UNIVERSIDADE ESTADUAL DE GOIÁS
Câmpus Central - Sede: Anápolis - CET
Curso de Matemática

O Fascinante Mundo dos Números Primos

ANNA KAROLLYNE CINTRA BUENO

Anápolis
2022

ANNA KAROLLYNE CINTRA BUENO

O Fascinante Mundo dos Números Primos

Trabalho de Curso (TC) apresentado, à Coordenação Setorial do Curso de Matemática, como parte dos requisitos para obtenção do título de Graduado no Curso de Matemática da Universidade Estadual de Goiás.

Orientador: Prof. Dra. Selma Marques de Paiva

Anápolis

2022

Elaborada pelo Sistema de Geração Automática de Ficha Catalográfica da UEG
com os dados fornecidos pelo(a) autor(a).

BB928 f

Bueno, Anna Karollyne Cintra
O fascinante mundo dos números primos / Anna Karollyne Cintra Bueno; orientador Selma Marques de Paiva. -- Anápolis, 2022.
82 p.

Graduação - Matemática -- Câmpus Central - Sede: Anápolis - CET, Universidade Estadual de Goiás, 2022.

1. Teoria dos números. 2. Criptografia. 3. Congruência. I. Paiva, Selma Marques de , orient. II. Título.

UNIVERSIDADE ESTADUAL DE GOIÁS

CÂMPUS CENTRAL – SEDE: ANÁPOLIS - CET

TERMO DE AUTORIZAÇÃO PARA DISPONIBILIZAÇÃO DE MONOGRAFIAS DIGITAIS NO BANCO DE DADOS DO CÂMPUS CENTRAL – SEDE: ANÁPOLIS - CET

Eu Anna Karollyne Cintra Bueno

Curso Matemática Licenciatura

Na qualidade de titular dos direitos de autor que recaem sobre a minha monografia de Conclusão de Curso, intitulada O Fascinante Mundo dos Números Primos

Defendida em 17 / 03 / 2022, junto à banca examinadora do curso com fundamento nas disposições da lei nº 9.610 de 19 de fevereiro de 1998, autorizo a disponibilizar gratuitamente a obra citada, sem ressarcimento de direitos autorais, para fins de impressão e/ou *downloading* pela *internet*, a título de divulgação da produção científica gerada pela Universidade Estadual de Goiás / Câmpus Central – SEDE: Anápolis - CET, a partir desta data.

(x) autorizo texto (completo)

( ) autorizo parcial (resumo)

Assim, autorizo a liberação total ou resumo de meu trabalho, estando ciente que o conteúdo disponibilizado é de minha inteira responsabilidade.

Anápolis, 24 de março de 2022

Assinatura do autor

Anna Karollyne Cintra Bueno

Assinatura do orientador

Selma Marques de Paiva

Universidade Estadual de Goiás

ESTADO DE GOIÁS
UNIVERSIDADE ESTADUAL DE GOIÁS - UEG
COORDENAÇÃO SETORIAL MATEMÁTICA ANÁPOLIS

ANNA KAROLLYNE CINTRA BUENO

O FASCINANTE MUNDO DOS NÚMEROS PRIMOS

Trabalho de Curso II de Matemática apresentado à Banca Examinadora como parte dos requisitos para a obtenção do grau de graduado em Licenciatura em Matemática.

Aprovado. Banca Examinadora do Trabalho de Curso II do curso de Matemática do Campus Central: Sede - Anápolis - CET da Universidade Estadual de Goiás.

Anápolis - Goiás, 17 de março de 2022.

_____
Dra. Selma Marques de Paiva
Orientador(a)/Presidente da banca examinadora

_____
M.e Cleber Giugioli Carrasco
1º Membro da Banca Examinadora

_____
Dr. Fabiano Boaventura de Miranda
2º Membro da Banca Examinadora

Documento assinado eletronicamente por **SELMA MARQUES DE PAIVA**, **Docente de Ensino Superior**, em 22/03/2022, às 16:57, conforme art. 2º, § 2º, III, "b", da Lei 17.039/2010 e art. 3ºB, I, do Decreto nº 8.808/2016.

Documento assinado eletronicamente por **FABIANO BOAVENTURA DE MIRANDA**, **Docente de Ensino Superior**, em 22/03/2022, às 21:14, conforme art. 2º, § 2º, III, "b", da Lei 17.039/2010 e art. 3ºB, I, do Decreto nº 8.808/2016.

Documento assinado eletronicamente por **CLEBER GIUGIOLI CARRASCO**, **Docente de Ensino Superior**, em 23/03/2022, às 08:41, conforme art. 2º, § 2º, III, "b", da Lei 17.039/2010 e art. 3ºB, I, do Decreto nº 8.808/2016.

A autenticidade do documento pode ser conferida no site **http://sei.go.gov.br/sei/controlador_externo.php?**

acao=documento_conferir&id_orgao_acesso_externo=1 informando o código verificador **000028533913** e o código CRC **BCC92D44**.

