

UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ

DENISE JANKOSKI

**CONJUNTOS NUMÉRICOS INSTIGANTES: PROPOSTAS DE ATIVIDADES PARA
DESENVOLVER O PENSAMENTO COMPUTACIONAL NA EDUCAÇÃO BÁSICA**

CURITIBA

2025

DENISE JANKOSKI

**CONJUNTOS NUMÉRICOS INSTIGANTES: PROPOSTAS DE ATIVIDADES PARA
DESENVOLVER O PENSAMENTO COMPUTACIONAL NA EDUCAÇÃO BÁSICA**

**Intriguing numerical sets: proposed activities to develop computational thinking in
Elementary Education**

Dissertação apresentada como requisito para obtenção do título de Mestra em Matemática, Área de Concentração: Matemática na Educação Básica, no Programa Mestrado Profissional em Matemática em Rede Nacional - PROFMAT da Universidade Tecnológica Federal do Paraná - UTFPR.

Linha de pesquisa: Matemática na Educação Básica e suas Tecnologias.

Orientador: Prof. Dr. Rudimar Luiz Nós.

Coorientadora: Profa. Dra. Olga Harumi Saito.

CURITIBA

2025



[4.0 Internacional](https://creativecommons.org/licenses/by-nc-sa/4.0/)

Esta licença permite que outros remixem, adaptem e criem a partir do trabalho licenciado para fins não comerciais, desde que atribuam ao autor o devido crédito e que licenciem as novas criações sob termos idênticos.



**Ministério da Educação
Universidade Tecnológica Federal do Paraná
Campus Curitiba**



DENISE JANKOSKI

CONJUNTOS NUMÉRICOS INSTIGANTES: PROPOSTAS DE ATIVIDADES PARA DESENVOLVER O PENSAMENTO COMPUTACIONAL NA EDUCAÇÃO BÁSICA

Trabalho de pesquisa de mestrado apresentado como requisito para obtenção do título de Mestre Em Matemática da Universidade Tecnológica Federal do Paraná (UTFPR). Área de concentração: Matemática Na Educação Básica.

Data de aprovação: 12 de Maio de 2025

Dr. Rudimar Luiz Nos, Doutorado - Universidade Tecnológica Federal do Paraná

Dra. Gisele Teixeira Paula, Doutorado - Universidade Federal do Paraná (Ufpr)

Dra. Mari Sano, Doutorado - Universidade Tecnológica Federal do Paraná

Documento gerado pelo Sistema Acadêmico da UTFPR a partir dos dados da Ata de Defesa em 12/05/2025.

Dedico este trabalho a Deus, pela força e sabedoria concedidas ao longo desta jornada, e aos meus pais pelo incentivo e apoio aos meus estudos.

AGRADECIMENTOS

A Deus e a Nossa Senhora Aparecida, a quem recorri em muitos momentos de aflição e que me concederam força durante todo esse percurso.

Aos meus pais, Ozilda e Laurindo, pelo apoio e dedicação incondicional que sempre me proporcionaram. Desde os primeiros passos na educação até este momento culminante da minha vida acadêmica, sempre estiveram ao meu lado, oferecendo palavras de encorajamento, sabedoria e, acima de tudo, um exemplo inspirador de integridade e perseverança.

Aos meus amigos, em especial a Kellen Laureano Soares, Maria Liria Chaves Schicovski e Wilma Granza Madureira, que estiveram presentes nos momentos mais difíceis e delicados, oferecendo não apenas sua companhia, mas também suas palavras de incentivo e compreensão. Suas conversas e conselhos foram fundamentais.

Às minhas colegas e amigas, Adrieli Muchau Kosinski e Caroline Witt Guerber, pelo companheirismo ao longo desses dois anos.

Ao meu orientador, Prof. Dr. Rudimar Luiz Nós, e à minha coorientadora, Profa. Dra. Olga Harumi Saito, cuja paciência e sabedoria foram essenciais para a realização deste projeto.

À Sociedade Brasileira de Matemática que, na busca da melhoria do ensino de matemática na Educação Básica, viabilizou a implementação do PROFMAT.

À CAPES, pela recomendação do PROFMAT por meio do parecer do Conselho Técnico Científico da Educação Superior.

O presente trabalho foi realizado com apoio da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - Brasil (CAPES) - Código de Financiamento 001.

Sonhos determinam o que você quer. Ação determina o que você conquista. Aldo Novak (1962–), jornalista, coach, palestrante e escritor brasileiro.

RESUMO

JANKOSKI, Denise. **Conjuntos numéricos instigantes: propostas de atividades para desenvolver o pensamento computacional na Educação Básica**. 190 f. Dissertação - Programa de Mestrado Profissional em Matemática em Rede Nacional - PROFMAT, Universidade Tecnológica Federal do Paraná. Curitiba, 2025.

Este trabalho apresenta atividades abrangendo conjuntos numéricos instigantes, empregados como ferramenta pedagógica para desenvolver o pensamento computacional de acordo com as competências gerais e específicas delineadas na Base Nacional Comum Curricular (BNCC) para o Ensino de Matemática. Com base em uma estrutura bem fundamentada que inclui divisibilidade, números primos, números perfeitos e números amigáveis, investigamos conceitos matemáticos por meio de teoremas, conjecturas e padrões numéricos, estabelecendo conexões entre teoria e prática. Organizamos atividades que estimulam a resolução de problemas e a compreensão de conceitos relacionados aos conjuntos abordados, usando recursos tecnológicos como o soroban digital, o GeoGebra e o GNU Octave. Neste contexto, propomos sequências didáticas detalhadas e alinhadas com a BNCC, com o objetivo de auxiliar os(as) professores(as) de matemática da Educação Básica a conduzir as aulas de forma eficaz e engajadora. As atividades são contextualizadas e desafiadoras, estimulando o raciocínio lógico e a criatividade, além de aprimorar as habilidades de pensamento computacional. As tecnologias digitais utilizadas não apenas permitem explorar a beleza e a complexidade dos conjuntos numéricos selecionados, mas também destacam sua relevância para a evolução da curiosidade científica dos estudantes, preparando-os para desafios futuros.

Palavras-chave: números primos; números perfeitos; números amigáveis; soroban digital; GeoGebra; GNU Octave.

ABSTRACT

JANKOSKI, Denise. **Intriguing numerical sets: proposed activities to develop computational thinking in Elementary Education**. 190 pg. Dissertation - Programa de Mestrado Profissional em Matemática em Rede Nacional - PROFMAT, Universidade Tecnológica Federal do Paraná. Curitiba, 2025.

This work presents activities encompassing intriguing numerical sets, a pedagogical tool to develop computational thinking according to the general and specific competencies outlined in the National Common Curricular Base (BNCC) for Mathematics Education. Based on a well-founded structure that includes divisibility, prime numbers, perfect numbers, and amicable numbers, we investigate mathematical concepts through theorems, conjectures, and numerical patterns, establishing connections between theory and practice. We organize activities that stimulate problem-solving and understanding of concepts related to the addressed sets, using technological resources such as the digital soroban, GeoGebra, and GNU Octave. In this context, we propose detailed didactic sequences aligned with the BNCC, aiming to assist mathematics teachers in Basic Education conducting classes effectively and engagingly. The activities are contextualized and challenging, encouraging logical reasoning and creativity and enhancing computational thinking skills. The digital technologies used not only allow for exploring the beauty and complexity of the selected numerical sets but also highlight their relevance to the evolution of students' scientific curiosity, preparing them for future challenges.

Keywords: prime numbers; perfect numbers; amicable numbers; digital soroban; GeoGebra; GNU Octave.

LISTA DE FIGURAS

Figura 1.1 – Tirinha sobre números perfeitos	19
Figura 1.2 – Charge sobre números amigáveis	20
Figura 2.1 – Soroban	40
Figura 2.2 – Representação do número 567 no soroban	41
Figura 2.3 – Desenvolvimento do cálculo de $12 + 21$ no soroban: (a) representação do número 12; (b) adicionando 2 às dezenas; (c) adicionando 1 às unidades . .	41
Figura 2.4 – Desenvolvimento do cálculo de $31 + 11$ no soroban: (a) representação do número 31; (b) adicionando 1 às dezenas; (c) adicionando 1 às unidades . .	42
Figura 2.5 – Desenvolvimento do cálculo de $32 + 14$ no soroban: (a) representação do número 32; (b) adicionando 1 às dezenas; (c) adicionando 4 às unidades . .	43
Figura 2.6 – Desenvolvimento do cálculo de $418 + 183$ no soroban: (a) representação do número 418; (b) adicionando 1 às centenas; (c) adicionando 8 às dezenas; (d) adicionando 3 às unidades	44
Figura 2.7 – Termos da divisão	45
Figura 2.8 – Representação do número 312 no soroban	46
Figura 2.9 – Representação da divisão de 3 (centenas) por 2 no soroban	46
Figura 2.10–Representação da divisão de 11 (dezenas) por 2 no soroban	47
Figura 2.11–Quociente 156: resultado final da divisão $312 \div 2$	47
Figura 2.12–Representação do número 735 no soroban	47
Figura 2.13–Representação da divisão de 7 (centenas) por 5 no soroban	48
Figura 2.14–Representação da divisão de 23 por 5 no soroban	48
Figura 2.15–Quociente 147: resultado final da divisão $735 \div 5$	49
Figura 2.16–Representação do número 254 no soroban	49
Figura 2.17–Representação da divisão de 25 por 3 no soroban	50
Figura 2.18–Representação da divisão de 14 por 3 no soroban	50
Figura 3.1 – Sistema retangular de coordenadas	62
Figura 3.2 – Matemáticos que estudaram os números primos	65
Figura 3.3 – Frequência dos números primos: (a) intervalo de 0 a 100; (b) intervalo de 0 a 1000	67
Figura 3.4 – Números palíndromos ou capicua	71
Figura 3.5 – Números primos palíndromos	71
Figura 3.6 – Pirâmide de números primos palíndromos começando em 2 e com altura 5 .	72
Figura 3.7 – Pirâmides de primos palíndromos	72
Figura 3.8 – Números primos reversos	73
Figura 3.9 – <i>Emirp</i> cíclico	73
Figura 3.10–Quadrados de <i>emirps</i>	73

Figura 3.11–Distribuição dos primos gêmeos, primos primos e primos <i>sexy</i> até 70	75
Figura 3.12–Criptografia com chave assimétrica	79
Figura 3.13–Reta crítica da hipótese de Riemann	86
Figura 4.1 – Matemáticos que estudaram os números perfeitos: Euclides de Alexandria, René Descartes, Leonhard Euler e James Joseph Sylvester	89
Figura 4.2 – Computador SWAC	89
Figura 4.3 – Números triangulares	108
Figura 4.4 – Números hexagonais	108
Figura 5.1 – Capa <i>Nova Acta Eruditorum</i> - 1747	115
Figura 5.2 – Pares de números amigáveis menores que 20.000.000	117
Figura 5.3 – Números amigos quadráticos	128
Figura 6.1 – Números triangulares: (a) $T = 10$; (b) $T = 15$; (c) $T = 28$; (d) $T = 55$. . .	131
Figura 6.2 – Número triangular para $n = 6$	132
Figura 6.3 – Script para calcular números triangulares entre 100 e 200	132
Figura 6.4 – Números triangulares entre 100 e 200	133
Figura 6.5 – Script para calcular o número triangular para $n = 20$	133
Figura 6.6 – Número triangular para $n = 20$	134
Figura 6.7 – Script para verificar se T é um número triangular	135
Figura 6.8 – Verificação de números triangulares	135
Figura 6.9 – Números quadrangulares	136
Figura 6.10–Números pentagonais	136
Figura 6.11–Números hexagonais	137
Figura 6.12–Espaço para decodificação da frase	139
Figura 6.13–Fatoração dos números da sequência fornecida	140
Figura 6.14–Frase decodificada	140
Figura 6.15–Caça-palavras sobre números perfeitos	144
Figura 6.16–Script para a soma dos algarismos do número 496	144
Figura 6.17–Script para calcular a diferença entre 496 e 28	145
Figura 6.18–Script para obter os divisores do número 8128	145
Figura 6.19–Script para obter o resultado de 6 elevado ao quadrado	146
Figura 6.20–Script para obter a fração irredutível entre o segundo e o primeiro números perfeitos	147
Figura 6.21–Script para calcular a porcentagem que o divisor 7 representa do número perfeito 28	147
Figura 6.22–Script para calcular a parte inteira da raiz quadrada de 8128	148
Figura 6.23–Script para calcular a média aritmética aproximada dos três primeiros núme- ros perfeitos	149
Figura 6.24–Script para determinar a mediana dos divisores próprios do número perfeito 6	149
Figura 6.25–Script para calcular o valor numérico da expressão com números perfeitos .	150

Figura 6.26–Respostas do Desafio 6.9 no caça-palavras	150
Figura 6.27–Progressões aritméticas com 20 termos: (a) $a_n = 2 + (n - 1) \cdot 3$; (b) $a_n = 3 + (n - 1) \cdot 2$; (c) $a_n = 4 + (n - 1) \cdot 7$; (d) $a_n = 7 + (n - 1) \cdot 3$; (e) $a_n = 11 + (n - 1) \cdot 2$	153
Figura 6.28–Primalidade dos 20 primeiros termos da PA $a_n = 2 + (n - 1) \cdot 3$	154
Figura 6.29–Primalidade dos 20 primeiros termos da PA $a_n = 3 + (n - 1) \cdot 2$	154
Figura 6.30–Primalidade dos 20 primeiros termos da PA $a_n = 4 + (n - 1) \cdot 7$	155
Figura 6.31–Primalidade dos 20 primeiros termos da PA $a_n = 7 + (n - 1) \cdot 3$	155
Figura 6.32–Primalidade dos 20 primeiros termos da PA $a_n = 2 + (n - 1) \cdot 3$	156
Figura 6.33–Porcentagem de números primos nos 20 primeiros termos das progressões aritméticas do Desafio 6.10	156
Figura 6.34–PA $a_n = 2 + (n - 1) \cdot 3$: (a) 25 primeiros termos; (b) 30 primeiros termos	157
Figura 6.35–Primalidade dos 25 primeiros termos da PA $a_n = 2 + (n - 1) \cdot 3$	157
Figura 6.36–Primalidade dos 30 primeiros termos da PA $a_n = 2 + (n - 1) \cdot 3$	158
Figura 6.37–Porcentagem de números primos nos 25 e 30 primeiros termos da PA $a_n = 2 + (n - 1) \cdot 3$	158
Figura 6.38–Progressão aritmética $a_n = 3 + (n - 1) \cdot 2$: (a) 25 primeiros termos; (b) 30 primeiros termos	159
Figura 6.39–Primalidade dos 25 primeiros termos da PA $a_n = 3 + (n - 1) \cdot 2$	159
Figura 6.40–Primalidade dos 30 primeiros termos da PA $a_n = 3 + (n - 1) \cdot 2$	160
Figura 6.41–Porcentagem de números primos nos 25 e 30 primeiros termos da PA $a_n = 3 + (n - 1) \cdot 2$	160
Figura 6.42–Progressões aritméticas com um único número primo: (a) $a_n = 2 + (n - 1) \cdot 2$, $n > 1$; (b) $a_n = 5 + (n - 1) \cdot 10$, $n > 1$	161
Figura 6.43–Script para somar os divisores próprios de 6 a 1184 na Tabela 6.2	164
Figura 6.44–Script para somar os divisores próprios de 1210 a 5564 na Tabela 6.2	164
Figura 6.45–Script para somar os divisores próprios de 5847 a 6368 na Tabela 6.2	165
Figura 6.46–Solução do Desafio 6.13 no soroban: o número misterioso é 195	169
Figura 6.47–Algarismo das unidades do número misterioso no Desafio 6.14	170
Figura 6.48–Solução do Desafio 6.14 no soroban: o número misterioso é 9564	171
Figura 6.49–Algarismo das dezenas de milhar do número misterioso no Desafio 6.15	172
Figura 6.50–Algarismo das dezenas do número misterioso no Desafio 6.15	173
Figura 6.51–Solução do Desafio 6.15 no soroban: o número misterioso é 39270	173
Figura 6.52–Algarismo das unidades do número misterioso no Desafio 6.16	175
Figura 6.53–Solução do Desafio 6.16 no soroban: o número misterioso é 123456	176

LISTA DE TABELAS

Tabela 2.1 – Paridade da soma e do produto de dois números inteiros	39
Tabela 3.1 – Sequências aritméticas com os 10 primeiros termos primos	60
Tabela 3.2 – Vinte maiores primos gêmeos já encontrados	69
Tabela 3.3 – Tabela para pré-codificação	79
Tabela 4.1 – Dez maiores números perfeitos	90
Tabela 4.2 – Números k -hiperperfeitos para diferentes valores de k	100
Tabela 4.3 – Relação entre números ciclopes e números perfeitos	112
Tabela 6.1 – Tabela para descobrir a mensagem secreta	139
Tabela 6.2 – Lista de números para o Desafio 6.12	163
Tabela 6.3 – Pares de números amigáveis do Desafio 6.12	165

LISTA DE ABREVIATURAS E SIGLAS

BNCC	Base Nacional Comum Curricular
CAPES	Coordenação de Aperfeiçoamento de Pessoal de Nível Superior
GIMPS	Great Internet Mersenne Prime Search
HI	Hipótese de Indução
OBMEP	Olimpíada Brasileira de Matemática das Escolas Públicas
PA	Progressão Aritmética
PNE	Plano Nacional de Educação
PROFMAT	Mestrado Profissional em Matemática em Rede Nacional
RSA	Rivest Shamir Adleman
SBM	Sociedade Brasileira de Matemática
SWAC	Standards Western Automatic Computer
TFA	Teorema Fundamental da Aritmética
UTFPR	Universidade Tecnológica Federal do Paraná

LISTA DE SÍMBOLOS

$a \mid b$	a divide b
$a \nmid b$	a não divide b
$ a $	Módulo de a
$\exists$	Existe
$\in$	Pertence
$\cup$	União
$\forall$	Para todo
$\leq$	Menor ou igual do que
$\geq$	Maior ou igual do que
$\neq$	Diferente de
$\Rightarrow$	Implica
$\Leftrightarrow$	Equivalente a
Σ	Somatório
$a \equiv b \pmod{m}$	a congruente a b módulo m
$(p, a) = 1$	Máximo divisor comum entre p e a é igual a 1
$\mathbb{N}$	Conjunto dos números naturais
$\mathbb{Z}$	Conjunto dos números inteiros
ζ	Função zeta
σ, s ou f	Soma dos divisores positivos de $n \in \mathbb{N}$

SUMÁRIO

1	INTRODUÇÃO	17
1.1	Justificativa para a escolha do tema	21
1.2	Revisão da bibliografia	22
1.3	Objetivos	23
1.3.1	Objetivo geral	23
1.3.2	Objetivos específicos	23
1.4	Procedimentos metodológicos	24
1.5	Recurso Educacional	25
1.6	Estrutura do trabalho	25
2	DIVISIBILIDADE	27
2.1	Definição e propriedades	27
2.2	CrITÉRIOS de divisibilidade	31
2.3	Paridade	36
2.4	A divisibilidade no soroban	39
2.4.1	Simple soroban	51
3	NÚMEROS PRIMOS	53
3.1	Teorema fundamental da aritmética	55
3.2	Teorema de Dirichlet: primos em progressão aritmética	57
3.3	Teorema de ouro	61
3.4	Conjecturas	64
3.4.1	Distribuição dos números primos	65
3.4.2	Primos gêmeos	68
3.4.3	Primos palíndromos e primos reversos	70
3.5	Primos gêmeos, primos primos e primos sexy	74
3.6	Padrões numéricos e aplicações	76
3.6.1	Quem quer ser milionário?	83
3.6.2	A hipótese de Riemann	84
4	NÚMEROS PERFEITOS	88
4.1	Teorema de Euclides-Euler	90
4.2	Paridade	94
4.2.1	Número perfeito ímpar	96
4.2.2	Números hiperperfeitos	98
4.3	Outros teoremas	102

4.4	Padrões numéricos e aplicações	106
4.4.1	Números geométricos	107
4.4.2	Números ciclopes	109
5	NÚMEROS AMIGÁVEIS	113
5.1	Contribuições de Euler	115
5.2	Teoremas	118
5.3	Padrões numéricos e aplicações	124
5.3.1	Números mutuamente amigos e amigos quadráticos	126
6	RECURSO EDUCACIONAL: ATIVIDADES PARA A EDUCAÇÃO BÁSICA	129
6.1	Atividade 1: Explorando os números poligonais	129
6.2	Atividade 2: Decifrando mensagens secretas com números primos	137
6.3	Atividade 3: Rastreando números perfeitos	140
6.4	Atividade 4: Investigando números primos em progressões aritméticas	151
6.5	Atividade 5: Descobrimos os pares amigáveis	161
6.6	Atividade 6: Desvendando mistérios numéricos com o soroban e o GNU Octave	166
7	CONCLUSÃO	178
	REFERÊNCIAS	180
	Índice	189

1 INTRODUÇÃO

A Matemática, presente em todas as esferas da vida, revela-se como uma linguagem universal que molda nossa compreensão do mundo. Dentre seus diversos ramos, a Teoria dos Números, com sua elegância e complexidade, desperta a curiosidade de matemáticos e entusiastas há milênios. A busca por padrões, relações e propriedades numéricas tem impulsionado o desenvolvimento de diversas áreas do conhecimento.

De acordo com Martinez *et al.* (2013, prefácio):

Assim, é de certa forma surpreendente que a Teoria dos Números seja atualmente uma das áreas de pesquisa mais efervescentes da Matemática e que, mais do que nunca, continue a fascinar e desafiar as atuais gerações de matemáticos. Diferentemente de muitas outras áreas da Matemática, a Teoria dos Números se distingue muito menos por seus métodos mas mais sim por seus problemas, cujo tema comum subjacente é o de número inteiro.

[...] enquanto um analista utiliza-se de métodos analíticos para resolver seus problemas e um algebrista empregue métodos algébricos para atacar questões algébricas, em Teoria dos Números um mesmo problema pode requerer para a sua solução a utilização simultânea de métodos algébricos, analíticos, topológicos, geométricos e combinatórios, além de uma boa dose de imaginação! Talvez seja este aspecto multidisciplinar, aliado à simplicidade de seus conceitos e ao caráter fundamental, que torna a Teoria dos Números um dos ramos mais populares em toda a Matemática, cativando pessoas de formação totalmente diversas.

Na vastidão do universo dos números, descobrimos que eles não estão sozinhos. Castro (2020, n.p), em seu site Mapa de Mileto, destaca que: “Tal como nós imitamos as habilidades de multiplicar e dividir dos números, também eles se assemelharam a nós na capacidade de formar família. A simetria me faz questionar: Seriam os números humanos ou, como acreditou Pitágoras, nós é que somos números?”

Os números, assim como os membros de uma família, possuem características individuais e histórias que os tornam únicos. Enquanto alguns são conhecidos por sua solidão entre os números primos, outros formam laços estreitos com uma gama diversa de parentes matemáticos. Compreender essas relações não apenas enriquece nosso entendimento sobre os números, mas também nos permite explorar aplicações práticas em diversas áreas.

Portanto, ao adentrar no universo dos números, é crucial reconhecer que, assim como nós, eles têm parentes que moldam suas identidades e influenciam suas interações no vasto campo da Matemática. Explorar essas conexões nos revela um panorama rico e dinâmico, onde cada número tem seu lugar na complexa árvore genealógica matemática.

Neste contexto, o presente trabalho tem como objetivo aprofundar a investigação de alguns conjuntos numéricos particulares presentes na Teoria dos Números – primos, perfei-

tos e amigáveis, e explorar seu potencial para estimular o desenvolvimento do pensamento computacional na Educação Básica.

Conforme salienta a Base Nacional Comum Curricular – BNCC (Brasil, 2018), o desenvolvimento do pensamento computacional está profundamente ligado à construção de habilidades matemáticas, como o raciocínio lógico, a resolução de problemas, a abstração, a análise de dados e a modelagem matemática. Ao estimular o desenvolvimento dessas habilidades, o pensamento computacional auxilia os estudantes a se tornarem aprendizes mais autônomos e críticos.

O pensamento computacional, entendido como a habilidade de resolver problemas de forma sistemática e eficiente, utilizando conceitos da computação, tem ganhado cada vez mais reconhecimento e valorização em um mundo cada vez mais digital. A Teoria dos Números, por sua vez, oferece um rico terreno para o desenvolvimento dessas habilidades, uma vez que exige a formulação de algoritmos, a análise de dados e a construção de modelos abstratos.

Já o estudo dos números primos, perfeitos e amigáveis justifica-se por diversos motivos. Os números primos, definidos por Sautoy (2013, p. 163) como os “átomos da aritmética”, são os números a partir dos quais todos os números naturais podem ser construídos através da multiplicação. A distribuição dos números primos entre os números naturais é um problema que tem desafiado matemáticos há séculos e continua sendo um tema de pesquisa ativa. Os números perfeitos e amigáveis, por sua vez, representam uma classe especial de números que satisfazem propriedades de divisibilidade particulares. A busca por novos exemplos desses números e a investigação de suas propriedades têm sido objeto de estudo desde a antiguidade.

A divisibilidade e a paridade, juntamente com os números primos, constituem a base para a compreensão de muitos conceitos matemáticos. Os critérios de divisibilidade, ao fornecerem regras simples para determinar se um número é divisível por outro sem realizar a divisão diretamente, facilitam a compreensão da estrutura numérica e são fundamentais para a resolução de problemas. Além disso, o uso do soroban, um ábaco japonês, como ferramenta para explorar a divisibilidade, oferece uma abordagem prática e lúdica, promovendo o aprendizado ativo e significativo.

O Teorema Fundamental da Aritmética, que garante a decomposição única de um número inteiro em fatores primos, é a pedra angular da Teoria dos Números. A partir desse teorema, diversas propriedades dos números primos são exploradas, como a sua distribuição irregular, a existência de infinitos primos em determinadas progressões aritméticas – Teorema de Dirichlet, e a formulação de conjecturas ainda não demonstradas, como a dos primos gêmeos. Abordamos alguns conjuntos de primos especiais, como os primos palíndromos e os primos reversos, além da famosa hipótese de Riemann, que desafia matemáticos há séculos e oferece um prêmio milionário para sua solução.

Outro conjunto que fascina matemáticos desde a antiguidade devido à sua peculiaridade é o dos números perfeitos. A busca por esses números raros e enigmáticos, cuja soma dos divisores

próprios é igual ao número, iniciou-se com os gregos e impulsionou o desenvolvimento da Teoria dos Números. A Figura 1.1 ilustra de maneira divertida a definição de número perfeito.

Figura 1.1 – Tirinha sobre números perfeitos



Fonte: Tenório (2011).

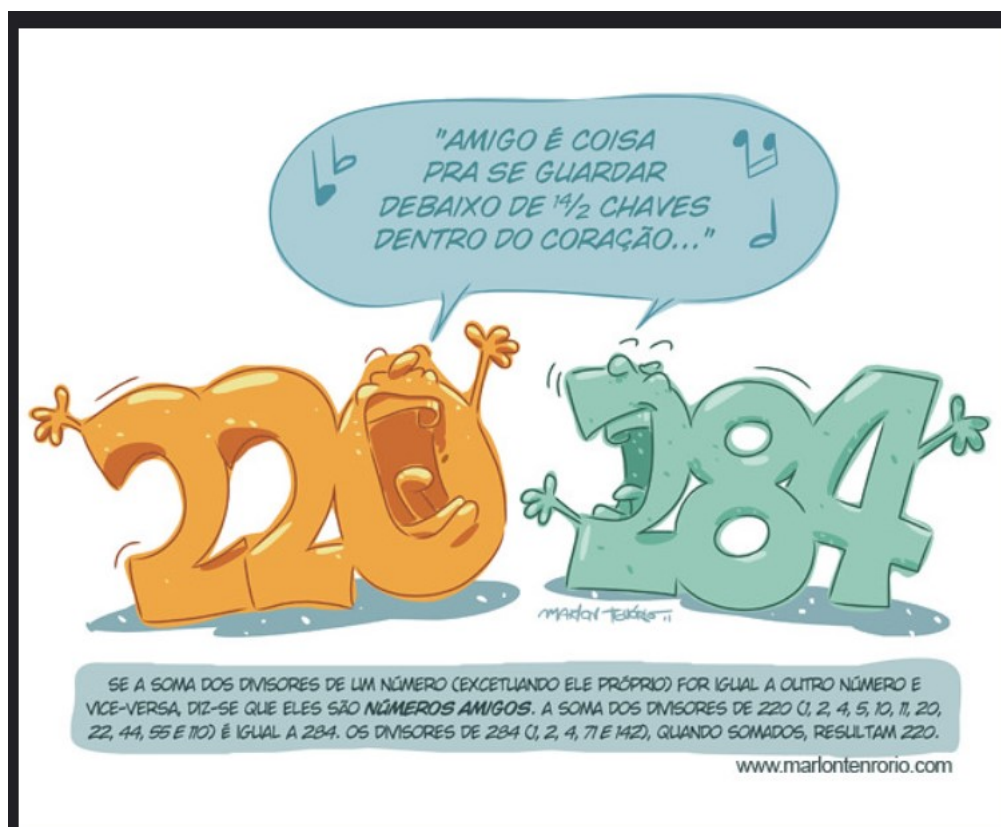
Já Viana (2024b, n.p) apresenta uma definição mais formal:

A noção é bem antiga: um número diz-se perfeito se ele é igual à soma dos seus divisores próprios, ou seja, dos divisores que são menores que o próprio número. Por exemplo, 6 é um perfeito porque os seus divisores próprios são 1, 2 e 3 e a soma deles dá precisamente 6. Analogamente, os divisores próprios do número 28 são 1, 2, 4, 7 e 14, e a soma deles é igual a 28.

Dentro do conjunto dos números perfeitos, analisamos suas propriedades, desde a demonstração de que todos os números perfeitos conhecidos são pares até a investigação da possibilidade de existência de números perfeitos ímpares, uma questão em aberto que intriga a comunidade matemática. Além disso, aprofundamos nosso estudo em conceitos relacionados, como números hiperperfeitos, Teorema de Euclides-Euler e outros, buscando identificar padrões numéricos e possíveis aplicações. Por fim, estabelecemos conexões entre os números perfeitos e outras classes de números, como os números geométricos, explorando, por exemplo, a relação entre números perfeitos e números triangulares.

A Matemática, repleta de enigmas e curiosidades, nos presenteia com números que estabelecem relações inesperadas. Os números amigos, com sua singularidade de serem a soma dos divisores próprios um do outro, são um exemplo fascinante dessas elaboradas redes de conexões numéricas. A Figura 1.2 ilustra o famoso par de amigos: 220 e 284.

Figura 1.2 – Charge sobre números amigáveis



Fonte: Tenório (2013).

De acordo com Neto e Toillier (2020, p. 92):

Dois números são ditos amigáveis quando a soma dos divisores próprios de um deles resulta no outro. Como exemplo desses pares de números, temos o 220 e o 284, aquele citado por Pitágoras. Veja que os divisores próprios de 220 são 1, 2, 4, 5, 10, 11, 20, 22, 44, 55 e 110, que, quando somados, resultam em 284. Já os divisores próprios de 284 são 1, 2, 4, 71 e 142, que, quando somados, resultam em 220.

Dentro deste contexto, exploramos as propriedades dos números amigáveis, desde as contribuições pioneiras de Euler até as pesquisas mais recentes. Investigamos teoremas, padrões numéricos e possíveis aplicações, além de estabelecer conexões com conceitos como números mutuamente amigos e quadrados amigos.

Com o intuito de tornar o estudo dos números primos, perfeitos e amigáveis mais dinâmico e significativo para os estudantes da Educação Básica, propomos atividades, na forma de sequências didáticas, que exploram desde a representação geométrica de números triangulares no GeoGebra (2025) até a implementação de algoritmos em linguagens de programação como o GNU Octave (2025). Essa abordagem gradual permitirá que os estudantes construam conhecimentos de forma progressiva, desde a visualização de padrões até a resolução de problemas mais complexos.

1.1 JUSTIFICATIVA PARA A ESCOLHA DO TEMA

“*A matemática é a rainha das ciências e a teoria dos números é a rainha da matemática*”
– Carl Friedrich Gauss (1777-1855): matemático, físico e astrônomo alemão.

Desde os tempos mais remotos, os números têm sido objeto de fascínio e contemplação para os estudiosos. Suas propriedades complexas e sua presença constante na natureza despertam nossa curiosidade e instigam a exploração de seus segredos mais profundos. Como Gauss tão eloquentemente expressou, a Teoria dos Números ocupa um lugar de destaque na hierarquia das disciplinas matemáticas, revelando-se uma fonte inesgotável de desafios intelectuais e descobertas surpreendentes (Euler *et al.*, 2015).

Os números estão presentes em diversas situações da nossa vida, desde as tarefas mais simples até as mais complexas. A BNCC, que é um marco legal para a educação brasileira, reflete essa realidade, destacando o estudo dos números como um pilar fundamental da Educação Básica e definindo um conjunto de aprendizagens essenciais que devem ser desenvolvidas por todos os estudantes. Esse documento, alinhado ao Plano Nacional de Educação (PNE), visa garantir a qualidade da educação e promover a formação integral dos estudantes, preparando-os para a vida em sociedade (Brasil, 2018).

A BNCC divide o ensino da Matemática em unidades temáticas, com o objetivo de desenvolver habilidades específicas em cada área. Dentro das unidades temáticas, temos a unidade temática Números, que tem como foco central o estudo dos conjuntos numéricos. Essa unidade desempenha um papel central na construção do pensamento matemático, proporcionando aos estudantes uma compreensão profunda dos diferentes conjuntos numéricos e suas aplicações. Ao longo do Ensino Fundamental, os estudantes são estimulados a explorar os conjuntos numéricos, a resolver problemas em diversos contextos, a desenvolver habilidades de cálculo, a compreender o valor posicional dos algarismos, a relacionar os números com grandezas e medidas, a desenvolver o raciocínio lógico-matemático e a conectar a Matemática com outras áreas do conhecimento (Brasil, 2018).

Para garantir o desenvolvimento das habilidades matemáticas propostas pela BNCC, são definidas dez competências gerais e oito específicas. Estas competências contribuem para o desenvolvimento integral dos estudantes, preparando-os para uma vida plena e participativa. As competências gerais 2 e 5, que enfatizam a importância do desenvolvimento de habilidades digitais, destacam a necessidade de:

[...]2. Exercitar a curiosidade intelectual e recorrer à abordagem própria das ciências, incluindo a investigação, a reflexão, a análise crítica, a imaginação e a criatividade, para investigar causas, elaborar e testar hipóteses, formular e resolver problemas e criar soluções (inclusive tecnológicas) com base nos conhecimentos das diferentes áreas.

[...]5. Compreender, utilizar e criar tecnologias digitais de informação e comunicação de forma crítica, significativa, reflexiva e ética nas diversas práticas sociais (incluindo as escolares) para se comunicar, acessar e disseminar informações, produzir conhecimentos, resolver problemas e exercer protagonismo e

autoria na vida pessoal e coletiva (Brasil, 2018, p. 9).

Já nas competências específicas, destacamos a competência 5 (Brasil, 2018, p. 265), segundo a qual o estudante deve: “Utilizar processos e ferramentas matemáticas, inclusive tecnologias digitais disponíveis, para modelar e resolver problemas cotidianos, sociais e de outras áreas de conhecimento, validando estratégias e resultados”.

O pensamento computacional é uma competência essencial na formação dos estudantes. Esse pensamento é entendido como um conjunto de habilidades que permite formular problemas, organizar e analisar dados, desenvolver soluções automatizáveis e utilizá-las na resolução de questões em diversos contextos (Brasil, 2018).

Desta forma, fica evidente a necessidade de uma abordagem interdisciplinar que combine o estudo teórico dos números com a aplicação prática em ambientes computacionais. Essa combinação, em consonância com a BNCC, promove a formação integral dos estudantes, desenvolvendo habilidades essenciais para a sociedade contemporânea, marcada pela crescente demanda por competências digitais e pensamento lógico.

1.2 REVISÃO DA BIBLIOGRAFIA

Em pesquisa realizada em 2024 no banco de dissertações do Mestrado Profissional em Matemática em Rede Nacional (PROFMAT) da Sociedade Brasileira de Matemática (SBM), utilizando o termo “primo”, obtivemos um total de 63 trabalhos. Dentre esses, as pesquisas de Carvalho (2013) e Quintans (2020) merecem destaque.

Carvalho (2013) dedica seu trabalho ao estudo dos números primos, apresentando conceitos fundamentais e demonstrações clássicas. O autor se concentra em uma abordagem mais prática, com a apresentação de métodos para encontrar e testar a primalidade de números, além da explorar a criptografia como aplicação dos números primos. Em contrapartida, apresentamos um enfoque mais teórico, fundamentado em teoremas, como o de Dirichlet e o de Ouro, e em conjecturas importantes, como a de Goldbach e a dos primos gêmeos.

O trabalho de Quintans (2020) oferece uma análise profunda e geral dos números primos, explorando sua história, propriedades e teoremas. O autor enfatiza a importância de integrar esses conceitos no currículo escolar, propondo atividades que estimulem o raciocínio matemático e a resolução de problemas, sempre buscando conexões com outros tópicos da matemática. Em nosso trabalho, além da análise geral, abordamos tipos específicos de números primos, como números primos palíndromos e reversos. No âmbito educacional, exploramos o potencial dos números primos e de outros conjuntos de números para desenvolver habilidades computacionais, utilizando ferramentas como o soroban digital, o GeoGebra e o GNU Octave.

Em uma nova busca no banco de dissertações do PROFMAT, utilizando a palavra “perfeito”, obtivemos 10 resultados. Dentre os resultados obtidos, salientamos o trabalho de

Brandão (2021), que apresenta uma investigação sobre a teoria dos números, com foco especial em números perfeitos. O autor explora não apenas as propriedades básicas desses números, mas também se aprofunda em tópicos como números multiperfeitos e números práticos. A pesquisa utiliza ferramentas teóricas como o teorema de Euler e o teorema de Touchard, além de realizar análises comparativas entre os componentes de um potencial número perfeito ímpar. Em contrapartida, nosso trabalho estabelece conexões entre números perfeitos, números triangulares e outros padrões geométricos, com maior foco em aplicações pedagógicas.

Ao realizar uma nova busca no banco de dissertações do PROFMAT, com a palavra-chave “amigáveis”, encontramos um único resultado, o trabalho de Santos Júnior (2020), que inicia sua pesquisa com uma contextualização histórica, explorando as contribuições de diversas civilizações antigas para o estudo dos números perfeitos e amigáveis. Em seguida, o autor apresenta os conceitos fundamentais da Teoria dos Números, fornecendo uma base sólida para a compreensão dos tópicos abordados. A parte central da dissertação é dedicada aos números perfeitos e amigáveis, com uma análise detalhada de suas propriedades, características e relações com outros conceitos matemáticos. A pesquisa culmina com uma discussão sobre os principais resultados obtidos ao longo da história e as perspectivas futuras para a área. Já nosso trabalho investiga as conexões entre os números amigáveis e as contribuições de Euler, além de identificar padrões interessantes nesses números.

Nenhum dos trabalhos analisados nesta revisão tem semelhança íntegra com o presente trabalho.

1.3 OBJETIVOS

1.3.1 OBJETIVO GERAL

Promover a aprendizagem significativa de números primos, perfeitos e amigáveis na Educação Básica por meio de atividades práticas interdisciplinares, utilizando ferramentas computacionais, como o GeoGebra e o GNU Octave.

1.3.2 OBJETIVOS ESPECÍFICOS

1. **Explorar a divisibilidade:** investigar os conceitos de paridade e divisibilidade, destacando suas propriedades e aplicações.
2. **Analisar os números primos:** estudar os números primos, incluindo o Teorema Fundamental da Aritmética, o teorema de Dirichlet e conjecturas importantes.
3. **Investigar os números perfeitos:** explorar as propriedades dos números perfeitos, incluindo o teorema de Euclides-Euler e os padrões numéricos associados.

4. **Estudar os números amigáveis:** analisar as relações entre números primos, perfeitos e amigáveis, destacando as contribuições de Euler e elencando padrões numéricos e aplicações.
5. **Organizar atividades para a sala de aula:** desenvolver atividades interativas para o ensino de conjuntos numéricos utilizando recursos computacionais.

1.4 PROCEDIMENTOS METODOLÓGICOS

A metodologia usada neste trabalho é quantitativa, bibliográfica e descritiva.

1. É quantitativa porque:

Focaliza uma quantidade pequena de conceitos;
 Inicia com ideias preconcebidas do modo pelo qual os conceitos estão relacionados;
 Utiliza procedimentos estruturados e instrumentos formais para coleta de dados;
 Coleta os dados mediante condições de controle;
 Enfatiza a objetividade, na coleta e análise dos dados;
 Analisa os dados numéricos através de procedimentos estatísticos (Gerhardt; Silveira, 2009, p. 34).

2. É bibliográfica pois

[...] é feita a partir do levantamento de referências teóricas já analisadas, e publicadas por meios escritos e eletrônicos, como livros, artigos científicos, páginas de web sites. Qualquer trabalho científico inicia-se com uma pesquisa bibliográfica, que permite ao pesquisador conhecer o que já se estudou sobre o assunto. Existem porém pesquisas científicas que se baseiam unicamente na pesquisa bibliográfica, procurando referências teóricas publicadas com o objetivo de recolher informações ou conhecimentos prévios sobre o problema a respeito do qual se procura a resposta (Gerhardt; Silveira, 2009, p. 37 *apud* Fonseca, 2002, p. 32).

3. É descritiva porque “exige do investigador uma série de informações sobre o que deseja pesquisar. Esse tipo de estudo pretende descrever os fatos e fenômenos de determinada realidade” (Gerhardt; Silveira, 2009, p. 35 *apud* Triviños, 1987).

Com base nas descrições das metodologias usadas, os procedimentos metodológicos adotados foram:

- Estabelecimento do objeto de estudo e das questões de pesquisa;
- Criação de critérios para selecionar os materiais mais adequados e relevantes para a pesquisa, priorizando obras de autores reconhecidos na área, publicações recentes e fontes acadêmicas indexadas;

- Realização da revisão bibliográfica, etapa fundamental da pesquisa, que proporcionou a construção de um referencial teórico sólido. Através da análise crítica de uma variedade de fontes (livros, artigos, monografias, dissertações, teses, vídeos e sites confiáveis), foi possível extrair informações relevantes e corroborar a validade de resultados;
- Elaboração de atividades fundamentadas na BNCC que colaborem com o desenvolvimento do pensamento computacional dos estudantes na Educação Básica, utilizando softwares como o GeoGebra e o GNU Octave.

Quanto aos critérios utilizados para considerar os sites como confiáveis, foram observados os seguintes aspectos:

- Afiliação institucional ou autoria identificável, como universidades, institutos de pesquisa ou especialistas da área;
- Presença de referências bibliográficas ou links para publicações científicas;
- Atualização regular do conteúdo, com datas de publicação recentes;
- Clareza, objetividade e linguagem técnico-científica compatível com a proposta acadêmica.

1.5 RECURSO EDUCACIONAL

O recurso educacional associado a esta dissertação, descrito no Capítulo 6, consiste em uma coleção de atividades, organizadas na forma de sequências didáticas, que investigam propriedades e padrões dos números primos, perfeitos e amigáveis. Nas atividades, empregamos ferramentas computacionais, como o GeoGebra e o GNU Octave, na constituição de pequenos scripts para que os estudantes visualizem, explorem padrões e resolvam problemas relacionados a esses conjuntos numéricos.

As atividades propostas no Capítulo 6 estão alinhadas às competências da BNCC, estimulando o desenvolvimento do pensamento computacional, a resolução de problemas, a colaboração e a criatividade. Ao final de cada sequência didática, esperamos que os estudantes sejam capazes de compreender as propriedades dos números primos, perfeitos e amigáveis, aplicando esses conhecimentos em diferentes contextos.

1.6 ESTRUTURA DO TRABALHO

O presente trabalho está estruturado em sete capítulos.

1. Capítulo 1: contextualizamos o tema da pesquisa apresentando sua relevância e justificativa; detalhamos a revisão bibliográfica, os objetivos, a metodologia, o recurso educacional e a estrutura do trabalho.

2. Capítulo 2: apresentamos os conceitos fundamentais de divisibilidade e paridade, destacando propriedades e a relação com o algoritmo da divisão; introduzimos o soroban como ferramenta pedagógica para auxiliar os estudantes na compreensão dos critérios de divisibilidade.
3. Capítulo 3: expomos um breve histórico sobre os números primos, ressaltando a importância desses números desde a antiguidade até os dias atuais; apresentamos a definição formal de número primo, suas propriedades e aplicações em diversas áreas, como criptografia e Teoria dos Números; abordamos teoremas e conjecturas clássicas, como o Teorema Fundamental da Aritmética e a Hipótese de Riemann; elencamos tipos especiais de números primos, como os gêmeos, palíndromos e reversos.
4. Capítulo 4: exibimos a definição de número perfeito, um breve histórico de seu estudo e os principais teoremas relacionados, com destaque para o Teorema de Euclides-Euler; estabelecemos conexões entre os números perfeitos e hiperperfeitos, assim como com padrões numéricos e geométricos.
5. Capítulo 5: apresentamos a definição e as propriedades dos números amigáveis, mencionando as contribuições de Euler; discutimos diferentes tipos de números amigáveis, como os mutuamente amigos e os quadrados amigos, destacando padrões que envolvem esses conceitos.
6. Capítulo 6: organizamos o recurso educacional em uma coleção de atividades, desenvolvidas na forma de sequências didáticas e fundamentadas nas competências da BNCC.
7. Capítulo 7: apresentamos as conclusões do trabalho.

2 DIVISIBILIDADE

A divisibilidade é um conceito fundamental na Teoria dos Números que estabelece a propriedade de um número inteiro ser dividido por outro sem deixar resto. Esse conceito é crucial não apenas para a compreensão de operações básicas em Matemática, mas também tem aplicações profundas em áreas como criptografia, teoria dos códigos e algoritmos. Além disso, a divisibilidade é a base para tópicos mais avançados, como o Teorema Fundamental da Aritmética, que afirma que “todo número natural maior do que um (1) ou é primo ou se escreve de modo único, a menos da ordem dos fatores, como um produto de números primos” (Hefez, 2022, p. 119).

A importância do conceito de divisibilidade também se estende ao campo educacional, onde é frequentemente utilizado como uma ferramenta pedagógica para o ensino de aritmética e álgebra. Segundo Resende (2007), a Teoria dos Números, ao evidenciar o estudo dos números inteiros, é considerada um campo ideal para o desenvolvimento de atividades investigativas. Isso se deve à exploração de padrões e relações numéricas, que envolvem inteiros, divisibilidade e números primos, aspectos sempre presentes na Matemática e passíveis de serem explorados nas atividades escolares em qualquer nível.

2.1 DEFINIÇÃO E PROPRIEDADES

Para compreender melhor o conceito de divisibilidade, é essencial apresentar a Definição 2.1 e as Proposições 2.1 a 2.8 que estabelecem algumas propriedades (Hefez, 2022, p. 38-42).

Definição 2.1. *Sejam $a, b \in \mathbb{Z}$. Dizemos que:*

- $a \mid b$ (lê-se: “ a divide b ”) se existe $c \in \mathbb{Z}$ tal que

$$b = a \cdot c.$$

Nesse caso, a é um divisor (ou fator) de b , e b é um múltiplo de a , ou dizemos que b é divisível por a .

- $a \nmid b$ (lê-se: “ a não divide b ”) se não existe $c \in \mathbb{Z}$ tal que

$$b = a \cdot c.$$

Os próximos resultados exprimem as principais propriedades da divisibilidade.

Proposição 2.1. *Sejam $a, b, c \in \mathbb{Z}$. Tem-se que:*

- i) $1 \mid a$, $a \mid a$ e $a \mid 0$;

- ii) $0|a$ se, e somente se, $a = 0$;
- iii) a divide b se, e somente se, $|a|$ divide $|b|$;
- iv) se $a|b$ e $b|c$, então $a|c$.

Demonstração.

- i) Decorre das igualdades $a = a \cdot 1$, $a = 1 \cdot a$ e $0 = 0 \cdot a$.
- ii) Suponhamos que $0|a$. Logo, existe $c \in \mathbb{Z}$ tal que $a = c \cdot 0$.
Pela Proposição 2.1(i), temos que $a \cdot 0 = 0$ para todo $a \in \mathbb{Z}$. Disso, concluímos que $a = 0$.
Para a recíproca, basta observarmos que $0|0$, o que foi provado no item anterior.
- iii) Suponhamos que $a|b$. Desta forma, existe $c \in \mathbb{Z}$ tal que $b = ac$. Consequentemente, temos que $|b| = |ac|$ e $|b| = |a||c|$. Logo, $|a||c| = |b|$.
Reciprocamente, temos que se $|a| \mid |b|$, então existe $c \in \mathbb{Z}$ tal que $|b| = |a||c|$, ou equivalentemente, $|b| = |ac|$. Portanto, $b = \pm ac$ e $a \mid b$.
- iv) Se $a|b$ e $b|c$, então existem $f, g \in \mathbb{Z}$, tais que $b = fa$ e $c = gb$. Substituindo o valor de b da primeira equação na segunda e usando a propriedade associativa da multiplicação, obtemos que:

$$c = gb = g(fa) = (gf)a,$$

o que mostra que $a|c$.

□

Uma decorrência dos itens (i) e (iii) da Proposição 2.1 é que todo número inteiro a é divisível por ± 1 e por $\pm a$. O item (i) também inclui o caso $0|0$ e, afirma que zero tem infinitos divisores.

Suponhamos que $a|b$ e que $a \neq 0$. Seja $c \in \mathbb{Z}$ tal que $b = ca$. O número inteiro c é denominado *quociente* de b por a e denotado por $c = \frac{b}{a}$.

Proposição 2.2. Se $a, b, c, d \in \mathbb{Z}$, então

$$a|b \text{ e } c|d \Rightarrow ac|bd.$$

Demonstração. Se $a|b$ e $c|d$, então existem $f, g \in \mathbb{Z}$ tais que $b = fa$ e $d = gc$. Portanto, $bd = (fg)(ac)$. Logo, $ac|bd$.

□

Em particular, se $a|b$, então $ac|bc$ para todo $c \in \mathbb{Z}$.

Proposição 2.3. *Sejam $a, b, c \in \mathbb{Z}$. Se $a|(b \pm c)$, então*

$$a|b \Leftrightarrow a|c.$$

Demonstração. Suponhamos que $a|(b + c)$. Logo, existe $f \in \mathbb{Z}$ tal que $b + c = fa$.

Agora, se $a|b$, temos que existe $g \in \mathbb{Z}$ tal que $b = ga$. Substituindo a segunda igualdade na primeira, obtemos que

$$ga + c = fa,$$

donde segue que $c = (f - g)a$. Logo, $a|c$.

A prova da implicação contrária é totalmente análoga.

Por outro lado, se $a|(b - c)$ e $a|b$, pelo caso anterior temos que $a| -c$, o que implica que $a|c$.

□

Proposição 2.4. *Se $a, b, c \in \mathbb{Z}$ são tais que $a|b$ e $a|c$, então para todo $x, y \in \mathbb{Z}$*

$$a|(xb + yc).$$

Demonstração. Como $a|b$ e $a|c$, existem $f, g \in \mathbb{Z}$ tais que $b = fa$ e $c = ga$. Logo,

$$xb + yc = x(fa) + y(ga) = (xf + yg)a,$$

ou seja, a divide $(xb + yc)$.

□

Proposição 2.5. *Se $a, b \in \mathbb{Z}$, onde $b \neq 0$, então*

$$a|b \Rightarrow |a| \leq |b|.$$

Demonstração. De fato, $a|b$ implica que existe $c \in \mathbb{Z}$ tal que $b = ca$. Em módulo, temos que $|b| = |c||a|$. Como $b \neq 0$, segue que $c \neq 0$. Logo, $1 \leq |c|$ e, consequentemente, $|a| \leq |a||c| = |b|$.

□

Em particular, se $a \in \mathbb{Z}$ e $a|1$, então $0 < |a| \leq 1$. Logo, $|a| = 1$ e, portanto, $a = \pm 1$.

Como, para $b \neq 0$, temos que todo divisor a de b é tal que $|a| \leq |b|$, segue, neste caso, que b tem um número finito de divisores que satisfazem $-|b| \leq a \leq |b|$.

Baseados em algumas das proposições demonstradas até aqui, podemos afirmar que a divisibilidade em $\mathbb{N} \cup 0$ é uma relação de ordem, pois

1. é reflexiva: para todo $a \in \mathbb{N}$, $a|a$ (Proposição 2.1 (i)),

2. é transitiva: se $a|b$ e $b|c$, então $a|c$ (Proposição 2.1 (iv)),
3. é antissimétrica: se $a|b$ e $b|a$, então $a = b$ (decorrência da Proposição 2.5).

Entretanto, a divisibilidade não é uma relação de ordem em $\mathbb{Z}$, pois, apesar de ainda ser reflexiva e transitiva, ela não é antissimétrica. De fato, $-2|2$ e $2|-2$, mas $2 \neq -2$.

Proposição 2.6. *Se $a, b \in \mathbb{Z}$ e $n \in \mathbb{N}$, então*

$$(a - b) \mid (a^n - b^n).$$

Demonstração. Efetuaremos a prova por indução sobre n .

A propriedade é verdadeira para $n = 1$, pois $a - b$ divide $a^1 - b^1 = a - b$.

Suponhamos que a propriedade é verdadeira para $n = k$, isto é, $(a - b) \mid (a^k - b^k)$. Desta forma, temos que

$$a^{k+1} - b^{k+1} = aa^k - ba^k + ba^k - bb^k = (a - b)a^k + b(a^k - b^k). \quad (2.1)$$

Como $(a - b) \mid (a - b)$ e $(a - b) \mid (a^k - b^k)$ (HI), decorre de (2.1) e da Proposição 2.4 que $(a - b) \mid (a^{k+1} - b^{k+1})$. Logo, a propriedade é verdadeira para $k + 1$. Portanto, pelo teorema de indução finita, a propriedade é válida para todo $n \in \mathbb{N}$.

□

Uma aplicação interessante da Proposição 2.6 é o fato de que todo número da forma $10^n - 1$, onde $n \in \mathbb{N}$, é divisível por 9. De fato, considerando $a = 10$ e $b = 1$ na Proposição 2.6, obtemos que $a - b = 9$ divide $a^n - b^n = 10^n - 1$.

Proposição 2.7. *Se $a, b \in \mathbb{Z}$ e $n \in \mathbb{N} \cup \{0\}$, então*

$$(a + b) \mid (a^{2n+1} + b^{2n+1}).$$

Demonstração. Provaremos por indução sobre n .

A propriedade é verdadeira para $n = 0$, pois $a + b$ divide $a^1 + b^1 = a + b$.

Suponhamos agora que a propriedade é verdadeira para $n = k$, ou seja, $(a + b) \mid (a^{2k+1} + b^{2k+1})$. Assim, temos que

$$\begin{aligned} a^{2(k+1)+1} + b^{2(k+1)+1} &= a^2 a^{2k+1} - b^2 a^{2k+1} + b^2 a^{2k+1} + b^2 b^{2k+1} \\ &= (a^2 - b^2) a^{2k+1} + b^2 (a^{2k+1} + b^{2k+1}). \end{aligned} \quad (2.2)$$

Como $(a + b) \mid (a^2 - b^2) = (a + b)(a - b)$ e $(a + b) \mid (a^{2k+1} + b^{2k+1})$ (HI), decorre de (2.2) e da Proposição 2.4 que $(a + b) \mid (a^{2(k+1)+1} + b^{2(k+1)+1})$. Dessa forma, a propriedade é

verdadeira para $k + 1$. Logo, pelo teorema de indução finita, a propriedade é verdadeira para todo $n \in \mathbb{N}$.

□

Proposição 2.8. *Se $a, b \in \mathbb{Z}$ e $n \in \mathbb{N}$, então*

$$(a + b) \mid (a^{2n} - b^{2n}).$$

Demonstração. Usaremos indução sobre n para efetuar a prova.

A propriedade é verdadeira para $n = 1$, pois $a + b$ divide $a^2 - b^2 = (a + b)(a - b)$.

Suponhamos que a propriedade é válida para $n = k$, isto é, $(a + b) \mid (a^{2k} - b^{2k})$ (HI). Desta forma, temos que

$$a^{2(k+1)} - b^{2(k+1)} = a^2 a^{2k} - b^2 a^{2k} + b^2 a^{2k} - b^2 b^{2k} = (a^2 - b^2) a^{2k} + b^2 (a^{2k} - b^{2k}). \quad (2.3)$$

Como $(a + b) \mid (a^2 - b^2)$ e $(a + b) \mid (a^{2k} - b^{2k})$, decorre de (2.3) e da Proposição 2.4 que $(a + b) \mid (a^{2(k+1)} - b^{2(k+1)})$. Logo, a propriedade é verdadeira para $k + 1$. Portanto, pelo teorema de indução finita, a propriedade é válida para todo $n \in \mathbb{N}$.

□

A definição e proposições apresentadas fornecem uma base sólida para a compreensão do tema abordado neste capítulo. Ao explorar as propriedades da divisibilidade, esclarecemos a estrutura e as implicações teóricas do assunto. Esses elementos essenciais não apenas fundamentam a análise realizada, mas também abrem caminho para futuras investigações e aplicações práticas. Assim, a compreensão profunda da definição e das proposições é crucial para avançarmos no estudo do referido tema.

2.2 CRITÉRIOS DE DIVISIBILIDADE

Os critérios de divisibilidade constituem um conjunto de regras que permitem determinar a divisibilidade de um número por outro de forma rápida e eficiente, sem a necessidade de efetuar a divisão propriamente dita. Essas regras se baseiam em propriedades aritméticas específicas, explorando padrões numéricos característicos aos números inteiros no sistema decimal.

Esse sistema, também conhecido como sistema de numeração de base 10, é um caso particular de um sistema posicional de base b , no qual o valor de cada dígito depende de sua posição e das potências da base. Dado um número N representado em base b , ele pode ser escrito na forma

$$N = a_n b^n + a_{n-1} b^{n-1} + \cdots + a_1 b^1 + a_0 b^0,$$

onde:

- b é a base (um número inteiro maior que 1);
- a_i são os dígitos do número, com $0 \leq a_i < b$;
- n é a posição do dígito mais significativo (à esquerda).

Cada posição corresponde a uma potência da base b , e o valor total do número é a soma dos produtos de cada dígito pela sua respectiva potência. No caso da base decimal ($b = 10$), utilizam-se os dígitos de 0 a 9, e essa estrutura posicional é a base para o funcionamento dos critérios de divisibilidade, já que muitos deles se apoiam nas propriedades das potências de 10 e na maneira como os dígitos se distribuem nas diferentes ordens (unidades, dezenas, centenas, entre outras).

Exemplo 2.1. O número 3457 na base 10.

$$3 \cdot 10^3 + 4 \cdot 10^2 + 5 \cdot 10^1 + 7 \cdot 10^0 = 3000 + 400 + 50 + 7 = 3457$$

A decomposição apresentada no Exemplo 2.1 ilustra como os dígitos contribuem para o valor total de um número no sistema decimal, o que é fundamental para compreender o funcionamento dos critérios de divisibilidade.

Ao analisar a estrutura de um número, os critérios de divisibilidade permitem identificar se um determinado divisor deixa resto zero. Esta característica os torna ferramentas indispensáveis em diversas áreas da Matemática, como Teoria dos Números, Aritmética e Álgebra.

Apresentamos os critérios de divisibilidade por 2, 3, 4, 5, 6, 7, 8 e 9 - Teoremas 2.1 a 2.8, baseados, respectivamente em, Costa (2021a, 17 s), Costa (2021b, 15 s), Costa (2021c, 18 s), Costa (2021d, 16 s), Silva (2019, p. 37), Costa (2021e, 23 s), Silva (2019, p. 39) e Alves (2021, p. 40).

CRITÉRIO DE DIVISIBILIDADE POR 2

Teorema 2.1. Um número inteiro n é divisível por 2 se, e somente se, o seu algarismo da unidade for par.

Demonstração. Seja $a_k a_{k-1} \dots a_2 a_1 a_0$ a representação decimal de n . Desta forma, temos que:

$$\begin{aligned} n &= 10^k a_k + 10^{k-1} a_{k-1} + \dots + 10^2 a_2 + 10 a_1 + a_0; \\ n &= 10 \left(10^{k-1} a_k + 10^{k-2} a_{k-1} + \dots + 10 a_2 + a_1 \right) + a_0. \end{aligned} \quad (2.4)$$

Consideremos $A = 10 \left(10^{k-1} a_k + 10^{k-2} a_{k-1} + \dots + 10 a_2 + a_1 \right)$ em (2.4) e que n é divisível por 2. Assim, como $2|n$ e $2|A$, segue que $2|(n - A)$, ou seja, $2|a_0$.

Reciprocamente, suponhamos que $2|a_0$. Como $2|A$, segue que $2|(A + a_0)$. Portanto, $2|n$.

□

CRITÉRIO DE DIVISIBILIDADE POR 3

Teorema 2.2. *Um número inteiro n é divisível por 3 se, e somente se, a soma dos seus algarismos é divisível por 3.*

Demonstração. Seja $a_k a_{k-1} \dots a_2 a_1 a_0$ a representação decimal de n . Assim, temos que:

$$\begin{aligned} n &= 10^k a_k + 10^{k-1} a_{k-1} + \dots + 10^2 a_2 + 10 a_1 + a_0; \\ n &= \underbrace{99\dots 9}_{k \text{ vezes}} a_k + \underbrace{99\dots 9}_{k-1 \text{ vezes}} a_{k-1} + \dots + 99 a_2 + 9 a_1 + (a_k + a_{k-1} + \dots + a_2 + a_1 + a_0). \end{aligned} \quad (2.5)$$

Consideremos $n = A + B$, onde

$$\begin{aligned} A &= \underbrace{99\dots 9}_{k \text{ vezes}} a_k + \underbrace{99\dots 9}_{k-1 \text{ vezes}} a_{k-1} + \dots + 99 a_2 + 9 a_1 \\ &= 3 \left(\underbrace{33\dots 3}_{k \text{ vezes}} a_k + \underbrace{33\dots 3}_{k-1 \text{ vezes}} a_{k-1} + \dots + 33 a_2 + 3 a_1 \right), \\ B &= a_k + a_{k-1} + \dots + a_2 + a_1 + a_0 \end{aligned}$$

em (2.5) e n é divisível por 3. Desta forma, como $3|n$ e $3|A$, segue que $3|(n - A)$. Portanto, $3|B$.

Reciprocamente, suponhamos que $3|B$. Como $3|A$, segue que $3|(A + B) = n$.

□

CRITÉRIO DE DIVISIBILIDADE POR 4

Teorema 2.3. *Um número inteiro n é divisível por 4 se, e somente se, o número formado pelos dois últimos algarismos é divisível por 4.*

Demonstração. Seja $a_k a_{k-1} \dots a_2 a_1 a_0$ a representação decimal de n . Desta forma, temos que:

$$\begin{aligned} n &= 10^k a_k + 10^{k-1} a_{k-1} + \dots + 10^2 a_2 + 10 a_1 + a_0; \\ n &= 100 \left(10^{k-2} a_k + 10^{k-3} a_{k-1} + \dots + a_2 \right) + (10 a_1 + a_0). \end{aligned} \quad (2.6)$$

Escrevamos $n = A + B$, onde

$$\begin{aligned} A &= 100 \left(10^{k-2} a_k + 10^{k-3} a_{k-1} + \dots + a_2 \right), \\ B &= 10 a_1 + a_0 \end{aligned}$$

em (2.6) e suponhamos que n é divisível por 4. Assim, como $4|n$ e $4|A$, segue que $4|(n - A)$. Logo, $4|B$.

Reciprocamente, se $4|B$, como $4|A$, segue que $4|(A + B) = n$.

□

CRITÉRIO DE DIVISIBILIDADE POR 5

Teorema 2.4. *Um número inteiro n é divisível por 5 se, e somente se, o seu último algarismo é 0 ou 5.*

Demonstração. Seja $a_k a_{k-1} \dots a_2 a_1 a_0$ a representação decimal de n . Assim, temos:

$$\begin{aligned} n &= 10^k a_k + 10^{k-1} a_{k-1} + \dots + 10^2 a_2 + 10 a_1 + a_0; \\ n &= 10 \left(10^{k-1} a_k + 10^{k-2} a_{k-1} + \dots + 10 a_2 + a_1 \right) + a_0. \end{aligned} \quad (2.7)$$

Consideremos $A = 10 \left(10^{k-1} a_k + 10^{k-2} a_{k-1} + \dots + 10 a_2 + a_1 \right)$ em (2.7) e suponhamos que n é divisível por 5. Desta forma, como $5|n$ e $5|A$, segue que $5|(n - A)$. Portanto, $5|a_0$ e $a_0 = 0$ ou $a_0 = 5$.

Reciprocamente, suponhamos que $a_0 = 0$ ou $a_0 = 5$. Como $5|A$ e $5|a_0$ para ambos os casos, segue que $5|(A + a_0) = n$.

