a ela. Quanto a operação de subtração, que é a operação inversa da soma, pode ser usada para explicar a divisão.

Dentro do conjunto dos números ímpares já aparece o detalhe que a soma deles desde o primeiro (o número um), e seguindo a soma em sequência, obtemos o conjunto dos quadrados perfeitos. No livro didático “Projeto Araribá” (GAY M.G., 2007), encontramos uma definição para quadrado perfeito, se referindo aos números naturais:

« “Os números que podem ser escritos como potência de base inteira e expoente 2 são chamados quadrados perfeitos” . (GAY M.G., 2007)

No caso nos referimos à sequência dos números obtidos sequencialmente à partir da multiplicação de um número natural multiplicado por ele mesmo desde o 1, 2, 3, 4, 5, ... e obtendo 1, 4, 9, 16, ... , quando somamos os números ímpares encontramos a mesma sequência, isto é $1 + 3 = 4$, $1 + 3 + 5 = 9$, $1 + 3 + 5 + 7 = 16$, ...

A afirmação acima tem o primeiro registro do Princípio da Indução Matemática feita por Francesco Maurolycus (3) em 1575 e foi referenciada a partir do exemplo dado por Hefez (4) em 2011.



FIGURA 3 – Francesco Maurolycus



FIGURA 4 – Abramo Hefez

Exemplo 1. Trata-se da determinação de uma fórmula exata em função de $n \leq 1$ para a soma dos n primeiros números naturais ímpares. Ou seja, busca-se uma fórmula

para determinarmos a soma dos números ímpares, denotemos por S_n , afirmamos que $S_n = 1 + 3 + 5 \dots + (2n - 1)$.

Vamos verificar S_n para alguns valores de n :

$$\begin{cases} S_1 = 1; \\ S_2 = 1 + 3 = 4; \\ S_3 = 1 + 3 + 5 = 9; \\ S_4 = 1 + 3 + 5 + 7 = 16; \\ S_5 = 1 + 3 + 5 + 7 + 9 = 25 \end{cases}$$

Os casos particulares acima nos conduzem a conjecturar que $S_n = n^2$.

Mas como ter certeza que não estamos cometendo o engano da galinha de Bertrand Russel :

« “ Havia uma galinha no quintal de uma velha senhora. Diariamente, ao entardecer, a boa senhora levava milho à galinhas. No primeiro dia, a galinha desconfiada, esperou que a senhora se retirasse para se alimentar. No segundo dia, a galinha prudentemente, foi se alimentando enquanto a senhora se retirava. No centésimo dia ao se aproximar a senhora , a galinha, por indução , foi ao encontro dela para reclamar o seu milho. Qual a não foi a sua surpresa quando a senhora pegou-a pelo pescoço com a intenção de pô-la na panela. ” (HEFEZ, 2016).

Para ter certeza devemos usar o Princípio de Indução Finita (o axioma 4 de Peano (MORGADO; CARVALHO, 2015)). O método da indução finita é um procedimento matemático para provar propriedades que são verdadeiras para uma seqüência de objetos. É um método bastante utilizado em qualquer domínio da Matemática.

Utilizaremos com o nome de **Princípio da Indução Finita -1a Forma**. Se pudermos provar que valem as duas condições:

1. $P(n_0)$ é verdadeira (ou seja, vale a propriedade para n_0);
2. Se $P(n)$ implicar em $P(n + 1)$ ser verdade para todo $n \geq n_0$.

Então podemos afirmar que a propriedade $P(n)$ é verdadeira para todo $\geq n_0$.

Proposição 1. A soma dos números ímpares é dada por $S_n = n^2$.

Demonstração:

Definimos $p(n) : S_n = n^2$ e verificaremos as condições do PIF.

Temos que $p(1) = 1 = 1^2$, portanto verdade.

Para provar que a implicação $p(n) \rightarrow p(n+1)$ é verdade que para todo $n \in \mathbb{N}$, basta mostrar que, se supusermos $p(n)$ verdade, então $p(n+1)$ é verdade, qualquer que seja $n \in \mathbb{N}$.

De fato, supondo $p(n)$ verdade, ou seja, $S_n = n^2$, e somando $2n+1$ a ambos os lados desta última igualdade, obtemos:

$S_{n+1} = S_n + 2n + 1 = n^2 + 2n + 1 = (n+1)^2$, o que nos diz que $p(n+1)$ é verdade.

Pelo Princípio de Indução Finita, $p(n)$ é verdade para todo $n \in \mathbb{N}^*$. ■

Agora, podemos encontrar diversos outros fatos Matemáticos que foram descobertos e formalizados, como a soma de uma sequência de números naturais ou outros detalhes, às vezes, não muito fáceis de serem descobertos.

Ao longo do desenvolvimento das civilizações modernas, a Matemática foi lentamente sendo descoberta e se tornando uma ferramenta preciosa, uma fonte de teoremas que as vezes não sabemos exatamente onde aplicar e, quando menos esperamos, vemos seus frutos aparecendo.

2.2 NÚMEROS PRIMOS

No livro do Hefez (HEFEZ, 2016), temos o enunciado do Teorema Fundamental da Aritmética da seguinte forma: *“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”*.

Esta definição já aparece de certa forma nos escritos de Euclides de Alexandria (cerca de 300 a.C.) e acredita-se que quando Euclides registrou este conceito ele já era conhecido em outros lugares, mas Euclides (5) se notabilizou pelo registro e pela forma de arranjar estes registros.



FIGURA 5 – Euclides

No livro “A História da Matemática” de Boyer, é descrito que:

« “No livro IX, o último dos três sobre teoria dos números, contém vários teoremas interessantes. Desses, o mais célebre é a proposição 20: ‘números primos são mais do que qualquer quantidade fixada de números primos’. Isto é, Euclides dá aqui a prova elementar bem conhecida do fato de que há infinitos números primos. A prova é indireta, pois mostra-se que a hipótese de haver só um número finito de primos

leva a uma contradição. Seja P o produto de todos os primos, supostos em número finito e consideremos o número $N = P + 1$. Logo, N é composto e deve ser medido por algum número p . Mas p não pode ser nenhum dos fatores primos que entram em P , se não seria um fator de 1. Logo, p deve ser um primo diferente de todos os fatores de P , portanto a hipótese de P ser o produto de todos os primos é falsa". (BOYER, 1974)

Para termos um panorama mais completo deste teorema podemos voltar um pouco. Podemos imaginar a construção do Conjunto dos Números Naturais simplesmente como a sequência onde iniciamos pelo número um e vamos adicionando uma unidade para encontrar o próximo.

A partir deste conceito percebemos os conceitos de sucessor e antecessor. Depois podemos começar a observar as propriedades elementares destes números. Percebe-se assim, pois, que este caminho é um caminho que flui com certa naturalidade. Destas propriedades chega-se a compreensão da construção do Conjunto dos Números Naturais a partir do Teorema Fundamental da Aritmética, que diz que "Todo número natural maior do que 1 ou é primo ou pode ser representado de modo único como um produto de números primos, a menos de um fator".

Quando construímos este conjunto (dos números naturais) pode-se perceber os conceitos de múltiplos e que todo número é múltiplo de um, os pares são múltiplos de dois e que o conjunto dos múltiplos de um número é infinito e obtido multiplicando este número pelos elementos do conjunto dos números naturais.

Para construirmos o conjunto dos divisores já não é tão imediato e para tal vamos precisar do conjunto dos números primos. Neste ponto o conjunto dos números naturais como uma sequência não oferece as ferramentas necessárias para uma determinação rápida e precisa.

Mas antes disso vamos observar o que é o conjunto dos divisores de um número: se como o produto dos números naturais por um número qualquer temos os múltiplos desse número qual seria o caminho para determinarmos seus divisores.

Sabemos que: "Um número é divisor de outro, quando está contido nesse outro um certo número de vezes", podemos por exaustão encontrar todos os divisores experimentando um a um de um até o próprio número.

Este procedimento pode ser usado somente até certo ponto pois não prevê por antecipação quais e quantos são estes números, desta forma quem são estes. Este princípio se encerra em si mesmo sem maiores possibilidades.

Depois de passarmos pelos múltiplos e divisores de um número podemos concluir que um número primo é aquele que possui unicamente dois divisores distintos ou seja o um e ele mesmo.



FIGURA 6 – Eratóstenes

Eratóstenes (6) se tornou célebre em aritmética devido a um dispositivo conhecido como crivo, usado para se acharem todos os números primos menores que um número n dado. Anotam-se, em ordem e começando por 3, todos os números ímpares menores que n . Eliminam-se os números compostos da sequência riscando-se, a partir do 3 (exclusive) todos os terceiros números que se seguem, depois, a partir do 5 (exclusive) todos os quintos números que se seguem e assim por diante. Nesse procedimento riscam-se alguns números mais do que uma vez. Todos os números não-riscados, mais o número 2, formam a lista dos primos menores que n (EVES, 2004). É um processo exaustivo mas é um modo de determinar vários primos.

1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

Primos	Múltiplos de 5
Pares	Ímpares nem múltiplos de cinco nem primos

TABELA 1 – Fonte: Próprio autor

Na tabela 1 apresentamos os números primos em azul, em vermelho os pares, em verde os múltiplos de cinco e destacados em amarelo os ímpares que não são múltiplos de cinco e não são primos.

Mas os Matemáticos de diversas gerações buscam uma forma de determinar um número primo sem ter que realizar todos estes cálculos, por métodos computacionais pode-se ir muito longe nesta busca mas somente ela será concluída quando

for determinada com exatidão por meios algébricos todos estes números, ainda não chegamos lá.

Quando Gauss iniciou seus estudos com números primos ele acreditava que poderia chegar a determinar qual seria o número de números primos em determinados grupos de números. Em seus estudos percebeu que o número de números primos sofre uma queda conforme estabelecemos conjuntos maiores.

Por exemplo, até o 10 temos 4 números primos, ou seja, 1 a cada 2,5 números são primos.

1	2	3	4	5	6	7	8	9	10
---	---	---	---	---	---	---	---	---	----

4 primos, ou seja, 1 cada 2,5 números são primos.

TABELA 2 – Fonte: Próprio autor

Se olharmos até 100 temos 25 números primos, ou seja, 1 a cada 4 números são primos.

1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

25 primos, ou seja, 1 cada 4 números são primos.

TABELA 3 – Fonte: Próprio autor

Até 1000 são 168, ou seja, aproximadamente 1 a cada 6 números é primo.

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60	61	62	63	64	65	66	67	68	69	70	71	72	73	74	75
76	77	78	79	80	81	82	83	84	85	86	87	88	89	90	91	92	93	94	95	96	97	98	99	100
101	102	103	104	105	106	107	108	109	110	111	112	113	114	115	116	117	118	119	120	121	122	123	124	125
126	127	128	129	130	131	132	133	134	135	136	137	138	139	140	141	142	143	144	145	146	147	148	149	150
151	152	153	154	155	156	157	158	159	160	161	162	163	164	165	166	167	168	169	170	171	172	173	174	175
176	177	178	179	180	181	182	183	184	185	186	187	188	189	190	191	192	193	194	195	196	197	198	199	200
201	202	203	204	205	206	207	208	209	210	211	212	213	214	215	216	217	218	219	220	221	222	223	224	225
226	227	228	229	230	231	232	233	234	235	236	237	238	239	240	241	242	243	244	245	246	247	248	249	250
251	252	253	254	255	256	257	258	259	260	261	262	263	264	265	266	267	268	269	270	271	272	273	274	275
276	277	278	279	280	281	282	283	284	285	286	287	288	289	290	291	292	293	294	295	296	297	298	299	300
301	302	303	304	305	306	307	308	309	310	311	312	313	314	315	316	317	318	319	320	321	322	323	324	325
326	327	328	329	330	331	332	333	334	335	336	337	338	339	340	341	342	343	344	345	346	347	348	349	350
351	352	353	354	355	356	357	358	359	360	361	362	363	364	365	366	367	368	369	370	371	372	373	374	375
376	377	378	379	380	381	382	383	384	385	386	387	388	389	390	391	392	393	394	395	396	397	398	399	400
401	402	403	404	405	406	407	408	409	410	411	412	413	414	415	416	417	418	419	420	421	422	423	424	425
426	427	428	429	430	431	432	433	434	435	436	437	438	439	440	441	442	443	444	445	446	447	448	449	450
451	452	453	454	455	456	457	458	459	460	461	462	463	464	465	466	467	468	469	470	471	472	473	474	475
476	477	478	479	480	481	482	483	484	485	486	487	488	489	490	491	492	493	494	495	496	497	498	499	500
501	502	503	504	505	506	507	508	509	510	511	512	513	514	515	516	517	518	519	520	521	522	523	524	525
526	527	528	529	530	531	532	533	534	535	536	537	538	539	540	541	542	543	544	545	546	547	548	549	550
551	552	553	554	555	556	557	558	559	560	561	562	563	564	565	566	567	568	569	570	571	572	573	574	575
576	577	578	579	580	581	582	583	584	585	586	587	588	589	590	591	592	593	594	595	596	597	598	599	600
601	602	603	604	605	606	607	608	609	610	611	612	613	614	615	616	617	618	619	620	621	622	623	624	625
626	627	628	629	630	631	632	633	634	635	636	637	638	639	640	641	642	643	644	645	646	647	648	649	650
651	652	653	654	655	656	657	658	659	660	661	662	663	664	665	666	667	668	669	670	671	672	673	674	675
676	677	678	679	680	681	682	683	684	685	686	687	688	689	690	691	692	693	694	695	696	697	698	699	700
701	702	703	704	705	706	707	708	709	710	711	712	713	714	715	716	717	718	719	720	721	722	723	724	725
726	727	728	729	730	731	732	733	734	735	736	737	738	739	740	741	742	743	744	745	746	747	748	749	750
751	752	753	754	755	756	757	758	759	760	761	762	763	764	765	766	767	768	769	770	771	772	773	774	775
776	777	778	779	780	781	782	783	784	785	786	787	788	789	790	791	792	793	794	795	796	797	798	799	800
801	802	803	804	805	806	807	808	809	810	811	812	813	814	815	816	817	818	819	820	821	822	823	824	825
826	827	828	829	830	831	832	833	834	835	836	837	838	839	840	841	842	843	844	845	846	847	848	849	850
851	852	853	854	855	856	857	858	859	860	861	862	863	864	865	866	867	868	869	870	871	872	873	874	875
876	877	878	879	880	881	882	883	884	885	886	887	888	889	890	891	892	893	894	895	896	897	898	899	900
901	902	903	904	905	906	907	908	909	910	911	912	913	914	915	916	917	918	919	920	921	922	923	924	925
926	927	928	929	930	931	932	933	934	935	936	937	938	939	940	941	942	943	944	945	946	947	948	949	950
951	952	953	954	955	956	957	958	959	960	961	962	963	964	965	966	967	968	969	970	971	972	973	974	975
976	977	978	979	980	981	982	983	984	985	986	987	988	989	990	991	992	993	994	995	996	997	998	999	1000

TABELA 4 – Fonte: Próprio autor

E até 10.000 temos 1218 números primos, ou seja aproximadamente 1 a cada 8,2 é primo, vemos que estas proporções não são exatas e mesmo que estivessem corretas fica cada vez mais difícil saber quais seriam estes números primos.

Dentro das formas de serem determinados quantos e quais são os números primos tem sido razão de pesquisa e estudo de gerações de Matemáticos, apesar de ninguém ter conseguido a forma desejada, estes estudos trouxeram uma série de descobertas sobre a forma como as propriedades dos números naturais ou inteiros se comportam:

Vamos olhar sobre o conjunto dos divisores de um número de uma forma mais objetiva.

O primeiro passo é sabermos duas coisas: o primeiro divisor de qualquer número é o número 1 e o último é o próprio número. Segundo Pérez e Marin (MARIN, 1928), com esta simples conclusão percebemos que o conjunto dos divisores de um número qualquer tem um início e fim determinados, isto reduz drasticamente o número

de candidatos a elemento deste conjunto.

Utilizando a decomposição de um número composto qualquer em fatores primos podemos fácil e precisamente determinar quantos são seus divisores e se o número é um quadrado perfeito ou não.

