Andressa de Lima Pereira

Números Primos e a Conjectura de Goldbach

Santo André, 2017

UNIVERSIDADE FEDERAL DO ABC

CENTRO DE MATEMÁTICA, COMPUTAÇÃO E COGNIÇÃO

ANDRESSA DE LIMA PEREIRA

NÚMEROS PRIMOS E A CONJECTURA DE GOLDBACH

Orientador: Prof. Dr. Mauricio Firmino Silva Lima

Dissertação de mestrado apresentada ao Centro de Matemática, Computação e Cognição para obtenção do título de Mestre

ESTE EXEMPLAR CORRESPONDE A VERSÃO FINAL DA DISSERTAÇÃO DEFENDIDA PELA ALUNA ANDRESSA DE LIMA PEREIRA, E ORIENTADA PELO PROF. DR. MAURICIO FIRMINO SILVA LIMA.

SANTO ANDRÉ, 2017

Sistema de Bibliotecas da Universidade Federal do ABC
Elaborada pelo Sistema de Geração de Ficha Catalográfica da UFABC
com os dados fornecidos pelo(a) autor(a).

Pereira, Andressa de Lima
Números primos e a conjectura de Goldbach / Andressa de Lima Pereira. — 2017.

74 fls. : il.

Orientador: Mauricio Firmino Silva Lima

Dissertação (Mestrado) — Universidade Federal do ABC, Mestrado Profissional em Matemática em Rede Nacional - PROFMAT, Santo André, 2017.

1. números primos. 2. Conjectura de Goldbach. I. Lima, Mauricio Firmino Silva. II. Mestrado Profissional em Matemática em Rede Nacional - PROFMAT, 2017. III. Título.

Este exemplar foi revisado e alterado em relação à versão original, de acordo com as observações levantadas pela banca no dia da defesa, sob responsabilidade única do autor e com a anuência de seu orientador.

Santo André, 07 **de** Julho **de 20**17.

Assinatura do autor: ______________________________

Assinatura do orientador: ______________________________

MINISTÉRIO DA EDUCAÇÃO
Fundação Universidade Federal do ABC
Programa de Pós-Graduação em Mestrado Profissional em Matemática em Rede Nacional
Avenida dos Estados, 5001 – Bairro Santa Terezinha – Santo André – SP
CEP 09210-580 · Fone: (11) 4996-0017
profmat@ufabc.edu.br

FOLHA DE ASSINATURAS

Assinaturas dos membros da Banca Examinadora que avaliou e aprovou a Defesa de Dissertação de Mestrado da candidata Andressa de Lima Pereira, realizada em 9 de junho de 2017:

Prof.(a) Dr.(a) **Maurício Firmino Silva Lima** (Universidade Federal do ABC) – Presidente

Prof.(a) Dr.(a) **Jeferson Cassiano** (Universidade Federal do ABC) – Membro Titular

Prof.(a) Dr.(a) **Paola Andrea Gaviria Kassama** (Universidade Federal de São Paulo) – Membro Titular

Prof.(a) Dr.(a) **Eduardo Guéron** (Universidade Federal do ABC) – Membro Suplente

Prof.(a) Dr.(a) **Claudio Aguinaldo Buzzi** (Universidade Estadual Paulista Júlio de Mesquita Filho) – Membro Suplente

Dedico este trabalho aos meus avós, que me incentivaram, mesmo sem entender o conteúdo desse trabalho, com o olhar de orgulho a cada conquista acadêmica e profissional.

AGRADECIMENTOS

Primeiramente à Deus, pelo dom da vida.

Ao professor orientador Mauricio Lima, pelas inúmeras colaborações para a realização deste trabalho e para a ampliação dos meus conhecimentos.

Aos demais professores do curso do ProfMat da UFABC, pelas aulas e socialização dos conhecimentos.

À SBM, por acreditar no projeto ProfMat, contribuindo para melhora da educação matemática

Ao CAPES, pelo apoio financeiro.

A todos os professores que passaram pela minha vida acadêmica, da pré-escola até a graduação, pela minha formação.

Aos meus pais, Edenir e Vânia, pela paciência, incentivo para concluir esse trabalho e por me ajudarem a manter o desejo de aprender sempre mais.

À minha irmã, Vanessa e ao meu cunhado, Paulo, por todo o apoio, em tudo.

À minha família e amigos, por confiarem no meu potencial acadêmico.

À amiga e revisora, Valceli, pelo apoio e conselhos, além da leitura, correções e sugestões neste texto.

Aos colegas do curso do ProfMat, pela troca de conhecimentos e por tornarem os momentos de estudo mais agradavéis. Em especial, àqueles que o curso deixará como amigos para a vida.

À equipe da Escola Estadual Professor José Jorge, por permitirem a realização das atividades contidas nesse trabalho e pela confiança em minha capacidade profissional.

Aos colegas de trabalho ao longo de anos do magistério, por me ensinarem, apoiarem e facilitarem a realização desse trabalho.

Às escolas EE Prof José Jorge, Fundação Bradesco - Jd Conceição e EE Prof Fanny M. dos Santos, pela otimização dos horários das aulas durante a realização do curso ProfMat.

À psicóloga Kelly e à psiquiatra Lívia, por me auxiliarem a manter minha saúde mental.

E aos meus alunos, ex-alunos e futuros alunos, pois é por eles e para eles que tento aprender cada dia mais.

"Eu gosto de números primos... Acho que os números primos são como a vida. São muito lógicos, mas a gente nunca consegue entender as regras, mesmo que se passe a vida toda pensando nelas."

(Mark Haddon, *O estranho caso do cachorro morto.*)

RESUMO

Este trabalho apresenta os números primos, para isso é abordado seu papel na história da matemática, verificando sua atual relevância para a criptografia, analisadas as principais propriedades e resultados e sugere uma sequência didática para abordar o tema com alunos da educação básica. Também, são discutidos os avanços obtidos no estudo da conjectura de Goldbach, a partir da análise de trabalhos e artigos de alguns matemáticos que se dedicaram a decifrar a famosa conjectura.

Palavras-chave: Números Primos, Conjectura de Goldbach

ABSTRACT

This paper presents the prime numbers, it approaches their role in mathematics' history, verifies their current relevance for cryptography, analyzes the main properties and results and suggests a didactic sequence to study the theme with basic education's students. It is also discussed the advances obtained in the study of the Goldbach conjecture, based on analysis of works and articles of some mathematicians who dedicated themselves to deciphering the famous conjecture.

Keywords: Prime Number, Goldbach Conjecture

CONTEÚDO

INTRODUÇÃO

$2, 3, 5, 7, 11, 13, 17, 19, 23, \cdots$

Os primos estendem-se ao infinito, nunca se esgotam. São blocos que formam todos os números, são essenciais à matemática.

Podemos considerar os números primos como um presente da natureza, sua capacidade de gerar todo número não primo é fascinante e misteriosa.

Euclides provou que os números primos são infinitos, Gauss disse que eram escolhidos ao acaso. A história desses números estende-se ao mundo matemático, mesmo com reviravoltas ou com o uso de tecnologias, o mistério dos números primos continua. [7, 16, 17]

Números primos são protagonistas de diversas teorias, aparentemente simples, como a questão formulada por Goldbach: *Todo número inteiro maior que 2 pode ser representado como a soma de dois números primos*. Ainda hoje, quase três séculos depois de enunciada, a conjectura de Goldbach segue sem demonstração, apesar de já ter sido testada empiricamente até 10^{18}. Tornou-se um dos problemas mais intrigantes da Matemática.

Todo esse acervo de informações sobre números primos podem e devem ser utilizados na educação matemática, sendo mais uma ferramenta para a formação ampla e plural do aluno.

Com a visão de que os números primos são necessários para o desenvolvimento da matemática e de que a Conjectura de Goldbach exerce um fascínio impulsionando e motivando os estudos sobre a teoria dos números, este trabalho tem o intuito de contribuir com aqueles que pretendem conhecer a Conjectura de Goldbach e compreender a importância dos números primos.

No primeiro capítulo, faremos uma contextualização histórica, observando a presença e significância dos números primos em diversos períodos da história da matemática. Nos dias atuais, exemplificaremos a importância dos números primos com a criptografia. Também conheceremos alguns personagens importantes para a evolução dos conhecimentos sobre números primos, tais como Euclides e Gauss.

No segundo capítulo, definiremos Número Primo, apresentaremos e discutiremos algumas propriedades acerca desses números.

Já no terceiro capítulo, conheceremos a conjectura de Goldbach, analisando estudos que mostram resultados parciais a respeito da, ainda não demonstrada, conjectura.

Por sua vez, no quarto capítulo, faremos uma abordagem pedagógica, sugerindo atividades que desenvolvam o raciocínio lógico-dedutível dos educandos, utilizando números primos e a conjectura de Goldbach.

1

HISTÓRIA DO NÚMERO PRIMO

Os números primos ostentam uma longa história, desde a antiguidade até o presente. [2, 8]

Em várias bibliotecas da Grécia Antiga, havia tabelas de números primos nas paredes, alguns gregos acreditavam que entrariam para a história se fossem capazes de escrever todos os números primos, incentivados pelo lema de Pitagóras[1] *Números são tudo!*, até o século III a.C. quando é provada a infinitude dos números primos.

O célebre matemático grego Euclides[2] definia os números primos como blocos para construção de todos os números. Em seu livro "*Elementos*", o autor aborda significativos resultados a respeito dos números primos; no livro IX, ele apresenta a proposição IX 14, a qual é equivalente ao *Teorema Fundamental da Aritmética*. No mesmo livro, Euclides prova, de maneira considerada modelo de elegância matemática, a proposição IX 20, a qual aponta os números primos como infinitos, nessa demonstração é empregado o método *reduction ad absurdum*.

Um pouco depois, outro grego, Erastóstenes[3] criou o primeiro algoritmo que fornece os números primos, tal algoritmo ficou conhecido como *Crivo de Erastóstenes*.

Anos se passaram sem grandes avanços sobre a teoria dos números primos.

No final do século XVI, o frade francês Marin Mersenne[4] discutiu alguns pontos sobre os números primos em seu trabalho *Cogitata physico-mathematica*, ficando conhecido devido aos chamados primos de Mersenne.

1 Pitágoras de Samos (570 aC - 495 aC) filósofo e matemático grego, tem como principais trabalhos o Teorema de Pitágoras e Proporção áurea.
2 Euclides de Alexandria (360 aC - 295 aC) matemático conhecido como Pai da Geometria.
3 Erastóstenes de Cirene (276 aC - 194 aC) matemático, geógrafo e astrônomo, conhecido por calcular a circunferência da Terra e pelo crivo que determina os números primos.
4 Marin Mersenne (1588 - 1648) téologo, filósofo e matemático francês.

No século XVII, o ilustre matemático Pierre de Fermat[5] fez diversas contribuições à teoria dos números, várias contendo conjecturas sobre primos, como o *Pequeno Teorema de Fermat*, enunciado em uma carta de 18 de outubro de 1640 a Frénicle de Bessy[6]. O *Pequeno Teorema de Fermat* só foi demonstrado quase um século depois de enunciado. Com seu perfil investigativo, Fermat conjecturou uma fórmula para encontar números primos, porém anos depois Euler revelou que a conjectura era falsa.

Euler[7] mostrou-se um dos mais brilhantes e reconhecidos matemáticos do século XVIII, trocando correspondência com vários matemáticos, em particular com Christian Goldbach que, em 1742, enunciou o que ficaria conhecido como *Conjectura de Goldbach*. Euler respondeu-lhe que estava absolutamente certo sobre isso, porém não demonstrou a conjectura. Até os dias atuais essa conjectura está em aberto.

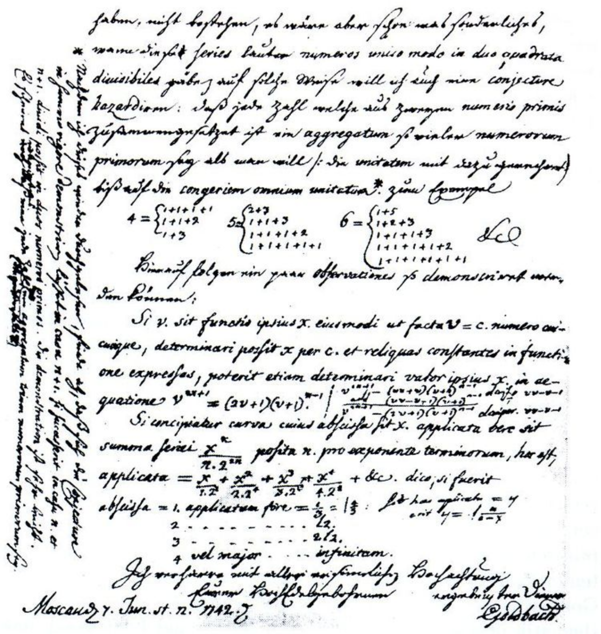


Figura 1: Carta escrita por Goldbach a Euler em 1742

5 Pierre de Fermat (1601 - 1665) matemático e cientista francês com enormes contribuições para o cálculo infinetesimal e para Teoria dos Números.

6 Bernard Frénicle de Bessy (1604 - 1674) matemático francês responsável por inúmeros artigos sobre Teoria dos Números.

7 Leonhard Paul Euler (1707 - 1783), matemático e físico suíço, fez importantes descobertas matemáticas, considerado o maior matemático do século XVIII.

Em 1792, o então menino, Carl Friedrich Gauss[8] ganha um livro que continha uma tabela de números primos, fascinado com esse mundo desconhecido, Gauss tenta criar relações entre os números primos. Como não encontra qualquer relação, ele passa a se dedicar a descobrir quantos números primos há em um intervalo numérico, criando uma nova perspectiva em relação ao estudo dos números primos.

Analisando os estudos de Gauss, Bernhard Riemann[9] cria a *função zeta*, declarando em 1859 que todos os zeros da *função zeta* pertencem à mesma *linha crítica*, ficando conhecida essa declaração como *Hipótese de Riemann*, um dos pilares do Cálculo Diferencial e Integral, ainda não demonstrado.

Allan Turing[10], no início do século XX, usou seus conhecimentos sobre números primos para decifrar mensagens criptografadas alemãs durante a grande guerra. Após o fim da guerra, Turing fez algumas tentativas fracassadas de mostrar que a *Hipótese de Riemann* era falsa.

Nos meados do século XX, com o advento da computação [5] são descobertos, cada vez mais, números primos. Em 1952, um computador foi capaz de revelar um novo número primo, até então desconhecido.

Com o crescimento da necessidade de segurança na comunicação eletrônica a comunidade acadêmica do século XXI mostra-se interessada nos números primos.

Em janeiro de 2016, o pesquisador Curtis Cooper calculou o maior número primo conhecido atualmente. Batizado de M74207281[11] por ser um primo de Mersenne ($2^{74207281} - 1$) que tem 22.338.618 dígitos.

1.1 CRIPTOGRAFIA

A criptografia tem a função de proteger informações que circulam entre rede de computadores, como dados bancários.

8 Carl Friedrich Gauss (1777 - 1855) foi um matemático, astrônomo e físico alemão que contribuiu muito em diversas áreas da ciência, dentre elas a teoria dos números, estatística, análise matemática e geometria.

9 Georg Friedrich Bernhard Riemann (1826 - 1866) foi um matemático alemão, com contribuições fundamentais para a análise e a geometria diferencial.

10 Alan Mathison Turing (1912 - 1954) foi um matemático, lógico, criptoanalista e cientista da computação britânico.

11 Primos de Mersenne recebem a notação Mp, onde p é um número primo tal que $Mp = 2^p - 1$.

A criptografia funciona em codificar e decodificar mensagens. O remetente escreve a mensagem, o sistema codifica, transmite o código pela rede, o destinatário apenas terá acesso à mensagem caso tenha a "chave" para decodificá-la.

Os números primos são fundamentais no método RSA de criptografia, utilizado hoje pelas instituições financeiras e grandes empresas.

O método RSA baseia-se na utilização de um código x, em que $x = p \cdot q$, p e q são números primos. Para codificar a mensagem é necessário conhecer x e para decodificá-la precisa saber os fatores p e q. Por isso a necessidade de serem primos, pois utiliza-se da unicidade da fatoração.

Esse método é interessante e útil, pois, sabendo os primos p e q facilmente determinamos a "chave" x. Porém se p e q são números muito grandes, mesmo conhecendo a "chave" x não temos um método simples, rápido e eficaz para determinar seus valores, o que dificulta a tentativa de decodificar sem ser pelo destinatário.

Ou seja, o método RSA é eficaz pela dificuldade em fatorar x. Quanto maior os números primos p e q utilizados, mais complexa fica sua fatoração, portanto mais difícil de ser descoberto por pessoas alheias à mensagem criptografadas. Com isso, o interesse em encontrar números primos cada vez maiores vem aumentando.

Para codificar uma sentença no padrão RSA, usamos os números primos p e q. Determinamos n, $\phi(n)$ e e. Onde:

$$n = p \cdot q$$
$$\phi(n) = \phi(p, q) = (p-1) \cdot (q-1)$$
$$mdc(e, \phi(n)) = 1$$

Sendo a, $(a < n)$ o valor a ser codificado descobrimos $C(a)$ por meio da fórmula:

$$a^e \equiv C(a)\ (mod\ n)$$

Para decodificar a sentença, determinamos o valor de d tal que

$$d \cdot e \equiv 1\ (mod\ \phi(n))$$

Retornando ao valor a pela fórmula:

$$a \equiv C(a)^d\ (mod\ n)$$

Para facilitar a interpretação dos cálculos utilizados, o exemplo a seguir é feito com números "pequenos" e uma tabela hipotética.