□

CRITÉRIO DE DIVISIBILIDADE POR 6

Teorema 2.5. *Um número inteiro $n = a_k a_{k-1} \dots a_2 a_1 a_0$ é divisível por 6 se, e somente se, n for divisível simultaneamente por 2 e 3.*

O Teorema Fundamental da Aritmética (Teorema 3.2) proporciona uma justificativa sólida para o critério de divisibilidade por 6. De fato, a decomposição em fatores primos de 6 é única (a menos da ordem dos fatores) e dada por $6 = 2 \cdot 3$.

Demonstração. Seja n um número inteiro. Considerando $n = 6t = 2(3t)$ e $x = 3t$, temos que $n = 2x$, com $x \in \mathbb{Z}$. Logo, $2|n$. De maneira análoga, consideremos $n = 6t = 3(2t)$ e $y = 2t$. Portanto, $n = 3y$, com $y \in \mathbb{Z}$, e $3|n$.

Por outro lado, suponhamos que n seja divisível por 2 e 3. Assim, como $2|n$, existe $k \in \mathbb{Z}$ tal que $n = 2k$. Multiplicando a igualdade $3 - 2 = 1$ por k , obtemos que:

$$\begin{aligned} 3k - 2k &= k; \\ 3k - n &= k. \end{aligned} \quad (2.8)$$

Ainda, como $3|n$, existe $t \in \mathbb{Z}$ tal que $n = 3t$. Substituindo esta igualdade em (2.8), temos que:

$$\begin{aligned} 3k - 3t &= k; \\ 3(k - t) &= k. \end{aligned} \tag{2.9}$$

Considerando $(k - t) = y$ em (2.9), temos $k = 3y$, com $y \in \mathbb{Z}$. De $n = 2k$ e $k = 3y$, decorre que $n = 6y$. Logo, $6|n$.

□

CRITÉRIO DE DIVISIBILIDADE POR 7

Teorema 2.6. *Um número inteiro $n = a_k a_{k-1} \dots a_2 a_1 a_0$ é divisível por 7 se, e somente se, $(a_k a_{k-1} \dots a_2 a_1) - 2a_0$ é divisível por 7.*

Demonstração. Suponhamos que n é divisível por 7. Como:

$$\begin{aligned} (a_k a_{k-1} \dots a_2 a_1) - 2a_0 &= \frac{(a_k a_{k-1} \dots a_2 a_1 a_0) - a_0}{10} - 2a_0; \\ &= \frac{(a_k a_{k-1} \dots a_2 a_1 a_0) - 21a_0}{10}, \end{aligned}$$

e $7|n$, $7|21a_0$, $(7, 10) = 1$, segue que $7|(a_k a_{k-1} \dots a_2 a_1) - 2a_0$.

Reciprocamente, suponhamos que $7|(a_k a_{k-1} \dots a_2 a_1) - 2a_0$.

Logo, $7|10[(a_k a_{k-1} \dots a_2 a_1) - 2a_0]$. Contudo:

$$\begin{aligned} 10[(a_k a_{k-1} \dots a_2 a_1) - 2a_0] &= (a_k a_{k-1} \dots a_2 a_1 0) - 20a_0 \\ &= (a_k a_{k-1} \dots a_2 a_1 0) + a_0 - 20a_0 - a_0 \\ &= n - 21a_0. \end{aligned}$$

Como $7|21a_0$, segue que $7|[(n - 21a_0) + 21a_0]$. Logo, $7|n$.

□

CRITÉRIO DE DIVISIBILIDADE POR 8

Teorema 2.7. *Um número inteiro $n = a_k a_{k-1} \dots a_2 a_1 a_0$, com mais de três algarismos, é divisível por 8 se, e somente se, o número formado por seus três últimos algarismos for divisível por 8.*

Demonstração. Seja $a_k a_{k-1} \dots a_2 a_1 a_0$ a representação decimal de n . Desta forma, temos que:

$$\begin{aligned} n &= 10^k a_k + 10^{k-1} a_{k-1} + \dots + 10^2 a_2 + 10a_1 + a_0; \\ n &= 10^3 (10^{k-3} a_k + 10^{k-4} a_{k-1} + \dots + a_3) + (10^2 a_2 + 10a_1 + a_0). \end{aligned} \tag{2.10}$$

Consideremos $n = A + B$, onde

$$A = 10^3 (10^{k-3}a_k + 10^{k-4}a_{k-1} + \cdots + a_3),$$

$$B = 10^2a_2 + 10a_1 + a_0$$

em (2.10) e suponhamos que n é divisível por 8. Assim, como $8|n$ e $8|A$, segue que $8|(n - A)$. Logo, $8|B$.

Reciprocamente, suponhamos que $8|B$. Como $8|A$, segue que $8|(A + B)$. Portanto, $8|n$.

□

CRITÉRIO DE DIVISIBILIDADE POR 9

Teorema 2.8. *Um número inteiro $n = a_k a_{k-1} \dots a_2 a_1 a_0$ é divisível por 9 se, e somente se, a soma de seus algarismos, $a_k + a_{k-1} + \cdots + a_2 + a_1 + a_0$, for divisível por 9.*

Demonstração. Seja $a_k a_{k-1} \dots a_2 a_1 a_0$ a representação decimal de n . Assim, temos que:

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

$$n = \underbrace{99\dots9}_{k \text{ vezes}} a_k + \underbrace{99\dots9}_{k-1 \text{ vezes}} a_{k-1} + \cdots + 99a_2 + 9a_1 + (a_k + a_{k-1} + \cdots + a_2 + a_1 + a_0).$$
(2.11)

Consideremos

$$A = \underbrace{99\dots9}_{k \text{ vezes}} a_k + \underbrace{99\dots9}_{k-1 \text{ vezes}} a_{k-1} + \cdots + 99a_2 + 9a_1$$

$$= 9 \left(\underbrace{11\dots1}_{k \text{ vezes}} a_k + \underbrace{11\dots1}_{k-1 \text{ vezes}} a_{k-1} + \cdots + 11a_2 + a_1 \right),$$

$$B = a_k + a_{k-1} + \cdots + a_2 + a_1 + a_0$$

em (2.11) e que n é divisível por 9. Desta forma, como $9|n$ e $9|A$, segue que $9|(n - A)$. Logo, $9|B$.

Reciprocamente, suponhamos que $9|B$. Como $9|A$, segue que $9|(A + B)$. Portanto, $9|n$.

□

Além dos critérios de divisibilidade apresentados, existem muitos outros, incluindo aqueles baseados na composição de critérios, como o do número 12, que combina os critérios de 3 e 4. Há também critérios menos usuais, como os que envolvem potências de 2 e números compostos com fatores primos entre si. É possível consultar alguns desses critérios em <https://pt.wikipedia.org/wiki/Crit%C3%A9rios_de_divisibilidade>.

2.3 PARIDADE

Ao discutir o conceito de divisibilidade, é indispensável mencionarmos Euclides. A divisão euclidiana é um método fundamental que estabeleceu as bases para a Aritmética e a Teoria dos Números. Segundo Hefez (2022), mesmo quando um número inteiro $b \neq 0$ não divide o número inteiro a , Euclides, em sua obra “Os elementos” (Euclides, 2009), utiliza implicitamente o fato de que sempre é possível realizar a divisão de a por b , resultando em um quociente e um resto. O Teorema 2.9 (Bezerra, 2018, p. 26-27) estabelece o algoritmo de Euclides para a divisão.

Teorema 2.9. *(Algoritmo da Euclides) Dados dois números inteiros a e b , com $b \neq 0$, existem dois números inteiros q e r , únicos, tais que*

$$a = bq + r,$$

com $0 \leq r < |b|$.

Demonstração.

(I) Existência de q e r .

Inicialmente, mostraremos a existência de q e r . Como $b \neq 0$, temos dois casos possíveis.

Caso 1: $b > 0$.

Consideremos o conjunto $S : \{a - bx; x \in \mathbb{Z} \text{ e } a - bx \geq 0\}$. Para garantir que $S \neq \emptyset$, precisamos mostrar que quaisquer que sejam a e b inteiros com $b > 0$, sempre existe $x \in \mathbb{Z}$ tal que $a - bx \geq 0$. Considerando $x = -|a|$, como $b \geq 1$ segue que

$$a - bx = a + b|a| \geq a + |a| \geq 0.$$

Assim, $a - bx = a + b|a| \in S$ quaisquer que sejam a e b . Logo, $S \neq \emptyset$. Disso, temos pelo Princípio da Boa Ordem (Hefez, 2022) que existe $r = \min S$. Assim, $r \in S$, $r = a - bq$, para algum $q \in \mathbb{Z}$, $a = bq + r$, com $q, r \in \mathbb{Z}$.

Agora precisamos mostrar que $0 \leq r < b$. Pela definição de S , temos que $r = \min S \geq 0$. Resta mostrar que $r < b$. Suponhamos, por absurdo, que $r \geq b$ ou equivalentemente $r - b \geq 0$. Como $r \in S$, $r = a - bx$ para algum $x \in \mathbb{Z}$. Assim,

$$0 \leq r - b = (a - bx) - b = a - b(x + 1) \Rightarrow (r - b) \in S,$$

o que é um absurdo pois $r - b < r = \min S$. Portanto, $0 \leq r < b$.

Caso 2: $b < 0$.

Neste caso, $|b| = -b > 0$ e, pelo Caso 1, existem q' e r' tais que:

$$a = |b|q' + r' = b(-q') + r', \text{ com } 0 \leq r' < |b|.$$

Assim, basta considerar $q = -q'$ e $r = r'$.

(II) Unicidade de q e r .

Suponhamos que existam $q_1, q_2, r_1, r_2 \in \mathbb{Z}$, tais que:

$$a = bq_1 + r_1;$$

$$a = bq_2 + r_2,$$

com $0 \leq r_1, r_2 < |b|$.

Se $r_1 \neq r_2$, consideremos $r_1 < r_2$. Desta forma,

$$0 < r_2 - r_1 = b(q_1 - q_2) \Rightarrow b|(r_2 - r_1) \Rightarrow |b| \leq |r_2 - r_1| = r_2 - r_1,$$

o que é um absurdo pois $r_2 - r_1 \leq r_2 < |b|$. Assim, $r_1 = r_2$ e $b(q_1 - q_2) = 0$ e, como $b \neq 0$, $q_1 = q_2$.

□

A paridade dos números inteiros, que se refere a um número ser par ou ímpar, está diretamente ligada ao algoritmo de Euclides. De acordo com Hefez (2022, p. 46): “Dado um número inteiro $n \in \mathbb{Z}$ qualquer, temos duas possibilidades:

- i) o resto da divisão de n por 2 é 0, isto é, existe $q \in \mathbb{Z}$ tal que $n = 2q$; ou
- ii) o resto da divisão de n por 2 é 1, ou seja, existe $q \in \mathbb{Z}$ tal que $n = 2q + 1$ ”.

Ainda segundo Hefez (2022, p. 46):

Portanto, os números inteiros dividem-se em duas classes, a dos números da forma $2q$ para algum $q \in \mathbb{Z}$, chamados de *números pares*, e a dos números da forma $2q + 1$, chamados de *números ímpares*. Os naturais são classificados em pares e ímpares, pelo menos desde Pitágoras, 500 anos antes de Cristo. A paridade de um número inteiro é o caráter do número ser par ou ímpar.

Compreender a forma dos números pares e ímpares possibilita o entendimento de algumas propriedades ligadas a eles (Hefez, 2015, p. 58-59).

- A soma de dois números pares é par.

De fato, os dois números podem ser escritos na forma $2a$ e $2b$, em que $a, b \in \mathbb{Z}$, cuja soma é $2(a + b)$, logo par;

- A soma de dois números ímpares é par.

De fato, os dois números podem ser escritos na forma $2a + 1$ e $2b + 1$, em que $a, b \in \mathbb{Z}$, cuja soma é $2(a + b + 1)$, logo par;

- A soma de um número par com um número ímpar é ímpar.

De fato, os dois números podem ser escritos na forma $2a$ e $2b + 1$, em que $a, b \in \mathbb{Z}$, cuja soma é $2(a + b) + 1$, logo ímpar;

- O produto de dois números pares é par.

De fato, os números sendo da forma $2a$ e $2b$, nos quais $a, b \in \mathbb{Z}$, temos que o seu produto é $4ab$ e, portanto, múltiplo de 4, logo par;

- O produto de dois números ímpares é ímpar.

De fato, sendo os números da forma $2a + 1$ e $2b + 1$, nos quais $a, b \in \mathbb{Z}$, o seu produto é $2(2ab + a + b) + 1$, logo ímpar.

- O produto de um número par por um número ímpar é par.

De fato, um número da forma $2a$ e um número da forma $2b + 1$, com $a, b \in \mathbb{Z}$, têm um produto igual a $2a(2b + 1)$, que é par;

A paridade, isto é, a qualidade de ser par ou ímpar, da soma e do produto de dois números inteiros só depende da paridade de cada um dos números e não dos números em si. Assim, podemos decidir a paridade de uma expressão complexa envolvendo produtos e somas de inteiros da seguinte maneira: atribuímos, em alusão ao resto deixado por esses números na divisão por 2, o símbolo $\bar{0}$ aos números pares e o símbolo $\bar{1}$ aos números ímpares, e empregamos as propriedades da paridade descritas anteriormente. A Tabela 2.1 resume a paridade da soma e do produto de dois números inteiros, enquanto que o Exemplo 2.2 mostra como empregar essa tabela para determinar a paridade de um número elevado.

Tabela 2.1 – Paridade da soma e do produto de dois números inteiros

+	$\bar{0}$	$\bar{1}$	×	$\bar{0}$	$\bar{1}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{0}$	$\bar{1}$

Fonte: Hefez (2015).

Exemplo 2.2. Para determinar a paridade do número

$$20^{10} \times 11^{200} + 21^{19},$$

substituímos o número 20 por $\bar{0}$, por ser par, e os números 11 e 21 por $\bar{1}$, por serem ímpares, obtendo a expressão

$$\bar{0}^{10} \times \bar{1}^{200} + \bar{1}^{19},$$

que operada segundo a Tabela 2.1 resulta em $\bar{1}$. Portanto, o número $20^{10} \times 11^{200} + 21^{19}$ é ímpar.

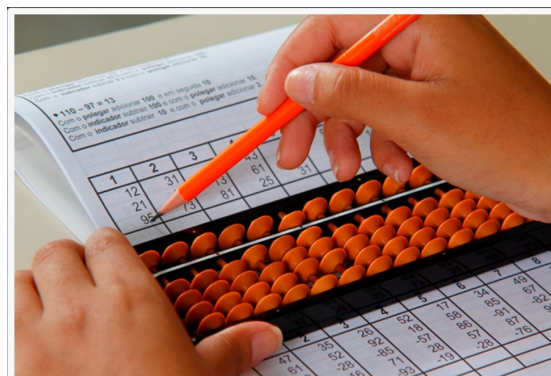
A paridade é um conceito simples, mas poderoso na Matemática. Desde a classificação básica de números inteiros até aplicações avançadas em diversas áreas, a distinção entre números pares e ímpares permeia muitos aspectos do conhecimento matemático. Por meio da exploração da paridade, podemos obter uma compreensão mais profunda de padrões numéricos e estruturas algébricas, bem como aplicar esses conhecimentos para resolver problemas práticos.

2.4 A DIVISIBILIDADE NO SOROBAN

Desde os primórdios, a Matemática tem sido uma companheira inseparável da humanidade, auxiliando na compreensão do mundo e no desenvolvimento de tecnologias. Ao longo dos séculos, diversas ferramentas foram criadas para facilitar os cálculos, e o soroban, o ábaco¹ japonês, destaca-se como um exemplo marcante de como a cultura e a inovação podem se unir para criar instrumentos que transcendem épocas e fronteiras, permanecendo relevantes até os dias atuais.

O ábaco, instrumento de cálculo milenar, passou por diversas transformações ao longo da história. O soroban, representado na Figura 2.1, sofreu diversas transformações desde sua importação da China no século XVII. Sua evolução, marcada por adaptações às diferentes culturas e sistemas numéricos, culminou no modelo moderno, com contas lenticulares e configuração decimal. Essa trajetória, que se iniciou com simples sulcos na areia e pequenas pedras, demonstra a engenhosidade humana na busca por ferramentas de cálculo cada vez mais eficientes (Resende, 2018).

Figura 2.1 – Soroban



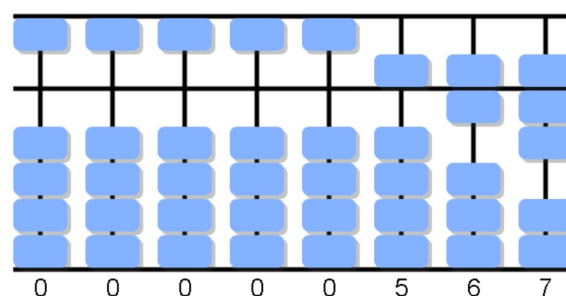
Fonte: Supera (2023).

O soroban foi introduzido no Brasil por imigrantes japoneses em 1908. Sua popularização se deu em meados do século XX, com destaque para o trabalho de Fukutaro Kato. A adaptação do soroban para o ensino de deficientes visuais, realizada por Joaquim Lima de Moraes em 1949, foi um marco. A adição de borracha compressora tornou o instrumento mais acessível e eficaz, facilitando o aprendizado de conceitos matemáticos como unidade, dezena e centena. Essa adaptação contribuiu significativamente para a inclusão de pessoas com deficiência visual no ensino da Matemática, promovendo a autonomia e o desenvolvimento do raciocínio lógico (Alves; Souza, 2024).

¹ A palavra ábaco deriva do grego “Abai”, que significa tábua de contar.

O soroban é um instrumento de cálculo manual composto por hastes verticais com contas deslizantes. Cada haste representa uma posição decimal: unidades, dezenas, centenas, e assim por diante. As contas na parte superior valem 5 e as da parte inferior, 1. Representamos os números no soroban movimentando as contas em direção à barra horizontal. A Figura 2.2 ilustra a representação do número 567 no soroban. Este instrumento de cálculo é utilizado sobre uma superfície plana e lido da esquerda para a direita. A versão mais comum possui 21 hastes (Alves; e Souza, 2024).

Figura 2.2 – Representação do número 567 no soroban



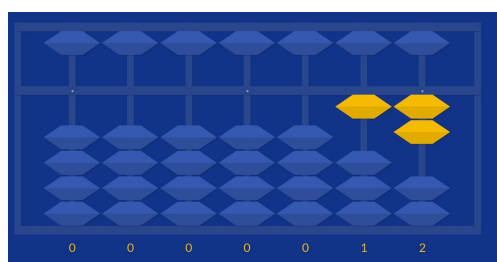
Fonte: Efuturo (2024).

O soroban é uma ferramenta visual e interativa que permite realizar operações básicas de forma intuitiva. De acordo com Alves e Souza (2024, n.p), “para somar no soroban, primeiro representamos o primeiro número da soma e depois vamos adicionando o segundo número nas contas da esquerda para direita”. Os Exemplos 2.3 a 2.6 ilustram o uso do soroban para efetuar somas.

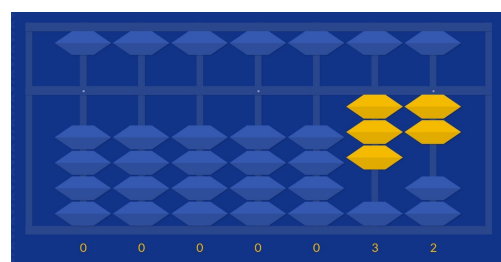
Exemplo 2.3. Qual é o resultado de $12 + 21$?

A Figura 2.3, mostra o passo a passo de como resolver esse cálculo usando o soroban. Primeiro representamos o número 12 no soroban – Figura 2.4(a). Em seguida, somamos 2 à haste das dezenas – Figura 2.4(b) – e 1 à haste das unidades – Figura 2.4 (c), obtendo o resultado 33.

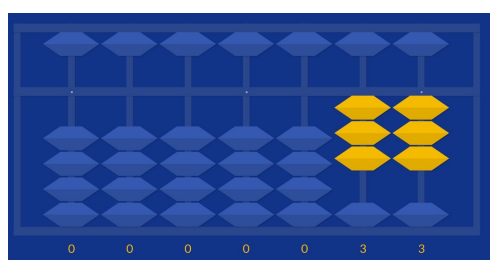
Figura 2.3 – Desenvolvimento do cálculo de $12 + 21$ no soroban: (a) representação do número 12; (b) adicionando 2 às dezenas; (c) adicionando 1 às unidades



(a)



(b)



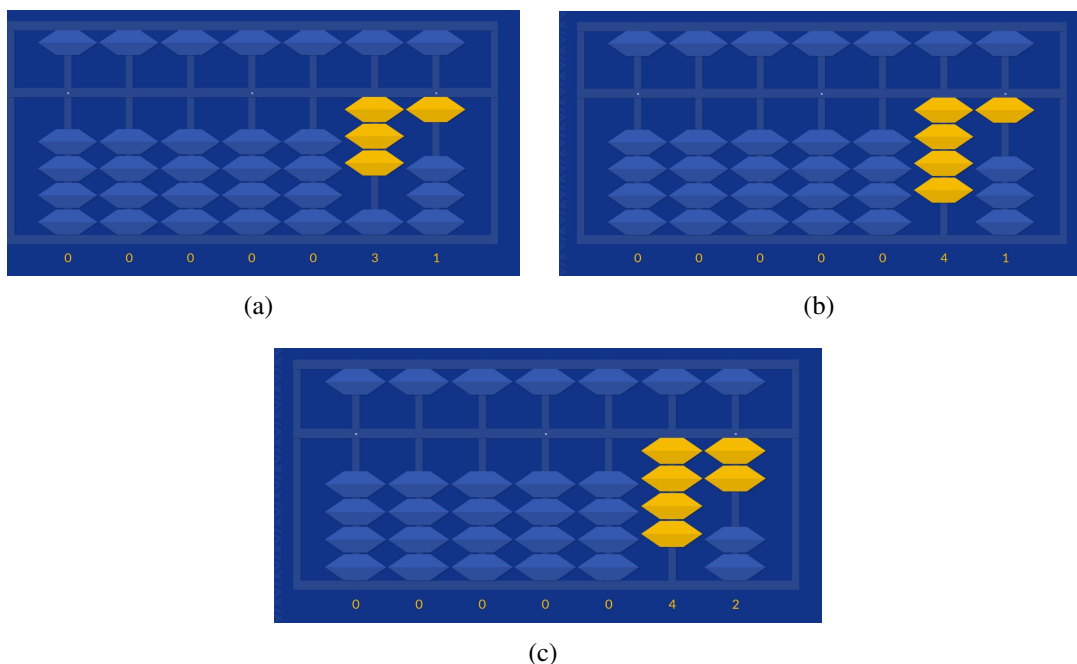
(c)

Fonte: Autora.

Exemplo 2.4. Qual é o resultado de $31 + 11$?

Primeiramente, representamos o número 31 no soroban – Figura 2.4(a). Na sequência, somamos 1 à haste das dezenas – Figura 2.4(b) – e 1 à haste das unidades – Figura 2.4(c), obtendo o resultado 42.

Figura 2.4 – Desenvolvimento do cálculo de $31 + 11$ no soroban: (a) representação do número 31; (b) adicionando 1 às dezenas; (c) adicionando 1 às unidades



Fonte: Autora.

Embora os Exemplos 2.3 e 2.4 tenham sido realizados de forma direta, sem complicações, é importante ressaltar que nem sempre esse processo é tão simples, como aquele ilustrado no Exemplo 2.5.

Exemplo 2.5. Qual é o resultado de $32 + 14$?

Seguindo o mesmo processo dos Exemplos 2.3 e 2.4, representaríamos o número 32 no soroban. Em seguida, adicionaríamos 1 às dezenas e, ao tentar adicionar 4 às unidades, encontraríamos um problema: não haveria contas suficientes para movimentar. É nesse ponto que introduzimos o conceito de números amigos no soroban.

No soroban, números amigos são pares de números cuja soma resulta em 5 ou 10. Esses pares facilitam significativamente as operações aritméticas. Ao realizar somas que exigem ajustes entre as colunas, os números amigos agilizam o processo, otimizando os cálculos (Rck, 2023). É importante ressaltar que os números amigos no soroban possuem significado diferente dos números amigáveis que abordaremos no Capítulo 5 deste trabalho.

O princípio geral consiste em retirar o número amigo do valor que se deseja somar e, em seu lugar, adicionar 5 ou 10 na haste correspondente. Iniciemos destacando os pares de números

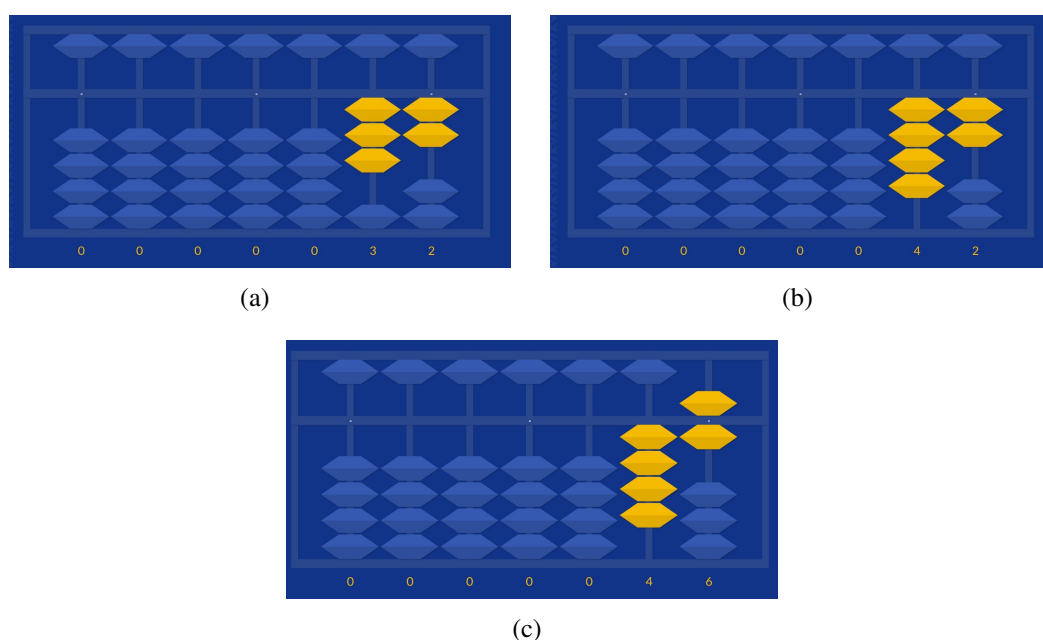
que, somados, resultam em 5: $1 + 4$; $2 + 3$; $3 + 2$; $4 + 1$. Portanto, formamos os pares de números amigos 1 e 4, e 2 e 3, sendo que a amizade entre os números é recíproca (Rck, 2023).

Por exemplo, ao tentar somar 3 em uma haste onde já há 2 contas ativas, não há contas suficientes disponíveis. Nesse caso, retira-se o 2, que é amigo do 3, e adiciona-se uma conta de 5, solucionando a operação.

Aplicando este método, podemos determinar no soroban o resultado da soma $32 + 14$.

A Figura 2.5 apresenta o passo a passo de como resolver o cálculo: primeiramente, representamos o número 32 no soroban – Figura 2.5(a); em seguida, somamos 1 à haste das dezenas – Figura 2.5(b) – e, para que consigamos adicionar 4 à haste das unidades – Figura 2.5(c), teremos que retirar o seu amigo, que no caso é o 1, e adicionar 5. Após o término desse processo, obtemos o resultado 46.

Figura 2.5 – Desenvolvimento do cálculo de $32 + 14$ no soroban: (a) representação do número 32; (b) adicionando 1 às dezenas; (c) adicionando 4 às unidades



Fonte: Autora.

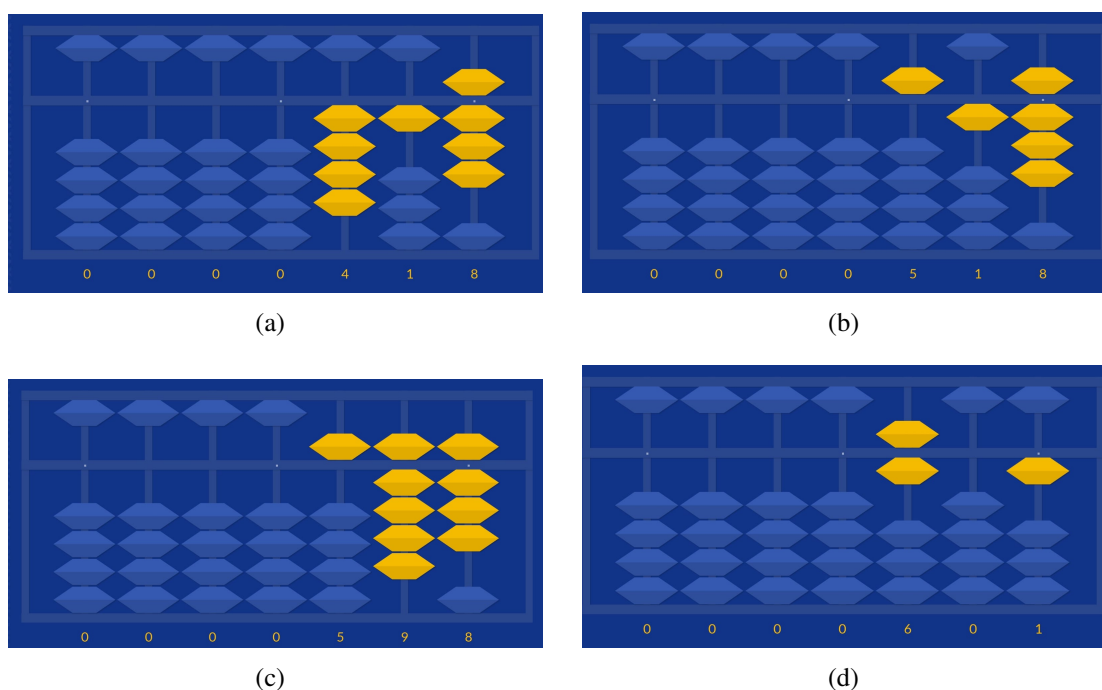
Exemplo 2.6. Qual é o resultado de $418 + 183$?

Para efetuar essa soma, precisamos dos pares de amigos cuja soma é 10: 1 e 9, 2 e 8, 3 e 7, 4 e 6, e 5 e 5, cuja amizade é recíproca.

Inicialmente, representamos o número 418 no soroban – Figura 2.6(a). Em seguida, adicionamos 1 à haste das centenas – Figura 2.6(b). Para adicionar esse 1, verificamos que $4 + 1 = 5$, ou seja, temos que utilizar os pares de amigos cuja soma é 5. Como o amigo de 1 é 4, retiramos 4 da haste das centenas e adicionamos 5 a ela. Posteriormente, adicionamos 8 à haste das dezenas – Figura 2.6(c). Para adicionar 3 à haste das unidades, temos que retirar o amigo 7, uma vez que $8 + 3 > 10$. Assim, retiramos 7 das unidades e passamos 1 para as dezenas.

Mas, para adicionarmos esse 1 às dezenas, temos que tirar seu amigo 9, pois $1 + 9 = 10$. Assim, retiramos 9 unidades das dezenas e então adicionamos 1 às centenas, obtendo assim o resultado 601 – Figura 2.6(d).

Figura 2.6 – Desenvolvimento do cálculo de $418 + 183$ no soroban: (a) representação do número 418; (b) adicionando 1 às centenas; (c) adicionando 8 às dezenas; (d) adicionando 3 às unidades



Fonte: Autora.

A escolha dos pares de amigos que serão utilizados em cada cálculo depende da soma dos números em cada uma das hastes. Para as hastes cuja soma seja maior do que 10, utilizamos os pares de amigos que resultam em 10. Caso contrário, utilizamos os pares que resultam em 5.

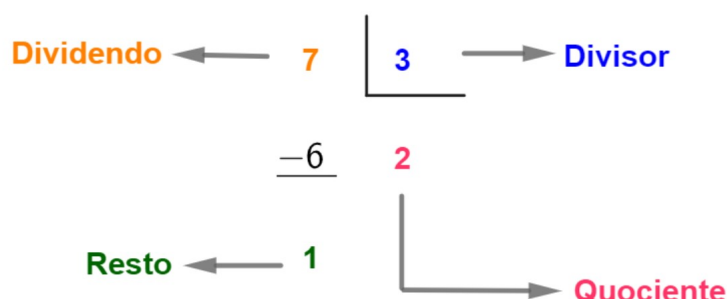
Os pares de números amigos no soroban desempenham um papel essencial não apenas na adição, mas também em outras operações fundamentais, como subtração, multiplicação e divisão. Essa compreensão se deve à propriedade dos números amigos de simplificar os cálculos ao reduzir a quantidade de ajustes manuais necessários durante as operações. Apesar de sua ampla aplicação, não detalharemos exemplos práticos das operações de subtração e multiplicação no presente texto, a fim de manter o foco no tema principal.

Após explorarmos a adição no soroban, vamos nos aprofundar na divisão. A divisão é, em essência, a operação inversa da multiplicação. Enquanto na multiplicação unimos grupos de igual tamanho, na divisão separamos um conjunto em grupos iguais. No soroban, essa dinâmica se torna visualmente clara. Ao dividir um número, estamos, na prática, respondendo à pergunta: *Quantos grupos de determinado tamanho posso formar com este número?* A representação das contas no ábaco nos permite visualizar essa separação de forma concreta.

Para entendermos melhor os exemplos de divisão no soroban, relembremos as denomi-

nações de cada um dos termos envolvidos em uma divisão. A Figura 2.7 ilustra os termos da divisão.

Figura 2.7 – Termos da divisão



Fonte: Marciano (2020).

Para garantir a eficiência e a precisão dos cálculos de divisão no soroban, a configuração inicial do ábaco é crucial. A forma como posicionamos os números influencia diretamente os resultados das operações. Embora existam diferentes abordagens, adotamos neste trabalho a configuração descrita a seguir.

- Escolha uma coluna de referência: use uma coluna central no soroban como ponto inicial para os cálculos. Isso ajuda a organizar os valores e a manter espaço suficiente para os quocientes e os restos.
- Posição do dividendo: coloque o dividendo no lado esquerdo do ábaco, utilizando as colunas específicas. Por exemplo, se o dividendo for 125, posicione o 1, o 2 e o 5 em colunas adjacentes à esquerda.
- Posicionamento do divisor: insira o divisor nas colunas à direita da representação do dividendo no soroban. Deixe o espaço de uma haste livre entre o último algarismo do dividendo e o primeiro algarismo do divisor. Também é possível realizar a divisão sem representar o divisor no soroban, mas para isso, é preciso memorizá-lo.
- Deixe espaço para o quociente: reserve algumas colunas à direita do divisor para registrar o quociente (o resultado da divisão). O quociente será construído durante os cálculos.
- Espaço para os restos: no mesmo espaço do dividendo, os restos intermediários serão manipulados conforme você avança no cálculo. Não é necessária uma área separada para isso, já que o dividendo será substituído progressivamente pelos restos.

Após a descrição da configuração, apresentamos alguns exemplos práticos da divisão no soroban – Exemplos 2.7 a 2.9.

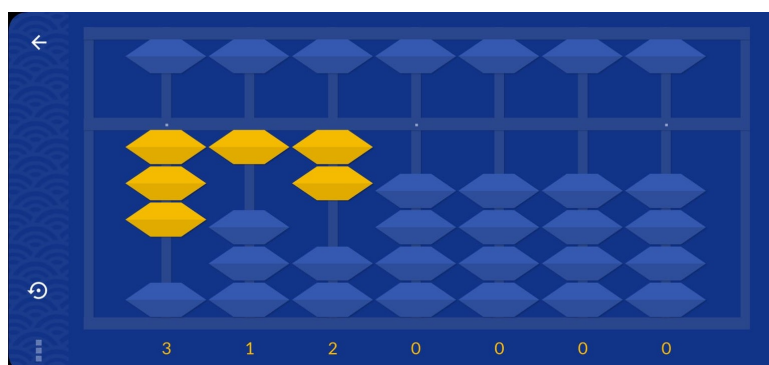
Exemplo 2.7. Qual é o resultado de $312 \div 2$?

Devido à limitação de hastes do soroban que estamos utilizando, optamos por não visualizar o divisor no ábaco. Assim, para realizar a divisão, memorizaremos o número pelo qual dividimos.

Segue o passo a passo de como resolver a divisão.

1º. Representamos o número 312 no soroban. A Figura 2.8 ilustra essa representação.

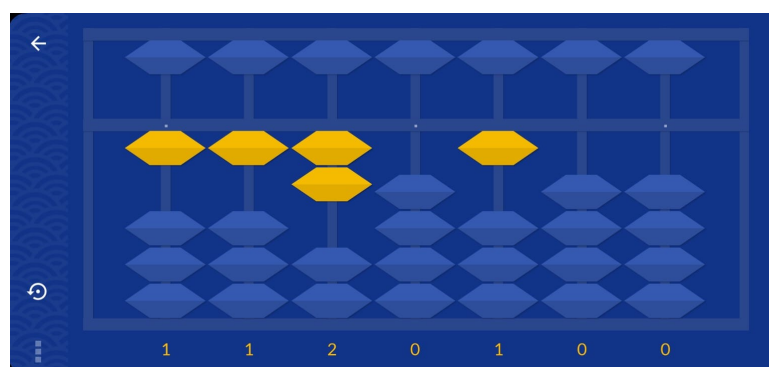
Figura 2.8 – Representação do número 312 no soroban



Fonte: Autora.

2º. Realizamos a divisão de 3 (centenas) por 2. Observemos que 3 é maior que 2; portanto, a divisão é possível. O resultado dessa divisão é 1, com resto 1. Esse quociente 1 é adicionado à casa das centenas do resultado final, uma vez que o 3 que estamos dividindo está localizado na casa das centenas do dividendo e o resto 1 é o que permanece na casa das centenas do dividendo – Figura 2.9.

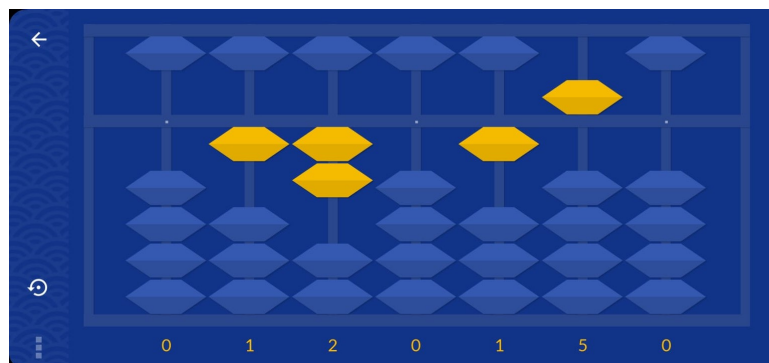
Figura 2.9 – Representação da divisão de 3 (centenas) por 2 no soroban



Fonte: Autora.

3º. Após a realização do 2º passo, ficamos com o número 112 representado no soroban. A próxima etapa é dividir 112 por 2. Inicialmente, dividimos 11 por 2. O resultado dessa divisão é 5, que posicionamos na casa das dezenas do quociente. Em seguida, multiplicamos esse 5 por 2, obtendo 10. Subtraímos esse 10 de 11, restando 1 unidade para a próxima etapa – Figura 2.10.

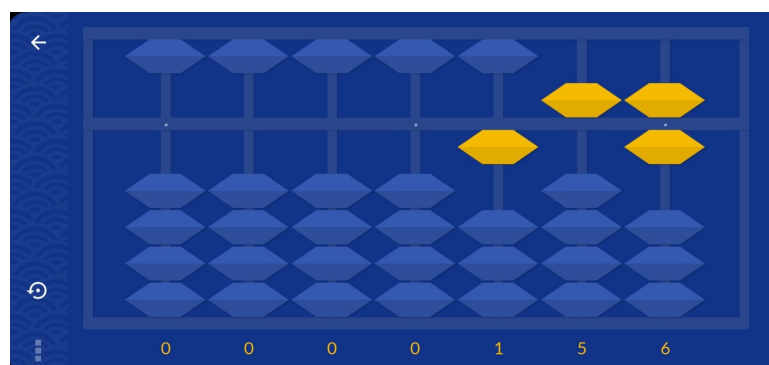
Figura 2.10 – Representação da divisão de 11 (dezenas) por 2 no soroban



Fonte: Autora.

- 4º. Para concluir o cálculo, dividimos os 12 restantes por 2, resultando em 6 sem deixar resto. Assim, o quociente da divisão de 312 por 2 é 156 – Figura 2.11.

Figura 2.11 – Quociente 156: resultado final da divisão $312 \div 2$

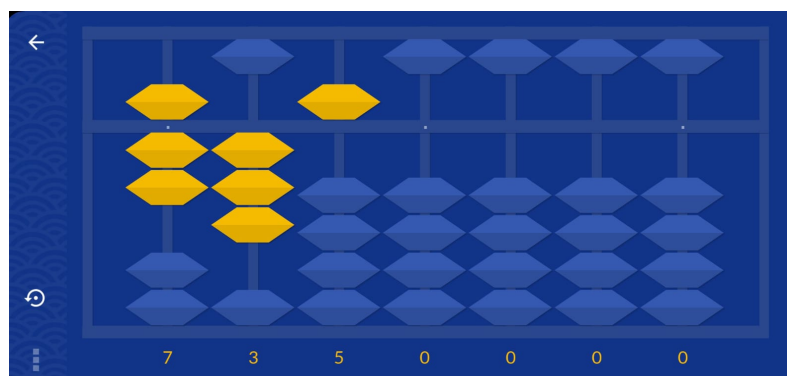


Fonte: Autora.

Exemplo 2.8. Qual é o resultado de $735 \div 5$?

- 1º. Representamos o número 735 no soroban. A Figura 2.12 ilustra essa representação.

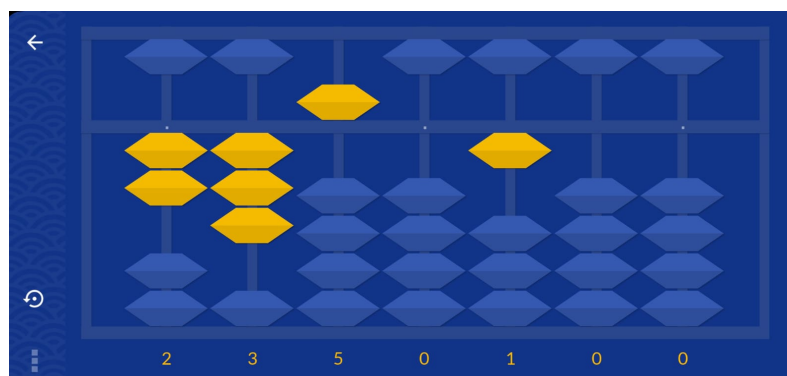
Figura 2.12 – Representação do número 735 no soroban



Fonte: Autora.

- 2º. Realizamos a divisão de 7 (centenas) por 5. Observemos que 7 é maior que 5; portanto, a divisão é possível. O resultado dessa divisão é 1, com resto 2. Esse quociente 1 é adicionado à casa das centenas do resultado final, uma vez que o 7 que estamos dividindo está localizado na casa das centenas do dividendo e o resto 2 é o que permanece na casa das centenas do dividendo – Figura 2.13.

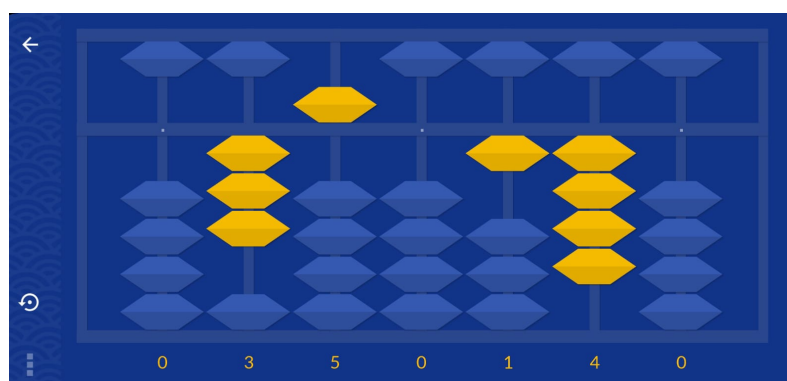
Figura 2.13 – Representação da divisão de 7 (centenas) por 5 no soroban



Fonte: Autora.

- 3º. Após a realização do 2º passo, ficamos com o número 235 representado no soroban. A próxima etapa é dividir 235 por 5. Inicialmente, dividimos 23 (dezenas) por 5. O resultado dessa divisão é 4, que posicionamos na casa das dezenas do quociente. Em seguida, multiplicamos esse 4 por 5, obtendo 20. Subtraímos esse 20 de 23, restando 3 dezenas para a próxima etapa – Figura 2.14.

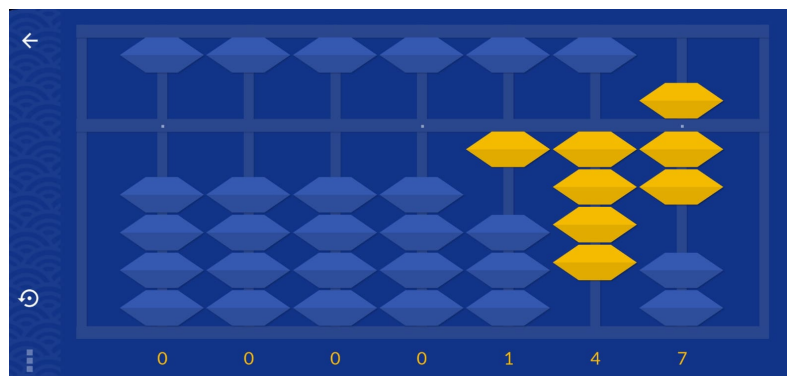
Figura 2.14 – Representação da divisão de 23 por 5 no soroban



Fonte: Autora.

- 4º. Para concluir o cálculo, dividimos os 35 restantes por 5, resultando em 7 sem deixar resto. Assim, o quociente completo da divisão de 735 por 5 é 147 – Figura 2.15.

Figura 2.15 – Quociente 147: resultado final da divisão $735 \div 5$



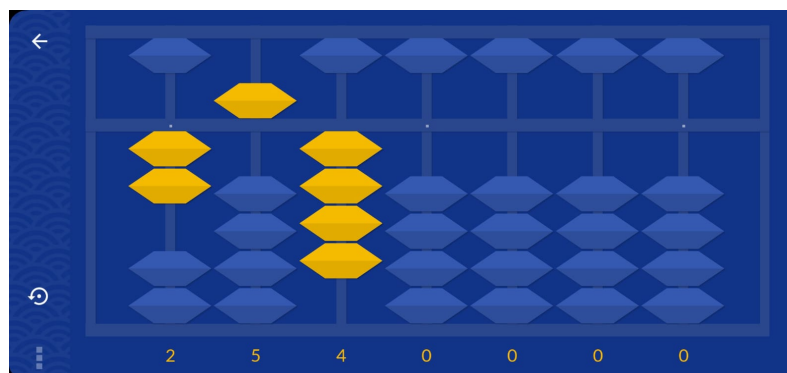
Fonte: Autora.

A divisibilidade está intimamente ligada ao conceito de resto na divisão. Quando dividimos um número por outro e sobra alguma quantidade, dizemos que a divisão não é exata e que o número não é divisível pelo divisor. No soroban, o resto da divisão é representado pelas contas que não puderam ser agrupadas. Ao observar essas contas restantes, podemos determinar se a divisão é exata ou não. O Exemplo 2.9 ilustra uma divisão que não é exata.

Exemplo 2.9. Qual é o resultado de $254 \div 3$?

1º. Representamos o número 254 no soroban. A Figura 2.16 ilustra essa representação.

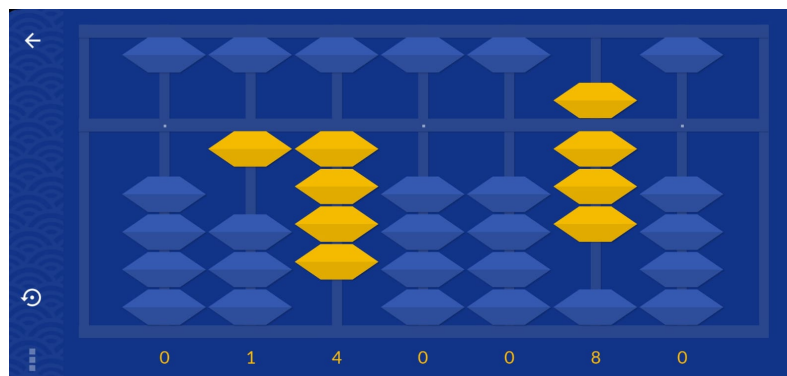
Figura 2.16 – Representação do número 254 no soroban



Fonte: Autora.

2º. Como 2 (centenas) é menor do que 3 (divisor), agrupamos com o 5 (dezenas), formando 25. Dividimos as 25 dezenas por 3, determinando 8 como quociente e 1 como resto. Esse quociente 8 é colocado na casa das dezenas do resultado, uma vez que dividimos 25 dezenas. O resto 1 permanece na casa das dezenas do dividendo para a próxima etapa da divisão – Figura 2.17.

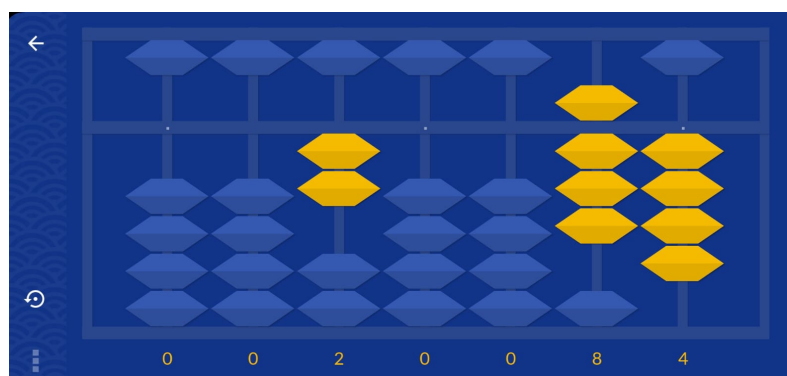
Figura 2.17 – Representação da divisão de 25 por 3 no soroban



Fonte: Autora.

- 3º. Continuando o processo, dividimos as 14 unidades restantes por 3. O quociente dessa divisão é 4, pois 4 multiplicado por 3 resulta em 12. Subtraindo 12 de 14, obtemos um resto 2. Assim, o quociente da divisão de 254 por 3 é 84 com resto igual a 2 – Figura 2.18.

Figura 2.18 – Representação da divisão de 14 por 3 no soroban



Fonte: Autora.

O soroban é muito mais que uma simples calculadora: ele é uma ferramenta visual que torna a Matemática, especialmente a divisibilidade, mais intuitiva. Essa ferramenta transforma os critérios de divisibilidade de regras abstratas em uma experiência concreta e visual. Ao manipular as contas, os estudantes estabelecem uma conexão mais profunda entre os números e suas propriedades, tornando o aprendizado mais intuitivo. Essa abordagem, além de facilitar a compreensão, estimula o desenvolvimento de habilidades como a observação, a análise e a resolução de problemas.

Podemos aplicar os critérios de divisibilidade no soroban?

- Divisibilidade por 2 e 5: uma questão de olhar.

Verificar se um número é divisível por 2 ou 5 no soroban é simples: basta observar o último dígito. Se ele for par (0, 2, 4, 6 ou 8), o número é divisível por 2; se terminar em 0 ou 5, a divisibilidade por 5 está garantida. A representação visual dos dígitos no soroban torna essa verificação imediata.

- Divisibilidade por 3 e 9: a soma dos dígitos.

Para determinar a divisibilidade por 3 ou 9, somamos os valores representados por cada conta do soroban. Se essa soma for divisível por 3 ou 9, respectivamente, o número original também será. A visualização dos dígitos no ábaco facilita a realização dessa soma mental.

- Divisibilidade por 4 e 8: olhando para os últimos dígitos.

A divisibilidade por 4 e 8 depende dos dois ou três últimos dígitos do número, respectivamente. Se esses dígitos formarem um número divisível por 4 ou 8, o número original também será. A flexibilidade do soroban permite manipular esses dígitos de forma eficiente para essa verificação.

- Divisibilidade por 6: a combinação perfeita.

Para ser divisível por 6, um número precisa ser divisível por 2 e por 3 simultaneamente. No soroban, aplicamos os critérios anteriores para verificar ambas as condições.

Materiais como o soroban são pontes que conectam o abstrato ao concreto no ensino da Matemática. Ao transformar conceitos complexos em representações tangíveis, essas ferramentas tornam a aprendizagem mais acessível, especialmente para aqueles que têm dificuldades em visualizar ideias abstratas. Por meio da manipulação do soroban, os alunos constroem uma compreensão mais profunda dos números e das operações, desenvolvendo habilidades como o raciocínio lógico e a resolução de problemas, essenciais para a Matemática.

No soroban, os números amigos são uma ferramenta para cálculos mais rápidos. Já na teoria dos números, se referem a pares de números com uma propriedade específica: a soma dos divisores próprios de um é igual ao outro. Essa diferença evidencia a diversidade de significados que um mesmo termo pode adquirir nas diferentes áreas da Matemática. Mesmo com significados diferentes, ambos os conceitos demonstram a riqueza e a beleza dos padrões numéricos, revelando a dualidade da Matemática: prática e teórica.

2.4.1 SIMPLE SOROBAN

O *simple soroban*, a tecnologia digital utilizada para o desenvolvimento da Seção 2.4, é um aplicativo gratuito para Android que simula um ábaco japonês, também conhecido como soroban. Com ele, você pode aprender e praticar operações matemáticas como adição, subtração, multiplicação (de 1 e 2 dígitos) e divisão, tudo de forma interativa e divertida.

O aplicativo oferece dois modos principais:

- Modo Livre: permite que você use o ábaco livremente, explorando suas funcionalidades e praticando diferentes cálculos;
- Modo Desafio: apresenta desafios matemáticos com três níveis de dificuldade (fácil, médio e difícil) para você testar suas habilidades.

Além disso, o *simple soroban* inclui tutoriais básicos que explicam os conceitos fundamentais do ábaco e como realizar as operações matemáticas. Desenvolvido por Bruno Takahashi Carvalhas de Oliveira, o aplicativo pode ser baixado no Google Play Store através do link: <https://play.google.com/store/apps/details?id=br.net.btco.soroban>.

3 NÚMEROS PRIMOS

O conceito de número é uma das invenções fundamentais da humanidade. O desenvolvimento dos números foi um processo longo e complexo, envolvendo várias culturas no decorrer de milênios. Sumérios, babilônios, egípcios, chineses e hindus são exemplos de civilizações antigas que contribuíram de maneira significativa para o advento dos números (Boyer, 1974).

O surgimento dos números é uma história de inovação contínua e intercâmbio cultural. Cada civilização contribuiu com avanços únicos, culminando no sistema decimal posicional que usamos hoje. Este desenvolvimento não só facilitou os cálculos aritméticos, mas também abriu caminho para avanços significativos em todas as áreas da Matemática.

Um exemplo importante são os números primos. Caracterizados na Definição 3.1, eles têm fascinado matemáticos ao longo dos séculos devido à sua simplicidade e, ao mesmo tempo, à sua complexidade. Desde os tempos antigos até os dias atuais, a exploração dos números primos tem sido um campo de intensa investigação matemática, revelando profundas conexões com outras áreas da ciência e com aplicações práticas essenciais.

Definição 3.1. *Um número inteiro p , com $p > 1$, é um número primo se possuir exatamente dois divisores positivos: 1 e p .*

Partindo da definição, Rizel (2014, p. 8) complementa: “O número 1, só possui um divisor, ele mesmo. Não sendo, portanto, um número primo. Todos os demais números inteiros maiores do que 1 e não primos, possuem mais de dois divisores. Eles são chamados de números compostos, logo, poderão ser fatorados em seus elementos constituintes.”

De acordo com Andrade (2018b), indícios apontam que a Escola Pitagórica, fundada por Pitágoras por volta de 530 a.C., já compreendia e investigava os números primos, embora não utilizasse essa terminologia específica. Os pitagóricos designavam os números primos como números lineares e os números compostos como números não lineares, representando estes últimos por retângulos para sugerir que eram formados pelos primeiros. Os pitagóricos acreditavam que os números tinham propriedades místicas.

Eves (2011) destaca que a importância dos números primos foi reconhecida desde a antiguidade. De acordo com o autor, os primeiros registros de estudos sobre números primos vêm dos matemáticos gregos, particularmente Euclides, que por volta de 300 a.C. demonstrou que há infinitos números primos em sua obra *Os elementos* (Euclides, 2009). A prova de Euclides é considerada um marco na história da Matemática e mostra a beleza dos argumentos matemáticos.

Outro matemático grego, Erastóstenes de Cirene, assim como Euclides, focou seus estudos nos números primos e desenvolveu, por volta de 200 a.C., o Crivo de Erastóstenes, uma

tabela que facilita a identificação de números primos e é usada até hoje no Ensino Fundamental devido à sua simplicidade e eficácia (Andrade, 2018b).

Andrade (2018b, p. 22) ainda aponta que:

Mas foi somente por volta de 500 d.C. que os números primos saíram da Grécia e foram sendo estudados em outras partes do mundo. O romano Boethius, no seu livro *De Institutione Arithmetica*, empregou pela primeira vez a expressão *númerus primus*. Durante a Idade Média, esse livro foi praticamente a única fonte de estudo sobre o tema.

No início do século XVII, Pierre de Fermat (1607–1655) fez avanços significativos na teoria dos números primos ao provar uma conjectura de Albert Girard (1595–1632), estabelecendo que todo número primo pode ser expresso como a soma dos quadrados de dois números inteiros de um único modo. Além disso, Fermat desenvolveu métodos para escrever qualquer número inteiro positivo como a soma de quatro quadrados, introduziu uma nova técnica para fatorar números primos grandes e formulou o Teorema 3.1 (Bayer; Reis, 2020).

Teorema 3.1. (*Pequeno Teorema de Fermat*) *Se p é um número primo, então para qualquer número inteiro a , com $(a, p) = 1$, tem-se que $a^{p-1} \equiv 1 \pmod{p}$.*

O Teorema 3.1 “[...]” é de fundamental importância em teoria dos números, assim como em outros ramos da Matemática, e a teoria dos números do século XIX foi fortemente impulsionada pelos grandes resultados de Fermat nessa área” (Padilha, 2013, p. 5).

Nos séculos XVIII e XIX, a teoria dos números primos foi enriquecida por muitas descobertas e avanços. Matemáticos como Johann Carl Friedrich Gauss (1777–1855) e Leonhard Paul Euler (1707–1783) fizeram contribuições significativas, desenvolvendo fórmulas e teoremas que aprofundaram o entendimento dos números primos. Gauss, por exemplo, formulou a conjectura sobre a distribuição dos números primos que mais tarde se tornaria a base para a hipótese de Riemann (Stewart, 2014).

Sauty (2008) descreve que a hipótese de Riemann, proposta por Bernhard Riemann (1826–1866) em 1859, está relacionada à distribuição dos números primos e continua sem solução até hoje. Muitos matemáticos acreditam que a prova (ou refutação) desta hipótese teria um impacto profundo na Matemática.

Os números primos, com sua simplicidade fundamental e complexidade inerente, continuam a ser um tema central na Matemática. Desde as primeiras provas de Euclides até os desafios modernos como a hipótese de Riemann, a busca por compreender os números primos tem levado a muitos dos mais profundos avanços na Matemática. Suas aplicações em criptografia, teoria dos números e outras áreas científicas mostram que, embora antigos, os números primos permanecem tão relevantes e intrigantes como sempre.

3.1 TEOREMA FUNDAMENTAL DA ARITMÉTICA

O Teorema Fundamental da Aritmética (TFA) é um dos pilares da teoria dos números e afirma que todo número inteiro maior que um pode ser decomposto de maneira única como um produto de números primos, a menos da ordem dos fatores. Segundo Fonseca, Monteiro e Fonseca (2021), o TFA foi formalizado por Gauss em sua obra *Disquisitiones Arithmeticae* publicada em 1801. Para Sautoy (2008), o TFA destaca os números primos como blocos de construção essenciais dos inteiros. A unicidade dessa decomposição é crucial para várias áreas da Matemática. Conforme ressaltado por Apostol (1984), essa propriedade permite uma compreensão profunda da estrutura dos números inteiros, proporcionando uma base sólida para muitos desenvolvimentos matemáticos subsequentes.

Antes de abordarmos formalmente o TFA, torna-se necessário analisar os resultados estabelecidos na Proposição 3.1 (Hefez, 2022, p. 118) e no Corolário 3.1 (Hefez, 2022, p. 119).

Proposição 3.1. (*Lema de Euclides*) Sejam a, b e $p \in \mathbb{Z}$, com p primo. Se $p \mid ab$, então $p \mid a$ ou $p \mid b$.

Demonstração. Sejam $a, b \in \mathbb{Z}$ tais que $p \mid ab$.

Se $p \mid a$, a demonstração está concluída.

Se $p \nmid a$, então $(a, p) = 1$ e, como $p \mid ab$, temos que existe $r \in \mathbb{Z}$ tal que

$$ab = rp. \quad (3.1)$$

Como $(p, a) = 1$, então, pelo teorema de B́achet-Bézout¹, existem $m, n \in \mathbb{Z}$ tais que

$$ma + np = 1. \quad (3.2)$$

Multiplicando por b ambos os lados da igualdade (3.2), temos que

$$mab + npb = b. \quad (3.3)$$

Substituindo (3.1) em (3.3), obtemos que

$$b = mrp + npb = p(mr + nb).$$

Logo, $p \mid b$.

□

Corolário 3.1. Se $p, p_1, \dots, p_n$ são números primos e $p \mid (p_1 \cdots p_n)$, então $p = p_i$ para algum $i = 1, \dots, n$.

¹ Dados $a, b \in \mathbb{Z}$, existem $x, y \in \mathbb{Z}$ tais que $ax + by = (a, b)$.

Demonstração. Vamos provar por indução sobre n .

Para $n = 1$, é imediato.

Suponhamos que a afirmação é verdadeira para $n = k$, com $k \in \mathbb{N}$ e $k \geq 2$, ou seja,

$$\text{se } p \mid (p_1 \cdots p_k), \text{ então } p \mid p_i \text{ para algum } i = 1, 2, 3, \dots, k.$$

Mostraremos que a afirmação é válida para $n = k + 1$. Neste caso, temos que

$p \mid (p_1 p_2 \cdots p_{k+1})$ ou equivalentemente $p \mid (p_1 \cdots p_k) p_{k+1}$. Pela Proposição 3.1, $p \mid (p_1 \cdots p_k)$ ou $p \mid p_{k+1}$ (HI), $p \mid p_i$ para algum $i (1 \leq i \leq k)$.

Assim, em qualquer dos casos, p divide um dos inteiros $p_1, p_2, \dots, p_{k+1}$. Logo, existe um i , com $1 \leq i \leq k + 1$, tal que $p \mid p_i$. Pelo princípio da indução temos que, para todo $n \in \mathbb{N}$, se $p \mid p_1 \cdots p_n$ então $p \mid p_i$, para algum $i = 1, 2, \dots, n$. Como os únicos divisores positivos de p_i são 1 e p_i , segue que $p = 1$ ou $p = p_i$. Mas, $p > 1$ porque p é primo. Portanto, $p = p_i$.

□

Após a apresentação da Proposição 3.1 e do Corolário 3.1, podemos demonstrar o Teorema 3.2 (Hefez, 2022, p. 119).

Teorema 3.2. (TFA) *Todo número natural maior do que um ou é primo ou se escreve de modo único (a menos da ordem dos fatores) como um produto de números primos.*

Demonstração. Usaremos a segunda forma do princípio de indução. Se $n = 2$, o resultado é obviamente verificado.

Suponhamos o resultado válido para todo número natural menor do que n (HI) e vamos provar que vale para n . Se o número n é primo, nada temos a demonstrar. Suponhamos, então, que n seja composto. Logo, existem números naturais n_1 e n_2 tais que $n = n_1 n_2$, com $1 < n_1 < n$ e $1 < n_2 < n$. Pela hipótese de indução, temos que existem números primos $p_1, \dots, p_r$ e $q_1, \dots, q_s$ tais que $n_1 = p_1 \cdots p_r$ e $n_2 = q_1 \cdots q_s$. Portanto, $n = p_1 \cdots p_r q_1 \cdots q_s$.

Vamos, agora, provar a unicidade da escrita. Suponha que tenhamos $n = p_1 \cdots p_r = q_1 \cdots q_s$, onde os p_i e os q_j são números primos. Como $p_1 \mid (q_1 \cdots q_s)$, temos pelo Corolário 3.1 que $p_1 = q_j$ para algum j , que, após reordenamento de $q_1, \dots, q_s$, podemos supor que seja q_1 . Portanto,

$$p_2 \cdots p_r = q_2 \cdots q_s.$$

Como $p_2 \cdots p_r < n$, a hipótese de indução acarreta que $r = s$ e os p_i e q_j são iguais aos pares.