Vejamos, por exemplo, o número 144 decomposto em fatores primos é igual a $2^4 \cdot 3^2$, a partir daí determinamos que 144 possui quinze divisores e que ele é um quadrado perfeito.

Sabemos isto pois os divisores de um número são obtidos a partir das combinações possíveis dos fatores 2 e 3 com o expoente do dois variando de 0 até 4, que resulta cinco possibilidades e do três como o expoente variando de 0 até 2 que resulta em três possibilidades, pelo princípio multiplicativo concluímos que ele possui quinze combinações possíveis para divisores.

Ordenando todas estas combinações em ordem crescente fica determinado perfeitamente o conjunto dos divisores do número escolhido para sabermos se é um quadrado perfeito basta olhar que o número de divisores só será ímpar quando todos os expoentes dos fatores na decomposição foram pares, condição necessária e suficiente para que o número seja um quadrado perfeito.

Vemos que quando o conjunto dos divisores de um número possui um número par de elementos o produto de dois termos da primeira metade em ordem crescente com os da segunda metade em ordem decrescente sempre resulta no próprio número e quando for ímpar o divisor que fica no meio do conjunto é a raiz quadrada do número. Outras propriedades podem ser concluídas a partir do uso da decomposição de um número em fatores primos, isto pode ser percebido que nos estudos do ensino fundamental e médio estamos sempre nos servindo deles para explicar conteúdos e resolver problemas.

Definimos o conjunto dos divisores de um número de forma tão direta e precisa e voltamos no tempo quando isso não era conhecido, os matemáticos determinavam estes conjuntos e estudavam suas propriedades, vemos que apesar da evolução do conhecimento e dos recursos tecnológicos as descobertas feitas anteriormente são os fundamentos para novas formas de pensamento.

Definição 1. *Um número natural maior do que 1 e que só é divisível por 1 e por si próprio é chamado de número primo.*

Definição 2. *Diremos que um número inteiro $d \geq 0$ é um máximo divisor comum (mdc) de a e b , se possuir as seguintes propriedades:*

(i) *d é um divisor comum de a e b , e*

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

O mdc de a e b será denotado por (a, b) .

Dados dois números primos p e q e um número natural a , decorrem da definição de número primo os seguintes fatos:

I. Se $p \mid q$ então $p = q$

II. Se $p \mid a$, então $(p, a) = 1$

Depois de explicar estas observações, Hefez conclui:

« “Do ponto de vista da estrutura multiplicativa dos naturais, os números primos são os mais simples e ao mesmo tempo são suficientes para gerar todos os números naturais, conforme veremos mais tarde no Teorema Fundamental da Aritmética”. (HEFEZ, 2016)

Estas afirmações são muito simples, do ponto de vista prático no ensino de Matemática nos anos finais do ensino fundamental, em geral, é ensinado simplesmente como um fato.

No livro didático (CASTRUCI; GIOVANNI J.R.AND GIOVANNI JUNIOR, 2019) a decomposição em fatores primos é apresentada como um fato.

De uma forma simples, depois de apresentar os números primos e alguns exemplos e diferenciar de número composto, define: “Vimos que todo número natural maior do que 1 que não é primo é chamado de número composto, pois ele pode ser expresso como a multiplicação de dois ou mais fatores primos”.

Olhando outros livros didáticos do ensino fundamental dos sextos e sétimos anos vemos sempre a fatoraçoão como um algoritmo e a construção do Conjunto dos Números Naturais a partir do zero somando 1 e encontrado o seu sucessor.

Em outro capítulo na BNCC (BRASIL, 2018), desde o primeiro ano se preconiza o ensino da decomposição de um número, mas sempre da forma decimal e assim é construída a noção de construção do conjunto dos números naturais como resultado de uma contagem no sistema decimal, inclusive utilizando ábacos e o material dourado, até o quinto ano.

O Ábaco (7) é considerado como a primeira calculadora inventada pelo homem, o ábaco é um instrumento composto de pequenos discos ou bolas inseridas dentro de hastes, onde cada haste é perfilada em sequência, definindo assim, as casas decimais como: unidade, dezena, centena, milhar e assim por diante. O Material Dourado foi idealizado pela médica e educadora italiana Maria Montessori para o trabalho na



FIGURA 7 – Ábaco escolar



FIGURA 8 – Material dourado

disciplina de matemática e depois foi adaptado por Lubienska de Lenval, seguidora de Montessori, construindo-o em madeira na forma que encontramos atualmente (8).

No final do quinto ano aparece a soma e subtração de números racionais na forma de frações de denominadores diferentes sem se ocupar com os números primos. No sexto ano aparece pela primeira vez, formalmente os números primos, no item Unidades Temáticas (Números) e como Objeto de Conhecimento (Números Primos e compostos), mas a opção sempre é de construir o sistema de numeração decimal sem associá-lo com números primos, conforme podemos observar abaixo:

(EF06MA01) Comparar, ordenar, ler e escrever números naturais e números racionais cuja representação decimal é finita, fazendo uso da reta numérica.

(EF06MA02) Reconhecer o sistema de numeração decimal, como o que prevaleceu no mundo ocidental, e destacar semelhanças e diferenças com outros sistemas, de modo a sistematizar suas principais características (base, valor posicional e função do zero), utilizando, inclusive, a composição e decomposição de números naturais e números racionais em sua representação decimal.

Adiante aparece, formalmente, pela primeira vez para os estudantes do ensino fundamental os números primos:

(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.

Sobre a divisibilidade por dois, fica bem, explicar antes para os estudantes do sexto ano que a soma de dois números pares é um número par e a diferença entre dois números pares também é par. Este fato, não precisa de demonstração para se tornar claro.

No ensino fundamental, iniciando pelo sexto ano é perfeito explicar que todo número par é divisível por dois. Nesta parte do ensino podemos mostrar que um número de pedras ou outros meios materiais, por exemplo milho ou tampinhas de plástico e pode se separar de dois em dois e quando o número é par não tem sobra, resto zero.

Neste momento podemos mostrar no concreto que a soma de dois números naturais pares ou a diferença entre eles resulta em um número par. Este fato é importante para a compreensão de um teorema no concreto. Depois podemos explicar que esse fato acontece com quaisquer múltiplos e em qualquer quantidade.

Nesta etapa de ensino onde os alunos tem cerca de onze anos, sabemos que o uso do raciocínio abstrato ainda é insuficiente, este tipo de trabalho favorece a construção desta modalidade de raciocínio e a apropriação de conteúdos básicos de Matemática abstrata.

Os outros critérios também podem ser verificados utilizando objetos simples de contagem como a divisibilidade por três, quatro, cinco, seis e, por que não sete?

Neste ponto observa se que o conhecimento nas escolas, por vezes demora a incorporar fatos recentes. Nos livros didáticos não existe, em geral, o critério de divisibilidade por sete. Vamos refletir sobre este fato.

Por que não é apresentado o critério de divisibilidade por sete nos sextos anos do ensino fundamental. Na aula 41 do Programa de Iniciação Científica (OBMEP, s.d.), acesso em 14/06/2024, é apresentada a demonstração da proposição abaixo e um exemplo.

Faremos a demonstração:

Proposição 2. *O número $(10a + b)$ é divisível por 7 se, e somente se $(a - 2b)$ for divisível por 7.*

Demonstração:

Primeiro, supondo que $10a + b$ é divisível por 7, logo existe um $k \in \mathbb{Z}$ tal que $10a + b = 7k$ e escrevendo $b = 21b - 20b$ assim $10a + 21b - 20b = 7k$ isto implica que $10a - 20b = 7k - 21b = 7k'$ e colocando 10 em evidência temos $10(a - 2b) = 7k'$, como 7 não divide 10, logo ele divide $(a - 2b)$, o que prova a ida.

Para provar a volta, suponha que $a - 2b$ é divisível por 7 então podemos escrever $a - 2b = 7k$ e multiplicamos a equação toda por $(\cdot 10)$. Assim $10a - 20b = 7 \cdot 10 \cdot k$. Para encontrar b somando em ambos o termo $21b$ e chamando $70k = 7k'$, reescrevemos por $10a - 20b + 21b = 7k' + 21b \rightarrow 10a + b = 7k''$, portanto $(10a + b)$ é divisível por 7, o que prova a equivalência. ■

Esta demonstração não é necessária ou desejável para ser explicada no sexto

ano, mas a aplicação do critério de divisibilidade sim. Utilizando a mesma ideia e alterando o número, temos o seguinte lema.

Lema 1. *O número $(10a + b)$ é divisível por 7 se, e somente se $(a + 5b)$ é divisível por 7.*

Demonstração:

Primeiro, suponha que $a+5b$ é divisível por 7 então podemos escrever $a+5b = 7k$ e multiplicamos a equação por $(.10)$. Assim $10a + 50b = 7.10.k$. Escrevendo $50b = b + 49b$ temos $10a + b + 49b = 7k_1$ então $10a + b = 7k_1 - 49b$ e chamando $7k_1 - 49b = 7k_2$ temos que $10a + b = 7k_2$ é divisível por 7.

Agora suponha que $10a + b$ é divisível por 7 podemos escrever $b = 50b - 49b$ assim $10a + 50b - 49b = 7k$ e podemos reescrever por $10a + 50b = 7k + 49b$ e colocando 10 em evidência, encontramos $10(a + 5b) = 7k_1$, como 7 não divide 10, logo ele divide $(a + 5b)$, o que prova a equivalência. ■

Esta demonstração, assim como a outra não é apropriada para ser ensinada no sexto ano, mas a aplicação é bastante simples e também útil para o ensino nesta faixa de estudos.

Exemplo 2. *Se queremos saber se 182 é divisível por 7, fazemos a divisão e percebemos que 182 é igual a $7 \cdot 26$, logo 182 é divisível por 7. Podemos, de outra forma retirar o último algarismo, isto é, o 2, multiplicar por 2 e subtrair de 18, ou seja, $18 - 2 \cdot 2 = 14$, e conclui-se que se 14 é divisível por 7, 182 também o será.*

Para construirmos os critérios de divisibilidade por dois utilizamos o fato que a soma ou a diferença entre dois ou mais múltiplos de um número também é múltiplo desse número. Como a representação de um número em fatores primos é única a menos da ordem dos fatores, podemos afirmar que o 10 é igual a $2 \cdot 5$.

Quando aparece um zero em um número qualquer no final desse este número obrigatoriamente será múltiplo de dois e de cinco. Como sabemos a decomposição de um número decimal a partir da casa das dezenas apresenta a soma de números terminados sempre em zero.

Portanto um número será divisível por dois quando for par, e por cinco de acordo com o número da casa das unidades for zero ou cinco.

Exemplo 3. *O número 2340 é divisível por dois e por cinco, pois $2340 = 2 \cdot 1000 + 3 \cdot 100 + 4 \cdot 10 + 0$. Como temos uma adição onde todos os termos são divisíveis por dois e por cinco o resultado da soma também o será.*

Quando ensinamos os critérios de divisibilidade se torna curioso e auxilia no aprendizado sobre os números primos, e então, podemos nos aprofundar um pouco

mais e começar a construção do conjunto dos números naturais a partir dos números primos.

Nesta época de estudos ainda não podemos nos aprofundar muito pois o raciocínio abstrato em crianças de aproximadamente 11 anos é ainda limitado, entretanto o ensino como regras e aplicações se torna bastante produtivo.

No sétimo ano a BNCC (BRASIL, 2018) fala muito pouco, ou quase nada sobre números primos, em Unidades Temáticas (Números) e Objetos de Conhecimento (Múltiplos e divisores de um número natural) e nas Habilidades temos:

(EF07MA01) Resolver e elaborar problemas com números naturais, envolvendo as noções de divisor e de múltiplo, podendo incluir máximo divisor comum ou mínimo múltiplo comum, por meio de estratégias diversas, sem a aplicação de algoritmos.

(EF07MA05) Comparar e ordenar frações associadas às ideias de partes de inteiros, resultado da divisão, razão e operador.

Neste caso não aparecem explicitamente o estudo dos números primos, mas é fácil de perceber que estas habilidades estão diretamente ligadas ao conceito de números primos.

Quando saímos um pouco das estruturas da BNCC (BRASIL, 2018) podemos buscar outros focos como a preparação para OBMEP no nível 1 que abrange estudantes dos sextos e sétimos anos, então os números primos alcançam outros significados e podemos nos aventurar por outros conceitos.

Voltando ao crivo de Eratóstenes percebemos a forma rudimentar de encontrarmos números primos, certamente é um método seguro. Nos livros didáticos a tabela do Crivo de Eratóstenes aparece, em geral, com todos os números até cinquenta ou cem e seguidamente vamos eliminando os múltiplos anteriores (Tabela 1). Isto é um procedimento didático, mas pouco prático pois sabemos que o único número par primo é o 2 logo poderíamos fazer uma tabela a partir do 1, 2, 3, ... e depois somente números ímpares o trabalho fica reduzido:

1	2	3	5	7	6	9	11	13	15
17	19	21	23	25	27	29	31	33	35
37	39	41	43	45	47	49	51	53	55
57	59	61	63	65	67	69	71	73	75
77	79	81	83	85	87	89	91	93	95
97	99	101	103	105	107	109	111	113	115
117	119	121	123	125	127	129	131	133	135
137	139	141	143	145	147	149	151	153	155
157	159	161	163	165	167	169	171	173	175
177	179	181	183	185	187	189	191	193	195

TABELA 5 – Fonte: Próprio autor

Observamos que simplesmente tirando os números pares maiores do que dois conseguimos encontrar mais 18 números primos (Tabela 5). Poderíamos ainda excluir os números terminados em cinco e a tabela avançaria mais um pouco, estes raciocínios podem ser implementados em programas de computação e economizariam linhas de processamento, tornando os programas mais eficientes.

Quando vamos verificar se um único número é primo vamos verificando a divisão por todos os números primos até chegar ao maior número primo cujo quadrado é menor do que o número que estamos verificando, se até este limite não encontramos nenhum divisor o número é primo.

Por exemplo o próximo número da tabela acima seria 197 teria que verificar a divisibilidade de 197 por 2, 3, 5, 7, 11 e 13, como não é divisível por nenhum deles, podemos concluir que 197 é primo pois o próximo número primo é o 17 e $17^2 = 289$ e portanto qualquer número primo maior do que 13 que dividir 197 terá um resultado menor do que 13 e como todos os números já foram verificados não há mais o que ser verificado. Pensando assim o trabalho fica muito reduzido.

Esta propriedade é atribuída ao próprio Eratóstenes, segundo Pérez Y Marin (MARIN, 1928), escrevem-se os números 1, 2, e todos os ímpares até o limite que se deseja; depois se cancelam, a partir do três, os números que ocupam o terceiro lugar, porque são todos múltiplos de três ; depois desde o cinco ,os que ocupam o quinto lugar, por serem múltiplos de cinco e assim se continua até chegar a um número primo, cujo quadrado seja imediatamente inferior ao limite da tabela. Os números que ficaram sem cancelar formarão a tábua de números primos pedida. Este conceito também é atribuído ao Eratóstenes e demonstrado em lema no livro de Hefez (HEFEZ, 2016).

Quando queremos descobrir os fatores primos que compõe um número espe-

cífico podemos começar verificando se este número é divisível por algum dos primos conhecidos. Neste caso os critérios de divisibilidade ajudam bastante.

Nos conteúdos trabalhados no ensino fundamental quase sempre trabalhamos com números primos pequenos, quando os números primos começam a ficar um pouco maior os estudantes começam a apresentar muita dificuldade. Estas experiências com números primos maiores são mais apropriadas para nível superior ou para Olimpíadas de Conhecimento.

Durante este trabalho buscamos apresentar conteúdos que sejam diretamente aplicáveis aos anos finais do ensino fundamental na perspectiva de construir um conteúdo que auxilie o trabalho neste grupo de estudantes.

Segundo Pérez e Marin (MARIN, 1928), as propriedades mais importantes dos números primos se baseiam nos seguintes teoremas, cuja demonstração encontra-se no livro.