Exemplo 1.1. Usando os valores de $p = 11$ e $q = 17$, determine as fórmulas de codificação e decodificação para a tabela:

A	B	C	D	E	F	G	H	I	J	K	L	M
11	12	13	14	15	16	17	18	19	20	21	22	23
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
24	25	26	27	28	29	30	31	32	33	34	35	36
espaço	0	1	2	3	4	5	6	7	8	9	.	?
99	80	81	82	83	84	85	86	87	88	89	90	91

Codificação: $n = p \cdot q \Rightarrow n = 11 \cdot 17 \Rightarrow n = 187$

$\phi(n) = \phi(p, q) = (p-1) \cdot (q-1) \Rightarrow$
$\phi(187) = \phi(11, 17) = (11-1) \cdot (17-1) = 10 \cdot 16 = 160 \Rightarrow \phi(187) = 160$

$mdc(e, \phi(n)) = 1 \Rightarrow$
$mdc(e, \phi(187)) = 1 \Rightarrow mdc(e, 160) = 1 \Rightarrow e = 3$

$$a^e \equiv C(a)\ (mod\ n)$$

$$a^3 \equiv C(a)\ (mod\ 187)$$

Decodificação: $d \cdot e \equiv 1\ (mod\ \phi(n)) \Rightarrow d \cdot 3 \equiv 1\ (mod\ 160) \Rightarrow d = 107$

$$a \equiv C(a)^d\ (mod\ n)$$

$$a \equiv C(a)^{107}\ (mod\ 187)$$

Problema 1. Usando o exemplo 1.1, codifique a sentença: **NUMEROS PRIMOS**.

N	U	M	E	R	O	S	espaço	P	R	I	M	O	S
24	31	23	15	28	25	29	99	26	28	19	23	25	29

Reagrupando os valores, tal que $a < 187$. Para evitar conflitos, o valor de a não deve iniciar com o algarismo 0.

24	31	23	152	82	52	99	92	62	81	92	32	52	9

Utilizando a fórmula $a^3 \equiv C(a)\ (mod\ 187)$ temos:

a	$a^3 \equiv C(a)\ (mod\ 187)$	C(a)
24	$24^3 \equiv C(a)\ (mod\ 187)$	173
31	$31^3 \equiv C(a)\ (mod\ 187)$	58
23	$23^3 \equiv C(a)\ (mod\ 187)$	12
152	$152^3 \equiv C(a)\ (mod\ 187)$	135
82	$82^3 \equiv C(a)\ (mod\ 187)$	92
52	$52^3 \equiv C(a)\ (mod\ 187)$	171
99	$99^3 \equiv C(a)\ (mod\ 187)$	143
92	$92^3 \equiv C(a)\ (mod\ 187)$	20
62	$62^3 \equiv C(a)\ (mod\ 187)$	90
81	$81^3 \equiv C(a)\ (mod\ 187)$	174
92	$92^3 \equiv C(a)\ (mod\ 187)$	20
32	$32^3 \equiv C(a)\ (mod\ 187)$	43
52	$52^3 \equiv C(a)\ (mod\ 187)$	171
9	$9^3 \equiv C(a)\ (mod\ 187)$	168

Assim o código transmitido será:

$$173 - 58 - 12 - 135 - 92 - 171 - 143 - 20 - 90 - 174 - 20 - 43 - 171 - 168$$

.

Problema 2. Usando o exemplo 1.1, decodifique a mensagem: $12 - 22 - 72 - 135 - 58 - 124 - 127 - 164 - 1$

Usando a fórmula: $a \equiv C(a)^{107}\ (mod\ 187)$, temos:

C(a)	$a \equiv C(a)^{107}\ (mod\ 187)$	a
12	$a \equiv 12^{107}\ (mod\ 187)$	23
22	$a \equiv 22^{107}\ (mod\ 187)$	11
72	$a \equiv 72^{107}\ (mod\ 187)$	30
135	$a \equiv 135^{107}\ (mod\ 187)$	152
58	$a \equiv 58^{107}\ (mod\ 187)$	31
124	$a \equiv 124^{107}\ (mod\ 187)$	130
127	$a \equiv 127^{107}\ (mod\ 187)$	19
164	$a \equiv 164^{107}\ (mod\ 187)$	131
1	$a \equiv 1^{107}\ (mod\ 187)$	1

Reagrupando os valores de a em dezenas.

23	11	30	15	23	11	30	19	13	11

Comparando com a tabela de codificação:

23	11	30	15	23	11	30	19	13	11
M	A	T	E	M	A	T	I	C	A

A mensagem codificada é: **MATEMATICA**

1.2 PRIMOS GRANDES

Durante muito tempo o maior número primo conhecido foi 524.287.

Com os estudos da teoria dos números, esse recorde foi sendo superado. Até que em 1772, Euler provou que 2.147.483.647 era primo. Esse número com 10 dígitos, foi detentor do recorde até 1867.

Em 1876 é encontrado o número primo M127, com 39 dígitos, iniciando o período de descobertas dos grandes números primos.

Os números primos com 60 dígitos, hoje utilizados na criptografia, foram, em sua maioria, descobertos no início do século XX.

Com os avanços tecnológicos, utilizando computadores, o ano de 1952 ficou marcado por diversas descobertas: M521, M607, M1279, M22203 e M2281, respectivamente, com 157, 183, 386, 664 e 687 dígitos.

As tecnologias foram evoluindo até que em 2005 surgiu a GIMPS[12], um software que utiliza o tempo ocioso do computador para efetuar cálculos e procurar primos de Mersenne.

Então, em 04 de setembro de 2006, com auxilio de GIMPS, um matemático amador descobriu um número primo com 9,8 milhões de dígitos.

Nesse período, começa uma corrida para descobrir o primeiro primo com mais de 10 milhões de dígitos, o interesse não era apenas acadêmico, mas também, financeiro, pois havia um prêmio de 100 mil dólares para a pessoa que descobrisse tal número. Em 06 de setembro de 2008, o matemático amador alemão Hans-Michael Elvenich descobriu um número primo com mais de 11 milhões de dígitos, mas sua empolgação não durou muito pois 15 dias antes, Edson Smith do departamento de Matemática da Universidade da Califórnia descobrira um número primo com 12,9 milhões de dígitos.

12 Na sigla em Inglês, Great Internet Mersenne Prime seartch - Grande Busca de Primos de Mersenne via Internet.

O maior número primo conhecido atualmente é M74207281, com mais de 22 milhões de dígitos, ele foi descoberto em janeiro de 2016, por um grupo de matemáticos da Universidade Central do Missouri.

Como os números primos são infinitos, esse recorde pode ser superado. Existe premiação em dinheiro que incentiva a procura por outros números primos, há um prêmio de 3 mil dólares para cada novo número primo de Mersenne encontrado e, se esse número chegar a 1 bilhão de dígitos, o responsável pela descoberta terá direito a 200 mil dólares.

2

NÚMEROS PRIMOS

Na formação do conjunto dos números naturais, existe um tipo de número que possui a propriedade de ser divisível somente por um e por ele mesmo, recebendo a denominação de número primo. A descoberta dos números primos é imprescindível na matemática, pois eles intitulam o princípio central na teoria dos números, consistindo no Teorema Fundamental da Aritmética.

Definição 2.1. Um número natural n $(n > 1)$ possuindo somente dois divisores n e 1 é chamado de *primo*.

Se $n > 1$ não é primo dizemos que n é *composto*.

Iremos denotar como $\wp$ o conjunto dos números primos.

2.1 PROPRIEDADES CLÁSSICAS

Alguns teoremas têm grande importância para o estudo dos números primos, sendo assim, vamos analisar alguns desses teoremas importantes para a Teoria dos Números [15, 18].

Reconhecer números primos é necessário, bem como, os números não primos, chamados de compostos.

Teorema 2.2. ***(Primalidade e Fatoração)*** *Todo número natural $n > 1$ ou é primo, ou é divisível por um número primo.*

Demonstração. Por indução matemática e definição de números primos.

Se $n = 2$ ele é um número primo e então, o teorema é verdadeiro.

Supondo que a hipótese do teorema seja verdadeira para todo k com $2 \leq k \leq n$.

Vamos considerar o número $n + 1$.

Se $n + 1$ é primo então o teorema é verdadeiro.

Se não, então $n + 1 = a \cdot b$,
em que a e b são números naturais com $2 \leq a \leq b \leq n + 1$.

Aplicando a hipótese de indução aos números a e b, ou a e b são primos, ou divisíveis por um número primo.

Concluindo a demonstração. □

Euclides provou, no século III a. C., que os números primos são infinitos.

Teorema 2.3. ***(Infinidade)*** *$\wp$ é um conjunto infinito.*

Demonstração. Como 2 é número primo, óbvio que $\wp \neq \varnothing$. Supondo, por absurdo, que exista uma quantidade finita de números primos, isto é,

$$\wp = \{p_1, p_2, p_3, \cdots, p_n\}.$$

Seja então $q \in \mathbb{N}$ da forma

$$q = p_1 \cdot p_2 \cdot p_3 \cdot \cdots \cdot p_n + 1.$$

Sabemos que $q > p_i$ para todo $1 \leq i \leq n$.

Existem duas opções para q:

1. q é um número primo.

   Fato que contraria a hipótese. O que não ocorre, visto que $q > p_i, i \in \{1, 2, 3, \cdots, n\}$, em particular $q \notin \wp$.

2. q é composto.

   Nesse caso, pelo teorema 2.2, q é divisível por um número primo. No entanto, o resto da divisão de q por $p_i, i \in \{1, 2, \cdots, n\}$ é 1 e portanto p_i não é divisivel por q.

O que conclui a demonstração. □

O teorema da Primalidade e Fatoração apresenta uma propriedade dos números compostos: todo número composto é divisível por, pelo menos, um número primo.

O Teorema Fundamental da Aritmética sustenta que todos os números inteiros positivos maiores que 1 podem ser decompostos em um produto de números primos, sendo essa decomposição única, a menos de permutações dos fatores.

Teorema 2.4. ***(Teorema Fundamental da Aritmética)*** *Todo número natural maior que 1 pode ser representado de maneira única (a menos da ordem) como um produto de fatores primos.*

Demonstração. A prova da primeira parte será feita por indução completa.

Afirmação: Dado $n \in \mathbb{N}$, n se escreve como o produto de números primos.

Seja $n \in \mathbb{N}$.

Se $n = 2$ (Ok!)

Suponha a afirmação verdadeira para todo natural nenor que n.

Se n for primo então nada temos a fazer.

Se n for composto então existe $p \in \wp$, $p \mid n$. Daí,

$$n = p \cdot n_1, 1 < n_1 < p.$$

Pela hipotese de indução n_1 se escreve como produto de primos e o mesmo, então, vale para n.

Assim, todo número natural pode ser representado como um produto de primos.

Agora, precisamos mostrar a unicidade.

Para isso, vamos supor que exista outra representação, isto é,

$$n = p_1 \cdot p_2 \cdot p_3 \cdots p_k = q_1 \cdot q_2 \cdot q_3 \cdots q_w$$

Para essa igualdade ser verdadeira devemos ter

$$p_1 \mid q_1 \cdot q_2 \cdot q_3 \cdots q_w$$

Porém, como $q_1, q_2, q_3, \cdots, q_w$ são primos,

$p_1 = q_j$ para algum $1 \leq j \leq w$

Cancelando p_1 e q_j, temos $p_2 \cdot p_3 \cdots p_k = q_1 \cdot q_2 \cdot q_3 \cdots q_{j-1} \cdot q_{j+1} \cdots q_w$.

Repetindo o processo, teremos sempre $p_u = q_v$ para $1 \leq u \leq k$ e $1 \leq v \leq w$. Concluimos que os dois lados da igualdade coencidem e o resultado segue. $\square$

Exemplo 2.1. Usando a decomposição em fatores primos, em decorrência do teorema anterior, temos:

- $30 = 2 \cdot 3 \cdot 5$
- $50 = 2 \cdot 5^2$
- $393040 = 2^3 \cdot 3^4 \cdot 5 \cdot 11^2 = 2^3 \cdot 3^4 \cdot 5^1 \cdot 7^0 \cdot 11^2$

2.2 TESTES DE PRIMALIDADE

Uma das perguntas mais abrangentes da teoria dos números primos é determinar se um número é primo ou composto.

Para ser possível essa resposta, vamos analisar alguns resultados obtidos sobre algortímos que sejam capazes de verificar se um número é primo, ou não.

Teorema 2.5. *Se n não é primo, então n possui, necessariamente, um fator primo menor ou igual que $\sqrt{n}$.*

Demonstração. Sendo n composto, então $n = a \cdot b$ onde $1 < a \leq b < n$. Supondo por absurdo que $a > \sqrt{n}$ e $b > \sqrt{n}$. teriamos que $n = a \cdot b > \sqrt{n} \cdot \sqrt{n} = n$ obtendo que $n > n$.

Logo, $a \leq \sqrt{n}$ ou $b \leq \sqrt{n}$.

Assim, n possui, necessariamente um fator menor que $\sqrt{n}$, e pelo Teorema Fundamental da Aritmética (teorema 2.4) esse fator é um primo menor que $\sqrt{n}$. $\square$

2.2.1 *Crivo de Erastóstenes*

O Crivo de Erastóstenes é um algoritmo simples para determinar o números primos até um valor n.

O algoritmo:

1. Inicia com os números de 2 até n.

2. Retiram-se todos os múltiplos de 2, maior que 2.
3. Observa o próximo número m não retirado, que será primo.
4. Retiram-se todos os múltiplos de m, maior que m
5. Repetir os itens (3) e (4) até que $m \geq \sqrt{n}$.
6. Os números restantes serão primos.

Exemplo 2.2. Vamos determinar os números primos até 100.
Iniciamos com os números de 2 até 100.

Tabela 1: Números naturais até 100.

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

Tabela 2: Retirando os múltiplos de 2.

•	2	3	•	5	•	7	•	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	•

Tabela 3: Retirando os múltiplos de 3.

•	2	3	•	5	•	7	•	•	•
11	•	13	•	•	•	17	•	19	•
•	•	23	•	25	•	•	•	29	•
31	•	•	•	35	•	37	•	•	•
41	•	43	•	•	•	47	•	49	•
•	•	53	•	55	•	•	•	59	•
61	•	•	•	65	•	67	•	•	•
71	•	73	•	•	•	77	•	79	•
•	•	83	•	85	•	•	•	89	•
91	•	•	•	95	•	97	•	•	•

Tabela 4: Retirando os múltiplos de 5.

•	2	3	•	5	•	7	•	•	•
11	•	13	•	•	•	17	•	19	•
•	•	23	•	•	•	•	•	29	•
31	•	•	•	•	•	37	•	•	•
41	•	43	•	•	•	47	•	49	•
•	•	53	•	•	•	•	•	59	•
61	•	•	•	•	•	67	•	•	•
71	•	73	•	•	•	77	•	79	•
•	•	83	•	•	•	•	•	89	•
91	•	•	•	•	•	97	•	•	•

Tabela 5: Retirando os múltiplos de 7.

•	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	•	•	•

Restando somente os números primos.

$$\wp = \{2,3,5,7,11,13,17,19,23,29,31,37,41,43,47,53,59,61,67,71,73,79,83,89,97\}$$

2.2.2 *Divisões Sucessivas*

O método de divisões sucessivas consiste em efetuar a divisão do número que se deseja verificar a primalidade n por todos os números primos até o número $\sqrt{n}$, observando o valor do resto das divisões, todos devem ser distintos a zero.

Em outras palavras, para se verificar se o número natural n é primo não pode ocorrer à congruência

$$n \equiv 0 \, (mod \;\, p)$$

para todo p primo menor ou igual $\sqrt{n}$. [1]

Exemplo 2.3. Analisando o número 97.
$97 \equiv 1 \, (mod \; 2)$
$97 \equiv 1 \, (mod \; 3)$
$97 \equiv 2 \, (mod \; 5)$
$97 \equiv 6 \, (mod \; 7)$

97 é primo.

1 Ao mencionar o método das divisões sucessivas no ensino básico da matemática utilizamos a definição que "o resto da divisão por p é zero".

Exemplo 2.4. Analisando o número 1203.
$1203 \equiv 1 \, (mod \; 2)$
$1203 \equiv 0 \, (mod \; 3)$

1203 não é primo.

2.2.3 *Teste de Fermat*

O teste de primalidade de Fermat oferece um teste simples para ignorar números não-primos.

Qualquer número que falhe o teste não é primo.

Teorema 2.6. ***Teste de Fermat*** *Se p é primo, então para qualquer a tal que $mdc(a, p) = 1$, temos:*

$$a^{p-1} \equiv 1 \, (mod \; p)$$

Demonstração. A prova da primeira parte será feita por indução completa.

Afirmação: Dado $n \in \mathbb{N}$, n se escreve como o produto de números primos.

Seja $n \in \mathbb{N}$.

Se $n = 2$ (Ok!)

Suponha a afirmação verdadeira para todo natural nenor que n.

Se n for primo então nada temos a fazer.

Se n for composto então existe $p \in \wp$, $p \mid n$. Daí, $n = p \cdot n_1$, $1 < n_1 < p$.

Pela hipótese de indução n_1 se escreve como produto de primos e o mesmo, então, vale para n.