□

O Teorema 3.2 constitui a base da Aritmética e da Teoria dos Números. Sua prova reforça a compreensão sobre a estrutura dos números inteiros e suas propriedades, e suas implicações

vão além da teoria, impactando áreas práticas. Assim, esse teorema consolida os fundamentos matemáticos, promovendo avanços contínuos na Matemática.

3.2 TEOREMA DE DIRICHLET: PRIMOS EM PROGRESSÃO ARITMÉTICA

O Teorema 3.3, proposto pelo matemático alemão Johann Peter Gustav Lejeune Dirichlet (1805–1859), é um resultado significativo na Teoria dos Números. Esse teorema estabelece que existem infinitos números primos em qualquer progressão aritmética da forma

$$a, a + d, a + 2d, a + 3d, a + 4d, \dots$$

com $d \geq 2$, $a \neq 0$ e $(a, d) = 1$ (Ribenoim, 2014 *apud* Silva Júnior, 2017).

A relevância do Teorema 3.3 não se limita à confirmação da existência infinita de números primos em progressões aritméticas, mas também na introdução de métodos científicos inovadores na Teoria dos Números, com destaque para o uso das séries L de Dirichlet. Estas séries são fundamentais na prova do teorema, permitindo que se analise a distribuição dos números primos utilizando Análise Complexa. A aplicação dessas séries, em conjunto com os caracteres de Dirichlet, estabelece uma conexão profunda entre Análise e Teoria dos Números (Apostol, 1984).

Teorema 3.3. *Em uma progressão aritmética (PA) de números naturais, com primeiro termo e razão primos entre si, existem infinitos números primos.*

De acordo com Hefez (2022, p. 140), a demonstração do Teorema 3.3 “[...] é bem difícil e pertence à teoria analítica dos números”. Sendo assim, apresentamos somente alguns casos particulares para $n \in \mathbb{N}$ decorrentes do teorema.

O primeiro caso particular – Proposição 3.2, trata da sequência dos números ímpares $2n + 1$ (Silva Júnior, 2017, p. 12).

Proposição 3.2. *Na progressão aritmética $1, 3, 5, \dots, 2n + 1, \dots$ existem infinitos números primos.*

Demonstração. Todo número primo maior do que 2 é ímpar. Como existem infinitos números primos e na sequência $1, 3, 5, \dots, 2n + 1, \dots$ estão todos os números ímpares, então existem infinitos primos na progressão aritmética $S = \{2n + 1\}_{n \in \mathbb{N}}$.

□

O segundo caso particular – Proposição 3.3, apresenta a sequência de números da forma $4n + 3$ (Hefez, 2022, p. 140).

Proposição 3.3. *Na progressão aritmética $3, 7, 11, 15, \dots, 4n + 3, \dots$ existem infinitos números primos.*

Demonstração. Inicialmente, notemos que todo primo ímpar é da forma $4n + 1$ ou $4n + 3$.

Em seguida, observemos que o conjunto $A = \{4n + 1; n \in \mathbb{N}\}$ é fechado multiplicativamente. De fato,

$$(4n + 1)(4n' + 1) = 4(4nn' + n + n') + 1.$$

Suponhamos agora, por absurdo, que haja apenas um número finito de números primos $3 < p_1 < \dots < p_k$ da forma $4n + 3$. Portanto, o número $a = 4(p_1 p_2 \dots p_k) + 3$ não é divisível por nenhum dos números primos $3, p_1, \dots, p_k$ e, conseqüentemente, sua decomposição em fatores primos só pode conter primos da forma $4n + 1$. Assim, concluiríamos que a é da forma $4n + 1$, o que é uma contradição, pois a é da forma $4n + 3$. □

As Proposições 3.4 e 3.5 estabelecem que há infinitos números primos nas sequências $6n + 5$ e $3n + 2$, respectivamente (Silva Júnior, 2017, p. 13-14).

Proposição 3.4. *Na progressão aritmética $5, 11, 17, 23, \dots, 6n + 5, \dots$ existem infinitos números primos.*

Demonstração. Observemos inicialmente que todo número ímpar é de uma das formas $6n + 1$, $6n + 3$ ou $6n + 5$. Como todos os números da forma $6n + 3 = 3(2n + 1)$ são divisíveis por 3, todo primo ímpar, diferente de 3, é da forma $6n + 1$ ou $6n + 5$.

Em seguida, de modo análogo ao caso da Proposição 3.3, notemos que o conjunto $B = \{6n + 1; n \in \mathbb{N}\}$ é fechado multiplicativamente. Agora suponhamos, por absurdo, que haja somente uma quantidade finita de primos da forma $6n + 5$, isto é $5 < p_1 < p_2 < \dots < p_k$, e defina

$$b = 6(p_1 p_2 \dots p_k) + 5.$$

Desta forma, b não é divisível por nenhum dos primos $2, 3, 5, p_1, p_2, \dots, p_k$. Logo, sua decomposição em fatores primos só pode conter primos da forma $6n + 1$. Como o conjunto $B = \{6n + 1; n \in \mathbb{N}\}$ é fechado multiplicativamente, então b é da forma $6n + 1$, o que é um absurdo, pois b é claramente da forma $6n + 5$. □

Proposição 3.5. *Na progressão aritmética $2, 5, 8, 11, \dots, 3n + 2, \dots$ existem infinitos números primos.*

Demonstração. Observemos que todo primo, diferente de 3, é da forma $3n + 1$ ou $3n + 2$.

Suponhamos, por absurdo, que haja uma quantidade finita de primos da forma $3n + 2$, isto é $2 < p_1 < p_2 < \dots < p_k$, e seja

$$c = 3(p_1 p_2 \dots p_k) + 2.$$

Como c não é divisível por nenhum dos primos $2, 3, p_1, p_2, \dots, p_k$, sua decomposição em fatores primos só contém primos da forma $3n + 1$. E, novamente, como $C = \{3n + 1; n \in \mathbb{N}\}$ é fechado multiplicativamente, então c é da forma $3n + 1$, o que é um absurdo, pois c é da forma $3n + 2$.

□

Ainda sobre progressões aritméticas com infinitos números primos, apresentamos na Proposição 3.6 o caso da progressão $4n + 1$. Contudo, “[...] mostrar que existem infinitos primos da forma $4n + 1$ é um pouco mais sutil” (Hefez, 2022, p. 140). Para tanto, precisamos provar inicialmente o Lema 3.1 (Hefez, 2022, p. 140-141).

Lema 3.1. *Se $x \in \mathbb{N}$, com $x \geq 2$, então todo divisor ímpar de $x^2 + 1$ é da forma $4n + 1$.*

Demonstração. Provaremos que todo divisor primo $p \neq 2$ de $x^2 + 1$ é da forma $4n + 1$. Já demonstramos, no decorrer da Proposição 3.3, que o conjunto $A = \{4n + 1; n \in \mathbb{N}\}$ é fechado multiplicativamente.

Suponhamos, então, que $p \mid (x^2 + 1)$, com p primo maior do que 2. Temos assim que $\frac{p-1}{2} \in \mathbb{N}$ e, para algum $\lambda \in \mathbb{N}$, que $x^2 + 1 = \lambda p$. Consequentemente,

$$x^2 = \lambda p - 1. \quad (3.4)$$

Elevando à potência $\frac{p-1}{2}$ ambos os lados da igualdade (3.4), temos pelo binômio de Newton, para alguns $\mu, \mu' \in \mathbb{N}$, que:

$$x^{p-1} = (x^2)^{\frac{p-1}{2}} = (\lambda p - 1)^{\frac{p-1}{2}} = \begin{cases} \mu p + 1, & \text{se } \frac{p-1}{2} \text{ é par} \\ \mu' p - 1, & \text{se } \frac{p-1}{2} \text{ é ímpar} \end{cases}.$$

No caso ímpar, subtraindo 1 de ambos os lados de $x^{p-1} = \mu' p - 1$, obtemos que

$$x^{p-1} - 1 = \mu' p - 2. \quad (3.5)$$

Como $p \mid (x^2 + 1)$, segue que $p \nmid x$. Logo, pelo Pequeno Teorema de Fermat, temos que $p \mid (x^{p-1} - 1)$ e, consequentemente, por (3.5), $p \mid 2$, o que é uma contradição.

Portanto, a única alternativa possível é que $\frac{p-1}{2}$ seja par, o que implica que p é da forma $4n + 1$.

□

Proposição 3.6. *Na progressão aritmética $1, 5, 9, \dots, 4n + 1, \dots$ existem infinitos números primos.*

Demonstração. Suponhamos, por absurdo, que haja um número finito $p_1, \dots, p_k$ de primos na forma $4n + 1$. Consideremos o número

$$a = 4p_1^2 \cdots p_k^2 + 1.$$

Como $p_i \nmid a$, para todo $i = 1, \dots, k$, segue que todo divisor primo de a é da forma $4n + 3$, o que é um absurdo ante o Lema 3.1. $\square$

Resumindo, apresentamos na Tabela 3.1 algumas sequências aritméticas com os seus dez primeiros números primos. Essas progressões, caracterizadas por um termo inicial e uma razão – diferença entre dois termos consecutivos de uma sequência, ilustram a distribuição dos números primos nas sequências.

Tabela 3.1 – Sequências aritméticas com os 10 primeiros termos primos

PROGRESSÃO ARITMÉTICA	PRIMEIRO TERMO	RAZÃO	10 PRIMEIROS PRIMOS DA SEQUÊNCIA
$2n + 1$	1	2	3, 5, 7, 11, 13, 17, 19, 23, 29, 31,...
$3n + 1$	1	3	7, 13, 19, 31, 37, 43, 61, 67, 73, 79,...
$3n + 2$	2	3	2, 5, 11, 17, 23, 29, 41, 47, 53, 59,...
$4n + 1$	1	4	5, 13, 17, 29, 37, 41, 53, 61, 73, 89,...
$4n + 3$	3	4	3, 7, 11, 19, 23, 31, 43, 47, 59, 67,...
$5n + 1$	1	5	11, 31, 41, 61, 71, 101, 131, 151, 181, 191,...
$5n + 3$	3	5	3, 13, 23, 43, 53, 73, 83, 103, 113, 163,...
$5n + 7$	7	5	7, 17, 37, 47, 67, 97, 107, 127, 137, 157,...
$5n + 9$	9	5	19, 29, 59, 79, 89, 109, 139, 149, 179, 199,...
$6n + 5$	5	6	5, 11, 17, 23, 29, 41, 47, 53, 59, 71,...
$7n + 1$	1	7	29, 43, 71, 113, 127, 197, 211, 239, 281, 337,...
$7n + 3$	3	7	3, 17, 31, 59, 73, 101, 157, 199, 227, 241,...
$7n + 5$	5	7	5, 19, 47, 61, 89, 103, 131, 173, 229, 257, ...
$7n + 9$	9	7	23, 37, 79, 107, 149, 163, 191, 233, 317, 331,...
$8n + 1$	1	8	17, 41, 73, 89, 97, 113, 137, 193, 233, 241,...
$8n + 3$	3	8	3, 11, 19, 43, 59, 67, 83, 107, 131, 139,...
$8n + 5$	5	8	5, 13, 29, 37, 53, 61, 101, 109, 149, 157,...
$8n + 7$	7	8	7, 23, 31, 47, 71, 79, 103, 127, 151, 167,...
$9n + 1$	1	9	19, 37, 73, 109, 127, 163, 181, 199, 271, 307,...
$9n + 2$	2	9	2, 11, 29, 47, 83, 101, 137, 173, 191, 227,...
$9n + 4$	4	9	13, 31, 67, 103, 139, 157, 193, 211, 229, 283,...
$9n + 5$	5	9	5, 23, 41, 59, 113, 131, 167, 239, 257, 293,...
$9n + 7$	7	9	7, 43, 61, 79, 97, 151, 223, 241, 277, 313,...
$9n + 8$	8	9	17, 53, 71, 89, 107, 179, 197, 233, 251, 269,...
$11n + 1$	1	11	23, 67, 89, 199, 331, 353, 397, 419, 463, 617,...
$11n + 2$	2	11	2, 13, 57, 79, 101, 167, 211, 233, 277, 409,...
$11n + 3$	3	11	3, 47, 113, 157, 179, 223, 311, 421, 443, 487,...
$11n + 4$	4	11	37, 59, 103, 191, 257, 367, 389, 433, 499, 521,...

Fonte: Autora.

Durante a elaboração da Tabela 3.1, que reúne os primeiros 10 números primos pertencentes a diversas progressões aritméticas, observamos que algumas dessas progressões apresentavam os mesmos primos nos termos iniciais. Foi o caso, por exemplo, das progressões da forma $3n + 1$, $6n + 1$ e $6n + 7$, bem como $5n + 1$ e $10n + 1$. Embora não tenhamos investigado o comportamento

para todos os números primos, essa coincidência nos primeiros termos motivou a decisão de incluir apenas uma entre essas progressões na tabela, com o objetivo de evitar redundâncias na apresentação dos dados.

É importante destacar que tais coincidências ocorrem, em parte, porque algumas dessas progressões são subconjuntos de outras. Por exemplo, a progressão $6n + 1$ é um subconjunto da progressão $3n + 1$, pois todo número da forma $6n + 1$ também satisfaz a forma $3m + 1$, com $m = 2n$. Esse tipo de relação entre progressões contribui para a sobreposição de primos em seus primeiros termos, evidenciando padrões interessantes na distribuição dos números primos em sequências aritméticas diferentes, ainda que não generalizáveis sem demonstração formal.

Os primos em progressões aritméticas revelam uma dinâmica fascinante na Teoria dos Números, mostrando que padrões simples podem resultar em complexidades inesperadas. A regularidade das progressões, caracterizada por uma razão constante entre os termos consecutivos, contrasta com a aparente irregularidade dos números primos, criando um campo intrigante para a exploração matemática.

3.3 TEOREMA DE OURO

As primeiras anotações sobre a Lei da Reciprocidade Quadrática foram realizadas por Fermat, que se dedicava à Matemática como um hobby. Seus estudos e descobertas eram abordados de maneira informal, pois ele tinha como costume fazer suas anotações em páginas de livros e em cartas trocadas com outros matemáticos. Apesar dessa abordagem singular, suas contribuições foram fundamentais para o avanço da demonstração da reciprocidade quadrática (Araújo, 2013).

De acordo com Araújo (2013), embora Fermat tenha sido o primeiro a fazer anotações sobre o tema, foi Euler quem deu continuidade ao trabalho, provando as conjecturas de Fermat e expandindo significativamente o conhecimento sobre a reciprocidade quadrática. Outro matemático que se dedicou ao estudo da reciprocidade quadrática foi Adrien-Marie Legendre (1752–1833), contudo este, assim como Euler, não conseguiu prová-la.

A Lei da Reciprocidade Quadrática, conjecturada inicialmente por Euler e Legendre e demonstrada por Gauss em 1796 (Hefez, 2022) e presente em seu livro *Disquisitiones Arithmeticae* publicado em 1801 (Ore, 1948), é considerada um dos resultados mais importantes na Teoria dos Números. Segundo Oliveira e Andrade (2020, p. 434-435):

Nesse trabalho, Gauss inseriu a noção de congruência entre os números inteiros referentes a um módulo denotado por $a \equiv b \pmod{c}$ quando $c \mid (a - b)$, o que se tornou o primeiro exemplo algébrico do conceito de relação de equivalência, demonstrou a lei de reciprocidade quadrática, elaborou a teoria da composição de representações quadráticas e analisou a equação ciclotômica.

Quando Gauss conseguiu apresentar a demonstração correta da Lei da Reciprocidade Quadrática pela primeira vez, ficou tão entusiasmado que chamou esse resultado de Teorema

de Ouro. Gauss apresentou oito provas diferentes para o Teorema 3.4, seis delas publicadas e duas encontradas em seus documentos não publicados. Atualmente, são conhecidas mais de 250 provas distintas do teorema (Viana, 2023).

Apresentamos o Teorema 3.4, que relaciona números primos ímpares através do símbolo de Legendre², como em Araújo (2013, p. 20-22). Na demonstração, emprega-se a função piso³ e a Proposição 3.7 (Hefez, 2022, p. 253).

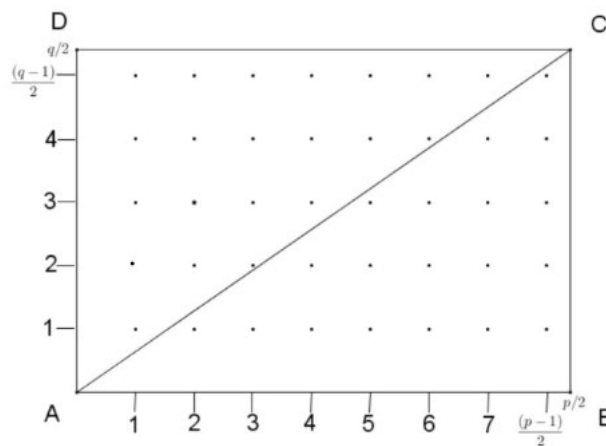
Proposição 3.7. *Sejam p e a dois números, com p primo ímpar e $(p, a) = 1$. Sejam $r_1, \dots, r_{\frac{p-1}{2}}$ os restos da divisão por p dos números $a, 2a, \dots, \frac{p-1}{2}a$, respectivamente. Se k é o número dos r_i que são maiores do que $\frac{p-1}{2}$, então $\left(\frac{a}{p}\right) = (-1)^k$.*

Teorema 3.4. *(Lei da Reciprocidade Quadrática de Gauss) Se p e q são dois números primos ímpares distintos, então*

$$\left(\frac{p}{q}\right) \left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2} \frac{q-1}{2}}.$$

Demonstração. Consideremos um sistema retangular de coordenadas. Neste, marcamos: sobre o eixo das abscissas, os pontos que distam $1, 2, \dots, \frac{(p-1)}{2}$ unidades da origem $A = (0, 0)$; sobre o eixo das ordenadas, os pontos que distam $1, 2, \dots, \frac{(q-1)}{2}$ unidades da origem A ; os pontos $B = \left(\frac{p}{2}, 0\right)$; $C = \left(\frac{p}{2}, \frac{q}{2}\right)$ e $D = \left(0, \frac{q}{2}\right)$; os pontos pertencentes ao produto cartesiano dos conjuntos $\{1, 2, 3, \dots, \frac{(p-1)}{2}\}$ e $\{1, 2, 3, \dots, \frac{(q-1)}{2}\}$ – Figura 3.1.

Figura 3.1 – Sistema retangular de coordenadas



Fonte: Adaptado de Araújo (2013).

² Quando a congruência $X^2 \equiv a \pmod{p}$ possui alguma solução, diz-se que a é resíduo quadrático módulo p ; caso contrário, diz-se que a é não resíduo quadrático módulo p . Se p é um número primo ímpar e a é um número inteiro tal que $p \nmid a$, define-se o símbolo de Legendre de um inteiro a , com respeito a p , como sendo

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & \text{se } a \text{ é resíduo quadrático módulo } p \\ -1, & \text{se } a \text{ é não resíduo quadrático módulo } p \end{cases}.$$

³ A função piso de um número real x , denotada por $\lfloor x \rfloor$, associa a x o maior número inteiro que é menor ou igual a x .

Na Figura 3.1, a reta que passa pelos pontos A e C tem equação $py = qx \Rightarrow y = \frac{q}{p}x$. Esta reta não passa por nenhum dos pontos interiores marcados no retângulo $ABCD$, uma vez que os elementos do conjunto $\{1, 2, \dots, \frac{(p-1)}{2}\}$ são primos com p .

Ainda, a reta $y = \frac{q}{p}x$ intersecta as retas $x = k$, $1 \leq k \leq p-1$, paralelas ao eixo y , nos pontos de coordenadas $(k, \frac{kq}{p})$. Como $\frac{kq}{p}$ não é inteiro, temos que o número de pontos de coordenadas naturais pertencentes à reta $x = k$, acima do eixo x e abaixo da reta $y = \frac{q}{p}x$, é $\left\lfloor \frac{kq}{p} \right\rfloor$. Assim, o número de pontos no interior do triângulo ABC é igual a:

$$M = \left\lfloor \frac{q}{p} \right\rfloor + \left\lfloor \frac{2q}{p} \right\rfloor + \left\lfloor \frac{3q}{p} \right\rfloor + \dots + \left\lfloor \frac{p-1}{2} \cdot \frac{q}{p} \right\rfloor.$$

Analogamente, o número de pontos de coordenadas naturais no interior do triângulo ACD é igual a:

$$N = \left\lfloor \frac{p}{q} \right\rfloor + \left\lfloor \frac{2p}{q} \right\rfloor + \left\lfloor \frac{3p}{q} \right\rfloor + \dots + \left\lfloor \frac{q-1}{2} \cdot \frac{p}{q} \right\rfloor.$$

Logo,

$$M + N = \frac{p-1}{2} \cdot \frac{q-1}{2}$$

é o número pontos de coordenadas naturais no interior do retângulo $ABCD$. Pela Proposição 3.7, temos que:

$$\left(\frac{q}{p}\right) = (-1)^M \text{ e } \left(\frac{p}{q}\right) = (-1)^N.$$

Portanto,

$$\left(\frac{p}{q}\right) \left(\frac{q}{p}\right) = (-1)^{M+N} = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}.$$

□

Os Corolários 3.2 e 3.3 decorrem do Teorema 3.4 (Hefez, 2022, p. 258).

Corolário 3.2. *Se p e q são dois números primos distintos, tais que $p \equiv q \equiv 3 \pmod{4}$, então q é resíduo quadrático módulo p , se, e somente se, p não é resíduo quadrático módulo q .*

Corolário 3.3. *Se p e q são dois números primos distintos, tais que $p \equiv 1 \pmod{4}$, ou $q \equiv 1 \pmod{4}$, então q é resíduo quadrático módulo p , se, e somente se, p é resíduo quadrático módulo q .*

Viana (2023, n.p) apresenta um enunciado informal dos Corolários 3.2 e 3.3.

Considere dois primos ímpares, p e q , quaisquer. Dizemos que p é um quadrado perfeito módulo q se existir algum inteiro n tal que $n \times n - p$ é múltiplo de q . Por exemplo, 5 é um quadrado perfeito módulo 19: basta considerar $n = 9$ e observar que $9 \times 9 - 5 = 76$ é múltiplo de 19.

Curiosamente, podemos inverter os papéis dos dois primos: 19 também é um quadrado perfeito módulo 5. Para ver isso, tome $n = 8$ e observe que $8 \times 8 - 19 = 45$ é múltiplo de 5. Dizemos que 5 e 19 são primos recíprocos.

Ora, Gauss mostrou que dois primos ímpares só podem ser recíprocos se pelo menos um for do tipo $4k+1$ [...].

Precisamente, o Teorema da Reciprocidade Quadrática diz que se algum dos primos p e q for do tipo $4k+1$ então vale um tudo ou nada: ou eles são recíprocos (é o caso de 5 e 19, como vimos), ou nenhum deles é um quadrado perfeito módulo o outro (como acontece com 5 e 13, por exemplo). Já se forem ambos do tipo $4k+3$ então exatamente um deles é quadrático perfeito módulo o outro. Por exemplo, 11 é quadrado perfeito módulo 7, mas 7 não é quadrado perfeito módulo 11 (verifique!). Em particular, nesse caso os dois primos nunca são recíprocos.

Apresentada por meio da linguagem matemática abstrata ou de maneira informal, é notório que a Lei da Reciprocidade Quadrática, ou o Teorema de Ouro, como descrito por Gauss, é um dos grandes resultados da Teoria dos Números. Desde seus primeiros rascunhos, passando pela sua primeira demonstração e chegando aos dias atuais, suas aplicações não se limitam ao campo da Teoria dos Números, mas são peças-chave no desenvolvimento de diversos ramos da Matemática. Destacamos, entre essas aplicações, sua influência na resolução de congruências quadráticas, na análise da distribuição dos números primos e na criptografia moderna.

3.4 CONJECTURAS

Ao longo da história, muitas das mais fascinantes descobertas surgiram não a partir de respostas, mas de perguntas ou ideias. Em diversas áreas, observações intrigantes e padrões recorrentes alimentaram a imaginação dos estudiosos, que formularam suposições ousadas, desafiando as fronteiras do que se conhecia até então. Esses intelectuais, muitas vezes embasados em evidências fragmentadas ou intuições profundas, tornaram-se motivadores de investigações complexas, atraindo a atenção de gerações de pesquisadores. De grandes problemas da Matemática até questões ainda em aberto em outras ciências, essas suposições têm moldado o progresso de diversas disciplinas, provocando avanços, refutações e a reformulação de teorias amplamente aceitas. São essas suposições que, ao permanecerem sem resposta por séculos, mantêm vivo o espírito investigativo.

As suposições ou ideias não provadas são chamadas de conjecturas. De acordo com Michaelis (2024, n.p), entende-se por conjectura:

1. Ato ou efeito de deduzir algo com base em suposições ou pressentimentos; hipótese.
2. Juízo ou opinião com fundamento incerto ou baseado em aparências, indícios ou probabilidades.

Para Onody (2021, n.p):

Mais do que em qualquer outra ciência, a Matemática possui conjecturas famosas em grande profusão. Propostas por matemáticos geniais e intuitivos, as conjecturas têm um papel muito importante em toda a história e o desenvolvimento da Matemática. Quer elas já tenham sido demonstradas ou não (ou,

eventualmente descartadas, caso inverídicas), as conjecturas matemáticas têm enorme potencial de atrair, fascinar e motivar pessoas, aglutinando e gerando novos conhecimentos.

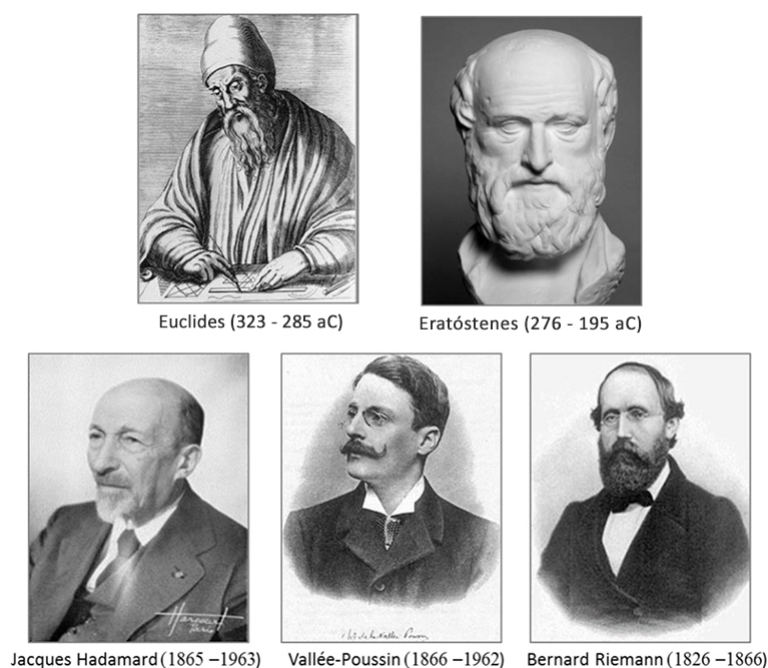
Na Matemática, existem numerosos problemas ainda sem solução, e a Teoria dos Números é um campo que se destaca pela abundância de questões não resolvidas. Entre os problemas mais conhecidos estão a Conjectura de Goldbach, que sugere que todo número par maior do que dois pode ser expresso como a soma de dois números primos, e a Conjectura dos Primos Gêmeos, que propõe a existência de infinitos pares de números primos cuja diferença é dois. Apesar de grandes avanços, essas conjecturas permanecem sem confirmação formal, desafiando matemáticos há séculos (Viana, 2022).

3.4.1 DISTRIBUIÇÃO DOS NÚMEROS PRIMOS

Os números primos têm sido uma fonte de fascínio na Matemática. Eles são os blocos de construção dos números inteiros, desempenhando um papel essencial na Aritmética, Teoria dos Números e, mais recentemente, em áreas como a Criptografia. Apesar da definição simples, os números primos escondem uma imensa complexidade que, por séculos, tem intrigado matemáticos de todas as épocas (Shalit, 2022).

Desde a Grécia Antiga, os números primos foram um campo de estudo constante. Euclides, um dos maiores matemáticos da antiguidade, provou que existem infinitos números primos, criando a base para séculos de pesquisa. A Figura 3.2 ilustra alguns dos matemáticos que dedicaram grande parte dos seus estudos aos números primos.

Figura 3.2 – Matemáticos que estudaram os números primos



Fonte: Shalit (2022).

Ao longo da história, outros matemáticos, como Pierre de Fermat, Leonhard Euler e Carl Friedrich Gauss, contribuíram significativamente para os avanços nesse campo de estudo (Boyer, 1974). Uma das descobertas mais notáveis de Fermat foi a de que certos números primos podem ser expressos na forma $2^{2^n} + 1$, conhecidos como números primos de Fermat. Infelizmente, embora Fermat tenha conjecturado que todos os números dessa forma fossem primos, apenas os primeiros cinco satisfazem essa condição (Burton, 2010).

A imprevisibilidade de sua distribuição é uma das razões pelas quais os números primos são tão empolgantes. A distribuição dos números primos é notoriamente irregular e imprevisível, sendo um dos grandes mistérios da Matemática. Não existe uma fórmula que permita prever quando o próximo número primo surgirá, o que faz com que sua descoberta seja um desafio. Embora possamos identificar facilmente os primeiros números primos, como 2, 3, 5, 7 e 11, a frequência com que eles aparecem diminui à medida que avançamos na reta numérica. Mesmo após séculos de investigação, os matemáticos ainda buscam entender completamente como os primos se distribuem ao longo dos números inteiros, uma questão central na Teoria dos Números (Peruzzo, 2012).

Segundo Hefez (2022), Carl Friedrich Gauss, ainda na sua adolescência, foi o primeiro a conjecturar um teorema sobre a distribuição dos primos, que se tornou conhecido como Teorema dos Números Primos – Teorema 3.5.

Teorema 3.5. (*Teorema dos Números Primos*) Se $\pi(x)$ é a função de contagem de primos, ou seja, é o número de primos menores ou iguais a x , então

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

A formulação precisa e os detalhes da prova do Teorema 3.5 exigem matemática avançada, mas, de forma simplificada, Shalit (2022) afirma que “o teorema dos números primos estabelece que a frequência dos números primos na vizinhança de x é inversamente proporcional à quantidade de algarismos em x ”.

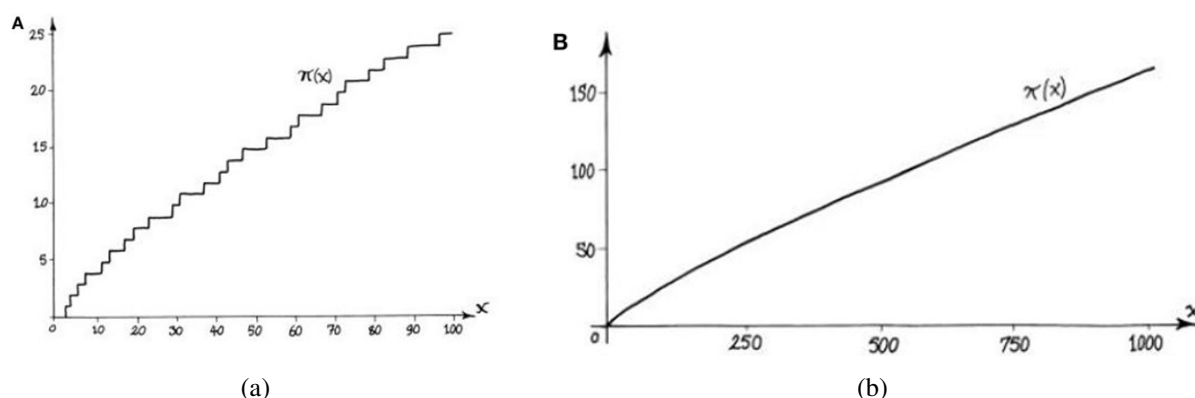
Quanto à distribuição dos números primos, Shalit (2022, n.p) apresenta os seguintes dados:

[...] a quantidade de primos em uma “janela” com a extensão de 1.000 em torno de um milhão (isto é, o intervalo entre um milhão e um milhão e um mil) será 50% maior que a quantidade de primos na mesma “janela” em torno de um bilhão (a razão é 9:6, tal como a razão entre a quantidade de zeros em um bilhão e um milhão) e cerca de duas vezes a quantidade de primos na mesma “janela” em torno de um trilhão (onde a razão da quantidade de zeros é 12:6). De fato, cálculos por computador mostram que há 75 números primos na primeira “janela”, 49 na segunda e apenas 37 na terceira, entre um trilhão e um trilhão e um mil.

A distribuição dos números primos pode ser visualizada graficamente, como ilustra a Figura 3.3, o que facilita a compreensão de certos padrões e lacunas na sequência dos primos.

Inicialmente, o gráfico – Figura 3.3(a) – formado pela quantidade de números primos $\pi(x)$ até x exibe um formato em “degrau”, que corresponde ao fato de que, ao longo do eixo x , cada vez que um novo primo é encontrado, o gráfico se eleva em uma unidade. Em escalas menores, no entanto, a identificação de um padrão consistente torna-se desafiadora. Mesmo assim, é possível demonstrar matematicamente que existem grandes intervalos sem a ocorrência de primos, resultando em trechos onde o gráfico permanece horizontal. Esse comportamento é contrastado pela conjectura dos primos gêmeos, que sugere a existência de infinitos pares de números primos cuja diferença é 2, o que criaria um “degrau” estreito no gráfico. Já em escalas maiores – Figura 3.3(b) – a tendência é que o gráfico assuma uma forma suave, comprovando o teorema dos números primos, que descreve a distribuição dos primos em grandes intervalos de números inteiros (Shalit, 2022).

Figura 3.3 – Frequência dos números primos: (a) intervalo de 0 a 100; (b) intervalo de 0 a 1000



Fonte: Shalit (2022).

Além da distribuição dos números primos, outra questão que fascina os matemáticos é a busca por números primos gigantes. O maior número primo conhecido até agora foi descoberto em outubro de 2024 e tem mais de 41 milhões de dígitos. O mais recente maior número primo da história é o 52º primo de Mersenne já descoberto (Lima, 2024), sendo que os números M_p de Mersenne têm a forma $2^p - 1$, com p primo.

Até então, o maior número primo conhecido era o $M_{82589933}$ com 24.862.048 dígitos, que deteve o recorde por 6 anos. Esse número foi superado pelo novo recordista, o $M_{136279841}$, com 16 milhões de dígitos a mais. Este último é representado por $2^{136279841} - 1$ (GIMPS, 2024a).

Os números primos são repletos de curiosidades matemáticas que fascinam até mesmo aqueles que não se dedicam exclusivamente à Teoria dos Números. Um exemplo interessante são os primos gêmeos, que são pares de números primos separados por apenas duas unidades, como 11 e 13, ou 17 e 19. Uma das grandes conjecturas da Matemática, a Conjectura dos Primos Gêmeos, sugere que há infinitos pares de primos gêmeos. Embora essa conjectura ainda esteja em aberto, muitos pares de primos gêmeos já foram identificados graças a extensas pesquisas, ao uso de teoria avançada dos números e de técnicas computacionais (Castro, 2023).

Apesar de seu caráter abstrato, os números primos têm aplicações práticas extremamente importantes. Nos últimos anos, o uso de números primos ganhou destaque devido ao método criptográfico RSA, fundamental para a segurança do sistema financeiro moderno. Esse método se baseia na dificuldade de decompor grandes números em seus fatores primos, tornando as transações financeiras, como compras com cartão de crédito e saques em caixas eletrônicos, seguras contra interceptações indesejadas. Caso fosse possível fatorar rapidamente esses números, toda a segurança do sistema criptográfico atual estaria comprometida (Spina, 2014).

Os números primos vão além de conceitos matemáticos abstratos. Eles exercem um impacto direto sobre a tecnologia moderna e há mais de dois mil anos despertam mistério e fascínio. Da sua simplicidade essencial à relevância em problemas matemáticos não resolvidos, os números primos continuam a desafiar e cativar os estudiosos. Seja através dos primos gêmeos, dos números de Mersenne ou de sua ligação com a criptografia, eles demonstram que, apesar dos avanços no nosso conhecimento, ainda há muito a ser desvendado e explorado no universo dos números primos.

3.4.2 PRIMOS GÊMEOS

Os números primos são objetos fascinantes da Teoria dos Números e, entre suas várias classes especiais, os números primos gêmeos se destacam por sua simplicidade e mistério. A Definição 3.2 estabelece o conceito de primos gêmeos (Castro, 2023, p. 23).

Definição 3.2. *Dois números p e q são considerados primos gêmeos quando p e q são primos e o módulo da diferença entre eles é igual a 2 ou seja, $|p - q| = 2$.*

Segundo a Definição 3.2, os seguintes pares de primos são gêmeos:

$$(3, 5), (5, 7), (11, 13), (17, 19).$$

Viana (2018, n.p) emprega a seguinte definição para primos gêmeos: “São pares de números primos ímpares consecutivos, ou seja, cuja diferença é igual a 2. Esta denominação foi usada pela primeira vez em 1916, pelo matemático alemão Paul Stäckel (1862 – 1919), mas o problema é muito mais antigo”.

De acordo com Costa (2021f, p. 2):

Os primeiros pares de primos gêmeos são: (3, 5), (5, 7), (11, 13), (17, 19), (29, 31), (41, 43),... Existem pares de primos gêmeos muito grandes, como $2.996.863.034.895 \times 2^{1290000} \pm 1$, que possuem 388.342 algarismos na base decimal (esse é o maior par de primos gêmeos conhecido até o momento e foi descoberto em 2016).

A importância desses pares de números vai além de sua definição simples. Eles representam uma janela para entender a distribuição dos números primos. Enquanto se sabe que os números primos são infinitos, pelo famoso teorema de Euclides, a questão sobre a infinidade

dos números primos gêmeos permanece aberta e é considerada um dos grandes problemas não resolvidos da Matemática moderna. Esse problema é conhecido como a Conjectura dos Primos Gêmeos e afirma que há infinitos pares de primos gêmeos, mas, até hoje não foi provada de forma definitiva (Silva, 2018). Elencamos na Tabela 3.2 os vinte maiores pares de números primos gêmeos encontrados até o momento.

Tabela 3.2 – Vinte maiores primos gêmeos já encontrados

CLASSIFICAÇÃO	PRIMOS	DÍGITOS	DATA
1	$2996863034895 \times 2^{1290000} \pm 1$	388342	Set 2016
2	$3756801695685 \times 2^{666669} \pm 1$	200700	Dez 2011
3	$669821552^{16384} - 669821552^{8192} \pm 1$	144605	Abr 2024
4	$222710306^{16384} - 222710306^{8192} \pm 1$	136770	Mar 2024
5	$65516468355 \times 2^{333333} \pm 1$	100355	Ago 2009
6	$201926367 \times 2^{266668} \pm 1$	80284	Mai 2024
7	$160204065 \times 2^{262148} \pm 1$	78923	Jul 2021
8	$1893611985^{8192} - 1893611985^{4096} \pm 1$	76000	Mar 2024
9	$1589173270^{8192} - 1589173270^{4096} \pm 1$	75376	Fev 2024
10	$996094234^{8192} - 996094234^{4096} \pm 1$	73715	Jan 2024
11	$895721531^{8192} - 895721531^{4096} \pm 1$	73337	Jan 2024
12	$795507696^{8192} - 795507696^{4096} \pm 1$	72915	Jan 2024
13	$691595760^{8192} - 691595760^{4096} \pm 1$	72417	Jan 2024
14	$647020826^{8192} - 647020826^{4096} \pm 1$	72180	Jan 2024
15	$629813654^{8192} - 629813654^{4096} \pm 1$	72084	Jan 2024
16	$504983334^{8192} - 504983334^{4096} \pm 1$	71298	Jan 2024
17	$314305725^{8192} - 314305725^{4096} \pm 1$	69611	Dez 2023
18	$184534086^{8192} - 184534086^{4096} \pm 1$	67716	Dez 2023
19	$414279340881715 \times 2^{222333} \pm 1$	66943	Nov 2023
20	$12770275971 \times 2^{222225} \pm 1$	66907	Jul 2017

Fonte: Caldwell, McLean e Slatkevičius (2024).

A Conjectura dos Primos Gêmeos é uma das questões não resolvidas mais famosas da Teoria dos Números, sendo um tema investigado por diversos matemáticos ao longo dos anos. Embora algumas fontes associem essa questão a Euclides, sua origem exata permanece incerta. Em 1849, o matemático francês Alphonse de Polignac (1826 – 1863) generalizou a conjectura ao propor que, para todo $k \in \mathbb{N}$, existem infinitos primos p tais que $p + 2k$ também é primo, sendo o caso específico $k = 1$ conhecido como a Conjectura dos Primos Gêmeos (Souza, 2019).

Quando se trata de números primos gêmeos, é interessante analisar a série dos inversos dos primos gêmeos (Coelho, 2021, p. 11). Se $P_g = \{(p, p + 2); p \text{ e } p + 2 \text{ são ambos primos}\}$, considere a série numérica

$$\sum_{(p,p+2) \in P_g} \left(\frac{1}{p} + \frac{1}{p+2} \right) = \left(\frac{1}{3} + \frac{1}{5} \right) + \left(\frac{1}{5} + \frac{1}{7} \right) + \cdots + \left(\frac{1}{p} + \frac{1}{p+2} \right) + \cdots,$$

onde P_g é o conjunto dos primos gêmeos.

Viggo Brun (1885 – 1978) demonstrou em 1915 que a soma dos inversos dos números primos gêmeos é convergente. Esse resultado notável, conhecido como a constante B de Brun, não resolve a questão sobre a infinitude dos primos gêmeos, mas mostra que, mesmo que existam infinitos desses números, sua densidade é muito menor que a dos números primos em geral. Posteriormente, essa constante foi refinada com o auxílio de computadores por matemáticos como Shanks, Wrench, Brent e Nicely (Coelho, 2021). Porém:

Este resultado não exclui que existam infinitos pares de primos gêmeos, mas informam que esses pares são encontrados cada vez mais longe, separados, então a soma de seus inversos permanece finita. Com base em considerações heurísticas sobre a distribuição de primos gêmeos, B foi calculado, por exemplo, por Shanks & Wrench (1974), por Brent (1976), e mais recentemente por Nicely (2001), que obtiveram, $B = 1,9021605823...$ (Coelho, 2021, p. 11 *apud* Ribenboim, 2004, p. 193).

Um marco recente no estudo dos números primos gêmeos foi o trabalho do matemático chinês Yitang Zhang. De acordo com Viana (2018, n.p):

O principal avanço na direção de resolver esse problema foi obtido em 2013 pelo chinês Yitang Zhang, nascido em Xangai em 1955. No lugar de pares de primos com diferença igual a 2, ele considerou diferenças quaisquer e provou que existe algum número N tal que a quantidade de pares de primos cuja diferença é N é infinita. Por essa façanha, Zhang foi convidado a dar a palestra de encerramento do Congresso Internacional de Matemáticos de 2014, em Seul, uma distinção. O argumento dele também mostrava que N pode ser tomado menor que 70 milhões. Um projeto colaborativo, com a participação de matemáticos (e computadores) do mundo todo, conseguiu melhorar muito essa estimativa. Agora sabemos que podemos tomar $N = 246$. O problema original, com $N = 2$, continua sem solução...

Embora os avanços sejam expressivos, a Conjectura dos Primos Gêmeos ainda permanece uma incógnita. A investigação contínua sobre a existência de infinitos desses pares tem impulsionado o progresso em várias áreas da Matemática, além de ampliar o entendimento sobre a distribuição dos números primos. A resolução da Conjectura dos Primos Gêmeos certamente representará um marco importante na história da Teoria dos Números, abrindo novas portas para a compreensão de padrões ainda não descobertos no comportamento dos números primos.

3.4.3 PRIMOS PALÍNDROMOS E PRIMOS REVERSOS

A Matemática, por vezes vista como uma disciplina árdua e complexa, revela um universo fascinante quando exploramos suas nuances e particularidades. Ao adentrarmos no mundo dos números, deparamo-nos com uma infinidade de curiosidades que desafiam nossa intuição e despertam nossa imaginação. Entre os objetos matemáticos curiosos, destacam-se os números palíndromos, os números primos palíndromos e os primos reversos. A Definição 3.3 caracteriza um número palíndromo (Cavalcante, 2006, p. 4).

Definição 3.3. *Um número inteiro n ($n \geq 1$) é palíndromo quando não se altera se os algarismos que o compõem são escritos na ordem inversa.*

Para Silva (2012a, n.p): “Número capicua ou número palíndromo é um número que pode ser lido tanto da esquerda para a direita quanto da direita para a esquerda, isto é, invertendo as posições dos seus algarismos esse número apresenta sempre o mesmo valor”. A Figura 3.4 ilustra alguns exemplos de números palíndromos.

Entre os números palíndromos, encontramos os números primos palíndromos – Definição 3.4 (Cavalcante, 2006).

Definição 3.4. *Primos palíndromos são números divisíveis apenas por 1 e por eles mesmos e seus algarismos podem ser lidos da direita para a esquerda na mesma ordem em que são lidos da esquerda para a direita, ou seja, possuem ao mesmo tempo as propriedades dos números primos e dos números palíndromos.*

A Figura 3.5 mostra alguns números primos palíndromos.

Figura 3.5 – Números primos palíndromos

2	181	95959	9324239
3	383	96769	9397939
5	787	97579	9400049
7	929	98689	9504059

Fonte: Cavalcante (2006).

Shareef Bacchus demonstrou por indução que, entre os números primos que se leem da mesma forma nos dois sentidos, o 11 é uma exceção única. Ele é o único número primo palíndromo com um número par de algarismos. Qualquer outro palíndromo com uma quantidade par de algarismos é divisível por 11, perdendo assim a condição de ser primo (Sena, 2008).

De acordo com Sena (2008, p. 20): “O maior primo palindrômico conhecido é $10^{180004} + 248797842 \times 10^{89998} + 1$, encontrado por Harvey Dubner em 2007”.

A investigação dos números primos palíndromos revela a existência de sequências organizadas em forma de pirâmide. As pirâmides de números primos palíndromos representam uma estrutura fascinante dentro do universo dos números. Essas pirâmides são formadas por sequências de números primos palíndromos, onde cada novo termo apresenta um novo primo palíndromo com os dígitos centrais iguais ao termo anterior. Já a altura da pirâmide é determinada pela quantidade de termos que a sequência possui, como ilustra a Figura 3.6. Essa organização

Figura 3.4 – Números palíndromos ou capicua



Fonte: Silva (2012a).

em camadas, semelhante a uma pirâmide, revela padrões e relações entre esses números especiais (Cavalcante, 2006).

Figura 3.6 – Pirâmide de números primos palíndromos começando em 2 e com altura 5

2
929
39293
7392937
373929373

Fonte: Cavalcante (2006).

Na Figura 3.7 temos mais algumas representações de pirâmides de números primos palíndromos construídas a partir de um número primo formado por um único algarismo. As duas primeiras pirâmides, à esquerda, iniciam pelo número primo 3 e possuem altura igual a 3; as três pirâmides centrais, iniciam pelo número primo 5 e possuem altura igual a 4; a última pirâmide, à direita, inicia pelo número primo 7 e possui altura igual a 3.

Figura 3.7 – Pirâmides de primos palíndromos

		5	5	5	
3	3	151	353	757	7
131	131	31513	33533	37573	373
11311	71317	3315133	1335331	9375739	93739

Fonte: Cavalcante (2006).

Outro grupo de números que se destacam dentro do universo dos números primos, são os números primos reversos - Definição 3.5 (Silva, 2012b).

Definição 3.5. *Um número primo é denominado reverso quando, escrito de maneira inversa, continua sendo primo.*

Os números primos reversos são conhecidos como *omirp* ou *emirp* (palavras primo e *prime* escritas inversamente). Alguns exemplos de números primos reversos são apresentados na Figura 3.8. Essa peculiaridade numérica demonstra a rica diversidade que encontramos no universo dos números primos.

Em sua obra, Gardner (1985) combina Matemática recreativa com elementos fictícios e lúdicos para introduzir conceitos matemáticos curiosos. Os *emirps* são um dos tópicos que ele apresenta como parte de um universo maior de números interessantes. Segundo Gardner, o conceito de *emirps*, números primos que permanecem primos quando seus dígitos são invertidos,

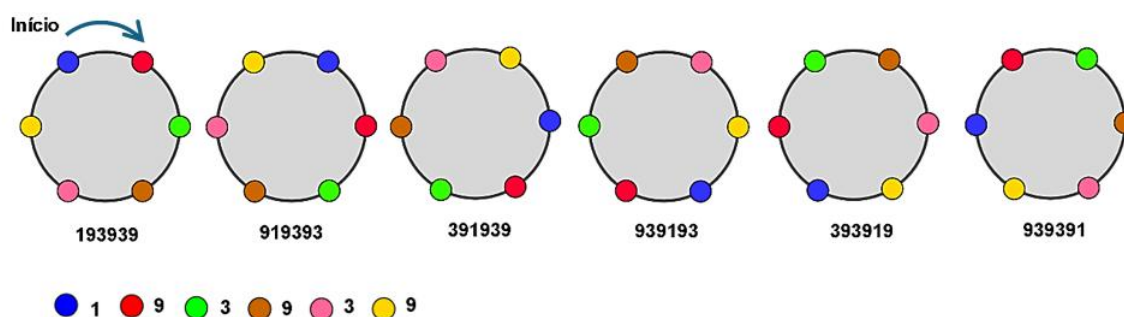
Figura 3.8 – Números primos reversos



Fonte: Silva (2012b).

cativou matemáticos e entusiastas. O termo, introduzido por Jeremiah Paul Farrell (1937 – 2022), apresenta um aspecto intrigante da Teoria dos Números que explora a interação entre números primos e suas representações digitais.

A busca por *emirps* levou a explorações matemáticas adicionais, como a descoberta de *emirps* cíclicos. Esses números possuem uma propriedade notável: quando seus dígitos são deslocados ciclicamente, cada número resultante permanece primo. O único *emirp* cíclico de seis dígitos, 193939, como ilustrado na Figura 3.9, destaca os padrões e as simetrias que podem surgir no reino dos números primos (Gardner, 1985).

Figura 3.9 – *Emirp* cíclico

Fonte: A autora.

Além disso, a criação de quadrados de *emirps*, onde cada linha, coluna e diagonal principal forma um *emirp* distinto, apresenta um quebra-cabeça matemático desafiador. A existência de tais quadrados para ordens 4 e 5 demonstra o potencial para construir padrões desafiadores usando números primos. Na Figura 3.10, temos dois quadrados formados por *emirps*, o primeiro de ordem 4 e o segundo de ordem 5 (Gardner, 1985).

Figura 3.10 – Quadrados de *emirps*

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

Fonte: Gardner (1985).

No site *The On-Line Encyclopedia of Integer Sequences* (OEIS), Sloane (2024, n.p) apresenta a seguinte sequência (A006567) com alguns números *emirps*: “13, 17, 31, 37, 71, 73, 79, 97, 107, 113, 149, 157, 167, 179, 199, 311, 337, 347, 359, 389, 701, 709, 733, 739, 743, 751, 761, 769, 907, 937, 941, 953, 967, 971, 983, 991, 1009, 1021, 1031, 1033, 1061, 1069, 1091, 1097, 1103, 1109, 1151, 1153, 1181, 1193, 1201”.

Os números *emirps* tornam-se progressivamente mais difíceis de serem encontrados conforme avançamos para números maiores, da mesma forma que ocorre com os números primos em geral. O desafio adicional com os *emirps* é que, além de serem primos, eles precisam permanecer primos quando seus dígitos são invertidos. Isso reduz ainda mais o número de candidatos possíveis à medida que os números crescem.

Embora o estudo de *emirps* possa parecer abstrato, ele contribui para uma compreensão mais profunda da Teoria dos Números e das propriedades dos números primos. A exploração de *emirps*, *emirps* cíclicos e quadrados de *emirps* oferece um vislumbre do fascinante mundo da Matemática, onde conceitos aparentemente simples podem levar a descobertas complexas e intrigantes.

3.5 PRIMOS GÊMEOS, PRIMOS PRIMOS E PRIMOS SEXY

A distribuição dos números primos na reta numérica apresenta um padrão irregular, com intervalos de tamanho variável entre um primo e outro. Esses intervalos, denominados por Vieira (2023, p. 35) como “lacunas” ou, em inglês, “*gaps*”, têm sido alvo de inúmeras pesquisas. A análise do tamanho e das características dessas lacunas tem permitido aos matemáticos classificar os números primos em diferentes categorias. Dentro delas, daremos destaque aos chamados números primos gêmeos, primos primos e primos *sexy*, os quais apresentamos a seguir.

Conforme Vieira (2023), a distância entre um número primo e seu sucessor não é constante, variando significativamente ao longo da sequência dos números primos. Ao analisar pares de primos consecutivos, Ndiaye (2024) observou que as diferenças entre eles se concentram em três valores principais: 2, 4 e 6. Pares de primos com diferença 6 são denominados primos *sexy*, enquanto aqueles com diferença 4 são classificados como primos primos.

Seguindo a classificação de Jesus e Claudino (2014, p. 65-66), podemos definir os seguintes tipos de pares de números primos:

Primos gêmeos – são os pares de números primos da forma $p, p + 2$. A quantidade infinita de pares de primos gêmeos é ainda uma questão em aberto [...].

Primos “primos” – são os pares de números primos da forma $p, p + 4$. É facilmente verificada a existência de apenas 26 pares de primos “primos” menores do que 1000.

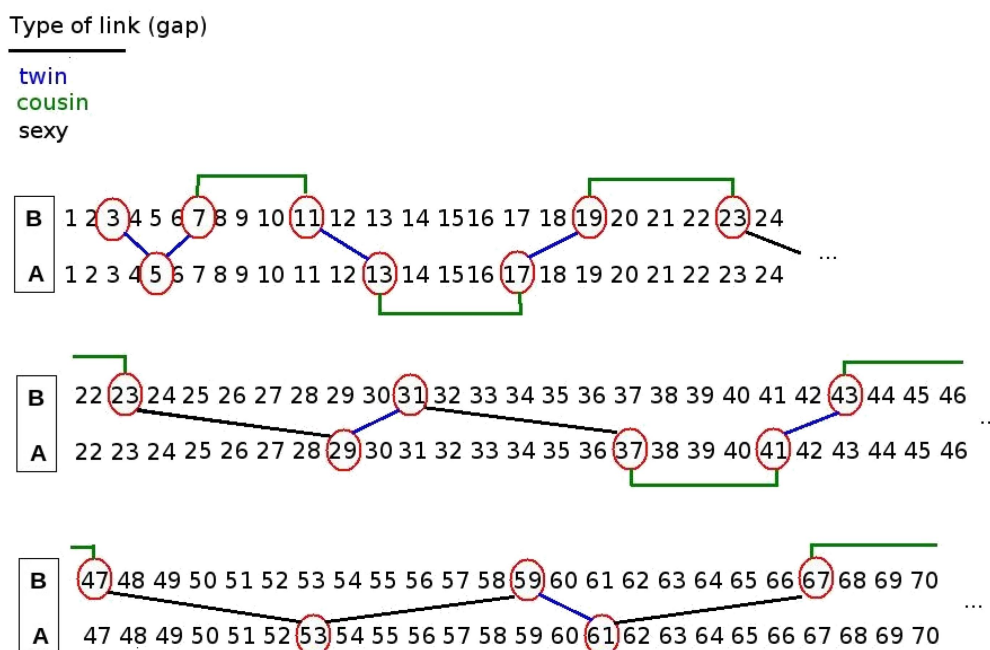
Primos sexy – são os pares de números primos da forma $p, p + 6$. O termo *sexy* vem do latim para a tradução tendenciosa do número “*six*” como sendo “sexo”. A tripla (47,53,59) é um exemplo de uma tripla sexy, a quádrupla (61,67,73,79) é um exemplo de uma quádrupla sexy, a sequência (5,11,17,23,29) é a única quádrupla sexy conhecida e não existe nenhuma sêxtupla sexy.

Prajapati (2021) destaca que o número 5 é único ao pertencer a dois pares distintos de primos gêmeos, mais especificamente nos pares (3, 5) e (5, 7). Além disso, o autor evidencia que, exceto pelo par (3, 5), todos os primos gêmeos podem ser expressos na forma $(6n - 1, 6n + 1)$, onde n é um número natural. A divisibilidade por 12 da soma dos pares de primos gêmeos, com a exceção citada, revela uma característica peculiar desses números, contribuindo para uma melhor compreensão de sua distribuição entre os primos.

Os primos primos também apresentam peculiaridades. O número 7 é o único a fazer parte de dois pares distintos: (3, 7) e (7, 11). Além disso, a existência de três primos primos consecutivos é restrita devido à divisibilidade por 3 de um dos números em qualquer conjunto de números da forma n , $n + 4$ e $n + 8$. O único trio possível é quando $n = 3$, que fornece o trio (3, 7, 11) (Prajapati, 2021).

A Figura 3.11 ilustra como ocorre a distribuição dos números primos gêmeos, primos primos e primos *sexy* nos números naturais até 70.

Figura 3.11 – Distribuição dos primos gêmeos, primos primos e primos *sexy* até 70



Fonte: Lacasa *et al.* (2018).

Segundo Prajapati (2021, p. 13), os primeiros pares de primos primos são: “(3,7), (7,11), (13,17), (19,23), (37,41), (43,47), (67,71), (79,83), (97,101), (103,107), (109,113), (127,131), (163,167), (193,197), [...]”.

Já os primeiros pares de primos *sexy* são: “(5,11), (7,13), (11,17), (13,19), (17,23), (23,29), (31,37), (37,43), (41,47), (47,53), (53,59), (61,67), (67,73), (73,79), (83,89), (97,103), (101,107), (103,109), (107,113), (131,137), (151,157), (157,163), (167,173), (173,179), (191,197), (193,199), [...]” (Prajapati, 2021, p. 17).

As particularidades dos primos gêmeos, primos primos e primos *sexy* demonstram que

a Teoria dos Números continua a oferecer desafios e oportunidades para os matemáticos. A investigação dessas sequências numéricas pode não apenas levar ao desenvolvimento de novas ferramentas matemáticas, mas também revelar padrões e conexões que contribuam para uma compreensão mais profunda da estrutura dos números inteiros. A relativa escassez de estudos sobre esses tópicos sugere que há um grande potencial para novas descobertas e avanços nessa área.

3.6 PADRÕES NUMÉRICOS E APLICAÇÕES

A investigação sobre os números primos tem evoluído ao longo dos séculos, com matemáticos buscando identificar padrões e regularidades nessa sequência aparentemente aleatória. Embora a fórmula definitiva para gerar todos os primos ainda seja desconhecida, a pesquisa nesse campo tem revelado propriedades e padrões intrigantes, muitos deles já abordados nesta dissertação. Para que nos aprofundemos ainda mais nesse vasto campo de estudo, veremos outros dois padrões numéricos importantes: os primos de Sophie Germain e de Marin Mersenne.

Os números primos de Sophie Germain representam um tema de grande relevância dentro da Teoria dos Números, especialmente devido às suas ligações com o Último Teorema de Fermat. Esses números receberam tal nome em homenagem à matemática francesa Sophie Germain (1776 – 1831). Segundo Castro (2023, p. 14): “Os primos de Sophie Germain são encontrados através da fórmula $2p + 1$, onde p é um número primo, caso o resultado seja outro número primo então p é chamado de primo de Sophie Germain”.

De acordo com Novaes (2023, p. 101): “os primeiros números de Germain são 2, 3, 5, 11, 23, 29, 41, 43, 83, 89, 113 e 131. Com uma verificação numérica, descobre-se que existem 190 primos de Germain no intervalo $[1, 10^4]$ ”.

Sophie Germain foi pioneira ao demonstrar resultados importantes para o caso especial do Último Teorema de Fermat. Novaes (2023) afirma que a jovem matemática demonstrou que, para a equação diofantina $x^n + y^n = z^n$, com n sendo um número natural maior do que 2 e primo de Germain, uma condição necessária para a existência de soluções inteiras é que x , y e z sejam divisíveis por n .

Outro matemático que contribuiu consideravelmente com o avanço da Teoria dos Números foi Marin Mersenne (1588 – 1648). De acordo com Hefez (2022, p. 139): “Os números de Mersenne são os números da forma $M_p = 2^p - 1$, onde p é um número primo”.

A condição para que um número seja considerado primo de Mersenne é que tanto M_p quanto p sejam números primos. Embora nem todos os números de Mersenne sejam primos, sua popularidade deve-se ao fato de que é possível verificar computacionalmente a primalidade desses números, mesmo para valores altos de p . Mersenne, ao longo de sua vida, contribuiu significativamente para a disseminação de conhecimentos científicos por meio de suas correspondências, envolvendo figuras notáveis como Fermat, Torricelli e Galileu, o que impulsionou o

desenvolvimento matemático de sua época (Andrade, 2018a).

Segundo Hefez (2022, p. 139): “No intervalo $2 \leq p \leq 5000$ os números de Mersenne que são primos, chamados de *primos de Mersenne*, correspondem aos seguintes valores de p : 2, 3, 5, 7, 13, 19, 31, 61, 89, 107, 127, 521, 607, 1279, 2203, 2281, 3217, 4253 e 4423”. O maior primo de Mersenne conhecido até o momento é o $M_{136279841}$ que tem 41.024.320 dígitos. Esse é o 52º primo de Mersenne descoberto (GIMPS, 2024a).

A infinitude dos números primos de Mersenne continua sendo uma questão em aberto na Matemática. Entretanto, a busca por uma resposta a essa pergunta mobiliza pessoas do mundo inteiro, que colaboram no *Great Internet Mersenne Prime Search* (GIMPS) com o objetivo de encontrar novos exemplos desses números e, quem sabe, desvendar esse mistério (Andrade, 2018a).

O GIMPS é um projeto colaborativo global que utiliza a força computacional de milhares de voluntários para encontrar novos números primos de Mersenne. Para incentivar a busca por esses raros gigantes numéricos, são oferecidos prêmios em dinheiro para cada novo primo de Mersenne descoberto, com um prêmio especial reservado para a primeira pessoa ou grupo a encontrar um número primo com 100 milhões de dígitos. Essa iniciativa transforma a busca por números primos em uma verdadeira corrida espacial da Matemática, mobilizando entusiastas e cientistas em todo o mundo na busca por essas joias numéricas (GIMPS, 2024a).

Embora os números primos apresentem padrões intrigantes e sejam objeto de estudo na Matemática Pura, suas aplicações se estendem muito além do campo teórico. A Criptografia, por exemplo, depende fundamentalmente das propriedades únicas dos números primos para garantir a segurança de dados digitais. Além disso, esses números são utilizados em algoritmos de diversos sistemas, desde atualizações de software até a geração de números aleatórios, evidenciando a relevância da Matemática Pura para o desenvolvimento de tecnologias modernas.

Segundo Peruzzo (2012, p. 91-92):

Por muito tempo a teoria dos números foi uma disciplina sem nenhuma aplicação prática [...].

A partir da década de 1970 essa área começou a despertar um grande interesse, principalmente quanto a sua utilização em criptografia. Por meio de um processo técnico o número resultante da multiplicação de dois números primos é utilizado para construir um meio muito eficiente para codificar mensagens, sendo que para quebrar esse código é necessário conhecer os fatores primos do inferido produto.

De acordo com Coutinho (2016), a Criptografia tem suas raízes na palavra grega *cryptos*, que significa oculto. Seu objetivo principal é garantir que apenas o destinatário autorizado consiga decifrar uma mensagem, transformando a comunicação em uma verdadeira arte dos códigos secretos.

Singh (2022) aponta que a Criptografia evoluiu significativamente ao longo da história.

A busca por comunicação segura remonta aos tempos antigos, quando os egípcios utilizavam hieróglifos e os romanos empregavam cifras simples para proteger suas mensagens. Ao longo dos séculos, a Criptografia evoluiu em resposta aos desafios de cada época, desde as guerras até a era digital, onde a segurança da informação se tornou um dos maiores desafios da sociedade. A descoberta dos números primos e sua aplicação na Criptografia moderna, especialmente no desenvolvimento de sistemas como o RSA, transformou a segurança digital, permitindo a proteção de informações em larga escala na era da comunicação eletrônica.

A revolução da Criptografia moderna pode ser atribuída ao algoritmo RSA, desenvolvido por Rivest, Shamir e Adleman em 1977. Essa inovação introduziu o conceito de criptografia assimétrica, utilizando um par de chaves - uma pública e outra privada - para garantir a segurança das comunicações digitais. Em contraste com os métodos simétricos, que dependem de uma única chave, o RSA eliminou a necessidade de compartilhar chaves secretas por canais inseguros, permitindo a aplicação da Criptografia em uma ampla gama de sistemas e serviços (Marinho, 2017).

A segurança da criptografia assimétrica é garantida pelo seguinte processo:

O servidor e o cliente geram as suas chaves públicas e privadas. O servidor envia para o cliente sua chave pública, e o cliente envia para o servidor sua chave pública.