COORDENAÇÃO SETORIAL MATEMÁTICA ANÁPOLIS
RODOVIA BR 153 S/Nº - Bairro ZONA RURAL - CEP 75132-903 - ANAPOLIS - GO
0- QUADRA ÁREA KM 99 (62)3328-1139

Referência: Processo nº 202200020004306 SEI 000028533913

Dedico este trabalho a Deus que com sua infinita graça me guiou
e me sustentou até aqui. Aos meus pais que me deram suporte e
me apoiaram com muito amor durante toda a minha vida.
Aos meus amigos que caminharam comigo nessa jornada.
E a todos aqueles que, de alguma forma,
possibilitaram a minha caminhada até aqui.

AGRADECIMENTOS

Agradeço primeiramente a Deus, que com sua infinita graça, até aqui me sustentou, me dando fé, coragem e perseverança nos momentos mais difíceis.

Aos meus pais por sempre me apoiarem com muito amor e investirem em meus estudos, possibilitando que eu chegasse até aqui.

Ao meu namorado, Daniel Israel Moreira, que viveu esta jornada acadêmica juntamente comigo e sempre me incentivou e apoiou com muito carinho em todos os momentos.

Aos meus amigos, Aline, José Eduardo, Lillian, Lucas Piedade, Nicolas, Sara, Vanessa e Welder que me apoiaram e caminharam comigo. Obrigada por me ajudarem, me ouvirem e por me presentearem com uma amizade tão linda, a qual espero levar por toda vida.

À minha orientadora, professora Dra. Selma Marques de Paiva, que acreditou no meu potencial, me orientou e me incentivou.

Aos professores que contribuíram para a minha formação acadêmica e que dedicaram o seu tempo a ensinar com excelência.

À Universidade Estadual de Goiás e aos seus servidores por propiciarem uma formação acadêmica de qualidade.

"Os matemáticos nunca param de fazer uma coisa só porque é impossível. Se for muito interessante, eles acham meios de torná-la possível."

(Ian Stewart)

RESUMO

Este trabalho tem a pretensão de abordar a história dos números primos e investigar suas origens, dando ênfase aos vestígios que mostram o uso desses números há mais de vinte mil anos. Far-se-á um levantamento histórico acerca dos primeiros matemáticos que estudaram esses números, retratando algumas de suas descobertas referentes à teoria dos números. Além disso, discorreremos brevemente sobre o uso da abordagem histórica no ensino dos números primos, com o intuito de estimular a criatividade dos educadores e favorecer o despertar da curiosidade de seus alunos pela Matemática. Esta investigação tem por finalidade elucidar o contexto histórico enredado pela jornada dos números primos em algumas etapas da sociedade humana. Sendo assim, para uma compreensão matemática mais aprofundada quanto a esses números, vamos destacar algumas definições, propriedades e particularidades relacionadas ao assunto, juntamente com a revisão de conteúdos fundamentais para a compreensão dos mesmos. Na tentativa de evidenciar a importância dos números primos, algumas aplicações serão mostradas. No tocante à criptografia, daremos ênfase à sua origem e relevância no cotidiano. Um interessante estudo relacionado às cigarras periódicas será trabalhado tendo em vista sua íntima ligação com os números primos, essenciais para sua sobrevivência.

Palavras-chave: Criptografia. Matemática. Teoria dos números.

LISTA DE ILUSTRAÇÕES

Figura 1.1 – Osso de Ishango 24
Figura 1.2 – Desenho dos dois lados do Osso de Ishango mostrando os entalhes 25
Figura 2.1 – Distribuição dos números primos de 1 a 100 em uma reta numérica 52
Figura 3.1 – Ciclo de vida de cigarras periódicas de 7 e 13 anos 67
Figura 3.2 – Ciclo de vida de cigarras periódicas de 6 e 12 anos 68

LISTA DE TABELAS

Tabela 1 – Lista de números primos gerada por $f(n)$ 54
Tabela 2 – Maiores números primos com algarismo inicial d, seguido de n algarismos 9 57
Tabela 3 – Tempo médio para quebrar o código RSA 66