Assim, todo número natural pode ser representado como um produto de primos.

Agora, precisamos mostrar a unicidade.

Para isso, vamos supor que exista outra representação.

$$n = p_1 \cdot p_2 \cdot p_3 \cdots p_k = q_1 \cdot q_2 \cdot q_3 \cdots q_w$$

Para essa igualdade ser verdadeira devemos ter

$$p_1 \mid q_1 \cdot q_2 \cdot q_3 \cdots q_w$$

Porém, como $q_1, q_2, q_3, \cdots, q_w$ são primos,

$p_1 = q_j$ para algum $1 \leq j \leq w$

Cancelando p_1 e q_j, temos $p_2 \cdot p_3 \cdots p_k = q_1 \cdot q_2 \cdot q_3 \cdots q_{j-1} \cdot q_{j+1} \cdots q_w$.

Repetindo o processo, teremos sempre $p_u = q_v$ para $1 \leq u \leq k$ e $1 \leq v \leq w$. Concluimos que os dois lados da igualdade coencidem e o resultado segue. □

Exemplo 2.5. Analisando o número 9.
$mdc(4, 9) = 1$

$$4^{9-1} = 4^8 = 256$$

$$256 \equiv 4\,(mod\ 9)$$

9 não é primo.

Exemplo 2.6. Analisando o número 10.
$mdc(11, 10) = 1$

$$11^{10-1} = 11^9 = 2357947691$$

$$2357947691 \equiv 1\,(mod\ 10)$$

Com esse resultado, nada pode se afirmar sobre o número 10.
$mdc(3, 10) = 1$

$$3^{10-1} = 3^9 = 19683$$

$$19683 \equiv 3\,(mod\ 10)$$

10 não é primo.

2.2.4 *Teste de Wilson*

Teorema 2.7. ***(Teorema de Wilson)*** *Um número natural é primo se, e somente, se, p divide $(p-1)! + 1$.*

Demonstração. Suponha p primo e seja $i \in \{1, 2, 3, \cdots, p-2, p-1\}$

Como $mdc(i, p) = 1$, segue que a congruência $iX \equiv 1\,(mod\ p)$ tem solução única. (Para solução de equações de congruência ver a referência bibliográfica [11])

Assim, exite um único $j \in \{1, 2, 3, \cdots, p-2, p-1\}$ tal que $ij \equiv 1\,(mod\ p)$.

Agora, se tivessemos $i = j$, obteríamos $i^2 \equiv 1\,(mod\ p)$ o que implica $p \mid i^2 - 1$. Como p é primo tem-se $p \mid (i+1)$ ou $p \mid (i-1)$ ou seja $i = 1$ ou $i = p-1$.

Daí, segue de $ij \equiv 1\,(mod\ p)$ que:

$$2 \cdot 3 \cdot 4 \cdots (p-3) \cdot (p-2) \equiv 1\,(mod\ p)$$

$$\Rightarrow 1 \cdot 2 \cdot 3 \cdot 4 \cdots (p-3) \cdot (p-2) \cdot (p-1) \equiv (p-1)\,(mod\ p)$$

$$\Rightarrow (p-1)! \equiv (p-1)\,(mod\ p)$$

$$\Rightarrow (p-1)! \equiv 1\,(mod\ p)$$

$$\Rightarrow p \mid [(p-1)! + 1]$$

□

Exemplo 2.7. Analisando o número 5.

$$5 \mid (5-1)! + 1 \Rightarrow 5 \mid 4! + 1 \Rightarrow 5 \mid 24 + 1 \Rightarrow 5 \mid 25$$

5 é primo

Exemplo 2.8. Analisando o número 6.

$$6 \dagger (6-1)! + 1 \Rightarrow 6 \dagger 5! + 1 \Rightarrow 6 \dagger 120 + 1 \Rightarrow 6 \dagger 121$$

6 não é primo

2.2.5 *Teste AKS*

A teoria AKS foi desenvolvida pelos matemáticos indianos Manindra Agrawal, Neeraj Kayal e Nitin Saxena e trata-se de um importante resultado sobre a primalidade de números naturais.

O teorema AKS oferece uma condição necessária e suficiente para detectar números primos. Por isso, pode ser aplicado a qualquer número, sem cotas superiores ao número a ser testado. Com auxílio de equipamentos para cálculos o teste AKS pode ser executado em um limite de tempo possível.

Teorema 2.8. ***(AKS)*** *Seja $m \in \mathbb{N}$, $a \in \mathbb{Z}$ e $mdc(a,m) = 1$. Então, m é primo se, e somente se,*

$$(x+a)^m \equiv x^m + a\,(mod\ m)$$

Exemplo 2.9. Analisando o número 3.
$m = 3$, $a = 2$, $mdc(3,2) = 1$

$$(x+2)^3 \equiv x^3 + 2\,(mod\ 3)$$

$$\begin{aligned}
(x+2)^3 &\equiv x^3 + 2\,(mod\ 3)\\
x^3 + 6x^2 + 12x + 8 &\equiv x^3 + 2\,(mod\ 3)\\
6x^2 + 12x + 8 &\equiv 2\,(mod\ 3)\\
6x^2 + 12x + 6 + 2 &\equiv 2\,(mod\ 3)\\
2 + \underbrace{3(2x^2 + 6x + 3)}_{\text{divisível por 3}} &\equiv 2\,(mod\ 3))\\
2 &\equiv 2\,(mod\ 3)
\end{aligned}$$

3 é número primo.

Exemplo 2.10. Analisando o número 4.
$m = 4$, $a = 3$, $mdc(4,3) = 1$

$$(x+3)^4 \equiv x^4 + 3\,(mod\ 4)$$

$$\begin{aligned}
(x+3)^4 &\equiv x^4 + 3\,(mod\ 4)\\
x^4 + 12x^3 + 64x^2 + 108x + 81 &\equiv x^4 + 3\,(mod\ 4)\\
12x^3 + 64x^2 + 108x + 81 &\equiv 3\,(mod\ 4)\\
12x^3 + 64x^2 + 108x + 80 + 1 &\equiv 3\,(mod\ 4)\\
1 + \underbrace{4(3x^3 + 16x^2 + 27x + 20)}_{\text{divisível por 4}} &\equiv 3\,(mod\ 4)\\
1 &\equiv 3\,(mod\ 4) \Rightarrow \text{(absurdo)}
\end{aligned}$$

4 não é número primo.

2.3 QUANTIDADE DE NÚMEROS PRIMOS

Diversas ferramentas matemáticas foram usadas para aprimorar os conhecimentos sobre os números primos. Entre essas ferramentas, Gauss introduziu a função $\pi(x)$.

A função $\pi(x)$ determina a quantidade de números primos até o número x.

Definição 2.9. Definimos o conjunto $\Pi(x)$ como:

$$\Pi(x) = \{p \in \varphi | p \leqslant x\}$$

Ou seja, $\Pi(x)$ é o conjunto de todos os números primos menores ou igual a x.

Definição 2.10. Para um número real x, a função $\pi(x)$ é definida por:

$$\pi(x) = card\ \Pi(x)$$

Ou seja, $\pi(x)$ é definido pela quantidade de elementos $\Pi(x)$

Exemplo 2.11. .

$\Pi(3) = \{2,3\}$ $\pi(3) = 2$	$\Pi(10) = \{2,3,5,7\}$ $\pi(10) = 4$	$\Pi(20) = \{2,3,5,7,11,13,17,19\}$ $\pi(20) = 8$

Para determinar a quantidade de números primos até números grandes, no final do século XIX, os matemáticos Cauchy, Hadamard e Valée Poussin apresentaram um teorema dos números primos que descreve o comportamento assintótico da função $\pi(x)$.

Teorema 2.11. ***Teorema do número Primo*** *Vale a igualdade:*

$$\lim_{x\to\infty} \frac{\pi(x)}{\frac{x}{\ln x}} = 1$$

Isso quer dizer que para um valor de x suficientemente grande, a função $\pi(x)$ é aproximada para $\frac{x}{lnx}$.

Tabela de Teorema de Número Primo

x	$\frac{x}{lnx}$	valor aproximado de $\pi(x)$	valor exato de $\pi(x)$
10	$4,343$	4	4
10^2	$21,715$	22	25
10^3	$144,765$	145	168
10^4	$1085,736$	1086	1229
10^5	$8685,89$	8686	9592
10^6	$72382,416$	72382	78498
10^9	$48254942,436$	48254942	50847534

Nos gráficos 2 e 3, a curva verde representa a função $f(x) = \frac{x}{lnx}$ e os pontos azuis representam os valores exatos de $\pi(x)$. Verificando visualmente que as duas funções têm valores estritamente próximos.

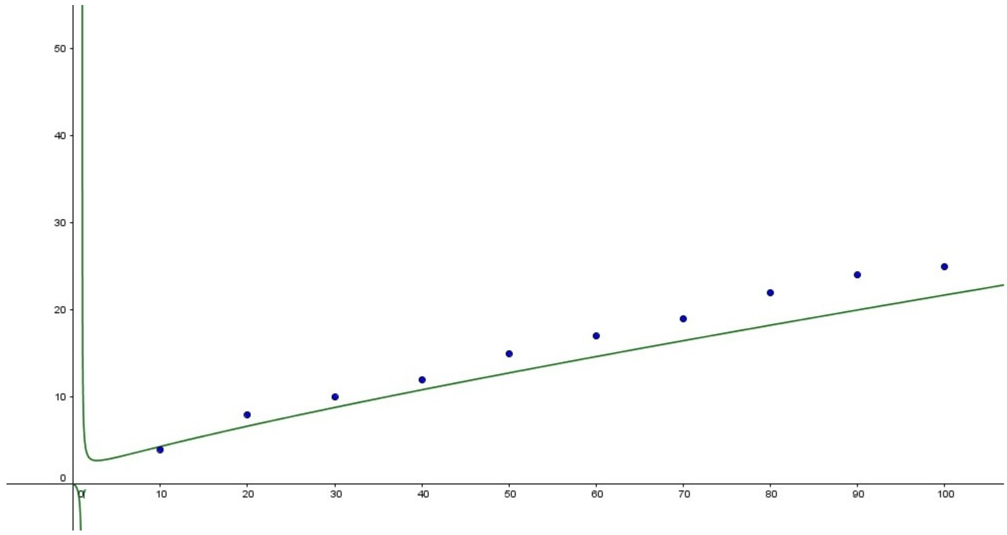


Figura 2: Comparação entre valor aproximado e exato de $\pi(x)$

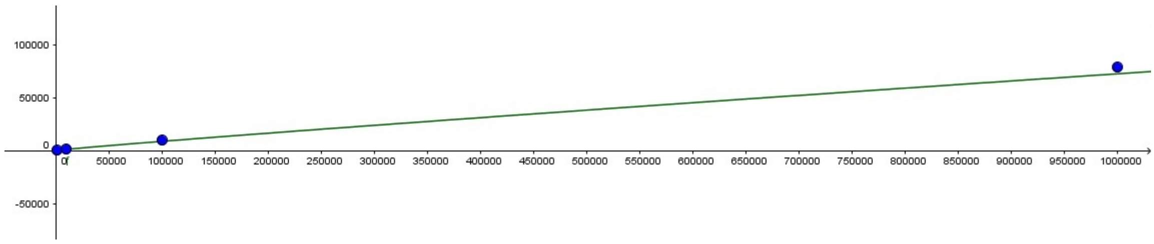


Figura 3: Comparação entre valor aproximado e exato de $\pi(x)$

3

CONJECTURA DE GOLDBACH

3.1 CHRISTIAN GOLDBACH

Christian Goldbach nasceu em 18 de março de 1690, na cidade de Königsberg, Brandemburgo - Prússia.

Figura 4: Christian Goldbach

Pouco se sabe sobre sua infância e juventude, a não ser que estudou legislação e matemática. Também viajou bastante pela Europa, durante suas viagens conheceu pessoalmente vários matemáticos famosos, entre eles, Gottfried Leibniz, Nicolau Brenoulli e Leonhard Euler.

Em 1725, ingressou para lecionar na, recém fundada, Academia das Ciências de São Pertersburg. Nesse período, Christian correspondia-se por meio de cartas com Euler[1], discutindo resoluções de problemas e, muitas vezes, solicitando que Euler verificasse seus resultados ou testasse suas teorias. Em uma dessas cartas, em 1942, foi enunciado, o que posteriormente ficou conhecido como, Conjectura de Goldbach.

Apesar da sua grande aptidão para a teoria dos números, acredita-se que Christian Goldbach tinha a matemática como atividade recreativa.

Goldbach faleceu em Moscou, no dia 20 de novembro de 1764, deixando parte de sua obra incompleta.

3.2 A CONJECTURA

Conjectura é uma proposição matemática que se acredita verdadeira, porém ainda não demonstrada.

Goldbach escreveu em uma carta para Euler que:

Afirmativa 3.1. *Verifica-se que:*

(A) Todo número inteiro par maior ou igual que 6 pode ser escrito como a soma de dois números primos ímpares.

(B) Todo número inteiro ímpar maior ou igual que 9 pode ser escrito como a soma de três números primos impares.

Euler respondeu que a afirmação lhe parecia correta, porém não conseguia demostrá-la.

Lema 3.2. *A conjectura (A) implica a conjectura (B), isto é,* $(A) \Rightarrow (B)$

Demonstração. Suponha válida (A). Então, para $k \in \mathbb{Z}$, $k \geqslant 3$ existe p_1 e p_2 são primos tal que $2k = p_1 + p_2$. Daí, $2k + 3 = p_1 + p_2 + 3$ o que implica $2k' + 1 = p_1 + p_2 + 3$ com $k' \geq 4$ e $p_1, p_2, 3$ primos.

Assim, concluimos que $(A) \Rightarrow (B)$. □

Além disso, sabemos que $4 = 2 + 2$, como 2 é primo.

Assim, Conjectura de Goldbach foi simplificada da seguinte forma:

1 Leonhard Paul Euler, matemático suiço (1707 - 1783)

Afirmativa 3.3. ***(Conjectura de Goldbach)*** *Todo número par maior ou igual a 4 pode ser escrito como a soma de dois números primos.*

3.3 ALGUNS RESULTADOS

Uma carta escrita em 1917, originou a conjectura de Goldbach, muitos esforços foram realizados para a comprovação dessa hipótese (ainda em aberto). Procurando a solução desse problema, foram obtidos alguns resultados preliminares [22].

Por exemplo, Lev Genrikhovich Shnirelmann, um matemático russo nascido em 1905 e que se suicidou em 1938, trabalhando no Instituto de Matemática Steklov, tentou provar a Conjectura de Goldbach. Ele utilizou o Crivo de Brun, e chegou ao resultado intermediário de que qualquer número inteiro maior ou igual a 2 pode ser escrito como soma, de um número limitado de parcelas primas.

Figura 5: Lev Genrikhovich Shnirelmann

Também inspirado no problema original, Ivan Matveevich Vinogradov (1891 - 1983), matemático russo reconhecido como um dos fundadores da teoria analítica dos números, provou que todo número ímpar *suficientemente grande* pode ser escrito como a soma de três primos.

Figura 6: Ivan Matveevich Vinogradov

Jing-Run Chen (1933 - 1996), matemático chinês, em 1966, enunciou e demonstrou o Teorema de Chen, provocando um grande impacto nos estudos da conjectura de Goldbach.

Figura 7: Jing-Run Chen

Teorema 3.4. ***(Teorema de Chen)*** *Todo número par suficientemente grande é uma soma de um número primo com um outro número que seja um produto entre dois números primos.*

Exemplo 3.1.

$$12 = 3 + 3 \cdot 3$$

$$50 = 11 + 3 \cdot 13$$

$$100 = 23 + 7 \cdot 11$$

$$974030 = 37441 + 1321 \cdot 709$$

Em 1995, Olivier Ramaré complementou o estudo do Teorema de Schnirelmann provando que todo número par é a soma de, no máximo, seis números primos. Esse resultado é em decorrência do Teorema de Vinogradov.

Figura 8: Matemático francês Olivier Ramaré

Teorema 3.5. *Todo número par é a soma de, no máximo, seis números primos.*

Conhecido na literatura como conjectura fraca de Golbach, também chamada de conjectura ternária de Goldbach, é de fato um teorema que ficou em suspenso por quase três séculos, quando em 2013, Harald Andrés Helfgott demonstrou no seu artigo "Major arcs for Goldbachs problem" [12].

Teorema 3.6. *Cada inteiro ímpar n maior que 5 pode ser expresso como a soma de três números primos.*

Figura 9: Harald Andrés Helfgott, matemático peruano

Esse trabalho faz parte de uma longa linha de artigos que usam uma técnica chamada "método do círculo de Hardy-Littlewood-Vinogradov". A ideia geral é transformar uma questão sobre números, neste caso, os primos, em integrais em círculos, usando técnicas originalmente provenientes da análise de planos complexos.

Vale observar que, segundo Helfgott, esse estudo não será útil para a demonstração da Conjectura de Goldbach.

3.4 UM OUTRO OLHAR PARA A CONJECTURA DE GOLDBACH

Nessa sessão apresentaremos uma das formas como a conjectura de Goldbach foi encarada na tentativa (até agora sem sucesso) de demonstrá-la.

A técnica que será apresentada é devida a Eduardo Garibaldi e pode ser encontrada no artigo Aproximações do problema de Goldbach [10].