O cliente criptografa seus dados com a chave pública (do servidor), e envia para o servidor.

O servidor descriptografa os dados com a sua chave privada.

O servidor criptografa o que será enviado para o cliente com a chave pública do cliente, e envia para o cliente.

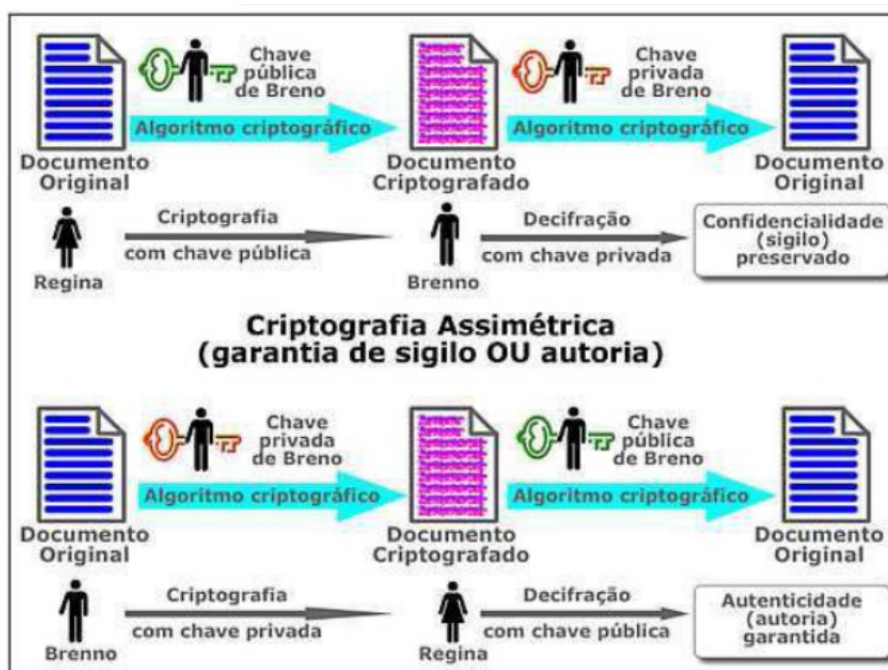
O cliente consegue, por fim, descriptografar o retorno do servidor, com sua chave privada (Marinho, 2017, n.p).

A Matemática está presente em cada etapa do processo de Criptografia. Podemos resumir esse processo em seis etapas.

1. Escolher dois números p e q com mais de 100 algarismos.
2. Calcular $n = p \cdot q$ e $\phi(n) = (p - 1) \cdot (q - 1)$, onde ϕ é a função de Euler.
3. Escolher e tal que $1 < e < \phi(n)$ e $(e, \phi(n)) = 1$.
4. Codificar a mensagem em blocos b . Cada bloco codificado, denotado por $C(b)$, é o resto da divisão de b^e por n .
5. Calcular d de modo que $d \cdot e \equiv 1 \pmod{\phi(n)}$.
6. Decodificar a mensagem em blocos a . Cada bloco decodificado, denotado por $D(a)$, é o resto da divisão de a^d por n .

A Figura 3.12 ilustra como ocorre o processo de criptografia usando chaves assimétricas.

Figura 3.12 – Criptografia com chave assimétrica



Fonte: Rocha (2017).

De acordo com Coutinho (2016), a Criptografia RSA opera com números inteiros. No entanto, nossas mensagens são, na maioria das vezes, textos. Portanto, o primeiro passo é transformar o texto em uma sequência numérica para podermos aplicar o algoritmo RSA. Essa primeira etapa recebe o nome de pré-codificação.

Para simplificar, consideremos apenas mensagens em letras maiúsculas, sem números. Assim, nossa mensagem original será composta por letras e espaços. Para realizarmos a pré-codificação, utilizaremos a Tabela 3.3 que associa cada letra a um número específico (Coutinho, 2016).

Tabela 3.3 – Tabela para pré-codificação

A	B	C	D	E	F	G	H	I	J	K	L	M
10	11	12	13	14	15	16	17	18	19	20	21	22
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
23	24	25	26	27	28	29	30	31	32	33	34	35

Fonte: Coutinho (2016).

Coutinho (2016) ainda esclarece que, a fim de diferenciar as palavras, substituímos os espaços por 99. Dessa forma, a frase AMO A OBMEP vira:

1022249910992411221425.

Para evitar confusões, cada letra é representada por um número de exatamente dois dígitos. Após

escolher os primos p e q para o RSA, calculamos $n = pq$. O número obtido na pré-codificação é dividido em blocos menores que n . Por exemplo, com $p = 17$ e $q = 23$, obtemos $n = 391$ e temos os blocos:

102-224-99-109-92-41-122-142-5.

A separação da mensagem em blocos é flexível, sem a necessidade de tamanhos iguais. No entanto, blocos iniciados por 0 devem ser evitados para prevenir ambiguidades na decodificação. É importante notar que os blocos não correspondem a unidades linguísticas, dificultando significativamente a quebra da cifra por análise de frequência (Coutinho, 2016).

Com a pré-codificação finalizada, podemos aplicar o algoritmo de criptografia RSA. A chave pública desse sistema é representada pelo número n , resultado da multiplicação dos primos p e q . Essa chave, chamada de chave pública, pode ser compartilhada publicamente, pois seu propósito é codificar a mensagem. Cada bloco da mensagem pré-codificada é codificado de forma independente. A mensagem codificada final é o agrupamento dos blocos codificados. É fundamental que cada bloco seja codificado separadamente, pois a junção dos blocos codificados em um único número tornaria a decodificação impossível (Coutinho, 2016).

A codificação de um bloco b é realizada por meio da seguinte operação: calculamos o resto da divisão de b^3 por n . Esse resto, que representa o bloco codificado $C(b)$, é obtido utilizando a aritmética modular (Coutinho, 2016).

Coutinho (2016, p. 150-151) apresenta os seguintes cálculos:

$$102^3 \equiv 102^2 \times 102 \equiv 238 \times 102 \equiv 24276 \equiv 34 \pmod{391}. \quad (3.6)$$

Codificando toda a mensagem passo a passo, temos o seguinte:

$$\begin{aligned} 224^3 &\equiv 224^2 \times 224 \equiv 128 \times 224 \equiv 129 \pmod{391}; \\ 99^3 &\equiv 99^2 \times 99 \equiv 26 \times 99 \equiv 228 \pmod{391}; \\ 109^3 &\equiv 109^2 \times 109 \equiv 151 \times 109 \equiv 37 \pmod{391}; \\ 92^3 &\equiv 92^2 \times 92 \equiv 253 \times 92 \equiv 207 \pmod{391}; \\ 41^3 &\equiv 41^2 \times 41 \equiv 117 \times 41 \equiv 105 \pmod{391}; \\ 122^3 &\equiv 122^2 \times 122 \equiv 26 \times 122 \equiv 44 \pmod{391}; \\ 142^3 &\equiv 142^2 \times 142 \equiv 223 \times 142 \equiv 386 \pmod{391}; \\ 5^3 &\equiv 5^2 \times 5 \equiv 25 \times 5 \equiv 125 \pmod{391}. \end{aligned}$$

Reunindo todos os blocos, descobrimos que a mensagem codificada é

34 - 129 - 228 - 37 - 207 - 105 - 44 - 386 - 125.

A decodificação de uma mensagem RSA requer uma chave secreta (n, d) , onde d é o inverso modular de 3 em relação a $(p - 1)(q - 1)$. Para decodificar um bloco codificado a , calculamos $D(a)$ como o resto da divisão de a^d por n . Em termos de aritmética modular, $D(a)$ é o resíduo de a^d módulo n . A validade desse processo de decodificação, ou seja, a garantia de que $D(C(b)) = b$, é um resultado fundamental da teoria RSA (Coutinho, 2016).

O processo de decodificação se baseia em propriedades específicas da aritmética modular. Essas propriedades, que não serão demonstradas neste texto, são fundamentais para garantir a correta recuperação dos dados originais. As demonstrações detalhadas podem ser encontradas na obra *Criptografia* de Coutinho (2016).

Antes de realizarmos um exemplo de decodificação, analisemos como calcular o valor de d de forma eficiente. Para exemplificar o processo, assumiremos que p e q deixam resto 5 na divisão por 6. Assim, temos que:

$$p \equiv 5 \pmod{6} \text{ e } q \equiv 5 \pmod{6}.$$

Assim, podemos concluir que:

$$(p - 1)(q - 1) \equiv 4 \times 4 \equiv 16 \equiv 4 \equiv -2 \pmod{6},$$

que pode ser escrito como

$$(p - 1)(q - 1) = 6 \times k - 2,$$

onde k é inteiro positivo (Coutinho, 2016).

Segundo Coutinho (2016, p.153): “o inverso de 3 módulo $(6k - 2)$ é igual a $(4k - 1)$. Logo, podemos tomar $d = 4k - 1$ ”.

Usando agora os valores de $p = 17$ e $q = 23$, obtemos

$$(p - 1)(q - 1) = 16 \times 22 = 352 = 6 \times 58 + 4,$$

que pode ser reescrito como

$$(p - 1)(q - 1) = 6 \times 59 - 2.$$

Obtemos desta forma $k = 59$ e $d = 4 \times 59 - 1 = 235$ (Coutinho, 2016).

Aplicando a fórmula de decodificação ao primeiro bloco (3.6), obtemos

$$D(34) = 34^{235} \pmod{391}. \quad (3.7)$$

A avaliação direta de (3.7) é computacionalmente difícil. Para contornar essa dificuldade, empregamos o Teorema Chinês do Resto (Hefez, 2022), que nos permite calcular o resultado desejado de forma mais eficiente. Assim, reduzimos o problema ao cálculo de 34^{235} módulo 17 e módulo 23, que são os fatores primos de 391 (Coutinho, 2016).

Como

$$34 \equiv 0 \pmod{17},$$

$$34 \equiv 11 \pmod{23},$$

temos que

$$34^{235} \equiv 0^{235} \equiv 0 \pmod{17},$$

$$34^{235} \equiv 11^{235} \equiv (11^{22})^{10} 11^{15} \equiv 11^{15} \pmod{23}.$$

Mas,

$$11 \equiv -12 \equiv -4 \cdot 3 \pmod{23},$$

de forma que

$$11^{235} \equiv 11^{15} \equiv -4^{15} \cdot 3^{15} \pmod{23}.$$

Contudo,

$$4^{11} \equiv 1 \pmod{23},$$

$$3^{11} \equiv 1 \pmod{23},$$

de modo que

$$4^{15} = 2^{30} = (2^{11})^2 \cdot 2^8 \equiv 2^8 \equiv 3 \pmod{23},$$

$$3^{15} = 3^{11} \cdot 3^4 \equiv 3^4 \equiv 12 \pmod{23}.$$

Donde podemos concluir que

$$11^{235} \equiv -4^{15} \cdot 3^{15} \equiv -3 \cdot 12 \equiv 10 \pmod{23}.$$

Portanto,

$$34^{235} \equiv 0 \pmod{17},$$

$$34^{235} \equiv 10 \pmod{23}.$$

Isto corresponde ao sistema

$$x \equiv 0 \pmod{17}, \tag{3.8}$$

$$x \equiv 10 \pmod{23}, \tag{3.9}$$

que podemos resolver utilizando o algoritmo chinês do resto. De (3.9), temos que

$$x = 10 + 23y. \tag{3.10}$$

Substituindo (3.10) em (3.8), obtemos que

$$10 + 23y \equiv 0 \pmod{17}.$$

Assim,

$$6y \equiv 7 \pmod{17}.$$

Porém, 6 tem inverso 3 módulo 17, de forma que

$$y \equiv 3 \cdot 7 \equiv 4 \pmod{17}.$$

Portanto,

$$x = 10 + 23y = 10 + 23(4) = 102,$$

como seria de esperar, afinal estamos decodificando 34, que corresponde à codificação do bloco 102.

No exemplo apresentado, a fatoração exigiu muitos cálculos, mesmo trabalhando com números primos relativamente pequenos. Imagine agora a dificuldade de fatorar a chave pública do RSA com um número gigantesco resultante da multiplicação de dois primos enormes. Essa tarefa é tão complexa que, mesmo com a mais avançada tecnologia computacional, levaria um tempo inimaginavelmente longo para ser realizada. Segundo Bluestein (2024, n.p): “Com a tecnologia atual, quebrar o padrão RSA mais avançado poderia levar bilhões de anos”.

No entanto, a ascensão da computação quântica traz uma grande ameaça a esse sistema. A computação quântica promete revolucionar a computação, e com ela, a capacidade de quebrar os sistemas de criptografia atuais. Peter Shor apresentou em 1994 um algoritmo quântico capaz de fatorar números inteiros em tempo polinomial, o que tornaria a quebra do RSA uma tarefa trivial para um computador quântico suficientemente poderoso. Considerando que cerca de 90% das conexões online dependem do RSA, as implicações dessa ameaça são vastas. Embora os computadores quânticos ainda estejam em desenvolvimento, projeções indicam que um dispositivo capaz de quebrar o RSA em menos de um dia pode estar disponível em menos de 15 anos (Bluestein, 2024).

A Criptografia RSA revolucionou a segurança digital. No entanto, a iminente era da computação quântica exige uma revisão dos sistemas de segurança vigentes. A capacidade dos computadores quânticos de quebrar a criptografia RSA em tempo recorde torna a busca por novos algoritmos pós-quânticos uma prioridade global. A transição para esses novos padrões, embora desafiadora, é fundamental para garantir a confidencialidade e a integridade das informações em um mundo cada vez mais digitalizado e dependente de tecnologias da informação.

3.6.1 QUEM QUER SER MILIONÁRIO?

A Matemática, com sua estrutura lógica e abstrata, desperta fascínio por abordar problemas que desafiam a mente humana ao longo dos séculos. Para muitos, a busca por soluções matemáticas é uma forma de prazer intelectual, mas para outros, essa busca também pode trazer recompensas materiais importantes. É o caso de pessoas que encaram desafios matemáticos

ligados aos números primos, que oferecem tanto a recompensa de um reconhecimento mundial quanto a possibilidade de receber um prêmio milionário.

Dois desafios de destaque relacionados aos números primos são: a conjectura dos primos gêmeos – que busca provar a existência infinita de pares de primos com diferença de 2 – e a conjectura de Goldbach, a qual afirma que todo número par maior que 2 pode ser decomposto na soma de dois números primos. Essas afirmações, embora não demonstradas, são consideradas verdadeiras pela comunidade matemática e representam dois dos maiores desafios da área. Quem conseguir desvendar qualquer um desses mistérios estará garantindo seu nome nos anais da história (Shalit, 2022).

Agora, se além da fama alguém quiser desfrutar um prêmio milionário, a conversa é outra. Em 2000, o *Clay Mathematics Institute* lançou os Problemas do Milênio, uma lista de sete problemas considerados fundamentais na Matemática. Cada um deles, se resolvido, garantiria ao solucionador uma recompensa de um milhão de dólares. Um desses problemas é a famosa hipótese de Riemann, que trata da distribuição dos números primos. Essa conjectura, proposta pelo matemático Bernhard Riemann em 1859, sugere que os zeros não triviais da função zeta (ζ) de Riemann possuem uma parte real igual a $\frac{1}{2}$, o que implica um padrão específico na distribuição dos números primos. A importância dessa hipótese não está apenas no campo teórico, mas também em áreas práticas, como a criptografia, onde os números primos desempenham um papel crucial na segurança de dados digitais (Lopes, 2017).

Dos sete problemas mencionados, um já foi solucionado. Segundo D’Ornelas (2014, n.p):

O único matemático que solucionou um dos problemas até o momento foi o russo Grigori Perelman, que encontrou a resposta de uma hipótese intitulada Conjectura de Poincaré. Em 2003, ele publicou uma série de artigos explicando a resolução do problema e, após análises cuidadosas, ele foi agraciado com o prêmio milionário – mas, para a surpresa de todos, ele recusou o prêmio e a Medalha Fields, em 2006 – o mais alto prêmio da área, considerado o Nobel de Matemática.

A resolução da hipótese de Riemann representaria um marco histórico na Matemática, revolucionando nossa compreensão dos números primos e abrindo portas para avanços em diversas áreas do conhecimento. A recompensa financeira, embora significativa, é apenas um reflexo do prestígio e do impacto que uma descoberta dessa magnitude teria na comunidade científica mundial. Resolver um dos problemas do milênio seria um feito de proporções épicas, digno dos maiores gênios matemáticos (Sautoy, 2008).

3.6.2 A HIPÓTESE DE RIEMANN

A hipótese de Riemann está diretamente ligada à busca por padrões na distribuição dos números primos, um problema que intriga matemáticos desde a antiguidade. Conhecida como um dos maiores mistérios da Matemática, a hipótese de Riemann tem suas raízes no século XIX,

mais precisamente em 1859, com o trabalho de Bernhard Riemann. O matemático alemão, ao expandir as ideias de Leonhard Euler sobre a função zeta, desenvolveu uma fórmula que permitia calcular a quantidade de números primos menores que um determinado valor. Essa fórmula, no entanto, dependia de uma suposição crucial sobre os zeros da função zeta, que Riemann não conseguiu provar. Essa suposição ficou conhecida como hipótese de Riemann (Sautoy, 2008).

Segundo Barata (2024), a função zeta, apresentada inicialmente por Leonhard Euler em seu artigo de 1748 intitulado *Variae observationes circa series infinitas*, é a série infinita

$$\sum_{n \geq 1} \frac{1}{n^s} = \frac{1}{1^s} + \frac{1}{2^s} + \frac{1}{3^s} + \frac{1}{4^s} + \frac{1}{5^s} + \dots,$$

também representada (Devlin, 2008, p. 65) como

$$\zeta(s) = \frac{1}{1^s} + \frac{1}{2^s} + \frac{1}{3^s} + \frac{1}{4^s} + \frac{1}{5^s} + \dots.$$

Euler começou os estudos da função zeta com valores de $s \in \mathbb{R}$. No decorrer de suas investigações, estabeleceu uma surpreendente ligação entre a série e os números primos, resultando na fórmula do produto de Euler:

$$\sum_{n \geq 1} \frac{1}{n^s} = \prod_p \frac{1}{1 - \frac{1}{p^s}},$$

onde p percorre o conjunto de todos os números primos. É relevante ressaltar que essa série converge uniformemente para $s > 1$. No caso particular em que $s = 1$, a série se reduz à série harmônica, conhecida por divergir (Barata, 2024).

A função zeta de Euler, embora definida por uma série infinita, apresenta propriedades matemáticas que a tornam um objeto de estudo fascinante. Seu gráfico contínuo e suave permite a aplicação de técnicas do Cálculo Diferencial e Integral. No entanto, quando restringimos a função zeta aos números reais, sua estrutura unidimensional limita nossa capacidade de explorar padrões mais complexos, como a distribuição dos números primos. Riemann, em uma demonstração de genialidade, ao substituir o número real s por um número complexo z , estendeu a função zeta para o domínio dos números complexos, fazendo com que os valores de $\zeta(z)$ também fossem complexos. Após isso, essa função ficou conhecida como função zeta de Riemann (Devlin, 2008).

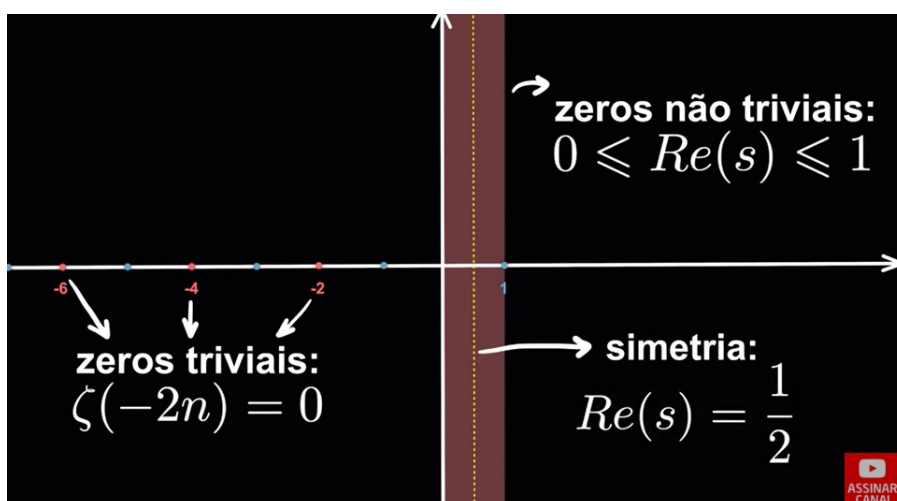
Essa extensão, realizada através da continuação analítica, permitiu calcular a função zeta para quase todos os números complexos, revelando uma estrutura rica e complexa. Riemann observou uma profunda conexão entre os zeros da função zeta no plano complexo e a distribuição dos números primos. Sua conjectura sobre a localização desses zeros, embora ainda não provada, forneceu as bases para a demonstração do Teorema dos Números Primos elaborada por Jacques Salomon Hadamard (1865 – 1963) e Charles-Jean Étienne Gustave Nicolas de la Vallée Poussin (1866 – 1962) em 1896 (Devlin, 2008).

Segundo Devlin (2008, p. 67): “O elo fundamental entre a função zeta e os números primos que Riemann encontrou foi a ligação estreita entre a função de densidade D_n e as soluções da equação $\zeta(z) = 0$ ”.

Os zeros da função zeta são os valores de z para os quais $\zeta(z)$ se anula. Riemann observou que a função zeta possui zeros triviais nos números inteiros pares negativos. No entanto, a parte mais intrigante da sua pesquisa diz respeito aos outros zeros, chamados de não triviais. Riemann conjecturou que todos esses zeros não triviais estão localizados em uma reta vertical específica no plano complexo, denominada reta crítica (Devlin, 2008).

Como salienta Barata (2024, item 4, n.p): “[...] Riemann, visando dar um norte no caminho para a demonstração do Teorema dos Números Primos, fez uma afirmação forte sobre os zeros não triviais: todos os zeros não triviais tem parte real igual a $\frac{1}{2}$ ”. A Figura 3.13 ilustra onde se encontram os zeros triviais e os zeros não triviais da hipótese de Riemann. A linha pontilhada amarela representa a reta crítica, onde Riemann afirma que todos os zeros não triviais se encontram.

Figura 3.13 – Reta crítica da hipótese de Riemann



Fonte: Nunes (2023).

A hipótese de Riemann, permanece sem solução há mais de 160 anos. Ela se resume a uma pergunta simples: todos os zeros não triviais da função zeta de Riemann estão localizados na reta crítica? Computadores já encontraram mais de 12 trilhões de zeros não triviais da função zeta, todos alinhados com a hipótese de Riemann. Godfrey Harold Hardy (1877 – 1947) também provou que existem infinitos zeros com parte real $\frac{1}{2}$. Apesar dessas evidências, a hipótese permanece um enigma (Nunes, 2023).

A resolução da hipótese de Riemann, embora seja um objetivo puramente matemático, poderia ter um impacto profundo e inesperado em nossa vida cotidiana. A segurança de muitas transações se baseia na dificuldade de fatorar grandes números primos. Uma compreensão mais profunda da distribuição desses números, proporcionada por uma prova da hipótese, poderia comprometer a segurança desses sistemas criptográficos. Há uma ironia em torno dessa questão,

a qual se evidencia no fato de que muitas empresas que dependem dessa segurança financiam pesquisas para provar a hipótese, criando uma dinâmica complexa entre a pesquisa fundamental e suas aplicações. Além das implicações para a criptografia, a prova da hipótese de Riemann teria um impacto profundo em diversas áreas da Matemática, revelando conexões entre diferentes ramos da ciência (Sautoy, 2008).

4 NÚMEROS PERFEITOS

A fascinação da humanidade pelos números perfeitos remonta à antiguidade. Esses números, que são iguais à soma de seus divisores próprios, despertaram a curiosidade de matemáticos e filósofos ao longo dos séculos. Para os gregos antigos, os números perfeitos carregavam um significado místico, associado à perfeição divina (Eves, 2011).

Os pitagóricos não enxergavam os números apenas como quantidades, mas viam neles qualidades especiais. Os números perfeitos, em particular, eram vistos como a representação da perfeição e da harmonia do universo. Na visão pitagórica, o número 6, por exemplo, representava o equilíbrio por ser o primeiro número perfeito (Boyer, 1974).

A Definição 4.1 estabelece o conceito de números perfeitos (Costa, 2015, p. 42). De acordo com Gomes, Costa e Santos (2008, p. 100), a função σ na Definição 4.1, estabelecida por Euler, é “a função que associa a cada natural n a soma de seus divisores, isto é, $\sigma(n)$ é a soma dos divisores positivos de n , incluindo o n ”.

Definição 4.1. *Um número natural diz-se perfeito se for igual à soma de todos os seus divisores positivos com exceção dele próprio, ou seja, se $n = \sigma(n) - n$ se, e somente se, $\sigma(n) = 2n$.*

Segundo Santos (2020, p. 1):

O mais antigo texto onde os números perfeitos são mencionados é também um dos textos matemáticos mais famosos jamais escritos: os Elementos de Euclides, que datam aproximadamente de 300 a.C.. Aí, Euclides define um número perfeito como sendo um número natural cuja soma dos divisores próprios (isto é, os divisores diferentes do próprio número) seja igual ao número de que se partiu. O menor número perfeito é 6: a soma dos seus divisores próprios (1, 2 e 3) é 6. O exemplo seguinte é 28. Os divisores próprios de 28 são 1, 2, 4, 7 e 14 e a soma destes números é 28.

Na época de Euclides, os números perfeitos 6, 28, 496 e 8128 já eram conhecidos, mas não foram objeto de estudo específico por parte do matemático grego. Euclides apresentou um resultado muito mais profundo: uma fórmula para a construção de números perfeitos. Segundo essa fórmula, se considerarmos um número natural n e verificarmos se $2^n - 1$ é um número primo, então o número resultante da multiplicação de $2^n - 1$ por 2^{n-1} será um número perfeito.

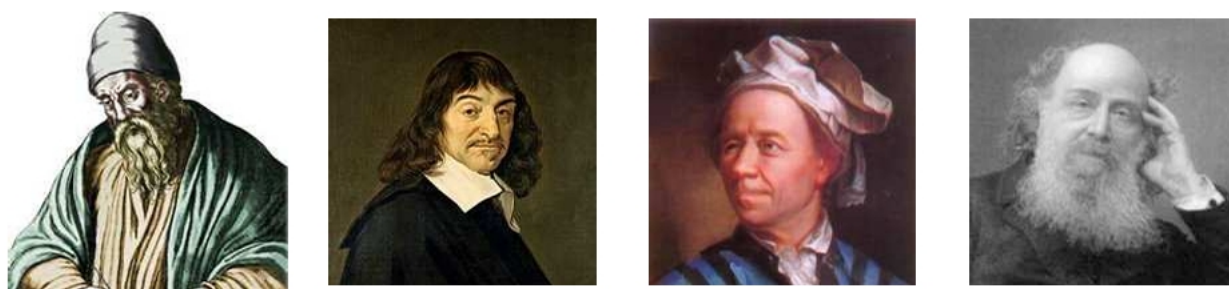
No século II d.C., matemáticos gregos como Nicômaco de Gerasa (60 – 120) e Theon de Esmirna (70 – 135) ampliaram o estudo dos números perfeitos, classificando os números naturais em três categorias: perfeitos, abundantes e deficientes. Nicômaco, em sua obra *Introdução à Aritmética*, apresentou os primeiros quatro números perfeitos conhecidos e definiu os conceitos de números abundantes e deficientes (Knill, 2007).

Segundo Fonseca e Lima (2001, p. 39):

Se n é um número natural, denotamos por $d(n)$ o conjunto dos divisores próprios (diferentes de n) de n , e $s(n)$ indica a soma desses divisores. Um número é dito abundante quando a soma de seus divisores próprios for maior que o próprio número. Quando a soma de seus divisores próprios for menor que ele, então o número é chamado deficiente. Por exemplo,
 $d(24) = \{1, 2, 3, 4, 6, 8, 12\}$, $s(24) = 1 + 2 + 3 + 4 + 6 + 8 + 12 = 36$, e, $s(24) > 24$, então 24 é um número abundante;
 $d(16) = \{1, 2, 4, 8\}$, $s(16) = 15$, e, $s(16) < 16$, então 16 é um número deficiente.

O estudo dos números perfeitos, iniciado na Antiguidade, ganhou um novo impulso a partir do segundo milênio, com a contribuição de grandes matemáticos como René Descartes (1596 – 1650), Leonhard Euler e James Joseph Sylvester (1814 – 1897). Seus trabalhos lançaram as bases para pesquisas mais aprofundadas sobre o tema (Knill, 2007). A Figura 4.1 ilustra alguns dos matemáticos que contribuíram para o estudo dos números perfeitos.

Figura 4.1 – Matemáticos que estudaram os números perfeitos: Euclides de Alexandria, René Descartes, Leonhard Euler e James Joseph Sylvester

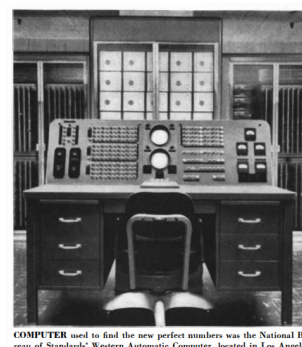


Fonte: Knill (2007).

Por séculos, apenas os quatro primeiros números perfeitos, registrados na obra de Nicômaco, eram conhecidos. A partir do século XVI, a busca por esses números raros ganhou novo impulso. Hudalrichus Regius foi o primeiro a expandir essa lista, em 1536. Na sequência, Pietro Antonio Cataldi (1548 – 1626) contribuiu com mais duas descobertas em 1588. Somente em 1750, Euler adicionou o oitavo número perfeito à sequência, demonstrando a persistência dos matemáticos em desvendar os mistérios desses números especiais (Koshy, 2007).

A partir da década de 1950, o uso de computadores como o SWAC – Figura 4.2, BESK e IBM 7090 impulsionou significativamente a descoberta de novos números perfeitos. Entre 1952 e 1961, diversos valores para n na fórmula de Euclides foram identificados, expandindo a lista de números perfeitos conhecidos. Em 1985, utilizando um supercomputador Cray X-MP, a quantidade de números perfeitos conhecidos chegou a 30, com o valor para n abaixo de 216.091. A evolução da capacidade computacional permitiu explorar valores cada vez maiores de

Figura 4.2 – Computador SWAC



COMPUTER used to find the new perfect numbers was the National Bureau of Standards' Western Automatic Computer, located in Los Angeles.

Fonte: Reid (1953).

n , revelando a complexidade e a raridade desses números (Eves, 2011). A Figura 4.2, apresenta o *Standards Western Automatic Computer* (SWAC), utilizado na descoberta dos novos números perfeitos no *National Bureau of Standards*, em Los Angeles (Reid, 1953).

Segundo o GIMPS (2024b), no dia 12 de outubro de 2024 foi descoberto um novo número perfeito. Com uma representação matemática de $2^{136.279.840} \times (2^{136.279.841} - 1)$, esse número possui mais de 82 milhões de dígitos, tornando-o o maior já encontrado. A Tabela 4.1 relaciona os dez maiores números perfeitos descobertos até outubro de 2024.

Tabela 4.1 – Dez maiores números perfeitos

CLASSIFICAÇÃO	PRIMOS	DÍGITOS(aproximado)	DATA
1	$2^{136279840} \times (2^{136279841} - 1)$	82 milhões	Out 2024
2	$2^{82589932} \times (2^{82589933} - 1)$	49 milhões	Dez 2018
3	$2^{77232916} \times (2^{77232917} - 1)$	46 milhões	Dez 2017
4	$2^{74207280} \times (2^{74207281} - 1)$	44 milhões	Jan 2016
5	$2^{57885160} \times (2^{57885161} - 1)$	34 milhões	Jan 2013
6	$2^{43112608} \times (2^{43112609} - 1)$	25 milhões	Ago 2008
7	$2^{42643800} \times (2^{42643801} - 1)$	25 milhões	Jun 2009
8	$2^{37156666} \times (2^{37156667} - 1)$	22 milhões	Set 2008
9	$2^{32582656} \times (2^{32582657} - 1)$	19 milhões	Set 2006
10	$2^{30402456} \times (2^{30402457} - 1)$	18 milhões	Dez 2005

Fonte: GIMPS (2024b).

Os números perfeitos têm uma história rica que atravessa civilizações, passando por um objeto de fascínio místico e simbólico a uma peça importante na Teoria dos Números. Essa jornada demonstra como certos conceitos matemáticos resistem ao tempo e continuam a ser explorados com ferramentas modernas, mantendo-se enigmáticos e instigantes.

4.1 TEOREMA DE EUCLIDES-EULER

Desde a antiguidade, os números perfeitos têm sido um mistério que intriga os amantes da Matemática. Dentre as joias da Teoria dos Números, certamente o Teorema de Euclides-Euler ocupa um lugar de destaque. Esse teorema esclarece parte desse enigma, revelando uma expressão concisa para a geração de números perfeitos pares.

O teorema de Euclides-Euler, resultado de um trabalho conjunto de dois grandes matemáticos, estabelece uma caracterização completa dos números perfeitos pares. Euclides demonstrou que se $2^p - 1$ é um número primo, então o número $N = 2^{p-1}(2^p - 1)$ é perfeito. Nicômaco conjecturou que todos os números perfeitos pares se encaixavam nessa fórmula. Euler, por volta de 1747, provou essa conjectura, resultando no teorema de Euclides-Euler: um número par N é perfeito se, e somente se, pode ser expresso na forma $N = 2^{p-1}(2^p - 1)$, onde $2^p - 1$ é um número primo (Viana, 2024a).

Para demonstrar o teorema de Euclides-Euler, é fundamental compreender a função sigma (σ), que associa a cada número natural a soma de seus divisores positivos. Segundo Garcia (2016, p. 5, tradução nossa): “ $\sigma(n)$ = a soma de todos os divisores únicos de n , incluindo 1 e n ”. Logo, quando $\sigma(n) = 2n$, temos um número perfeito. O Exemplo 4.1 ilustra a função sigma de alguns números naturais.

Exemplo 4.1. *Soma dos divisores de alguns números naturais:*

$$\sigma(4) = 1 + 2 + 4 = 7;$$

$$\sigma(5) = 1 + 5 = 6;$$

$$\sigma(6) = 1 + 2 + 3 + 6 = 12;$$

$$\sigma(10) = 1 + 2 + 5 + 10 = 18;$$

$$\sigma(15) = 1 + 3 + 5 + 15 = 24;$$

$$\sigma(20) = 1 + 2 + 4 + 5 + 10 + 20 = 42;$$

$$\sigma(28) = 1 + 2 + 4 + 7 + 14 + 28 = 56.$$

A função sigma possui algumas propriedades, as quais são detalhadas por Garcia (2016, p. 6-8, tradução nossa) no Teorema 4.1.

Teorema 4.1. *(Propriedades da função sigma)*

(a) Se p é um primo e $k \geq 1$, então

$$\sigma(p^k) = 1 + p + p^2 + \dots + p^k = \frac{p^{k+1} - 1}{p - 1}.$$

(b) Se $(m, n) = 1$, então

$$\sigma(mn) = \sigma(m)\sigma(n).$$

Demonstração.

(a) Se p é primo, então é divisível apenas por 1 e por si mesmo. Segue-se que os divisores de p^k são da forma p^i para todo i tal que $0 \leq i \leq k$. Ou seja, podemos escrever

$$\sigma(p^k) = 1 + p + p^2 + \dots + p^k. \quad (4.1)$$

Observe que a soma (4.1), é a soma de uma progressão geométrica e pode ser escrita na forma $\sum_{j=0}^n ar^j$. Começamos definindo S tal que

$$S = \sum_{j=0}^n ar^j. \quad (4.2)$$

Multiplicando (4.2) por r , obtemos:

$$\begin{aligned}
 rS &= r \sum_{j=0}^n ar^j; \\
 rS &= \sum_{j=0}^n ar^{j+1}; \\
 rS &= \sum_{k=1}^{n+1} ar^k; \\
 rS &= \sum_{k=0}^n ar^k + (ar^{n+1} - a); \\
 rS &= S + (ar^{n+1} - a); \\
 S &= \frac{ar^{n+1} - a}{r - 1}.
 \end{aligned} \tag{4.3}$$

De (4.1), temos que $a = 1$ e $r = p$. Substituindo esses valores em (4.3), concluímos que

$$\sigma(p^k) = \frac{p^{k+1} - 1}{p - 1}.$$

□

Para provar o item (b) do Teorema 4.1, devemos antes provar o Lema 4.1.

Lema 4.1. *Se a e b são números inteiros primos entre si, com $\{a_i : 1 \leq i \leq s\}$ e $\{b_j : 1 \leq j \leq t\}$ sendo todos os divisores de a e b , respectivamente, então $S = \{a_i b_j : 1 \leq i \leq s, 1 \leq j \leq t\}$ são todos os divisores de ab .*

Demonstração. Seja D o conjunto de todos os divisores positivos de ab . Como a e b são primos entre si, $a_i \mid a$, $b_j \mid b$ e $(a_i, b_j) = 1$, então $a_i b_j \mid ab$ e $a_i b_j$ é divisor de ab . Portanto, $S \subseteq D$.

Agora, consideremos um divisor d qualquer de ab . Como $(a, b) = 1$ e $d \mid ab$, existem inteiros positivos e e f únicos tais que

$$d = ef, \text{ com } e \mid a \text{ e } f \mid b.$$

Ou seja, todo divisor positivo de ab pode ser escrito unicamente como produto de um divisor de a por um divisor de b . Isso mostra que $D \subseteq S$.

Como mostramos que $S \subseteq D$ e $D \subseteq S$, concluímos que $S = D$. Portanto, o conjunto S contém todos os divisores positivos de ab .

□

Agora podemos prosseguir com a demonstração do item (b) do Teorema (4.1).

Demonstração.

- (b) Sejam $\{a_i : 1 \leq i \leq s\}$ e $\{b_j : 1 \leq j \leq t\}$ os divisores de a e b , respectivamente. Desta forma, temos que $\sigma(a)\sigma(b) = \sum_i a_i \sum_j b_j = \sum_i \sum_j a_i b_j = \sum_{d|ab} d = \sigma(ab)$.

□

Uma vez demonstradas as propriedades da função sigma, estamos aptos a demonstrar o teorema de Euclides-Euler - Teorema 4.2 (Gomes; Costa; Santos, 2008, p. 104-105).

Teorema 4.2. (*Euclides-Euler*) Um número natural n é um número perfeito par se, e somente se, $n = 2^{p-1}(2^p - 1)$, sendo $2^p - 1$ um número primo.

Demonstração. Suponhamos que $n = 2^{p-1}(2^p - 1)$, sendo $2^p - 1$ primo. Logo, $p > 1$ e, consequentemente, n é par. Como $2^p - 1$ é ímpar, temos que $(2^{p-1}, 2^p - 1) = 1$. Assim,

$$\sigma(n) = \sigma\left((2^{p-1})(2^p - 1)\right) = \sigma(2^{p-1})\sigma(2^p - 1) = \frac{(2^p - 1)}{2 - 1} 2^p = 2n.$$

Portanto, n é perfeito.

Reciprocamente, suponhamos que n é perfeito e par. Seja 2^{p-1} a maior potência de 2 que divide n . Logo, $p > 1$, $n = 2^{p-1}q$, com q ímpar, e $\sigma(n) = (2^p - 1)\sigma(q)$. Como $\sigma(n) = 2n$, segue que $(2^p - 1)\sigma(q) = 2^p q$. Disto decorre que $(2^p - 1) \mid q$, pois $(2^p, 2^p - 1) = 1$. Assim, existe $c \in \mathbb{N}$, com $c < q$, tal que $q = c(2^p - 1)$. Portanto, $(2^p - 1)\sigma(q) = 2^p q = 2^p(2^p - 1)c$ e $\sigma(q) = 2^p c$.

Temos que q e c são dois divisores distintos de q , tais que $c + q = 2^p c$. Nessa situação, $c = 1$. De fato, suponhamos que $c \neq 1$. Assim, $\sigma(q) \geq 1 + c + q > c + q = 2^p c$. Disto segue que $2^p c = c + q < \sigma(q) = 2^p c$, uma contradição. Portanto, $\sigma(q) = q + 1$, ou seja, q é primo. Desta forma, $n = 2^{p-1}(2^p - 1)$, sendo que $2^p - 1$ é primo.

□

Embora o teorema ofereça uma caracterização elegante dos números perfeitos pares, a questão da infinitude desses números permanece em aberto. Apesar dos esforços da comunidade matemática, uma resposta definitiva ainda é desconhecida (Koshy, 2007).

A descoberta de Euler e Euclides revolucionou a busca por números perfeitos pares, estabelecendo uma correspondência direta com os primos de Mersenne. Graças a essa relação, a tarefa de encontrar novos números perfeitos pares se resume à identificação de novos primos de Mersenne (Santos, 2020).

4.2 PARIDADE

Os números perfeitos, além de sua rica simbologia que transcende a Matemática, despertam curiosidade por suas propriedades únicas. Um fato interessante sobre esses números é que todos os números perfeitos conhecidos são pares.

Baseados nos quatro primeiros números perfeitos encontrados, os matemáticos da época formularam várias hipóteses que, posteriormente, se mostraram incorretas. De acordo com Bege e Fogarasi (2009, p. 74, tradução nossa), as hipóteses tomadas como verdadeiras eram:

Como a fórmula $2^{n-1}(2^n - 1)$ fornece os primeiros quatro números perfeitos para $n=2,3,5$ e 7 respectivamente, o quinto número perfeito seria obtido quando $n=11$. No entanto, $2^{11} - 1 = 23 \times 89$ não é primo, portanto este não produz um número perfeito.

O quinto número perfeito teria cinco dígitos, já que os quatro primeiros tinham 1, 2, 3 e 4 dígitos respectivamente, mas possui 8 dígitos. Os números perfeitos terminaria alternadamente em 6 ou 8.

O quinto número perfeito realmente termina com 6, mas o sexto também termina com um 6, portanto a alternância é perturbada.

Em 1747, Leonhard Euler apresentou uma prova definitiva de que todos os números perfeitos pares seguem a fórmula descrita por Euclides, confirmando uma antiga conjectura de Alhazém - Abu Ali Haçane ibne Alhaitame (965 – 1040). Essa descoberta desmistificou a ideia de que os números perfeitos apresentavam uma alternância regular entre os algarismos 6 e 8 nas unidades. Contudo, Euler e o matemático italiano Pietro Cataldi haviam notado anteriormente que o último dígito de qualquer número perfeito par, independentemente do método de obtenção, é necessariamente 6 ou 8 (Santos, 2020) – Proposição 4.1 (Voight, 1998, p. 8, tradução nossa).

Proposição 4.1. *Todo número par perfeito termina em 6 ou 8.*

Demonstração. Todo primo maior do que 2 é da forma $4m + 1$ ou $4m + 3$. Para a primeira forma, temos que:

$$\begin{aligned} N &= 2^{n-1}(2^n - 1) = 2^{4m}(2^{4m+1} - 1) = 16^m(2 \cdot 16^m - 1) \equiv 6^m(2 \cdot 6^m - 1) \pmod{10} \equiv \\ &\equiv 6(12 - 1) \pmod{10} \equiv 6 \pmod{10}, \end{aligned}$$

uma vez que, por indução, pode-se verificar que $6^m \equiv 6 \pmod{10}$ para todo m . Da mesma maneira, temos para a segunda forma que:

$$N = 4 \cdot 16^m(8 \cdot 16^m - 1) \equiv 4 \cdot 6(8 \cdot 6 - 1) \pmod{10} \equiv 4(8 - 1) \pmod{10} \equiv 8 \pmod{10},$$

isto porque $16^m \equiv 6 \pmod{10}$.

□

As Proposições 4.2 e 4.3 estabelecem outras propriedades dos números perfeitos pares (Gomes; Costa; Santos, 2008, p. 106-108).

Proposição 4.2. *Se $N > 6$ é um número perfeito par, então $N - 1$ é divisível por 3.*

Demonstração. Todo número perfeito par tem a forma $N = 2^{p-1}(2^p - 1)$, onde p é primo e $2^p - 1$ também é primo (primo de Mersenne). Como $N > 6$, temos $p > 2$, então p é ímpar.

Note que $2^p \equiv 2 \pmod{3}$ quando p é ímpar, pois as potências de 2 módulo 3 são periódicas com período 2: $2^1 \equiv 2$, $2^2 \equiv 1$, $2^3 \equiv 2$, e assim sucessivamente.

Assim:

$$2^p \equiv 2 \pmod{3} \Rightarrow 2^p - 1 \equiv 1 \pmod{3},$$

e

$$2^{p-1} \equiv 1 \pmod{3} \quad (\text{já que } p - 1 \text{ é par}).$$

Portanto,

$$N = 2^{p-1}(2^p - 1) \equiv 1 \cdot 1 = 1 \pmod{3} \Rightarrow N - 1 \equiv 0 \pmod{3}.$$

Logo, $3 \mid (N - 1)$.

□

Proposição 4.3. *A soma iterativa dos algarismos de um número perfeito par, distinto de 6, é igual a 1, isto é, dado um número perfeito par, se somarmos os seus algarismos e, em seguida somarmos sucessivamente os algarismos do resultado obtido, a soma final será igual a 1.*

Demonstração. Observemos inicialmente que a soma iterativa de um número é simplesmente a sua classe de congruência módulo 9, pois se $N = a_r \cdots a_1 a_0$, sendo a_i , com $i \in \{0, 1, 2, \dots, r\}$, os dígitos do número N , então

$$N = \sum_{i=0}^r a_i 10^i \equiv \sum_{i=0}^r a_i (1)^i = \sum_{i=0}^r a_i \pmod{9}.$$

Basta agora mostrar que se N é perfeito par, então $N \equiv 1 \pmod{9}$.

Seja $N = 2^{n-1}(2^n - 1)$ um número perfeito par. Se tivéssemos $n \equiv 0 \pmod{3}$, ou seja, 3 divide n , então n não seria primo e, portanto, $2^n - 1$ também não seria primo. Assim, N não seria perfeito, uma contradição.

Se $n \equiv 1 \pmod{3}$, isto é, $n = 3k_1 + 1$ para algum $k_1 > 0$, como n é primo e $N \neq 6$, segue que n é ímpar. Consequentemente, $n = 3k_1 + 1$ é também da forma $6k + 1$, com $k \in \mathbb{N}$ e $N = 2^{6k}(2^{6k+1} - 1) = (2^6)^k [2(2^6)^k - 1]$. Como $2^6 \equiv 1 \pmod{9}$, segue que $N \equiv 1(2 - 1) = 1 \pmod{9}$.

No caso em que $n \equiv 2 \pmod{3}$, isto é, $n = 3k_2 + 2$ para algum k_2 natural, como n não é par, temos que k_2 é ímpar. Assim, podemos escrever $n = 6k + 5$, onde $k_2 = 2k + 1$. Portanto,

$$\begin{aligned}
 N &= 2^{6k+4}(2^{6k+5} - 1) \\
 &= 16(2^6)^k[32(2^6)^k - 1] \\
 &\equiv 16(1)[32(1) - 1] \pmod{9} \\
 &\equiv (-2)[(-4) - 1] \pmod{9} \\
 &\equiv 10 \equiv 1 \pmod{9}.
 \end{aligned}$$

□

Os números perfeitos pares, com suas fascinantes propriedades e padrões, exemplificam ao mesmo tempo a simplicidade e a profundidade da Teoria dos Números. Desde sua descoberta foi possível perceber o vínculo entre números perfeitos e primos de Mersenne. Essas relações não apenas mostram uma estrutura singular e harmônica entre os números, mas também começam a inspirar os matemáticos a explorar os mistérios dos números perfeitos ímpares e de outros conceitos interligados. Assim, os números perfeitos pares não são apenas curiosidades matemáticas; esses números também abrem portas para novas descobertas na Teoria dos Números.

4.2.1 NÚMERO PERFEITO ÍMPAR

Um dos enigmas que desafiam a mente humana há séculos é a natureza dos números perfeitos. Embora os números perfeitos pares tenham sua estrutura desvendada por Euclides e Euler, que os relacionaram aos primos de Mersenne, a questão da existência de números perfeitos ímpares continua a ser um dos grandes mistérios da teoria dos números, intrigando matemáticos ao longo dos tempos.

A existência desses números é um dos grandes mistérios da Teoria dos Números. Ao longo dos séculos, matemáticos têm se dedicado a encontrar um número perfeito ímpar ou a provar que nenhum existe, mas até agora essa questão permanece sem resposta. No entanto, a pesquisa nessa área permitiu identificar algumas características que um número perfeito ímpar necessariamente teria, caso existisse (Gumarú; Casuco; Bernal, 2018).

Segundo Eves (2011, p. 99):

Os números perfeitos dados pela fórmula de Euclides são números pares, e Euler provou que todo número perfeito par tem essa forma. A existência ou não de números perfeitos ímpares é uma das célebres questões abertas da teoria dos números. Seguramente não há nenhum número desse tipo com menos do que 200 dígitos.

Euler, além de confirmar que a regra de Euclides engloba todos os números perfeitos pares, avançou ao demonstrar que, caso existam números perfeitos ímpares, estes têm uma

determinada estrutura (Beasley, 2013). O Teorema 4.3 descreve a forma que, segundo Euler, os números perfeitos ímpares devem ter (Beasley, 2013, p. 25, tradução nossa).

Teorema 4.3. *Se existe um número perfeito ímpar, então ele tem a forma $p^k s^2$, onde p é primo, $(p, s) = 1$ e $p \equiv k \equiv 1 \pmod{4}$.*

Demonstração. Seja N um número perfeito ímpar. Consideremos a função σ de Euler e a decomposição $N = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$, onde cada p_i é um primo ímpar e cada $k_i > 0$. Assim,

$$2N = \sigma(p_1^{k_1}) \sigma(p_2^{k_2}) \cdots \sigma(p_r^{k_r}).$$

Como $2N \equiv 2 \pmod{4}$, já que N é ímpar, exatamente um fator $\sigma(p_j^{k_j})$ é congruente com 2 módulo 4, com os outros fatores sendo todos ímpares. Além disso, como $\sigma(p_i^{k_i}) = 1 + p_i + p_i^2 + \cdots + p_i^{k_i}$, podemos considerar dois casos para p_i módulo 4.

- (a) Se $p_i \equiv 1 \pmod{4}$, então $\sigma(p_i^{k_i}) \equiv k_i + 1 \pmod{4}$. Como $\sigma(p_j^{k_j}) \equiv 2 \pmod{4}$, concluímos que $k_j \equiv 1 \pmod{4}$. Mas todos os outros $\sigma(p_i^{k_i})$ são ímpares, então k_i deve ser par para $i \neq j$.
- (b) Se $p_i \equiv 3 \equiv -1 \pmod{4}$, então os termos da soma

$$\sigma(p_i^{k_i}) = 1 + p_i + p_i^2 + \cdots + p_i^{k_i}$$

alternam-se entre $\pm 1 \pmod{4}$. Pode-se mostrar que:

- Se k_i é ímpar, então $\sigma(p_i^{k_i}) \equiv 0 \pmod{4}$;
- Se k_i é par, então $\sigma(p_i^{k_i}) \equiv 1 \pmod{4}$.

Mas, como exatamente um dos fatores $\sigma(p_j^{k_j})$ deve ser congruente a 2 $\pmod{4}$, e $\sigma(p_i^{k_i}) \equiv 0$ ou 1 $\pmod{4}$, concluímos que esse único fator não pode corresponder a um primo $p_i \equiv 3 \pmod{4}$. Logo, todos os expoentes k_i associados a tais primos devem ser pares, para que $\sigma(p_i^{k_i})$ permaneça ímpar.

□

Ao demonstrar a forma de um número perfeito ímpar, Euler abriu o caminho para que matemáticos posteriores aprofundassem a pesquisa sobre a existência desses números (Beasley, 2013).

Stevens (2012) vai além e aponta algumas restrições para a existência de números perfeitos ímpares. Uma dessas restrições é o limite inferior para o valor desses números, caso existam. Ao longo dos anos, diversos matemáticos dedicaram-se a aumentar esse limite. Kanold foi o primeiro a estabelecer um limite inferior, seguido por Tuckerman, Hagis, Brent e Cohen. Estes últimos utilizaram algoritmos sofisticados, como o método da curva elíptica, para elevar

significativamente esse limite. O recorde atual, de 10^{1500} , é resultado do trabalho de Ochem e Rao, que aperfeiçoaram os algoritmos anteriores.

Outra restrição diz respeito ao número de divisores primos de um número perfeito ímpar. Pesquisadores têm se dedicado a determinar o número mínimo de divisores primos distintos e o número total de fatores primos que um número perfeito ímpar deve possuir. Os estudos de diversos matemáticos contribuíram para estabelecer limites inferiores cada vez mais elevados. Atualmente, sabe-se que um número perfeito ímpar deve ter pelo menos 101 fatores primos, incluindo pelo menos 9 divisores primos distintos, e que seu maior divisor primo deve ser superior a 10^{62} (Stevens, 2012).

A existência de números perfeitos ímpares é condicionada não apenas pelo número de seus divisores primos, mas também pelo tamanho desses divisores. Pesquisadores como Hagis, Cohen, Jenkins e Goto dedicaram-se a determinar limites inferiores para o maior divisor primo de um número perfeito ímpar. Através de análises e algoritmos sofisticados, eles demonstraram que esse divisor primo deve ser superior a 10^8 . Além disso, Iannucci estabeleceu que os limites inferiores para o segundo e terceiro maiores divisores primos devem ser 10^4 e 10^2 respectivamente, contribuindo ainda mais para restringir as possibilidades de existência de números perfeitos ímpares (Stevens, 2012).

A busca por números perfeitos ímpares é um desafio antigo e persistente da Matemática. As rigorosas condições necessárias para a existência desses números, descobertas ao longo de séculos de investigação, sugerem que eles podem ser meramente teóricos. Apesar disso, a resolução desse enigma teria um impacto profundo na compreensão de muitas propriedades dos números inteiros.

4.2.2 NÚMEROS HIPERPERFEITOS

A busca por padrões e relações numéricas nos leva a explorar conceitos como os números perfeitos e suas extensões, os números hiperperfeitos. Enquanto os números perfeitos são caracterizados por uma relação particular entre seus divisores, os números hiperperfeitos generalizam essa ideia, definindo uma nova classe de números que satisfazem condições mais abrangentes. Essa ampliação do estudo dos divisores e suas propriedades contribui para um aprofundamento da Teoria dos Números.

A Definição 4.2 conceitua um número hiperperfeito (Purkayastha; Goswami; Debnath, 2017, p. 97, tradução nossa).

Definição 4.2. *Um número natural n é chamado de k -número hiperperfeito se existe um inteiro k tal que*

$$\sigma(n) = \frac{k+1}{k}n + \frac{k-1}{k}, \quad (4.4)$$

onde $\sigma(n)$ é a soma dos divisores positivos de n .

O Teorema 4.4 estabelece a forma de um k -número hiperperfeito (Puneeth, 2018, p. 65, tradução nossa).

Teorema 4.4. *Se $k + 1 = p$ é um primo, então o número da forma $n = p^{q-1}(p^q - k)$, onde $(p^q - k)$ é um primo, é um k -número hiperperfeito.*

Demonstração. Considerando $p = k + 1$ e $(p^q - k)$ primos, temos que:

$$\begin{aligned}
 n &= p^{q-1}(p^q - k); \\
 \sigma(n) &= \sigma(p^{q-1}(p^q - k)) \\
 &= \sigma(p^{q-1})\sigma(p^q - k) \\
 &= \frac{p^q - 1}{p - 1}(p^q - k + 1) \\
 &= \frac{p \cdot p^{q-1}(p^q - k)}{p - 1} + \frac{k - 1}{p - 1} \\
 &= \frac{p}{p - 1}n + \frac{k - 1}{p - 1} \\
 &= \frac{k + 1}{k}n + \frac{k - 1}{k}.
 \end{aligned}$$

□

De acordo com Purkayastha, Goswami and Debnath (2017), a nomenclatura hiperperfeito é frequentemente utilizada como uma forma abreviada de k -hiperperfeito. É importante notar que todo número perfeito é, por definição, 1-hiperperfeito. Assim, o número 6 é considerado hiperperfeito com $k = 1$, pois

$$\sigma(6) = \frac{k + 1}{k}6 + \frac{k - 1}{k} = 12 \Rightarrow k = 1.$$

Em um estudo abrangente, McCranie (2000) empreendeu a tarefa de enumerar todos os números hiperperfeitos que não excedessem 10^{11} . Ao final de seus cálculos, McCranie catalogou um total de 2.190 números hiperperfeitos, cada um correspondente a um valor particular do parâmetro k . Ao analisar a paridade do índice k , ele observou que 85 dos números hiperperfeitos possuem índice k ímpar, distribuídos em 80 valores distintos de k . A maioria dos números hiperperfeitos encontrados, mais especificamente 2.105 desses números, possui índice k par, com 1.852 valores distintos de k . Uma característica notável observada é que todos os números hiperperfeitos identificados são ímpares, com exceção dos números 1-hiperperfeitos, que correspondem aos números perfeitos.

A Tabela 4.2 menciona alguns números k -hiperperfeitos para diferentes valores de k .

Tabela 4.2 – Números k -hiperperfeitos para diferentes valores de k

k	k-número hiperperfeito
1	6, 28, 496, 8.128, ...
2	21, 2.133, 19.521, 176.661, ...
3	325, ...
4	1.950.625, 1.220.640.625, ...
6	301, 16.513, 60.110.701, ...
10	159.841, ...
12	697, 2.041, 1.570.153, 62.722.153, ...

Fonte: Bege e Fogarasi (2009).

Para determinar os valores presentes na Tabela 4.2, basta utilizar a relação (4.4) e verificar em qual dos parâmetros k o número hiperperfeito se encaixa. Os Exemplos 4.2 e 4.3 ilustram o cálculo de k para os números hiperperfeitos 28 e 21.

Exemplo 4.2. *Verificando o valor de k para o número hiperperfeito 28:*

$$\begin{aligned}
 \sigma(n) &= \frac{k+1}{k}n + \frac{k-1}{k}; \\
 \sigma(28) &= \frac{k+1}{k}28 + \frac{k-1}{k}; \\
 56 &= \frac{k+1}{k}28 + \frac{k-1}{k}; \\
 56k &= 28k + 28 + k - 1; \\
 27k &= 27; \\
 k &= 1.
 \end{aligned}$$

Logo, o número 28 é 1-hiperperfeito, chamado simplesmente de número perfeito.

Exemplo 4.3. *Verificando o valor de k para o número hiperpefeito 21:*

$$\begin{aligned}
 \sigma(n) &= \frac{k+1}{k}n + \frac{k-1}{k}; \\
 \sigma(21) &= \frac{k+1}{k}21 + \frac{k-1}{k}; \\
 32 &= \frac{k+1}{k}21 + \frac{k-1}{k}; \\
 32k &= 21k + 21 + k - 1; \\
 10k &= 20; \\
 k &= 2.
 \end{aligned}$$

Logo, o número 21 é 2-hiperperfeito.

Bege e Fogarasi (2009, p. 76-77, tradução nossa) apresentam alguns resultados sobre os números hiperperfeitos:

Se $k > 1$ é um inteiro ímpar e $p = \frac{3k+1}{2}$ e $q = 3k + 4$ são números primos, então p^2q é k -hiperperfeito; J. S. McCraine conjecturou em 2000 que todos os k -números hiperperfeitos para k ímpar > 1 são desta forma, mas a hipótese não foi provada até agora.

Se p e q são primos ímpares distintos tais que $k(p + q) = pq - 1$ para algum inteiro k , então $n = pq$ é k -hiperperfeito.

Se $k > 0$ e $p = k + 1$ é primo, então para todo $i > 1$ tal que $q = p^i - p + 1$ é primo, $n = p^{i-1}q$ é k -hiperperfeito.

Complementando os resultados anteriores, Bege e Fogarasi (2009, p. 78-79, tradução nossa) expandem o conhecimento sobre o assunto apresentando o resultado expresso na Proposição 4.4.

Proposição 4.4. *Se $n = 3^{k-1}(3^k - 2)$, onde $3^k - 2$ é primo, então n é um número 2-hiperperfeito.*

Demonstração. Como a função σ é multiplicativa, e se p é primo, valem as propriedades

$$\sigma(p) = p + 1$$

e

$$\sigma(p^\alpha) = \frac{p^{\alpha+1} - 1}{p - 1},$$

segue que:

$$\begin{aligned} \sigma(n) &= \sigma(3^{k-1}(3^k - 2)) = \sigma(3^{k-1})\sigma(3^k - 2) = \frac{3^{(k-1)+1} - 1}{3 - 1} \cdot (3^k - 2 + 1) \\ &= \frac{(3^k - 1) \cdot (3^k - 1)}{2} = \frac{3^{2k} - 2 \cdot 3^k + 1}{2} = \frac{3}{2}3^{k-1}(3^k - 2) + \frac{1}{2}. \end{aligned}$$

□

Outro resultado importante a respeito dos números hiperperfeitos está descrito no Teorema 4.5 (Puneeth, 2018, p. 66, tradução nossa).

Teorema 4.5. *Todo número 2-hiperperfeito é um número ímpar.*

Demonstração. Seja n um número 2-hiperperfeito. Então n é da forma $3^{q-1}(3^q - 2)$ tal que $3^q - 2$ é primo. Mostraremos que $n \equiv 1 \pmod{2}$.

Sabemos que

$$3 \equiv 1 \pmod{2},$$

$$3^q \equiv 1 \pmod{2},$$

e que

$$\begin{aligned} 3^{-1} &\equiv 1 \pmod{2}, \\ 3^{q-1} &\equiv 1 \pmod{2}. \end{aligned} \tag{4.5}$$

Como 3^q é ímpar para cada $q \in \mathbb{N}$, temos, usando (4.5), que:

$$\begin{aligned} 3^q - 2 &\equiv 1 \pmod{2}; \\ 3^{q-1}(3^q - 2) &\equiv 1 \pmod{2}; \\ n &\equiv 1 \pmod{2}. \end{aligned}$$

□

Os números hiperperfeitos representam uma expansão notável dos números perfeitos, oferecendo uma visão mais profunda dos números inteiros. A definição de hiperperfeição, ao introduzir uma nova perspectiva sobre a relação entre um número e seus divisores, desencadeia uma série de novas questões e possibilidades de investigação na Teoria dos Números.

4.3 OUTROS TEOREMAS

Para ampliar a discussão sobre números perfeitos, além do célebre teorema de Euclides-Euler, que estabelece uma relação clássica entre números perfeitos pares e números primos de Mersenne, elencamos outros teoremas que investigam a estrutura e as propriedades desses números enigmáticos. Iniciamos com o Teorema 4.6, que associa números hiperperfeitos à soma de cubos (Garcia, 2016, p. 12, tradução nossa).

Teorema 4.6. *Todo número par perfeito maior do que 6 pode ser expresso como a soma dos cubos de inteiros ímpares consecutivos.*

Demonstração. Na prova, precisamos da fórmula $\sum_{i=1}^n i^3 = \frac{n^2(n+1)^2}{4}$, que pode ser provada verdadeira usando indução.

Seja $m = 2^{\frac{p-1}{2}}$, com p primo ímpar. Queremos reescrever a soma dos cubos dos $2m - 1$ primeiros inteiros ímpares consecutivos para que seja da forma $2^{p-1}(2^p - 1)$, ou seja,

$$1^3 + 3^3 + \cdots + (2m - 1)^3 = 2^{p-1}(2^p - 1).$$

Como a soma dos cubos de inteiros positivos consecutivos menores que $2m$ é igual à diferença entre a soma dos cubos de todos os inteiros positivos menores que $2m$ e a soma dos

cubos de todos os inteiros positivos pares menores que $2m$, temos que:

$$\begin{aligned}
 1^3 + 3^3 + \cdots + (2m-1)^3 &= (1^3 + 2^3 + \cdots + (2m)^3) - (2^3 + 4^3 + \cdots + (2m)^3) \\
 &= \frac{(2m)^2(2m+1)^2}{4} - 2^3 \frac{m^2(m+1)^2}{4} \\
 &= m^2(2m+1)^2 - 2m^2(m+1)^2 \\
 &= m^2(4m^2 + 4m + 1 - 2m^2 - 4m - 2) \\
 &= m^2(2m^2 - 1).
 \end{aligned} \tag{4.6}$$

Substituindo $m = 2^{\frac{p-1}{2}}$ em (4.6), concluímos que:

$$1^3 + 3^3 + \cdots + (2m-1)^3 = \left(2^{\frac{p-1}{2}}\right)^2 \left(2 \left(2^{\frac{p-1}{2}}\right)^2 - 1\right) = 2^{p-1}(2^p - 1).$$

Em função do Teorema de Euclides-Euler, concluímos que todo número perfeito par $n = 2^{p-1}(2^p - 1)$ é a soma dos cubos dos $2^{\frac{p-1}{2}}$ primeiros números ímpares.

□

Algumas fatorações não geram números perfeitos, como demonstram os Teoremas 4.7 a 4.10 (Gomes; Costa; Santos, 2008, p. 102-103).