SUMÁRIO

Sumário **19**

INTRODUÇÃO **21**

1 ABORDAGEM HISTÓRICA DOS NÚMEROS PRIMOS **23**

1.1 De onde vêm os primos? **23**

1.2 Precursores dos números primos **26**

1.2.1 Euclides de Alexandria 26

1.2.2 Diofanto de Alexandria 27

1.2.3 Pierre de Fermat 29

1.2.4 Leonhard Euler 30

1.2.5 Carl Friedrich Gauss 31

1.3 Abordagem histórica no ensino dos números primos **31**

2 OS NÚMEROS PRIMOS **35**

2.1 Múltiplos e divisores **35**

2.1.1 Algoritmo de Euclides 36

2.1.2 Máximo divisor comum 37

2.1.3 Mínimo múltiplo comum 41

2.1.4 Congruência 43

2.2 Números primos e suas propriedades **45**

2.3 Como reconhecer que um número é primo? **48**

2.4 Como encontrar números primos? **52**

2.4.1 Algumas tentativas de gerar números primos 53

2.5 Tipos de números primos e algumas curiosidades **56**

3 APLICAÇÕES DE NÚMEROS PRIMOS **59**

3.1 Criptografia **59**

3.1.1 Criptografia RSA 61

3.2 As cigarras periódicas **66**

CONSIDERAÇÕES FINAIS **71**

REFERÊNCIAS **73**

APÊNDICES **75**

APÊNDICE A – CONJECTURA DE GOLDBACH 77

APÊNDICE B – HIPÓTESE DE RIEMANN 79

INTRODUÇÃO

O estudo dos números primos é uma das partes mais fundamentais da Matemática e desde sempre prende a atenção e causa o fascínio de diversos matemáticos. Sabe-se que os números primos $(2, 3, 5, 7, 11, 13, 17, 19, 23, 29, \ldots)$ são capazes de gerar os demais números naturais, com exceção do 1 (um), e seus únicos divisores positivos são 1 e eles mesmos. Segundo Sautoy (2008), eles podem ser considerados os átomos da aritmética e uma lista contendo todos os primos (lembrando que não é possível conter todos, já que são infinitos) seria considerada a tabela periódica do matemático. Tal comparação se deve ao fato conhecido de que cada molécula do mundo físico pode ser composta por átomos da tabela periódica de elementos químicos.

Dignos de encantamento e contemplação, os números primos, apesar de serem objetos estimados do mundo da Matemática, possuem diversos enigmas matemáticos que os envolvem. Basta observar a sequência dos primeiros números primos para perceber que o surgimento deles é totalmente aleatório e não traz consigo nenhuma dica de como determinar seus sucessores.

Qual seria a fórmula para desvendar esse enigma e definir uma regra geradora de qualquer número primo? Quantos números primos existem? Como os demais números são gerados pelos primos? Essas são perguntas que têm instigado os matemáticos de todas as épocas e eles não aceitam a ideia de que para algumas delas não existem respostas. Certamente continuarão causando a agitação dos interessados e aguçando a mente dos curiosos. “A aleatoriedade e o caos são anátemas para o matemático” (SAUTOY, 2008, p. 15)

A área da Matemática que estuda os números primos é chamada de Teoria dos Números. Todavia, ainda que eles ocupem papel fundamental, nem sempre é dado a eles seu devido valor. A pretensão de abordar parte da teoria dos números primos e mostrar algumas de suas aplicações, evidenciando a matemática presente no dia-a-dia e a sua essencial importância, é nosso objetivo maior.

A procura pela compreensão dos enigmas matemáticos que envolvem os primos conduziu a criação de vários procedimentos e hipóteses, os quais essa pesquisa pretende perscrutar. Além disso, faremos uma abordagem histórica sobre esses números junto a várias curiosidades peculiares com o propósito de inspirar os educadores na introdução do conteúdo de números primos e cativar a motivação dos alunos pelo interesse à matemática.

Sautoy (2008) referiu-se aos primos como uma dádiva da natureza para o matemático. Contudo, este trabalho possui o objetivo de evidenciar que os números primos não são um presente designado apenas aos matemáticos.

Para uma melhor compreensão acerca do mundo dos números primos, este trabalho encontra-se dividido em três capítulos. No primeiro apresentaremos a origem desses números,

dando ênfase a alguns vestígios encontrados que nos levam a crer na tese de que o ser humano já tinha o conhecimento dos primos há mais de 20.000 anos. Faremos também um levantamento histórico acerca de alguns matemáticos que se embrenharam nos estudos desses números e, para completar, citaremos algumas das descobertas referentes à teoria dos números que culminaram em certos questionamentos que não foram desvendados até o presente momento. Importante ressaltar também, ainda que brevemente, sobre o uso da história da matemática no ensino dos números primos.

O segundo capítulo se encarregará de expor o conteúdo dos números primos de uma maneira mais formal, apresentaremos nele uma revisão de conteúdos como múltiplos e divisores, máximo divisor comum, mínimo múltiplo comum e congruência, que são fundamentais para o entedimento das especificidades dos números primos, posteriormente, destacaremos algumas definições, propriedades, demonstrações e particularidades.

Passados os tópicos anteriores, chegamos ao terceiro capítulo que se dedica ao propósito de mostrar algumas aplicações dos números primos, falaremos também a respeito da importância da criptografia, bem como sua origem.