Essa abordagem usa a definição:

Definição 3.7. Seja C um subconjunto dos inteiros positivos. Dizemos que C é $L-$ *Goldbach* quando L for o menor inteiro positivo tal que, para cada $k \geq L$, podemos encontrar $m, n \in C$ satisfazendo $m + n = 2k$.

Em outras palavras, seja $C \subset \mathbb{Z}$, com $m_i, n_i \in C$ e $i = \{0, 1, 2, 3, \cdots\}$. Se C é $L - $ *Goldbach* então temos:

$$\begin{cases} 2L = m_0 + n_0 \\ 2(L+1) = m_1 + n_1 \\ 2(L+2) = m_2 + n_2 \\ 2(L+3) = m_3 + n_3 \\ \vdots \\ 2(L+j) = m_j + n_j \quad , j \in \mathbb{N} \end{cases}$$

Exemplo 3.2. C_1: conjunto dos números pares positivos é $2 - Goldbach$.
De fato, como $C_1 = \{2n; n \in \mathbb{N}\}$ então dado $k \geq 2$ tem-se:
$2k = 2 + (2k - 2)$ onde $2, 2k - 2 \in C_1$.
Portanto, C_1 é $2 - Goldbach$.

Exemplo 3.3. C_2: conjunto dos números ímpares positivos é $1 - Goldbach$.
De fato, como $C_2 = \{2n + 1; n \in \mathbb{N}\}$ então dado $k \geq 1$ tem-se:
$2k = 1 + (2k - 1)$ onde $1, 2k - 1 \in C_1$.
Portanto, C_2 é $1 - Goldbach$.

Definição 3.8. Definimos como G o conjunto dos números naturais maiores ou igual a 2.

$$G = \{g, g \in \mathbb{N}, n \geq 2\}$$

Definição 3.9. Definimos como wG o conjunto dos múltiplos de w exceto o próprio w.

$$wG = \{w \cdot n, n \in \mathbb{N}, n \geq 2\}$$

Definição 3.10. Definimos como G_w o conjunto G retirando o conjunto wG.

$$G_w = G \setminus wG$$

e $G_{w,y}$ o conjunto G_w retirando o yG.

$$G_{w,y} = G_w \setminus yG$$

Exemplo 3.4. $G = \{g, g \in \mathbb{N}, g \geq 2\}$
$G \;=\; \{2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, \cdots\}$
$G_2 \;=\; G \setminus 2G \;=\; \{2, 3, 5, 7, 9, 11, 13, 15, 17, 19, 21, 23, 25, \cdots\}$
$G_{2,3} \;=\; G_2 \setminus 3G \;=\; \{2, 3, 5, 7, 11, 13, 17, 19, 23, 25, \cdots\}$
$G_{2,3,5} \;=\; G_{2,3} \setminus 5G \;=\; \{2, 3, 5, 7, 11, 13, 17, 19, 23, \cdots\}$

O conjunto G_w é útil para a análise da conjectura de Goldbach, em especial, quando observamos os conjuntos G_{p_n} (p_n número primo), isto porque para cada p_nG retirado do conjunto G mais nos aproximamos do conjunto dos números primos.

Pelas definições apresentadas, podemos dizer que a Conjectura de Goldbach se equivale a afirmação $\wp$ é $2 - Goldbach$.

Proposição 3.11. *Dado $G \subseteq \mathbb{N}$ não vazio vale:*

$$G_{w_1,w_2,w_3,\cdots w_s} = G_{w_1} \bigcap G_{w_2} \bigcap G_{w_3} \bigcap \cdots \bigcap G_{w_s}$$

Demonstração. Mostremos por indução

(i) $G_{w_1} = G_{w_1}$ (óbvio).

(ii) Supondo que $G_{w_1,w_2,w_3,\cdots w_{s-1}} = G_{w_1} \cap G_{w_2} \cap G_{w_3} \cap \cdots \cap G_{w_{s-1}}$ temos que por definição $G_{w_1,w_2,w_3,\cdots w_s} = G_{w_1,w_2,w_3,\cdots w_{s-1}} \setminus w_sG$

$$\begin{aligned} G_{w_1,w_2,w_3,\cdots w_s} &= G_{w_1,w_2,w_3,\cdots w_{s-1}} \setminus w_sG \\ &= G_{w_1,w_2,w_3,\cdots w_{s-1}} \bigcap (w_sG)^c \\ &= G_{w_1,w_2,w_3,\cdots w_{s-1}} \bigcap G_{w_s} \end{aligned}$$

usando a hipótese de indução:

$$G_{w_1,w_2,w_3,\cdots w_s} = G_{w_1} \bigcap G_{w_2} \bigcap G_{w_3} \bigcap \cdots \bigcap G_{w_s}$$

Por (i) e (ii) segue que a afirmação é verdadeira. □

Observação: Note que $\bigcap\limits_{p \in \wp} G_p = \wp$.

Proposição 3.12. *Sejam $w_1, w_2, w_3, \cdots w_s \in \mathbb{N}$ e $p_1, p_2, p_3, \cdots p_r$ primos distintos que aparecem na decomposição de $w_1, w_2, w_3, \cdots w_s$. Então:*

$$G_{p_1,p_2,p_3,\cdots p_r} \subseteq G_{w_1,w_2,w_3,\cdots w_s}$$

Demonstração. Supondo $w_n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot p_3^{\alpha_3} \cdots p_r^{\alpha_r}$, com $n \in \{1, 2, 3, \cdots, s\}$

Podemos afirmar que $G_{p_1,p_2,p_3,\cdots p_r} \subseteq G_{w_n}$ pela proposição 3.11, temos

$$G_{p_1} \bigcap G_{p_2} \bigcap G_{p_3} \bigcap \cdots \bigcap G_{p_r} \subseteq G_{w_n}$$

Tome $x \in G_{p_1,p_2,p_3,\cdots p_r}$ então $x \in G\bigcap(p_1G)^c\bigcap(p_2G)^c\bigcap(p_3G)^c\bigcap\cdots\bigcap(p_rG)^c$.

Logo $x \in G$ e $x \neq p_i l$, com $i \in \{1,2,3,\cdots r\}$ e $l \geq 2$.

Portanto $x \in G$ e $x \neq w_n\tilde{l}$, com $\tilde{l} \geq 2$.

Pois caso o contrário teriamos $x = w_n\tilde{l}$, o que é equivalente a

$$x = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot p_3^{\alpha_3} \cdots p_r^{\alpha_r} \cdot \tilde{l} = p_1 \cdot (p_1^{\alpha_1 - 1} \cdot p_2^{\alpha_2} \cdots p_r^{\alpha_r} \cdot \tilde{l}) = p_1 \cdot l$$

.

Concluindo o absurdo de $x = p_1 \cdot l$.

Assim, temos:

$$\begin{array}{l} G_{p_1,p_2,p_3,\cdots p_r} \subseteq G_{w_1} \\ G_{p_1,p_2,p_3,\cdots p_r} \subseteq G_{w_2} \\ G_{p_1,p_2,p_3,\cdots p_r} \subseteq G_{w_3} \\ \qquad\vdots \\ G_{p_1,p_2,p_3,\cdots p_r} \subseteq G_{w_s} \end{array} \Rightarrow \mathrm{G}_{p_1,p_2,p_3,\cdots p_r} \subseteq G_{w_1}\bigcap G_{w_2}\bigcap\cdots\bigcap G_{w_s} \Rightarrow \mathrm{G}_{p_1,p_2,p_3,\cdots p_r} \subseteq G_{w_1,w_2,w_3,\cdots w_s}$$

□

No artigo *Aproximações ao Problema se Goldbach*, Eduardo Garibaldi mostrou que:

Lema 3.13. *O conjunto $G_{2,w}$ é $2-$ Goldbach.*

Demonstração. $G_{2,w}$ é $2-$ *Goldbach* se, somente se, existe $m_i + n_i = 2k$, com $k \in \mathbb{N}$ e $m, n \in G_{2,w}$.

Analisando por casos:

caso 1: k ímpar e $k \notin wG$.

Tomemos $m = n = k$.
Como m, n ímpar $\Rightarrow m, n \in G_2$, também $m, n \notin wG \Rightarrow m, n \in G_w$
Consequentemente $m, n \in G_{2,w}$
E $m + n = k + k = 2K$.

caso 2: k ímpar e $k \in wG$.

Tomemos $m = k + 2$ e $n = k - 2$.
Como m, n ímpar $\Rightarrow m, n \in G_2$, também $k \in wG \Rightarrow k \pm 2 \notin wG \Rightarrow m, n \in G_w$.
Consequentemente $m, n \in G_{2,w}$.
E $m + n = (k + 2) + (k - 2) = 2K$.

caso 3: k par e $k \in wG$.

Tomemos $m = k+1$ e $n = k-1$.
Como k par $\Rightarrow k \pm 1$ ímpar $\Rightarrow m, n \Rightarrow m, n \in G_2$, também $k \in wG \Rightarrow k \pm 1 \notin wG \Rightarrow m, n \in G_w$.
Consequentemente $m, n \in G_{2,w}$.
E $m + n = (k+1) + (k-1) = 2K$.

caso 4: k par e $k \notin wG$.

Tomemos $m = k + w$ e $n = k - w$. Como k par e w impar $\Rightarrow k \pm W$ ímpar $\Rightarrow m, n \Rightarrow m, n \in G_2$, também $k \in wG \Rightarrow k \pm w \notin wG \Rightarrow m, n \in G_w$.
Consequentemente $m, n \in G_{2,w}$.
E $m + n = (k+w) + (k-w) = 2K$.

Note que, em particular, se $w = p$ com p primo, $G_{2,p}$ é $2 - Goldbach$. Note, também, $\mid m - n \mid \leq 2 \cdot w$. □

Teorema 3.14. *$G_{p_1,p_2,p_3,\cdots p_r}$ é $L - Goldbach$ com $L \leq 4 \cdot (p_1 \dot{p}_2 \cdot p_3 p_{r-1}) + 2$.*

Demonstração. A demonstração se dará em três etapas.

Fizemos a_i inteiros não nulos tais que $\sum_{i=1}^{r} a_i \dot{p}_1 \cdot p_2 \cdots p_{i-1} \cdot p_{i+1} \cdots p_r = 1$.

Etapa 1:

Podemos tomar $L \leqslant p_1 \cdot p_2 \cdots p_r \cdot \sum_{i=1}^{r} \mid a_i \mid + 2$.

Sabemos que G_{2,p_i} é $2 - Goldbach$, para $i \in \{1, 2, \ldots, r\}$. Logo, para $k \geqslant 2$, com $k \in \mathbb{N}$, existem $m_i, n_i \in G_{2,p_1}$, satisfazendo $m_1 + n_1 = 2k$. Além disso, em decorrência do lema 3.13, podemos assumir que $\mid m_i - n_i \leqslant\mid 2 \cdot p_i$.

Definimos,

$m = \sum_{i=1}^{r} a_i \cdot p_1 \cdot p_2 \cdots p_{i-1} \cdot p_{i+1} \cdots p_r \cdot m_i$ e $n = \sum_{i=1}^{r} a_i \cdot p_1 \cdot p_2 \cdots p_{i-1} \cdot p_{i+1} \cdots p_r \cdot n_i$

Note que:

$$m + n = \sum_{i=1}^{r} a_i \cdot p_1 \cdot p_2 \cdots p_{i-1} \cdot p_{i+1} \cdots p_r \cdot (m_i + n_i)$$
$$m + n = \sum_{i=1}^{r} a_i \cdot p_1 \cdot p_2 \cdots p_{i-1} \cdot p_{i+1} \cdots p_r \cdot 2k$$
$$m + n = 2k \cdot \sum_{i=1}^{r} a_i \cdot p_1 \cdot p_2 \cdots p_{i-1} \cdot p_{i+1} \cdots p_r$$
$$m + n = 2k$$

Temos: $a_i \cdot p_1 \cdot p_2 \cdots p_{i-1} \cdot p_{i+1} \cdots p_r \equiv 1 \,(mod\ p_i)$, assim vale que: $m \equiv m_i\,(mod\ p_i)$ e $n \equiv n_i\,(mod\ p_i)$.

Consequentemente:
$m, n \notin p_i G \Rightarrow m, n \in G_{p_i} \Rightarrow m, n \in G \bigcap G_{p_1} \bigcap G_{p_2} \bigcap \cdots \bigcap G_{p_r} \Rightarrow m, n \in G_{p_1, p_2, \cdots, p_r}$.

Agora, basta mostra que $m, n \in G_2$

Assumindo $S = \{i : a_i \text{ é ímpar }\}$, observamos: $m \equiv \sum_{i \in S} m_i\,(mod\ 2)$ e $m \equiv \sum_{i \in S} n_i\,(mod\ 2)$

Como $\sum_{i \in S}^{r} a_i \equiv 1\,(mod\ 2)$, constatamos que $\#S$ é ímpar.

Assim, precisamos garantir que $2 \leqslant m, n \leqslant 2K - 2$.
Isto, contudo, equivale a $\mid m - n \mid \leqslant 2k - 4$.

Note,
$\mid m - n \mid \leqslant \sum_{i=1}^{r} a_i \cdot p_1 \cdot p_2 \cdots p_{i-1} \cdot p_{i+1} \cdots p_r \cdot \mid m_i - n_i \mid \leqslant 2 \cdot p_1 \cdot p_2 \cdots p_r \cdot \sum_{i=1}^{r} \mid a_i \mid$.

Estabelecendo a desigualdade para o caso $k \geqslant p_1 \cdot p_2 \cdots p_r \cdot \sum_{i=1}^{r} \mid a_i \mid + 2$

Como ocorre $\mid m_i - k \mid, \mid n_i - k \mid \leqslant p_i$.

Então $m_i, n_i \geqslant (p_1 \cdot p_2 \cdots p_{i-1} \cdot p_{i+1} \cdots p_r \cdot \sum_{i=1}^{r} \mid a_i \mid - 1) \cdot p_i + 2$.
Assim, $m_i, n_i \notin \{2, p_i\}$.

Portanto, $m, n \in G_{2, p_1, p_2, \cdots, p_r}$.

Etapa 2:

É possível assumir $L \leqslant p_1 \cdot p_2 \cdots p_r + 2$.

Consideremos a situação $p_1 \cdot p_2 \cdots p_r + 2 \leqslant k < p_1 \cdot p_2 \cdots p_r \cdot \sum_{i=1}^{r} \mid a_i \mid + 2$.

Seja N o menor inteiro não negativo tal que
$k + 2^N \cdot p_1 \cdot p_2 \cdots p_r \geqslant p_1 \cdot p_2 \cdots p_r \cdot \sum_{i=1}^{r} \mid a_i \mid + 2$.

Assumindo $S = \{i : a_i \text{ é ímpar }\}$, observamos: $m \equiv \sum_{i \in S} m_i\,(mod\ 2)$ e $m \equiv \sum_{i \in S} n_i\,(mod\ 2)$

Para $K_0 = k + 2^N \cdot p_1 \cdot p_2 p_r$, temos $u_0, v_0 \in G_{p_1, p_2, \cdots, p_r}$
Assim, para $m_i, n_i \in G_{2, p_i}$ sendo $m_i + m_i = 2 \cdot K_0$ e $\mid m_i - n_i \mid \leqslant 2 \cdot p_i$, verificamos que $u_0 + v_0 = 2 \cdot K_0$.
$u_0 \equiv m_i \neq 0\,(mod\ p_i)$, $v_0 \equiv n_i \neq 0\,(mod\ p_i)$
$u_0 \equiv \sum_{i \in S} m_i \neq 0\,(mod\ 2)$, $v_0 \equiv \sum_{i \in S} n_i \neq 0\,(mod\ 2)$

$$2 \leqslant v_0 \leqslant K_0 \leqslant u_0 \leqslant 2 \cdot K_0 - 2$$

Da igualdade inicial segue a expressão $u_0 + v_0 = 2(k + 2_N \cdot p_1 \cdot p_2 \cdots p_r)$.
temos a sequência de desigualdades

$$2 \leqslant v_0 \leqslant k + 2^N \cdot p_1 \cdot p_2 \cdots p_r \leqslant u_0 \leqslant 2(k + 2^N \cdot p_1 \cdot p_2 \cdots p_r) - 2$$

constatando que

$$(u^0 - 2^N \cdot p_1 \cdot p_2 \cdots p_r) + v_0 = 2(k + 2^{N-1} \cdot p_1 \cdot p_2 \cdots p_r)$$

$u_0 - 2^N \cdot p_1 \cdot p_2 \cdots p_r \equiv u_0 \,(mod\ p_i)$
$u_0 - 2^N \cdot p_1 \cdot p_2 \cdots p_r \equiv u_0 \,(mod\ 2)$

$$2 < k \leqslant u_0 - 2^N \cdot p_1 \cdot p_2 \cdots p_r \leqslant 2(k + 2^{N-1} \cdot p_1 \cdot p_2 \cdots p_r) - 2$$

Sejam $u_k = max\{u_{k-1} - 2^N \cdot p_1 \cdot p_2 \cdots p_r, v_{k-1}\}$ e $v_k = max\{u_{k-1} - 2^N \cdot p_1 \cdot p_2 \cdots p_r, v_{k-1}\}$.

Temos: $2 \leqslant k - p_1 \cdot p_2 \cdots p_r \leqslant u_N - 2 \cdot p_1 \cdot p_2 \cdots p_r \leqslant 2k - 2$

Portanto, se $m = u_N - 2 \cdot p_1 \cdot p_2 \cdots p_r$ e $n = v_N$,

segue $m, n \in G_{p_1 \cdot p_2 \cdots p_r}$ com $m + n = 2k$.