Definição 3. *Dados $n, m \in \mathbb{N}$ são chamados primos entre si se possuem como único divisor comum o número 1.*

Teorema 2.1. *Se um número primo p que não divide um inteiro a , então a e p são primos entre si.*

Demonstração:

Seja d o mdc de a e p . Então $d \mid a$ e $d \mid p$. Da relação $d \mid p$, resulta que $d = 1$ ou $d = p$, porque p é primo, e como a segunda igualdade é impossível, porque p não divide a , segue-se que $d = 1$, isto é, o $\text{mdc}(a, p) = 1$. Logo, a e p são primos entre si. ■

Corolário 2.1.1. *Se dois números não são primos entre si, admitem um divisor primo comum.*

Exemplo 4. *Dados os números 30 e 25 que não são primos entre si, pois os divisores de $D_{30} = \{1, 2, 3, 5, 6, 10, 15, 30\}$ e $D_{25} = \{1, 5, 25\}$, observe que admitem o 5 como divisor primo comum.*

Podemos demonstrar de forma simples pela razão de que um número primo só é divisível por um e por si próprio, logo se ele próprio não é divisor de um outro número, neste caso, só resta o número 1 como divisor comum e então os números são primos entre si. ■

Teorema 2.2. *Todo número composto tem pelo menos um fator primo.*

Demonstração: Para demonstrarmos este teorema percebemos que um número natural composto tem pelo menos um divisor d , se d for primo, temos um fator primo. Se não for

primo podemos dividir por um outro divisor p e assim sucessivamente até encontrarmos um fator primo, quando encontrarmos um como ultimo divisor então o penúltimo número será primo. ■

Teorema 2.3. *O conjunto dos números primos é infinito.*

Demonstração:

Provaremos por contradição, ou seja, consideramos que o conjunto dos números primos é finito. Sejam $p_1, p_2, p_3, p_4, \dots, p_k$ como sendo a representação de todos os primos. Considere agora o número n como sendo $n = p_1 \cdot p_2 \cdot p_3 \cdot p_4 \cdot \dots \cdot p_k + 1$, que é um inteiro maior que 1.

Mas n não é divisível por p_1 pois o quociente será $p_2 \cdot p_3 \cdot \dots \cdot p_k$ e resto 1. De forma análoga n não seria divisível por nenhum dos outros primos até p_k , pelo raciocínio acima. (FREIRE, 2016)

Como n é muito maior que p_k percebemos que n ou é primo ou é composto por primos não pertencentes ao suposto conjunto de todos os primos. O que leva a um absurdo.

Portanto a hipótese de existir um conjunto finito de números primos nos levou a uma contradição lógica e, conseqüentemente, a hipótese é falsa. Portanto o conjunto dos números primos é infinito. ■

Veremos algumas das propriedades dos números primos com multiplicação e potenciação de números.

Teorema 2.4. *Se um número primo n dividir um produto de vários fatores $a_1 \cdot a_2 \cdot a_3 \cdot \dots \cdot a_l$ então dividirá pelo menos um dos fatores a_i .*

Exemplo 5. *Seja $n = 7 \cdot 22 \cdot A$ e n é divisível por 3. Agora como 3 não divide 7 nem 22, então dividirá o fator A . Podemos Colocar $n = 1386$ e $A = 9$*

Corolário 2.4.1. *Todo número primo que divide uma potência de um número, divide também o próprio número.*

Exemplo 6. *Se 3 dividir A^3 , por exemplo, dividirá também A , porque $A^3 = A \cdot A \cdot A$; e 3 que por hipótese, divide o produto, divide necessariamente o único fator A .*

Corolário 2.4.2. *Se dois números são primos entre si, suas potências quaisquer também o são.*

Exemplo 7. *Sejam os números 3 e 7 primos entre si. As potências 3^n e 7^m , também o são; porque, se essas potências tivessem um divisor comum d , este divisor, dividindo 3^n também dividiria 3 e dividindo 7^m dividiria 7, de modo que 3 e 7 teriam também o fator comum d contradizendo a hipótese.*

Teorema 2.5. *Todo número primo com os fatores de um produto é primo com o produto, e todo número primo com o produto é primo com seus fatores.*

Exemplo 8. *Sejam $p = 1176 = 3 \cdot 49 \cdot 8$ e $r = 11$. Claro que r é primo com os fatores de p então r será primo com p .*

Teorema 2.6. *Seja p um número divisível por vários números primos entre si dois a dois $r_1, r_2, r_3, \dots, r_n$ então p será divisível pelo produto deles $q = r_1 \cdot r_2 \cdot r_3 \cdot \dots \cdot r_n$.*

Demonstração:

M um número divisível por cada um dos números primos $r_1, r_2, \dots, r_n$ os quais são primos entre si dois a dois.

Representando por q_1 o quociente de M por r_1 , assim $M = r_1 q_1$. Como r_2 divide o produto $M = r_1 q_1$ e é primo com r_1 logo divide q_1 . Chamando q_2 o quociente de q_1 por r_2 , temos que $q_1 = r_2 q_2$ e reescrevemos $N = 3 \cdot 5 \cdot q'$. O último divisor de N é 8 e como 8 é primo com 3 e 5 logo divide q' . Representando por q'' o quociente de q' por 8, temos $q' = 8 \cdot q''$ e $N = 3 \cdot 5 \cdot 8 \cdot q''$ logo $N : (3 \cdot 5 \cdot 8) = q''$ ■

Exemplo 9. *Tomemos $n = 240$ temos que $3|n$, $5|n$ e $8|n$, que são primos entre si. Multiplicando $3 \cdot 5 \cdot 8 = 120$ e $120|240$. Verificando o teorema.*

Corolário 2.6.1. *O mínimo múltiplo comum de vários números primos entre si é o seu produto.*

Quando trabalhamos estes conteúdos nos sextos e sétimos anos não é adequado trabalhar de forma muito abstrata. Mesmo em outros anos, muitos estudantes encontram dificuldade com questões desta natureza; entretanto, as aplicações inicialmente práticas ajudam na construção do abstrato, pois, aos poucos, vão construindo uma linguagem básica para um conhecimento mais elaborado.

Por exemplo podemos construir uma tabela com números primos da seguinte forma. Até o 25 por exemplo só temos que verificar se o número é divisível por 2 e 3, e temos: 2, 3, 5, 7, 11, 13, 17, 19, 23, para continuar até 121 temos que verificar se os números são divisíveis por 2, 3, 5 e 7.

Como estes números são contemplados com critérios simples de divisibilidade como vimos, concluímos que esses são os 30 primeiros números primos:

$$\left\{ \begin{array}{l} 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, \\ 79, 83, 89, 97, 101, 103, 107, 109, 113. \end{array} \right.$$

E poderíamos continuar a construir a tabela usando os mesmo critérios e excluindo os múltiplos de 11 até 169 e de 11 e 13 até 289.

2	3	5	7	11	13	17	19
23	29	31	37	41	53	59	61
67	71	73	79	83	89	97	101
103	109	113	127	131	137	139	149
151	157	163	167	173	179	181	191
193	197	199	211	223	227	229	233
239	241	251	257	263	271	277	281

TABELA 6 – Fonte: Próprio autor

Para os estudos do ensino fundamental esta tabela6 é de simples construção, e compreensão e útil para trabalharmos conceitos de Matemática Básica, alguns desses conceitos que podemos tratar indiretamente:

1. Conceito de Geometria Analítica da distância entre dois pontos na reta com o problema da formiga na régua.
2. Conceito que a adição e subtração de dois múltiplos de um número qualquer tem como resultado um múltiplo desse número (usando a tabuada)
3. Conceito de propriedade distributiva e fatoração de polinômios utilizando a tabuada.
4. Construção dos divisores de um número qualquer utilizando os expoentes da fatoração de um número composto em números primos.
5. Determinação da raiz quadrada exata pela construção do conjunto dos divisores de um número.

2.2.1 INTERVALOS DE NÚMEROS COMPOSTOS EM SEQUENCIA

Sabemos por observação conforme visto acima, que quando os números vão crescendo, temos cada vez menos números primos em relação ao número total de elementos.

	2	3		5		7				11		13				17		19				23	
			29		31					37					41		43					47	
		53						59		61						67				71		73	
			79				83						89								97		
101		103				107		109				113											
	127				131						137		139										149
151						157						163				167						173	
			179		181											191		193			197		199

TABELA 7 – Fonte: Próprio autor

Por exemplo, na tabela 7 temos os primos até 199, e observamos que a distância entre 2 e 3 é de apenas um número, de 3 para 5 é de dois números, de 7 para 11 é quatro.

Essas distâncias são imprevisíveis, entretanto podemos determinar algumas dessas distâncias, conseguimos determinar alguns intervalos realmente grandes usando alguns teoremas. Começamos utilizando o conceito de fatorial de um número.

Por exemplo, $4! = 4 \cdot 3 \cdot 2 \cdot 1 = 24$ sendo que o 24 não é primo. A partir deste número 24 vamos contando na sequência até aparecer o primeiro primo que neste caso é 29.

Se observamos os números deste intervalo temos: $\{24, 25, 26, 27, 28\}$ que são os 5 números compostos na sequência, sendo que 23 é primo e por isso não usamos os antecessores.

Para o caso do número 5 temos $5! = 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 = 120$. E fazendo a mesma ideia do 4 podemos encontrar um conjunto de 13 números compostos em sequência, ou seja, 114, 115, 116, 117, 118, 119, 120, 121, 122, 123, 124, 125, 126.

A razão que isto ocorre é a seguinte 119 e 121, que são os números anteriores e posteriores de 120 não são primos e daí vem uma sequência de números compostos pois $120 + 2$ e $120 - 2$ são divisíveis por 2, $120 + 3$ e $120 - 3$ são divisíveis por 3, $120 + 4$ e $120 - 4$ serão divisíveis por 4 e $120 + 5$ e $120 - 5$ serão divisíveis por 5. Como 115 e 125 são ímpares (e somando 1 viram pares logo divisíveis por 2) os próximos números também serão compostos.

Temos isso porque 120 é múltiplo de 2, 3, 4 e 5, e como $120 + 1$ não é primo e $120 - 1$ também é composto, sabemos que somando ou subtraindo um múltiplo de um número o resultado também o é.

Consultando estes intervalos, de números compostos, vemos que em torno dos fatoriais de números um pouco maiores os intervalos crescem rapidamente.

Podemos garantir que para $n! = k$: - Se o antecessor de k não for primo e o sucessor de k também não for primo, o intervalo total de números compostos tem no mínimo $2n + 1$ elementos. - Se o antecessor de k for primo e o sucessor de k não for, o intervalo de números compostos tem no mínimo $n + 1$ elementos. - Se o sucessor de k for primo e o antecessor de K não for, temos garantido um intervalo de números compostos de $n + 1$ termos. Esses intervalos podem ser maiores ainda, se depois de $n + 1$ números o antecessor deste número não for primo, temos mais $n + 1$ números compostos. O mesmo acontecendo para o sucessor.

Então temos:

$$6! = 720$$

- O antecessor é $720 - 1 = 719$ que é primo. Nosso intervalo inferior vai de 709 até 719 temos 9 números.
- O sucessor é $720 + 1 = 721 = 7 \cdot 103$, não sendo primo. Nosso intervalo superior fica de 720, $\dots$, 726, ou seja, de 7 números.

$$7! = 5.040$$

- O antecessor é $5.040 - 1 = 5.039$ é primo e o intervalo fica de 5.024 até 5.038, ou seja, 15 números.
- O sucessor é $5.040 + 1 = 5.041 = 71 \cdot 71$ não é primo e o intervalo fica de 5.040 até 5.050, ou seja, 11 números.

$$8! = 40.320$$

- O antecessor é $40.320 - 1 = 40.319 = 23 \cdot 1.753$ que não é primo.
- O sucessor é $40.320 + 1 = 40.321 = 61 \cdot 661$ que também não é primo.
- O intervalo fica de 40.290 até 40.342, ou seja, um intervalo de 53 números compostos.

$$9! = 362.880$$

- O antecessor é $362.880 - 1 = 362.879 = 112 \cdot 2.999$ que não é primo.
- O sucessor é $362.880 + 1 = 362.881 = 19 \cdot 71 \cdot 269$ que também não é primo.
- O intervalo fica de 362.868 até 362.896 com um intervalo de 29 números.

$$10! = 3.628.800$$

- O antecessor é $3.628.800 - 1 = 3.628.799 = 29 \cdot 125.131$ que não é primo.
- O sucessor é $3.628.800 + 1 = 3.628.801 = 3^4 \cdot 71 \cdot 631$ que também não é primo.
- O intervalo fica de 21 números, neste caso, exatamente $2n + 1 = 2 \cdot 10 + 1$.

$$11! = 39.916.800$$

- O antecessor é $39.916.800 - 1 = 39.916.799 = 13 \cdot 17 \cdot 23 \cdot 7.853$ que não é primo, o intervalo fica de 39.916.788 até 39.916.800 que são 13 números.

- O sucessor é $39.916.800 + 1 = 39.916.801$ é primo e o intervalo fica de 39.916.802 até 39.916.816 com 15 números.

$$12! = 479.001.600$$

- O antecessor é $479.001.600 - 1 = 479.001.599$ é primo e o intervalo fica de 479.001.588 até 479.001.598 com 11 números.
- O sucessor é $479.001.600 + 1 = 479.001.601 = 13^2 \cdot 2.834.329$ que não é primo e o intervalo fica de 479.001.600 até 479.001.628, com 29 números.

$$13! = 6.227.020.800$$

- O antecessor é $6.227.020.800 - 1 = 6.227.020.799 = 1.733 \cdot 3.593.203$ que não é primo.
- O sucessor é $6.227.020.800 + 1 = 6.227.020.801 = 83 \cdot 75.024.347$ também não é primo.
- O intervalo fica de 6.227.020.778 até 6.227.867 com 894 números compostos.

$$14! = 87.178.291.200$$

- O antecessor é $87.178.291.200 - 1 = 87.178.291.199$ que é primo e um intervalo de 15 números.
- O sucessor é $87.178.291.200 + 1 = 87.178.291.201$ que não é primo e um intervalo de 19 primos.
- O intervalo fica de 87.178.291.183 até 87.178.291.219.

$$15! = 1.307.674.368.000 \text{ e}$$

- O antecessor é $1.307.674.368.000 - 1 = 1.307.674.368.999$ que não é primo.
- O sucessor é $1.307.674.368.000 + 1 = 1.307.674.368.001$ que não é primo também.
- O intervalo é de 89 números de 1.307.674.368.953 até 1.307.674.368.043.

$$16! = 20.922.789.888.000$$

- O antecessor é $20.922.789.888.000 - 1 = 20.922.789.887.999$ não é primo.
- O sucessor é $20.922.789.888.000 + 1 = 20.922.789.888.001$ não é primo também.

- O intervalo fica de 75 números de 20.922.789.887.947 até 20.922.789.888.023.

$$17! = 355.687.428.096.000$$

- O antecessor é $355.687.428.096.000 - 1 = 355.687.428.095.999$ que não é primo
- O sucessor é $355.687.428.096.000 + 1 = 355.687.428.096.001$ também não é primo.
- O intervalo é de 89 números de 355.687.428.095.941 até 355.687.428.096.031.

$$18! = 6.402.373.705.728.000$$

- O antecessor é $6.402.373.705.728.000 - 1 = 6.402.373.705.727.999$ que não é primo.
- O sucessor é $6.402.373.705.728.000 + 1 = 6.402.373.705.728.001$ também não é primo.
- O intervalo é de 77 números de 6.402.373.705.727.959 até 6.402.373.705.728.037.

$$19! = 121.645.100.408.832.000$$

- O antecessor é $121.645.100.408.832.000 - 1 = 121.645.100.408.831.999$ não é primo.
- O sucessor é $121.645.100.408.832.000 + 1 = 121.645.100.408.832.001$ não é primo.
- O intervalo é de 189 números
- Fica de 121.645.100.408.831.899 até 121.645.100.408.832.089. Que é o maior intervalo até 21!.

$$20! = 2.432.902.008.176.640.000$$

- O antecessor é $2.432.902.008.176.640.000 - 1 = 2.432.902.008.176.639.999$ que não é primo.
- O sucessor é $2.432.902.008.176.640.000 + 1 = 2.432.902.008.176.640.001$ que não é primo.
- O intervalo vai de 2.432.902.008.176.639.969 até 2.432.902.008.176.640.029 com um total de 59 números.