Os números primos não são elementos matemáticos puramente abstratos, de fato, podemos encontrar e até mesmo utilizar esses números em nosso cotidiano. Por exemplo, no método criptográfico RSA, eles servem para garantir a segurança na transmissão de informações, que são reproduzidas intencionalmente de maneira incompreensível. Durante uma guerra as mensagens transmitidas são encriptografadas e protegidas por códigos para que o inimigo não consiga decifrar as estratégias militares. Da mesma forma que uma pessoa física, ao utilizar seu cartão de crédito, para fazer uma compra *online*, tem seus números e senha protegidos de roubo por meio da criptografia.

Por fim, ainda com o intuito de evidenciar a importância dos primos em nosso cotidiano, citaremos no último tópico do terceiro capítulo o caso das cigarras periódicas, insetos que dependem da lógica desses números para sua sobrevivência.

1 ABORDAGEM HISTÓRICA DOS NÚMEROS PRIMOS

Neste capítulo abordaremos sobre a origem dos números primos dando ênfase aos primeiros vestígios encontrados que levam a crer que o ser humano já tinha o conhecimento deles há mais de 20.000 anos. Também será feito um levantamento histórico acerca dos primeiros matemáticos que estudaram esses números. Além disso, serão retratadas algumas das descobertas referentes à teoria dos números que culminaram em certos questionamentos que não foram desvendados até o presente momento. Por fim, discorreremos brevemente sobre o uso da história da matemática no ensino dos números primos.

Esta abordagem tem por finalidade elucidar o contexto histórico enredado pela jornada dos números primos em algumas etapas da sociedade humana, com o intuito de estimular a criatividade dos educadores no ensino do conteúdo de números primos e também favorecer o despertar da curiosidade de seus alunos pela Matemática. Sendo assim, para uma compreensão matemática mais aprofundada quanto a esses números, iremos tratar posteriormente das definições e propriedades relacionadas ao assunto.

1.1 De onde vêm os primos?

Para desvendar por completo (se é que podemos dizer assim) as origens dos números primos seria necessário, primeiramente, investigar o desenvolvimento intelectual do ser humano ao longo da história e descobrir o momento em que o homem tomou consciência do significado do número. Contudo, descobrir de maneira exata o instante em que o homem tornou-se conhecedor da matemática seria uma tarefa praticamente impossível e, de acordo com Boyer (2012), os vestígios matemáticos são geralmente encontrados em culturas primitivas, o que torna a interpretação de sua significância ainda mais complexa.

> Noções primitivas relacionadas com os conceitos de número, grandeza e forma podem ser encontradas nos primeiros tempos da raça humana, e vislumbres de noções matemáticas se encontram em formas de vida que podem datar milhões de anos antes da humanidade (BOYER, 1974, p. 1).

Por mais que existam incertezas entre os historiadores quanto ao surgimento da matemática, conforme Boyer (1974), é improvável que apenas um indivíduo ou povo a tenha descoberto, é mais provável que ela tenha surgido de maneira gradual e o seu desenvolvimento pode ser tão antigo quanto o manuseio do fogo, há aproximadamente 300.000 anos.

Boyer (1974) apresenta duas teorias quanto à origem da Matemática, uma delas pensada por Heródoto e outra por Aristóteles, um acreditava que os instintos numéricos surgiram da necessidade de realizar tarefas básicas do cotidiano e o outro que a matémática havia surgido a partir do lazer sacerdotal e ritual. Nenhuma das teorias, por mais que sejam opostas, podem ser refutadas cientificamente, no entanto é notável o quanto a origem dos números é capaz de ser subestimada. "Podemos fazer conjecturas sobre o que levou os homens da Idade da Pedra a contar, medir, e desenhar. Que os começos da matemática são mais antigos que as mais antigas civilizações é claro" (BOYER, 1974, p. 5).

Assim como o primeiro vínculo entre o ser humano e a Matemática, o conhecimento dos números primos pode ser mais antigo que muitas civilizações. Segundo Sautoy (2008), a primeira indicação de que o homem havia descoberto o número primo foi encontrada nas montanhas da África Central Equatorial e é chamada de Osso de Ishango, um osso de babuíno com entalhes de números primos que, segundo Santos (2019), possui idade estimada de 20.000 anos.

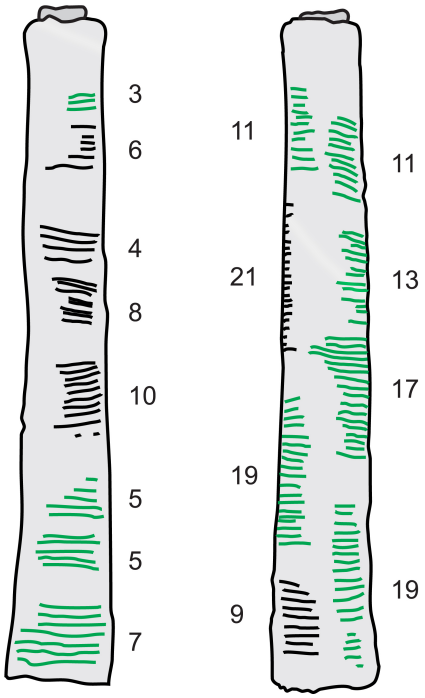
Figura 1.1 – Osso de Ishango

Fonte: Santos (2019, p. 123).