Teorema 4.7. *Um quadrado perfeito não é um número perfeito.*

Demonstração. Seja $n = s^2$ um quadrado perfeito. Suponhamos que s se decomponha da forma $s = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$. Assim, a soma dos divisores de s^2 é dada por

$$\sigma(s^2) = (1 + p_1 + p_1^2 + \cdots + p_1^{2\alpha_1})(1 + p_2 + p_2^2 + \cdots + p_2^{2\alpha_2}) \cdots (1 + p_k + p_k^2 + \cdots + p_k^{2\alpha_k}). \tag{4.7}$$

Como cada um dos fatores em (4.7) é um número ímpar, obtemos que $\sigma(s^2)$ é ímpar. Portanto, $\sigma(s^2) \neq 2s^2$.

□

Teorema 4.8. *Não há número perfeito cuja decomposição seja da forma $p^m q^n$, com $2 < p < q$ e p, q primos.*

Demonstração. Para que $p^m q^n$ seja um número perfeito, devemos ter que:

$$\begin{aligned}
 \sigma(p^m q^n) &= 2p^m q^n; \\
 \frac{p^{m+1} - 1}{p - 1} \cdot \frac{q^{n+1} - 1}{q - 1} &= 2p^m q^n; \\
 pqp^m q^n - p^{m+1} - q^{n+1} + 1 &= 2(p - 1)(q - 1)p^m q^n;
 \end{aligned}$$

$$\begin{aligned}
-p^{m+1} - q^{n+1} + 1 &= [2(p-1)(q-1) - pq] p^m q^n; \\
&= (pq - 2p - 2q + 2) p^m q^n; \\
&= [p(q-2) - 2(q-1)] p^m q^n; \\
&= \{[p(q-2) - 2[(q-1) - 1] - 2] p^m q^n; \\
&= [p(q-2) - 2(q-2) - 2] p^m q^n; \\
&= [(p-2) \cdot (q-2) - 2] p^m q^n.
\end{aligned} \tag{4.8}$$

Para que a identidade (4.8) seja válida, devemos ter $(p-2) \cdot (q-2) - 2 < 0$, ou equivalente, $\frac{(p-2) \cdot (q-2)}{2} < 1$.

Como $2 < p < q$ e p, q são primos, temos que $p \geq 3$ e $q \geq 5$ ou $p-2 \geq 1$ e $q-2 \geq 3$. Assim,

$$\frac{(p-2) \cdot (q-2)}{2} \geq \frac{1 \cdot 3}{2} = \frac{3}{2} > 1,$$

o que contradiz (4.8).

□

Teorema 4.9. Não há número perfeito cuja decomposição seja da forma $p^m q^n r^s$, com $5 \leq p < q < r$.

Demonstração. A demonstração segue o mesmo caminho da prova do Teorema 4.8.

Suponhamos que $p^m q^n r^s$ seja um número perfeito, isto é,

$$\sigma(p^m q^n r^s) = 2p^m q^n r^s.$$

Isso implica em

$$2(p-1)(q-1)(r-1) - pqr < 0,$$

ou

$$\frac{(p-1)}{p} \frac{(q-1)}{q} \frac{(r-1)}{r} < \frac{1}{2}. \tag{4.9}$$

Contudo, a desigualdade (4.9) nunca ocorre, pois

$$\frac{(p-1)}{p} \frac{(q-1)}{q} \frac{(r-1)}{r} > \left(\frac{p-1}{p}\right)^3 \geq \left(\frac{5-1}{5}\right)^3 > \frac{1}{2}.$$

□

Teorema 4.10. Não há número perfeito cuja decomposição seja $p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$, com $\frac{\sqrt[k]{2}}{\sqrt[k]{2}-1} \leq p_1 < p_2 < \cdots < p_k$.

Demonstração. Para que $p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ seja perfeito, devemos ter

$$\sigma(p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}) = \frac{p_1^{\alpha_1+1} - 1}{p_1 - 1} \cdot \frac{p_2^{\alpha_2+1} - 1}{p_2 - 1} \cdots \frac{p_k^{\alpha_k+1} - 1}{p_k - 1} = 2p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k},$$

ou seja,

$$(p_1^{\alpha_1+1} - 1)(p_2^{\alpha_2+1} - 1) \cdots (p_k^{\alpha_k+1} - 1) = 2(p_1 - 1)(p_2 - 1) \cdots (p_k - 1)p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}. \quad (4.10)$$

Subtraindo de (4.10) o número $p_1^{\alpha_1+1} p_2^{\alpha_2+1} \cdots p_k^{\alpha_k+1}$, constatamos que o primeiro membro é um número negativo. Logo,

$$2(p_1 - 1)(p_2 - 1) \cdots (p_k - 1) - p_1 p_2 \cdots p_k < 0,$$

isto é,

$$\frac{p_1 - 1}{p_1} \cdot \frac{p_2 - 1}{p_2} \cdots \frac{p_k - 1}{p_k} < \frac{1}{2}. \quad (4.11)$$

Porém a desigualdade (4.11) não ocorre, uma vez que

$$\frac{p_1 - 1}{p_1} \cdot \frac{p_2 - 1}{p_2} \cdots \frac{p_k - 1}{p_k} > \left(\frac{p_1 - 1}{p_1} \right)^k \geq \left(\frac{\frac{\sqrt[k]{2}}{\sqrt[k]{2}-1} - 1}{\frac{\sqrt[k]{2}}{\sqrt[k]{2}-1}} \right)^k = \frac{1}{2}.$$

□

Para finalizar, o Teorema 4.11 estabelece que um número perfeito não pode ter a forma $6k - 1$ (Knill, 2007, p. 3, tradução nossa).

Teorema 4.11. *Nenhum número perfeito n pode ter a forma $6k - 1$.*

Demonstração. Se $n = 6k - 1$, então $n \equiv -1 \pmod{3}$ e $2n \equiv 1 \pmod{3}$. Se d é um divisor de n , então $d \left(\frac{n}{d} \right) = n$ mostra que $d \equiv 1 \pmod{3}$ e $\frac{n}{d} \equiv -1 \pmod{3}$, ou $d \equiv -1 \pmod{3}$ e $\frac{n}{d} \equiv 1 \pmod{3}$. Em qualquer caso, $\left(d + \frac{n}{d} \right) \equiv 0 \pmod{3}$ e portanto

$$\sigma(n) = \sum_{d < \sqrt{n}} \left(d + \frac{n}{d} \right)$$

é divisível por 3. Mas $2n \equiv 1 \pmod{3}$, gerando uma contradição. Logo, n não pode ser da forma $6k - 1$.

□

A riqueza matemática dos números perfeitos é evidente na variedade de teoremas aqui apresentados. Apesar dos séculos de estudo, enigmas como a existência de números perfeitos ímpares continuam a desafiar os matemáticos. A constante emergência de novas propriedades e generalizações demonstra a vitalidade desse campo de pesquisa, que atrai a atenção de pesquisadores em busca de respostas para questões fundamentais.

4.4 PADRÕES NUMÉRICOS E APLICAÇÕES

A fascinante jornada dos números perfeitos, aqueles cuja soma dos divisores próprios é igual a eles mesmos, remonta à Antiguidade. Sua rara ocorrência e propriedades intrigantes têm cativado matemáticos ao longo dos séculos. As primeiras explorações de Euclides, seguidas pelas contribuições de Euler, revelaram uma complexa e bela arquitetura de padrões numéricos que se estende além do sistema decimal, estabelecendo conexões profundas com diversas áreas da Matemática, como a Teoria dos Números e a Geometria Algébrica.

Um dos aspectos mais notáveis dos números perfeitos está em sua representação no sistema binário. Ao contrário do sistema decimal, que utiliza dez dígitos (0 a 9), o sistema binário emprega apenas dois: 0 e 1. O sistema binário é a linguagem fundamental da computação e da eletrônica digital. A aritmética binária, segue regras específicas para adição, subtração e outras operações. Uma descoberta fascinante sobre os números perfeitos é sua representação binária: todos os números perfeitos pares apresentam uma sequência de n uns seguida de $(n - 1)$ zeros - Teorema 4.12 (Gomes; Costa; Santos, 2008, p. 108), onde n está diretamente ligado à fórmula de Euclides. Essa regularidade, revelada com o auxílio de computadores, evidencia a rica interação entre Teoria dos Números e Ciência da Computação (Marreiros *et al*, 2024).

Teorema 4.12. *Um número perfeito par $N = 2^{n-1}(2^n - 1)$ escrito na base 2 tem os n primeiros dígitos iguais a 1 seguidos de $(n - 1)$ zeros, isto é, $N = (\underbrace{11 \cdots 1}_n \underbrace{00 \cdots 0}_{n-1})_2$.*

Demonstração. Como $1 + 2 + 2^2 + \cdots + 2^{n-1} = 2^n - 1$, temos que

$$N = 2^{n-1}(2^n - 1) = 2^{n-1}(1 + 2 + 2^2 + \cdots + 2^{n-1}) = 2^{n-1} + 2^n + \cdots + 2^{2n-2}.$$

□

De acordo com Polidoro (2023, n.p): “ A conversão de números decimais em binários é realizada por meio da divisão sucessiva do número decimal por 2, anotando-se o resto de cada divisão e invertendo a ordem deles para obter a representação binária do número”. Os Exemplos 4.4 e 4.5 ilustram a representação de números perfeitos no sistema binário. Para tanto, utilizamos o algoritmo da Divisão Euclidiana (2.9).

Exemplo 4.4. *Representação do número perfeito 6 no sistema binário.*

$$a = bq + r$$

$$6 = 2 \cdot 3 + 0$$

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

$$1 = 2 \cdot 0 + 1$$

Logo, o número perfeito 6 é representado no sistema binário como $[110]_2$.

Exemplo 4.5. *Representação do número perfeito 28 no sistema binário.*

$$a = bq + r$$

$$28 = 2.14 + \mathbf{0}$$

$$14 = 2.7 + \mathbf{0}$$

$$7 = 2.3 + \mathbf{1}$$

$$3 = 2.1 + \mathbf{1}$$

$$1 = 2.0 + \mathbf{1}$$

Logo, o número perfeito 28 é representado no sistema binário como $[11100]_2$.

Os números perfeitos 496, 8.128 e 33.550.336 são representados no sistema binário como $[111110000]_2$, $[111111000000]_2$ e $[111111111111100000000000]_2$, respectivamente (Marreiros *et al*, 2024).

4.4.1 NÚMEROS GEOMÉTRICOS

Além de sua definição aritmética, os números perfeitos possuem uma forte relação com os números geométricos, também conhecidos como números poligonais. São exemplos de números geométricos os números triangulares e os números hexagonais. Essa associação enriquece o estudo dos números perfeitos, revelando padrões e interligações entre diferentes áreas da Matemática. Embora não seja uma aplicação direta dos números perfeitos, essa dualidade entre as formas aritmética e geométrica sugere uma beleza oculta na organização dos números e inspira investigações mais profundas sobre suas propriedades.

As Definições 4.3 e 4.4 estabelecem o conceito de número triangular e hexagonal, respectivamente (Abu-Arish, 2016, p. 17-19, tradução nossa).

Definição 4.3. *Um número triangular é um número que pode ser escrito na forma $T_k = \frac{k(k+1)}{2}$, $k \in \mathbb{N}$. Esse número é chamado de triangular porque pode ser representado de forma triangular quando organizado em linhas de 1, 2, 3, ... pontos que começam com um ponto e cada linha subsequente contém um elemento a mais que a anterior.*

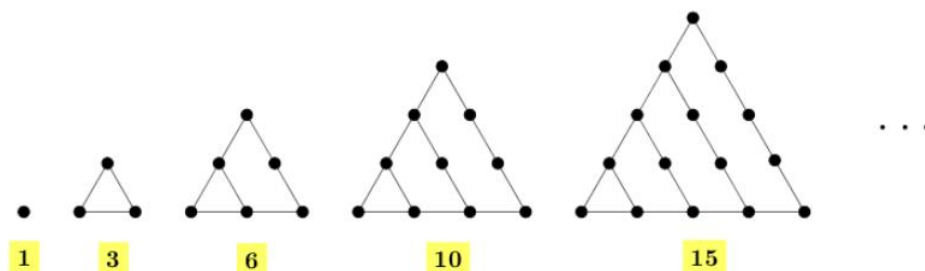
Definição 4.4. *Um número hexagonal é um número que pode ser escrito na forma $H_k = k(2k - 1)$, $k \in \mathbb{N}$. Esse número é chamado de hexagonal porque pode ser representado geometricamente por pontos dispostos ao longo dos contornos de hexágonos regulares. Cada valor de k corresponde ao número de pontos em cada lado do hexágono.*

As Figuras 4.3 e 4.4 ilustram as sequências dos números triangulares e hexagonais, respectivamente.

Após apresentar as definições e visualizar as formas geométricas dos números triangulares e hexagonais, podemos agora explorar os teoremas que estabelecem conexões entre essas sequências e os números perfeitos – Teoremas 4.13 a 4.15 (Abu-Arish, 2016, p. 17-19, tradução nossa).

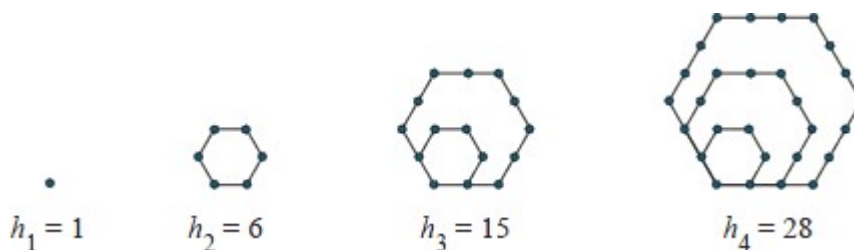
Teorema 4.13. *Todo número perfeito par é um número triangular.*

Figura 4.3 – Números triangulares



Fonte: Clubes de Matemática da OBMEP (2020).

Figura 4.4 – Números hexagonais



Fonte: Gabrielli e Monteiro (2009).

Demonstração. Seja

$$2^{n-1}(2^n - 1)$$

um número perfeito par. Considerando

$$k = 2^n - 1,$$

para qualquer inteiro positivo n , concluímos que:

$$\begin{aligned} k + 1 &= 2^n; \\ \frac{(2^n - 1)2^n}{2} &= \frac{k(k + 1)}{2} = T_k \end{aligned}$$

que é um número triangular.

□

Nem todo número triangular é um número perfeito. Apesar de existirem números triangulares que também são perfeitos (como 6 e 28), nem todos os triangulares possuem essa propriedade. Um contraexemplo simples é o número 3, que é triangular mas não é perfeito.

Teorema 4.14. *Todo número perfeito par é um número hexagonal.*

Demonstração. Seja

$$2^{n-1}(2^n - 1)$$

um número perfeito par. Considerando

$$k = 2^{n-1},$$

concluimos que:

$$\begin{aligned} 2^{n-1}(2^n - 1) &= 2^{n-1}(2 \cdot 2^{n-1} - 1) \\ &= k \cdot (2k - 1) = H_k, \end{aligned}$$

que é um número hexagonal.

□

Teorema 4.15. *Todo número hexagonal é, ao mesmo tempo, um número triangular.*

Demonstração. Considere o número hexagonal

$$H_k = k(2k - 1), \quad (4.12)$$

e seja

$$m = 2k \Rightarrow k = \frac{m}{2}, \quad (4.13)$$

$$m = 2k \Rightarrow 2k - 1 = m - 1. \quad (4.14)$$

Substituindo (4.13) e (4.14) em (4.12), concluimos que

$$H_k = k(2k - 1) = \frac{m(m - 1)}{2},$$

que é um número triangular.

□

Embora todo número hexagonal seja triangular, a recíproca não é verdadeira. Além disso, a propriedade de ser hexagonal não garante que o número seja perfeito (Abu-Arish, 2016).

As relações entre números perfeitos, triangulares e hexagonais demonstram que, mesmo em conceitos abstratos, a Matemática apresenta diversas conexões. Essas relações, além de enriquecer nosso entendimento sobre os números, também nos mostram como padrões aparentemente diferentes podem se unir em uma harmonia surpreendente. Ao investigar essas conexões, lembramos que a Matemática é, em essência, uma linguagem universal que revela a beleza oculta do mundo numérico e geométrico.

4.4.2 NÚMEROS CICLOPES

A Definição 4.5 conceitua números ciclopes.

Definição 4.5. *Um número ciclope é um número inteiro com um número ímpar de algarismos, contendo exatamente um zero posicionado na casa central.*

São ciclopes os números 101, 102, 103, 401, 11027 e 1520251. A denominação ciclope é uma alusão aos míticos ciclopes, gigantes de um único olho. A Definição 4.5 é válida para qualquer base numérica (Rosetta Code, 2024). Mesmo sendo possível escrever um número ciclope em qualquer base numérica, daremos ênfase à base 2, ou seja, aos números ciclopes binários.

Um número ciclope binário é constituído exclusivamente de dígitos 1, exceto por um único dígito 0 posicionado exatamente no centro da representação binária (Ramone, 2020), como, por exemplo, em 101, 11011, 1110111, 11111011111.

Pampena (2015) estabelece um procedimento para obtermos os números ciclopes na base 2. Inicialmente, encontramos os números na base 10 que possuem a seguinte forma: 989, 99899, 9998999, e assim por diante.

Sabemos que:

$$\begin{aligned} 9 &= 10 - 1; \\ 99 &= 10^2 - 1; \\ 999 &= 10^3 - 1; \\ &\vdots \\ \underbrace{99 \dots 99}_n &= 10^n - 1. \end{aligned} \quad (4.15)$$

Para obter os números na forma 989, 99899, 9998999, devemos utilizar somente os números na forma (4.15) que possuem uma quantidade ímpar de algarismos. Assim, temos que:

$$\begin{aligned} 989 &= 999 - 10 = 10^3 - 1 - 10; \\ 99899 &= 99999 - 100 = 10^5 - 1 - 10^2; \\ 9998999 &= 9999999 - 1000 = 10^7 - 1 - 10^3; \\ &\vdots \\ \underbrace{(99 \dots 8 \dots 99)}_n &= \underbrace{(99 \dots 9 \dots 99)}_n - 10^{\frac{n-1}{2}} = 10^n - 1 - 10^{\frac{n-1}{2}} \stackrel{n=2k+1}{=} 10^{2k+1} - 10^k - 1. \end{aligned} \quad (4.16)$$

Para conseguir os números na forma (4.16), ou seja, $\underbrace{99 \dots 8 \dots 99}_n$, basta utilizarmos $10^{2n+1} - 10^n - 1$ com n ímpar. Porém, nosso objetivo é determinar números ciclopes binários. Para tanto, trocamos $10^{2n+1} - 10^n - 1$ por $2^{2n+1} - 2^n - 1$ e substituímos os valores de n . Para $n = 1$:

$$2^{2n+1} - 2^n - 1 = 2^3 - 2^1 - 1 = 5.$$

Para $n = 2$:

$$2^{2n+1} - 2^n - 1 = 2^5 - 2^2 - 1 = 27.$$

Para $n = 3$:

$$2^{2n+1} - 2^n - 1 = 2^7 - 2^3 - 1 = 119.$$

Para $n = 4$:

$$2^{2n+1} - 2^n - 1 = 2^9 - 2^4 - 1 = 495.$$

Para $n = 6$:

$$2^{2n+1} - 2^n - 1 = 2^{13} - 2^6 - 1 = 8127.$$

Os Exemplos 4.6 a 4.8 ilustram a conversão de 5, 27 e 119, respectivamente, para a base 2 utilizando o algoritmo da Divisão Euclidiana (2.9).

Exemplo 4.6. *Representação do número 5 no sistema binário.*

$$a = bq + r$$

$$5 = 2 \cdot 2 + 1$$

$$2 = 2 \cdot 1 + 0$$

$$1 = 2 \cdot 0 + 1$$

Logo, o número 5 é representado no sistema binário pelo número ciclope $[101]_2$.

Exemplo 4.7. *Representação do número 27 no sistema binário.*

$$a = bq + r$$

$$27 = 2 \cdot 13 + 1$$

$$13 = 2 \cdot 6 + 1$$

$$6 = 2 \cdot 3 + 0$$

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

$$1 = 2 \cdot 0 + 1$$

Assim, o número 27 é representado no sistema binário pelo número ciclope $[11011]_2$.

Exemplo 4.8. *Representação do número 119 no sistema binário.*

$$a = bq + r$$

$$119 = 2 \cdot 59 + 1$$

$$59 = 2 \cdot 29 + 1$$

$$29 = 2 \cdot 14 + 1$$

$$14 = 2 \cdot 7 + 0$$

$$7 = 2 \cdot 3 + 1$$

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

$$1 = 2 \cdot 0 + 1$$

Logo, o número 119 é representado no sistema binário pelo número ciclope $[1110111]_2$.

Os números 495 e 8127 são representados no sistema binário pelos números ciclopes $[111101111]_2$ e $[1111110111111]_2$, respectivamente. Um fato curioso é que os primeiros números

ciclopes binários, quando convertidos para a base decimal, representam uma unidade a menos do que os números perfeitos. A Tabela 4.3 relaciona essa característica.

Tabela 4.3 – Relação entre números ciclopes e números perfeitos

Número ciclope binário	Conversão do número ciclope binário para a base 10	Número perfeito
101	5	6
11011	27	28
111101111	495	496
1111110111111	8.127	8.128
1111111111101111111111111111111	33.550.335	33.550.336
11111111111111111011111111111111111111111111111111	8.589.869.055	8.589.869.056

Fonte: Autora.

Analisando a Tabela 4.3, surge uma dúvida: Será que todo número perfeito par, menos 1, resulta em um número ciclope binário? Haran (2020) apresenta uma solução para essa dúvida.

A forma binária de um número ciclope com $2n + 1$ dígitos é

$$2^{2n+1} - 2^n - 1.$$

Já os números perfeitos pares têm forma

$$N = 2^{p-1}(2^p - 1). \quad (4.17)$$

Subtraindo 1 da expressão (4.17), temos que:

$$2^{p-1}(2^p - 1) - 1 = 2^{2p-1} - 2^{p-1} - 1. \quad (4.18)$$

Agora, considerando $p = n + 1$ e substituindo em (4.18), concluímos que:

$$2^{2p-1} - 2^{p-1} - 1 = 2^{2(n+1)-1} - 2^{n+1-1} - 1 = 2^{2n+1} - 2^n - 1,$$

que é a forma binária de um número ciclope com $2n + 1$ dígitos.

Embora números perfeitos e ciclopes não sejam utilizados em tarefas do dia a dia, a investigação da relação entre eles abre novas fronteiras para a pesquisa matemática. Essa conexão demonstra a estrutura oculta dos números e estimula a exploração de padrões e propriedades que podem não ser aparentes à primeira vista. A busca por essas relações contribui para um melhor entendimento da Teoria dos Números e pode gerar novas e interessantes descobertas matemáticas.

5 NÚMEROS AMIGÁVEIS

A busca por padrões e harmonia nos números sempre fascinou os pitagóricos. Ao investigarem as propriedades dos divisores, eles se depararam com um conceito que transcendia a mera aritmética: a amizade entre os números. Conforme Neto e Toillier (2020, p. 92 apud Karlson, 1961), quando questionado sobre o significado da amizade, Pitágoras teria utilizado uma metáfora numérica: “alguém que é um outro eu, como 220 e 284”. Estes números, chamados de amigáveis, possuem uma característica única: a soma dos divisores próprios de um é igual ao outro. Essa descoberta, ocorrida por volta de meados do século VI a.C., revela a profundidade com que os pitagóricos exploravam as relações numéricas e antecipa a Teoria dos Números, um campo que continua a intrigar matemáticos até os dias de hoje (Neto; Toillier, 2020).

A Definição 5.1 estabelece o conceito de números amigáveis (Euler *et al.*, 2015, p. 13), enquanto que o Exemplo 5.1 mostra um par de números amigáveis clássico.

Definição 5.1. *Números amigáveis são pares de números m e n que satisfazem a condição de que $s(m) = n$ e $s(n) = m$.*

Exemplo 5.1. *Os números 220 e 284 são amigáveis, pois:*

$$s(220) = 1 + 2 + 4 + 5 + 10 + 11 + 20 + 22 + 44 + 55 + 110 = 284;$$

$$s(284) = 1 + 2 + 4 + 71 + 142 = 220.$$

Dimitrov (2024, p. 1, tradução nossa), complementa a Definição 5.1: “Dois números naturais m e n são considerados amigáveis se $\sigma(m) = \sigma(n) = m + n$ ”.

A busca por significados ocultos dos números amigáveis levou muitos estudiosos a acreditarem que esses números estariam presentes na Bíblia. A sugestão de que números amigáveis são codificados na Bíblia é recorrente em algumas interpretações, porém não encontra suporte em fontes históricas ou textuais. A ideia de que Jacó, ao oferecer 220 animais a Esaú, teria escolhido intencionalmente esse número devido à sua relação com 284, é um exemplo clássico dessa abordagem. Da mesma forma, a análise numérica complexa de Ginsburg, que busca encontrar significados ocultos nos valores numéricos associados a palavras e conceitos bíblicos, revela uma tendência a sobrepor interpretações subjetivas ao texto original (Euler *et al.*, 2015).

Outro aspecto fascinante da história dos números amigáveis é sua relevância na cultura árabe. A crença na capacidade desses números de fortalecer laços e a sua utilização em práticas astrológicas, como evidenciado pelos trabalhos de Ibn Khaldun, Ibn el-Hasan e Ben Kalonymos, demonstram a importância cultural atribuída a eles. A influência da matemática grega, em particular a obra de Euclides, foi fundamental para o desenvolvimento desses estudos no mundo árabe. Thabit ibn Qurra (836 – 901), por sua vez, contribuiu significativamente para o campo da

Teoria dos Números ao desenvolver um método original – Método 5.1 – para encontrar pares de números amigáveis, demonstrando a profundidade do conhecimento matemático alcançado pelos árabes (Neto; Toillier, 2020).

Método 5.1. (*Qurra*) Seja $n \in \mathbb{N}$.

1. Calcule a, b e c :

$$a = 3 \cdot 2^n - 1;$$

$$b = 3 \cdot 2^{n-1} - 1;$$

$$c = 9 \cdot 2^{n-1} - 1.$$

2. Se a, b e c são primos distintos, com $b \neq 2$, calcule:

$$p = 2^n ab;$$

$$q = 2^n c.$$

Os números p e q constituem um par de números amigáveis.

O matemático árabe Thabit ibn Qurra deixou um legado significativo na teoria dos números amigáveis. Ao se inspirar na geometria euclidiana, ele desenvolveu uma fórmula algébrica para gerar pares desses números, demonstrando uma compreensão avançada da Aritmética para sua época. Seus trabalhos, embora pouco conhecidos durante séculos, revelam que Qurra já havia descoberto pares como (220, 284) e (17296, 18416), este último erroneamente atribuído a Fermat por muito tempo. A fórmula de Qurra, embora não englobasse todos os pares possíveis, abriu caminho para futuras pesquisas, como as de Euler, que generalizaram suas ideias (Neto; Toillier, 2020).

A jornada dos números amigáveis nos conduz por um labirinto de descobertas e influências culturais. A partir das contribuições de Thabit ibn Qurra, os árabes aprofundaram a teoria, enquanto os europeus a associaram a práticas esotéricas, limitando-se inicialmente ao par (220, 284). Séculos depois, Fermat, sem conhecimento prévio dos trabalhos de Qurra, redescobriu o par (17296, 18416) e desenvolveu um método geral, similar ao de Qurra, para encontrar outros pares. A semelhança entre os métodos levanta a questão da independência dessas descobertas (Euler *et al.*, 2015).

A análise histórica indica que Fermat provavelmente não teve acesso aos textos árabes mais teóricos sobre o tema, uma vez que os conhecidos na Europa eram de natureza astrológica ou mágica e não continham métodos detalhados. A disseminação tardia da aritmética árabe na Europa e a abordagem natural dos dois matemáticos a partir da proposição IX.36 de Euclides reforçam a hipótese de que tanto Qurra quanto Fermat chegaram a seus resultados de forma independente, impulsionados pela curiosidade e pelo desejo de desvendar os mistérios que envolviam esses números (Euler *et al.*, 2015).

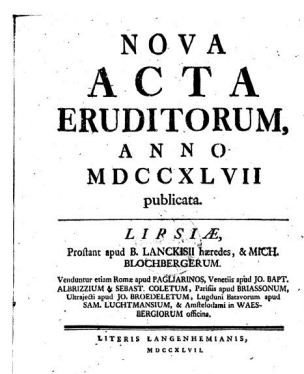
5.1 CONTRIBUIÇÕES DE EULER

A fascinante história dos números amigáveis, que remonta à antiguidade, ganhou um novo impulso com as contribuições de Leonhard Euler. Embora os pitagóricos tenham sido os primeiros a explorar essa curiosa relação entre números, foi Euler quem, com sua mente brilhante, desvendou os mistérios por trás desses pares. Seu método de abordagem permitiu identificar padrões e relações entre esses números, consolidando uma base teórica que influenciou os estudos posteriores. A obra de Euler não apenas aumentou a lista de exemplos conhecidos, mas também demonstrou sua capacidade única de compreensão intuitiva e rigor matemático.

Euler dedicou três trabalhos ao estudo dos números amigáveis. Os dois primeiros foram publicados em 1747 e 1750, respectivamente. O terceiro, publicado em 1849, após sua morte em 1783 (Leôncio, 2013).

O primeiro trabalho de Euler sobre números amigáveis – E100¹, intitulado *De numeris amicabilibus*, foi publicado em 1747 na revista *Nova Acta Eruditorum*, cuja capa está representada na Figura 5.1. Apesar do relativo desinteresse da comunidade matemática da época por questões teóricas dos números, Euler, inspirado por trabalhos pioneiros de Descartes e van Schooten, aprofundou-se nessa área. Em seu artigo, relativamente curto, Euler não apenas lamentou a escassez de pesquisas nessa área, mas também apresentou um mé-

Figura 5.1 – Capa *Nova Acta Eruditorum* - 1747



Fonte: Biblioteca Nacional da França (2009).

todo algébrico mais geral para encontrar pares de números amigáveis. A inclusão de uma tabela com 30 novos pares de números amigáveis atesta a eficácia de seu método e demonstra um avanço considerável em relação aos estudos anteriores (Euler *et al.*, 2015).

Segundo Neto e Toillier (2020), a pesquisa sobre números amigáveis avançou significativamente ao longo dos séculos, mas foi Euler quem forneceu o marco teórico mais sólido para essa área. Euler, com sua genialidade matemática, conseguiu simplificar e generalizar a fórmula proposta por Qurra, expressando-a em termos de potências de 2. Essa nova abordagem não apenas facilitou as demonstrações, mas também permitiu a descoberta de inúmeros novos pares de números amigáveis.

De acordo com Neto e Toillier (2020, p. 100), a generalização apresentada por Euler era

¹ Segundo Alan (2009) e D'Ambrosio (2021), os trabalhos de Euler sobre números amigáveis foram catalogados pelo historiador da matemática sueco Gustav Eneström como E100, E152 e E798, no Índice de Eneström. Neste índice, cada publicação é identificada por uma letra E seguida de um número.

a seguinte: “Sejam $p = 2^m(2^{n-m} + 1) - 1$, $q = 2^n(2^{n-m} + 1) - 1$ e $r = 2^{n+m}(2^{n-m} + 1)^2 - 1$, para $1 \leq m < n$. Se p , q e r são primos, então $\{2^npq, 2^nr\}$ é um par de números amigáveis”.

O segundo artigo de Euler sobre números amigáveis – E152, também intitulado *De numeris amicabilebus*, foi publicado em 1750 e aprofundou as investigações iniciadas em E100. O segundo artigo publicado é extenso e nele Euler detalha seu método para encontrar pares de números amigáveis, introduzindo a função soma dos divisores e demonstrando suas propriedades multiplicativas (Euler *et al.*, 2015).

Utilizando a notação σ para representar a soma de todos os divisores de um determinado número, incluindo o próprio número, Euler demonstra que dois números m e n são amigáveis se, e somente se, $\sigma(m) = \sigma(n) = m + n$. Essa equação caracteriza a relação entre dois números amigáveis, estabelecendo que a soma dos divisores de cada um deve ser igual à soma dos dois² (Euler *et al.*, 2015).

Euler também demonstrou a propriedade multiplicativa da função σ e apresentou um método geral para calcular σn para qualquer número natural n . Diante da dificuldade de encontrar pares de números amigáveis primos entre si, Euler optou por uma abordagem mais restrita. Assim, decidiu focar sua pesquisa em pares de números amigáveis que possuem um fator comum a , adotando a forma geral am e an , com m e n coprimos com a . Essa restrição permitiu a Euler obter resultados mais concretos e específicos (Euler *et al.*, 2015, p. 54):

$$(i) \quad \sigma m = \sigma n;$$

$$(ii) \quad \frac{a}{\sigma a} = \frac{\sigma m}{m+n} = \frac{\sigma n}{m+n};$$

$$(iii) \quad a(m+n) = \sigma a \cdot \sigma n.$$

Segundo Leôncio (2013), Euler apresentou cinco fórmulas para identificar pares de números amigáveis que compartilham um fator comum. Com base nas cinco fórmulas apresentadas, Euler propôs cinco problemas específicos. Cada um desses problemas apresentava um conjunto de regras e exemplos para guiar a busca por novos pares. A partir da resolução desses problemas, Euler conseguiu expandir significativamente o conjunto conhecido de números amigáveis, apresentando uma tabela com 61 pares, alguns destes presentes no primeiro artigo.

Publicado originalmente em 1849, após a morte de Euler, o terceiro artigo – E798, com o mesmo título dos anteriores, foi incluído na *Commentationes Arithmeticae* e posteriormente na *Opera Póstuma*, em 1862. Nessa obra, Euler aprofunda suas investigações sobre os números amigáveis. Após uma breve contextualização histórica, onde menciona outros matemáticos que se dedicaram ao tema, Euler apresenta uma nova formulação para os problemas propostos em seu segundo artigo. O texto, dividido em dezessete incisos, inclui uma breve revisão das propriedades da função sigma, fundamental para o estudo dos divisores de um número. Além disso, Euler

² Segundo Leôncio (2013), σn corresponde à função sigma, que atualmente é representada por $\sigma(n)$.

reapresentou a tabela soma de divisores, inicialmente publicada em seu segundo artigo (Leôncio, 2013).

Segundo Alan (2009), a maior parte da pesquisa de Euler sobre números amigáveis foi dedicada à construção de tabelas detalhadas. Analisando esses dados, ele procurou identificar padrões e formulou hipóteses sobre a natureza desses números. Antes de seus trabalhos, apenas três pares de números amigáveis eram conhecidos. Euler, por sua vez, apresentou uma lista com 61 pares, dos quais apenas dois se mostraram incorretos. As técnicas desenvolvidas por Euler serviram como base para pesquisas posteriores, permitindo a descoberta de mais de onze milhões de pares de números amigáveis. A Figura 5.2 mostra os pares de números amigáveis entre 1 e 20.000.000.

Figura 5.2 – Pares de números amigáveis menores que 20.000.000

a	b	a	b	a	b
220	284	1,328,470	1,483,850	8,619,765	9,627,915
1,184	1,210	1,358,595	1,486,845	8,666,860	10,638,356
2,620	2,924	1,392,368	1,464,592	8,754,130	10,893,230
5,020	5,564	1,466,150	1,747,930	8,826,070	10,043,690
6,232	6,368	1,468,324	1,749,212	9,071,685	9,498,555
10,744	10,856	1,511,930	1,598,470	9,199,496	9,592,504
12,285	14,595	1,669,910	2,062,570	9,206,925	10,791,795
17,296	18,416	1,798,875	1,870,245	9,339,704	9,892,936
63,020	76,084	2,082,464	2,090,656	9,363,584	9,437,056
66,928	66,992	2,236,570	2,429,030	9,478,910	11,049,730
67,095	71,145	2,652,728	2,941,672	9,491,625	10,950,615
69,615	87,633	2,723,792	2,874,064	9,660,950	10,025,290
79,750	88,730	2,728,726	3,077,354	9,773,505	11,791,935
100,485	124,155	2,739,704	2,928,136	10,254,970	10,273,670
122,265	139,815	2,802,416	2,947,216	10,533,296	10,949,704
122,368	123,152	2,803,580	3,716,164	10,572,550	10,854,650
141,664	153,176	3,276,856	3,721,544	10,596,368	11,199,112
142,310	168,730	3,606,850	3,892,670	10,634,085	14,084,763
171,856	176,336	3,786,904	4,300,136	10,992,735	12,070,305
176,272	180,848	3,805,264	4,006,736	11,173,460	13,212,076
185,368	203,432	4,238,984	4,314,616	11,252,648	12,101,272
196,724	202,444	4,246,130	4,488,910	11,498,355	12,024,045
280,540	365,084	4,259,750	4,445,050	11,545,616	12,247,504
308,620	389,924	4,482,765	5,120,595	11,693,290	12,361,622
319,550	430,402	4,532,710	6,135,962	11,905,504	13,337,336
356,408	399,592	4,604,776	5,162,744	12,397,552	13,136,528
437,456	455,344	5,123,090	5,504,110	12,707,704	14,236,136
469,028	486,178	5,147,032	5,843,048	13,671,735	15,877,065
503,056	514,736	5,232,010	5,799,542	13,813,150	14,310,050
522,405	525,915	5,357,625	5,684,679	13,921,528	13,985,672
600,392	669,688	5,385,310	5,812,130	14,311,688	14,718,712
609,928	686,072	5,459,176	5,495,264	14,426,230	18,087,818
624,184	691,256	5,726,072	6,369,928	14,443,730	15,882,670
635,624	712,216	5,730,615	6,088,905	14,654,150	16,817,050
643,336	652,664	5,864,660	7,489,324	15,002,464	15,334,304
667,964	783,556	6,329,416	6,371,384	15,363,832	16,517,768
726,104	796,696	6,377,175	6,680,025	15,938,055	17,308,665
802,725	863,835	6,955,216	7,418,864	16,137,628	16,150,628
879,712	901,424	6,993,610	7,158,710	16,871,582	19,325,698
898,216	980,984	7,275,532	7,471,508	17,041,010	19,150,222
947,835	1,125,765	7,288,930	8,221,598	17,257,695	17,578,785
998,104	1,043,096	7,489,112	7,674,088	17,754,165	19,985,355
1,077,890	1,099,390	7,577,350	8,493,050	17,844,255	19,895,265
1,154,450	1,189,150	7,677,248	7,684,672	17,908,064	18,017,056
1,156,870	1,292,570	7,800,544	7,916,696	18,056,312	18,166,888
1,175,265	1,438,983	7,850,512	8,052,488	18,194,715	22,240,485
1,185,376	1,286,744	8,262,136	8,369,864	18,655,744	19,154,336
1,280,565	1,340,235				

Fonte: VaxaSoftware (2024).

O trabalho de Leonhard Euler foi fundamental para o desenvolvimento da teoria dos números amigáveis. Através de uma abordagem rigorosa e inovadora, ele não apenas identificou novos pares de números amigáveis, mas também estabeleceu uma sólida base teórica para a compreensão desses números. Utilizando métodos algébricos avançados para sua época, Euler conseguiu generalizar os critérios existentes e estabelecer conexões entre os números amigáveis e outras áreas da Teoria dos Números, como a divisibilidade. Sua pesquisa abriu caminho para o estudo aprofundado das propriedades e das estruturas subjacentes aos números amigáveis, inspirando matemáticos por séculos.

5.2 TEOREMAS

A relação entre dois números amigáveis, repleta de mistérios, tem despertado a curiosidade de matemáticos ao longo dos séculos. Com o desenvolvimento da Teoria dos Números, o estudo desses pares ganhou maior profundidade. Teoremas específicos descrevem suas propriedades e fornecem ferramentas para sua identificação, tornando-os um objeto de pesquisa contínua.

Nesta Seção, abordamos teoremas e propriedades que marcaram o início do estudo dos números amigáveis, oferecendo uma base para compreender sua natureza intrigante. Embora existam atualmente outros teoremas sobre o assunto, estes exigem um estudo mais aprofundado devido à complexidade e ao avanço das ferramentas matemáticas modernas.

Leonhard Euler, um dos grandes matemáticos da história, contribuiu significativamente para a teoria dos números amigáveis ao identificar algumas condições que facilitaram a descoberta desses pares. Segundo Fossa e Leôncio (2013, p. 21): “Euler definiu o operador σn , onde n é um número inteiro positivo, como sendo a soma de todos os divisores positivos do número n ”³. O Exemplo 5.2 ilustra a aplicação do operador de Euler.

Exemplo 5.2. *Aplicando o operador de Euler aos números 220 e 284, obtemos que:*

$$\sigma(220) = 1 + 2 + 4 + 5 + 10 + 11 + 20 + 22 + 44 + 55 + 110 + 220 = 504;$$

$$\sigma(284) = 1 + 2 + 4 + 142 + 284 = 504.$$

Assim, a soma das partes alíquotas de n será $\sigma n - n$:

$$\sigma(220) - 220 = 504 - 220 = 284;$$

$$\sigma(284) - 284 = 504 - 284 = 220.$$

Portanto:

$$\sigma(220) = \sigma(284) = 220 + 284.$$

³ Utilizamos a notação atual da função sigma, $\sigma(n)$, em substituição à notação $\sigma(n)$ empregada por Euler.

A propriedade da soma das partes alíquotas é característica de todos os pares de números amigáveis (Fossa; Leôncio, 2013). Desta forma, se m e n são um par amigável, então cada um deles será igual à soma dos divisores próprios do outro. Matematicamente, podemos expressar essa relação como:

$$\sigma(m) - m = n, \quad (5.1)$$

$$\sigma(n) - n = m. \quad (5.2)$$

De (5.1) e (5.2), concluímos que:

$$\sigma(m) = \sigma(n) = m + n. \quad (5.3)$$

Em seus estudos sobre a função f , Euler estabeleceu as propriedades elencadas na Proposição 5.1 (Leôncio, 2013, p. 48-49).

Proposição 5.1.

- i. $\sigma(1) = 1$.
- ii. Para n primo, $\sigma(n) = n + 1$.
- iii. Para m, n primos entre si, $\sigma(mn) = \sigma(m) \cdot \sigma(n)$.
- iv. Para m, n, p primos distintos, $\sigma(mnp) = \sigma(m) \cdot \sigma(n) \cdot \sigma(p)$.
- v. Para m, n, p primos entre si, $\sigma(mnp) = \sigma(m) \cdot \sigma(n) \cdot \sigma(p)$.
- vi. Para n primo, $\sigma(n^k) = 1 + n + n^2 + \dots + n^k = \frac{n^{k+1}-1}{n-1}$.
- vii. Para n primo, $\sigma(n^{k+1}) = \sigma(n^k) + n^{k+1} = 1 + n\sigma(n^k)$.

Demonstração.

- i. $\sigma(1) = 1$ por definição.
- ii. Se n é primo, então os divisores de n são 1 e n . Logo, $\sigma(n) = n + 1$.
- iii. Se m e n são números primos entre si, tal que os divisores de m sejam $1, \alpha_1, \alpha_2, \dots, \alpha_k$ e os divisores de n sejam $1, \beta_1, \beta_2, \dots, \beta_l$, com $k, l \in \mathbb{N}$, temos que a soma dos divisores de m e n é, respectivamente, $\sigma(m) = 1 + \alpha_1 + \alpha_2 + \dots + \alpha_k$ e $\sigma(n) = 1 + \beta_1 + \beta_2 + \dots + \beta_l$, com $k, l \in \mathbb{N}$. Contudo, se γ divide mn , então $\gamma = \alpha\beta$, onde $\alpha \mid m$ e $\beta \mid n$. Portanto:

$$\sigma(mn) = 1.1 + 1.\alpha_1 + \dots + 1.\alpha_k + \dots + \beta_l.1 + \beta_l.\alpha_1 + \dots + \beta_l.\alpha_k;$$

$$\sigma(mn) = (1 + \alpha_1 + \alpha_2 + \dots + \alpha_k).(1 + \beta_1 + \beta_2 + \dots + \beta_l) = \sigma(m) \cdot \sigma(n).$$

iv. Se m, n e p são primos distintos, então:

$$\begin{aligned}
 \sigma(mnp) &= 1 + m + n + p + mn + mp + np + mnp \\
 &= 1 + m + n + mn + (1 + m + n + mn)p \\
 &= (1 + m + n + mn)(1 + p) \\
 &= (m + 1)(n + 1)(p + 1) = \sigma(m) \cdot \sigma(n) \cdot \sigma(p),
 \end{aligned}$$

ou

$$\begin{aligned}
 \sigma(mnp) &= 1 + m + n + p + mn + mp + np + mnp \\
 &= 1 + m + n + mn + (1 + m + n + mn)p \\
 &= (1 + m + n + mn)(1 + p) \\
 &= \sigma(mn) \cdot \sigma(p) = \sigma(m) \cdot \sigma(n) \cdot \sigma(p).
 \end{aligned}$$

v. Por m, n e p primos entre si, Euler entendeu primos entre si dois a dois. Desta forma:

$$\sigma(mnp) = \sigma(mn)\sigma(p) = \sigma(m) \cdot \sigma(n) \cdot \sigma(p).$$

vi. Por definição, temos que, para n primo, $\sigma(n) = 1 + n$. Sejam $\sigma(n^2) = 1 + n + n^2$, $\sigma(n^3) = 1 + n + n^2 + n^3, \dots$, $\sigma(n^k) = 1 + n + n^2 + n^3 + \dots + n^k$. Como a soma dos divisores da potência de um número primo n é igual à soma dos termos de uma progressão geométrica de razão n , concluímos que:

$$\begin{aligned}
 \sigma(n^2) &= \frac{1(n^3 - 1)}{n - 1} = \frac{(n^{2+1} - 1)}{n - 1}, \sigma(n^3) = \frac{1(n^4 - 1)}{n - 1} = \frac{(n^{3+1} - 1)}{n - 1}, \dots, \\
 \sigma(n^k) &= \frac{1(n^{k+1} - 1)}{n - 1} = \frac{n^{k+1} - 1}{n - 1}.
 \end{aligned}$$

vii. Para n primo, temos que:

$$\begin{aligned}
 \sigma(n^{k+1}) &= 1 + n + n^2 + n^3 + \dots + n^k + n^{k+1} = (1 + n + n^2 + n^3 + \dots + n^k) + n^{k+1} \\
 &= \sigma(n^k) + n^{k+1},
 \end{aligned}$$

ou

$$\begin{aligned}
 \sigma(n^{k+1}) &= 1 + n + n^2 + n^3 + \dots + n^k + n^{k+1} = 1 + (n + n^2 + n^3 + \dots + n^k + n^{k+1}) \\
 &= 1 + n(1 + n + n^2 + \dots + n^{k-1} + n^k) \\
 &= 1 + n\sigma(n^k).
 \end{aligned}$$

Portanto, $\sigma(n^{k+1}) = \sigma(n^k) + n^{k+1} = 1 + n\sigma(n^k)$.

□

A soma dos divisores de um número inteiro positivo n pode ser calculada utilizando-se o TFA e as propriedades de $\sigma(n)$, como mostra o Exemplo 5.3.

Exemplo 5.3. *Soma dos divisores do número 284:*

$$\begin{aligned}\sigma(284) &= \sigma(2^2 \cdot 71) \\ &= \sigma(2^2) \cdot \sigma(71) \\ &= \sigma(2^2) \cdot 72 \\ &= 7 \cdot 72 \\ &= 504.\end{aligned}$$

Conforme salientam Fossa e Leôncio (2013), após o cálculo da soma dos divisores, a obtenção da soma das partes alíquotas é imediata, bastando subtrair o número em questão. A fim de otimizar esses procedimentos, Euler elaborou uma tabela com os valores de $\sigma(p^k)$, onde p é um número primo menor do que mil e k assume os valores 1, 2 e 3, sendo que, para alguns primos menores, foram considerados valores mais elevados de k .

Thabit ibn Qurra foi pioneiro na busca por números amigáveis. Ele desenvolveu um método que, sob determinadas condições, gera pares desses números - Teorema 5.1 (Bulhões, 2020, p. 33).

Teorema 5.1. *Se $p = 3 \cdot 2^n - 1$, $q = 3 \cdot 2^{n-1} - 1$ e $r = 9 \cdot 2^{2n-1} - 1$ são primos maiores do que 2, então $2^n pq$ e $2^n r$ são números amigáveis.*

Demonstração. Empregando as propriedades (ii) e (iii) da Proposição 5.1 e a soma dos divisores próprios de n , dada por $\sigma(n) - n$, concluímos que:

$$\begin{aligned}\sigma(2^n pq) - 2^n pq &= \sigma(2^n) \sigma(p) \sigma(q) - 2^n pq \\ &= (2^{n+1} - 1) \cdot 3 \cdot 2^n \cdot 3 \cdot 2^{n-1} - 2^n (3 \cdot 2^n - 1)(3 \cdot 2^{n-1} - 1) \\ &= 9 \cdot 2^{2n-1} (2^{n+1} - 1) - 2^n (9 \cdot 2^{2n-1} - 3 \cdot 2^n - 3 \cdot 2^{n-1} + 1) \\ &= 9 \cdot 2^{3n} - 9 \cdot 2^{2n-1} - 9 \cdot 2^{3n-1} + 3 \cdot 2^{2n} + 3 \cdot 2^{2n-1} - 2^n \\ &= 18 \cdot 2^{3n-1} - 9 \cdot 2^{2n-1} - 9 \cdot 2^{3n-1} + 6 \cdot 2^{2n-1} + 3 \cdot 2^{2n-1} - 2^n \\ &= 9 \cdot 2^{3n-1} - 2^n \\ &= 2^n (9 \cdot 2^{2n-1} - 1) \\ &= 2^n r\end{aligned}$$

e

$$\begin{aligned}\sigma(2^n r) - 2^n r &= \sigma(2^n) \sigma(r) - 2^n r \\ &= (2^{n+1} - 1) \cdot 9 \cdot 2^{2n-1} - 2^n (9 \cdot 2^{2n-1} - 1) \\ &= 2^n \cdot (9 \cdot 2^{2n} - 9 \cdot 2^{n-1} - 9 \cdot 2^{2n-1} + 1)\end{aligned}$$

$$\begin{aligned}
\sigma(2^n r) - 2^n r &= 2^n \cdot (9 \cdot 2^{2n-1} - 6 \cdot 2^{n-1} - 3 \cdot 2^{n-1} + 1) \\
&= 2^n \cdot (9 \cdot 2^{2n-1} - 3 \cdot 2^n - 3 \cdot 2^{n-1} + 1) \\
&= 2^n (3 \cdot 2^n - 1)(3 \cdot 2^{n-1} - 1) \\
&= 2^n pq.
\end{aligned}$$

□

Segundo Euler *et al.* (2015), a demonstração de Qurra não seguiu o raciocínio apresentado na demonstração do Teorema 5.1. Na realidade, a regra proposta por ele para identificar números amigáveis apresenta uma semelhança notável com a regra de Euclides para números perfeitos. Essa similaridade levanta a questão sobre a origem da regra de Qurra e sugere que a mesma pode ter sido inspirada na proposição euclidiana.

A regra formulada por Qurra, apesar de inovadora, resultou em apenas três pares de números amigáveis. Inspirado nessa regra e em outras investigações sobre o tema, Euler dedicou-se a um estudo mais aprofundado dessas intrigantes relações numéricas (Leôncio, 2013). De acordo com Bulhões (2020, p. 34), Euler estabeleceu o Teorema 5.2 para determinar novos pares de números amigáveis.

Teorema 5.2. *Sejam m e n dois inteiros positivos, com $1 \leq m \leq n - 1$. Se*

$$\begin{aligned}
p &= 2^n(2^{n-m} + 1) - 1, \\
q &= 2^m(2^{n-m} + 1) - 1, \\
r &= 2^{n+m}(2^{n-m} + 1)^2 - 1,
\end{aligned}$$

são números primos, então $2^n pq$ e $2^n r$ é um par de números amigáveis.

Demonstração. Considerando $\xi = 2^{n-m} + 1$, temos que:

$$\begin{aligned}
p &= 2^n \xi - 1; \\
q &= 2^m \xi - 1; \\
r &= 2^{n+m} \xi^2 - 1.
\end{aligned}$$

Utilizando as propriedades estabelecidas na Proposição 5.1, obtemos que:

$$\begin{aligned}
\sigma(2^n pq) &= \sigma(2^n) \sigma(p) \sigma(q) \\
&= (2^{n+1} - 1) \cdot 2^n \xi \cdot 2^m \xi \\
&= (2^{n+1} - 1) \cdot 2^{n+m} \xi^2; \\
\sigma(2^n r) &= \sigma(2^n) \sigma(r) \\
&= (2^{n+1} - 1) \cdot 2^{n+m} \xi^2.
\end{aligned}$$

Assim, usando $\xi = 2^{n-m} + 1$, concluímos que:

$$\begin{aligned}
 2^n pq + 2^n r &= 2^n(pq + r) = 2^n \left[(2^n \xi - 1)(2^m \xi - 1) + 2^{n+m} \xi^2 - 1 \right] \\
 &= 2^n \left(2^{n+m} \xi^2 - 2^n \xi - 2^m \xi + 1 + 2^{n+m} \xi^2 - 1 \right) \\
 &= 2^{2n+m} \xi^2 - 2^{2n} \xi - 2^{n+m} \xi + 2^{2n+m} \xi^2 \\
 &= 2^{2n+m+1} \xi^2 - 2^{2n} \xi - 2^{n+m} \xi.
 \end{aligned} \tag{5.4}$$

Agora queremos verificar se (5.4) é igual a

$$(2^{n+1} - 1)2^{n+m} \xi^2. \tag{5.5}$$

Desenvolvendo a expressão (5.5), obtemos que:

$$(2^{n+1} - 1)2^{n+m} \xi^2 = 2^{2n+m+1} \xi^2 - 2^{n+m} \xi^2. \tag{5.6}$$

Igualando (5.6) e (5.4), concluímos que:

$$\begin{aligned}
 2^{2n+m+1} \xi^2 - 2^{n+m} \xi^2 &= 2^{2n+m+1} \xi^2 - 2^{2n} \xi - 2^{n+m} \xi \\
 2^{n+m} \xi^2 &= \xi (2^{2n} + 2^{n+m}) \\
 2^{n+m} \xi &= (2^{2n} + 2^{n+m}) \\
 \xi &= \frac{(2^{2n} + 2^{n+m})}{2^{n+m}} \\
 \xi &= 2^{n-m} + 1.
 \end{aligned}$$

Portanto, $2^n(pq + r) = \sigma(2^n pq) = \sigma(2^n r)$, o que conclui a demonstração de que $2^n pq$ e $2^n r$ são números amigáveis, sendo p, q e r primos.

□

Tanto as regras propostas por Qurra quanto as refinadas por Euler foram fundamentais para o avanço no estudo dos números amigáveis. A abordagem de Euler, em particular, provou ser extremamente eficaz na identificação de novos pares, transformando a pesquisa nessa área. Seus trabalhos ampliaram consideravelmente a lista de pares conhecidos até então e estabeleceram novas bases para a investigação desses números.

Os avanços tecnológicos e o desenvolvimento de novas técnicas matemáticas têm possibilitado a descoberta de um número cada vez maior de pares de números amigáveis. Apesar de a infinitude desses pares não ter sido provada, a comunidade matemática continua a buscar por eles. Uma das abordagens mais promissoras nesse campo é a de Riele – Teorema 5.3 (Silva Júnior, 2017, p. 60), que consiste em utilizar pares amigáveis já conhecidos como ponto de partida para gerar novos pares. Essa metodologia tem sido fundamental para os avanços recentes na área e continua a ser uma ferramenta valiosa na busca por esses números especiais (Santos Júnior, 2020).

Teorema 5.3. *Sejam $m = a \cdot u$ e $n = a \cdot p$ um par de números amigáveis conhecido, com $(a, u) = (a, p) = 1$, sendo p primo. Se existir um par de primos (r, s) , com $p < r < s$ e $(a, rs) = 1$, satisfazendo*

$$(r - p)(s - p) = \frac{\sigma(a)}{a} \sigma^2(u),$$

e se existir um terceiro primo q , com $(au, q) = 1$ e

$$q = r + s + u,$$

então $m_1 = a \cdot u \cdot q$ e $n_1 = a \cdot r \cdot s$ são números amigáveis.

5.3 PADRÕES NUMÉRICOS E APLICAÇÕES

A definição de números amigáveis, pares de inteiros cuja soma dos divisores próprios é reciprocamente igual, é um conceito clássico na Teoria dos Números. Embora essa caracterização seja fundamental, a investigação de números amigáveis revela uma complexidade inesperada, com a ocorrência de padrões não triviais que ampliam a perspectiva de estudo desses objetos matemáticos.

De acordo com Taneja (2017 *apud* Madachy, 1966), além da conhecida relação entre números amigáveis, existe outra categoria de pares numéricos que estabelecem uma conexão única através de seus quadrados, como ilustram os Exemplos 5.4 e 5.5.

Exemplo 5.4. *Soma de quadrados.*

$$\begin{aligned} 3869 &= 62^2 + 05^2 \Leftrightarrow 6205 = 38^2 + 69^2 \\ 5965 &= 77^2 + 06^2 \Leftrightarrow 7706 = 59^2 + 65^2 \\ 43354 &= 127^2 + 165^2 \Leftrightarrow 127165 = 43^2 + 354^2 \\ 137461 &= 231^2 + 290^2 \Leftrightarrow 231290 = 137^2 + 461^2 \\ 1261485 &= 222^2 + 1101^2 \Leftrightarrow 2221101 = 126^2 + 1485^2 \\ 1528804 &= 298^2 + 1200^2 \Leftrightarrow 2981200 = 1528^2 + 804^2 \\ 7414650 &= 2217^2 + 1581^2 \Leftrightarrow 22171581 = 741^2 + 4650^2 \end{aligned}$$

Exemplo 5.5. *Subtração de quadrados.*

$$\begin{aligned} 16 &= -3^2 + 5^2 \Leftrightarrow 35 = -1^2 + 6^2 \\ 28 &= -6^2 + 8^2 \Leftrightarrow 68 = 2^2 + 8^2 \\ 240 &= 16^2 - 04^2 \Leftrightarrow 1604 = 2^2 + 40^2 \\ 369 &= 12^2 + 15^2 \Leftrightarrow 1215 = 36^2 - 9^2 \\ 1155 &= -31^2 + 46^2 \Leftrightarrow 3146 = 11^2 + 55^2 \\ 2205 &= 42^2 + 021^2 \Leftrightarrow 42021 = -2^2 + 205^2 \\ 2880 &= 56^2 - 16^2 \Leftrightarrow 5616 = -28^2 + 80^2 \end{aligned}$$

Os pares de números dos Exemplos 5.4 e 5.5 são apresentados por Taneja (2017, p. 13) e demonstram uma intrigante interdependência entre seus dígitos. Ao decompor cada número em uma soma ou subtração de quadrados, percebe-se que os dígitos do outro número são utilizados para construir esses quadrados, criando uma espécie de quebra-cabeça numérico.

A ausência de uma teoria matemática formal para explicar essa relação torna a busca por mais pares extremamente desafiadora. O padrão contido, caso exista, é provavelmente bastante complexo e oculto. Embora exista a possibilidade de ser apenas uma coincidência numérica, essa descoberta nos lembra da rica diversidade e dos mistérios que permeiam o mundo dos números.

Em sua pesquisa, Taneja (2017, p. 2-3) também apresenta os números “*self-amicable*”, ou números autoamigáveis, que se distinguem dos pares de números relacionados por seus quadrados. A definição desses números é baseada em operações multiplicativas, como mostra o Exemplo 5.6.

Exemplo 5.6. *Decomposição multiplicativa.*

$$\begin{aligned} 168 &= 19 \times 8 + 2 \times 8 \Leftrightarrow 192 = 16 \times 8 + 8 \times 8 \\ 248 &= 25 \times 8 + 6 \times 8 \Leftrightarrow 256 = 24 \times 8 + 8 \times 8 \\ 1267 &= 187 \times 7 - 6 \times 7 \Leftrightarrow 1876 = 1 \times 7 + 267 \times 7 \\ 63 &= 8 \times 9 - 1 \times 9 \Leftrightarrow 81 = 6 \times 9 + 3 \times 9 \end{aligned}$$

Taneja (2017) destaca a ausência de pesquisas sobre padrões em números amigáveis na literatura. Para preencher essa lacuna, o autor apresenta novos exemplos, como o Exemplo 5.7 (Taneja, 2017, p. 3), e evidências que sugerem a existência de padrões nesses números, tanto amigáveis quanto autoamigáveis, estimulando futuras investigações nessa área.

Exemplo 5.7. *Outras decomposições multiplicativas.*

$$\begin{aligned} 165 &= 33 \times 5 + 0 \times 5 = 3 \times 5 + 30 \times 5 \Leftrightarrow 330 = 1 \times 5 + 65 \times 5 \\ 1665 &= 333 \times 5 + 0 \times 5 = 3 \times 5 + 330 \times 5 \Leftrightarrow 3330 = 1 \times 5 + 665 \times 5 \\ 16665 &= 3333 \times 5 + 0 \times 5 = 3 \times 5 + 3330 \times 5 \Leftrightarrow 33330 = 1 \times 5 + 6665 \times 5 \\ 166665 &= 33333 \times 5 + 0 \times 5 = 3 \times 5 + 33330 \times 5 \Leftrightarrow 333330 = 1 \times 5 + 66665 \times 5 \\ 1666665 &= 333333 \times 5 + 0 \times 5 = 3 \times 5 + 333330 \times 5 \Leftrightarrow 3333330 = 1 \times 5 + 666665 \times 5 \end{aligned}$$

Em seu estudo, Taneja (2017) explora uma nova dimensão dos números amigáveis, identificando padrões pouco convencionais que vão além dos exemplos tradicionais. Sua pesquisa abre portas para futuras investigações nessa área. Além dos exemplos abordados nesse trabalho, o autor apresenta outros padrões que podem ser encontrados em seu artigo.

Mergulhar no mundo dos números amigáveis é tentar desvendar um enigma matemático. A descoberta de padrões entre os quadrados desses números desafia nossa intuição e nos convida a escrutinar um território ainda inexplorado da Teoria dos Números, repleto de conexões surpreendentes.

5.3.1 NÚMEROS MUTUAMENTE AMIGOS E AMIGOS QUADRÁTICOS

A Matemática, com sua beleza peculiar, revela-se como uma verdadeira obra de arte. Seus padrões, como tesouros escondidos, aguardam para serem descobertos por aqueles que possuem olhos para vê-los. Essa busca por regularidades, que vai além da mera aplicação de fórmulas, exige criatividade e uma profunda apreciação pela harmonia dos números. A descoberta de novos padrões não apenas amplia as fronteiras do conhecimento, mas também nos permite apreciar a sofisticação e a complexidade do universo matemático.

Um exemplo dessa beleza e elegância são os números amigáveis, que estabelecem relações particulares e surpreendentes entre si. Essa noção, por sua vez, abre portas para conceitos mais abrangentes como números mutuamente amigos e amigos quadráticos, revelando a riqueza e a diversidade das interações numéricas.

A noção de números mutuamente amigos baseia-se na relação estabelecida a partir das razões entre a soma dos divisores de cada número e o próprio número. Essa abordagem proporciona uma generalização interessante, indo além da troca direta de somas entre divisores próprios, como ocorre nos números amigáveis clássicos.

O artigo de Bishop *et al.* (2021) expande a noção tradicional de números amigáveis, que se baseia na igualdade da soma dos divisores próprios. No artigo, os autores introduzem o índice de abundância como uma ferramenta para quantificar a divisibilidade de um número. Ao estabelecer uma relação entre o índice de abundância de dois números, uma nova definição de números amigáveis é proposta. Nessa perspectiva, a amizade entre números é caracterizada pela igualdade de seus índices de abundância.

De acordo com Bulhões (2020), a função Índice de Abundância $I(n)$ é definida como

$$I(n) = \frac{\sigma(n)}{n}, \text{ com } n \in \mathbb{N}.$$

Segundo Castro (2016, p. 1): “Dois números a e b são mutuamente amigos se a razão entre a soma de todos os divisores do número a e o número a é igual a razão entre a soma de todos os divisores do número b e o número b ”. Esta definição, juntamente com a função índice de abundância, nos permite formalizar o conceito de números mutuamente amigos - Definição 5.2.

Definição 5.2. *Dois números inteiros positivos a e b são mutuamente amigos quando*

$$\frac{\sigma(a)}{a} = \frac{\sigma(b)}{b}. \quad (5.7)$$

Os Exemplos 5.8 a 5.10 ilustram pares de números que satisfazem a relação (5.7).