$21! = 51.090.942.171.709.440.000$

- O antecessor é $51.090.942.171.709.440.000 - 1 = 51.090.942.171.709.439.999$ que não é primo.
- O sucessor é $51.090.942.171.709.440.000 + 1 = 51.090.942.171.709.440.001$ que não é primo.
- O intervalo vai de 51.090.942.171.709.439.970 até 51.090.942.171.709.440.031 com um total de 61 números.

Para trabalharmos com números com mais de 18 dígitos as ferramentas como Microsoft Excel, Libre Calc, Conversor-de-Medidas eles conseguem calcular o fatorial, mas quando pedimos para adicionar ou subtrair 1, com a quantidade de dígitos dadas eles não conseguem fazer, veja a tabela da figura 9 abaixo.

No.	Fatorial do número	Fatorial do número - 1	Fatorial do número +1
1	1	0	2
2	2	1	3
3	6	5	7
4	24	23	25
5	120	119	121
6	720	719	721
7	5040	5039	5041
8	40320	40319	40321
9	362880	362879	362881
10	3628800	3628799	3628801
11	39916800	39916799	39916801
12	479001600	479001599	479001601
13	6227020800	6227020799	6227020801
14	87178291200	87178291199	87178291201
15	1307674368000	1307674367999	1307674368001
16	20922789888000	20922789887999	20922789888001
17	355687428096000	355687428095999	355687428096001
18	6402373705728000	6402373705728000	6402373705728000
19	121645100408832000	121645100408832000	121645100408832000
20	2432902008176640000	2432902008176640000	2432902008176640000
21	51090942171709400000	51090942171709400000	51090942171709400000
22	1124000727777610000000	1124000727777610000000	1124000727777610000000

A partir do 17 o fatorial menos um e o fatorial mais um não apresenta mais diferença, e os números a partir deste também.

FIGURA 9 – Tabela com os intervalos de números compostos entre os primos com Excel

Seria portanto necessária a descoberta de outra ferramenta. Mas para constatação de que os intervalos de números compostos aumenta muito com o crescimento do fatorial.

2.3 NÚMEROS INTEIROS

De uma forma direta o conjunto dos números inteiros é apresentado da forma $\mathbb{Z} = \{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}$ e com as operações de adição e multiplicação sendo inicialmente sendo definidas.

Quando iniciamos o estudo do Conjunto dos Números Inteiros podemos começar com os números naturais e depois acrescentarmos os números negativos e o zero. Quando fazemos isso, este novo conjunto se torna fechado, em relação a operação de adição.

Agora temos que considerar que o conjunto dos divisores de um número inteiro fica acrescentado dos seus simétricos, por exemplo:

$$\begin{cases} \text{esta é uma das notações } D_{12} = \{-12, -6, -4, -3, -2, -1, 1, 2, 3, 4, 6, 12\} \\ \text{ou se preferirmos } D_{12} = \{\pm 1, \pm 2, \pm 3, \pm 4, \pm 6, \pm 12\} \end{cases}$$

Estas alterações tornam o conjunto dos Números Inteiros, um novo desafio para professores e estudantes, no início os estudantes levam um tempo para compreenderem as regras práticas para com as operações com números inteiros, no início a representação gráfica dos números inteiros ajuda muito pois torna visual a operação de adição e subtração desses números. Esta dificuldade é reconhecida inclusive na distribuição dos conteúdos no ensino fundamental, formalmente eles só vão aparecer no sétimo ano. Na BNCC (BRASIL, 2018) como Unidade Temática (Números) e Objeto de Conhecimento (Números inteiros: usos, história, ordenação, associação com pontos da reta numérica e operações) e Habilidades

(EF07MA03) comparar e ordenar números inteiros em diferentes contextos, incluindo o histórico, associá-los a pontos da reta numérica e utilizá-los em situações que envolvam adição e subtração.

(EF07MA04) resolver e elaborar problemas que envolvam operações com números inteiros.

Podemos perceber a vastidão de implicações dos números inteiros pois todo conteúdo compreendido até então agora é ampliado e isto implicará nas novas formas das quatro operações (adição, subtração, multiplicação e divisão), e suas aplicações em resolução de situações problema associados, todos estas novidades nos trazem a impressão de que o ensino nesta fase tem um grande degrau para ser alçado. Para melhorar a compreensão é recomendável utilizar diversos recursos para superar estes desafios.

Quando olhamos para o material da OBMEP (provas da 1a fase), encontramos um material vasto e bem-preparado para este fim, desde que vi alguns problemas e

apliquei em aulas a situação se tornou muito mais produtiva.

Por exemplo uns desses exercícios e a didática por trás deles:

Exemplo 10. *Uma formiguinha andou sobre a borda de uma régua, da marca de 6 cm até a marca de 20 cm. Ela parou para descansar na metade do caminho. Em que marca ela parou?*

- (a) 11 cm
- (b) 12 cm
- (c) 13 cm
- (d) 14 cm
- (e) 15 cm

Analisando esta questão da OBMEP de 2011, do nível 1, primeira fase, vemos que é uma questão aparentemente simples, pois o estudante pode, rapidamente, desenhar a régua e contar os centímetros, mas depois podemos utilizar esta questão para aprofundar este conteúdo.

Podemos imaginar a régua inteira e explicar que, se começássemos do zero o ponto final seria o trajeto completo, depois divide por dois e tem-se a metade do caminho, e quando falta o pedaço da régua temos que tirar aquele pedaço do número final e de uma forma elementar ensinamos que a distância entre dois pontos é o ponto final menos o inicial.

Além da introdução do conceito de média aritmética, este conceito, sabemos é essencial para a Matemática e a Ciência de uma forma geral, não há como compreender diversos conceitos Matemáticos sem este princípio da distância entre dois pontos.

Quando iniciamos o estudo dos números inteiros e os alunos já conhecem a história da formiga temos um bom ponto de partida para introduzir a diferença entre duas temperaturas uma positiva e outra negativa, ou saldo de uma conta bancária e assim por diante.

Quanto ao problema da formiga da OBMEP, podemos fazer algumas modificações e trabalhar outros conjuntos numéricos, como por exemplo o conjunto dos números inteiros, podemos supor a formiga caminhando numa escala de um termômetro.

Procurando compreender a dificuldade de trabalharmos as propriedades dos números inteiros, principalmente no sétimo ano, podemos atribuir, parte dela, ao fato de que a forma de executar as operações com números naturais é ligeiramente diferente da dos números inteiros, sabemos que toda mudança gera estresse e para quem possui alguma dificuldade esta passagem é difícil. Neste sentido toda forma de tornar este processo mais natural ajuda o desenvolvimento.

Neste aspecto, além da forma teórica de apresentação, podemos construir

alguns dispositivos práticos para este fim como por exemplo régua de cálculo para números inteiros, desta forma o conteúdo fica mais palpável para o aprendizado das “regras” para trabalharmos os números inteiros. Este processo se torna fundamental no início para compreendermos as regras, mais tarde não será mais possível trabalharmos desta forma pois conforme avançamos nos próximos conjuntos não há como fazermos régua para todas as situações em que trabalhamos com conjuntos mais amplos, mas o conhecimento básico continua sendo útil e verdadeiro.

Quando pensamos em números inteiros fica bastante ampliado o universo de possibilidades, nos livros didáticos, de uma forma geral, não apresenta explicitamente as propriedades das operações com números inteiros, elas são apresentadas como regras e podemos dizer que não existe uma cultura de estudo das propriedades das operações com números inteiros.

Nos livros do A. Hefez temos o Elementos de Aritmética (HEFEZ, 2006) que somente trata de números naturais e depois o Aritmética (HEFEZ, 2016) do mesmo autor que trata dos números inteiros.

Quando ele apresenta as propriedades começa com as da adição e multiplicação e apresenta a subtração como um caso particular da adição. E as define da seguinte forma (HEFEZ, 2016):

As operações de adição e multiplicação em $\mathbb{Z}$ possuem as seguintes propriedades:

1. A adição e a multiplicação são bem definidas:

Para todos $a, b, a', b' \in \mathbb{Z}$, se $a = a'$ e $b = b'$, então $a + b = a' + b'$ e $a \cdot b = a' \cdot b'$.

2. A adição e multiplicação são comutativas:

Para todos $a, b \in \mathbb{Z}$, $a + b = b + a$ e $a \cdot b = b \cdot a$.

3. A adição e a multiplicação são associativas:

Para todos $a, b, c \in \mathbb{Z}$, $(a + b) + c = a + (b + c)$ e $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.

4. A adição e a multiplicação possuem elementos neutros:

Para todo $a \in \mathbb{Z}$, $a + 0 = a$ e $a \cdot 1 = a$.

5. A adição possui elementos simétricos:

Para todo $a \in \mathbb{Z}$, existe $b (= -a)$ tal que $a + b = 0$.

6. A multiplicação é distributiva em relação a adição:

Para todo $a, b, c \in \mathbb{Z}$, $a \cdot (b + c) = a \cdot b + a \cdot c$.

Obs: Dados dois números inteiros a e b , define-se o número b menos a denotado por $b - a$, como sendo $b - a = b + (-a)$. Dizemos que $b - a$ é o resultado da subtração de b por a .

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

1. Fechamento de $\mathbb{N}$: O conjunto $\mathbb{N}$ é fechado para a adição e para a multiplicação, ou seja, para todos $a, b \in \mathbb{N}$, tem-se que $a + b \in \mathbb{N}$ e $a \cdot b \in \mathbb{N}$.
2. Tricotomia: dados $a, b \in \mathbb{N}$, uma e apenas uma, das seguintes possibilidades é verificada: (i) $a = b$ ou (ii) $b - a \in \mathbb{N}$ ou (iii) $-(b - a) \in \mathbb{N}$.

Com estas propriedades temos a possibilidade de resolver de uma forma bem estruturada os problemas tratados no ensino fundamental e médio. Estas propriedades servem também para fundamentar a continuidade destes estudos para outras aplicações mais trabalhosas, no ensino fundamental começamos no sétimo ano a utilizar de uma forma mais objetiva as aplicações destas propriedades. Após uma introdução inicial as propriedades são incluídas nos procedimentos das operações matemáticas e quase não se fala mais delas, apesar do seu uso frequente em todos os contextos. Podemos por exemplo analisar este problema:

Exemplo 11. *Maria foi fazer compras e comprou três peras, três maçãs e três laranjas, pagou três reais por cada pera. Dois por cada maçã e um real por cada laranja.*

Podemos resolver assim:

$$\text{Preço total} = 3 \cdot 3 + 3 \cdot 2 + 3 \cdot 1 = 9 + 6 + 3 = 18,$$

$$\text{ou preço total} = 3 \cdot 2 + 3 \cdot 3 + 3 \cdot 1 = 6 + 9 + 3 = 18.$$

$$\text{Ou ainda preço total} = 3 \cdot (3 + 2 + 1) = 3 \cdot 6 = 18.$$

Do ponto de vista das operações matemáticas, estamos aplicando propriedades, mas na maioria das vezes resolvemos expressões numéricas muito mais sofisticadas e nem nos damos conta de quais propriedades estamos aplicando, isto vale inclusive para operações mais complexas, por exemplo, alguém que procura por um número numa rua pensa assim se estou no número 4000, para chegar no número 5000, serão 1000, ou seja, ele utilizou a distância entre dois números na reta.

Sendo 1000 números ele deve andar dez quadras pois uma quadra tem aproximadamente 100 números, neste caso usou a regra de três simples, e rapidamente encontrou a solução, sem nem se recordar de quais propriedades ou operações fez.

Das propriedades das operações com números inteiros a divisão é a que mais ocupa nossas reflexões, pois não são totalmente previsíveis, especialmente quando queremos exatidão das divisões.

2.3.1 DIVISIBILIDADE

Prever as características de uma divisão especialmente com números muito grandes é uma arte da qual os Matemáticos têm se ocupado bastante. Podemos notar por exemplo que um dos livros mais famosos de todos os tempos “ Os Elementos de Euclides (EUCLIDES, 2009), trata de uma forma muito especial a operação de divisão e nos livros de Aritmética a maior parte deles trata desta operação em particular de forma mais demorada.

Definição 4. *Dados dois números inteiros a e b , diremos que a divide b , escrevendo $a \mid b$, quando existir $x \in \mathbb{Z}$ tal que $b = c \cdot a$. Nesse caso a é um divisor ou um fator de b .*

Exemplo 12. *São facilmente verificados que $0 \mid 0, 1 \mid 6$.*

Exemplo 13. *Também é facilmente verificados que $4 \nmid 15$, não existe inteiro c que satisfaça $15 = 4 \cdot c$.*

Nos livros didáticos mais antigos (SARDELA A. E MATTA, 1981), o autor inicia dizendo que a divisão nos inteiros não possui as propriedades de: fechamento, comutativa, elemento neutro e associativa.

2.4 DIVISÃO EUCLIDIANA

A Divisão Euclidiana é apresentada por A. Hefez (HEFEZ, 2006) da seguinte forma: Sejam a e b dois números inteiros com $b \neq 0$. Existem dois únicos números inteiros tais que: $a = b \cdot q + r$, com $0 \leq r < |b|$.

Da divisão Euclidiana temos que $r = 0 \leftrightarrow b \mid a$.

Exemplo 14. *Mostraremos dois exemplos para a divisão:*

$$\begin{cases} (a) 18 : 6 = 6 \cdot 3 + 0, \text{ logo dizemos que } 6 \text{ divide } 18, \text{ ou seja, } 6 \mid 18. \\ (b) 21 : 5 = 5 \cdot 4 + 1, \text{ logo dizemos que } 5 \text{ não divide } 21, \text{ ou seja, } 5 \nmid 21. \end{cases}$$

Podemos de imediato perceber que a divisão euclidiana é mais elaborada do que as outras operações estudadas até o momento, quando determinamos o resto r percebemos que ele pode ser, no máximo menor que o módulo de b . Desta forma conforme o número b se torna maior o número r cresce sempre uma unidade a menos do que b , portanto os restos possíveis crescem de acordo com o aumento de b .

Esta condição mostra que conforme aumentamos os números aparecem novas situações onde prever estes restos ou a combinação de restos de diversas divisões se torna cada vez mais complexo.

Neste contexto o autor (HEFEZ, 2006) não associa a divisibilidade com nenhuma operação em $\mathbb{Z}$, nem que a divisibilidade representa uma fração. Mais à frente

ele define o que será o quociente de a por b , e o faz assim: “Suponha que $a \mid b$ e que $a \neq 0$. Seja $c \in \mathbb{Z}$ tal que $b = ca$. O número inteiro c é único e determinado, é chamado de quociente de b por a e denotado por $c = \frac{b}{a}$. Observe que o quociente de b por a só está definido quando $a \neq 0$ e $a \in \mathbb{Z}$.”

Proposição 3. *Sejam $a, b, c, d \in \mathbb{Z}$, se $a \mid b$ e $c \mid d$ então $a \cdot c \mid b \cdot d$.*

Demonstração:

Se $a \mid b$ e $c \mid d$, então existem $f, g \in \mathbb{Z}$ tais que $b = f \cdot a$ e $d = g \cdot c$. Portanto, $b \cdot d = (f \cdot g)(a \cdot c)$ logo, $a \cdot c \mid b \cdot d$. Em particular, se $a \mid b$, então $a \cdot c \mid b \cdot c$, para todo $c \in \mathbb{Z}$. Como queríamos demonstrar. ■

Exemplo 15. *Para mostrar a aplicabilidade da proposição 3 escolhemos que $3 \mid 12$ e $2 \mid 4$ então $3 \cdot 2 \mid 12 \cdot 4$. E de forma particular: $3 \mid 12$ implica que $3 \cdot 2 \mid 12 \cdot 2$.*

Proposição 4. *Sejam $a, b, c \in \mathbb{Z}$, tais que $a \mid (b \pm c)$. Então $a \mid b$ se, e somente se, $a \mid c$.*

Demonstração:

Suponhamos que $a \mid (b + c)$, logo, existe $f \in \mathbb{Z}$ tal que $b + c = f \cdot a$. Agora se $a \mid b$, temos que existe $g \in \mathbb{Z}$, tal que $b = g \cdot a$. Juntando as igualdades acima, temos: $g \cdot a + c = f \cdot a$, donde segue-se que $c = (f - g) \cdot a$, donde segue-se que: $c = (f - g) \cdot a$, logo $a \mid c$; e continua: a prova da implicação contrária é totalmente análoga.