Etapa 3:

Temos $L \leqslant 4 \cdot p_1 \cdot p_2 \cdots p_r \cdot \sum_{i=1}^{r} \mid a_i \mid +2$.

Ao assumir $4 \cdot p_1 \cdot p_2 p_{r-1} + 2 \leqslant k < p_1 \cdot p_2 p_{r-1} + 2$.
Existem $u, v \in G_{2, p_1, p_2, \cdots, p_r} \setminus \{2, p_1, p_2, \cdots, p_{r-1}\}$ cumprindo $u + v = 2k$.
Supondo, $v \leqslant u$, é suficiente concluir que para $\theta \in \{0, 1, 2\}$, o primo p_r não divide $m = m(\theta) = u - 2 \cdot \theta \cdot p_1 \cdot p_2 \cdots p_{r-1}$ nem $n = n(\theta) = v - 2 \cdot \theta \cdot p_1 \cdot p_2 \cdots p_{r-1}$.

Decorre $m, n \in G_{p_1, p_2, \cdots, p_r}$ com $m + n = 2k$.

Sendo então, $m(\theta), n(\theta) \equiv 0 \,(mod\ p_r)$. Isso determina o absurdo $\theta_1 \equiv \theta_2 \,(mod\ p_r)$, para os distintos $\theta_1, \theta_2 \in \{0, 1, 2\}$.

Tal absurdo, encerra a demonstração.

□

Teorema 3.15. *Assuma $G_{p_1, p_2, p_3, \cdots p_r}$ é $L - Goldbach$ com $L \leq \frac{\pi_{s+1}^2 + 3}{2}$, sendo π_s o s-ésimo primo ímpar. Se $G_{\pi_1, \pi_2, \cdots \pi_s}$ for $2 - Goldbach$, então $G_{p_1, p_2, p_3, \cdots p_r}$ igualmente será $2 - Golgbach$*

Demonstração. Notamos que todos elementos de $G_{2, \pi_1, \pi_2, \cdots \pi_s} \bigcap \{1, 2, 3, \cdots, \pi_{s+1}^2 - 1\}$ são números primos.

Como $G_{2,\pi_1,\pi_2,\cdots\pi_s}$ é $2 - Goldbach$ para $3 \leqslant k < \frac{\pi_{s+1}^2+3}{2}$.

Se tomarmos $m, n \in G_{\pi_1,\pi_2,\cdots\pi_s}$ satisfazendo $m + n = 2k$, então segue que $m, n \leq 2k - 3 < \pi_{s-1}^2$.

(De fato, se $m > 2k - 3$ como m não é par temos $m \geq 2k - 1$ e daí $m + n \geq 2k + 1$)

Logo m, n são primos, onde $m, n \in G_{2,p_1,p_2,\cdots,p_r}$ e portanto $G_{2,p_1,p_2,\cdots,p_r}$ é $2 - Goldbach$.

□

A abordagem apresentada aqui refere-se a uma tentativa de demonstrar a conjectura de Goldbach por meio dos conjuntos $G_{2,p_1,p_2,\cdots,p_r}$.

Em decorrência do teorema 3.15, encontramos uma aplicação interessante: G_{2,p_1,p_2,p_3} é $2 - Goldbach$.

Efetivamente

Pelo lema 3.13, $G_{2,3}$ é $2 - Goldbach$.

Pelo teorema 3.14, $G_{2,3,p_2}$ é $L - Goldbach$, com $L \leqslant 4 \cdot (p_1) + 2 = 4 \cdot 3 + 2 = 14$

Assumindo $\pi_{s+1} = 7$, temos $\frac{\pi_{s+1}^2+3}{2} = \frac{7^2+3}{2} = \frac{49+3}{2} = 26$

Então, $L \leqslant \frac{\pi_{s+1}^2+3}{2}$, pelo teorema 3.15, $G_{2,3,5}$ é $2 - Goldbach$.

Agora temos, pelo teorema 3.14,
$G_{2,3,5,p_3}$ é $L - Goldbach$, com $L \leqslant 4 \cdot (p_1 \cdot p_2) + 2 = 4 \cdot (3 \cdot 5) + 2 = 62$

Assumindo $\pi_{s+1} = 11$, temos $\frac{\pi_{s+1}^2+3}{2} = \frac{11^2+3}{2} = \frac{121+3}{2} = 62$

Então, $L \leqslant \frac{\pi_{s+1}^2+3}{2}$, pelo teorema 3.15, $G_{2,3,5,7}$ é $2 - Goldbach$.

O próximo resultado, cuja demonstração será omitida, estabelece equivalência entre a conjectura de Goldbach e esses conjuntos.

Mais especificamente,

Teorema 3.16. *São equivalentes:*

(a) a conjectura de Goldbach.

(b) para todo $s > 1$ inteiro, $G_{2,\pi_1,\pi_2,\cdots\pi_s}$ é $L - Goldbach$, com $L \leq \frac{{\pi_s}^2+3}{2}$.

Com esse estudo, não demonstrada a conjectura de Goldbach, mas a substitui por um outro problema.

3.5 VERIFICAÇÃO DA CONJECTURA DE GOLDBACH

Na tentativa de demonstrar a conjectura de Goldbach muitas técnicas foram empregadas. Também verificações empíricas (que claramente não demonstra o resultado) foram usadas. Neste sentido, a validade da conjectura foi estabelecida para qualquer números par da ordem de 10^{18}.

No exemplo abaixo apresentamos alguns casos particulares:

Exemplo 3.5. Possibilidade de soma de primos para alguns números pares

- $4 = 2 + 2$
- $6 = 3 + 3$
- $8 = 3 + 5$
- $10 = 3 + 7$ ou $10 = 5 + 5$
- $12 = 5 + 7$
- $14 = 7 + 7$ ou $14 = 3 + 11$
- $16 = 3 + 13$ ou $16 = 5 + 11$
- $18 = 5 + 13$ ou $16 = 7 + 11$
- $20 = 3 + 17$ ou $16 = 7 + 13$
- $22 = 11 + 11$ ou $22 = 5 + 17$ ou $22 = 19 + 3$
- $\vdots$
- $100 = 97 + 3$
- $\vdots$
- $143800 = 104681 + 39119$
- $\vdots$
- $1000000 = 999983 + 17$
- $\cdots$

Seguindo essa linha de raciocínio, Georg Cantor[2], em 1894, enumerou todas as possíveis somas que satisfizessem a Conjectura de Goldbach para os números pares até 1000. No ano seguinte, A. Aubry ampliou estas decomposições para valores pares até 2000. Em 1897, R. Haussner, expandiu esta lista para valores pares até 5000.

No final do século XX, Jöeg Richstein [13] verificou a Conjectura de Goldbach até o valor $4 \cdot 10^{14}$. Ele utilizou um programa escrito em linguagem de computação C distribuído em 11 computadores. Esse programa tinha a capacidade de checar 10^7 números por segundo aproximadamente, completando a compilação em 130 dias.

Tomás Oliveira e Silva[3] tem um projeto de verificação da conjectura que utiliza o tempo livre de vários computadores compartilhados. Em abril de 2012, chegou à verificação de todos os números pares até $4 \cdot 10^{18}$.

De fato, para muitos números pares verificados até a atualidade, os cálculos de decomposição foram efetuados, e sempre se constatou dois números primos que satisfazem a Conjectura de Goldbach, porém o fato de não encontrarmos um contra-exemplo não garante sua prova.

2 Georg Ferdinand Ludwig Philip Cantor nasceu em São Petersburgo, na Rússia, a 3 de março de 1845, e faleceu em Halle, Alemanha, a 6 de janeiro de 1918.A teoria dos conjuntos, criada por Cantor, é uma das mais notáveis inovações matemáticas dos últimos séculos.

3 Matemático Português, professor da Universidade de Aveiro.

4

ABORDAGEM PEDAGÓGICA

Os números primos são o DNA da teoria dos números. Com toda essa magnitude e importância é esperado que números primos seja um tema com grande recorrência no conteúdo programático de matemática na educação básica.

Com essa expectativa, ao iniciar a análise dos Parâmetros Curriculares Nacionais - PCN [3] é surpreendente que a expressão "número primo" seja lida apenas uma vez, no capítulo "conteúdos propostos para o ensino de Matemática no terceiro ciclo".

> *Conceitos como os de "múltiplo" e "divisor" de um número natural ou o conceito de "número primo" podem ser abordados nesse ciclo como uma ampliação do campo multiplicativo.* [PCN-Matemática, 1998, p. 66]

Como os PCN de matemática visam à construção de um referencial que oriente a prática escolar e quanto aos conteúdos, apresentam maneiras de explorá-los não apenas em dimensão conceitual.

Passamos a analisar a matriz de conteúdos do Currículo oficial do estado de São Paulo [9] e, novamente, a expressão "número primo" é citada uma única vez. No quadro de conteúdos do 1º bimestre do sexto ano, orientando o professor a contemplar no seu plano de ensino as habilidades "saber identificar se um número é primo ou não" e "decompor um número em seus fatores primos".

Observando os livros didáticos de matemática do PNLD[1] [1,4,6], a maioria dos livros trata sobre o tema "números primos" unicamente no volume do 6º ano, apresentando a definição, algumas características desses números e algoritmo para determinar a decomposição em fatores primos.

1 Programa Nacional do Livro Didático

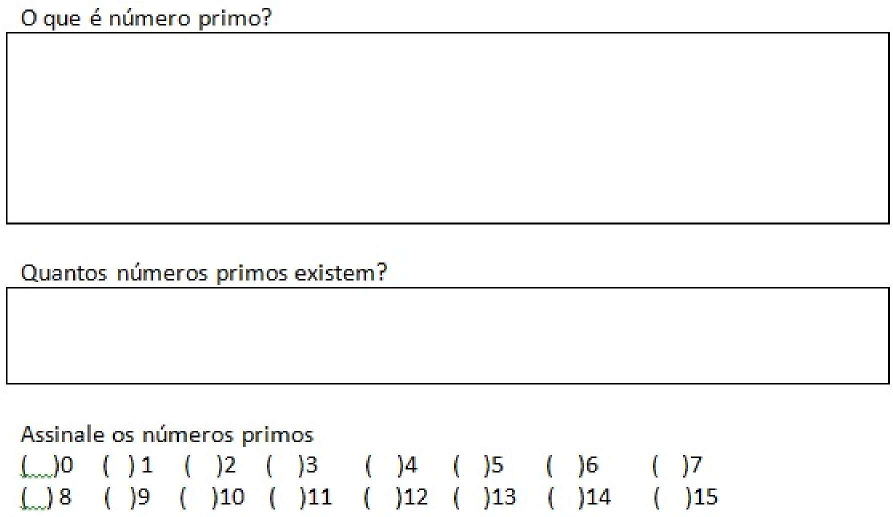
Sabendo da relevância dos números primos, surge a questão: Por que não se fala mais sobre números primos na educação básica de matemática?

4.1 PROBLEMÁTICA

A vivência em sala de aula permite-nos algumas análises sem o embasamento de uma pesquisa científica. Com esse conhecimento empírico e superficial, foi possível notar que os alunos do 3º ano do ensino médio e do 6º ano de ensino fundamental tinham conhecimentos similares sobre Números Primos.

Tal constatação inicial demonstrou-se intrigante, o que motivou a busca por dados estatísticos a fim de verificar tais premissas.

Foi solicitado que os alunos do 6º e 9º anos do EF (Ensino Fundamental) e do 3º ano do EM (Ensino Médio) respondessem, voluntariamente, a algumas questões sobre números primos.



O que é número primo?

Quantos números primos existem?

Assinale os números primos
( )0 ( )1 ( )2 ( )3 ( )4 ( )5 ( )6 ( )7
( )8 ( )9 ( )10 ( )11 ( )12 ( )13 ( )14 ( )15

Figura 10: Questionário

Após a aplicação do questionário acima com um grupo de 78 alunos do 6º ano do EF, 43 alunos do 9º ano do EF e 67 alunos do 3º ano do EM, os seguintes resultados foram verificados:

6º ano do EF

No que se refere a primeira pergunta proposta, entre os alunos do 6º ano do EF 21,5% responderam de forma precisa, apresentando a definição de número primo, 19% dos alunos, apesar de não apresentar um resposta precisa, utilizaram conceitos matemáticos para exemplificar os números primos, enquanto 59,5% dos alunos apresentaram respostas sem coerencia matemática.

Resposta precisa	21,5%
é utilizado para formar os números	5,1%
cita MMC	13,9%
resposta sem fundamentos matemáticos	59,5%

Tabela 6: O que é número primo?

Na segunda pergunta proposta, as respostas se distribuiram da seguinte forma:

Infinitos	25,3%
Muitos	13,9%
Vários	12,7%
indefinido	2,5%
Milhares	3,8%
Valores entre 3 e 10	19%
Valores entre 10 e 1000	7,6%
Cita alguns nºs	5,1%
em branco	10,1%

Tabela 7: Quantos números primos existem?

9º ano do EF

Na primeira questão, entre os alunos do 9º ano do EF 19,3% responderam de forma precisa, 14,7% dos alunos citaram a utilidade dos números primos para determimar o MMC, enquanto 66% dos alunos apresentaram respostas sem fundamentação matemática.

Resposta precisa	19,3%
é utilizado para formar os números	0%
cita MMC	14,7%
resposta sem fundamentos matemáticos	66%

Tabela 8: O que é número primo?

Na segunda questão, as respostas se distribuiram da seguinte forma:

Infinitos	50,1%
Milhares	3,6%
Valores entre 3 e 10	2,4%
Valores entre 10 e 1000	2,4%
em branco	41,5%

Tabela 9: Quantos números primos existem?

3º ano do EM

Em relação aos alunos do Ensino Médio os resultados encontrados foram similares ao dos alunos do Ensino Fundamental, na primeira pergunta 39,7% responderam de forma precisa, apresentando a definição de número primo, 5% dos alunos citaram o MMC como exemplo de utilização dos números primos, enquanto 55,1% dos alunos apresentaram respostas sem fundamentação matemática.

Resposta precisa	39,7%
é utilizado para formar os números	0%
cita MMC	5,2%
resposta sem fundamentos matemáticos	55,1%

Tabela 10: O que é número primo?

Na segunda pergunta, as respostas se distribuiram da seguinte forma:

Infinitos	64,1%
Milhares	2,3%
em branco	33,9%

Tabela 11: Quantos números primos existem?

Com os dados, levantados confirmamos o alto índice de respostoas não fundamentadas em todos os anos analisados. Por que isso ocorre? Como tentar resolver isso?

A proposta para modificar esse quadro é um mergulho sobre os números primos em diferentes momentos da escolarização do aluno.

Ainda, observamos que a capacidade de improvisar, própria dos alunos do 6º ano, em geral não se verifica nos alunos em idade escolar mais avançadas, as respostas "em branco" prevalecem sobre tentativas de respostas inusitadas.

4.2 PROPOSTA DE ABORDAGEM DOS NÚMEROS PRIMOS NO 6º ANO DO EF

Essa sessão apresenta uma sugestão de sequência didática com tema **Números Primos**, para ser aplicada em turmas do 6º ano do Ensino Fundamental.

Aqui entendemos por sequência didática um roteiro de atividades passo-a-passo que possibilita o desenvolvimento de um conteúdo, abordando diferentes habilidades e diversificando as metodologias utilizadas.

Dentro desta sequencia didática, 6 atividades foram propostas, as quais descrevemos a seguir.

Atividade 1: Atividade Motivacional

Ao iniciar o conteúdo a ideia é apresentar um desafio, ignorando, a princípio, definições e formalizações.

Jogos que desafiem a criança a criar hipóteses e diferentes soluções são motivacionais, como afirma Tezani [14]:

> *[O jogo] Estimula a observar e conhecer as pessoas e as coisas do ambiente que se vive. Por meio do jogo, o indivíduo pode brincar naturalmente testar hipóteses, explorar toda sua espontaneidade criativa. O jogo é essencial para que a criança manifeste sua criatividade, utilizando suas potencialidades de maneira integral.*

A proposta é que os alunos organizem diferentes quantidades de cartões, formando retângulos (com mesma quantidade de cartões em cada coluna).

A ideia por tras dessa atividade é explorar o conceito de divisibilidade.