Exemplo 5.8. *Os números 30 e 140 são mutuamente amigos:*

$$\begin{aligned}\sigma(30) &= 1 + 2 + 3 + 5 + 6 + 10 + 15 + 30 = 72; \\ \sigma(140) &= 1 + 2 + 4 + 5 + 7 + 10 + 14 + 20 + 28 + 35 + 70 + 140 = 336; \\ \frac{72}{30} &= \frac{336}{140} = \frac{12}{5}.\end{aligned}$$

Exemplo 5.9. *Os números 66 e 308 são mutuamente amigos:*

$$\begin{aligned}\sigma(66) &= 1 + 2 + 3 + 6 + 11 + 22 + 33 + 66 = 144; \\ \sigma(308) &= 1 + 2 + 4 + 7 + 11 + 14 + 22 + 28 + 44 + 77 + 154 + 308 = 672; \\ \frac{144}{66} &= \frac{672}{308} = \frac{24}{11}.\end{aligned}$$

Exemplo 5.10. *Os números 80 e 200 são mutuamente amigos:*

$$\begin{aligned}\sigma(80) &= 1 + 2 + 4 + 5 + 8 + 10 + 16 + 20 + 40 + 80 = 186; \\ \sigma(200) &= 1 + 2 + 4 + 5 + 8 + 10 + 20 + 25 + 40 + 50 + 100 + 200 = 465; \\ \frac{186}{80} &= \frac{465}{200} = \frac{93}{40}.\end{aligned}$$

Diversos números podem ter o mesmo índice de abundância. Por exemplo, além de 30 e 140, números como 2480, 6200 e 40640 também possuem índice de abundância igual a $\frac{12}{5}$. Quando o índice de abundância de um número é um quociente inteiro, o número é denominado *multiplamente perfeito*. Números perfeitos possuem um índice de abundância específico, igual a 2 (Bishop, 2021), como mostra o Exemplo 5.11.

Exemplo 5.11. *Os números 6 e 28 são perfeitos:*

$$\begin{aligned}\sigma(6) &= 1 + 2 + 3 + 6 = 12; \\ \sigma(28) &= 1 + 2 + 4 + 7 + 14 + 28 = 56; \\ \frac{12}{6} &= \frac{56}{28} = 2.\end{aligned}$$

Após explorar os números mutuamente amigos e suas características únicas, é interessante observar outra classe peculiar de números com relações numéricas especiais: os números amigos quadráticos - Definição 5.3 (Qconcursos, 2019).

Definição 5.3. *Dois números inteiros positivos a e b são amigos quadráticos quando a soma dos algarismos de a^2 resulta em b e a soma dos algarismos de b^2 resulta em a .*

A curiosa relação estabelecida na Definição 5.3 é mencionada em *O homem que calculava*, onde Tahan (2013, p. 36) a descreve como: “Vamos somar os algarismos de 256. Obtemos a soma 13. O quadrado de 13 é 169. Vamos, agora, somar os algarismos de 169. A soma dos algarismos de 169 é 16. Existe, portanto, entre os números 13 e 16, uma curiosa relação que poderia ser chamada a amizade quadrática”. Na Figura 5.3, observamos o par de números amigos quadráticos 13 e 16, descritos por Tahan (2013) em sua obra.

A pesquisa sobre números amigos quadráticos tem demonstrado ser um campo desafiador. A dificuldade em encontrar novos pares reflete a falta de estudos sistemáticos e as limitações computacionais atuais. No entanto, o par (13, 16) serve como um exemplo motivador. A continuidade das investigações, com o auxílio de métodos computacionais mais eficientes, poderá revelar padrões subjacentes e aprofundar nossa compreensão da estrutura dos números inteiros.

Figura 5.3 – Números amigos quadráticos



Fonte: Tenório (2019).

6 RECURSO EDUCACIONAL: ATIVIDADES PARA A EDUCAÇÃO BÁSICA

Neste capítulo, propomos uma série de atividades que visam consolidar e expandir os conhecimentos matemáticos sobre números primos, números perfeitos e números amigáveis. Por meio de problemas contextualizados e desafiadores, os estudantes serão estimulados a aplicar os conhecimentos adquiridos, desenvolvendo o raciocínio lógico, a criatividade e aprimorando suas habilidades de pensamento computacional. Para cada atividade, apresentamos uma sugestão de sequência didática detalhada, com o objetivo de auxiliar o professor na condução das aulas de forma eficaz e engajadora.

Na construção das sequências didáticas, utilizamos o soroban digital e dois softwares que desempenham um papel fundamental na visualização e exploração matemática: o GeoGebra e o GNU Octave. Tutoriais das duas ferramentas computacionais podem ser encontrados, respectivamente, em GeoGebraTeam (2025) e Wiki (2024).

O GeoGebra é um software dinâmico de Matemática que permite explorar conceitos algébricos, geométricos e estatísticos de maneira interativa. Ele possibilita a construção de gráficos, a manipulação de objetos geométricos e a criação de animações, tornando o aprendizado mais intuitivo e visual. Além disso, pode ser acessado diretamente pelo navegador, sem necessidade de instalação, por meio do site: <<https://www.geogebra.org/>>.

Já o GNU Octave é uma ferramenta para realizar cálculos numéricos, permitindo a realização de operações matemáticas complexas, análise de dados e programação matemática. O GNU Octave é uma excelente opção para simulação e modelagem de problemas matemáticos, sendo especialmente útil para atividades que envolvem padrões numéricos e algoritmos. Para utilizá-lo, é necessário baixá-lo em seu computador. O software pode ser obtido gratuitamente em: <<https://octave.org/>>. Neste trabalho, empregamos a versão 9.2.0. do GNU Octave.

A utilização dessas ferramentas contribuirá para tornar as atividades mais dinâmicas e interativas, incentivando a exploração matemática e o desenvolvimento do pensamento computacional.

6.1 ATIVIDADE 1: EXPLORANDO OS NÚMEROS POLIGONAIS

1.1 Nível: Ensino Fundamental II.

1.2 Ano: 8º e 9º.

1.3 Número de aulas: 4 (45 minutos cada).

1.4 Competências específicas da BNCC:

- Compreender as relações entre conceitos e procedimentos dos diferentes campos da Matemática (Aritmética, Álgebra, Geometria, Estatística e Probabilidade) e de outras áreas do conhecimento, sentindo segurança quanto à própria capacidade de construir e aplicar conhecimentos matemáticos, desenvolvendo a autoestima e a perseverança na busca de soluções;
- Utilizar processos e ferramentas matemáticas, inclusive tecnologias digitais disponíveis, para modelar e resolver problemas cotidianos, sociais e de outras áreas de conhecimento, validando estratégias e resultados.

1.5 Habilidades específicas BNCC:

(EF08MA10) Identificar a regularidade de uma sequência numérica ou figural não recursiva e construir um algoritmo por meio de um fluxograma que permita indicar os números ou as figuras seguintes;

(EF08MA11) Identificar a regularidade de uma sequência numérica recursiva e construir um algoritmo por meio de um fluxograma que permita indicar os números seguintes;

(EF09MA09) Compreender os processos de fatoração de expressões algébricas, com base em suas relações com os produtos notáveis, para resolver e elaborar problemas que possam ser representados por equações polinomiais do 2º grau.

(EF09MA15) Descrever, por escrito e por meio de um fluxograma, um algoritmo para a construção de um polígono regular cuja medida do lado é conhecida, utilizando régua e compasso, como também softwares.

1.6 Conteúdos abordados: sequências; números poligonais; equações do 2º grau.

1.7 Objetivos:

- Estimular a visualização dos números triangulares como padrões geométricos, utilizando o GeoGebra;
- Desenvolver habilidades de cálculo e análise numérica, utilizando o GNU Octave;
- Promover a busca por padrões e regularidades nas sequências de números triangulares;
- Proporcionar desafios que exigem a aplicação dos conhecimentos adquiridos;
- Relacionar os conceitos matemáticos com ferramentas computacionais.

1.8 Procedimento metodológico: aula expositiva e dialogada; solução de problemas.

1.9 Avaliação: observação do desempenho dos estudantes durante a realização da atividade.

Os números poligonais, ou números geométricos, são números que podem ser visualizados como pontos organizados em figuras geométricas regulares, como triângulos, quadrados,

pentágonos ou hexágonos. Um exemplo são os números triangulares, que formam triângulos equiláteros, onde cada lado possui um ponto a mais que o lado anterior.

Agora, embarcaremos em uma jornada de descobertas pelos números triangulares! Você terá que confrontar 7 desafios matemáticos – Desafios 6.1 a 6.7. Para responder às questões, você precisará utilizar o GeoGebra e o GNU Octave. O GeoGebra será útil para visualizar e construir figuras geométricas, enquanto o GNU Octave será utilizado para realizar cálculos e análises numéricas.

Desafio 6.1. *Quais dos seguintes números são triangulares: 9, 15, 29, 55?*

Use o controle deslizante na página do GeoGebra <<https://www.geogebra.org/m/eywn5mz4>> para resolver o Desafio 6.1.

Solução 6.1. (Desafio 6.1) *Clicamos no link disponibilizado no Desafio 6.1 e verificamos se os números são triangulares usando o controle deslizante. Observando as imagens da Figura 6.1, temos: para $n = 4$, $T = 10$; para $n = 5$, $T = 15$; para $n = 7$, $T = 28$; para $n = 10$, $T = 55$.*

Figura 6.1 – Números triangulares: (a) $T = 10$; (b) $T = 15$; (c) $T = 28$; (d) $T = 55$



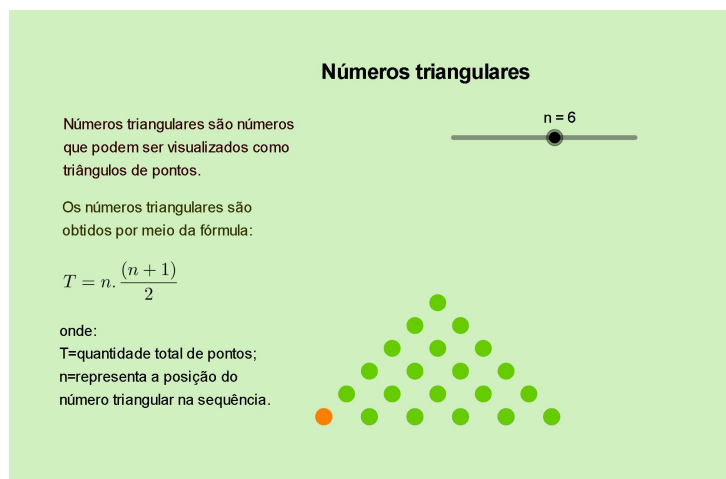
Fonte: Autora com o GeoGebra.

Logo, os números triangulares são 15 e 55.

Desafio 6.2. Qual é o número triangular de um triângulo que possui 6 pontos em cada lado? Use o controle deslizante na página do Geogebra <<https://www.geogebra.org/m/eywn5mz4>> para solucionar o Desafio 6.2.

Solução 6.2. (Desafio 6.2) Clicamos no link disponibilizado no Desafio 6.2, deslocamos o controle deslizante até $n = 6$ e contamos o total de pontos do triângulo.

Figura 6.2 – Número triangular para $n = 6$



Fonte: Autora com o GeoGebra.

Assim, para $n = 6$ temos que o número triangular é $T = 21$ – Figura 6.2.

Desafio 6.3. Encontre todos os números triangulares entre 100 e 200. Use o script do GNU Octave – Figura 6.3 – para responder o Desafio 6.3.

Figura 6.3 – Script para calcular números triangulares entre 100 e 200

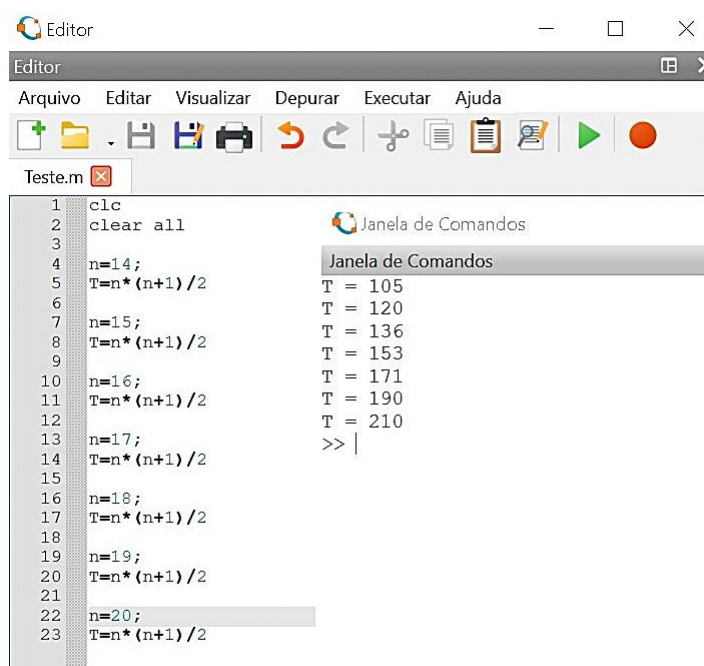
```

1  clc
2  clear all
3
4  n=14;
5  T=n*(n+1)/2
6
7  n=15;
8  T=n*(n+1)/2
9
10 n=16;
11 T=n*(n+1)/2
12
13 n=17;
14 T=n*(n+1)/2
15
16 n=18;
17 T=n*(n+1)/2
18
19 n=19;
20 T=n*(n+1)/2
21
22 n=20;
23 T=n*(n+1)/2
  
```

Fonte: Autora com o GNU Octave.

Solução 6.3. (Desafio 6.3) Para configurar o script no GNU Octave, é preciso definir as seguintes variáveis inteiras: T , que corresponde ao número triangular (total de pontos da figura); n , que corresponde à posição do número triangular na sequência (número de pontos dos lados do triângulo). A variável n é fornecida pelo usuário, enquanto que a variável $T = \frac{n(n+1)}{2}$ é calculada pelo GNU Octave. A Figura 6.4 ilustra a resolução do Desafio 6.3.

Figura 6.4 – Números triangulares entre 100 e 200



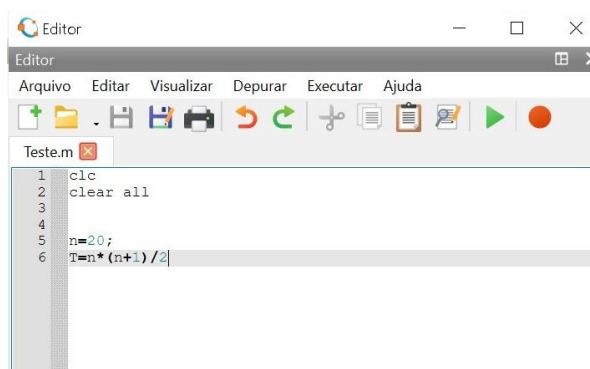
Fonte: Autora com o GNU Octave.

Portanto, os números triangulares entre 100 e 200 são: 105, 120, 136, 153, 171 e 190.

Desafio 6.4. Um auditório tem suas cadeiras dispostas em 20 fileiras, formando um grande triângulo. Sabendo que a primeira fila tem 1 cadeira, a segunda 2, a terceira 3 e assim sucessivamente, calcule quantas cadeiras há no auditório.

Use o script do GNU Octave – Figura 6.5 – para solucionar o Desafio 6.4.

Figura 6.5 – Script para calcular o número triangular para $n = 20$

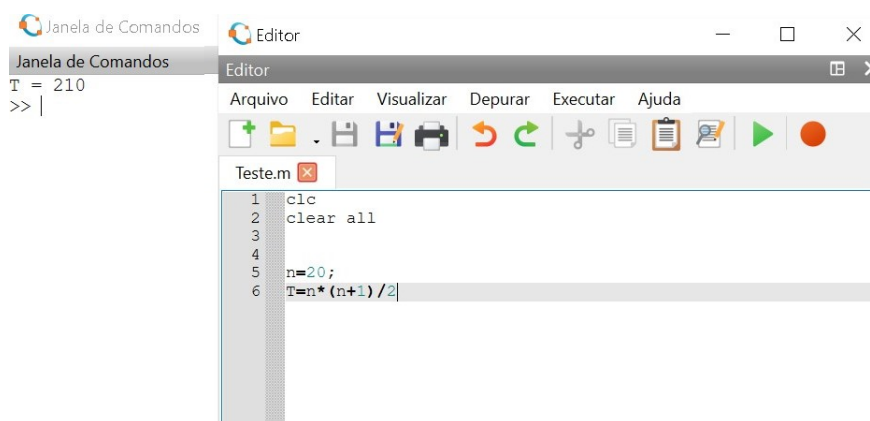


Fonte: Autora com o GNU Octave.

Solução 6.4. (Desafio 6.4) Para configurar o script no GNU Octave, é preciso definir as seguintes variáveis inteiras: T , que corresponde ao número triangular (total de pontos da figura); n , que corresponde à posição do número triangular na sequência (números de pontos dos lados do triângulo). A variável n é fornecida pelo usuário, enquanto que a variável $T = \frac{n(n+1)}{2}$ é calculada pelo GNU Octave.

Para solucionar o Desafio 6.4, o usuário deve substituir a variável n por 20 – Figura 6.6.

Figura 6.6 – Número triangular para $n = 20$



Fonte: Autora com o GNU Octave.

Logo, se a última fileira tem 20 cadeiras, há 210 cadeiras no auditório.

Desafio 6.5. Dado um número T , podemos verificar se esse número é triangular resolvendo a equação:

$$n = \frac{-1 \pm \sqrt{1 + 8T}}{2}.$$

Se n for um número inteiro positivo, então o número T é triangular.

Verifique se os seguintes números são triangulares:

a) $T = 45034795$;

b) $T = 6759361105$.

Use o script do GNU Octave – Figura 6.7 – para resolver o Desafio 6.5. Para configurar o script no GNU Octave, usamos os comandos `sqrt` (calcula a raiz quadrada), `floor` (determina a parte inteira de um número) e `fprintf` (exibe o resultado).

Solução 6.5. (Desafio 6.5) Para configurar o script no GNU Octave, é preciso definir as seguintes variáveis, inteira e real, respectivamente: T , que corresponde ao número triangular (total de pontos da figura); n , que corresponde à posição do número triangular na sequência (número de pontos dos lados do triângulo). A variável T é fornecida pelo usuário, enquanto que a variável n é calculada pelo GNU Octave. A Figura 6.8 ilustra a solução do Desafio 6.5.

Figura 6.7 – Script para verificar se T é um número triangular

```

1  clc
2  clear all
3
4
5  T=45034795; %
6  n1=(-1+sqrt(1+8*T))/2
7  n2=(-1-sqrt(1+8*T))/2
8
9  disp("n1 = "), disp(n1)
10 disp("n2 = "), disp(n2)
11
12 if floor(n1) == n1 && n1 > 0
13     disp("T é um número triangular!")
14 else
15     disp("T NÃO é um número triangular!")
16 endif
17 ;fprintf("\n")
18 fprintf("\n")
19 T=6759361105;
20 n1=(-1+sqrt(1+8*T))/2
21 n2=(-1-sqrt(1+8*T))/2
22
23 disp("n1 = "), disp(n1)
24 disp("n2 = "), disp(n2)
25
26 if floor(n1) == n1 && n1 > 0
27     disp("T é um número triangular!")
28 else
29     disp("T NÃO é um número triangular!")
30 endif

```

linha: 18 col: 14 codificação: UTF-8 fdl: CRLF

Fonte: Autora com o GNU Octave.

Figura 6.8 – Verificação de números triangulares

Janela de Comandos

```

n1 = 9490
n2 = -9491
n1 =
9490
n2 =
-9491
T é um número triangular!

n1 = 1.1627e+05
n2 = -1.1627e+05
n1 =
1.1627e+05
n2 =
-1.1627e+05
T NÃO é um número triangular!
>>

```

Editor

```

1  clc
2  clear all
3
4
5  T=45034795; %
6  n1=(-1+sqrt(1+8*T))/2
7  n2=(-1-sqrt(1+8*T))/2
8
9  disp("n1 = "), disp(n1)
10 disp("n2 = "), disp(n2)
11
12 if floor(n1) == n1 && n1 > 0
13     disp("T é um número triangular!")
14 else
15     disp("T NÃO é um número triangular!")
16 endif
17 ;fprintf("\n")
18 fprintf("\n")
19 T=6759361105;
20 n1=(-1+sqrt(1+8*T))/2
21 n2=(-1-sqrt(1+8*T))/2
22
23 disp("n1 = "), disp(n1)
24 disp("n2 = "), disp(n2)
25
26 if floor(n1) == n1 && n1 > 0
27     disp("T é um número triangular!")
28 else
29     disp("T NÃO é um número triangular!")
30 endif

```

linha: 18 col: 14 codificação: UTF-8 fdl: CRLF

Fonte: Autora com o GNU Octave.

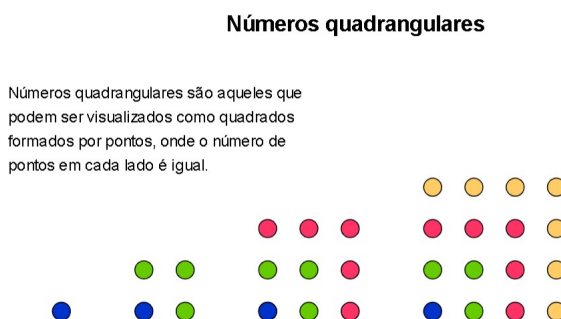
Assim, temos que: a) $T = 45034795$ é um número triangular; b) $T = 6759361105$ não é um número triangular.

Desafio 6.6. Calcule todos os números triangulares para n variando de 1 a 10. Verifique o padrão obtido e use-o para determinar qual é o número triangular para $n = 11$ e $n = 12$. Use o controle deslizante na página do Geogebra <<https://www.geogebra.org/m/eywn5mz4>> para solucionar o Desafio 6.6.

Solução 6.6. (Desafio 6.6) Clicamos no link disponibilizado no Desafio 6.6, deslocamos o controle deslizante e contamos quantos pontos são acrescentados para cada novo valor de n . Ao variar n de 1 a 10, obtemos a seguinte sequência de números triangulares: $\{1, 3, 6, 10, 15, 21, 28, 36, 45, 55\}$. Observamos que para determinar o próximo número triangular, basta somar o próximo valor de n ao último número obtido na sequência. Logo: para $n = 11$, temos $55 + 11 = 66$; para $n = 12$, temos $66 + 12 = 78$.

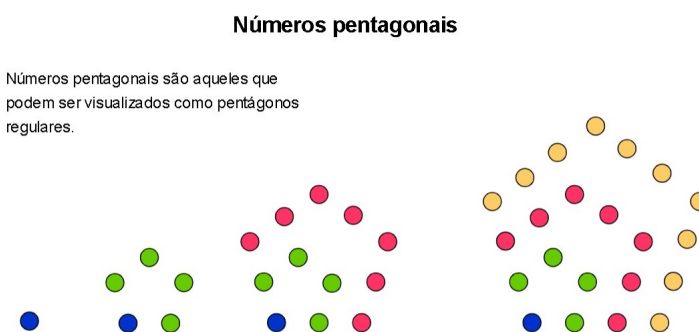
Desafio 6.7. As Figuras 6.9, 6.10 e 6.11 ilustram, respectivamente, números quadrangulares, pentagonais e hexagonais. Cada uma dessas figuras mostra uma sequência e um padrão. Constate o padrão e diga qual o próximo número de cada sequência.

Figura 6.9 – Números quadrangulares



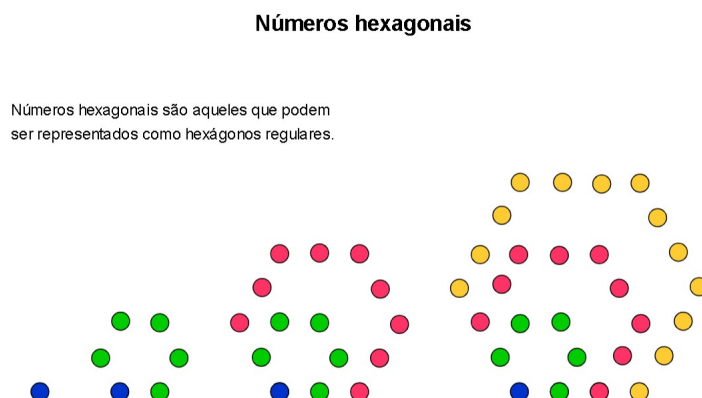
Fonte: Autora com o GeoGebra.

Figura 6.10 – Números pentagonais



Fonte: Autora com o GeoGebra.

Figura 6.11 – Números hexagonais



Fonte: Autora com o GeoGebra.

Solução 6.7. (Desafio 6.7) Nos números quadrangulares, a sequência é $\{1, 4, 9, 16, \dots\}$. A diferença entre dois números quadrangulares consecutivos aumenta sempre em 2: de 1 para 4, aumenta 3; de 4 para 9, aumenta 5; de 9 para 16, aumenta 7. Seguindo esse padrão, para obtermos o próximo número teremos que aumentar 9 unidades, ou seja, $16 + 9 = 25$. Logo, o próximo número da sequência é 25.

Nos números pentagonais, a sequência é $\{1, 5, 12, 22, \dots\}$. A diferença entre dois números pentagonais consecutivos aumenta sempre em 3: de 1 para 5, aumenta 4; de 5 para 12, aumenta 7; de 12 para 22, aumenta 10. Seguindo esse padrão, para obtermos o próximo número teremos que aumentar 13 unidades, isto é, $22 + 13 = 35$. Portanto, o próximo número da sequência é 35.

Nos números hexagonais, a sequência é $\{1, 6, 15, 28, \dots\}$. A diferença entre dois números hexagonais consecutivos aumenta sempre em 4: de 1 para 6, aumenta 5; de 6 para 15, aumenta 9; de 15 para 28, aumenta 13. Seguindo esse padrão, para obtermos o próximo número teremos que aumentar 17 unidades, ou seja, $28 + 17 = 45$. Logo, o próximo número da sequência é 45.

6.2 ATIVIDADE 2: DECIFRANDO MENSAGENS SECRETAS COM NÚMEROS PRIMOS

1.1 Nível: Ensino Fundamental II.

1.2 Ano: 6º.

1.3 Número de aulas: 4 (45 minutos cada).

1.4 Competências específicas BNCC:

- Compreender as relações entre conceitos e procedimentos dos diferentes campos da Matemática (Aritmética, Álgebra, Geometria, Estatística e Probabilidade) e de outras

áreas do conhecimento, sentindo segurança quanto à própria capacidade de construir e aplicar conhecimentos matemáticos, desenvolvendo a autoestima e a perseverança na busca de soluções;

- Utilizar processos e ferramentas matemáticas, inclusive tecnologias digitais disponíveis, para modelar e resolver problemas cotidianos, sociais e de outras áreas de conhecimento, validando estratégias e resultados.

1.5 Habilidades específicas BNCC:

(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.

(EF06MA06) Resolver e elaborar problemas que envolvam as ideias de múltiplo e de divisor.

1.6 Conteúdos abordados: números primos e compostos.

1.7 Objetivos:

- Consolidar o conceito de decomposição em fatores primos;
- Desenvolver habilidades de programação;
- Aplicar a Matemática em um contexto prático;
- Desenvolver o raciocínio lógico.

1.8 Procedimento metodológico: aula expositiva e dialogada; solução de problemas.

1.9 Avaliação: observação do desempenho dos estudantes durante a realização da atividade.

Agentes secretos usam códigos para se comunicar e proteger informações importantes. Você está pronto para se tornar um agente secreto da Matemática? No Desafio 6.8, vamos decifrar uma mensagem secreta usando uma ferramenta poderosa: a decomposição em fatores primos.

Desafio 6.8. *Cada número da mensagem codificada esconde duas letras. Para descobri-las, você precisará decompor o número em seus fatores primos e seguir as pistas que te daremos. Você está preparado para essa missão? Mas antes de começarmos, leia com atenção as instruções. Você receberá:*

1. *uma tabela - Tabela 6.1, na qual letras do alfabeto português e dois sinais (. e -) estão associadas a um número primo;*
2. *uma sequência de números que deverão ser fatorados.*

Como funciona a decodificação?

Tabela 6.1 – Tabela para descobrir a mensagem secreta

A	B	C	D	E	I	L	M	N	O	P	R	S
2	3	5	7	11	13	17	19	23	29	31	37	41

T	U	-	.
43	47	53	59

Fonte: Autora.

- **Sequência de números:** cada número da sequência esconde duas letras da mensagem secreta;
- **Quebrando o código:** para descobrir as letras, você precisa fatorar o número em números primos. É como montar um quebra-cabeça com números;
- **GNU Octave:** vamos empregá-lo para fatorar os números e nos auxiliar a desvendar esse mistério. No GNU Octave, o comando `factor(n)` determina a decomposição em fatores primos do número inteiro positivo n ;
- **Cores revelam a ordem:** os números da sequência (lista) terão cores diferentes. Se o número for vermelho, você escreve o fator primo menor primeiro e depois o maior. Mas se o número for azul, você escreve o fator primo maior primeiro e depois o menor. Por exemplo: se você tiver o número 15 na cor azul, você precisa decompor 15 em dois números primos: 3 e 5. Como o número é azul, você escreve primeiro o 5 e depois o 3. Em seguida, você procura os números primos 5 e 3 na Tabela 6.1 e descobre quais letras esses números representam;
- **Montando a frase:** depois de descobrir todos os pares de números primos, você consulta a Tabela 6.1 e monta a frase secreta.

Agora estamos prontos para começar!

Frase codificada:

1189/1081/209/1073/2173/1147/247/1189/82/1537/1189/51/145/1189/77/145/
943/1591/235/58/77/1247/203/2173/1189/1081/209/1073/2419

Figura 6.12 – Espaço para decodificação da frase

$\frac{1}{2} \quad \frac{1}{3} \quad \frac{1}{4} \quad \frac{1}{5} \quad \frac{1}{6} \quad \frac{1}{7} \quad \frac{1}{8} \quad \frac{1}{9} \quad \frac{1}{10} \quad \frac{1}{11} \quad \frac{1}{12} \quad \frac{1}{13} \quad \frac{1}{14} \quad \frac{1}{15}$

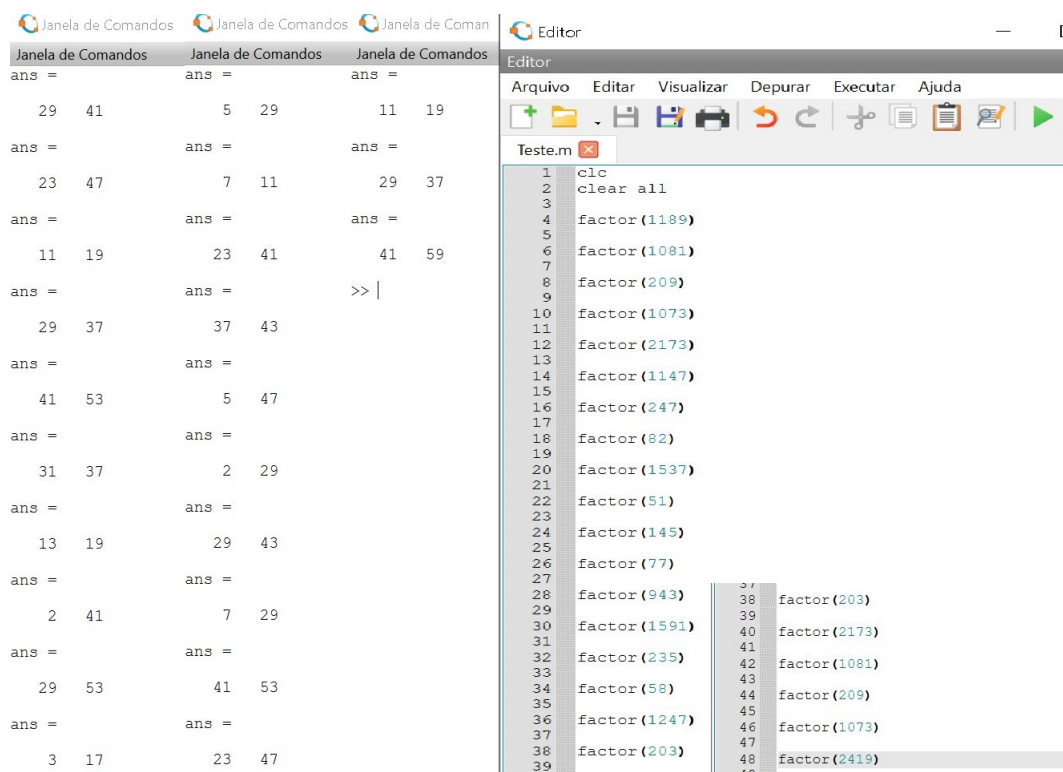
Fonte: Autora.

Preencha os espaços da Figura 6.12 com as letras obtidas e ao final escreva a frase encontrada.

Frase Final: ?

Solução 6.8. (Desafio 6.8) Para configurar o script de fatoração no GNU Octave, basta digitar *factor(n)*, onde *n* será substituído pelo número que se quer decompor. A Figura 6.13 ilustra a fatoração dos números da sequência fornecida com o GNU Octave. Já a Figura 6.14 apresenta a frase decodificada.

Figura 6.13 – Fatoração dos números da sequência fornecida



Fonte: Autora com o GNU Octave.

Figura 6.14 – Frase decodificada

OS/NU/ME/RO/S-/PR/IM/OS/SA/O-/OS/BL/OC/OS/DE/
CO/NS/TR/UC/AO/DE/TO/DO/S-/OS/NU/ME/RO/S

Fonte: Autora.

Logo, a decodificação resulta na frase: Os números primos são os blocos de construção de todos os números.

6.3 ATIVIDADE 3: RASTREANDO NÚMEROS PERFEITOS

1.1 Nível: Ensino Fundamental II.

1.2 Ano: 8º.

1.3 Número de aulas: 4 (45 minutos cada).

1.4 Competências específicas BNCC:

- Compreender as relações entre conceitos e procedimentos dos diferentes campos da Matemática (Aritmética, Álgebra, Geometria, Estatística e Probabilidade) e de outras áreas do conhecimento, sentindo segurança quanto à própria capacidade de construir e aplicar conhecimentos matemáticos, desenvolvendo a autoestima e a perseverança na busca de soluções;
- Utilizar processos e ferramentas matemáticas, inclusive tecnologias digitais disponíveis, para modelar e resolver problemas cotidianos, sociais e de outras áreas de conhecimento, validando estratégias e resultados.

1.5 Habilidades específicas BNCC:

- (EF08MA04) Resolver e elaborar problemas, envolvendo cálculo de porcentagens, incluindo o uso de tecnologias digitais;
- (EF08MA06) Resolver e elaborar problemas que envolvam cálculo do valor numérico de expressões algébricas, utilizando as propriedades das operações;
- (EF08MA25) Obter os valores de medidas de tendência central de uma pesquisa estatística (média, moda e mediana) com a compreensão de seus significados.

1.6 Conteúdos abordados: números perfeitos; média e mediana; porcentagens; expressões algébricas; potenciação e radiciação.

1.7 Objetivos:

- Consolidar os conceitos matemáticos dos conteúdos abordados;
- Desenvolver habilidades computacionais;
- Estimular o raciocínio lógico e a resolução de problemas.

1.8 Procedimento metodológico: aula expositiva e dialogada; solução de problemas.

1.9 Avaliação: observação do desempenho dos estudantes durante a realização da atividade.

Prepare-se para uma expedição matemática! No Desafio 6.9 com caça-palavras, você vai explorar um mundo de números com características especiais: os números perfeitos. Ao encontrar as palavras-chave, você estará desvendando códigos secretos e revelando propriedades únicas dos números. Descubra os mistérios que se escondem por trás dos algarismos! A aventura começa agora!

Desafio 6.9. *Utilize o GNU Octave como ferramenta para realizar os cálculos necessários e responder às seguintes perguntas:*

1. *Qual é o menor número perfeito?*

2. Qual é o próximo número perfeito após 6?
3. Se um número é perfeito, quanto é a soma de seus divisores próprios?
4. Como é denominado o número cuja soma dos divisores próprios é maior do que ele mesmo?
5. Como é chamado o número cuja soma dos divisores próprios é menor do que ele mesmo?
6. Qual é a soma dos algarismos do número perfeito 496?
Para configurar o script no GNU Octave, basta digitar $\text{num} = 496$ e o comando $\text{soma} = \text{sum}(\text{str2num}(\text{num2str}(\text{num})(:)))$.
7. Qual é a diferença entre o terceiro e o segundo números perfeitos?
Para configurar o script no GNU Octave, basta digitar $a = 28$, $b = 496$ e o comando $b - a$.
8. Quantos divisores possui o número perfeito 8128?
Para configurar o script no GNU Octave, basta digitar $\text{num} = 8128$ e o comando $\text{divisores} = \text{find}(\text{mod}(\text{num}, 1:\text{num}) == 0)$.
9. Qual é o resultado de elevar o menor número perfeito ao quadrado?
Para configurar o script no GNU Octave, basta digitar $a = 6$ e o comando a^2 .
10. Qual é a fração irredutível que representa a razão entre o segundo e o primeiro números perfeitos?
Para configurar o script no GNU Octave, é necessário digitar os seguintes comandos:
 - i) $\text{gcd}(\text{num}, \text{den})$ — Calcula o máximo divisor comum (MDC) entre o numerador e o denominador;
 - ii) num / mdc — Simplifica o numerador;
 - iii) den / mdc — Simplifica o denominador;
 - iv) $\text{fprintf}(\dots)$ — Exibe o resultado da fração simplificada.
11. Qual é a porcentagem que o divisor 7 representa do número perfeito 28?
Para configurar o script no GNU Octave, é preciso fornecer os dois números $A = 7$ e $B = 28$ e usar os comandos:
 - i) $\text{porcentagem} = (A/B)*100$ — Calcula a porcentagem;
 - ii) $\text{fprintf}(\dots)$ — Exibe o resultado.
12. Qual é a parte inteira da raiz quadrada do maior número perfeito citado no Desafio 6.9?
Para configurar o script no GNU Octave, é preciso fornecer $\text{num} = ?$ e usar os comandos:
 - i) $\text{parte inteira} = \text{floor}(\text{sqrt}(\text{nm}))$ — Calcula a parte inteira da raiz quadrada;

ii) `fprintf(...)` – Exibe o resultado.

13. Qual é a média aritmética aproximada dos três primeiros números perfeitos? Arredonde a média para o próximo número inteiro.

Para configurar o script no GNU Octave, é preciso fornecer `valores = [a, b, c]` e usar os comandos:

i) `media = mean(valores)` – Calcula a média aritmética dos três valores fornecidos;

ii) `media_arredondada = ceil(media)` – Arredonda a média para o próximo inteiro;

iii) `fprintf(...)` – Exibe o resultado.

14. Qual é a mediana¹ dos divisores próprios do número perfeito 6?

Para configurar o script no GNU Octave, é preciso fornecer `num = 6` e usar os comandos:

i) `divisores_proprios = find(mod(num, 1:num-1) == 0)` – Determina os divisores próprios;

ii) `mediana = median(divisores_proprios)` – Calcula a mediana;

iii) `fprintf(...)` – Exibe o resultado.

15. Considerando $A = 6$, $B = 28$, $C = 496$ e $D = 8128$, qual será o resultado da expressão $D \cdot A^2 - (C^2 + B \cdot A^4)$?

Para configurar o script no GNU Octave, é preciso digitar $A = 6$, $B = 28$, $C = 496$, $D = 8128$ e em seguida, a expressão algébrica $D \cdot A^2 - (C^2 + B \cdot A^4)$.

Após responder às questões, encontre as respostas no caça-palavras da Figura 6.15.

Solução 6.9. (Desafio 6.9) As cinco primeiras perguntas do Desafio 6.9 exploram a compreensão teórica sobre números perfeitos, não sendo necessário o uso de operações matemáticas para respondê-las. Nas demais questões, empregamos o GNU Octave para efetuar os cálculos.

1. Qual é o menor número perfeito? **6**

2. Qual é o próximo número perfeito após 6? **28**

3. Se um número é perfeito, quanto é a soma de seus divisores próprios? **ele mesmo**

4. Como é denominado o número cuja soma dos divisores próprios é maior do que ele mesmo? **abundante**

5. Como é chamado o número cuja soma dos divisores próprios é menor do que ele mesmo? **deficiente**

¹ Valor central de um conjunto de dados ordenados.

Figura 6.15 – Caça-palavras sobre números perfeitos

```

T I S L A S E I S E N R T O N V
C G E S V O Q R E A O P T O I V
M E L W I R U C I U V S T A R I
O A E B N G A M E P E N I B S N
F U M E T T T L N I N M O U K T
G F E L E U R I K T T P D N E E
U S S Y E O O R I T A E E D S E
D P M O O C C F S Y T I Z A Z C
N P O S I O E L W I N E M N C I
A F C V T U N I S O R G I T E N
L U A T O N T I E F O L L E N C
I T A S G N O M C U E D T O T O
I A Q T S D S R I W F O R E O P
U C T R I E E S O T N P E E E O
B O I C A P S N O W D A Z T S R
T R I N T A E S E I S L E O E C
I C E Q T S S R N O L C N E T E
Q P U N A R S O D D P Y T T E N
U A N M E R E I E E A C O T N T
A D M V I N N R Z F A S S T T O
T D K E O S T R E I U N E E A C
O T L P M I A A N C T O Q R E S
R N D Q I T E O O I C B U M S I
Z A N C G O O S V E T Y A E E Z
E I N F S R I A E N O E T H T S
L N V K O E T T U T L Q R C E E
I S U W T H O V G E S M O C U H
Q U A T O R Z E T E R C O S T R

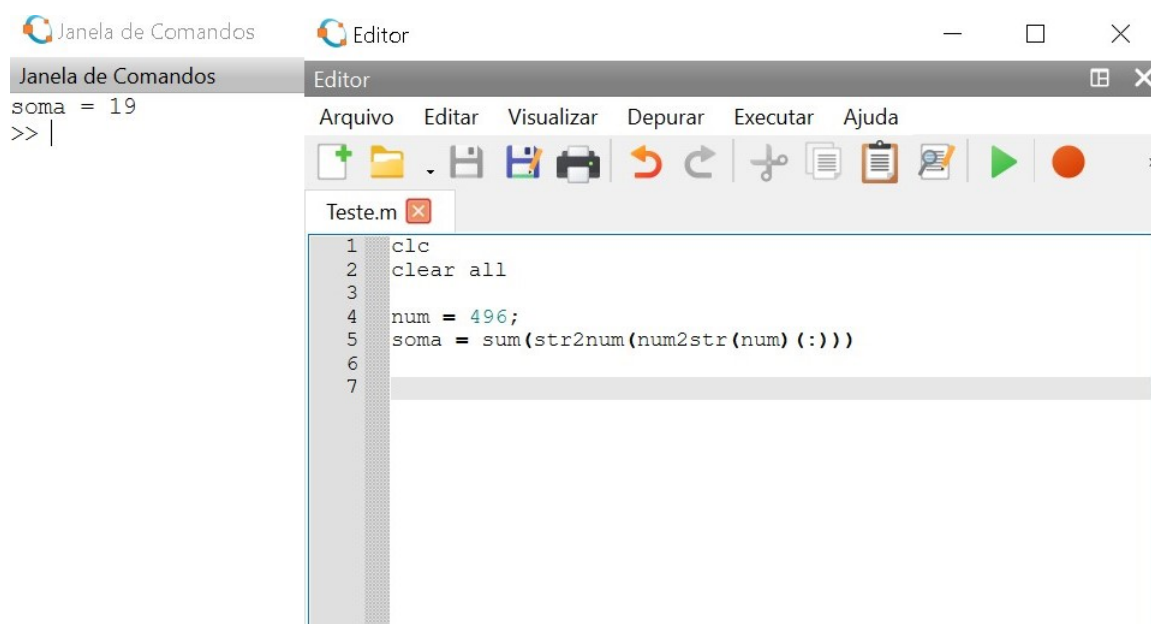
```

Fonte: Oh, My Dots (2025).

6. Qual é a soma dos algarismos do número perfeito 496?

A Figura 6.16 ilustra o script para a soma dos algarismos do número 496.

Figura 6.16 – Script para a soma dos algarismos do número 496



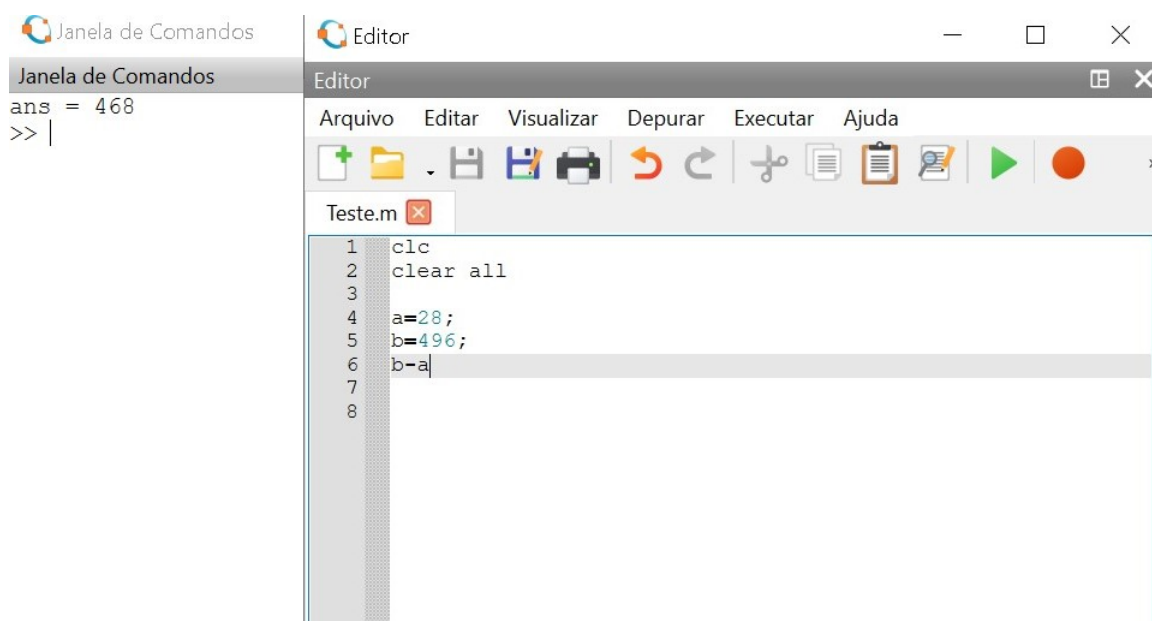
Fonte: Autora com o GNU Octave.

Logo, a soma dos algarismos do número 496 é 19.

7. *Qual é a diferença entre o terceiro e o segundo números perfeitos?*

A Figura 6.17 mostra o script no GNU Octave para determinar a diferença entre os números perfeitos.

Figura 6.17 – Script para calcular a diferença entre 496 e 28



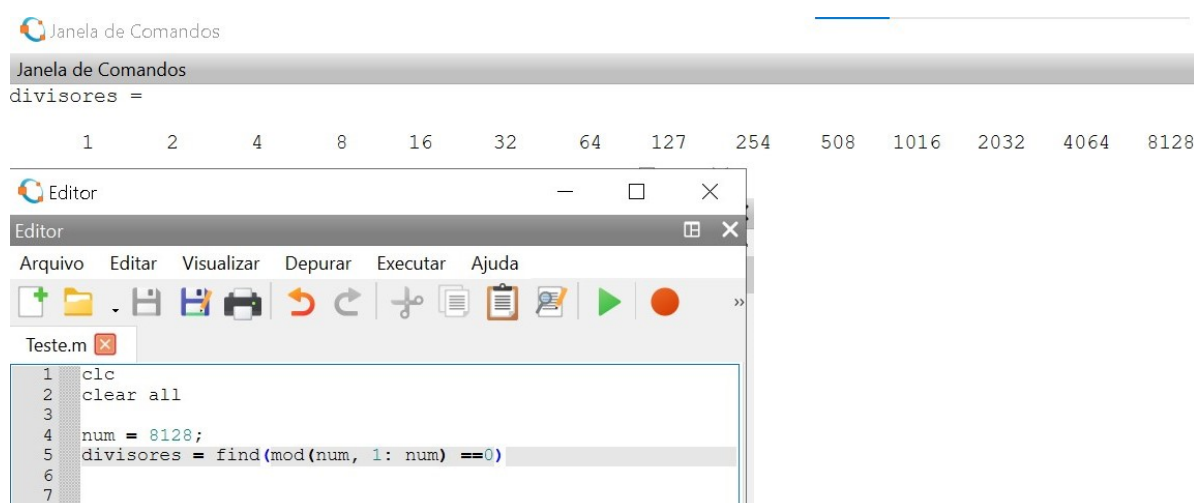
Fonte: Autora com o GNU Octave.

Assim, a diferença entre o terceiro e o segundo números perfeitos é 468.

8. *Quantos divisores possui o número perfeito 8128?*

A Figura 6.18 ilustra o script no GNU Octave para determinar o número de divisores de 8128.

Figura 6.18 – Script para obter os divisores do número 8128



Fonte: Autora com o GNU Octave.

Sobre os comandos utilizados, temos que:

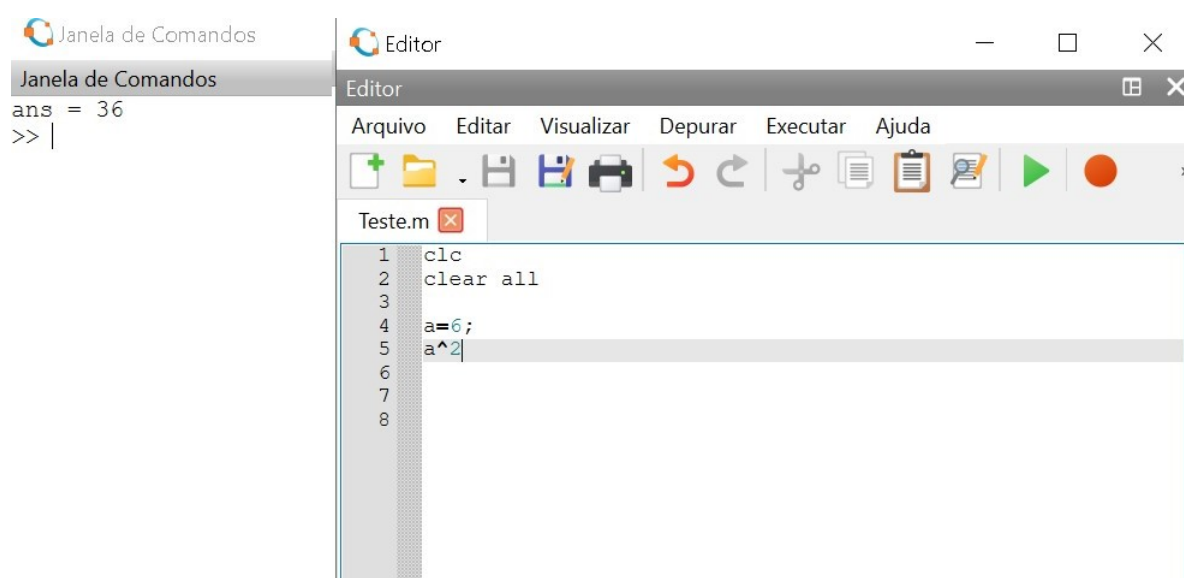
- i) $1:num$ – Gera uma sequência de números de 1 até num;
- ii) $mod(num, 1:num)$ – Calcula o resto da divisão do número num para cada número da sequência;
- iii) $find(... == 0)$ – Retorna os índices dos números que num divide sem deixar resto.

Portanto, o número 8128 possui 14 divisores.

9. Qual é o resultado de elevar o menor número perfeito ao quadrado?

A Figura 6.19 mostra o script no GNU Octave para elevar o número ao quadrado.

Figura 6.19 – Script para obter o resultado de 6 elevado ao quadrado



Fonte: Autora com o GNU Octave.

Logo, o resultado do quadrado do primeiro número perfeito é 36.

10. Qual é a fração irredutível que representa a razão entre o segundo e o primeiro números perfeitos?

A Figura 6.20 ilustra o script no GNU Octave para determinar a fração irredutível.

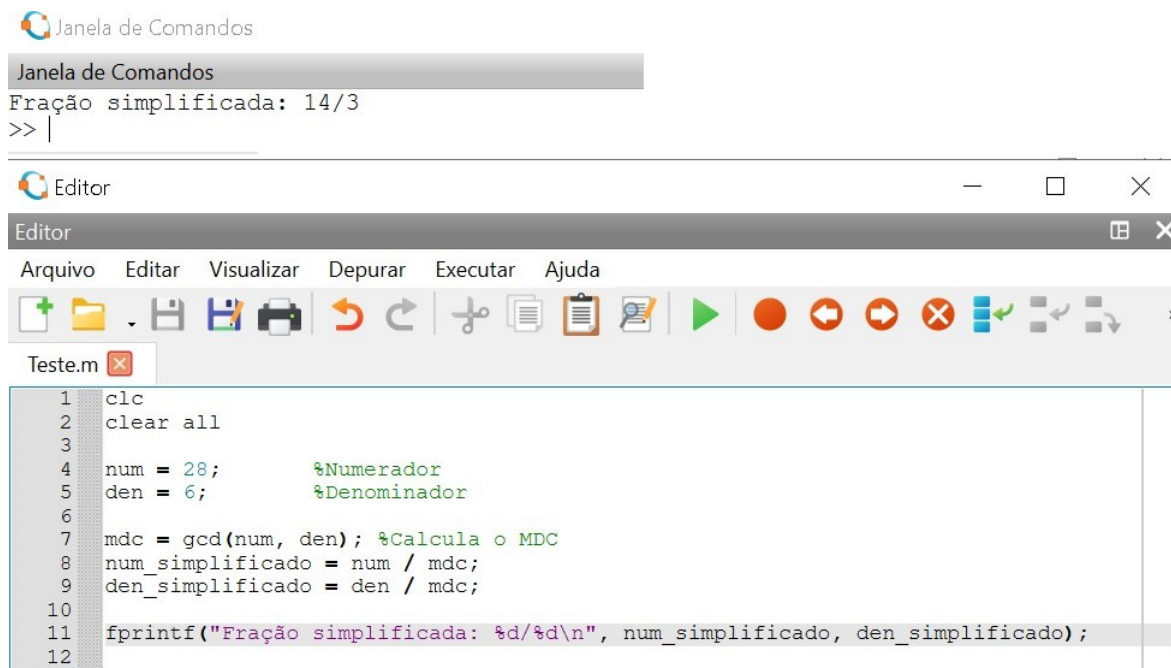
Com isso, temos que a fração irredutível entre o segundo e o primeiro números perfeitos é $\frac{14}{3}$.

11. Qual é a porcentagem que o divisor 7 representa do número perfeito 28?

A configuração do script no GNU Octave para determinar a porcentagem é ilustrada na Figura 6.21.

Desta forma, 7 representa 25% de 28.

Figura 6.20 – Script para obter a fração irredutível entre o segundo e o primeiro números perfeitos



The screenshot shows the GNU Octave environment. The 'Janela de Comandos' (Command Window) displays the output 'Fração simplificada: 14/3' and the prompt '>>'. The 'Editor' window shows a script named 'Teste.m' with the following code:

```

1 clc
2 clear all
3
4 num = 28;      %Numerador
5 den = 6;       %Denominador
6
7 mdc = gcd(num, den); %Calcula o MDC
8 num_simplificado = num / mdc;
9 den_simplificado = den / mdc;
10
11 fprintf("Fração simplificada: %d/%d\n", num_simplificado, den_simplificado);
12

```

Fonte: Autora com o GNU Octave.

Figura 6.21 – Script para calcular a porcentagem que o divisor 7 representa do número perfeito 28



The screenshot shows the GNU Octave environment. The 'Janela de Comandos' (Command Window) displays the output 'O número 7 representa 25.00% de 28' and the prompt '>>'. The 'Editor' window shows a script named 'Teste.m' with the following code:

```

1 clc
2 clear all
3
4 A = 7; %Número A
5 B = 28; %Número B
6
7 porcentagem = (A / B) * 100;
8 fprintf("O número %d representa %.2f%% de %d\n", A, porcentagem, B);
9

```

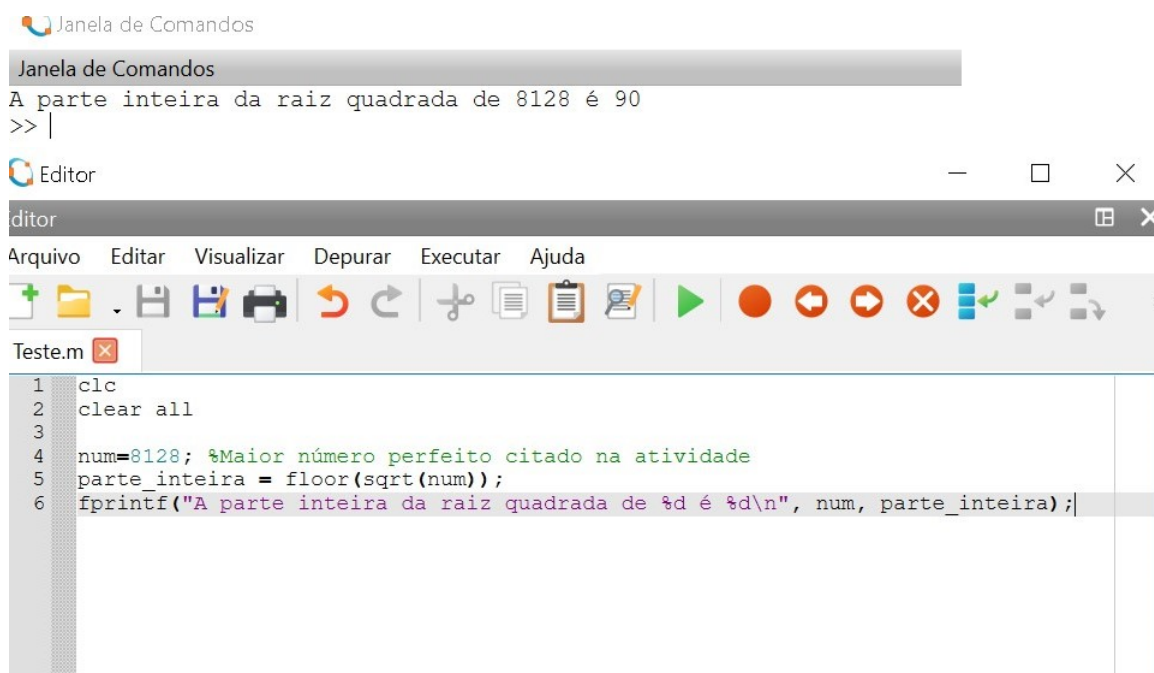
Fonte: Autora com o GNU Octave.

12. Qual é a parte inteira da raiz quadrada do maior número perfeito citado no Desafio 6.9?

A Figura 6.22 ilustra o script no GNU Octave para determinar a parte inteira da raiz quadrada de 8128.

Sobre os comandos utilizados, destacamos que:

Figura 6.22 – Script para calcular a parte inteira da raiz quadrada de 8128



Fonte: Autora com o GNU Octave.

i) $\text{sqrt}(\text{num})$ — Calcula a raiz quadrada do número;

ii) $\text{floor}(x)$ — Retorna a parte inteira de x , arredondando para baixo.

Portanto, a parte inteira da raiz quadrada de 8128 é 90.

13. Qual é a média aritmética aproximada dos três primeiros números perfeitos? Arredonde a média para o próximo número inteiro.

A Figura 6.23 mostra o script no GNU Octave para determinar a média aritmética de três valores.

Como a questão pede para arredondarmos para o próximo número inteiro, a média é 177.

14. Qual é a mediana dos divisores próprios do número perfeito 6?

A Figura 6.24 mostra o script no GNU Octave para calcular a mediana dos divisores próprios de um número perfeito.

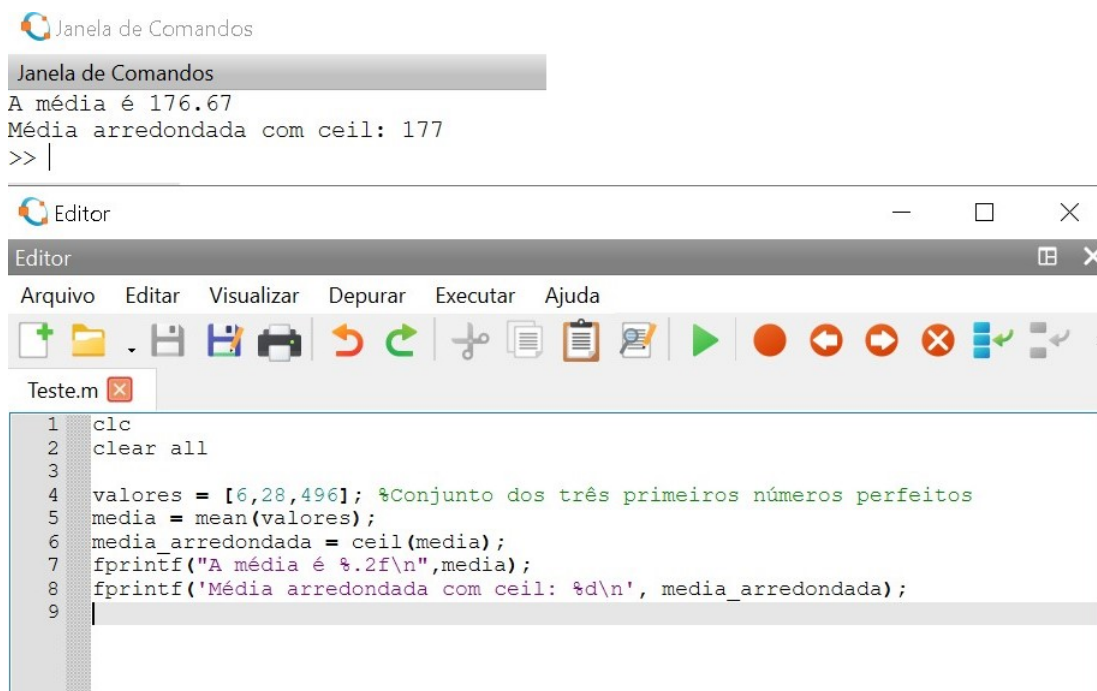
Logo, a mediana dos divisores próprios do número perfeito 6 é 2.

15. Considerando $A = 6$, $B = 28$, $C = 496$ e $D = 8128$, qual será o resultado da expressão: $D \cdot A^2 - (C^2 + B \cdot A^4)$?

A Figura 6.25 ilustra o script no GNU Octave para calcular o valor numérico da expressão algébrica.

Logo, o valor numérico da expressão $D \cdot A^2 - (C^2 + B \cdot A^4)$ é 10304.

Figura 6.23 – Script para calcular a média aritmética aproximada dos três primeiros números perfeitos



The screenshot shows the GNU Octave environment. The 'Janela de Comandos' (Command Window) displays the output: 'A média é 176.67' and 'Média arredondada com ceil: 177'. The 'Editor' window shows a script named 'Teste.m' with the following code:

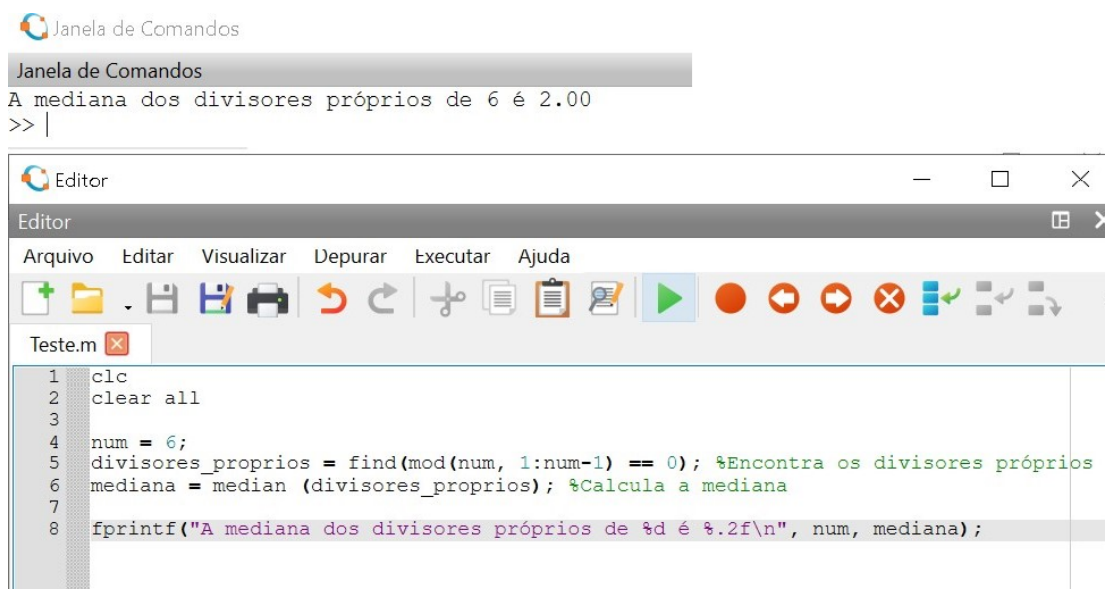
```

1 clc
2 clear all
3
4 valores = [6,28,496]; %Conjunto dos três primeiros números perfeitos
5 media = mean(valores);
6 media_arredondada = ceil(media);
7 fprintf("A média é %.2f\n",media);
8 fprintf('Média arredondada com ceil: %d\n', media_arredondada);
9

```

Fonte: Autora com o GNU Octave.