Por outro lado, se $a \mid (b - c)$ e $a \mid b$, pelo caso anterior, temos $a \mid -c$, o que implica que $a \mid c$. Como queríamos demonstrar. ■

Esta proposição é muito interessante do ponto de vista da aplicação no ensino fundamental quando falamos dos critérios de divisibilidade. É fácil a compreensão pelos alunos de que a soma de dois números divisíveis por dois, por exemplo, resulta em um outro número também divisível por dois e que a diferença entre dois números divisíveis por outro também tem como resultado um número também divisível por ele, de uma forma lúdica podemos explicar se “reunirmos” pacotes de dois em dois o resultado sempre são pacotes de dois e se “retiramos” pacotes de dois de um conjunto o que resta também são pacotes de dois, este raciocínio é facilmente aplicável a qualquer número e deste preceito podemos com tranquilidade dizer que a soma de dois números pares é sempre um número par.

Esta ideia apesar de intuitiva e muito simples não deixa de ter muitas aplicações, continuando o raciocínio podemos estendê-lo para qualquer número, ou seja, a soma e a diferença entre múltiplos de um determinado número é também múltiplo deste mesmo número.

Proposição 5. Se $a, b, c \in \mathbb{Z}$ são tais que $a \mid b$ e $a \mid c$, então para todo $x, y \in \mathbb{Z}$ temos que $a \mid (xb + yc)$.

Demonstração:

$a \mid b$ e $a \mid c$ implicam que existem $f, g \in \mathbb{Z}$ tais que $b = fa$ e $c = ga$, logo $xb + yc = x(fa) + y(ga) = (xf + yg)a$, o que prova o resultado. ■

Proposição 6. Dados $a, b \in \mathbb{Z}$, onde b é não nulo, tem-se que $a \mid b$ implica que $|a| \leq |b|$.

Demonstração:

De fato, se $a \mid b$, existe $c \in \mathbb{Z}$ tal que $b = c \cdot a$. Tomando módulos, temos que: $|b| = |c| \cdot |a|$. Como $b \neq 0$, temos que $c \neq 0$, logo $1 \leq |c|$ e, conseqüentemente, $|a| \leq |a||c| = |b|$. Em particular, se $a \in \mathbb{Z}$ e $a \mid 1$, então $0 < |a| \leq 1$, logo $|a| = 1$ e, portanto, $a = \pm 1$. Para $b \neq 0$, temos 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 $-|b| \leq a \leq |b|$. ■

Note que a relação de divisibilidade em $\mathbb{N} \cup \{0\}$ é uma relação de ordem, pois:

- (i) É reflexiva: $\forall a \in \mathbb{N}, a \mid a$
- (ii) É transitiva: se $a \mid b$ e $b \mid c$, então $a \mid c$.
- (iii) É antissimétrica: se $a \mid b$ e $b \mid a$, então $a = b$

Entretanto, a relação de divisibilidade não é uma relação de ordem em $\mathbb{Z}$, pois apesar de ainda ser reflexiva e transitiva, ela não é antissimétrica.

De fato, se $-2 \mid 2$ e $2 \mid -2$, mas $-2 \notin \mathbb{N}$.

Esta forma de apresentação é algo recente, nos livros mais antigos não encontramos uma construção tão aprimorada. Quando ensinamos Aritmética no ensino fundamental não existe uma preocupação destas demonstrações, mas para os educadores é necessário um cuidado mais apurado, alguns conceitos são amplamente utilizados na resolução de problemas. Em alguns livros mais detalhados que os didáticos e que são dedicados ao ensino fundamental e médio estas proposições são apresentadas como propriedades.

No livro de André Pérez e Marin (MARIN, 1928), por exemplo, a proposição 4 é apresentada da seguinte forma: “Todo número que divide as parcelas de uma soma divide também a soma.” (aplicamos na proposição 5 com $x = y = 1$).

Exemplo 16. Podemos citar: se 7 divide 14, 21 e 49 também dividirá $14 + 21 + 49 = 84 = 12 \cdot 7$.

Podemos continuar aplicando propriedades, $14 = 2.7$, $21 = 3.7$ e $49 = 7.7$ e $7 + 2 + 3 = 12$, estas propriedades ou proposições acabam sendo quase que curiosidades da aritmética, neste aspecto terminam por despertar além da Matemática como utilidade também como arte.

Mais adiante o autor continua “O número que divide outros dois, dividirá também a sua diferença. Aqui podemos complementar que a propriedade também é verdadeira para os números inteiros.

Proposição 7. *Sejam $a, b \in \mathbb{Z}$ e $n \in \mathbb{N}$. Temos que $a - b$ divide $a^n - b^n$.*

Demonstração:

É óbvio que a afirmação é verdadeira para $n = 1$ De fato: $a - b$ divide $a^1 - b^1 = a - b$, supondo, agora, que $a - b \mid a^n - b^n$, por indução. Vamos mostrar que vale para $n + 1$: $a^{n+1} - b^{n+1} = a.a^n - b.a^n + b.a^n - b$, $b^n = (a - b).a^n + b(a^n - b^n)$. Como $a - b \mid a - b$ e por hipótese, $a - b \mid a^n - b^n$, decorre da igualdade acima e da proposição 3.5 que $a - b \mid a^{n+1} - b^{n+1}$ estabelecendo, assim, o resultado para todo $n \in \mathbb{N}$.

Depois, Hefez (HEFEZ, 2006) diz:

“Uma aplicação interessante da proposição acima é o fato de que todo número da forma $10^n - 1$, onde n é natural, seja divisível por 9. De fato, basta pôr na posição $a = 10$ e $b = 1$, obtendo que $a - b = 9$ divide $a^n - b^n = 10^n - 1$.

Utilizando esta proposição do A. Hefez podemos concluir o critério de divisibilidade por nove e, conseqüentemente, por três. Se considerarmos que $9 \mid 10^n - 1$, com efeito, $10 = 9 + 1$, $100 = 99 + 1$, $1000 = 999 + 1$, como consequência, temos que todo número significativo seguido de zeros é um múltiplo de 9, mais o algarismo significativo.

Seja o número 500, podemos escrever $500 = 5.100 = 5.(99 + 1) = 5.99 + 5$ que é um múltiplo de 9 mais 5, como podemos decompor qualquer número no sistema decimal em múltiplos de 10 vezes o dígito escolhido.

Exemplo 17. *Considere $54725 = 50.000 + 4.000 + 700 + 20 + 5$ para cada parte temos $50.000 = 5.10.000 = 5.(9999 + 1) = 5.9999 + 5$; $4.000 = 4.(999 + 1) = 4.999 + 4$; $700 = 7.100 = 7(99 + 1) = 7.99 + 7$; $20 = 2.10 = 2(9 + 1) = 2.9 + 2$ e $5 = 5$. Logo 54.725 pode ser escrito como uma soma de múltiplos de 9 mais a soma dos valores absolutos de seus algarismos que resulta $9.k + 5 + 4 + 7 + 2 + 5 = 23$, neste caso podemos concluir, como já foi demonstrado que se um número divide uma parcela de uma soma de dois números e não divide a outra então a soma não é divisível pelo número.*

Desta forma em livros didáticos do ensino médio se mostrava como era o critério de divisibilidade por nove. Especificamente no Aritmética de Andre Perez e Marin “ desta forma decompondo um número em suas diversas ordens de unidades e

aplicando o princípio precedente concluímos que um número qualquer pode ser escrito na forma $N = 9.k + S$, onde N será divisível por 9 se e somente se S for divisível por 9, e finaliza: Como todo múltiplo de 9 é também múltiplo de 3, podemos substituir na igualdade 9 por 3 e daí resultará: $N = 3K + S$ e de forma semelhante se 3 divide S dividirá N , ou seja, $3 \mid N$ se e somente se $3 \mid S$.

Proposição 8. *Sejam $a, b \in \mathbb{Z}$ e $n \in \mathbb{N} \cup \{0\}$. Temos que $a + b$ divide $a^{2n+1} + b^{2n+1}$.*

Demonstração:

Vamos provar por indução sobre n . Assim a afirmação é verdadeira para $n = 0$, pois $a + b$ divide $a^1 + b^1 = a + b$. Suponhamos agora, que $a + b \mid a^{2n+1} + b^{2n+1}$. Escrevemos $a^{2(n+1)+1} + b^{2(n+1)+1} = a^2 \cdot a^{2n+1} - b^2 \cdot a^{2n+1} + b^2 \cdot a^{2n+1} + b^2 \cdot b^{2n+1} = (a^2 - b^2) \cdot a^{2n+1} + b^2 \cdot (a^{2n+1} + b^{2n+1})$

Como $a + b$ divide $a^2 - b^2 = (a + b)(a - b)$ e, por hipótese $a + b \mid a^{2n+1} + b^{2n+1}$, decorre das igualdades acima e da proposição 4, que $a + b \mid a^{2(n+1)+1} + b^{2(n+1)+1}$, estabelecendo, assim, o resultado para todo $n \in \mathbb{N}$.

Proposição 9. *Sejam $a, b \in \mathbb{Z}$ e $n \in \mathbb{N}$. Temos que $a + b$ divide $a^{2n} - b^{2n}$.*

Demonstração:

Novamente usaremos indução sobre n . A afirmação é verdadeira para $n = 1$, pois $a + b$ divide $a^2 - b^2 = (a + b)(a - b)$. Suponhamos agora, que $a + b \mid a^{2n+1} + b^{2n+1}$. Vamos mostrar que vale para $n + 1$: $a^{2(n+1)} - b^{2(n+1)} = a^2 a^{2n} - b^2 a^{2n} + b^2 a^{2n} - b^2 b^{2n} = (a^2 - b^2) \cdot a^{2n} + b^2 (a^{2n} - b^{2n})$. Como $a + b \mid a^2 - b^2$ e por hipótese, $a + b \mid a^{2n} - b^{2n}$, decorre das igualdades acima e da proposição 8 que $a + b \mid a^{2(n+1)} - b^{2(n+1)}$, o que estabelece, desse modo, o resultado para todo $n \in \mathbb{N}^*$.

Aplicando as proposições 8 e 9 encontramos, de imediato que $11 \mid 10^{2n+1} + 1$ e $11 \mid 10^{2n} - 1$ e verificamos: $11 = 10 + 1$, $11 \cdot 9 = 99$ e assim por diante.

E estas afirmações fundamentam a explicação do critério de divisibilidade por 11, que no Aritmética Teórica Prática de Andre Pérez e Marin; “Um número é divisível por 11, quando a diferença entre a soma dos algarismos de ordem ímpar e a dos da ordem par, contando da direita para a esquerda é um múltiplo de 11.

Os critérios de divisibilidade tornam se particularmente interessantes para decompormos um número em fatores primos. Utilizaremos neste caso os critérios somente para os números primos.

Assim sendo vamos continuar mais um pouco com critérios para divisibilidade por números primos.

Depois de pesquisar os critérios de divisibilidade semelhante ao usado para verificar a divisibilidade por sete, encontrei trabalhos na Revista do Professor de

Matemática (TORRES, 2005) que utilizavam este método para números primos até cem e analisando cuidadosamente percebi que o método aditivo e subtrativo de divisibilidade se aplica para qualquer número que seja primo com dez, isto é, que não seja par ou termine em cinco.

3 CRITÉRIOS UNIVERSAIS DE DIVISIBILIDADE

Apresentamos este capítulo intitulado “Critérios Universais de divisibilidade”, abordando aqui os critérios já conhecidos e ampliando a ideia para outros números.

A principal ideia é deixar mais acessível tanto aos professores que utilizarem este material bem como aos alunos que se interessem pelo assunto.

Podemos encontrar facilmente um critério para qualquer número que seja primo com dez. Estes critérios como vamos perceber não são únicos, existem infinitos números positivos e negativos que podem ser utilizados para qualquer número primo com dez.

Antes de entrarmos nos critérios, vamos abordar tópicos que serão utilizados nos teoremas e demonstrações que surgirão.

3.1 O SISTEMA DE NUMERAÇÃO DECIMAL

O conceito de número e o processo de contar desenvolveram-se tão antes dos primeiros registros histórico (EVES, 2004). Conforme a humanidade foi evoluindo as suas civilizações foram construindo sistemas de numeração próprios. Estes exemplos são os mais citados nos livros de matemática, por exemplo, a coleção de (JUNIOR, 2022) nos capítulos que se referem aos sistemas de numeração, exemplos como a numeração dos egípcios, dos babilônicos e dos romanos.

O sistema decimal com o próprio nome diz tem dez símbolos que chamamos de algarismos, que são: 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, sendo que o 0 (zero) é a representação da ausência de algarismo.

Como na dissertação (GOMES, 2024) o sistema decimal é também um sistema posicional onde 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 posicionada mais à direita tem peso um;
2. O seguinte, sempre da direita para a esquerda, tem peso 10^1 ;
3. O subsequente tem peso 10^2 ;
4. O seguinte tem peso 10^3 e assim por diante.

Exemplo 18. *Seja o número 45302 que na base 10 tem a representação posicional dada por $4 \cdot 10^4 + 5 \cdot 10^3 + 3 \cdot 10^2 + 0 \cdot 10^1 + 2$*

Teorema 3.1. *Sejam dados os números inteiros a e b , com $a > 0$ e $b > 1$. Existem números inteiros $n \geq 0$ e $0 \leq r_0, r_1, r_2, \dots, r_n < b$, com $r_n \neq 0$, univocamente determinados, tais que*

$$a = r_0 + r_1b + r_2b^2 + \dots + r_nb^n$$

Demonstração:

Usando Indução Completa sobre a .

Para $a = 0$, a igualdade $a = r_0 + r_1b + r_2b^2 + \dots + r_nb^n$ é satisfeita trivialmente com $n = 0$ e $r_0 = 0$, que é menor que b e positivo (considerando 0 como um caso trivialmente válido).

Usando a hipótese de indução: suponha que a afirmação seja verdadeira para um número inteiro $k \geq 0$, ou seja, suponhamos que exista uma sequência de coeficientes $r_0, r_1, \dots, r_n$, com $0 \leq r_i < b$ e $r_n \neq 0$, tal que $k = r_0 + r_1b + r_2b^2 + \dots + r_nb^n$.

Queremos provar que a propriedade vale para $k + 1$, ou seja, que podemos expressar $k + 1$ na forma $k + 1 = s_0 + s_1b + s_2b^2 + \dots + s_mb^m$, com coeficientes $0 \leq s_i < b$ e $s_m \neq 0$.

Se $r_0 < b - 1$, podemos simplesmente definir $s_0 = r_0 + 1$ e manter os demais coeficientes iguais. Neste caso, a representação ainda satisfaz as condições do teorema.

Caso contrário, se $r_0 = b - 1$, somamos 1 a k resulta em um "transbordamento" na base b , então precisamos reajustar os coeficientes:

- Definimos $s_0 = 0$.
- Somamos 1 ao próximo coeficiente r_1 .

Se $r_1 < b - 1$, então podemos definir $s_1 = r_1 + 1$ e manter os demais coeficientes.

Se $r_1 = b - 1$, ocorre um novo transbordamento e repetimos esse processo nos coeficientes seguintes, até que o primeiro coeficiente menor que $b - 1$ receba o incremento.

Esse processo necessariamente termina, pois k é finito e temos um número finito de dígitos em sua representação na base b . Conclusão

Portanto, conseguimos expressar $k + 1$ na mesma forma exigida pelo teorema, garantindo que a propriedade vale para todos os $a \geq 0$. Isso conclui a demonstração por indução. ■

Esta representação é chamada de expansão relativa à base b . Se $b = 10$ temos a expansão decimal e se $b = 2$ teremos a expansão binária.