Apesar do Osso de Ishango não provar que o homem já possuía a consciência da primalidade é evidente que em sua superfície há a representação de números primos. De acordo com Santos (2019), este artefato é apontado como o objeto matemático mais antigo e tem-se revelado um enigma para aqueles que se dedicam a desvendá-lo.

Há diversas interpretações acerca da utilidade do Osso de Ishango (ver Figura 1.1), porém suas marcas gravadas de maneira assimétrica levam a crer que ele não era apenas um objeto decorativo, Crevecouer et al., conforme citado por Santos (2019), conclui que esses entalhes tratam-se de representações matemáticas.

Figura 1.2 – Desenho dos dois lados do Osso de Ishango mostrando os entalhes



Fonte: Elaborado pela autora a partir de Pejlare e Bräting (2019).

Como pode-se ver na Figura 1.2, os entalhes em verde representam os números primos, os quais podem ser reunidos no seguinte conjunto: $I = \{3, 5, 7, 11, 13, 17, 19\}$, logo, sem contar as repetições, tem-se a representação de 7 números primos. Stewart (2014) acredita que esses padrões possam ter sido entalhados aleatoriamente, no entanto, ressalta que talvez haja algumas possibilidades de significação, como a de um calendário lunar.

Inicialmente, alguns estudiosos, consideravam que o osso de Ishango poderia ter sido usado apenas para contagem, mas conforme Pejlare e Bräting (2019) menciona De Heinzelin, os agrupamentos de números gravados sugerem mais que isso, pois esses padrões numéricos podem denotar um entendimento de aritmética simples, como pode-se observar na Figura 1.2, os quatro primeiros grupos de entalhes, representados por 3 e 6, 4 e 8, mostram a possível noção do conceito de dobro, ou seja: $3 \cdot 2 = 6$ e $4 \cdot 2 = 8$.

Os vestígios matemáticos encontrados não conseguem provar que o ser humano possuía noção formal de números primos há 20.000 anos, no entanto, mesmo que de maneira rudimentar ou utilitária, é possível perceber por intermédio do Osso de Ishango que havia um conhecimento acerca desses números. Sabe-se que para existir uma noção formal de números primos seria necessário o entendimento do conceito de divisão e, segundo Pejlare e Bräting (2019), não há indícios que nessa época o ser humano tinha essa compreensão.

Por fim, é plausível dizer que a noção formal de números primos só viria mais tarde com

o desenvolvimento de outros conceitos matemáticos mais profundos. No entanto, fundamentando-se nos indícios históricos, verifica-se que é inegável a presença da matemática e, mais especificamente, dos números primos no cotidiano do homem de milhares de anos atrás.

1.2 Precursores dos números primos

Mesmo passados 20.000 anos dos primeiros vestígios de números primos no cotidiano do homem, é possível perceber que não foi perdido o interesse por eles, mas sim o oposto, deu-se início a questionamentos cada vez mais perspicazes. Logo, para o surgimento de dúvidas bem elaboradas foi preciso um certo aprofundamento dos conceitos matemáticos e para responder às indagações propostas foi necessário o desenvolvimento de algumas técnicas mais refinadas. Em razão disso, apresentamos a seguir os principais colaboradores no estudo dos números primos.

1.2.1 Euclides de Alexandria

Euclides de Alexandria (325-270 a.C) é conhecido por esse nome por ter sido chamado por Alexandre, O Grande, para lecionar em Alexandria. Ele viveu no Egito helenístico, porém seu local de nascimento, de acordo com Boyer (1974), é desconhecido e, comparado a grandiosidade de seu trabalho, sabe-se pouco sobre os detalhes de sua vida.

A sua produção mais conhecida é nomeada *Os Elementos*, um dos escritos de maior repercussão na história da Matemática e, como Pickover (2009) afirma, mesmo que ele não fosse o primeiro a realizar algumas das provas publicadas em seu livro, a sua organização e estilos claros tornaram seu trabalho de significado duradouro, servindo de inspiração para muitos matemáticos. A primeira impressão foi feita em 1482 e, desde então, mais de 1000 edições já foram lançadas.