Figura 6.24 – Script para determinar a mediana dos divisores próprios do número perfeito 6



The screenshot shows the GNU Octave environment. The 'Janela de Comandos' (Command Window) displays the output: 'A mediana dos divisores próprios de 6 é 2.00'. The 'Editor' window shows a script named 'Teste.m' with the following code:

```

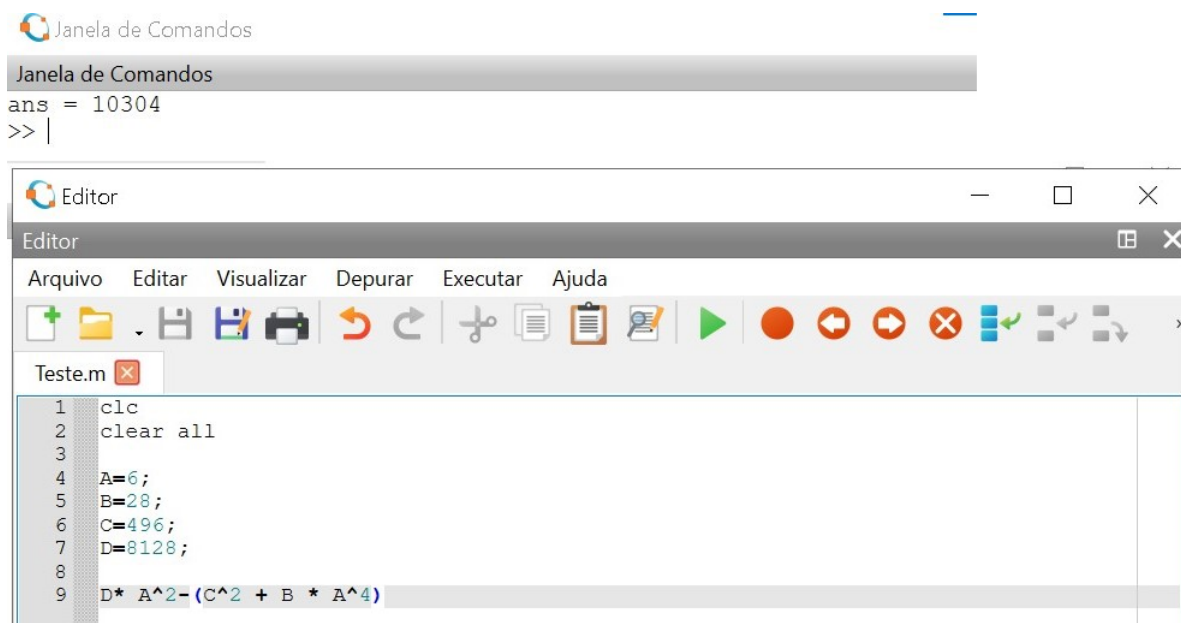
1 clc
2 clear all
3
4 num = 6;
5 divisores_proprios = find(mod(num, 1:num-1) == 0); %Encontra os divisores próprios
6 mediana = median (divisores_proprios); %Calcula a mediana
7
8 fprintf("A mediana dos divisores próprios de %d é %.2f\n", num, mediana);
9

```

Fonte: Autora com o GNU Octave.

Após responder a todas as questões propostas, devemos localizar as respostas correspondentes no caça-palavras da Figura 6.15. O caça-palavras utilizado para o desenvolvimento desta sequência didática foi elaborado por meio da ferramenta disponível no site <<https://pt.ohmydots.com/creator-crossword.html>>, que permite a criação personalizada de atividades desse tipo de forma simples e acessível. A Figura 6.26 ilustra a conclusão do Desafio 6.9.

Figura 6.25 – Script para calcular o valor numérico da expressão com números perfeitos



Fonte: Autora com o GNU Octave.

Figura 6.26 – Respostas do Desafio 6.9 no caça-palavras



Fonte: Autora.

6.4 ATIVIDADE 4: INVESTIGANDO NÚMEROS PRIMOS EM PROGRESSÕES ARITMÉTICAS

1.1 Nível: Ensino Médio.

1.2 Ano: 1º.

1.3 Número de aulas: 3 (45 minutos cada).

1.4 Competências específicas BNCC:

- Utilizar estratégias, conceitos e procedimentos matemáticos, em seus campos – Aritmética, Álgebra, Grandezas e Medidas, Geometria, Probabilidade e Estatística – para interpretar, construir modelos e resolver problemas em diversos contextos, analisando a plausibilidade dos resultados e a adequação das soluções propostas, de modo a construir argumentação consistente;
- Compreender e utilizar, com flexibilidade e fluidez, diferentes registros de representação matemáticos (algébrico, geométrico, estatístico, computacional), na busca de solução e comunicação de resultados de problemas, de modo a favorecer a construção e o desenvolvimento do raciocínio matemático;
- Investigar e estabelecer conjecturas a respeito de diferentes conceitos e propriedades matemáticas, empregando recursos e estratégias como observação de padrões, experimentações e tecnologias digitais, identificando a necessidade, ou não, de uma demonstração cada vez mais formal na validação das referidas conjecturas.

1.5 Habilidades específicas BNCC:

(EM13MAT303) Resolver e elaborar problemas envolvendo porcentagens em diversos contextos e sobre juros compostos, destacando o crescimento exponencial;

(EM13MAT406) Utilizar os conceitos básicos de uma linguagem de programação na implementação de algoritmos escritos em linguagem corrente e/ou matemática;

(EM13MAT507) Identificar e associar sequências numéricas (PA) a funções afins de domínios discretos para análise de propriedades, incluindo dedução de algumas fórmulas e resolução de problemas.

1.6 Conteúdos abordados: progressões aritméticas; números primos; porcentagem.

1.7 Objetivos:

- Identificar padrões em sequências numéricas simples e resolver problemas básicos;
- Desenvolver habilidades computacionais;
- Compreender a natureza dos números primos;
- Desenvolver o raciocínio lógico e investigativo.

1.8 Procedimento metodológico: aula expositiva e dialogada; solução de problemas.

1.9 Avaliação: observação do desempenho dos estudantes durante a realização da atividade.

Os números primos são um dos temas mais fascinantes da Matemática. Eles aparecem de forma inesperada e estão ligados a diversos ramos do conhecimento, como a criptografia e a segurança digital. Além disso, os números primos também podem ser encontrados em progressões aritméticas, ou seja, em sequências numéricas nas quais a diferença entre dois termos consecutivos é sempre a mesma.

Nesta atividade, você será desafiado – Desafios 6.10 e 6.11 – a investigar como os números primos aparecem em diferentes progressões aritméticas. Será que existe algum padrão? Será que podemos prever onde encontrar números primos? Vamos descobrir juntos por meio de uma investigação prática e divertida que vai estimular o seu raciocínio lógico e investigativo!

Desafio 6.10. *Consideremos cinco progressões aritméticas representadas por sequências numéricas $(a_n)_{n \in \mathbb{N}}$ definidas recursivamente por:*

$$\text{Sequência 1 } a_n = 2 + (n - 1) \cdot 3, n > 1; \quad (6.1)$$

$$\text{Sequência 2 } a_n = 3 + (n - 1) \cdot 2, n > 1; \quad (6.2)$$

$$\text{Sequência 3 } a_n = 4 + (n - 1) \cdot 7, n > 1; \quad (6.3)$$

$$\text{Sequência 4 } a_n = 7 + (n - 1) \cdot 3, n > 1; \quad (6.4)$$

$$\text{Sequência 5 } a_n = 11 + (n - 1) \cdot 2, n > 1. \quad (6.5)$$

Para cada uma das sequências (6.1) a (6.5):

1. gere os 20 primeiros termos usando os controles deslizantes na página do GeoGebra <<https://www.geogebra.org/m/crk44j3f>>;
2. classifique cada termo como primo ou composto utilizando no GNU Octave a função `isprime`, que retorna o valor 1 quando o número é primo e 0 quando é composto;
3. conte quantos números primos cada uma das sequências obtidas possuiu e em seguida determine, usando a função `percent` no GNU Octave, a porcentagem de números primos entre os 20 primeiros termos de cada sequência.

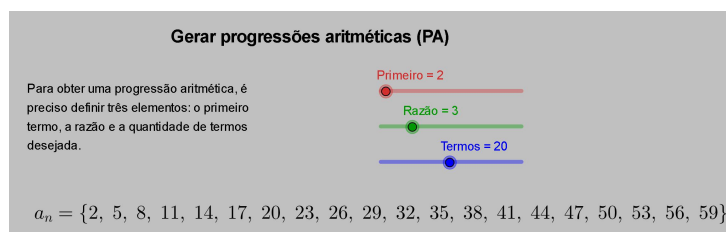
Para as sequências (6.1) e (6.2):

4. expanda cada sequência adicionando mais 5 termos, e depois mais 5 termos. Para cada conjunto de (20, 25, 30) termos, determine empregando o GNU Octave:
 - a quantidade de números primos;
 - a porcentagem de números primos em relação ao total de termos.

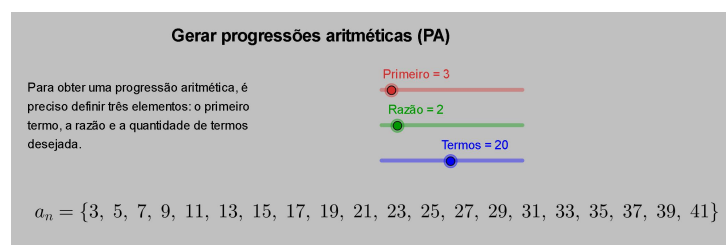
À medida que aumentamos o intervalo, a quantidade e a porcentagem de números primos tendem a aumentar, diminuir ou se manter constantes?

Solução 6.10. (Desafio 6.10) Clicamos no link disponibilizado e geramos os 20 primeiros termos de cada sequência. As Figuras 6.28 a 6.32 ilustram os termos obtidos em cada sequência.

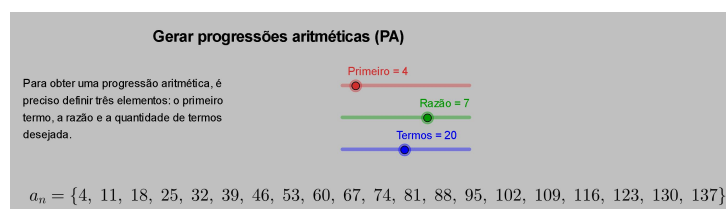
Figura 6.27 – Progressões aritméticas com 20 termos: (a) $a_n = 2 + (n - 1) \cdot 3$; (b) $a_n = 3 + (n - 1) \cdot 2$; (c) $a_n = 4 + (n - 1) \cdot 7$; (d) $a_n = 7 + (n - 1) \cdot 3$; (e) $a_n = 11 + (n - 1) \cdot 2$



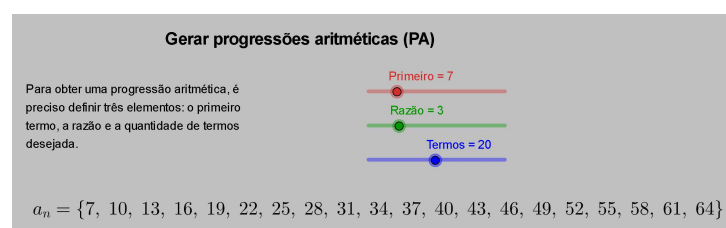
(a)



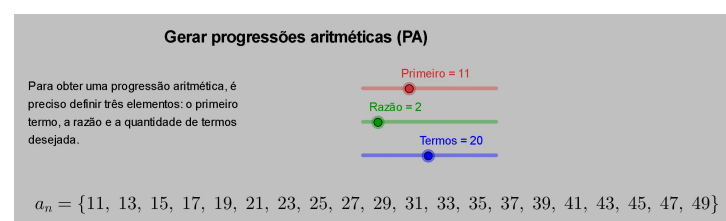
(b)



(c)



(d)



(e)

Fonte: Autora com o GeoGebra.

Em seguida, analisamos cada termo das sequências para determinar se ele é um número primo ou composto. Para isso, utilizamos a função `isprime` no GNU Octave. Essa função retorna o valor 1 quando o número é primo e 0 quando é composto. Dessa forma, obtemos uma sequência de zeros e uns que indica a primalidade de cada termo. As Figuras 6.28 a 6.32 mostram o comando usado no GNU Octave e os resultados correspondentes.

Figura 6.28 – Primalidade dos 20 primeiros termos da PA $a_n = 2 + (n - 1) \cdot 3$

The screenshot shows the GNU Octave environment. The 'Janela de Comandos' (Command Window) displays the result of the `isprime` function applied to the first 20 terms of the arithmetic progression $a_n = 2 + (n - 1) \cdot 3$. The output is a row vector of 20 elements: 1 1 0 1 0 1 0 1 0 1 0 0 0 1 0 1 0 1 0 1. The 'Editor' window shows the script 'Teste.m' with the following code:

```
1 clc
2 clear all
3
4 numeros = [2,5,8,11,14,17,20,23,26,29,32,35,38,41,44,47,50,53,56,59];
5 primo = isprime (numeros)
```

Fonte: Autora com o GNU Octave.

Figura 6.29 – Primalidade dos 20 primeiros termos da PA $a_n = 3 + (n - 1) \cdot 2$

The screenshot shows the GNU Octave environment. The 'Janela de Comandos' (Command Window) displays the result of the `isprime` function applied to the first 20 terms of the arithmetic progression $a_n = 3 + (n - 1) \cdot 2$. The output is a row vector of 20 elements: 1 1 1 0 1 1 0 1 1 0 1 0 0 1 1 0 0 1 0 1. The 'Editor' window shows the script 'Teste.m' with the following code:

```
1 clc
2 clear all
3
4 numeros = [3,5,7,9,11,13,15,17,19,21,23,25,27,29,31,33,35,37,39,41];
5 primo = isprime (numeros)
```

Fonte: Autora com o GNU Octave.

Figura 6.30 – Primalidade dos 20 primeiros termos da PA $a_n = 4 + (n - 1) \cdot 7$

Janela de Comandos

```
primo =
```

```
0 1 0 0 0 0 0 1 0 1 0 0 0 0 0 1 0 0 0 1
```

Editor

Arquivo Editar Visualizar Depurar Executar Ajuda

Teste.m

```
1 clc
2 clear all
3
4 numeros = [4,11,18,25,32,39,46,53,60,67,74,81,88,95,102,109,116,123,130,137];
5 primo = isprime (numeros)
```

Fonte: Autora com o GNU Octave.

Figura 6.31 – Primalidade dos 20 primeiros termos da PA $a_n = 7 + (n - 1) \cdot 3$

Janela de Comandos

```
primo =
```

```
1 0 1 0 1 0 0 0 1 0 1 0 1 0 0 0 0 0 1 0
```

Editor

Arquivo Editar Visualizar Depurar Executar Ajuda

Teste.m

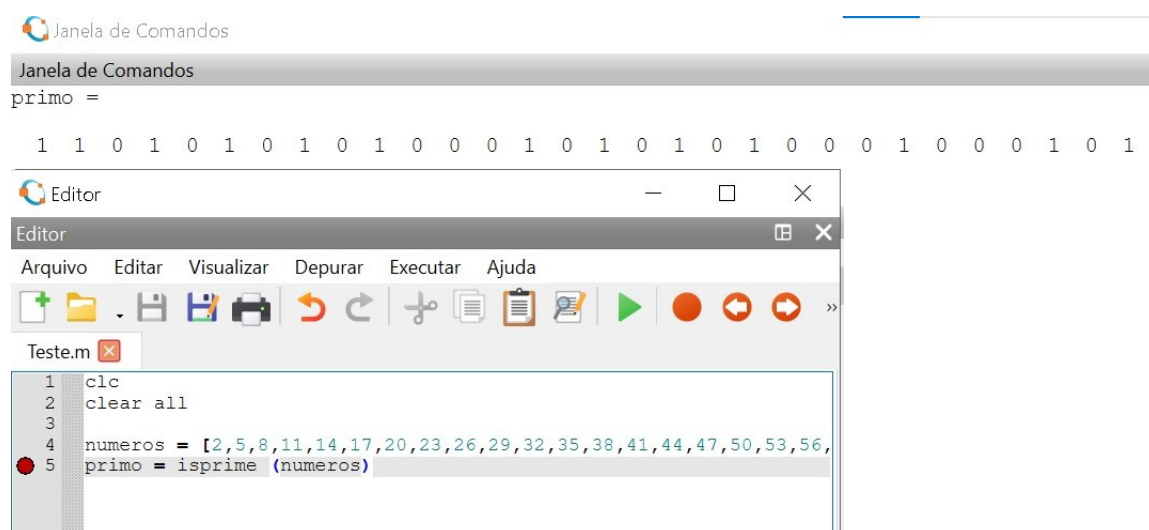
```
1 clc
2 clear all
3
4 numeros = [7,10,13,16,19,22,25,28,31,34,37,40,43,46,49,52,55,58,61,64];
5 primo = isprime (numeros)
```

Fonte: Autora com o GNU Octave.

As Figuras 6.28 a 6.32 evidenciam que o número de primos nos 20 primeiros termos das progressões aritméticas $a_n = 2 + (n - 1) \cdot 3$, $a_n = 3 + (n - 1) \cdot 2$, $a_n = 4 + (n - 1) \cdot 7$, $a_n = 7 + (n - 1) \cdot 3$ e $a_n = 11 + (n - 1) \cdot 2$ é, respectivamente: 10 – 50%; 12 – 60%; 5 – 25%; 7 – 35%; 11 – 55%. A porcentagem de números primos nos 20 primeiros termos de cada PA é calculada com o GNU Octave seguindo os passos ilustrados na Figura 6.33.

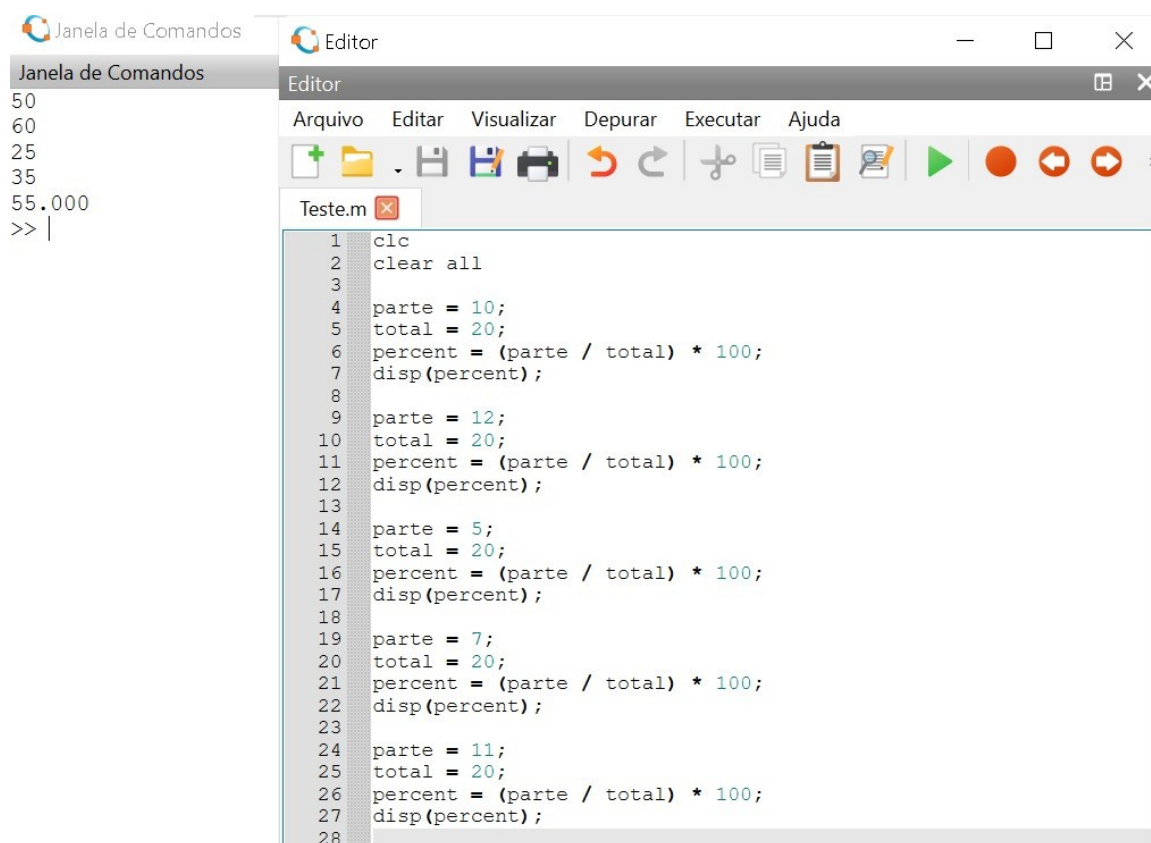
Para investigar a distribuição dos números primos, analisemos as progressões aritméticas definidas por $a_n = 2 + (n - 1) \cdot 3$ e $a_n = 3 + (n - 1) \cdot 2$ considerando um número maior de

Figura 6.32 – Primalidade dos 20 primeiros termos da PA $a_n = 2 + (n - 1) \cdot 3$



Fonte: Autora com o GNU Octave.

Figura 6.33 – Porcentagem de números primos nos 20 primeiros termos das progressões aritméticas do Desafio 6.10

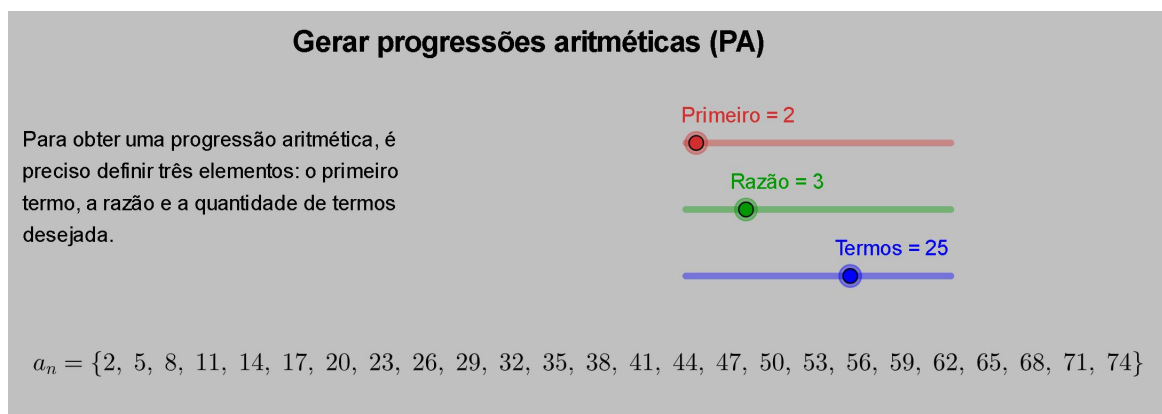


Fonte: Autora com o GNU Octave.

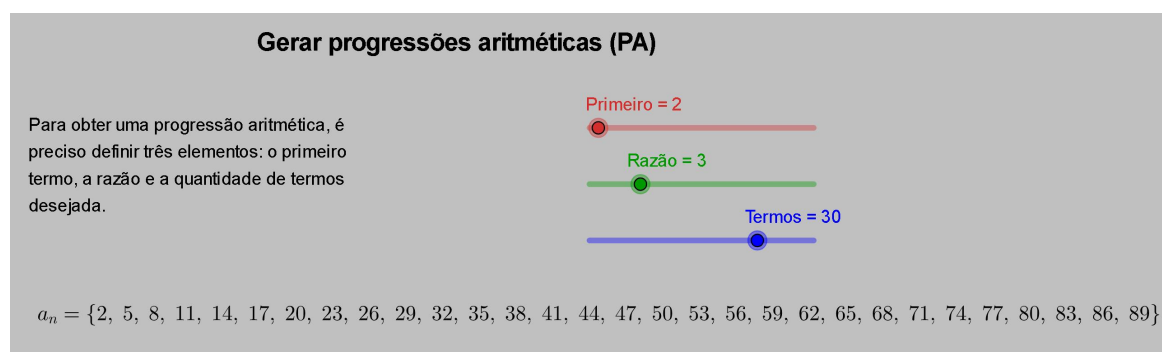
termos: 25 e 30 para ambas as progressões.

Iniciemos com a PA $a_n = 2 + (n - 1) \cdot 3$. A Figura 6.34 ilustra os termos da PA, as Figuras 6.35 e 6.36 mostram a primalidade dos elementos e a Figura 6.37 apresenta a porcentagem de primos na quantidade de termos considerada.

Figura 6.34 – PA $a_n = 2 + (n - 1) \cdot 3$: (a) 25 primeiros termos; (b) 30 primeiros termos



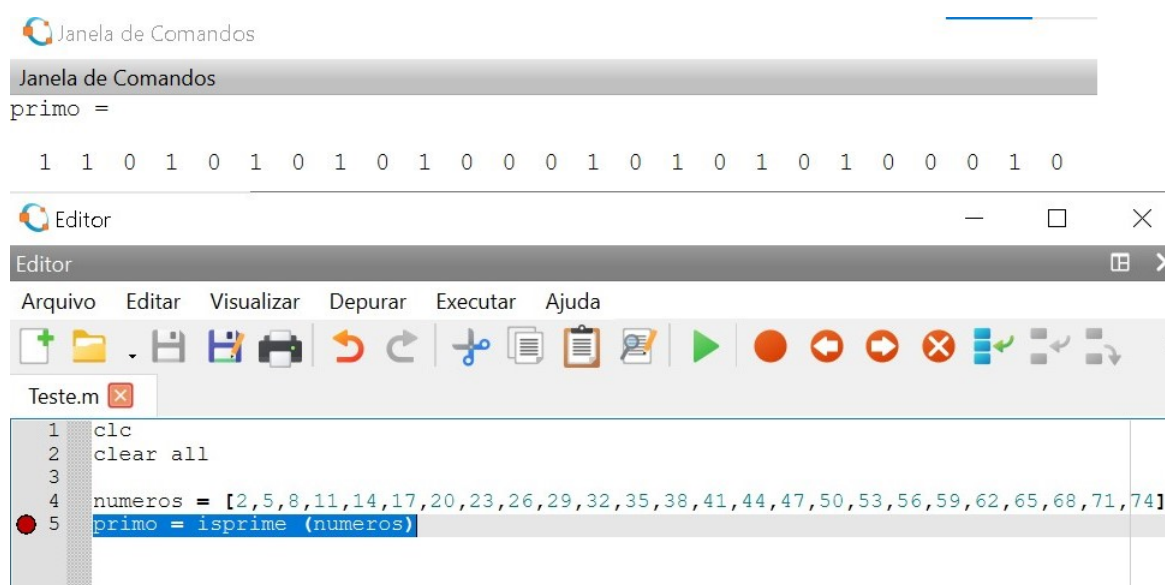
(a)



(b)

Fonte: Autora com o GeoGebra.

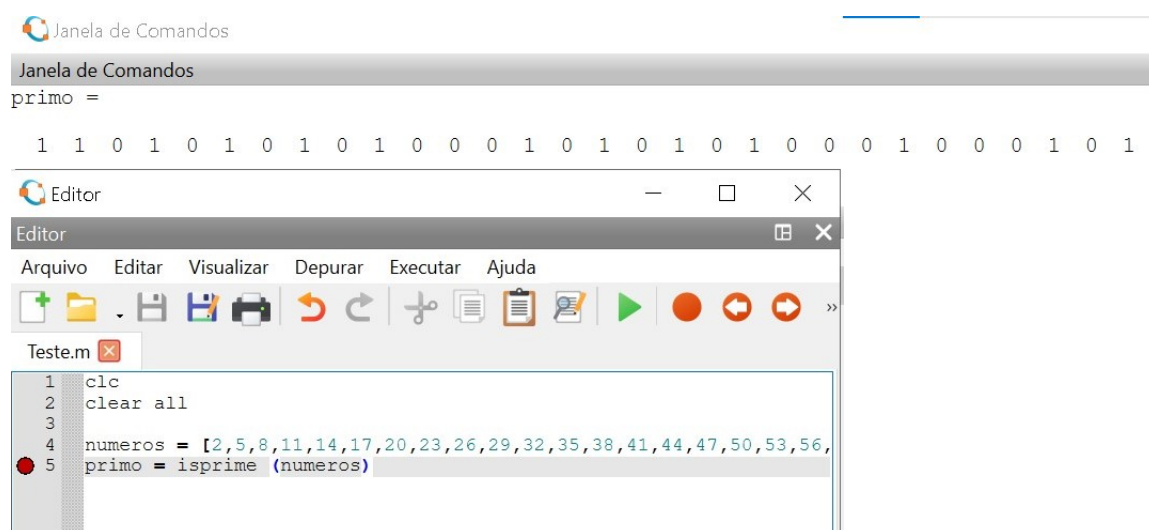
Figura 6.35 – Primalidade dos 25 primeiros termos da PA $a_n = 2 + (n - 1) \cdot 3$



Fonte: Autora com o GNU Octave.

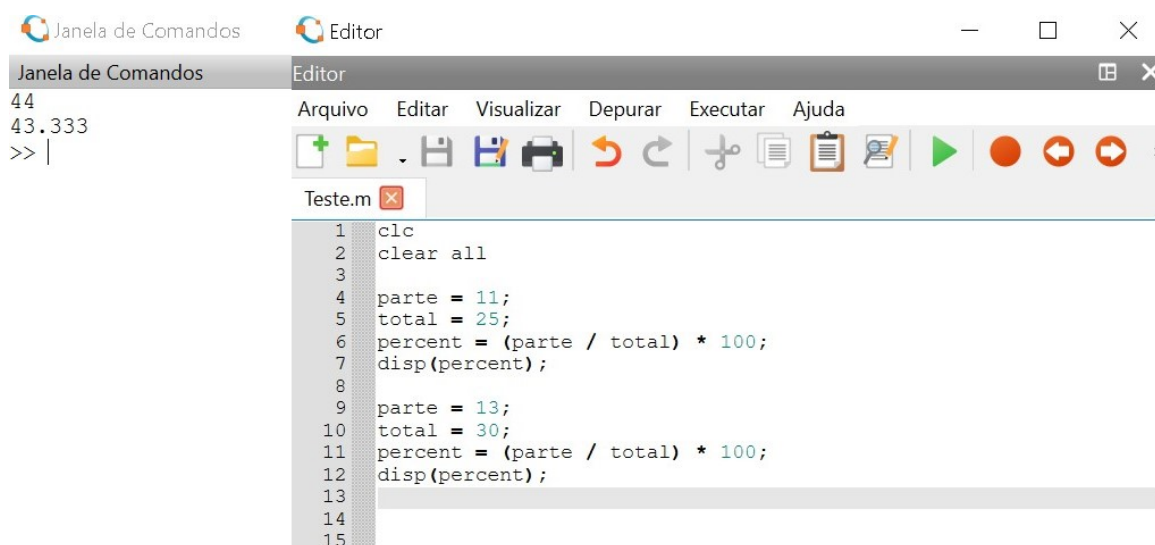
Usando o GNU Octave, comprovamos – Figuras 6.35, 6.36 e 6.37 – que há na PA $a_n = 2 + (n - 1) \cdot 3$: 11 números primos entre os 25 primeiros termos, o que corresponde a 44%; 13 números primos entre os 30 primeiro termos, o que corresponde a 43,33%.

Figura 6.36 – Primalidade dos 30 primeiros termos da PA $a_n = 2 + (n - 1) \cdot 3$



Fonte: Autora com o GNU Octave.

Figura 6.37 – Porcentagem de números primos nos 25 e 30 primeiros termos da PA $a_n = 2 + (n - 1) \cdot 3$



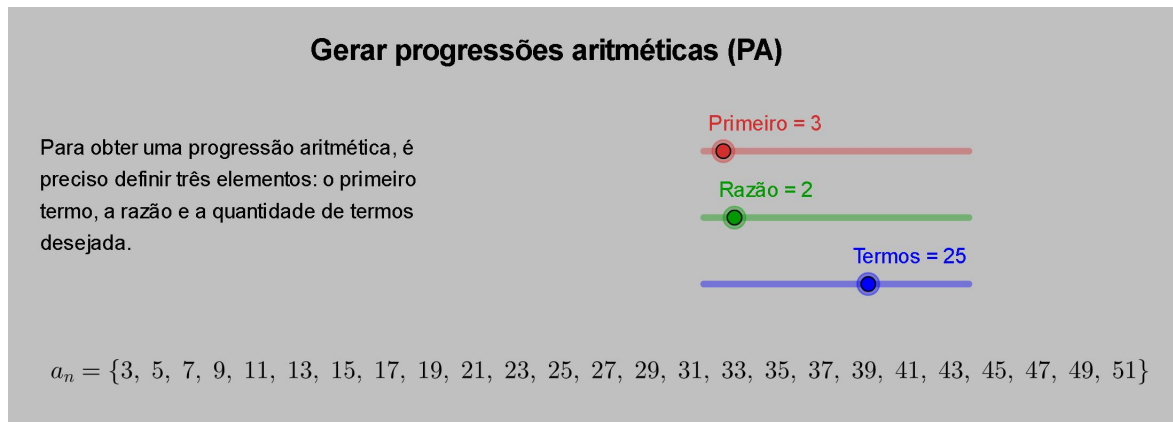
Fonte: Autora com GNU Octave.

Repetindo a análise para a PA $a_n = 3 + (n - 1) \cdot 2$, constatamos – Figuras 6.38, 6.39, 6.40 e 6.41 – que há: 14 números primos entre os 25 primeiros termos, o que corresponde a 56%; 17 números primos entre os 30 primeiros termos, o que corresponde a 56,67%.

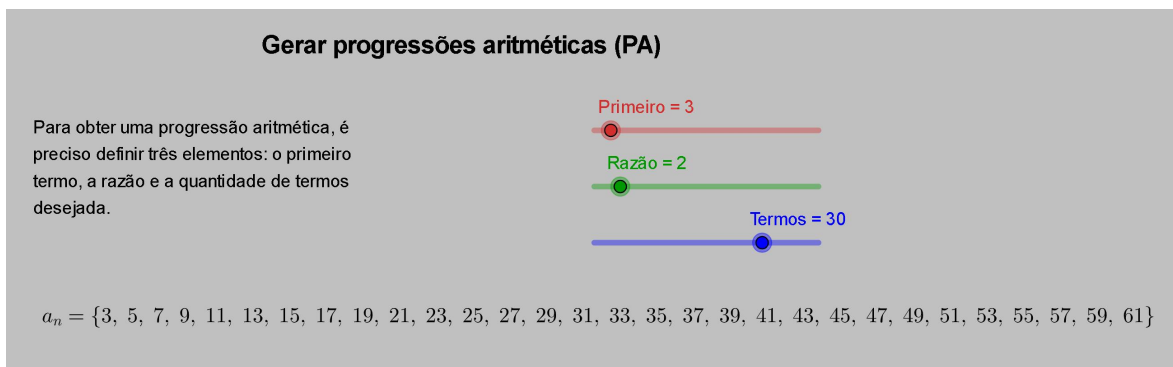
Analisando a distribuição de primos na expansão do número de termos das progressões aritméticas $a_n = 2 + (n - 1) \cdot 3$ e $a_n = 3 + (n - 1) \cdot 2$, constatamos duas tendências aparentemente contraditórias, porém coerentes com a literatura.

1. *Aumento da quantidade: à medida que consideramos intervalos com maior número de elementos nas progressões aritméticas, a quantidade total de números primos tende a aumentar.*

Figura 6.38 – Progressão aritmética $a_n = 3 + (n - 1) \cdot 2$: (a) 25 primeiros termos; (b) 30 primeiros termos



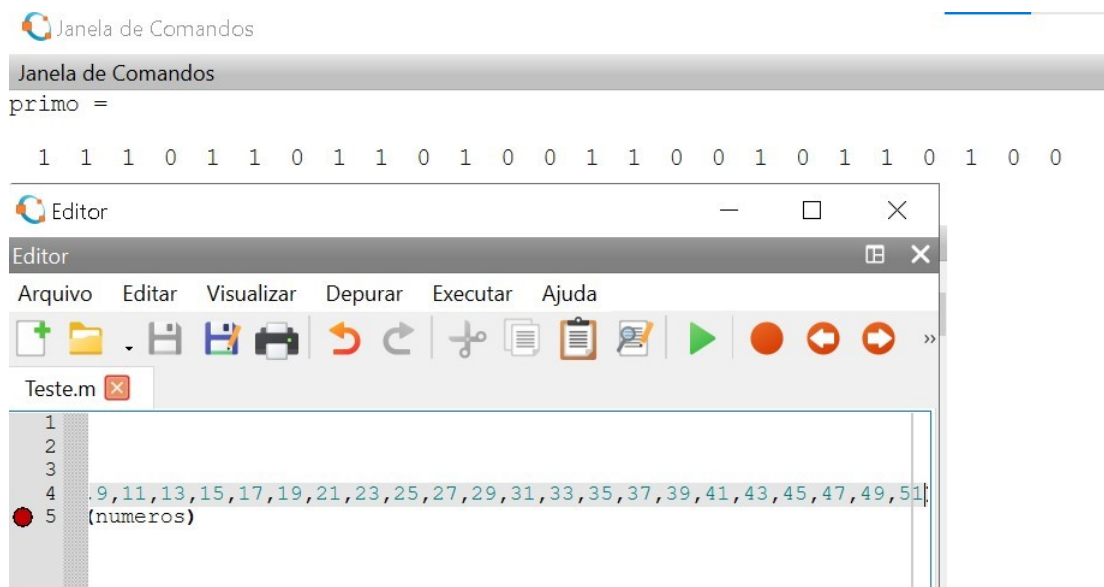
(a)



(b)

Fonte: Autora com o GeoGebra.

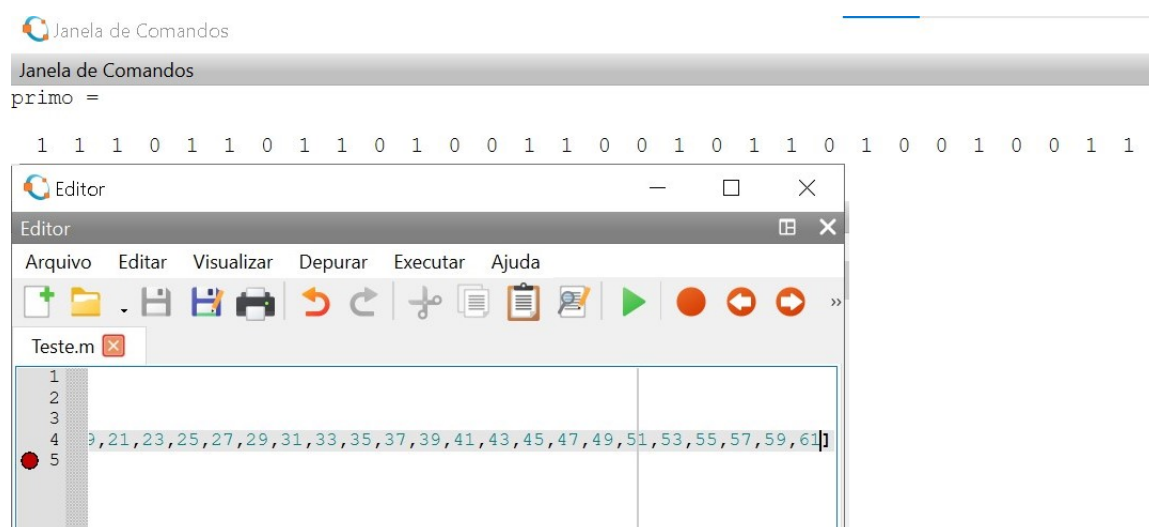
Figura 6.39 – Primalidade dos 25 primeiros termos da PA $a_n = 3 + (n - 1) \cdot 2$



Fonte: Autora com o GNU Octave

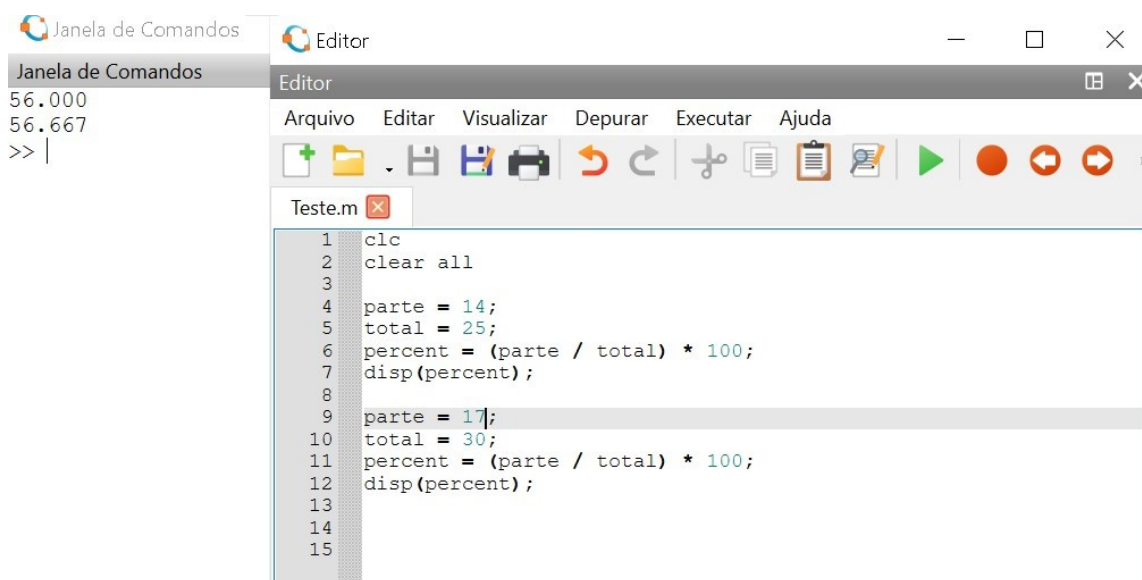
2. *Primos mais distantes: a proporção de números primos em relação ao total de números no*

Figura 6.40 – Primalidade dos 30 primeiros termos da PA $a_n = 3 + (n - 1) \cdot 2$



Fonte: Autora com o GNU Octave

Figura 6.41 – Porcentagem de números primos nos 25 e 30 primeiros termos da PA $a_n = 3 + (n - 1) \cdot 2$



Fonte: Autora com o GNU Octave.

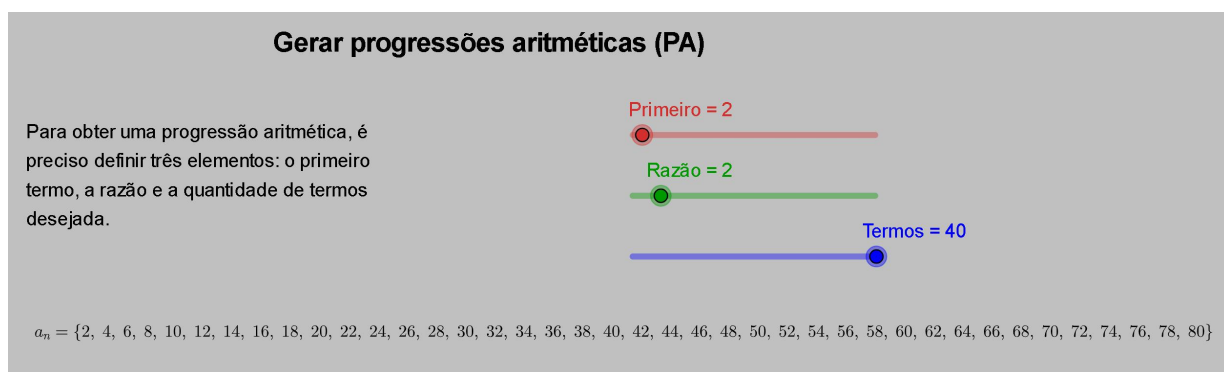
intervalo tende a diminuir.

Isso significa que, embora haja mais números primos em intervalos de maior amplitude, eles se tornam mais esparsos.

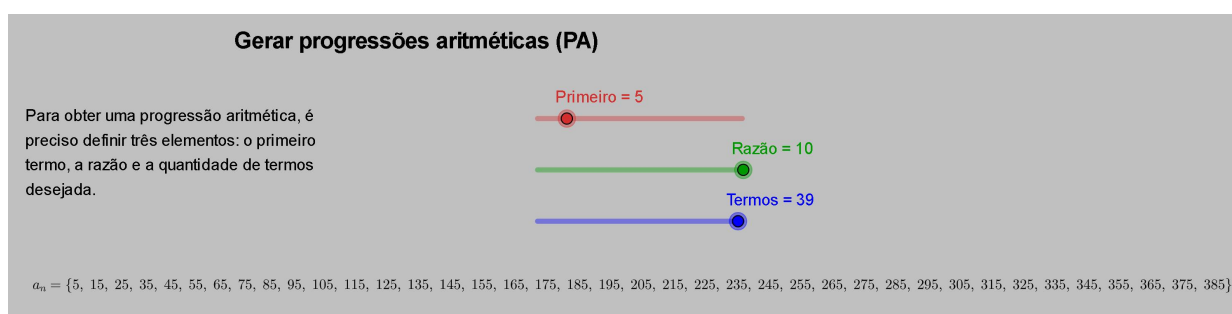
Desafio 6.11. *Empregando os controles deslizantes na página do GeoGebra <<https://www.geogebra.org/m/crk44j3f>>, escreva uma progressão aritmética com no máximo um número primo.*

Solução 6.11. *(Desafio 6.11) O Desafio 6.11 tem diversas soluções. A Figura 6.42 ilustra duas soluções possíveis.*

Figura 6.42 – Progressões aritméticas com um único número primo: (a) $a_n = 2 + (n - 1) \cdot 2$, $n > 1$; (b) $a_n = 5 + (n - 1) \cdot 10$, $n > 1$



(a)



(b)

Fonte: Autora com o GNU Octave.

Dirichlet fez uma descoberta fascinante sobre os números primos: em muitas sequências de números que seguem um padrão específico, podemos encontrar infinitos números primos. Essa descoberta é chamada de teorema de Dirichlet.

Mas qual é esse padrão específico? Para que uma sequência tenha infinitos números primos, de acordo com o teorema de Dirichlet, o primeiro número da sequência e a diferença entre cada número, chamada de razão, precisam ser primos entre si, ou seja, não podem ter nenhum divisor comum além do 1. No entanto, a forma como esses números primos se distribuem é um verdadeiro mistério. Ainda não é possível prever exatamente onde o próximo número primo vai aparecer.

6.5 ATIVIDADE 5: DESCOBRINDO OS PARES AMIGÁVEIS

1.1 Nível: Ensino Fundamental.

1.2 Ano: 7º.

1.3 Número de aulas: 4 (45 minutos cada).

1.4 Competências específicas BNCC:

- Compreender as relações entre conceitos e procedimentos dos diferentes campos da Matemática (Aritmética, Álgebra, Geometria, Estatística e Probabilidade) e de outras áreas do conhecimento, sentindo segurança quanto à própria capacidade de construir e aplicar conhecimentos matemáticos, desenvolvendo a autoestima e a perseverança na busca de soluções;
- Utilizar processos e ferramentas matemáticas, inclusive tecnologias digitais disponíveis, para modelar e resolver problemas cotidianos, sociais e de outras áreas de conhecimento, validando estratégias e resultados.

1.5 Habilidades específicas BNCC:

(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.

1.6 Conteúdos abordados: Múltiplos e divisores de um número natural; números amigáveis.

1.7 Objetivos:

- Compreender conceitos de divisibilidade;
- Compreender o conceito de números amigáveis;
- Desenvolver habilidades de programação;
- Desenvolver o raciocínio lógico e investigativo.

1.8 Procedimento metodológico: aula expositiva e dialogada; solução de problemas.

1.9 Avaliação: observação do desempenho dos estudantes durante a realização da atividade.

Você já se perguntou se os números podem ser amigos? Nesta atividade - Desafio 6.12, você vai explorar os números amigáveis, pares de números que possuem uma relação muito especial: a soma dos divisores próprios de um número é igual ao outro.

Desafio 6.12. *A Tabela 6.2 apresenta 20 números inteiros positivos. Utilizando as funções `find` e `sum` no GNU Octave, determine se cada um desses números compõe um par de números amigáveis. Para tanto, determine os divisores próprios, calcule a soma dos divisores próprios e compare as somas com os números da Tabela 6.2.*

O GNU Octave será sua ferramenta para simplificar e acelerar o trabalho, permitindo explorar não apenas pequenos números, mas também pares amigáveis maiores e mais complexos. Vamos investigar juntas essas relações numéricas e descobrir se os números realmente podem fazer amigos!

Quais são os pares de números amigáveis na Tabela 6.2?

Tabela 6.2 – Lista de números para o Desafio 6.12

NÚMERO	DIVISORES PRÓPRIOS	SOMA DOS DIVISORES PRÓPRIOS	AMIGO?
6			
12			
30			
220			
284			
399			
825			
1184			
1210			
2620			
2727			
2924			
3563			
4727			
5020			
5564			
5847			
6232			
6300			
6368			

Fonte: Autora.

Solução 6.12. (Desafio 6.12) Para configurar o script no GNU Octave, basta digitar $num = e$ digitar o valor desejado. Em seguida, usamos o comando

$$divisores_propios = find(mod(num, 1 : num - 1) == 0).$$

Este comando terá como saída os divisores próprios do número informado. Para obter a soma dos divisores próprios, basta acrescentar o comando

$$soma = sum(divisores_propios).$$

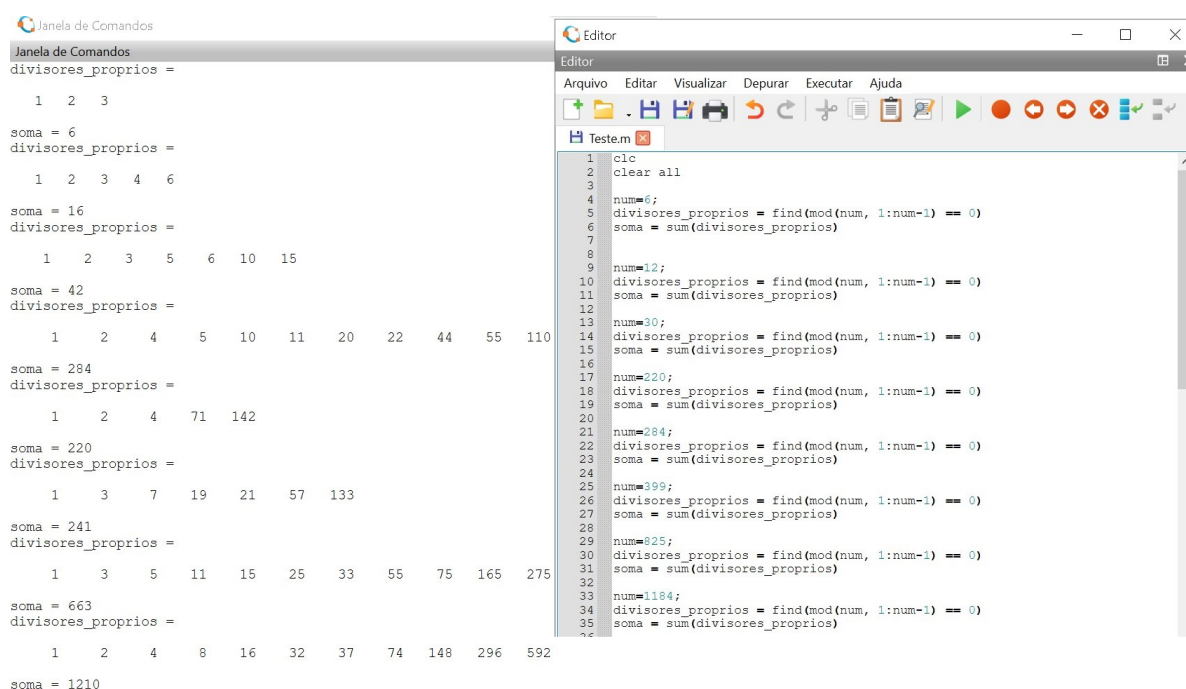
As Figuras 6.43 a 6.45 ilustram a configuração desses comandos para calcular a soma dos divisores próprios dos números relacionados na Tabela 6.2.

Após determinar todos os divisores próprios dos números na Tabela 6.2 e calcular suas somas, obtemos a Tabela 6.3.

Logo, os pares de números amigáveis na Tabela 6.2 são:

$$(220, 284), (1184, 1210), (2620, 2924), (5020, 5564), (6232, 6368).$$

Figura 6.43 – Script para somar os divisores próprios de 6 a 1184 na Tabela 6.2



Janela de Comandos

```
divisores_proprios =
1 2 3

soma = 6
divisores_proprios =
1 2 3 4 6

soma = 16
divisores_proprios =
1 2 3 5 6 10 15

soma = 42
divisores_proprios =
1 2 4 5 10 11 20 22 44 55 110

soma = 284
divisores_proprios =
1 2 4 71 142

soma = 220
divisores_proprios =
1 3 7 19 21 57 133

soma = 241
divisores_proprios =
1 3 5 11 15 25 33 55 75 165 275

soma = 663
divisores_proprios =
1 2 4 8 16 32 37 74 148 296 592

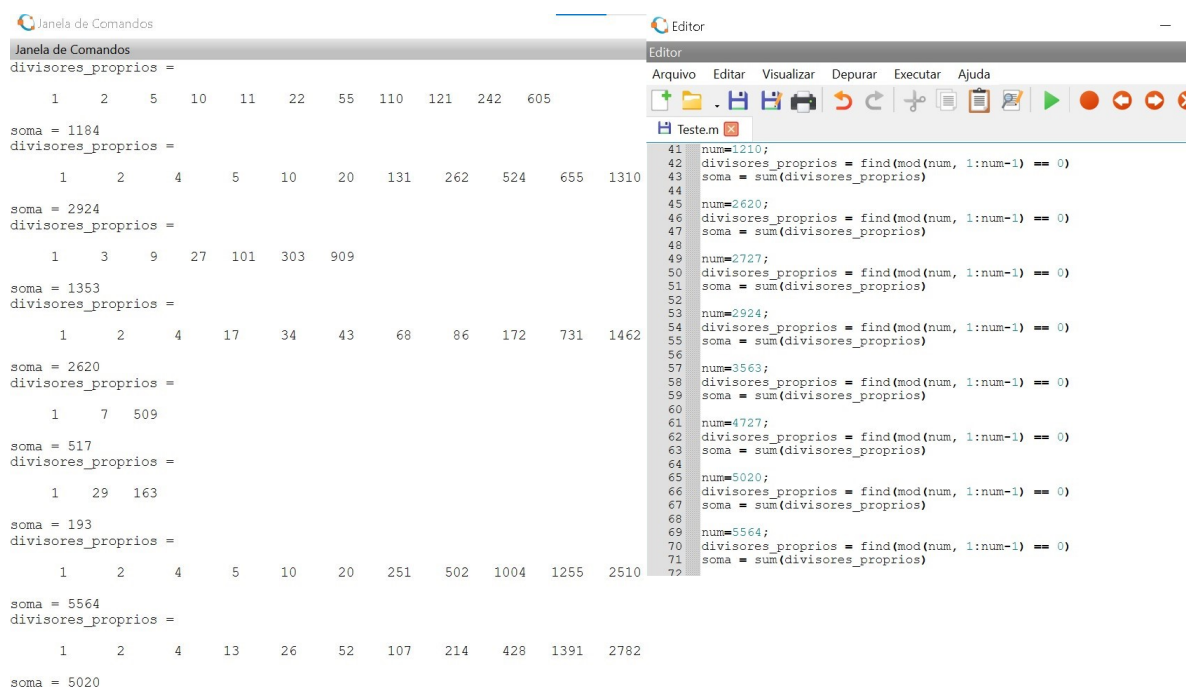
soma = 1210
```

Editor

```
1 clc
2 clear all
3
4 num=6;
5 divisores_proprios = find(mod(num, 1:num-1) == 0)
6 soma = sum(divisores_proprios)
7
8
9 num=12;
10 divisores_proprios = find(mod(num, 1:num-1) == 0)
11 soma = sum(divisores_proprios)
12
13 num=30;
14 divisores_proprios = find(mod(num, 1:num-1) == 0)
15 soma = sum(divisores_proprios)
16
17 num=220;
18 divisores_proprios = find(mod(num, 1:num-1) == 0)
19 soma = sum(divisores_proprios)
20
21 num=284;
22 divisores_proprios = find(mod(num, 1:num-1) == 0)
23 soma = sum(divisores_proprios)
24
25 num=399;
26 divisores_proprios = find(mod(num, 1:num-1) == 0)
27 soma = sum(divisores_proprios)
28
29 num=625;
30 divisores_proprios = find(mod(num, 1:num-1) == 0)
31 soma = sum(divisores_proprios)
32
33 num=1184;
34 divisores_proprios = find(mod(num, 1:num-1) == 0)
35 soma = sum(divisores_proprios)
```

Fonte: Autora com o GNU Octave.

Figura 6.44 – Script para somar os divisores próprios de 1210 a 5564 na Tabela 6.2



Janela de Comandos

```
divisores_proprios =
1 2 5 10 11 22 55 110 121 242 605

soma = 1184
divisores_proprios =
1 2 4 5 10 20 131 262 524 655 1310

soma = 2924
divisores_proprios =
1 3 9 27 101 303 909

soma = 1353
divisores_proprios =
1 2 4 17 34 43 68 86 172 731 1462

soma = 2620
divisores_proprios =
1 7 509

soma = 517
divisores_proprios =
1 29 163

soma = 193
divisores_proprios =
1 2 4 5 10 20 251 502 1004 1255 2510

soma = 5564
divisores_proprios =
1 2 4 13 26 52 107 214 428 1391 2782

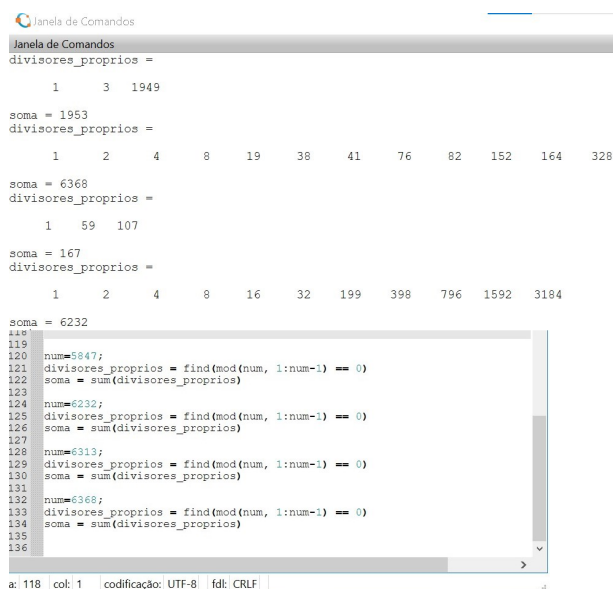
soma = 5020
```

Editor

```
41 num=1210;
42 divisores_proprios = find(mod(num, 1:num-1) == 0)
43 soma = sum(divisores_proprios)
44
45 num=2620;
46 divisores_proprios = find(mod(num, 1:num-1) == 0)
47 soma = sum(divisores_proprios)
48
49 num=2727;
50 divisores_proprios = find(mod(num, 1:num-1) == 0)
51 soma = sum(divisores_proprios)
52
53 num=2924;
54 divisores_proprios = find(mod(num, 1:num-1) == 0)
55 soma = sum(divisores_proprios)
56
57 num=3563;
58 divisores_proprios = find(mod(num, 1:num-1) == 0)
59 soma = sum(divisores_proprios)
60
61 num=4727;
62 divisores_proprios = find(mod(num, 1:num-1) == 0)
63 soma = sum(divisores_proprios)
64
65 num=5020;
66 divisores_proprios = find(mod(num, 1:num-1) == 0)
67 soma = sum(divisores_proprios)
68
69 num=5564;
70 divisores_proprios = find(mod(num, 1:num-1) == 0)
71 soma = sum(divisores_proprios)
72
```

Fonte: Autora com o GNU Octave.

Figura 6.45 – Script para somar os divisores próprios de 5847 a 6368 na Tabela 6.2



```

Janela de Comandos
divisores_proprios =
    1     3    1949

soma = 1953
divisores_proprios =
    1     2     4     8    19    38    41    76    82    152    164    328

soma = 6368
divisores_proprios =
    1    59   107

soma = 167
divisores_proprios =
    1     2     4     8    16    32   199   398   796   1592   3184

soma = 6232
119
120 num=5847;
121 divisores_proprios = find(mod(num, 1:num-1) == 0)
122 soma = sum(divisores_proprios)
123
124 num=6232;
125 divisores_proprios = find(mod(num, 1:num-1) == 0)
126 soma = sum(divisores_proprios)
127
128 num=6313;
129 divisores_proprios = find(mod(num, 1:num-1) == 0)
130 soma = sum(divisores_proprios)
131
132 num=6368;
133 divisores_proprios = find(mod(num, 1:num-1) == 0)
134 soma = sum(divisores_proprios)
135
136
a: 118 | col: 1 | codificação: UTF-8 | fd: CRLF

```

Fonte: Autora com o GNU Octave.

Tabela 6.3 – Pares de números amigáveis do Desafio 6.12

NÚMERO	DIVISORES PRÓPRIOS	SOMA DOS DIVISORES PRÓPRIOS	AMIGO?
6	1,2,3	6	Não
12	1,2,3,4,6	16	Não
30	1,2,3,5,6,10,15	42	Não
220	1,2,4,5,10,11,20,22,44,55,110	284	Sim
284	1,2,4,71,142	220	Sim
399	1,3,7,19,21,57,133	241	Não
825	1,3,5,11,15,25,33,55,75,165,275	663	Não
1184	1,2,4,8,16,32,37,74,148,296,592	1210	Sim
1210	1,2,5,10,11,22,55,110,121,242,605	1184	Sim
2620	1,2,4,5,10,20,131,262,524,655,1310	2924	Sim
2727	1,3,9,27,101,303,909	1353	Não
2924	1,2,4,17,34,43,68,86,172,731,1462	2620	Sim
3563	1,7,508	517	Não
4727	1,29,163	193	Não
5020	1,2,4,5,10,20,251,502,1004,1255,2510	5564	Sim
5564	1,2,4,13,26,52,107,214,428,1391,2782	5020	Sim
5847	1,3,1949	1953	Não
6232	1,2,4,8,19,38,41,76,82,152,164,328,779,1558,3116	6368	Sim
6300	1,59,107	167	Não
6368	1,2,4,8,16,32,199,398,796,1592,3184	6232	Sim

Fonte: Autora.

6.6 ATIVIDADE 6: DESVENDANDO MISTÉRIOS NUMÉRICOS COM O SOROBAN E O GNU OCTAVE

1.1 Nível: Ensino Fundamental.

1.2 Ano: 6º.

1.3 Número de aulas: 4 (45 minutos cada).

1.4 Competências específicas BNCC:

- Compreender as relações entre conceitos e procedimentos dos diferentes campos da Matemática (Aritmética, Álgebra, Geometria, Estatística e Probabilidade) e de outras áreas do conhecimento, sentindo segurança quanto à própria capacidade de construir e aplicar conhecimentos matemáticos, desenvolvendo a autoestima e a perseverança na busca de soluções;
- Utilizar processos e ferramentas matemáticas, inclusive tecnologias digitais disponíveis, para modelar e resolver problemas cotidianos, sociais e de outras áreas de conhecimento, validando estratégias e resultados;
- Interagir com seus pares de forma cooperativa, trabalhando coletivamente no planejamento e desenvolvimento de pesquisas para responder a questionamentos e na busca de soluções para problemas, de modo a identificar aspectos consensuais ou não na discussão de uma determinada questão, respeitando o modo de pensar dos colegas e aprendendo com eles.

1.5 Habilidades específicas BNCC:

(EF06MA03) Resolver e elaborar problemas que envolvam cálculos (mentais ou escritos, exatos ou aproximados) com números naturais, por meio de estratégias variadas, com compreensão dos processos neles envolvidos com e sem uso de calculadora;

(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;

(EF06MA06) Resolver e elaborar problemas que envolvam as ideias de múltiplo e de divisor.

1.6 Conteúdos abordados: múltiplos e divisores de um número natural; critérios de divisibilidade; operações (adição, subtração, multiplicação, divisão e potenciação) com números naturais.

1.7 Objetivos:

- Consolidar o entendimento de operações aritméticas, divisibilidade e sistemas de numeração;
- Promover a utilização do soroban como ferramenta manual e do GNU Octave como ferramenta computacional, demonstrando a versatilidade de ambas;
- Estimular a troca de ideias, a discussão de estratégias e a cooperação entre os alunos;
- Desenvolver o raciocínio lógico e investigativo.

1.8 Procedimento metodológico: aula expositiva e dialogada; solução de problemas.

1.9 Avaliação: observação do desempenho dos estudantes durante a realização da atividade.

Preparem-se para uma jornada emocionante no mundo da Matemática! Hoje, vocês serão divididos em grupos de até cinco detetives numéricos. Utilizando o poder do soroban digital em seus celulares e a versatilidade do GNU Octave, vocês trabalharão em equipe para desvendar mistérios envolvendo números e divisibilidade.

Em cada um dos desafios – Desafios 6.13 a 6.16, haverá pistas sobre um número misterioso. Utilizando o soroban digital, vocês deverão encontrar o número que se encaixa perfeitamente nas pistas. Em seguida, para verificar suas respostas e explorar conceitos mais avançados, vocês utilizarão o GNU Octave, uma poderosa ferramenta de computação numérica.