3.2 CRITÉRIO DE DIVISIBILIDADE DE UM NÚMERO POR 2

Podemos começar com o números dois, todo número par é divisível por dois como já foi mostrado. E também que todo número cujos dois últimos algarismos formam um número divisível por quatro (2^2), será divisível por 4 e da mesma forma todo número cujo número formado pelos três últimos algarismos for divisível por oito (2^3), será divisível por 8 e assim por diante.

Proposição 10. *Um número natural $n = a_k \cdot a_{k-1} \dots a_2 \cdot a_1 \cdot a_0$ 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, temos que

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

Podemos reescrever n como $n = 10 \cdot m + a_0$, sendo $m = a_k \cdot 10^{k-1} + a_{k-1} \cdot 10^{k-2} + \dots + a_2 \cdot 10 + a_1$. Como 10 é divisível por 2, claro que m será divisível por 2, então n só será divisível por 2 se a_0 é divisível por 2, ou seja, $a_0 \in \{0, 2, 4, 6, 8\}$ que são os múltiplos de 2. ■

Proposição 11. *Um número natural $n = a_k \cdot a_{k-1} \dots a_2 \cdot a_1 \cdot a_0$ é divisível por 2^2 se, e somente se, o número formado pelos seus dois últimos algarismos for um múltiplo de 2^2 .*

Escrevendo o número natural n na base 10, temos que

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

Podemos reescrever n como $n = 10^2 \cdot m + a_1 \cdot 10 + a_0$, sendo $m = a_k \cdot 10^{k-1} + a_{k-1} \cdot 10^{k-2} + \dots + a_2$. Como 10^2 é divisível por 2^2 , claro que m será divisível por 2^2 , então n só será divisível por 2^2 se $a_1 \cdot 10 + a_0$ é divisível por 2^2 , ou seja, $a_1 \cdot 10 + a_0$ pertence ao conjuntos dos múltiplos de 2^2 . ■

Proposição 12. *Um número natural $n = a_k \cdot a_{k-1} \dots a_2 \cdot a_1 \cdot a_0$ é divisível por 2^3 se, e somente se, o número formado pelos seus três últimos algarismos pertence ao conjunto dos múltiplos de 2^3 .*

Escrevendo o número natural n na base 10, temos que

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

Podemos reescrever n como $n = 10^3 \cdot m + a_2 \cdot 10^2 + a_1 \cdot 10 + a_0$, sendo $m = a_k \cdot 10^{k-1} + a_{k-1} \cdot 10^{k-2} + \dots + a_3$. Como 10^3 é divisível por 2^3 , claro que m será divisível por 2^3 , então n só será divisível por 2^3 se $a_2 \cdot 10^2 + a_1 \cdot 10 + a_0$ é divisível por 2^3 , ou seja, $a_2 \cdot 10^2 + a_1 \cdot 10 + a_0$ pertence ao conjunto dos múltiplos de 2^3 . ■

Teorema 3.2. *Se o número n tiver os últimos r algarismos formando um número divisível por 2^r , então todo o número será divisível por 2^r .*

Demonstração:

Utilizando a mesma ideia das proposições 10, 11 e 12 e escrevendo o número natural n na base 10, temos que

$$n = a_k \cdot 10^k + a_{k-1} \cdot 10^{k-1} \dots a_2 \cdot 10^2 + a_1 \cdot 10 + a_0, k \geq r.$$

Podemos reescrever n como $n = 10^r \cdot m + 10^{r-1} \cdot a_{r-1} + \dots + a_2 \cdot 10^2 + a_1 \cdot 10 + a_0$, sendo $m = 10^{k-r} \cdot a_{k-r} + \dots + 10 \cdot a_{r-1} + a_r$. Como 10^r é divisível por 2^r , claro que m será divisível por 2^r , então n só será divisível por 2^r se os últimos r algarismos formarem um número múltiplo de 2^r . ■

3.3 CRITÉRIO DE DIVISIBILIDADE DE UM NÚMERO POR 5

Proposição 13. *Um número natural $n = a_k \cdot a_{k-1} \dots a_2 \cdot a_1 \cdot a_0$ é divisível por 5 se, e somente se, seu último algarismo pertence ao conjunto $\{0, 5\}$.*

Demonstração:

Escrevendo o número natural n na base 10, temos que

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

Podemos reescrever n como $n = 10 \cdot m + a_0$, sendo $m = a_k \cdot 10^{k-1} + a_{k-1} \cdot 10^{k-2} + \dots + a_2 \cdot 10 + a_1$. Como 10 é divisível por 5, claro que m será divisível por 5, então n só será divisível por 5 se a_0 é divisível por 5, ou seja, $a_0 \in \{0, 5\}$ que são os múltiplos de 5. ■

Proposição 14. *Um número natural $n = a_k \cdot a_{k-1} \dots a_2 \cdot a_1 \cdot a_0$ é divisível por 5^2 se, e somente se, seus dois últimos algarismos formarem um número múltiplo de 5^2 .*

Escrevendo o número natural n na base 10, temos que

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

Podemos reescrever n como $n = 10^2 \cdot m + a_1 \cdot 10 + a_0$, sendo $m = a_k \cdot 10^{k-1} + a_{k-1} \cdot 10^{k-2} + \dots + a_2$. Como 10^2 é divisível por 5^2 , claro que m será divisível por 5^2 , então n só será divisível por 5^2 se $a_1 \cdot 10 + a_0$ é divisível por 5^2 , ou seja, $a_1 \cdot 10 + a_0$ pertence ao conjunto dos múltiplos de 5^2 . ■

Proposição 15. *Um número natural $n = a_k \cdot a_{k-1} \dots a_2 \cdot a_1 \cdot a_0$ é divisível por 5^3 se, e somente se, seus três últimos algarismos formarem um número múltiplo de 5^3 .*

Escrevendo o número natural n na base 10, temos que

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

Podemos reescrever n como $n = 10^3 \cdot m + a_2 \cdot 10^2 + a_1 \cdot 10 + a_0$, sendo $m = a_k \cdot 10^{k-1} + a_{k-1} \cdot 10^{k-2} + \dots + a_3$. Como 10^3 é divisível por 5^3 , claro que m será divisível por 5^3 , então n só será divisível por 5^3 se $a_2 \cdot 10^2 + a_1 \cdot 10 + a_0$ é divisível por 5^3 , ou seja, $a_2 \cdot 10^2 + a_1 \cdot 10 + a_0$ pertence ao conjunto dos múltiplos de 5^3 . ■

Teorema 3.3. *Se o número n tiver os últimos r algarismos formando um número divisível por 5^r , então todo o número será divisível por 5^r .*

Demonstração:

Utilizando a mesma ideia das proposições 13, 14 e 15 e escrevendo o número natural n na base 10, temos que

$$n = a_k \cdot 10^k + a_{k-1} \cdot 10^{k-1} \dots a_2 \cdot 10^2 + a_1 \cdot 10 + a_0, k \geq r.$$

Podemos reescrever n como $n = 10^r \cdot m + 10^{r-1} \cdot a_{r-1} + \dots + a_2 \cdot 10^2 + a_1 \cdot 10 + a_0$, sendo $m = 10^{k-r} \cdot a_{k-r} + \dots + 10 \cdot a_{r-1} + a_r$. Como 10^r é divisível por 5^r , claro que m será divisível por 5^r , então n só será divisível por 5^r se os últimos r algarismos formarem um número múltiplo de 5^r . ■

Excluindo todos os números divisíveis por 2 ou por 5 restam os números terminados em 1, 3, 7 ou 9, todos esses números tem um critério quase que imediato que pode ser usado pelo número individualmente ou por um determinado conjunto formado exclusivamente com números terminados em 1, 3, 7 ou 9.

3.4 CRITÉRIO DE DIVISIBILIDADE DE NÚMEROS PRIMOS COM 10

Como podemos chegar a essa conclusão?

Começamos pelo número 3: um número será divisível por 3 quando o número sem o último algarismo somado com o último algarismo multiplicado por 1 também o for.

Exemplo 19. *A seguir mostamos dois exemplos:*

O processo pode ser repetido quantas vezes for necessário até que o número seja suficientemente pequeno e que pode ser possível identificar visualmente que o número é divisível por três. De forma semelhante podemos considerar o número sem o último algarismo subtraído do último algarismo multiplicado por dois. Se somarmos

5206 é divisível por 3? Tomamos $520 + 6.1 = 526$ Continuando $52+6.1=58$ E por fim $5+8.1=13$ 13 não é divisível por 3 logo 5206 não é divisível por 3.	5205 é divisível por 3 ? Tomamos $520+5.1 = 525$ Continuando $52+5.1=57$ E por fim $5+7.1=12$ 12 é divisível por 3 logo 5205 é divisível por 3.
---	--

FIGURA 10 – Fonte: Próprio autor

$1 + 2 = 3$. Este fato se repete de forma semelhante para todo número terminado em 1, 3, 7 ou 9. E não somente pela adição do último número multiplicado por um ou a subtração do último número multiplicado por dois.

Podemos afirmar que o conjunto composto de infinitos números inteiros como critério de divisibilidade aditivo e subtrativo para o número 3 pode ser escrito da seguinte forma: $A = \{\dots, -8, -5, -2, 1, 4, \dots\}$. Sendo os números positivos do critério aditivo e os números negativos do critério subtrativo.

Quando demonstrarmos isso ficará fácil perceber que o processo é semelhante para todo número terminado em 1, 3, 7 ou 9.

Teorema 3.4. *O número $(10 \cdot a + b)$ é divisível por 3 se, e somente se, $(a - 2b)$ é divisível por 3.*

Demonstração:

Primeiro provaremos que se $a - 2b$ é divisível por 3 então $(10 \cdot a + b)$ é divisível por 3.

Podemos escrever $a - 2b = 3k$ e multiplicamos a equação por $(.10)$. Assim $10a - 20b = 3 \cdot 10 \cdot k$, somando em ambos os termos $21b$ e chamando $30k = 3k'$, reescrevemos por $10a - 20b + 21b = 3k' + 21b \rightarrow 10a + b = 3k''$, portanto $(10a + b)$ é divisível por 3.

Agora Suponha que $10a + b$ é divisível por 3, logo $10a + b = 3k$ e podemos escrever $b = 21b - 20b$ assim $10a + 21b - 20b = 3k \rightarrow 10a - 20b = 3k - 21b = 3k'$ e colocando 10 em evidência temos $10(a - 2b) = 3k'$, como 3 não divide 10, logo ele divide $(a - 2b)$, o que prova a equivalência. ■

Exemplo 20. *Se queremos saber se um número qualquer é divisível por três, por exemplo se 183 é divisível por três, fazemos a divisão e percebemos que 183 é igual a $3 \cdot 61$, logo 183 é divisível por 3. Podemos, de outra forma podemos retirar o último*

algarismo, isto é, o 3, multiplicar por 2 e subtrair de 18, ou seja, $18 - 2 \cdot 3 = 12$, e conclui-se que se 12 é divisível por 3, 183 também o será.

Como $10 = 2 \cdot 5$ e o número que desejamos estabelecer o critério nunca será divisível por 10 pois termina em 1, 3, 7 ou 9 ele sempre dividirá o outro termo seja ele qual for, e a forma do número será:

- (I) Se o número terminar em 3, temos que ele pode ser escrito como $10n + 3$ e o número encontrado para o critério de divisibilidade por 3 será da forma $1 + 3.n$.
- (II) Se o número terminar em 7, temos que ele pode ser escrito como $10n + 7$ e o número encontrado para o critério de divisibilidade por 7 será da forma $5 + 7.n$.
- (III) Se o número terminar em 1, temos que ele pode ser escrito como $1 + 10n$ e o número encontrado para o critério de divisibilidade será da forma $1 + 9.n$.
- (IV) Se o número terminar em 9, temos que ele pode ser escrito como $9 + 10n$ e o número encontrado para o critério de divisibilidade por 9 será da forma $1 + n$.

Pois, no caso dos números usados para o critério de divisibilidade da forma $10n + 3$, é fácil perceber que o menor número positivo para $n = 0$ somado, em módulo, com o maior número negativo será sempre igual ao número primo do qual estamos tratando, por exemplo se o número que temos para multiplicar o último dígito do critério para 3 é o número 1, então o maior número negativo será o 2, pois $1 + 2 = 3$, a sequência não possui início ou fim. Fazendo uma tabela temos:

I) Sendo $a = \{0, 1, 2, 3, \dots, n\}$

a	n=0	n=1	n=2	n=3	n=4	n=5	n=n
3	1	4	7	10	13	16	$1+3n$
13	4	17	30	43	56	69	$4+13n$
23	7	30	53	76	99	122	$7+23n$
...	...	...	...	...	...	...	...
$10n+3$	$1+3n$	$4+13n$	$7+23n$	$10+33n$	$13+43n$	$16+53n$	f^*

TABELA 8 – Tabela 1a

$$f^* = (1 + 3n) + (10n + 3) \cdot n$$

$$g^* = (-2 - 7n) - (10n + 3) \cdot n$$

No caso do 7 temos o primeiro número positivo sendo o 5 logo o maior número negativo será o -2 . O motivo que justifica a característica desta soma é que para acharmos o próximo número da direita somamos 7 e para à esquerda é subtraído 7, logo os dois números, o primeiro positivo e o primeiro negativo somados resultam no próprio número.

a	n=0	n=1	n=2	n=3	n=4	n=5	n=n
3	-2	-5	-8	-11	-14	-17	-2-3n
13	-9	-22	-35	-48	-61	-74	-9-13n
23	-16	-39	-62	-85	-108	-131	-16-23n
...	...	...	...	...	...	...	...
10n+3	-2-7n	-5-17n	-8-27n	-11-37n	-14-47n	-17-57n	g^*

TABELA 9 – Tabela 1b

À partir desta lógica concluímos que para os números cujo dígito das unidades é o 7 ficam da seguinte forma:

a	n=0	n=1	n=2	n=3	n=4	n=5	n=n
7	5	12	19	26	33	40	5+7n
17	12	29	46	63	80	97	12+17n
27	19	46	73	100	127	154	19+27n
...	...	...	...	...	...	...	...
10n+7	5+7n	12+17n	19+27n	26+37n	33+47n	40+57n	h^*

TABELA 10 – Tabela 2a

$$h^* = (5 + 7n) + (10n + 7) \cdot n$$

a	n=0	n=1	n=2	n=3	n=4	n=5	n=n
7	-2	-9	-16	-23	-30	-37	5-7n
17	-5	-22	-39	-56	-73	-90	-5-17n
27	-8	-35	-62	-89	-116	-143	-8-27n
...	...	...	...	...	...	...	...
10n+7	-2-3n	-9-13n	-16-23n	-23-33n	-30-43n	-37-53n	i^*

TABELA 11 – Tabela 2b

$$i^* = (-2 - 3n) - (10n + 7) \cdot n$$

Usando a mesma ideia para os números cujo dígito das unidades é o 1 aparece nas próximas tabelas.

a	n=0	n=1	n=2	n=3	n=4	n=5	n=n
11	10	21	32	43	54	65	10+11n
21	19	40	61	82	103	124	19+21n
31	28	59	90	121	152	183	29+31n
...	...	...	...	...	...	...	...
11+10n	10+9n	21+9n	32+29n	43+39n	54+49n	65+59n	j^*

TABELA 12 – Tabela 3a

$$j^* = (10 + 9n) + (11 + 10n) \cdot n$$

$$k^* = -(n + 1) - (11 + 10n) \cdot n$$

a	n=0	n=1	n=2	n=3	n=4	n=5	n=n
11	-1	-12	-23	-34	-45	-56	-1-11n
21	-2	-23	-44	-65	-86	-107	-2-21n
31	-3	-34	-65	-96	-127	-158	-3-33n
...	...	...	...	...	...	...	...
11+10n	-1-n	-12-11n	-23-21n	-34-31n	-45-41n	-56-51n	k^*

TABELA 13 – Tabela 3b

a	n=0	n=1	n=2	n=3	n=4	n=5	n=n
9	1	10	19	28	37	46	1+9n
19	2	21	40	59	78	97	2+19n
29	3	32	61	90	119	148	3+29n
...		...	...	...	...	...	...
19+10n	1+n	10+11n	19+21n	28+31n	37+41n	46+51n	l^*

TABELA 14 – Tabela 4a

$$l^* = (n + 1) + (9 + 10n) \cdot n$$

a	n=0	n=1	n=2	n=3	n=4	n=5	n=n
9	-8	-17	-26	-35	-44	-53	-8-9n
19	-17	-36	-55	-74	-93	-112	-17-19n
29	-26	-30	-53	-76	-99	-122	-26-29n
...	...	...	...	...	...	...	...
19+10n	-8-9n	-17-19n	-26-29n	-35-39n	-44-49n	-53-59n	m^*

TABELA 15 – Tabela 4b

$$m^* = (-8 - 9n) - (9 + 10n) \cdot n$$

3.5 ARITMÉTICA DOS RESTOS

Seja m um número natural diferente de zero. Diremos que dois números a e b são congruentes módulo m se os restos de sua divisão por m são iguais .