A obra *Os Elementos* causou tanto impacto na vida de alguns estudiosos que, de acordo com Pickover (2009), influenciou intensamente cientistas como Galileu[1] e Newton[2], além do filósofo Bertrand Russel[3] que compara o estudo da obra *Os Elementos* ao primeiro amor,

[1] Galileu Galilei (1564-1642) nasceu em Pisa e iniciou sua vida acadêmica estudando medicina, mas, assim que conseguiu aprovação para mudar o rumo de sua carreira, dedicou-se à ciência e à matemática. Suas descobertas e invenções apresentavam um toque de harmonia entre a teoria e a prática, dentre elas: ele inventou o microscópio moderno e o compasso de setores, compreendeu a equipotência de conjuntos infinitos (fundamental na teoria dos conjuntos de Cantor), além disso, ele foi o primeiro a identificar a natureza parabólica da trajetória de um projétil no vácuo (EVES, 2011).

[2] Isaac Newton (1642-1727) nasceu em Woolsthorpe, coincidentemente, no ano do falecimento de Galileu. Desde cedo, Newton revelou sua criatividade e inteligência inventando miniaturas mecânicas, como um relógio movido a água e um moinho de brinquedo que triturava trigo. Seus talentos propiciaram sua permanência nos estudos, até que, aos 18 anos, em Cambrigde, por meio de um livro de astrologia, a matemática ganhou seu coração. Ele é considerado um dos maiores matemáticos do mundo, responsável por inúmeras descobertas, dentre elas: as leis da natureza, conhecidas como Leis de Newton, e, o método dos fluxos (EVES, 2011).

[3] "Bertrand Arthur William Russell (1872-1970) nasceu perto de Trelleck, País de Gales. Ganhador de uma bolsa de estudos pública no Trinity College, Cambridge, foi aluno de Whitehead e distinguiu-se notavelmente em matemática e filosofia. Além de lecionar amplamente em universidades americanas, escreveu mais de 40 livros, entre matemática, lógica, filosofia, sociologia e educação" (EVES, 2011, p. 679).

descrevendo a experiência como a sensação mais deleitável do mundo.

Boyer (1974) relata que metade do que Euclides escreveu perdeu-se, mas que seus cinco livros sobreviventes são os tratados gregos mais antigos, sendo eles: *Os Elementos, Os Dados, Divisão das figuras, Os fenômenos* e *Óptica*. Nenhuma descoberta é atribuída a ele, porém era conhecido pela sua habilidade de transmitir conhecimento, e essa foi uma das razões de ele ter se tornado tão famoso.

> *Os Elementos* de Euclides superaram de tanto seus competidores que foram os únicos a sobreviver. Não eram, como se pensa às vezes, um compêndio de todo o conhecimento geométrico; ao contrário, trata-se de um texto introduzido cobrindo toda a matemática *elementar* - isto é, aritmética (no sentido de "teoria dos números"), geometria sintética (de pontos, retas, círculos e esferas), e álgebra (não no sentido simbólico moderno, mas um equivalente em roupagem geométrica) (BOYER, 1974, p.76).

Os Elementos é um conjunto de livros formado por 13 volumes (ou capítulos) - os seis primeiros falam sobre geometria elementar, o VII, VIII e o IX tratam-se de teoria dos números, o de número X fala sobre incomensuráveis e o XI, XII e XII discorrem sobre a geometria tridimensional.

Segundo Boyer (1974), o primeiro livro dedicado à teoria dos números trabalha com conceitos e diferenças entre os seguintes tipos de números: ímpares e pares, primos e compostos, planos e sólidos e o número perfeito. A linguagem das demonstrações utilizadas por Euclides pode causar estranheza aos matemáticos modernos, pois ele fazia provas que pareciam "álgebra disfarçando-se de geometria", exemplo disso: a representação de um número inteiro por um segmento de reta, podendo ser chamado de número *AB*, ou mesmo o uso dos termos "é medido por"e "mede respectivamente"no lugar de "é um múltiplo de"ou "é um fator de".

Os livros VII, VIII e IX também trazem conceitos relativos ao máximo divisor comum (algoritmo de Euclides), mínimo múltiplo comum, algumas proposições e teoremas - dentre eles a prova de que existem infinitos números primos, demonstrada de maneira indireta, ou seja, a hipótese de que há uma quantidade finita de números primos que leva a uma contradição.

Nenhuma outra obra matemática conseguiu ter a mesma influência que *Os Elementos*, chegando a ser comparado por Boyer (1974) com a Bíblia pela sua quantidade de edições e por ter sido tão usado e estudado. Essa obra foi concebida por volta de 300 a.C., no entanto, a lógica de Euclides é admirada até os dias atuais, dada a sua importância.

1.2.2 Diofanto de Alexandria

Não há muitas informações a respeito da vida de Diofanto (200-284), a não ser pelo seguinte enigma encontrado em uma coleção de problemas chamada "Antologia Grega", que retratam os escritos em seu túmulo:

> Deus lhe concedeu ser um menino pela sexta parte de sua vida, e somando uma duodécima parte a isso cobriu-lhe as faces de penugem; Ele lhe acendeu a lâmpada nupcial após uma sétima parte, e cinco anos após seu casamento concedeu-lhe um filho. Ai! infeliz criança tardia; depois de chegar à medida de metade da vida de seu pai, o Destino frio o levou. Depois de se consolar de sua dor durante quatro anos com a ciência dos números ele terminou sua vida (BOYER, 1974, p. 130).