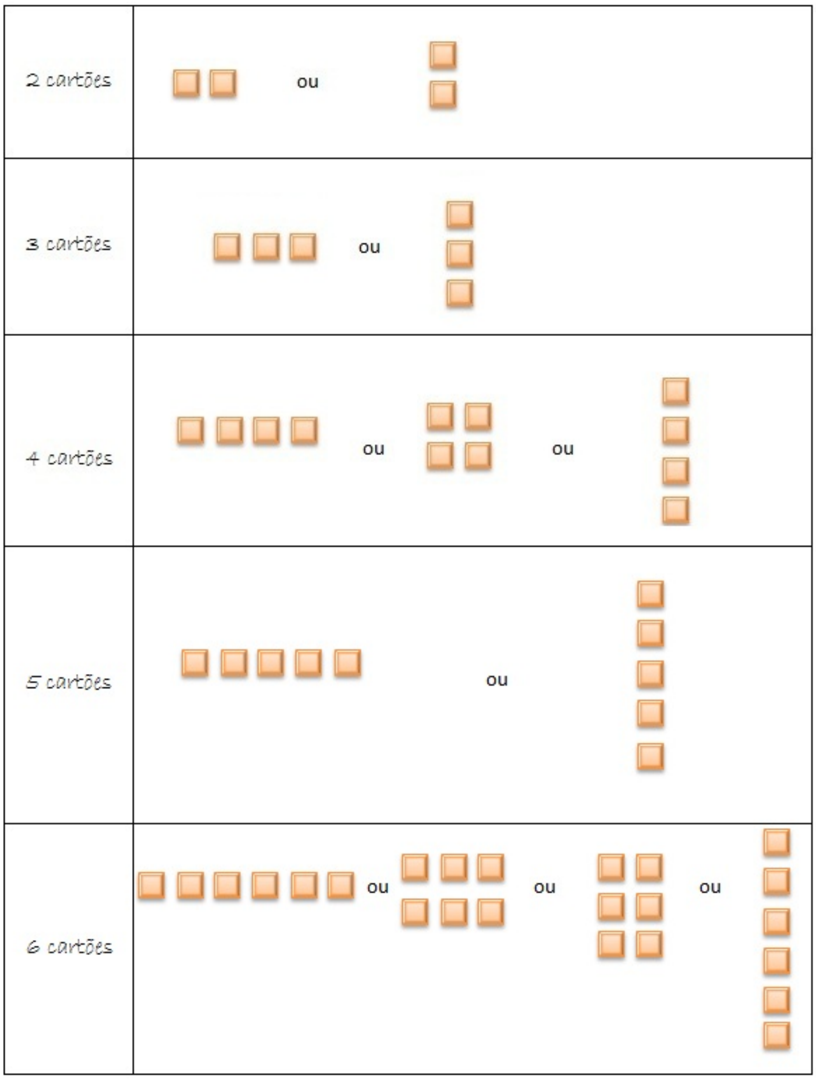


Figura 11: Solução desejada da atividade motivacional

Depois de aplicada a atividade em sala de aula (trabalhando com pequenas quantidades de cartões) os alunos foram incentivados a questionar a(s) razão(ões) pela quais algumas quantidades de cartões, por mais que tentassem, só havia duas soluções.

Após esses questionamentos, foi solicitado que os alunos tentassem organizar, da mesma maneira, 31 cartões (sem tê-los fisicamente).

Além disso, enfatizamos essa características “especial” de algumas quantidades de cartões,qual seja, a de que apenas duas soluções são possíveis.

Atividade 2: O que é número primo?

A formalização dos conceitos é necessária para o ensino da matemática. Para formalizar o conceito dos números primos a proposta é classificar os números em primos ou composto.

Atividade: Números Primos

1. **Divisores** de um número natural são os números com os quais se efetua uma divisão com resto zero.

Exemplos: $D(30)=\{1;2;3;5;6;10;15;30\}$
$D(31)=\{1;31\}$

Determine os divisores:

$D(1)=\{\quad\}$	$D(6)=\{\quad\}$	$D(11)=\{\quad\}$	$D(16)=\{\quad\}$
$D(2)=\{\quad\}$	$D(7)=\{\quad\}$	$D(12)=\{\quad\}$	$D(17)=\{\quad\}$
$D(3)=\{\quad\}$	$D(8)=\{\quad\}$	$D(13)=\{\quad\}$	$D(18)=\{\quad\}$
$D(4)=\{\quad\}$	$D(9)=\{\quad\}$	$D(14)=\{\quad\}$	$D(19)=\{\quad\}$
$D(5)=\{\quad\}$	$D(10)=\{\quad\}$	$D(15)=\{\quad\}$	$D(20)=\{\quad\}$

2. **Números Primos:** números que tem exatamente dois divisores, sendo 1 e o próprio número.
Números Compostos: números que tem mais de dois divisores

Complete a tabela, com os números usados no exercício anterior:

Números Primos	Números Compostos
31	30

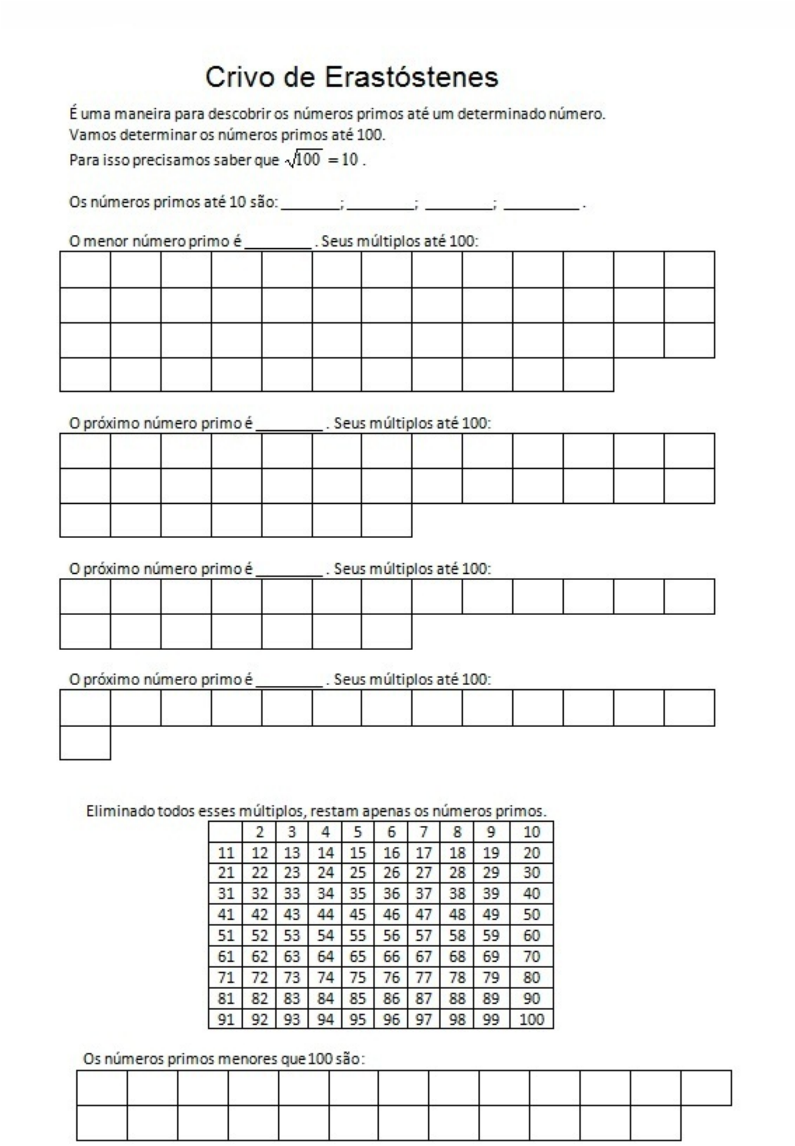
Figura 12: atividade: Classificação dos números primos

É notório que a matemática tem uma linguagem própria e o domínio dessa linguagem é uma das habilidades requeridas dos alunos, esse é um momento propício para introduzir termos matemáticos empregados na sua forma padrão.

Atividade 3: Crivo de Erastóstenes

Reconhecer os números primos é de fundamental importância para o estudo da matemática básica. Uma das atividades interessantes para a introdução dos números primos é o Crivo de Erastóstenes.

Na atividade proposta determinamos os números primos até 100. Para a realização dessa atividade o aluno já conhece a definição de número primo.



Crivo de Erastóstenes

É uma maneira para descobrir os números primos até um determinado número.
Vamos determinar os números primos até 100.
Para isso precisamos saber que $\sqrt{100} = 10$.

Os números primos até 10 são: ______; ______; ______; ______ .

O menor número primo é ______ . Seus múltiplos até 100:

O próximo número primo é ______ . Seus múltiplos até 100:

O próximo número primo é ______ . Seus múltiplos até 100:

O próximo número primo é ______ . Seus múltiplos até 100:

Eliminado todos esses múltiplos, restam apenas os números primos.

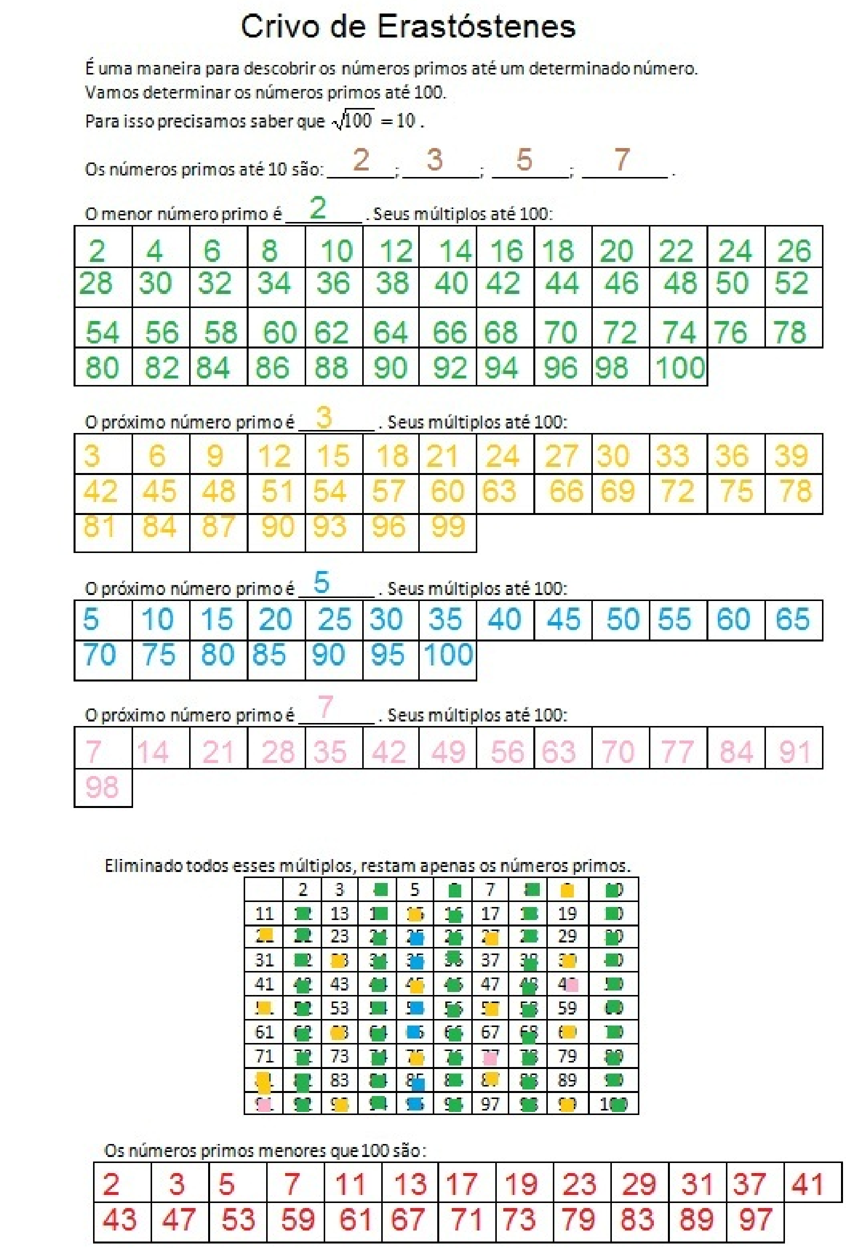
	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

Os números primos menores que 100 são:

Figura 13: atividade: Crivo de Erastóstenes

Espera-se que o aluno responda corretamente. Se necessário, vale retomar o conceito de múltiplos e, também, introduzir tópicos da História da Matemática [21] discutindo a biografia de Erastóstenes e a importância dos conhecimentos matemáticos da Grécia Antiga.

> *[...] a partir do momento que se conhece a História da Matemática, as aulas ficam mais interessantes e com aprendizado de qualidade.* - [Encontro Nacional de Educação Matemática - 2007]



Crivo de Erastóstenes

É uma maneira para descobrir os números primos até um determinado número.
Vamos determinar os números primos até 100.
Para isso precisamos saber que $\sqrt{100} = 10$.

Os números primos até 10 são: 2; 3; 5; 7.

O menor número primo é 2. Seus múltiplos até 100:

2	4	6	8	10	12	14	16	18	20	22	24	26
28	30	32	34	36	38	40	42	44	46	48	50	52
54	56	58	60	62	64	66	68	70	72	74	76	78
80	82	84	86	88	90	92	94	96	98	100		

O próximo número primo é 3. Seus múltiplos até 100:

3	6	9	12	15	18	21	24	27	30	33	36	39
42	45	48	51	54	57	60	63	66	69	72	75	78
81	84	87	90	93	96	99						

O próximo número primo é 5. Seus múltiplos até 100:

5	10	15	20	25	30	35	40	45	50	55	60	65
70	75	80	85	90	95	100						

O próximo número primo é 7. Seus múltiplos até 100:

7	14	21	28	35	42	49	56	63	70	77	84	91
98												

Eliminado todos esses múltiplos, restam apenas os números primos.

	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			

Os números primos menores que 100 são:

2	3	5	7	11	13	17	19	23	29	31	37	41
43	47	53	59	61	67	71	73	79	83	89	97	

Figura 14: Crivo de Erastóstenes

Atividade 4: Jogo dos números primos

Uma atividade lúdica é sempre atrativa aos olhos das crianças. Quando se há a necessidade de lembrar alguns dos números primos o jogo proposto a seguir permite o desenvolvimento de tal habilidade.

O jogo tem importância na aquisição de conhecimento e também no desenvolvimento das relações afetivas. Como pondera Rodrigues [20].

> *O jogo é uma atividade rica e de grande efeito que responde às necessidades lúdicas, intelectuais e afetivas. Isso estimula a vida social e representa, assim, importante contribuição na aprendizagem.* [Thaís Cristina Rodriguês Tezani]

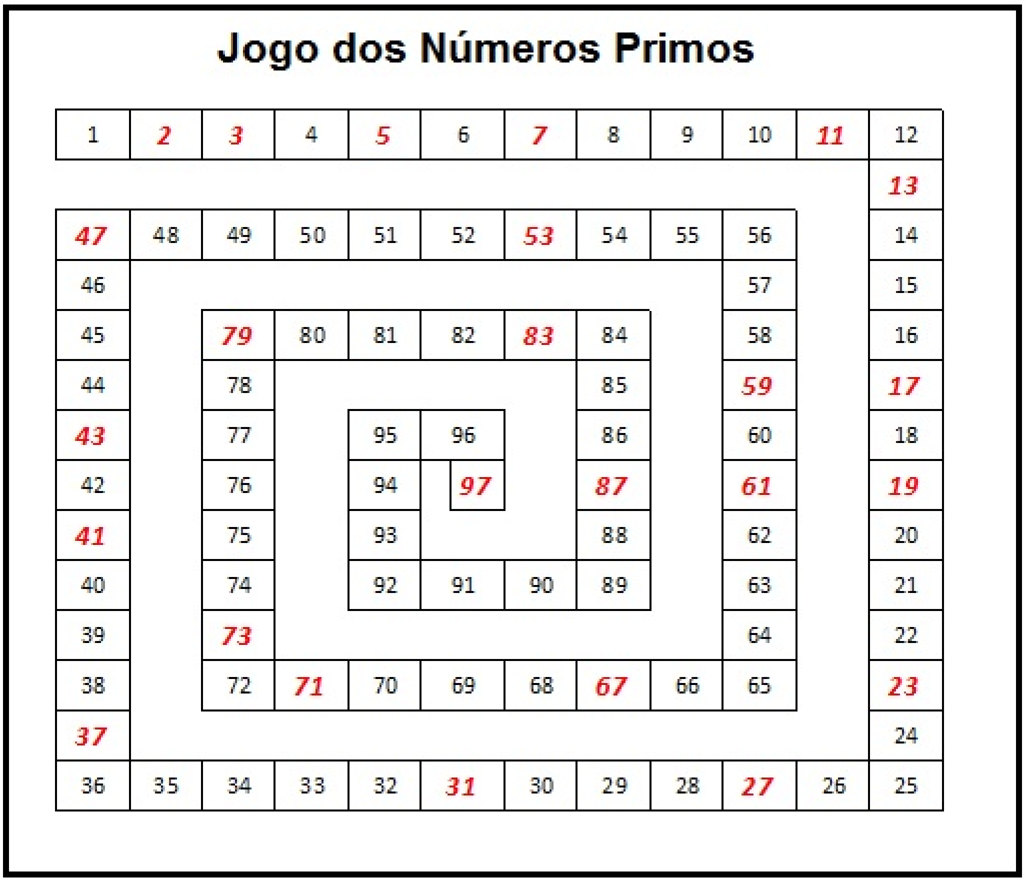


Figura 15: Tabuleiro do Jogo dos números primos

Regras:

- Partidas serão disputadas por dois jogadores.
- Decide quem inicia o jogo no "par ou ímpar"
- O primeiro jogador posiciona seu pino na casa desejada.
- O segundo jogador também posiciona o pino, de igual maneira.
- O primeiro e o segundo jogadores movimentam seus pinos alternadamente.
- Os pinos só podem ser posicionados em casas com números primos.
- Os dois pinos não podem ocupar a mesma casa.
- O pino não pode retornar a um número menor do atual.
- O pino não pode avançar mais do que 5 casas em cada jogada.
- Acaba o jogo, quando um dos jogadores ficar impossibilitado de movimentar seu pino, segundo as regras.
- O outro jogador é declarado campeão.