Quando os inteiros a e b são congruentes módulo m , escrevemos $a \equiv b \pmod{m}$.

O teorema Chinês dos Restos resolve sistemas de congruências e como os critérios de divisibilidade subtrativo e aditivo para números terminados em 1, 3, 7 e 9 podem ser representados por congruências então o teorema Chinês dos Restos pode ser usado para encontrar números que são critérios de divisibilidade comum para diversos números.

Com estas tabelas, percebemos que estes critérios valem para todo número terminado em 1, 3, 7 ou 9, sendo primo ou não. Percebemos também que os números se repetem, isto é um mesmo número pode ser critério para diversos outros. Assim sendo podemos utilizar o Teorema Chinês do Resto para determinar quais são esses números .

Lembramos que o máximo divisor comum entre a e b é representado por (a, b) e o mínimo múltiplo comum de a e b por $mmc(a, b)$.

Teorema 3.5 (Teorema Chinês do Resto). *Se $(m_i, m_j) = 1$, para todo par (m_i, m_j) com $i \neq j$, então o sistema de congruências (1) possui uma única solução módulo $M = m_1 \cdot m_2 \cdot m_3 \cdot \dots \cdot m_r$.*

$$X \equiv c_i \pmod{m_i} \quad i = 1, \dots, r \quad (1)$$

As soluções são $x = M_1 y_1 c_1 + \dots + M_r y_r c_r + tM$ onde $t \in \mathbb{Z}$, $M_i = \frac{M}{m_i}$ e y_i é solução de $M_i Y \equiv 1 \pmod{m_i}$, $i = 1, \dots, r$.

Demonstração:

Vamos provar inicialmente que x é uma solução simultânea do sistema.

De fato, como $m_i | M_j$, se $i \neq j$ e $M_i y_i \equiv 1 \pmod{m_i}$, segue-se que $X = M_1 y_1 c_1 + \dots + M_r y_r c_r \equiv M_i y_i c_i \equiv c_i \pmod{m_i}$

Por outro lado, se $x \equiv x' \pmod{m_i}$, para todo $i = 1, \dots, r$. Como $(m_i, m_j) = 1$ para $i \neq j$, segue-se que $[m_1, \dots, m_r] = m_1 \dots m_r = M$

E, conseqüentemente, pelas propriedades adicionais das congruências relacionadas com a multiplicação temos que $x \equiv x' \pmod{M}$. Como queríamos demonstrar.

Exemplo 21. *Explorando a linha dos números do critério de divisibilidade por 7, ao ser dividido por 7 deixa resto 5 e a linha dos números do critério de divisibilidade por 11 tem como resto ao ser dividido por 11 o número 10, logo se considerarmos o conjunto dos números que são usados nos critérios de divisibilidade por 7 e por 11 (conjunto K) usamos as seguintes congruências e determinamos K pelo Teorema Chinês do Resto:*

i	Equações	A	M	$\overline{M}$	$\overline{M}^{-1}$	A.M. $\overline{M}^{-1}$	
1	$K \equiv 5 \pmod{7}$	5	11	4	2	110	$670 \pmod{77}$
2	$K \equiv 10 \pmod{11}$	10	7	7	8	560	$670 \equiv 54 \pmod{77}$
						670	$K = \{ \dots, -23, 54, \dots \}$

Observe que na penúltima coluna somamos $110 + 560 = 670$, assim $670 \pmod{77} (= 11 \cdot 7)$ como 670 dividido por 77 dá 8 e sobra 54 portanto $670 \equiv 54 \pmod{77}$ para encontrarmos K e um dos elementos é 54 e o outro $54 - 77 = -23$.

Faremos uma verificação do exemplo acima, temos que $54 = 7 \cdot 7 + 5$ e também $54 = 11 \cdot 4 + 10$.

Queremos saber se o número 761761 é divisível por 7 e por 11 . Utilizando o método aditivo:

$$761761 \rightarrow 76176 + 54 = 76230;$$

$$76230 \rightarrow 7623 + 0 = 7623;$$

$$7623 \rightarrow 762 + 3 \cdot 54 = 924;$$

$$924 \rightarrow 92 - 4 \cdot 23 = 0.$$

como 7 e 11 dividem zero, logo 7 e 11 dividem 761761, e podemos confirmar :

$$761761 = 7 \cdot 11 \cdot 9893$$

$$76.230 = 7 \cdot 11 \cdot 990$$

$$924 = 7 \cdot 11 \cdot 12$$

$$0 = 0 \cdot 7 \cdot 11$$

Por outro lado, somando 1 ao número 761761 ele não será divisível nem por 7 nem por 11, vejamos o que acontece:

$$761761 + 1 \rightarrow 761762;$$

$$761762 \rightarrow 76176 + 2 \cdot 54 = 76284;$$

$$76284 \rightarrow 7628 + 4 \cdot 54 = 7844;$$

$$7844 \rightarrow 784 + 4 \cdot 54 = 1000;$$

$$1000 \rightarrow 100 + 0 \cdot 54 = 100;$$

$$100 \rightarrow 10 + 0 \cdot 54 = 10;$$

$$10 \rightarrow 1 + 0 \cdot 54 = 1.$$

E como o número 1 não é divisível por 7 ou 11, o número 61762 não é divisível por 7 ou 11.

Os processos já haviam sido confirmados por teoremas conhecidos, estas verificações são meramente ilustrativas.

Exemplo 22. Consideremos agora outro sistema:

$$\begin{cases} K \equiv 5 \pmod{7} \\ K \equiv 10 \pmod{11} \\ K \equiv 4 \pmod{13} \end{cases}$$

i	Equações	A	M	$\overline{M}$	$\overline{M}^1$	A.M. $\overline{M}^1$	
1	$K \equiv 5 \pmod{7}$	5	143	3	5	3575	$10911 \pmod{1001}$
2	$K \equiv 10 \pmod{11}$	10	91	3	4	3640	$10911 \equiv 901 \pmod{1001}$
3	$K \equiv 4 \pmod{13}$	4	77	12	12	3696	$K \equiv 901 \pmod{1001}$
						10911	$K = \{ \dots, -100, 901, \dots \}$

Faremos uma verificação do exemplo acima, temos que $901 = 126 \cdot 7 + 5$, $901 = 81 \cdot 11 + 10$ e também $901 = 69 \cdot 13 + 4$.

Queremos saber se o número 821.821 é divisível por 7, 11 e por 13. Utilizando o método aditivo:

$$821821 \rightarrow 82182 + 1 \cdot 901 = 83083;$$

$$83083 \rightarrow 8308 + 3 \cdot 901 = 11011;$$

$$11011 \rightarrow 1101 + 901 = 2002;$$

$$2002 \rightarrow 200 - 2 \cdot 100 = 0.$$

Como os números 7, 11 e 13 são divisores de zero então são também de 821.821 e podemos confirmar escrevendo os passos:

$$821.821 = 7 \cdot 11 \cdot 13 \cdot 821$$

$$83083 = 7 \cdot 11 \cdot 13 \cdot 81$$

$$11011 = 7 \cdot 11 \cdot 13 \cdot 11$$

$$2002 = 7 \cdot 11 \cdot 13 \cdot 2$$

$$0 = 7 \cdot 11 \cdot 13 \cdot 0$$

Exemplo 23. *Agora um outro exemplo para firmar a ideia:*

i	Equações	A	M	$\overline{M}$	$\overline{M}^{-1}$	A.M. $\overline{M}^{-1}$	
1	$K \equiv 5 \pmod{7}$	5	117	5	3	1755	$3358 \pmod{819}$
2	$K \equiv 1 \pmod{9}$	1	91	1	1	91	$3358 \equiv 82 \pmod{819}$
3	$K \equiv 4 \pmod{13}$	4	63	11	6	1512	$K \equiv 82 \pmod{819}$
						3358	$K = \{ \dots, -819, 82, \dots \}$

Notamos que os exercícios que compreendem o Teorema Chinês do Resto e critérios de divisibilidade são de certa forma complexos de serem resolvidos, mas facilmente verificáveis.

Faremos uma verificação do exemplo acima, temos que $82 = 11 \cdot 7 + 5$, $82 = 9 \cdot 9 + 1$ e também $82 = 6 \cdot 13 + 4$

A pergunta é se o número 605.241 é divisível por 7, 11 e 13. Utilizando o método aditivo:

$$605241 \rightarrow 60524 + 1 \cdot 82 = 60606;$$

$$60606 \rightarrow 6060 + 6 \cdot 82 = 6552;$$

$$6552 \rightarrow 655 + 2 \cdot 82 = 819;$$

$$819 \rightarrow 819 = 7 \cdot 11 \cdot 13.$$

E podemos confirmar :

$$605.241 = 7 \cdot 11 \cdot 13 \cdot 739$$

$$60.606 = 7 \cdot 11 \cdot 13 \cdot 74$$

$$6552 = 7 \cdot 11 \cdot 13 \cdot 8$$

$$819 = 7 \cdot 11 \cdot 13$$

4 CONCLUSÃO

O ensino da Matemática é um campo dinâmico, onde não há certezas absolutas sobre o próprio trabalho. Muitas vezes, nos deparamos com surpresas positivas que nos estimulam e, em outros momentos, com desafios que se tornam oportunidades de reflexão para o aprimoramento da prática docente.

Neste estudo, buscamos atingir os objetivos propostos: introduzir os conceitos da reta numérica e os princípios algébricos de forma concreta, estudando os conjuntos numéricos desde os naturais, explorando as características dos números primos e compreendendo os números inteiros e a divisão euclidiana. Ao longo do percurso, conseguimos trabalhar esses conteúdos de maneira acessível, proporcionando uma base sólida para o entendimento dos fundamentos matemáticos.

Desde o início deste curso, apresentei aos meus alunos os conteúdos de forma apropriada, destacando a importância do Princípio Fundamental da Aritmética, essencial para a transição dos primeiros anos do ensino fundamental para os anos finais, a partir do sexto ano. A abordagem adotada mostrou-se eficaz ao associar grandes descobertas matemáticas a matemáticos jovens, como Carl Friedrich Gauss, que, aos dez anos, já havia feito contribuições notáveis. Ao despertar a curiosidade dos alunos e mostrar que princípios simples podem ter um impacto significativo, o ensino se tornou mais atrativo e produtivo.

Nos estudos sobre números primos, investigamos os critérios de divisibilidade, compreendendo sua aplicabilidade universal. Essa pesquisa nos permitiu aprofundar conceitos que, muitas vezes, não são explorados nos estudos matemáticos convencionais. Embora os números primos tenham sido amplamente estudados ao longo da história, ainda representam um mistério, pois não há uma fórmula definitiva para determinar seu sucessor ou antecessor.

Um dos tópicos mais fascinantes que podem ser explorados são os números primos de Mersenne, definidos pela expressão $M_n = 2^n - 1$, onde n também é um número primo. Exemplos clássicos desses números incluem:

- Para $n = 2$: $M_2 = 2^2 - 1 = 3$, que é primo.
- Para $n = 3$: $M_3 = 2^3 - 1 = 7$, que também é primo.
- Para $n = 5$: $M_5 = 2^5 - 1 = 31$, outro número primo.
- Para $n = 7$: $M_7 = 2^7 - 1 = 127$, que continua sendo primo.

Esses números desempenham um papel importante na busca pelos maiores primos conhecidos, uma vez que, utilizando computadores de alto desempenho, matemáticos conseguiram encontrar números de Mersenne com mais de 24 milhões de dígitos. Entretanto, ainda não há uma forma exata de prever onde estará o próximo número primo de Mersenne, tornando esse estudo um desafio constante.

Além disso, conseguimos verificar na prática as dificuldades de cálculos envolvendo números extremamente grandes. Calculadoras comuns operam até cerca de 18 dígitos, enquanto ferramentas online, como o site Numbermatics, chegam a aproximadamente 21 dígitos. A partir desse limite, entramos em um território ainda desconhecido, onde novas estratégias computacionais precisam ser desenvolvidas para avançarmos nesse estudo.

Com este trabalho, atingimos nosso objetivo de apresentar os conceitos fundamentais da reta numérica e princípios algébricos de maneira acessível e concreta. Além disso, proporcionamos aos alunos uma visão mais ampla sobre a Matemática, indo além dos cálculos e fórmulas para estimular a curiosidade e a pesquisa. Como toda boa investigação matemática, fica um questionamento para futuras pesquisas: quais seriam as formas mais eficazes para calcular e analisar números extremamente grandes? Certamente, essa questão será levada adiante, e os próximos avanços nessa área nos trarão novas e surpreendentes descobertas.

ANEXO

Neste anexo colocamos as demonstrações dos critérios para divisibilidade aditivos e subtrativos.

Critérios para divisibilidade aditivos e subtrativos para números terminados em 1 (um)

Esta é a demonstração da coluna da tabela (tabela 3a = aditivo e 3b = subtrativo)

Proposição 16. *A equação $(10a + b) = (10n + 1) \cdot k$ é verdadeira se, e somente se $[a + b(1 + 9n)] = (10n + 1) \cdot q$ também é verdadeira.*

$(\Rightarrow)$

Provaremos primeiro que se $(10a + b) = (10n + 1) \cdot k$ então $(a + b(1 + 9n)) = (10n + 1) \cdot q$.

Seja $(10a + b) = (10n + 1) \cdot k$ somando em ambos os lados $9b(10n + 1)$ encontramos:

$$(10a + b) + 9b(10n + 1) = (10n + 1) \cdot k + 9b(10n + 1)$$

$$10a + b + 90bn + 9b = (10n + 1) \cdot (k + 9b)$$

$$10a + 10b + 90bn = (10n + 1) \cdot k_1; k_1 = k + 9b$$

$$10 \cdot (a + b + 9bn) = (10n + 1) \cdot k_1$$

$$10 \cdot (a + b(1 + 9n)) = (10n + 1) \cdot k_1$$

$$(10, 10n + 1) = 1$$

$$(a + b(1 + 9n)) = (10n + 1) \cdot k_2$$

$$k_2 = q$$

O que prova a 1a implicação.

$(\Leftarrow)$

Agora se $(a + b(1 + 9n)) = (10n + 1) \cdot q$ então $(10a + b) = (10n + 1) \cdot k$.