De acordo com esse enigma a idade de Diofanto ao morrer será considerada como a incógnita x, analogamente, os seguintes dados podem ser retirados:

$$\frac{x}{6} = \textit{infância}$$
$$\frac{x}{12} = \textit{adolescência}$$
$$\frac{x}{7} = \textit{casamento}$$

5 anos após o casamento nasceu seu filho

$$\frac{x}{2} = \textit{tempo que seu filho viveu}$$

Diofanto dedicou sua vida aos números por 4 anos antes de sua morte

A solução para esse problema leva a uma equação do primeiro grau.

$$x = \frac{x}{6} + \frac{x}{12} + \frac{x}{7} + 5 + \frac{x}{2} + 4$$
$$x - \frac{x}{6} - \frac{x}{12} - \frac{x}{7} - \frac{x}{2} = 9$$
$$\frac{84x - 14x - 7x - 12x - 42x}{84} = 9$$
$$9x = 9 \cdot 84$$
$$\not{9}x = \not{9} \cdot 84$$
$$x = 84$$

$\therefore$ *Diofanto morreu aos 84 anos.*

Esse matemático grego, conforme Eves (2011), viveu por volta do século III e ficou conhecido como o pai da álgebra por conta de sua principal obra *Arithmetica*, que foi produzida por volta do ano 250 e com seis livros sobreviventes dos treze que foram escritos. A parte que sobreviveu trata-se da resolução de 130 problemas matemáticos relacionados a equações do primeiro e do segundo grau, e às vezes de grau maior, com duas ou três incógnitas.

O trabalho de Diofanto ficou conhecido por sua dedicação à álgebra e por ter influenciado fortemente aqueles que posteriormente iriam empenhar-se na teoria dos números. Pickover (2009) conta que ele estava interessado em encontrar soluções inteiras para as equações da forma $ax + by = c$, as quais foram chamadas equações diofantinas em honra a seu nome. No entanto, Eves (2011) afirma que os problemas encontrados em *Arithmetica* (também chamados "problemas diofantinos") procuram soluções racionais positivas e que a restrição aos inteiros é um uso moderno.

Diofanto também produziu outras duas obras: "Sobre números poligonais"e "Porismas", além de ser considerado um matemático muito importante pelo seu progresso em notações matemáticas[4] e pelo seu tratamento de frações como números.

1.2.3 Pierre de Fermat

Pierre de Fermat (1601?-1665)[5], conforme Eves (2011) relata sua história, nasceu em Beuamont de Lomagne, comunidade francesa próxima à Toulose e era de uma família afortunada. Seus pais o proporcionaram uma boa educação que o levou a escolher e seguir a profissão de advogado e, mesmo sendo um amante da Matemática, ele a deixou reservada apenas para os momentos de lazer.

Apesar da matemática não ter ocupado o lugar principal em sua carreira profissional, foi ela quem trouxe o conhecimento de seu nome ao mundo. As contribuições de Fermat estão ligadas à teoria matemática das probabilidades, cálculo infinitesimal e teoria dos números, mas seus maiores feitos estão relacionados à última opção, sendo chamado por Boyer (1974) de fundador da moderna teoria dos números. Também foi autor de muitos teoremas, dentre os mais conhecidos estão o chamado *Pequeno Teorema de Fermat*[6] e *o "Último" Teorema de Fermat* (também chamado de *"Grande"*).

Segundo Stewart (2014), após Diofanto, a teoria dos números permaneceu sem evoluções por mais de mil anos e só saiu de sua condição de inércia por causa das várias descobertas de Fermat. Ele correspondia-se com vários outros matemáticos e os desafiava com os problemas que ele criava e, mesmo que não tenha feito muitas publicações em vida, por conta de sua influência, segundo Eves (2011), estima-se que tenha sido o maior matemático francês do século XVII.

Acredita-se, de acordo com Eves (2011), que as contribuições mais importantes de Fermat para a teoria dos números sejam provenientes da influência de Diofanto, mais especificamente, sua obra *Arithmetica* (versão traduzida por Bachet de Méziriac em 1621), pois muitas

[4] "Diofanto tinha abreviações para a incógnita, potências da incógnita até a de expoente seis, subtração, igualdade e inversos" (EVES, 2011, p. 210).

[5] "Em sua laje tumular, originalmente na igreja dos agostinianos em Toulouse e depois transferida para o museu local, consta a data precedente como a da morte de Fermat, com 57 anos de idade. Devido a esse conflito de datas costuma-se escrever (1601?-1665) para nascimento e morte de Fermat. De fato, por várias razões, seu ano de nascimento, a julgar pelas informações de vários escritores, varia de 1590 a 1608" (EVES, 2011, p. 389-390).