Atividade 5: Jogo Online

Segundo Stahl [19]:

> *Um jogo educativo por computador é uma atividade de aprendizagem inovadora, na qual, as características do ensino apoiado em computador e as estratégias de jogo são integradas para alcançar um objetivo educacional específico.*

Com a prerrogativa de que atende aos múltiplos interesses dos alunos e mantem o objetivo de que eles sejam capazes de reconhecer um número primo, propor o jogo online disponível em <http://nautilus.fis.uc.pt/mn/primos/index.html> é indicado.

Tal atidade inicia-se com a escolha do nível, podendo optar entre 25 números ou uma centena, os números naturais são organizados em ordem crescente. Como na imagem abaixo.

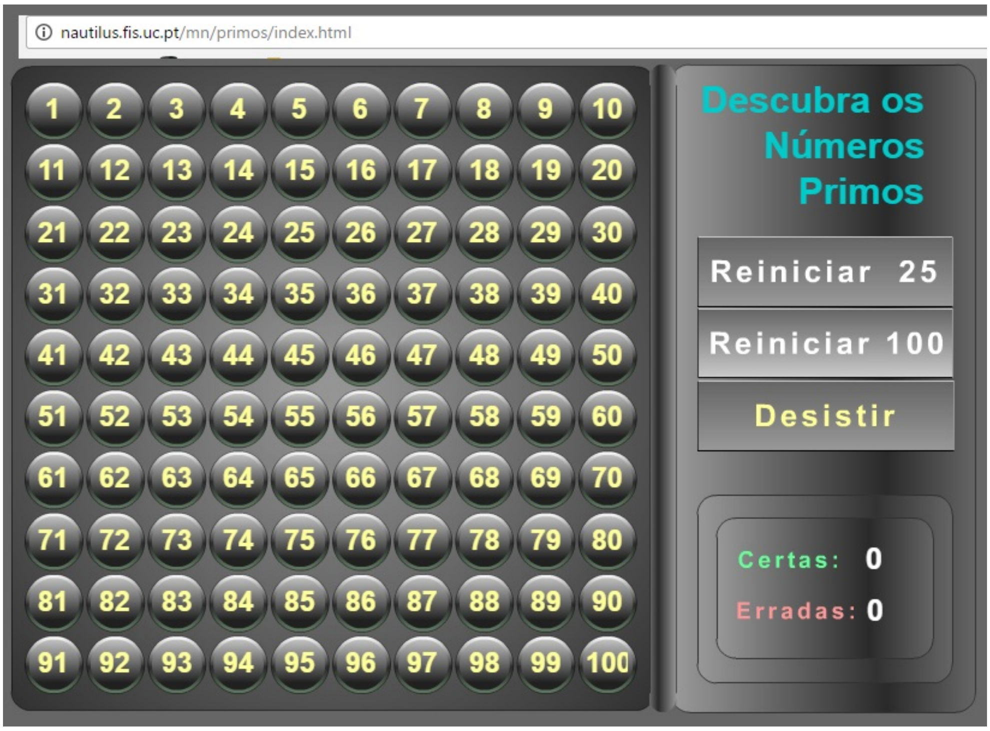


Figura 16: apresentação do jogo online

O objetivo do jogo é "clicar" em todos os números primos presentes na lista. Ao selecionar um número primo este é destacado de verde, ao selecionar um número não primo será destacado de vermelho. Ao marcar todos os números primos presentes na tela será informado a mensagem "GANHOU!!!"

A tela abaixo ilustra as respostas de um aluno do 6º ano que participou da atividade.

Figura 17: resposta de um aluno do 6º ano

Nessa atividade o entusiasmo dos alunos foi contagiante. Todos os alunos se envolveram, sempre tentando se superar. Frases como 49 está na tabuada do 7." ou 57 é múltiplo de 3" foram ouvidas durante a atividade sem a interferência do professor.

Atividade 6: Verificando Primalidade

Durante muito tempo, a aula expositiva foi o único procedimento empregado em sala de aula. Com o passar do tempo, no entanto, ela perdeu espaço na escola e até passou a ser malvista por muitos educadores, já que se tornou a representação de um ensino tradicional, que tem por base a transmissão do conhecimento, contudo, nem sempre é assim, se bem planejada e realizada, essa estratégia de ensino - em que o professor conduz os alunos por um raciocínio - pode ser o melhor meio de ensinar determinados conteúdos e garantir a aprendizagem.

Portanto, a aula expositiva é uma ótima ferramenta para se apresentar aos alunos o algoritmo para verificar a primalidade de um número.

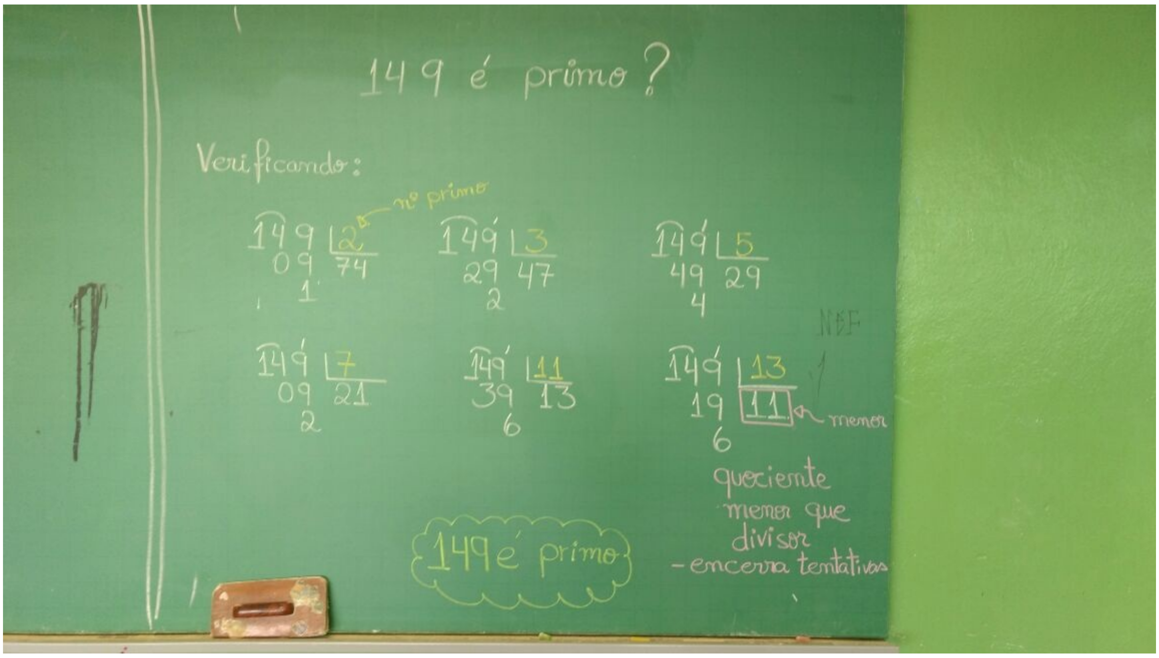


Figura 18: utilização da lousa para uma aula expositiva

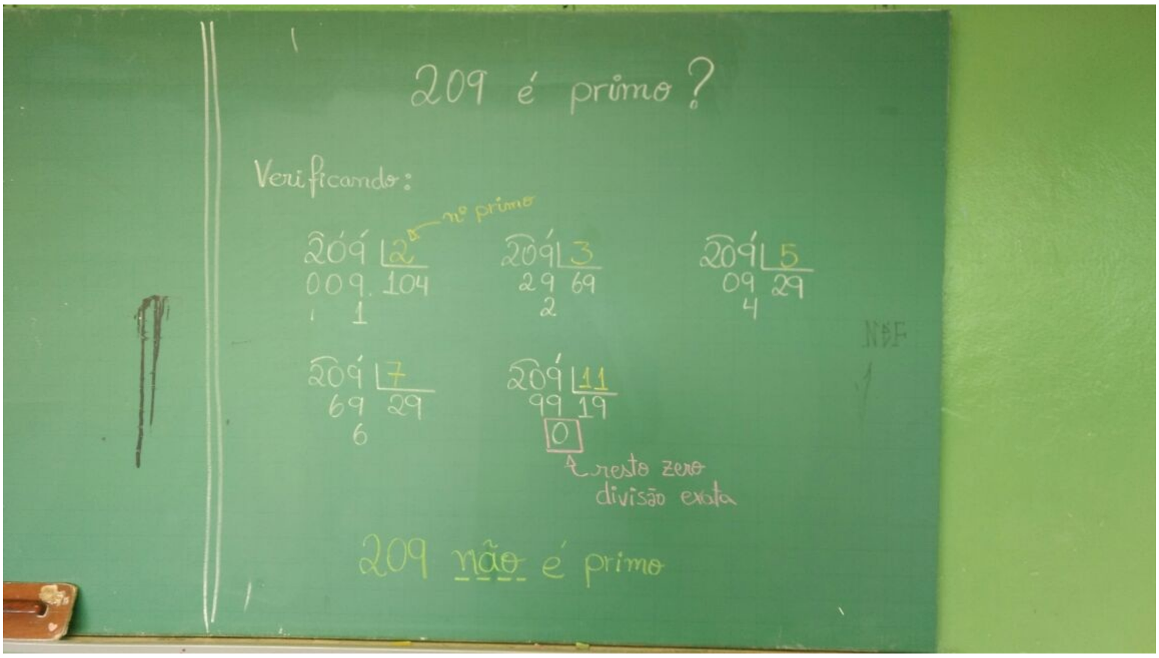


Figura 19: utilização da lousa para uma aula expositiva

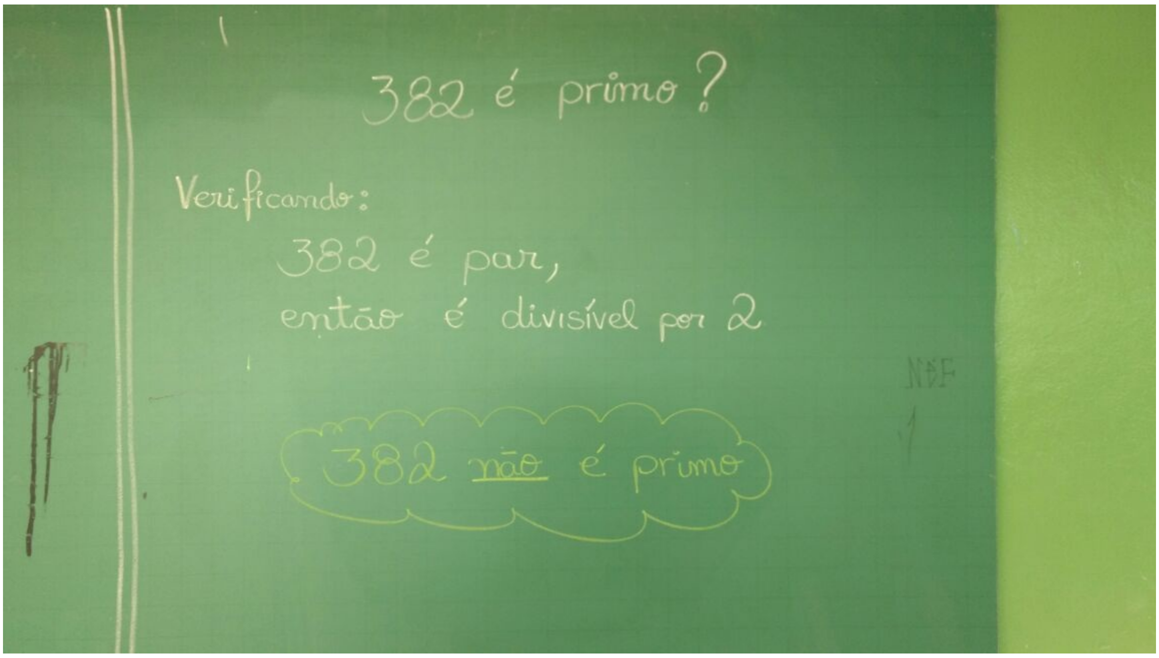


Figura 20: utilização da lousa para uma aula expositiva

Atividade aplicada com Alunos com Necessidades Especiais

A presença de alunos com necessidades especiais é uma realidade nas escolas, a adequação curricular é necessária para garantir a aprendizagem de todos. Por se tratar de uma atividade com atrativos visuais, essa é uma sugestão para desenvolver o reconhecimento dos números primos de uma aluno com idade cronológica divergente da idade intelectual.

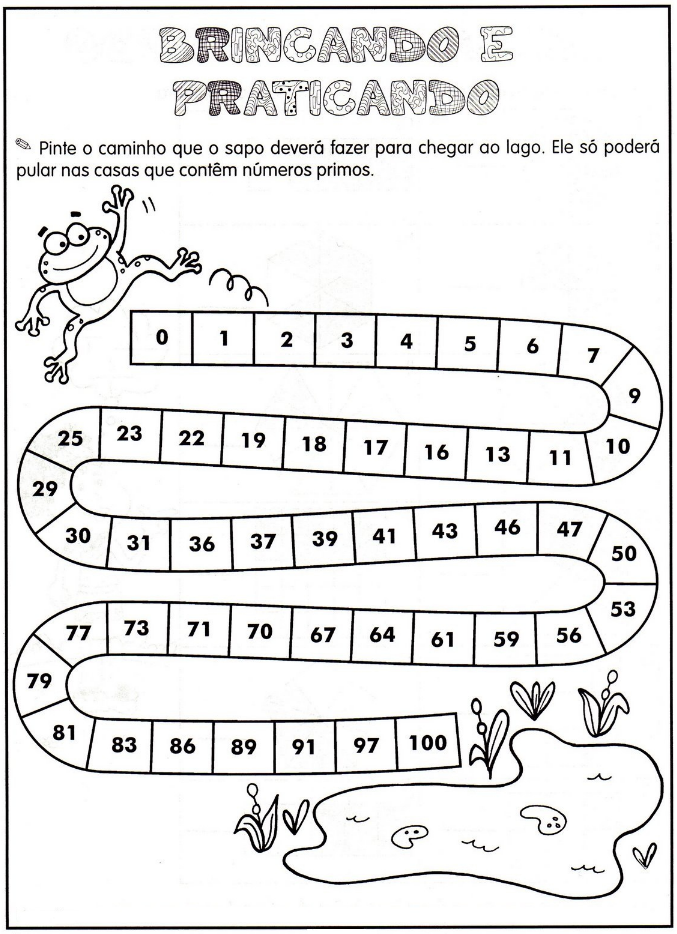


Figura 21: atividade proposta para uma aluna com necessidades especiais de aprendizagem

4.2.1 *Resultados*

A sequência didática foi aplicada em uma turma de 6º ano com 34 alunos, durante 12 aulas. Na aula subsequente foi aplicada uma avaliação.

Avaliação de Matemática

1. O que é número primo?

2. "O único número par e primo é o 2."

a) Essa afirmação é verdadeira ou falsa?

( ) verdadeira ( ) falsa

b) Justifique sua resposta.

3. Dentre os números abaixo, assinale os números primos.

4. O número 71 é um número primo? Justifique sua resposta.

5. O número 875 é um número primo? Justifique sua resposta.

Figura 22: Avaliação sobre números primos

Essa avaliação foi resolvida por 32 alunos. Onde todos os alunos obtiveram rendimento superior a 30% da avaliação, 27 alunos obtiveram rendimento superior a 50% e 6 alunos responderam corretamente todas as questões.

4.3 ATIVIDADES COMPLEMENTARES

Analisando documentos sobre o conteúdo programático de matemática para a educação básica notamos que o tópico Números Primos não é citado muitas vezes ao longo do curso, sendo mencionado apenas no 6º ano do Ensino Fundamental.

Pela experiência em sala de aula, acredita-se que a retomada cíclica do assunto possibilitaria a criação de novas oportunidades para os alunos se apropriarem do tema. Porém, é notório que o conteúdo programático já é extenso o suficiente, não sendo conveniente incluir novos tópicos a serem discutidos durante o curso. Portanto, a solução encontrada é agregar o tema Números Primos" em atividades que abordem outros conteúdos.

Algumas propostas de atividades com essas características serão apresentadas a seguir.

Atividade Complementar 1: Sistemas de Numeração

De acordo com o currículo do estado de São Paulo, durante o 1º bimestre do 7º ano do ensino fundamental, são requeridas as habilidades:

1. Sistema de numeração na antiguidade: Decodificar a estrutura lógica da escrita matemática.
2. Transpor as ideias relacionadas à base de um sistema de numeração para prática na computação (sistema binário).

A atividade a seguir é uma sugestão para aplicação dos números primos nesses contextos.

Sistemas de numeração

a) Escreva os números primos menores que 50, no sistema de numeração romana.

b) Escreva o menor número primo maior que 100, em algarismos egípcios.

c) Escreva o maior número primo menor que 100, no sistema binário de numeração.

Figura 23: Atividade sugerida

Sistemas de numeração

a) Escreva os números primos menores que 50, no sistema de numeração romana.

2 – II	11 – XI	23 – XXIII	41 – XLI
3 – III	13 – XIII	29 – XXIX	43 – XLIII
5 – V	17 – XVII	31 – XXXI	47 – XLVII
7 – VII	19 – XIX	37 – XXXVII	

b) Escreva o menor número primo maior que 100, em algarismos egípcios.

101

c) Escreva o maior número primo menor que 100, no sistema binário de numeração.

$$97_{(10)} = 0110\ 0001_{(2)}$$

Figura 24: Solução proposta para atividade

Atividade Complementar 2: Porcentagem

A importância e recorrência do tema porcentagem é notória tanto na matemática como na vida cotidiana.