Seja $(a + b(1 + 9n)) = (10n + 1) \cdot q$ multiplicando a equação por 10 encontramos:

$$\begin{aligned}
10 \cdot (a + b(1 + 9n)) &= 10 \cdot [(10n + 1) \cdot q] \\
10a + 10b(1 + 9n) &= (10n + 1) \cdot q_1; q_1 = 10 \cdot q \\
10a + 10b + 90bn &= (10n + 1) \cdot q_1 \\
10a + b + 9b + 90bn &= (10n + 1) \cdot q_1 \\
(10a + b) + 9b(1 + 10n) &= (10n + 1) \cdot q_1 \\
(10a + b) &= (10n + 1) \cdot q_1 - [9b(1 + 10n)] \\
(10a + b) &= (10n + 1) \cdot (q_1 - 9b) \quad (10a + b) = (10n + 1) \cdot q_2 \\
q_2 &= k
\end{aligned}$$

O que prova a 2a implicação. ■

Exemplo 24. *Tomemos dois valores para n*

(a) *Para $n = 0$:*

- *temos o número $(10n + 1) = 1$ e*
- *seu critério aditivo de divisibilidade é $(1 + 9n) = 1$.*
- *Como todo número é divisível por um temos que sempre será verdadeiro*

(b) *Para $n = 1$*

- *temos o número $(10n + 1) = 11$ e*
- *seu critério aditivo de divisibilidade é $(1 + 9n) = 10$.*
- *Escolhendo $157.861 = 11 \cdot 14351$ é múltiplo de 11 e o critério aditivo aplicado repetidamente determina sempre um múltiplo de 11.*
- *Observe que 157.861 fica $15.786 + 10 \cdot 1 = 15.796 = 11 \cdot 1436$ (somando sem o último algarismo) e 15.796 fica $1579 + 6 \cdot 10 = 1639 = 11 \cdot 149$ (igualmente somando sem o último algarismo) e 1639 fica $163 + 9 \cdot 10 = 253 = 11 \cdot 23$ e por fim 253 fica $25 + 3 \cdot 10 = 55 = 11 \cdot 5$.*
- *Colocamos um número sabidamente múltiplo de onze, para evidenciar que durante o processo se o número é divisível por onze, todos números encontrados durante o processo também serão.*

(c) *Para $n = 613$:*

- *temos o número $(10n + 1) = 6131$ e*
- *seu critério aditivo de divisibilidade é $(1 + 9n) = 5518$.*
- *Como todo número é divisível por um temos que sempre será verdadeiro*

- Escolhendo 692.803 é divisível por 6131, e o critério aditivo aplicado, observe que 692.803 fica $69280 + 3 \cdot 5518 = 85834$ (somando sem o último algarismo) e 85834 fica $8583 + 4 \cdot 5518 = 30655 = 5 \cdot 6131$.

Crêterios para divisibilidade aditivos e subtrativos para nùmeros terminados em 3 (três)

Proposiçãõ 17. A equaçãõ $(10a + b) = (10n + 3) \cdot k$ é verdadeira se, e somente se $(a + b(1 + 3n)) = (10n + 3) \cdot q$ também é verdadeira.

$(\Rightarrow)$

$$(10a + b) + 3b(10n + 3) = (10n + 3) \cdot k + 3b(10n + 3)$$

$$10a + b + 9b + 30bn = (10n + 3) \cdot (k + 3b)$$

$$10a + 10b + 30bn = (10n + 3) \cdot k_1; k_1 = k + 3b$$

$$10 \cdot (a + b + 3bn) = (10n + 3) \cdot k_1$$

$$10 \cdot (a + b(1 + 3n)) = (10n + 3) \cdot k_1$$

$$(10, 10n + 3) = 1$$

$$(a + b(1 + 3n)) = (10n + 3) \cdot k_2$$

$$k_2 = q$$

O que prova a 1a implicação.

$(\Leftarrow)$

Agora se $(a + b(1 + 3n)) = (10n + 3) \cdot q$ então $(10a + b) = (10n + 3) \cdot k$.

Seja $(a + b(1 + 3n)) = (10n + 3) \cdot q$ multiplicando a equação por 10 encontramos:

$$10 \cdot (a + b(1 + 3n)) = 10 \cdot ((10n + 3) \cdot q)$$

$$10a + 10b(1 + 3n) = (10n + 3) \cdot q_1; q_1 = 10 \cdot q$$

$$10a + 10b + 30bn = (10n + 3) \cdot q_1$$

$$10a + b + 9b + 30bn = (10n + 3) \cdot q_1$$

$$(10a + b) + 3b(3 + 10n) = (10n + 3) \cdot q_1$$

$$(10a + b) = (10n + 3) \cdot q_1 - [3b(3 + 10n)]$$

$$(10a + b) = (10n + 3) \cdot (q_1 - 3b)(10a + b) = (10n + 3) \cdot q_2$$

$$q_2 = k$$

O que prova a 2a implicação. ■

Exemplo 25. Tomemos dois valores para n

(a) Para $n = 0$:

- temos o número $(10n + 3) = 3$ e
- seu critério aditivo de divisibilidade é $(1 + 3n) = 1$.

- Se desejarmos saber se 111.555.777 é divisível por 3, fazemos:

111.555.777 = $3 \cdot 37 \cdot 185 \cdot 259$ fica 11.155.577 + $1 \cdot 7 = 11.155.584 = 3 \cdot 3718 \cdot 528$, e 11.155.584 fica 1.155.558 + $1 \cdot 4 = 1.115.562 = 3 \cdot 371 \cdot 854$, e 1.115.562 fica 111.556 + $2 \cdot 1 = 111.558 = 3 \cdot 37 \cdot 186$, e 111.558 fica 11.155 + $1 \cdot 8 = 11 \cdot 163 = 3 \cdot 3 \cdot 721$, e 11.163 fica 1116 + $1 \cdot 3 = 1 \cdot 119 = 3 \cdot 373$, e 1119 fica 111 + $1 \cdot 9 = 120 = 3 \cdot 40$, e 120 fica 12 + $1 \cdot 0 = 12 = 3 \cdot 4$ e 12 fica 1 + 2 = 3.

- Colocamos um número sabidamente múltiplo de três, para evidenciar que durante o processo se o número é divisível por três, todos números encontrados durante o processo também serão.

(b) Para $n = 113$:

- temos o número $(10n + 3) = 1133$ e
- seu critério aditivo de divisibilidade é $(1 + 3n) = 340$.
- Se desejarmos saber se 132.561 é divisível por 1.133. E o critério aditivo aplicado, observe que 132.561 fica 13256 + $1 \cdot 340 = 13.596$ (somando sem o último algarismo) e 13596 fica 1359 + $6 \cdot 340 = 3399 = 113 \cdot 3$.

Crítérios para divisibilidade aditivos e subtrativos para números terminados em 7 (sete)

Proposição 18. A equação $(10a + b) = (10n + 7) \cdot k$ é verdadeira se, e somente se $(a + b(5 + 7n)) = (10n + 7) \cdot q$ também é verdadeira.

($\Rightarrow$)

$$(10a + b) + 7b(10n + 7) = (10n + 7) \cdot k + 7b(10n + 7)$$

$$10a + b + 49b + 70bn = (10n + 7) \cdot (k + 7b)$$

$$10a + 50b + 70bn = (10n + 7) \cdot k_1; k_1 = k + 7b$$

$$10 \cdot (a + 5b + 7bn) = (10n + 7) \cdot k_1$$

$$10 \cdot (a + b(5 + 7n)) = (10n + 7) \cdot k_1$$

$$(10, 10n + 7) = 1$$

$$(a + b(5 + 7n)) = (10n + 7) \cdot k_2$$

$$k_2 = q$$

O que prova a 1a implicação.

($\Leftarrow$)

Agora se $(a + b(5 + 7n)) = (10n + 7) \cdot q$ então $(10a + b) = (10n + 7) \cdot k$.

Seja $(a + b(5 + 7n)) = (10n + 7) \cdot q$ multiplicando a equação por 10 encontramos:

$$\begin{aligned}
10 \cdot (a + b(5 + 7n)) &= 10 \cdot ((10n + 7) \cdot q) \\
10a + 10b(5 + 7n) &= (10n + 7) \cdot q_1; q_1 = 10 \cdot q \\
10a + 50b + 70bn &= (10n + 7) \cdot q_1 \\
10a + b + 49b + 70bn &= (10n + 7) \cdot q_1 \\
(10a + b) + 7b(7 + 10n) &= (10n + 7) \cdot q_1 \\
(10a + b) &= (10n + 7) \cdot q_1 - (7b \cdot (7 + 10n)) \\
(10a + b) &= (10n + 7) \cdot (q_1 - 7b) \quad (10a + b) = (10n + 7) \cdot q_2 \\
q_2 &= k
\end{aligned}$$

O que prova a 2a implicação. ■

Exemplo 26. *Tomemos dois valores para n*

(a) *Para $n = 0$:*

- *temos o número $(10n + 7) = 7$ e*
- *seu critério aditivo de divisibilidade é $(5 + 7n) = 5$.*
- *Se desejarmos saber se 819 é divisível por 7, fazemos:*
 $819 = 7.117$ e aplicando o critério aditivo fica $81 + 5 \cdot 9 = 126 = 7 \cdot 18$, e 126 fica $12 + 6 \cdot 5 = 42 = 6 \cdot 7$, e 42 fica $4 + 2 \cdot 5 = 14 = 2 \cdot 7$, e 14 fica $1 + 4 \cdot 5 = 21 = 3 \cdot 7$, e 21 fica $2 + 1 \cdot 5 = 7$,
- *Colocamos um número sabidamente múltiplo de sete, para evidenciar que durante o processo se o número é divisível por sete, todos números encontrados durante o processo também serão.*

(b) *Para $n = 917$:*

- *temos $(10n + 7) = 9177$ e $(5 + 7n) = 6424$, sendo 9177*
- *e o número e 6424 seu critério aditivo de divisibilidade.*
- *Se desejarmos saber se 1.037.001 é divisível por 9.177, fazemos:*
 $1,037001$ fica $103.700 + 1 \cdot 6424 + 1 = 110.124$ e 110.124 fica $11.012 + 4 \cdot 6424 = 36708$ e 36.708 fica $3670 + 8 \cdot 6424 = 55.062$ e 55.062 fica $5506 + 2 \cdot 6424 = 18.354 = 9177 \cdot 2$

Crítérios para divisibilidade aditivos e subtrativos para números terminados em 9 (nove)

Proposição 19. *A equação $(10a + b) = (10n + 9) \cdot k$ é verdadeira se, e somente se $(a + b(1 + n)) = (10n + 9) \cdot q$ também é verdadeira.*

$(\Rightarrow)$

$$(10a + b) + b(10n + 9) = (10n + 9) \cdot k + b(10n + 9)$$

$$10a + b + 10bn + 9b = (10n + 9) \cdot (k + b)$$

$$10a + 10b + 10bn = (10n + 9) \cdot k_1; k_1 = k + b$$

$$10 \cdot (a + b + bn) = (10n + 9) \cdot k_1$$

$$10 \cdot (a + b(1 + n)) = (10n + 9) \cdot k_1$$

$$(10, 10n + 9) = 1$$

$$(a + b(1 + n)) = (10n + 9) \cdot k_2$$

$$k_2 = q$$

O que prova a 1a implicação.

$(\Leftarrow)$

Agora se $(a + b(1 + n)) = (10n + 9) \cdot q$ então $(10a + b) = (10n + 9) \cdot k$.

Seja $(a + b(1 + n)) = (10n + 9) \cdot q$ multiplicando a equação por 10 encontramos:

$$10 \cdot (a + b(1 + n)) = 10 \cdot ((10n + 9) \cdot q)$$

$$10a + 10b(1 + n) = (10n + 9) \cdot q_1; q_1 = 10 \cdot q$$

$$10a + 10b + 10bn = (10n + 9) \cdot q_1$$

$$10a + b + 9b + 10bn = (10n + 9) \cdot q_1$$

$$(10a + b) + b(9 + 10n) = (10n + 9) \cdot q_1$$

$$(10a + b) = (10n + 9) \cdot q_1 - (b \cdot (9 + 10n))$$

$$(10a + b) = (10n + 9) \cdot (q_1 - b)(10a + b) = (10n + 9) \cdot q_2$$

$$q_2 = k$$

O que prova a 2a implicação. ■

Exemplo 27. Tomemos dois valores para n

(a) Para $n = 0$:

- temos o número $(10n + 9) = 9$ e $(1 + 9n) = 1$, sendo 9 o número e 1 seu critério aditivo de divisibilidade.
- Se desejarmos saber se 333.666 é divisível por nove, fazemos:
 $333.666 = 9 \cdot 37074$ fica $33.366 + 1 \cdot 6 = 33.372 = 9 \cdot 3708$, e 33.372 fica $3.337 + 1 \cdot 2 = 3.339 = 9 \cdot 371$, e 3.339 fica $333 + 1 \cdot 9 = 342 = 9 \cdot 38$, e 342 fica $34 + 1 \cdot 2 = 36 = 9 \cdot 4$, e 36 fica $3 + 1 \cdot 6 = 9$,
- Colocamos um número sabidamente múltiplo de nove, para evidenciar que durante o processo se o número é divisível por nove, todos números encontrados durante o processo também serão.

(b) Para $n = 500$,

- Temos $(10n + 9) = 5009$ e $(1 + 9n) = 4501$, sendo 5009 o número
- E 4501 seu critério aditivo de divisibilidade.
- Se desejarmos saber se 508500 é divisível por 5.009, fazemos:

5.085.000 *fica* $508.500 + 0 \cdot 4501 = 508.500$ e 508.500 *fica* $50850 + 0 \cdot 4501 = 50850$ e 50850 *fica* $5085 + 0 \cdot 4501 = 5085$ e $5085 = 9 \cdot 565$.

REFERÊNCIAS

- ALVARENGA, Geisa Feltrin Santana de. **CRITÉRIOS DE DIVISIBILIDADE: uma abordagem de acordo com a BNCC**. 2022. Diss. (Mestrado) – UNIVERSIDADE FEDERAL DE SÃO PAULO, Profmat. Citado 1 vez na página 14.
- BOYER, C. Edição: Edgard Blucher. [S.l.]: São Paulo, 1974. Citado 3 vezes nas páginas 13, 18.
- BRASIL. Edição: MEC. [S.l.]: Brasília, 2018. Citado 4 vezes nas páginas 23, 27, 38.
- CASTRUCI, B.; GIOVANNI J.R. AND GIOVANNI JUNIOR, J.R. Edição: FTD. [S.l.]: São Paulo, 2019. Citado 1 vez na página 23.
- EUCLIDES. **Os Elementos**. 1. ed. São Paulo: Editora Unesp., 2009. Citado 1 vez na página 42.
- EVES, H. **Introdução à história da matemática**. 1. ed. São Paulo: Editora UNICAMP, 2004. Citado 2 vezes nas páginas 19, 48.
- FREIRE, Benedito Tadeu V. Números Primos. Os algoritmos de Euclides e aplicações. **Revista do Professor de Matemática**, n.58, SBM, SP, 2016. Citado 1 vez na página 30.
- GAY M.G., SILVA W.R. **Araribá mais: matemática**. 1. ed. São Paulo: Editora Moderna, 2007. Citado 2 vez na página 15.
- GOMES, D.B. **CRITÉRIOS DE DIVISIBILIDADE: provas aritméticas das regras tratadas no ensino de matemática da educação básica**. 2024. Diss. (Mestrado) – UNIVERSIDADE FEDERAL DO MARANHÃO, Profmat. Citado 1 vez na página 48.
- HEFEZ, A. **Aritmética**. 1. ed. Rio de Janeiro: Editora SBM, 2016. Citado 6 vezes nas páginas 16, 17, 23, 28, 40.
- _____. **Elementos de Aritmética**. 2. ed. Rio de Janeiro: Editora SBM, 2006. Citado 4 vezes nas páginas 40, 42, 45.
- JUNIOR, J. R.G. **A conquista da matemática**. 1. ed. São Paulo: Editora FTD, 2022. Citado 1 vez na página 48.
- MARIN, PÉREZ Y. **Aritmética Teoria e prática**. 1. ed. Rio de Janeiro: Ed. Lyceu Coração de Jesus, 1928. Citado 4 vezes nas páginas 21, 28, 29, 44.
- MORGADO, A.C.; CARVALHO, P.C.P. **Matemática Discreta**. 2. ed. Rio de Janeiro: Editora SBM, 2015. Citado 2 vezes nas páginas 14, 16.
- OBMEP. **Programa de Iniciação Científica da OBMEP**. Disponível em: <<https://www.youtube.com/watch?v=SnesXs9xlmg&t=30s%20%5C>>. Citado 1 vez na página 25.

SARDELA A. E MATTA, E. **Matemática**, 5^a **sérier**. 1. ed. Rio de Janeiro: Editora Ática, 1981. Citado 1 vez na página 42.

TORRES, Guilherme Zamalloa. Divisibilidade por 3,7,9,11,13,17,... **Revista do Professor de Matemática**, n.58, SBM, SP, 2005. Citado 1 vez na página 47.