Lembrem-se: a colaboração é a chave para o sucesso! Compartilhem ideias, testem diferentes possibilidades e utilizem tanto o soroban digital quanto o GNU Octave como ferramentas para visualizar, manipular e analisar os números.

Estão prontos para colocar suas habilidades matemáticas em prática e explorar um novo mundo de possibilidades? Para começar, baixe o aplicativo Simple Soroban gratuitamente na Google Play Store: <<https://play.google.com/store/apps/details?id=br.net.btco.soroban>>.

Mas o que é o simple soroban?

O *simple soroban* é um aplicativo que simula um ábaco japonês (soroban), permitindo aos usuários praticar operações matemáticas como adição, subtração, multiplicação (de 1 e 2 dígitos) e divisão. O app oferece dois modos principais: um modo livre para uso do ábaco e um modo desafio com três níveis de dificuldade (fácil, médio e difícil). Além disso, inclui tutoriais básicos sobre os conceitos fundamentais e as operações mencionadas. Desenvolvido por Bruno Takahashi Carvalhas de Oliveira, o aplicativo foi criado como um projeto de hobby e não contém anúncios nem compras internacionais. Ele também não coleta nem transmite dados dos usuários, garantindo que todas as configurações e informações de uso sejam armazenadas localmente no dispositivo.

Desafio 6.13. *Neste desafio, use o soroban para determinar um número:*

- *que possui 3 algarismos;*

- cuja soma dos algarismos é 15;
- cujo algarismo das centenas é 1;
- que é divisível por 5.

Disponha as contas no soroban para encontrar o número misterioso. Você pode tirar uma foto e anexá-la ou fazer um desenho de como ficou essa representação em seu soroban. Em seguida, responda às seguintes perguntas:

- a) Qual é o número misterioso?
- b) Esse número é divisível por 2? Por quê?
- c) Esse número é divisível por 3? Por quê?
- d) Esse número é divisível por 4? Por quê?

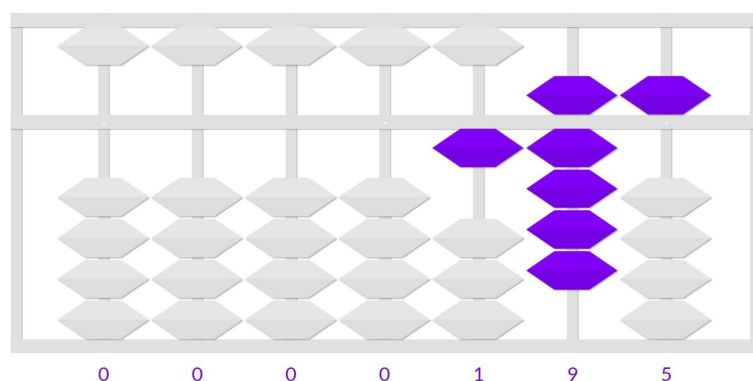
Solução 6.13. (Desafio 6.13) Para determinar o número misterioso, os grupos devem analisar as pistas fornecidas:

- 1º Como o número possui 3 algarismos, limitaremos o cálculo no soroban às hastes que correspondem às unidades, dezenas e centenas;
- 2º Adicionamos uma conta a casa das dezenas, pois de acordo com a pista fornecida, o algarismo das centenas é 1;
- 3º O número que queremos formar tem a soma de seus algarismos igual a 15. Já sabemos que o algarismo das centenas é 1. Para descobrir os outros dois algarismos, calculamos a diferença $15 - 1 = 14$. Então, precisamos encontrar dois algarismos que, quando somados, resultem em 14;
- 4º Uma pista importante que nos foi fornecida é que o número que estamos procurando é divisível por 5. Portanto, esse número terá 0 ou 5 como último algarismo;
- 5º A soma dos dois últimos algarismos precisa ser 14. E o último algarismo só pode ser 0 ou 5. Se for 0, o outro algarismo teria que ser 14, o que não faz sentido, pois os algarismos vão de 0 a 9. Então, o último algarismo é 5. Para que a soma seja 14, o algarismo das dezenas precisa ser 9.

A Figura 6.46 ilustra a solução do Desafio 6.13 no soroban.

Finalizada a análise, as perguntas sobre primeiro número misterioso podem ser respondidas.

Figura 6.46 – Solução do Desafio 6.13 no soroban: o número misterioso é 195



Fonte: Autora.

a) Qual é o número misterioso?

195

b) Esse número é divisível por 2? Por quê?

Não, pois para ser divisível por 2 o número deve ser par. E números pares sempre terminam em 0, 2, 4, 6 ou 8.

c) Esse número é divisível por 3? Por quê?

Sim, pois um número é divisível por 3 se a soma de seus algarismos também for divisível por 3. Como a soma dos algarismos de 195 é 15, e 15 dividido por 3 é 5, então 195 é divisível por 3.

d) Esse número é divisível por 4? Por quê?

Não, porque um número é divisível por 4 somente se os seus dois últimos algarismos formarem um número divisível por 4. Como 95 (os dois últimos algarismos de 195) não é divisível por 4, então 195 também não é divisível.

Desafio 6.14. Neste desafio, empregue o soroban e o GNU Octave para determinar um número:

- que possui 4 algarismos;
- que está entre 9000 e 9999;
- cuja soma dos algarismos é 24;
- cujo algarismo das centenas é 5;
- cujo algarismo das unidades é igual a $10^2 - (9^2 + 15)$.

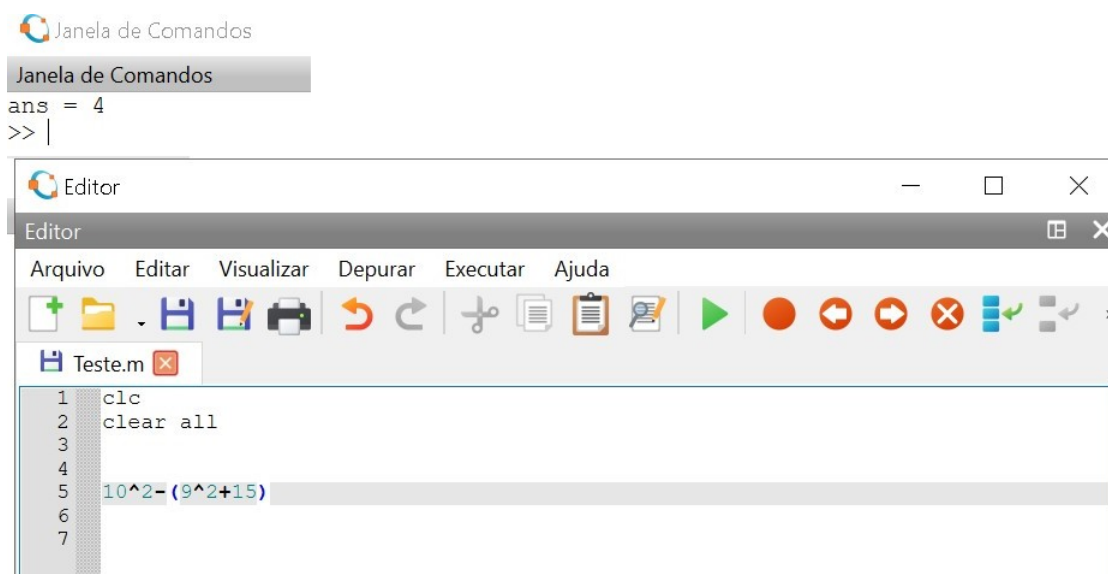
Calcule o algarismo das unidades com o GNU Octave e disponha as contas no soroban para determinar o número misterioso. Você pode tirar uma foto e anexá-la ou fazer um desenho de como ficou essa representação em seu soroban. Logo após, responda às seguintes questões:

- a) Qual é o número misterioso?
- b) Esse número é divisível por 2? Por quê?
- c) Esse número é divisível por 3? Por quê?
- d) Esse número é divisível por 5? Por quê?

Solução 6.14. (Desafio 6.14) Para obter o segundo número misterioso, os grupos devem analisar as pistas fornecidas:

- 1º Como o número possui 4 algarismos, limitaremos o cálculo no soroban às hastes que correspondem às unidades, dezenas, centenas e unidades de milhar;
- 2º Adicionamos 9 contas na casa das unidades de milhar, pois de acordo com a dica fornecida, o número está entre 9000 e 9999. Logo, o algarismo das unidades de milhar é 9;
- 3º Adicionamos 5 contas na casa das centenas de acordo com a dica fornecida;
- 4º Colocamos 4 na casa das unidades, que é o valor da expressão $10^2 - (9^2 + 15)$. Esse valor pode ser calculado/conferido com o GNU Octave, como ilustra a Figura 6.47;

Figura 6.47 – Algarismo das unidades do número misterioso no Desafio 6.14

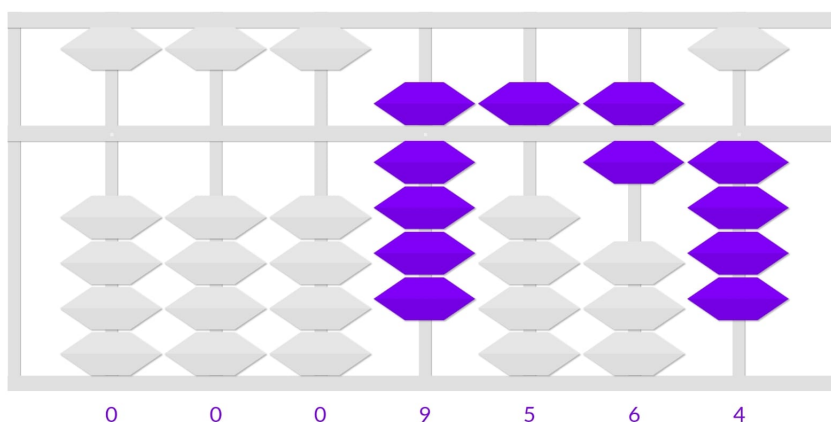


Fonte: Autora com o GNU Octave.

- 5º Queremos um número cuja soma dos algarismos resulte em 24. Já sabemos que os algarismos das unidades de milhar, centenas e unidades são 9, 5 e 4, respectivamente. Para descobrir o algarismo faltante, que é o das dezenas, basta efetuarmos a soma $9 + 5 + 4 = 18$ e depois a diferença $24 - 18 = 6$. Assim, adicionamos 6 contas à casa das dezenas.

A Figura 6.48 ilustra a solução do Desafio 6.14 no soroban.

Figura 6.48 – Solução do Desafio 6.14 no soroban: o número misterioso é 9564



Fonte: Autora.

Finda a análise, as questões sobre o segundo número misterioso podem ser respondidas.

a) Qual é o número misterioso?

9564

b) Esse número é divisível por 2? Por quê?

Sim, o número 9564 é divisível por 2 porque ele termina em 4. E os números que terminam em 0, 2, 4, 6 ou 8 são pares e, portanto, divisíveis por 2.

c) Esse número é divisível por 3? Por quê?

Sim, porque um número é divisível por 3 se a soma de seus algarismos também for divisível por 3. Como a soma dos algarismos de 9564 é 24, e 24 dividido por 3 é 8, então 9564 é divisível por 3.

d) Esse número é divisível por 5? Por quê?

Não, pois para ser divisível por 5 o número precisa terminar em 0 ou 5. E 9564 termina em 4. Logo, não é divisível por 5.

Desafio 6.15. Neste desafio, empregue o soroban e o GNU Octave para determinar um número:

- que possui 5 algarismos;
- cujo algarismo das dezenas de milhar é igual a $(6 + 5 \times 3) \div (8 \times 2 - 3^2)$;
- cujo algarismo das unidades de milhar é o triplo do algarismo das dezenas de milhar;
- cujo algarismo das dezenas é o resultado de $\sqrt{625} - 3 \times \sqrt{36}$;
- cujo algarismo das centenas é 5 unidades a menos do que o algarismo das dezenas;

- que é par e cuja soma dos algarismos é 21.

Calcule o algarismo das dezenas de milhar e o das dezenas com o GNU Octave e disponha as contas no soroban para determinar o número misterioso. Você pode tirar uma foto e anexá-la ou fazer um desenho de como ficou essa representação em seu soroban. Em seguida, responda às seguintes perguntas:

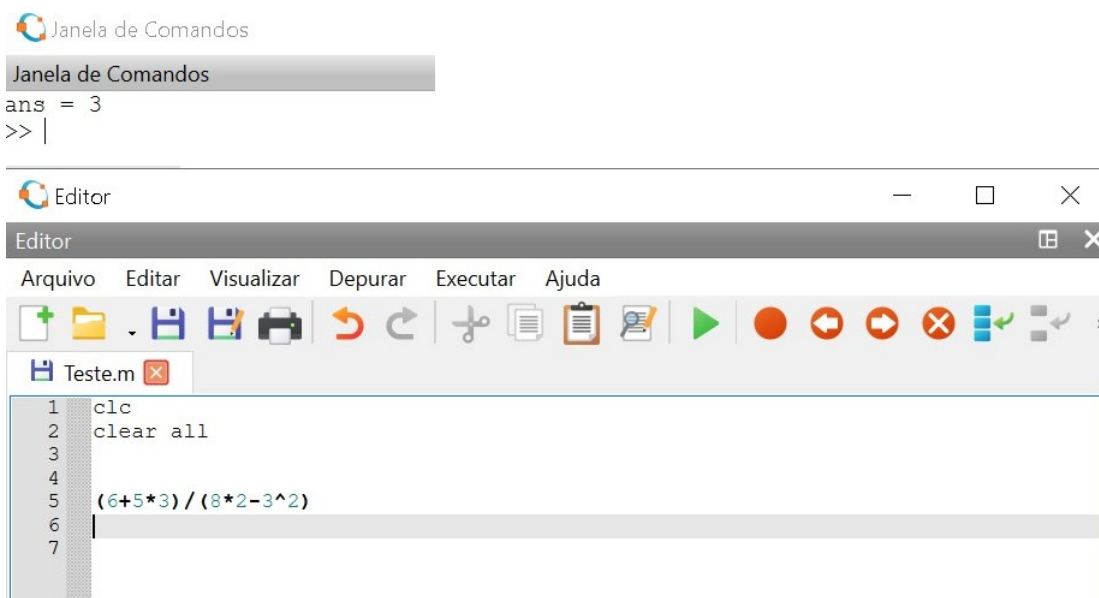
- Qual é o número misterioso?
- Esse número é divisível por 2? Por quê?
- Esse número é divisível por 3? Por quê?
- Esse número é divisível por 10? Por quê?

Solução 6.15. (Desafio 6.15) Para descobrir o terceiro número misterioso, os grupos devem analisar as dicas fornecidas:

1º Como o número possui 5 algarismos, limitaremos o cálculo no soroban às hastes que correspondem às unidades, dezenas, centenas, unidades de milhar e dezenas de milhar;

2º Adicionamos 3 contas à casa das dezenas de milhar, que é o valor da expressão $(6 + 5 \times 3) \div (8 \times 2 - 3^2)$, calculado com o GNU Octave – Figura 6.49;

Figura 6.49 – Algarismo das dezenas de milhar do número misterioso no Desafio 6.15

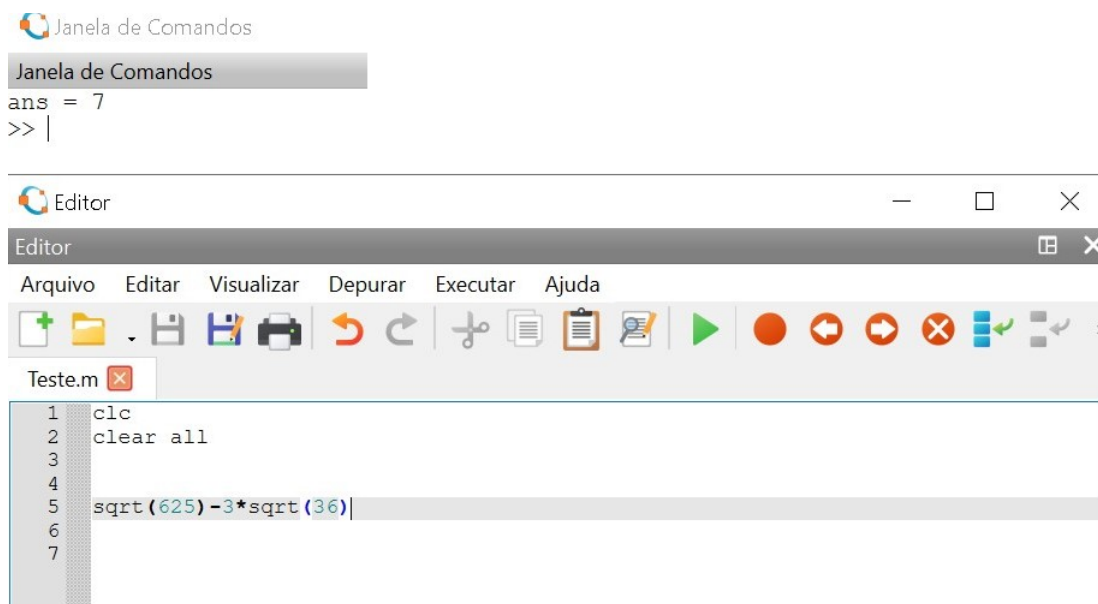


Fonte: Autora com o GNU Octave.

3º Sabemos que o algarismo das unidades de milhar é o triplo do algarismo das dezenas de milhar. Como o algarismo das dezenas de milhar é 3, o algarismo das unidades de milhar é $3 \times 3 = 9$. Assim, adicionamos 9 contas na casa das unidades de milhar para representar esse valor;

4º Colocamos 7 contas na casa das dezenas, pois este é o resultado da expressão $\sqrt{625} - 3 \times \sqrt{36}$, calculado no GNU Octave – Figura 6.50;

Figura 6.50 – Algarismo das dezenas do número misterioso no Desafio 6.15



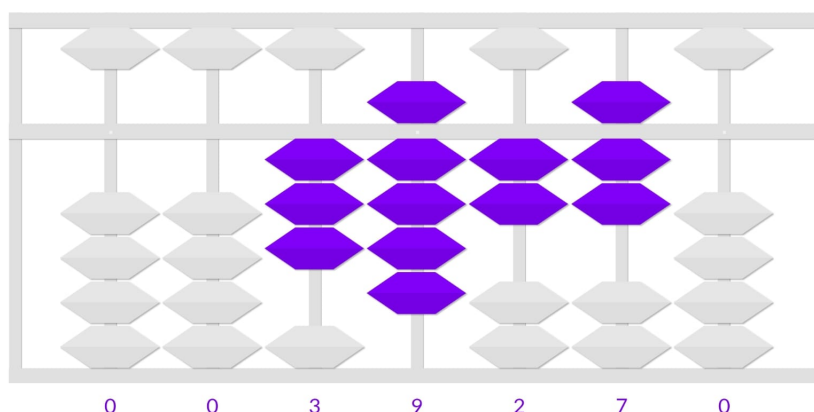
Fonte: Autora com o GNU Octave.

5º Sabemos que o algarismo das centenas é 5 unidades a menos do que o algarismo das dezenas. Como o algarismo das dezenas é 7, o algarismo das centenas é $7 - 5 = 2$. Logo, adicionamos 2 contas na casa das centenas para representar esse valor;

6º Sabemos também que o número misterioso é par e a soma dos seus algarismos é igual a 21. Somando os algarismos já descobertos, temos $3 + 9 + 7 + 2 = 21$. Portanto, o algarismo das unidades é 0. Desta forma, não serão adicionadas contas à casa das unidades.

A Figura 6.51 ilustra a solução do Desafio 6.15 no soroban.

Figura 6.51 – Solução do Desafio 6.15 no soroban: o número misterioso é 39270



Fonte: Autora.

Finalizada a análise, as perguntas sobre o terceiro número misterioso podem ser respondidas.

a) *Qual é o número misterioso?*

39270

b) *Esse número é divisível por 2? Por quê?*

Sim, o número 39270 é divisível por 2 porque ele termina em 0. Os números que terminam em 0, 2, 4, 6 ou 8 são pares e, portanto, divisíveis por 2.

c) *Esse número é divisível por 3? Por quê?*

Sim, porque um número é divisível por 3 se a soma de seus algarismos também é divisível por 3. Como a soma dos algarismos de 39270 é 21 e 21 dividido por 3 é 7, então 39270 é divisível por 3.

d) *Esse número é divisível por 10? Por quê?*

Sim, pois para ser divisível por 10 o número precisa terminar em 0. Como 39270 termina em 0, é divisível por 10.

Desafio 6.16. *Neste desafio, empregue o soroban e o GNU Octave para determinar um número:*

- *que possui 6 algarismos;*
- *cujos algarismos das unidades é o resultado de $(2^3 \times 5) - (5^2 + 9)$;*
- *cujos algarismos que representa as dezenas é uma unidade menor do que o algarismo que representa as unidades;*
- *cujos algarismos das centenas é o número par imediatamente anterior ao algarismo que representa as unidades;*
- *cujos algarismos que representa as centenas de milhar é o primeiro algarismo não nulo do sistema decimal;*
- *cujos soma dos algarismos é 21;*
- *cujos algarismos que representam as dezenas de milhar e as unidades de milhar são dois números consecutivos em ordem crescente.*

Calcule o algarismo das unidades com o GNU Octave e disponha as contas no soroban para determinar o número misterioso. Você pode tirar uma foto e anexá-la ou fazer um desenho de como ficou essa representação em seu soroban. Logo após, responda às seguintes questões:

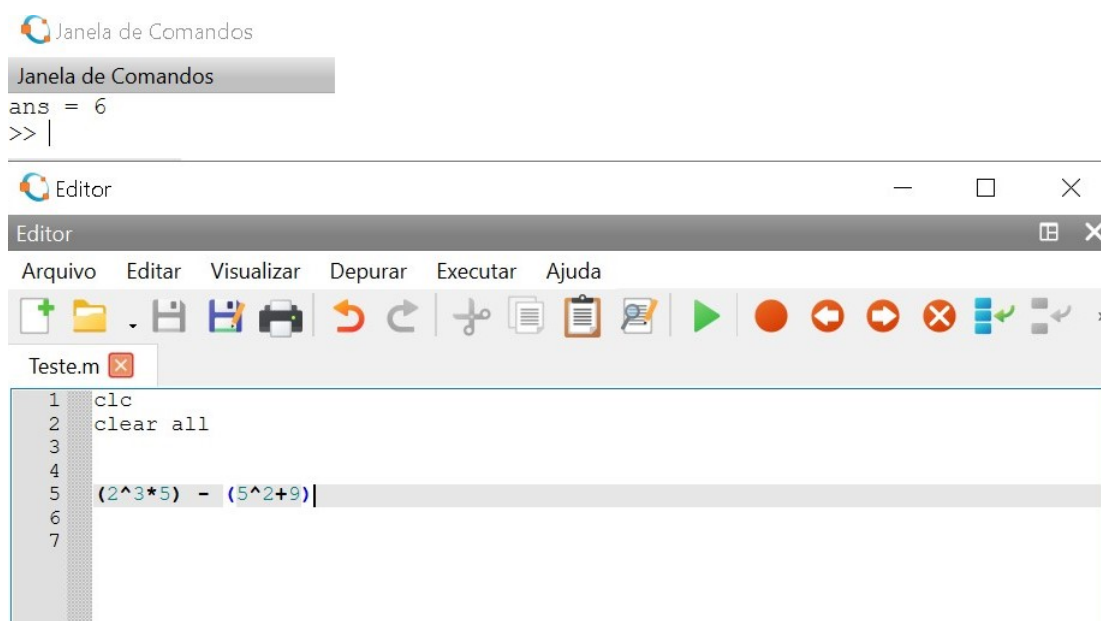
a) *Qual é o número misterioso?*

- b) Esse número é divisível por 2? Por quê?
- c) Esse número é divisível por 3? Por quê?
- d) Esse número é divisível por 4? Por quê?
- e) Esse número é divisível por 6? Por quê?
- f) Esse número é divisível por 8? Por quê?
- g) Esse número é divisível por 10? Por quê?

Solução 6.16. (Desafio 6.16) Para determinar o quarto número misterioso, os grupos devem analisar as pistas fornecidas:

- 1º Como o número possui 6 algarismos, limitaremos o cálculo no soroban às hastes que correspondem às unidades, dezenas, centenas, unidades de milhar, dezenas de milhar e centenas de milhar;
- 2º Colocamos 6 contas na casa das unidades, pois $(2^3 \times 5) - (5^2 + 9) = 6$. O valor da expressão é calculado com o GNU Octave – Figura 6.52;

Figura 6.52 – Algarismo das unidades do número misterioso no Desafio 6.16



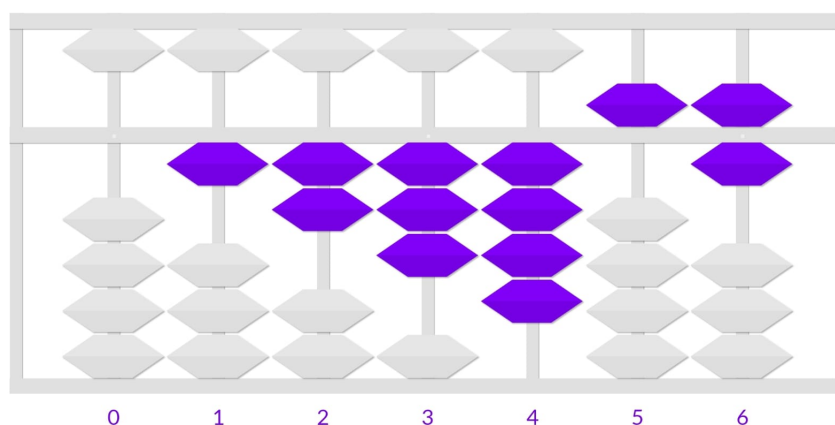
Fonte: Autora com o GNU Octave.

- 3º Sabemos que o algarismo que representa as dezenas é uma unidade menor do que o algarismo que representa as unidades. Como $6 - 1 = 5$, adicionamos 5 contas na casa das dezenas para representar esse valor;
- 4º O algarismo que representa as centenas é o número par imediatamente anterior ao algarismo que representa as unidades. Como o algarismo das unidades é 6, o par imediatamente anterior é o 4. Assim, adicionamos 4 contas à casa das centenas;

- 5º O algarismo que representa as centenas de milhar é o primeiro algarismo não nulo do sistema decimal. Logo, o menor algarismo não nulo possível para as centenas de milhar é 1. Desta forma, adicionamos 1 conta à casa das centenas de milhar;
- 6º A soma dos algarismos do número misterioso é 21. Somando os algarismos já descobertos, temos $6 + 5 + 4 + 1 = 16$. Logo, os dois algarismos faltantes devem somar 5, pois $21 - 16 = 5$. Desta forma, temos as seguintes somas possíveis: $0 + 5 = 5$ ou $5 + 0 = 5$, $1 + 4 = 5$ ou $4 + 1 = 5$ e $2 + 3 = 5$ ou $3 + 2 = 5$;
- 7º Para finalizarmos a busca, temos uma pista final que é muito valiosa: os algarismos que representam as dezenas de milhar e as unidades de milhar são dois números consecutivos em ordem crescente. Como os dois números consecutivos nas possíveis somas apresentadas são 2 e 3 e os mesmos devem ser colocados em ordem crescente, adicionamos 2 contas à casa das dezenas de milhar e 3 contas à casa das unidades de milhar.

A Figura 6.53 ilustra a solução do Desafio 6.16 no soroban.

Figura 6.53 – Solução do Desafio 6.16 no soroban: o número misterioso é 123456



Fonte: Autora.

Finda a análise, as questões sobre o quarto número misterioso podem ser respondidas.

- a) Qual é o número misterioso?
123456
- b) Esse número é divisível por 2? Por quê?
Sim, o número 123456 é divisível por 2 porque termina em 6. Os números que terminam em 0, 2, 4, 6 ou 8 são pares e, portanto, divisíveis por 2.
- c) Esse número é divisível por 3? Por quê?
Sim, porque um número é divisível por 3 se a soma de seus algarismos também é divisível por 3. Como a soma dos algarismos de 123456 é 21 e 21 dividido por 3 é 7, então 123456 é divisível por 3.

d) Esse número é divisível por 4? Por quê?

Sim, pois um número é divisível por 4 se os seus dois últimos algarismos formam um número divisível por 4. Como 56 (os dois últimos algarismos de 123456) é divisível por 4, então 123456 também é divisível.

e) Esse número é divisível por 6? Por quê?

Sim, pois um número é divisível por 6 se é par e a soma dos algarismos é divisível por 3. Como o número 123456 é par (termina em 6) e a soma dos algarismos é 21, que é divisível por 3, temos que 123456 é divisível por 6.

f) Esse número é divisível por 8? Por quê?

Sim, porque um número é divisível por 8 se os três últimos algarismos formam um número divisível por 8. Como 456 (os três últimos algarismos de 123456) é divisível por 8 ($57 \times 8 = 456$), então 123456 também é divisível.

g) Esse número é divisível por 10? Por quê?

Não, pois para ser divisível por 10 o número precisa terminar em 0. Como 123456 termina em 6, não é divisível por 10.

7 CONCLUSÃO

O presente trabalho abordou aspectos fundamentais da Teoria dos Números, com destaque para os conjuntos dos números primos, perfeitos e amigáveis, bem como suas relações com conceitos de divisibilidade, paridade e o pensamento computacional. Esse estudo buscou não apenas explorar a beleza essencial desses números, mas também destacar sua aplicabilidade no ensino, visando estimular a curiosidade e o raciocínio lógico dos estudantes da Educação Básica.

Ao analisarmos os números primos, considerados os átomos da aritmética, exploramos desde suas propriedades mais essenciais, como a fatoração única e a distribuição irregular, avançando para resultados elaborados, como o teorema de Dirichlet e a hipótese de Riemann. Além disso, investigamos classes especiais de números primos, como os palíndromos e os reversos, revelando a rica diversidade desse conjunto numérico e destacamos a importância das conjecturas ainda em aberto, como a dos primos gêmeos, para inspirar e impulsionar as novas gerações de matemáticos.

Por outro lado, os números perfeitos e amigáveis, com sua singularidade e propriedades de divisibilidade, nos transportaram por uma jornada histórica, desde as primeiras investigações dos antigos gregos até as pesquisas mais recentes sobre números hiperperfeitos e amigos quadráticos, nos fazendo refletir sobre suas implicações matemáticas e seu papel na construção do conhecimento numérico.

Outro ponto de destaque foi a inclusão de ferramentas didáticas e computacionais, como o soroban, o GNU Octave e o GeoGebra, para facilitar a compreensão de conceitos abstratos e promover o desenvolvimento do pensamento computacional na Educação Básica. Tais recursos foram integrados ao contexto educacional, evidenciando sua importância para a formação de estudantes mais críticos e autônomos.

Assim, este trabalho reafirma a relevância da Teoria dos Números como campo fértil para o Ensino de Matemática, não apenas por sua riqueza teórica, mas também por seu potencial de conectar conceitos antigos e modernos de forma acessível e instigante. A combinação entre o rigor matemático, a criatividade e a aplicação prática possibilita que temas tão abstratos sejam ferramentas transformadoras no processo de ensino-aprendizagem, despertando o interesse e o encantamento dos estudantes pela Matemática. Em síntese, os conjuntos numéricos investigados transcendem a mera curiosidade acadêmica e oferecem perspectivas concretas para o ensino e o aprendizado, contribuindo significativamente para a formação de habilidades matemáticas essenciais.

Quanto a trabalhos futuros, pretendemos aprimorar o Capítulo 6 incluindo mais atividades. Uma sugestão é abordar os teoremas de Mertens (Yaglom; Yaglom, 1987, p. 40-42), que relacionam números primos e logaritmos decimais e neperianos, em atividades computacionais

com o GNU Octave para o Ensino Médio.

REFERÊNCIAS

- ABU-ARISH, H. **Perfect numbers and perfect polynomials: motivating concepts from kindergarten to college**. 119 f. Dissertação (Mestrado) — The Ohio State University, Ohio, 2016. 107, 109
- ALLAN, N. D. A matemática recreativa de Euler: números amigos. **Revista Brasileira de História da Matemática**, v. 9, n. 17, p. 77–88, 2009. 115, 117
- ALVES, J. S. S.; SOUZA, L. F. de. **O Soroban e sua importância no ensino da matemática**. 2024. Disponível em: <https://sbm.org.br/xi-bienal/wp-content/uploads/sites/31/2024/07/XI_BM_POSTER_Jaqueline_Alves.pdf>. Acesso em: 30 dez. 2024. 40, 41
- ALVES, R. P. **Um estudo sobre os critérios de divisibilidade: questionamento sobre a inserção deste como conteúdo a ser abordado no ensino médio**. 79 f. Dissertação (Mestrado) — Universidade Federal de Tocantins, Arraias, Tocantins, 2021. 32
- ANDRADE, D. Números primos e números de Mersenne. **Jornal Eletrônico de Ensino e Pesquisa de Matemática**, v. 2, n. 1, p. 81–89, 2018a. Disponível em: <https://dma.uem.br/kit/jeepema-1/art3_1801.pdf>. Acesso em: 16 out. 2024. 77
- ANDRADE, R. T. B. de. A história dos números primos. **Revista de História da Matemática para Professores**, v. 4, n. 1, p. 18–27, 2018b. 53, 54
- APOSTOL, T. M. **Introducción a la teoría analítica de los números**. 1a. ed. Barcelona: Reverté, 1984. 435 p. 55, 57
- ARAÚJO, L. R. de. **Congruências quadráticas, reciprocidade e aplicações em sala de aula**. 64 f. Dissertação (Mestrado) — Universidade Federal do Paraíba, João Pessoa, Paraíba, 2013. 61, 62
- BARATA, G. A. A hipótese de Riemann e a distribuição dos números primos. **XI bienal de matemática**, 2024. Disponível em: <https://sbm.org.br/xi-bienal/wp-content/uploads/sites/31/2024/07/XI_BM_POSTER_Gustavo_Alves.pdf>. Acesso em: 23 out. 2024. 85, 86
- BEASLEY, B. D. Euler and the ongoing search for odd perfect numbers. **ACMS 19th Biennial Conference Proceedings**, p. 21–31, 2013. Disponível em: <<https://pillars.taylor.edu/acms-2013/11>>. Acesso em: 07 nov. 2024. 97
- BEGE, A.; FOGARASI, K. Generalized perfect numbers. **Acta Univ. Sapientiae, Mathematica**, v. 1, n. 1, p. 73–82, 2009. Disponível em: <<https://www.emis.de/journals/AUSM/C1-1/MATH1-6.PDF>>. Acesso em: 31 out. 2024. 94, 100, 101
- BEZERRA, N. **Teoria dos números: um curso introdutório**. 1a. ed. Belém: EditAedi, 2018. 193 p. 37
- BISHOP, J. et al. The abundancy index and feebly amicable numbers. **Ball State Undergraduate Mathematics Exchange**, v. 15, n. 1, p. 65–77, 2021. Disponível em: <<https://digitalresearch.bsu.edu/mathexchange/wp-content/uploads/2021/12/BPeet-et-al.pdf>>. Acesso em: 26 dez. 2024. 126, 127

- BLUESTEIN, A. **Computação quântica vai tornar a criptografia atual obsoleta. Mas há uma saída.** 2024. Disponível em: <<https://fastcompanybrasil.com/tech/computacao-quantica-vai-tornar-a-criptografia-atual-obsoleta-mas-ha-uma-saida/>>. Acesso em: 21 out. 2024. 83
- BOYER, C. B. **História da matemática.** 1a. ed. São Paulo: Edgard Blucher, Editora da Universidade de São Paulo, 1974. 488 p. 53, 66, 88
- BRANDÃO, C. L. **Números perfeitos.** 44 f. Dissertação (Mestrado) — Universidade Federal do Ceará, Fortaleza, Ceará, 2021. 23
- BRASIL. **Base Nacional Comum Curricular.** Brasília, 2018. Disponível em: <https://www.gov.br/mec/pt-br/escola-em-tempo-integral/BNCC_EI_EF_110518_versaofinal.pdf>. Acesso em: 10 out. 2024. 18, 21, 22
- BULHÕES, J. W. I. **Aspectos aritméticos e históricos de certos números inteiros especiais.** 40 f. Dissertação (Mestrado) — Universidade Federal de São Paulo, São José dos Campos, São Paulo, 2020. 121, 122, 126
- BURTON, D. M. **Elementary number theory.** 7a. ed. New York: McGraw Hill, 2010. 448 p. 66
- CALDWELL, C.; MCLEAN, R.; SLATKEVICIUS, R. **The top twenty: twin primes.** 2024. Disponível em: <<https://t5k.org/top20/page.php?id=1>>. Acesso em: 07 out. 2024. 69
- CARVALHO, G. C. A. de. **Números primos: pequenos tópicos.** 38 f. Dissertação (Mestrado) — Universidade Federal de Goiás, Goiânia, Goiás, 2013. 22
- CASTRO, G. **Números têm família.** 2020. Disponível em: <<https://mapademileto.wordpress.com/2020/07/22/numeros-tem-familia/>>. Acesso em: 07 jul. 2024. 17
- CASTRO, M. **Números mutuamente amigos.** 2016. Disponível em: <https://www.inf.ufsc.br/~bosco.sobral/ensino/Numeros_Mutuamente_Amigos.pdf>. Acesso em: 26 dez. 2024. 126
- CASTRO, M. F. de. **O estudo da proficuidade dos números primos de Sophie Germain.** 57 f. Dissertação (Mestrado) — Universidade Estadual do Ceará, Fortaleza, Ceará, 2023. 67, 68, 76
- CAVALCANTE, A. L. Pirâmides de números primos palíndromos. **Revista de Informática**, v. 1, n. 1, p. 1–10, 2006. Disponível em: <https://institucional.upis.br/biblioteca/pdf/revistas/revista_informatica/cavalcante_palindromos.pdf>. Acesso em: 08 out. 2024. 70, 71, 72
- COELHO, J. E. C. **Uma introdução aos primos gêmeos: caracterizações e ilustrações.** 68 f. Dissertação (Mestrado) — Universidade Tecnológica Federal do Paraná, Curitiba, Paraná, 2021. 69, 70
- COM-OBMEP, E. **Números triangulares.** Clubes de Matemática da OBMEP, 2020. Disponível em: <<https://clubes.obmep.org.br/blog/sala-de-leitura-numeros-triangulares/>>. Acesso em: 18 nov. 2024. 108
- COSTA, A. **O critério de divisibilidade por 2.** 2021. Disponível em: <<https://www.youtube.com/watch?v=SZSGNCohVLA>>. Acesso em: 24 jan. 2025. 32
- COSTA, A. **O critério de divisibilidade por 3.** 2021. Disponível em: <<https://www.youtube.com/watch?v=kruZo0nv41g>>. Acesso em: 25 jan. 2025. 32

COSTA, A. **O critério de divisibilidade por 4**. 2021. Disponível em: <<https://www.youtube.com/watch?v=Z9Pfh4EaBII>>. Acesso em: 25 jan. 2025. 32

COSTA, A. **O critério de divisibilidade por 5**. 2021. Disponível em: <<https://www.youtube.com/watch?v=GiLRUH1Ji2Q>>. Acesso em: 25 jan. 2025. 32

COSTA, A. **O critério de divisibilidade por 7**. 2021. Disponível em: <<https://www.youtube.com/watch?v=bJl64KkWldA&t=549s>>. Acesso em: 27 jan. 2025. 32

COSTA, G. D. **O crivo de Brun para primos gêmeos**. 29 f. Dissertação (Mestrado) — Universidade Federal de Ouro Preto, Ouro Preto, Minas Gerais, 2021. 68

COSTA, T. J. M. B. da. **Os números perfeitos e os primos de Mersenne**. 65 f. Dissertação (Mestrado) — Universidade de Lisboa, Lisboa, Portugal, 2015. 88

COUTINHO, S. C. **Criptografia**. Rio de Janeiro: IMPA, 2016. 217 p. 77, 79, 80, 81

DEVLIN, K. **Os problemas do milênio**. 2a. ed. Rio de Janeiro: Record, 2008. 310 p. 85, 86

DIMITROV, S. I. Generalizations of amicable numbers. **arXiv**, p. 1–12, 2024. Disponível em: <<https://arxiv.org/abs/2408.07387>>. Acesso em: 28 nov. 2024. 113

DOTS, O. M. **Gerador de caça-palavras gratuito**. Oh, My Dots!, 2025. Disponível em: <<https://pt.ohmydots.com/creator-word-search.html>>. Acesso em: 11 jan. 2025. 144

D'AMBROSIO, U. Euler, um matemático multifacetado. **RHMP - Revista História da Matemática para Professores**, v. 7, n. 1, p. 91–111, 2021. 115

D'ORNELAS, S. **Os problemas de matemática que valem 1 milhão de dólares**. 2014. Disponível em: <<https://hypescience.com/problemas-matematica/>>. Acesso em: 23 out. 2024. 84

EATON, J. W. **GNU Octave: scientific programming language**. S.l.: GNU Octave, 2025. Disponível em: <<https://octave.org/>>. Acesso em: 08 abr. 2025. 20

EFUTURO. **Soroban**. 2024. Disponível em: <<https://www.efuturo.com.br/jogosseducoficial/soroban/>>. Acesso em: 30 dez. 2024. 41

EUCLIDES. **Os Elementos**. São Paulo: Unesp, 2009. 593 p. 37, 53

EULER, L. et al. **Sobre números amigáveis**. Natal: EDUFRRN, 2015. v. 9. 234 p. 21, 113, 114, 115, 116, 122

EVES, H. **Introdução à história da matemática**. 5a. ed. Campinas, São Paulo: Editora da Unicamp, 2011. 848 p. 53, 88, 90, 96

FONSECA, R. V.; LIMA, M. da G. C. Mais curiosidades numéricas: números abundantes e deficientes. **Revista do Professor de Matemática**, n. 47, p. 39–41, 2001. 88

FONSECA, R. V.; MONTEIRO, A. T. M.; FONSECA, R. C. V. O teorema fundamental da aritmética - números primos e sutilezas ocultas da aritmética. **Matemática & Ciência**, v. 4, n. 2, p. 67–93, 2021. 55

FOSSA, J. A.; LEÔNICIO, S. M. S. **Introdução aos métodos de Euler para achar números amigáveis**. Natal: Sociedade Brasileira de História da Matemática, 2013. 100 p. 118, 119, 121

- FRANÇA, B. N. da. **Nova acta eruditorum. 1747**. 2009. Disponível em: <<https://gallica.bnf.fr/ark:/12148/bpt6k500647#>>. Acesso em: 04 dez. 2024. 115
- GABRIELLI, A. M.; MONTEIRO, M. S. Atividades com números poligonais e sequências. **Revista do Professor de Matemática**, n. 68, 2009. Disponível em: <<https://rpm.org.br/cdrpm/68/2.html>>. Acesso em: 20 nov. 2024. 108
- GARCIA, A. **On perfect numbers**. 2016. Disponível em: <<https://pt.scribd.com/document/699740473/Arturo-Garcia>>. Acesso em: 05 nov. 2024. 91, 102
- GARDNER, M. **The magic numbers of Dr. Matrix**. Buffalo, New York: Prometheus Books, 1985. 329 p. 72, 73
- GEOGEBRA. **Ensine e aprenda matemática de uma forma mais inteligente**. S.l.: GeoGebra, 2025. Disponível em: <<https://www.geogebra.org/>>. Acesso em: 08 abr. 2025. 20
- GEOGEBRATEAM. **Learn GeoGebra Classic**. S.l.: GeoGebra, 2025. Disponível em: <<https://www.geogebra.org/m/XUv5mXTm>>. Acesso em: 28 mar. 2025. 129
- GERHARDT, T. E.; SILVEIRA, D. T. **Métodos de pesquisa**. Porto Alegre: Editora da UFRGS, 2009. 120 p. 24
- GIMPS. **Great internet Mersenne prime search**. 2024a. Disponível em: <<https://www.mersenne.org/>>. Acesso em: 16 out. 2024. 67, 77
- GIMPS. **Great internet Mersenne prime search**. 2024b. Disponível em: <<https://www.mersenne.org/primes/>>. Acesso em: 31 out. 2024. 90
- GOMES, A. J.; COSTA, E. A. da; SANTOS, R. A. dos. Números perfeitos e primos de Mersenne. **Revista da Olimpíada**, n. 7, p. 99–111, 2008. 88, 93, 94, 103, 106
- GUMARU, R. C. R.; CASUCO, L. S.; BERNAL, H. L. Formulating an odd perfect number: an in depth case study. **Pure and Applied Mathematics Journal**, v. 7, n. 5, p. 63–67, 2018. Disponível em: <<https://www.sciencepublishinggroup.com/article/10.11648/j.pamj.20180705.11>>. Acesso em: 02 nov. 2024. 96
- HARAN. **The relation with perfect numbers , triangular numbers and cyclops numbers**. 2020. Mathematics Stack Exchange. Disponível em: <<https://math.stackexchange.com/q/3667674>>. Acesso em: 25 nov. 2024. 112
- HEFEZ, A. **Iniciação à aritmética**. Rio de Janeiro: IMPA, 2015. 127 p. 38, 39
- HEFEZ, A. **Aritmética**. 3a. ed. Rio de Janeiro: SBM, 2022. 290 p. 27, 36, 37, 38, 55, 56, 57, 59, 61, 62, 63, 66, 76, 77, 81
- JESUS, A. F. de; CLAUDINO, R. A. A linguagem C na obtenção dos primos gêmeos: uma abordagem descritiva na teoria dos números. **Trilhas Pedagógicas**, v. 4, n. 4, p. 64–78, 2014. 74
- KNILL, O. The oldest open problem in mathematics. **Math Circle**, p. 1–26, 2007. Disponível em: <<https://people.math.harvard.edu/~knill/seminars/perfect/handout.pdf>>. Acesso em: 30 out. 2024. 88, 89, 105
- KOSHY, T. **Elementary number theory with applications**. 2nd ed.: Academic Press, 2007. 800 p. 89, 93

LACASA, L. et al. On a dynamical approach to some prime number sequences. **Entropy**, v. 20, n. 2, p. 131, 2018. Disponível em: <<https://doi.org/10.3390/e20020131>>. Acesso em: 15 out. 2024. 75

LEÔNICIO, S. M. S. **Os artigos de Euler sobre os números amigáveis**. 132 f. Dissertação (Mestrado) — Universidade Federal do Rio Grande do Norte, Natal, Rio Grande do Norte, 2013. 115, 116, 117, 119, 122

LIMA, E. **Programador descobre maior número primo conhecido, com 41 milhões de dígitos**. 2024. Super interessante. Disponível em: <<https://super.abril.com.br/ciencia/programador-descobre-maior-numero-primo-conhecido-com-41-milhoes-de-digitos>>. Acesso em: 23 fev. 2025. 67

LOPES, M. **Os problemas do milênio – parte I**. 2017. Disponível em: <<https://sophiaofnature.wordpress.com/2017/04/30/os-problemas-do-milenio-parte-i/>>. Acesso em: 23 out. 2024. 84

MARCIANO, E. **Para que serve o resto da divisão?** 2020. Disponível em: <<https://escolaeducacao.com.br/para-que-serve-o-resto-da-divisao/>>. Acesso em: 17 jan. 2025. 45

MARINHO, T. **Criptografia assimétrica RSA**. 2017. Disponível em: <<https://medium.com/@tarcisioma/algorithm-de-criptografia-assim%C3%A9trica-rsa-c6254a3c7042>>. Acesso em: 16 out. 2024. 78

MARREIROS, E. C. do N. et al. Números perfeitos: uma abordagem computacional. **Revista ft**, v. 28, n. 135, 2024. Disponível em: <<https://revistaft.com.br/numeros-perfeitos-uma-abordagem-computacional/#:~:text=N%C3%A9meros%20PERFEITOS%20EM%20BIN%C3%81RIOS,de%20computadores%20e%20dispositivos%20eletr%C3%B4nicos.>> Acesso em: 17 nov. 2024. 106, 107

MARTINEZ, F. E. B. et al. **Teoria dos números: um passeio com primos e outros números familiares pelo mundo inteiro**. 2013. Disponível em: <https://edisciplinas.usp.br/pluginfile.php/4576649/mod_resource/content/1/Um%20passeio%20pelos%20primos%20e%20outros%20n%C3%BAmoros%20familiares..pdf>. Acesso em: 07 jul. 2024. 17

MCCRANIE, J. S. A study of hyperperfect numbers. **Journal of Integer Sequences**, v. 3, n. Article 00.1.3, 2000. Disponível em: <<http://www.kurims.kyoto-u.ac.jp/EMIS/journals/JIS/VOL3/mccranie.html>>. Acesso em: 12 nov. 2024. 99

MICHAELIS. **Dicionário brasileiro da língua portuguesa**. 2024. Disponível em: <<https://michaelis.uol.com.br/moderno-portugues/busca/portugues-brasileiro/conjectura/>>. Acesso em: 24 set. 2024. 64

NDIAYE, M. Origin of sexy prime numbers, origin of cousin prime numbers, equations from supposedly prime numbers, origin of the Mersenne number, origin of the fermat number. **Advances in Pure Mathematics**, v. 14, n. 9, p. 321–332, 2024. 74

NETO, S. C. de G.; TOILLIER, J. S. **Pitágoras para além do teorema**. Porto Velho, Rondônia: EDUFRO, 2020. 174 p. 20, 113, 114, 115

NOVAES, P. R. M. de A. A Sophie Germain e seu legado na matemática, na ciência e tecnologia. **Revista Babilônia**, v. 9, n. 9, p. 98–105, 2023. Disponível em: <<https://bdex.eb.mil.br/jspui/bitstream/123456789/13535/1/A%20Sophie%20Germain.pdf>>. Acesso em: 15 out. 2024. 76

NUNES, D. **A hipótese de Riemann: o problema mais famoso da matemática**. 2023. Disponível em: <https://www.youtube.com/watch?v=Zx_PvQSqdLY&t=611s>. Acesso em: 24 out. 2024. 86

OLIVEIRA, R. R. de; ANDRADE, M. H. de. Carl Friedrich Gauss: contribuições matemáticas. **Boletim Cearense de Educação e História da Matemática**, v. 7, n. 20, p. 427–439, 2020. Disponível em: <<https://revistas.uece.br/index.php/BOCEHM/article/view/3554/3064>>. Acesso em: 20 set. 2024. 61

ONODY, R. N. **Conjecturas matemáticas e a máquina de Ramanujan**. 2021. Disponível em: <<https://www2.ifsc.usp.br/portaal-ifsc/conjecturas-matematicas-e-a-maquina-de-ramanujan/>>. Acesso em: 24 set. 2024. 64

ORE, O. **Number theory and its history**. New York: McGraw-Hill Book Company, 1948.
370 p. 61

PADILHA, J. C. R. **Números primos**. 72 f. Dissertação (Mestrado) — Universidade Federal do Paraíba, João Pessoa, Paraíba, 2013. 54

PAMPENA, S. **Glitch primes and cyclops numbers-numberphile**. 2015. Disponível em: <<https://www.youtube.com/watch?v=HPfAnX5blO0>>. Acesso em: 21 nov. 2024. 110

PERUZZO, J. **O fascínio dos números primos**. 1a. ed. Irani: Clube de Autores, 2012. 125 p.
66, 77

POLIDORO, P. **Código binário: como converter palavras e números.** 2023. Disponível em: <<https://www.locaweb.com.br/blog/temas/codigo-aberto/codigo-binario-como-converter-palavras-e-numeros/#:~:text=A%20convers%C3%A3o%20de%20n%C3%BAmeros%20decimais,a%20representa%C3%A7%C3%A3o%20bin%C3%A1ria%20do%20n%C3%BAmero.>> Acesso em: 17 nov. 2024. 106

PRAJAPATI, S. K. **Twin primes, cousin primes and sexy primes**. 2021. Disponível em: <<https://pt.slideshare.net/slideshow/twin-primes-cousin-primes-and-sexy-primes/249853333>>. Acesso em: 15 out. 2024. 75

PUNEETH, V. On k-hyperperfect and super hyperperfect numbers. **International Journal of Mathematics Trends and Technology**, v. 63, n. 1, p. 65–67, 2018. Disponível em: <<https://ijmtjournal.org/public/assets/volume-63/number-1/IJMTT-V63P508.pdf>>. Acesso em: 12 nov. 2024. 99, 101

PURKAYASTHA, S.; GOSWAMI, J.; DEBNATH, B. Characterization of a hyperperfect group. **MATEMATIKA**, v. 33, n. 1, p. 97–103, 2017. Disponível em: <

- QCONCURSOS. **Números amigos quadráticos**. 2019. Disponível em: <<https://www.qconcursos.com/questoes-de-concursos/questoes/e4c4eb5d-fa>>. Acesso em: 27 dez. 2024. 127
- QUINTANS, J. **O ensino dos números primos inter-relacionados a conteúdos diversos através da resolução de problemas**. 134 p. Dissertação (Mestrado) — Universidade de São Paulo, São Carlos, São Paulo, 2020. 22
- RAMONE, C. **Cyclops numbers puzzle-python-codewars**. 2020. Disponível em: <<https://www.youtube.com/watch?v=byirDzB1PSQ>>. Acesso em: 21 nov. 2024. 110
- RCK, D. **O que são os números amigos? Dicas pra adição/soma Soroban**. 2023. Disponível em: <<https://www.youtube.com/watch?v=hg6gDVi9K1U>>. Acesso em: 30 dez. 2024. 42, 43
- REID, C. Perfect numbers. **Scientific American**, v. 188, n. 3, p. 84–87, 1953. Disponível em: <<https://www.jstor.org/stable/24944161>>. Acesso em: 31 out. 2024. 89, 90
- REIS, C. C. dos; BAYER, V. Números primos: relação histórica e algumas curiosidades. **Revista Ifesciência**, v. 6, n. 4, p. 242–256, 2020. 54
- RESENDE, M. R. **Re-significando a disciplina teoria dos números na formação do professor de matemática na licenciatura**. Tese (Doutorado) — Pontifícia Universidade Católica de São Paulo, 2007. 27
- RESENDE, T. R. M. **O ensino da matemática por meio do soroban**. 2018. Disponível em: <<https://trocandosaberes.com.br/wp-content/uploads/2023/09/Cartilha-Soroban.pdf>>. Acesso em: 30 dez. 2024. 40
- RIZEL, A. C. **Números primos**. 60 f. Monografia (Especialização) — Universidade Federal de Minas Gerais, Belo Horizonte, 2014. 53
- ROCHA, E. **Criptografia**. 2017. Disponível em: <<https://www.goconqr.com/mapamental/7956687/criptografia>>. Acesso em: 21 out. 2024. 79
- ROSETTA_CODE. **Cyclops numbers**. 2024. Disponível em: <https://rosettacode.org/wiki/Cyclops_numbers>. Acesso em: 21 nov. 2024. 110
- SANTOS, J. C. Números perfeitos. **Revista de Ciência Elementar**, v. 8, n. 4, p. 1–5, 2020. Disponível em: <<https://rce.casadasciencias.org/rceapp/pdf/2020/056/>>. Acesso em: 29 out. 2024. 88, 93, 94
- SANTOS JÚNIOR, R. J. dos. **Números perfeitos e amigáveis**. 68 p. Dissertação (Mestrado) — Universidade Estadual do Paraíba, Campina Grande, Paraíba, 2020. 23, 123
- SAUTOY, M. du. **A música dos números primos: a história de um problema não resolvido na matemática**. Rio de Janeiro: Zahar, 2008. 470 p. 54, 55, 84, 85, 87
- SAUTOY, M. du. **Os mistérios dos números: uma viagem pelos grandes enigmas da matemática (que até hoje ninguém foi capaz de resolver)**. Rio de Janeiro: Zahar, 2013. 304 p. 18
- SENA, H. T. A. de. **Algumas evidências computacionais da infinitude dos números primos palindrômicos e generalizações destes**. 96 f. Monografia (Graduação) — Universidade Federal do Rio Grande do Norte, Natal, Rio Grande do Norte, 2008. 71

SHALIT, E. de. **Números primos: por que são tão empolgantes?** 2022. Disponível em: <<https://parajovens.unesp.br/numeros-primos-por-que-sao-tao-empolgantes/>>. Acesso em: 02 out. 2024. 65, 66, 67, 84

SILVA, J. G. de L. **O ensino de números primos através de problemas abertos.** 46 f. Monografia (Graduação) — Instituto Federal de Educação, Ciência e Tecnologia do Rio Grande do Norte, Natal, Rio Grande do Norte, 2018. 69

SILVA JÚNIOR, J. C. **O teorema de Dirichlet: primos em progressão aritmética.** 63 f. Dissertação (Mestrado) — Universidade Federal do Paraíba, João Pessoa, Paraíba, 2017. 57, 58, 123

SILVA, R. J. da. **Número Capicua.** 2012a. Disponível em: <<http://www.osfantasticosnumerosprimos.com.br/011-estudos-250-numero-capicua.html>>. Acesso em: 08 out. 2024. 71

SILVA, R. J. da. **Números primos reversos - omirp - 267.** 2012b. Disponível em: <<http://www.osfantasticosnumerosprimos.com.br/011-estudos-267-numeros-primos-reversos.html>>. Acesso em: 08 out. 2024. 72, 73

SILVA, T. P. da. **CrITÉrios de divisibilidade: usuais, incomuns e curiosos.** 61 f. Dissertação (Mestrado) — Universidade Federal do Paraíba, João Pessoa, Paraíba, 2019. 32

SINGH, S. **O livro dos códigos.** 14a. ed. Rio de Janeiro: Record, 2022. 448 p. 77

SLOANE, N. J. A. **List emirp.** S. l.: The On-Line Encyclopedia of Integer Sequences (OEIS), 2024. Disponível em: <<https://oeis.org/search?q=list+emirp&go=Procurar>>. Acesso em: 09 out. 2024. 74

SOUZA, J. de B. **Conjecturas em teoria dos números e suas histórias.** 57 f. Dissertação (Mestrado) — Universidade Federal do Paraíba, João Pessoa, Paraíba, 2019. 69

SPINA, A. V. **Números primos e criptografia.** 43 f. Dissertação (Mestrado) — Universidade Estadual de Campinas, Campinas, São Paulo, 2014. 68

STEVENS, B. **The necessary conditions for odd perfect numbers.** S.l.: Digital Commons @ University of South Florida, 2012. Disponível em: <https://digitalcommons.usf.edu/honors_et/101>. Acesso em: 02 nov. 2024. 97, 98

STEWART, I. **Em busca do infinito: uma história da matemática dos primeiros números à teoria do caos.** 1a. ed. Rio de Janeiro: Zahar, 2014. 384 p. 54

SUPERA, A. de I. **Soroban: concentração, agilidade de raciocínio e muito mais!** 2023. Disponível em: <<https://metodosupera.com.br/o-soroban-aprimoramento-da-concentracao-da-agilidade-de-raciocinio/>>. Acesso em: 30 dez. 2024. 40

TAHAN, M. **O homem que calculava.** 83a. ed. Rio de Janeiro: Ediora Record, 2013. 263 p. 128

TANEJA, I. J. Amicable numbers with patterns in products and powers. **RGMIA Research Report Collection**, v. 20, p. 1–25, 2017. 124, 125

TENÓRIO, M. **Números perfeitos.** 2011. Disponível em: <<https://www.flickr.com/photos/marlontenorio/5932367184/in/photolist-a3dW5Q>>. Acesso em: 28 out. 2024. 19

TENÓRIO, M. **Números amigos**. 2013. Disponível em: <<https://www.flickr.com/photos/marlontenorio/9330242394/in/photolist-fdtW1b-a68ybg-5aJnQS>>. Acesso em: 28 out. 2024. 20

TENÓRIO, M. **A amizade quadrática**. 2019. Disponível em: <<https://www.flickr.com/photos/marlontenorio/48331394311/in/photolist-2gCT2FV-fdtW1b-KjVdTq>>. Acesso em: 27 dez. 2024. 128

VAXASOFTWARE. **Lista de parejas de números amigos de 1 a 20 000 000**. 2024. Disponível em: <https://www.vaxasoftware.com/doc_edu/mat/numamigos_esp.pdf>. Acesso em: 04 dez. 2024. 117

VIANA, M. **Primos gêmeos constituem um dos mistérios mais intrigantes da aritmética**. 2018. Disponível em: <<https://www1.folha.uol.com.br/colunas/marceloviana/2018/03/primos-gemeos-constituem-um-dos-misterios-mais-intrigantes-da-aritmetica.shtml>>. Acesso em: 07 out. 2024. 68, 70

VIANA, M. **Na folha, Viana fala de problemas não resolvidos**. 2022. Disponível em: <<https://impa.br/noticias/na-folha-viana-fala-de-problemas-matematicos-nao-resolvidos/>>. Acesso em: 24 set. 2024. 65

VIANA, M. **Folha: números primos e o teorema de ouro**. 2023. Disponível em: <<https://impa.br/noticias/folha-numeros-primos-e-o-teorema-de-ouro/>>. Acesso em: 20 set. 2024. 62, 63

VIANA, M. **Folha: O teorema de Euclides-Euler**. 2024. Disponível em: <<https://impa.br/noticias/folha-o-teorema-de-euclides-euler/#:~:text=Em%20um%20trabalho%20realizado%20por,2p%E2%80%931%20%C3%A9%20primo.>> Acesso em: 04 nov. 2024. 90

VIANA, M. **Na folha, Marcelo Viana fala sobre números perfeitos**. 2024. Disponível em: <<https://impa.br/noticias/folha-a-perfeicao-nos-numeros/>>. Acesso em: 11 out. 2024. 19

VIEIRA, M. O. **O teorema dos números primos**. 99 f. Dissertação (Mestrado) — Universidade Federal de Sergipe, São Cristovão, Sergipe, 2023. 74

VOIGHT, J. **Perfect numbers: an elementary introduction**. 1998. Disponível em: <<https://jvoight.github.io/notes/perfelem-051015.pdf>>. Acesso em: 02 nov. 2024. 94

WIKI. **Using Octave**. S.l.: MediaWiki, 2024. Disponível em: <https://wiki.octave.org/Using_Octave>. Acesso em: 28 mar. 2025. 129

YAGLOM, A. M.; YAGLOM, I. M. **Challenging mathematical problems with elementary solutions**. New York: Dover, 1987. v. 2. 214 p. 178

ÍNDICE

- Conjectura
 - de Goldbach, 65
 - de Polignac, 69
 - primos gêmeos, 65, 68
- Criptografia, 77
 - RSA, 78
- Divisibilidade
 - algoritmo de Euclides, 37
 - critérios de, 31–36
 - definição, 27
 - propriedades, 27–31
- Função
 - piso, 62
 - zeta de Riemann, 85
 - índice de abundância, 126
- GeoGebra, 129
- GNU Octave, 129
- Hipótese de Riemann, 84
- Lema
 - de Euclides, 55
- Matemáticos
 - Alhazém, 94
 - Brun, 70
 - Cataldi, 89
 - Descartes, 89
 - Dirichlet, 57, 161
 - Eratóstenes, 53
 - Euclides, 36, 53
 - Euler, 54, 115
 - Fermat, 54
 - Gauss, 21, 54
 - Germain, 76
 - Girard, 54
 - Hadamard, 85
 - Hardy, 86
 - Legendre, 61
 - Mersenne, 76
 - Nicômano de Gérasa, 88
 - Polignac, 69
 - Poussin, 85
 - Qurra, 113
 - Riemann, 54
 - Sylvester, 89
 - Theon de Esmirna, 88
- Mediana, 143
- Número abundante, 88
- Número ciclope, 109
 - binário, 110
- Número deficiente, 88
- Número geométrico
 - hexagonal, 107, 136
 - pentagonal, 136
 - quadrangular, 136
 - triangular, 107, 131
- Número palíndromo, 70
- Número perfeito
 - conceito, 88
 - hiperperfeito, 98
 - multiplamente perfeito, 127
 - par, 94
 - sistema binário, 106
 - ímpar, 96
- Número primo
 - conceito, 53
 - de Germain, 76
 - de Mersenne, 77
 - distribuição, 65
 - palíndromo, 71

- primo, 74
- reverso, 72
 - cíclico, 73
- sexy, 74
- Números amigos quadráticos, 127
- Números amigáveis, 113
- Números autoamigáveis, 125
- Números mutuamente amigos, 126
- Paridade, 36
- Pirâmide de primos palíndromos, 71
- Quadrados de primos reversos, 73
- Sequência didática
 - divisibilidade, 166
 - números amigáveis, 161
 - números geométricos, 129
 - números perfeitos, 140
 - números primos, 137
 - primos em progressão aritmética, 151
- Soroban, 18, 39, 167
 - adição, 41
 - critérios de divisibilidade, 50
 - divisão, 45
 - simple soroban, 51
- Símbolo de Legendre, 62
- Teorema
 - de Bâchet-Bézout, 55
 - de Dirichlet, 57, 161
 - de Euclides-Euler, 93
 - de ouro, 62
 - dos números primos, 66
 - fundamental da aritmética, 55, 56
 - pequeno teorema de Fermat, 54, 59