Tema este que durante a educação básica é abordado diversas e diversificadas vezes. A proposta é uma atividade que apresente porcentagem para ser aplicada aos alunos do 7º ano, exigindo a capacidade de leitura de gráficos e análise estatística.

Porcentagem

a) Considerando os números naturais até 10, determine a porcentagem de números primos.

b) Considerando os números naturais até 100.
Analise o gráfico:

Quantos números primos menores que 100 existem?

Figura 25: Atividade sugerida

Porcentagem

a) Considerando os números naturais até 10, determine a porcentagem de números primos.

Números primos: 4

Total: 10

Razão: $\frac{4}{10}$

Decimal: 0,4

Porcentagem: **40%**

b) Considerando os números naturais até 100.

Analise o gráfico:

Quantos números primos menores que 100 existem?

Porcentagem de números primos: 25% (um quarto do total)

Total: 100

25% de 100 = 25.

Existem 25 números primos menores que 100.

Figura 26: Solução proposta para atividade

Atividade Complementar 3: Probabilidade

A atividade a seguir é sugerida para turmas do 9º ano do Ensino Fundamental, na qual é solicitada a abordagem da habilidade: *Identificar a razão que representa a probabilidade de um evento.*

Figura 27: Atividade sugerida

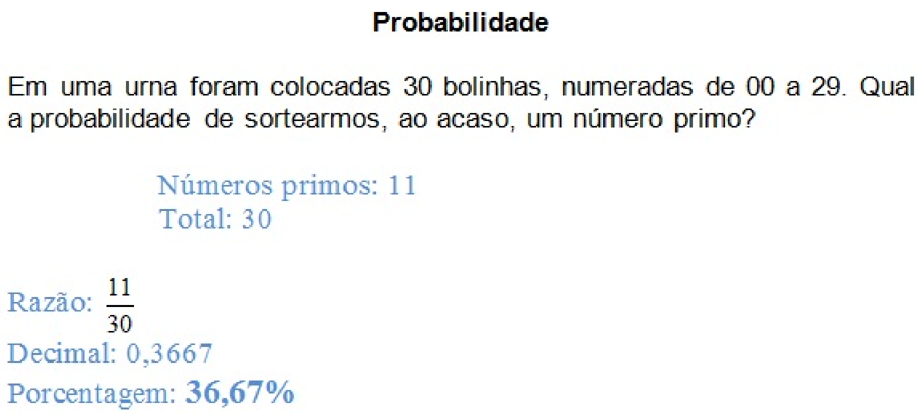


Figura 28: Solução proposta para atividade

Atividade Complementar 4: Charge

A capacidade de leitura é fundamental para a formação de um aluno, a interpretação de imagens relacionadas ao texto escrito é uma habilidade essencial para a construção de um bom leitor. Dessa maneira, a utilização de Charges torna-se interessante para aprimorar tais habilidades nos alunos.

Responda às questões:

a) A charge utiliza a palavra primos com duplo sentido. Quais são os dois significados possíveis para a palavra primos" no contexto acima?

b) Os números 3 e 7 são primos? Por quê?

c) A palavra dividir também é apresentada com duplo sentido. Quais são as interpretações possíveis para a frase Você nunca poderá nos dividir!"?

d) O número 0 pode dividir o número 3, em outras palavras, é possível fazer o cálculo $3 \div 0$? Justifique sua resposta.

Atividade Complementar 5: Teste de Wilson

Ao inserir o conteúdo Fatorial, no ensino médio, tradicionalmente é utilizado como forma de exercícios para treino do algoritmo de resolução comandos: calcule 5! ou determine o valor de 7!. Assim, utilizar o teste de Wilson pode ser atrativo e desafiador aos alunos e serão desenvolvidas diversas habilidades, bem como a revisão de conteúdos do ensino fundamental.

Enunciado da Atividade:

Teste de Wilson

O teste de Wilson é um teste para verificar se o número analisado é primo ou composto. Para isso calculamos o valor da expressão: $(p-1)!+1$

Se o resultado da expressão for múltiplo de p, então p é primo, caso contrário, p é composto.

Usando o teste de Wilson, verifique se os números abaixo são primos.

p	n = (p − 1)! + 1	$n \div p$	Divisão Exata?	Conclusão
3	n = (3 − 1)! + 1 n = 2! + 1 n = 2 . 1 + 1 n = 2 + 1 n = 3	$3 \div 3 = 1$	(x) sim ( ) não	(x) 3 é primo ( ) 3 é composto
4			( ) sim ( ) não	( ) 4 é primo ( ) 4 é composto
5			( ) sim ( ) não	( ) 5 é primo ( ) 5 é composto
8	n = (8 − 1)! + 1 n = 7! + 1 n = 7 . 6. 5. 3. 4. 3. 2 . 1 + 1 n = 5040 + 1 n = 5041	$5041 \div 8 = 630{,}125$	( ) sim (x) não	( ) 8 é primo (x) 8 é composto
12			( ) sim ( ) não	( ) 12 é primo ( ) 12 é composto
13			( ) sim ( ) não	( ) 13 é primo ( ) 13 é composto
15			( ) sim ( ) não	( ) 15 é primo ( ) 15 é composto

Figura 29: Atividade proposta

Atividade Complementar 6: Conjectura de Goldbach

Uma das habilidades requeridas na educação básica da matemática é a capacidade de abstrair, de imaginar situações fictícias, de projetar situações ainda não existentes.

> *As competências gerais, norteadoras [...] capacidade de argumentação, de construção de análises, justificativas de procedimentos,demonstrações etc.;[...]*
> [Currículo do estado de São Paulo - Matemática e suas tecnológias, p. 54]

A atividade a seguir explora essa habilidade, a proposta é solicitar aos alunos que respondam à atividade em forma de desafio, sem mencionar termos como “conjectura” ou “hipótese”, permitindo a descoberta de teorias e a discussão entre eles.

Números Primos: 02, 03, 05, 07, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, ...

Usando somente números primos, complete as igualdades para torna-las verdadeiras.

4 = ______ + ______	28 = ______ + ______
6 = ______ + ______	30 = ______ + ______
8 = ______ + ______	32 = ______ + ______
10 = ______ + ______	34 = ______ + ______
12 = ______ + ______	36 = ______ + ______
14 = ______ + ______	38 = ______ + ______
16 = ______ + ______	40 = ______ + ______
18 = ______ + ______	42 = ______ + ______
20 = ______ + ______	44 = ______ + ______
22 = ______ + ______	46 = ______ + ______
24 = ______ + ______	48 = ______ + ______
26 = ______ + ______	50 = ______ + ______

Em 1742, Christian Goldbach disse que todos os números pares maior que 2 pode ser escrito como a soma de dois números primos.
Você concorda com essa afirmação?

Figura 30: Atividade Investigativa: Conjectura de Goldbach

Sugerida para turmas do 9º ano do ensino fundamental, a primeira parte da atividade espera-se que os alunos desenvolvam com tranquilidade e observem a possibilidade de diferentes respostas corretas, por exemplo, $28 = 11 + 17$ ou $28 = 5 + 23$.

Na segunda parte da atividade os alunos terão a oportunidade de argumentar, sem dar uma resposta padrão.

Durante a aplicação da atividade algumas das observações dos alunos foram:

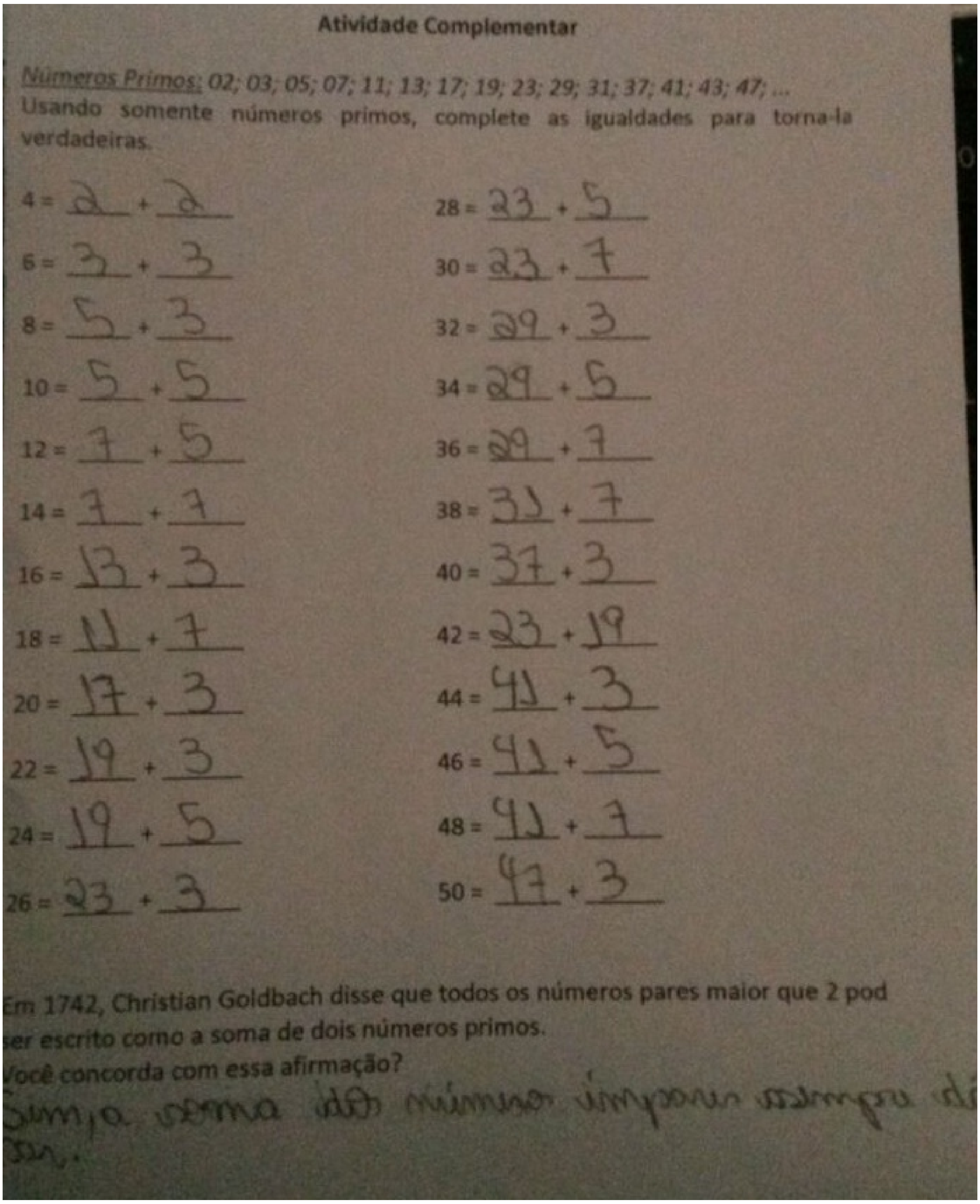
A- Eu acredito que a afirmação dele seja verdadeira pois se continuasse daí em diante daria certo. $52 = 47 + 5$ e $54 = 47 + 7$.

B- Os números primos são basicamente ímpar e ímpar + ímpar é par, então ele está certo.

C- Sim, todos os números são infinitos, os números pares são infinitos, os números primos são infinitos.

D- Não. Porque os números pares são infinitos e vai ser difícil de encontrar os números primos para dar um número par muito grande.

Para finalizar e concluir a atividade, é interessante mostrar que, apesar de terem apresentado teorias, nenhuma delas realmente justifica matematicamente a Conjectura de Goldbach, aproveitando o momento para mostrar a necessidade de generalizações na matemática.



Atividade Complementar

Números Primos: 02; 03; 05; 07; 11; 13; 17; 19; 23; 29; 31; 37; 41; 43; 47; ...
Usando somente números primos, complete as igualdades para torna-la verdadeiras.

4 = 2 + 2
6 = 3 + 3
8 = 5 + 3
10 = 5 + 5
12 = 7 + 5
14 = 7 + 7
16 = 13 + 3
18 = 11 + 7
20 = 17 + 3
22 = 19 + 3
24 = 19 + 5
26 = 23 + 3

28 = 23 + 5
30 = 23 + 7
32 = 29 + 3
34 = 29 + 5
36 = 29 + 7
38 = 31 + 7
40 = 37 + 3
42 = 23 + 19
44 = 41 + 3
46 = 41 + 5
48 = 41 + 7
50 = 47 + 3

Em 1742, Christian Goldbach disse que todos os números pares maior que 2 pod
ser escrito como a soma de dois números primos.
Você concorda com essa afirmação?
Sim, a soma dos números impares sempre dá par.

Figura 31: Atividade realizada por um aluno do 9º ano do Ensino Fundamental

CONSIDERAÇÕES FINAIS

Este trabalho teve como principal objetivo a ampliação dos conhecimentos sobre números primos e a conjectura de Goldbach.

No desenvolvimento do trabalho notamos que os conhecimentos sobre os números primos foram agregados durante séculos, com citações na Grécia Antiga e, ainda, com possibilidades de novos resultados e/ou aplicações desses números.

No trabalho, conhecemos algumas das propriedades dos números primos e analisamos alguns teoremas que dão embasamento à teoria dos números. Concordando com Gauss, que disse:

> *"O problema de distinguir números primos de números compostos e decompor os compostos em fatores primos é o conhecimento mais importante e útil na aritmética."*
>
> (Carl Friedrich Gauss)

Também estudamos a conjectura de Goldbach,a partir da qual verificamos que, apesar de ainda não demonstrada foi inspiração para se concluir importantes resultados. Vimos uma abordagem empírica do problema, que se verificou a conjectura para quadrilhões de valores, porém, Karl Popper tem uma analogia interessante para essa situação.

> *"Não importa quantos cisnes brancos você veja ao longo da vida; isso nunca dará certeza de que cisnes negros não existam."*
>
> (Karl Popper)

Por compreendermos que o conhecimento só é útil se compartilhado e por concordarmos com a professora Irene de Albuquerque, que diz:

> *"Um bom ensino da matemática, forma melhores hábitos de pensamentos e habilita o indivíduo a usar melhor a sua inteligência."*
>
> (Irene de Albuquerque)

Sendo assim, vimos uma sequência didática para o ensino dos números primos e sugestões de atividades que aprimoram os conhecimentos sobre o tema ao longo do ensino básico, enfatizando a citação de John Young.

> *"É claro que a principal finalidade do estudo da Matemática deve ser a de fazer os alunos pensarem."*
>
> (John Young)

BIBLIOGRAFIA

[1] ANDRINI Álvaro e M. J. VASCONCELLOS: *Praticando Matemática*. Editora do Brasil, 2014.

[2] BOYER, C. B.: *Historia da matemática*. São Paulo: Blucher, 2012.

[3] BRASIL: *PCN, Parâmetros Curriculares Nacionais - Matemática*. Secretária de Educação Fundamental. Brasília: MEC / SEF, 1998.

[4] CHAVANTE, E.: *Matemática*. SM, 2015.

[5] CRANDALL, R. e C. POMERANCE: *Prime Numbers: a Computacional Perspective*. Springer Science, 2006.

[6] DANTE, L. R.: *Tudo é Matemática*. Ática, 2008.

[7] DOXIADIS, A.: *Tio Petros e conjectura de Goldbach*. Editora 34, 2001.

[8] EVES, H. W.: *Introdução à história da matemática*. Unicamp, 1995.

[9] FINI, M. I. e outros: *Proposta curricular do Estado de São Paulo*. São Paulo, 2008.

[10] GARIBALDI, E.: *Aproximações ao Problema de Goldbach*. Matemática Universitária, (34):19–33, 2003.

[11] HEFEZ, A.: *Coleção PROFMAT: Aritmética*. SBM, 2016.

[12] HELFGOTT, H. A.: *Major arcs for Goldbachs problem*. arXiv preprint arXiv: 1305.2897.

[13] RICHSTEIN, J.: *Verificando a conjectura de Goldbach até* $4 \cdot 10^{14}$. Matemática de computação, 70(236):1745–1749, 2001.

[14] RODRIGUES, M.: *O desenvolvimento do pré-escolar e o jogo*. São Paulo: Ícone, 1992.

[15] SANTOS, J. P. O.: *Introdução à Teoria dos números*. Instituto de Matemática Pura e Aplicada, 1998.

[16] SAUTOY, M. D.: *A música dos números primos: a história de um problema não resolvido na matemática*. Zahar, 2007.

[17] SAUTOY, M. D.: *Os mistérios dos números: Uma viagem pelos grandes enigmas da matemática*. Zahar, 2013.

[18] SHOKRANIAN, S.: *Uma introdução à Teoria dos números*. Ciência Moderna, 2008.

[19] STAHL, M. M.: *Ambientes de ensino-aprendizagem computadorizados: da sala de aula convencional ao mundo da fantasia*. Rio de Janeiro: COPPE-UFRJ, 1991.

[20] TEZANI, T. C. R.: *O Jogo e Os Processos de Aprendizagem e Desenvolvimento: aspectos cognitivos e afetivos*. Educação em Revista, 7(1-2):1–16, 2006.

[21] VIANA, M. C. V. e C. M. SILVA: *Concepções de Professores de Matemática sobre a utilização da História da Matemática no processo de Ensino-Aprendizagem*. Encontro Nacional De História Da Matemática, Belo Horizonte. BH, 2007.

[22] WANG, Y.: *The Goldbach Conjecture*, vol. 4. World scientific, 2002.