[6] "Se $p > 1$ é um número primo que não divide o inteiro a, então: $a^{p-1} \equiv 1(mod\ p)$" (DOMINGUES, 1991, p. 144).

de suas descobertas foram encontradas escritas na margem de um livro desses. Inclusive, o tão famoso *Último Teorema de Fermat*[7] foi enunciado por ele em seu exemplar da *Arithmetica* de Diofanto.

O último "teorema" de Fermat fez com que muitos matemáticos se esforçassem para chegar à resposta do problema, Pickover (2009) afirma que tornou-se paixão para alguns mas teria levado outros ao engano e insanidade. Por essas razões ele ganhou a fama de ser o problema matemático com a maior quantidade de provas incorretas já publicadas. Porém, em 1995, soube-se que o *Grande Teorema de Fermat* era mesmo um teorema, quando o matemático Andrew Willes publicou a primeira demonstração provando que não existem inteiros positivos x, y, z que satisfaçam a equação $x^n + y^n = z^n$, quando $n > 2$. Dessa forma, após 350 anos, a prova desse último teorema pensado por Fermat juntou-se aos muitos outros que já foram demonstrados como verdadeiros.

1.2.4 Leonhard Euler

Leonhard Euler (1707-1783), conforme sua história é relatada por Eves (2011), nasceu na cidade de Basileia, Suíça e intencionou-se à teologia como carreira, mas acabou decidindo-se pelos encantos da matemática. Seu pai era um pastor calvinista que também possuía afeição pela matemática então pôde ajudar a seu filho ensinando-o. Além disso, ele também conseguiu que Euler estudasse com Johann Bernoulli[8] já que ele havia estudado com Jakob Bernoulli.

No ano de 1735 Euler já era cego de seu olho direito, o que pode explicar a maneira com que ele pousava para as fotografias. Após o ano de 1766 ele ficou completamente cego, mas esse infortúnio não o impediu de ser produtivo. Ele possuía uma memória incrível e todas as suas criações eram anotadas pelo seu secretário, chegando a fazer 530 publicações em vida, o que torna impossível fazer aqui a exposição de cada um de seus trabalhos escritos.

As contribuições de Euler foram numerosas e de grande valor para a matemática, por isso é tão comum a grande quantidade de matemáticos que se sentiram ou sentem-se influenciados por ele. É muito difícil encontrar uma especialidade da matemática em que Euler não tenha contribuído de alguma forma. Na teoria dos números por exemplo, encontra-se o *Teorema de Euler*[9] e a *função φ de Euler*[10].

O físico e astrônomo François Arago(1786-1853) diz que "Euler calculava sem nenhum esforço aparente, assim como os homens respiram e as águias se mantêm suspensas no ar". Mas

[7] Na nota marginal de Fermat lê-se, "Dividir um cubo em dois cubos, uma quarta potência ou, em geral uma potência qualquer em duas potências da mesma denominação acima da segunda é impossível, e eu seguramente encontrei uma prova admirável desse fato, mas a margem é demasiado estreita para contê-la" (EVES, 2011, p. 391). É devido a esse fato que não há certeza sobre Fermat ter demonstrado corretamente esse teorema.

[8] A família Bernoulli era destaque no ramo da Matemática.

[9] "Para todo inteiro $m > 1$ e para todo $a \in \mathbb{Z}$ vale a congruência: $a^{\varphi(m)} \equiv 1 (mod\ m)$" (DOMINGUES, 1991, p. 143).

[10] "A função $\varphi : \mathbb{N}^* \to \mathbb{N}^*$ que associa a cada $m \in \mathbb{N}^*$ o número de elementos do conjunto $\{k \in \mathbb{N}^* | 1 \leq k \leq m$ e $mdc(k,m) = 1\}$ é chamada *função φ de Euler*" (DOMINGUES, 1991, p. 143).

seu conhecimento estendia-se além da Matemática e da Física, abrangendo também a astronomia, medicina, botânica, química, teologia e as línguas orientais.

1.2.5 Carl Friedrich Gauss

Carl Friedrich Gauss (1777-1855), de acordo com a descrição de Eves (2011), nasceu em Brunswick, Alemanha. Sua genialidade contribuiu para que fosse notado pelo duque de Brunswick que o ajudou a ingressar no *Collegium Carolinum de Brunswick* e na Universidade de Göttingen, onde, aos 18 anos de idade, tomou sua decisão definitiva pela Matemática.

Com apenas três anos de idade Carl começou a mostrar o seu talento matemático ao corrigir um erro aritmético de seu pai. Aos dez anos de idade, cumpriu rapidamente o desafio de seu professor que pedia o resultado da soma de todos os números inteiros de 1 a 100. Seu raciocínio surgiu da observação que $100+1=101$, $99+2=101$, e assim por diante, totalizando 50 pares com soma igual a 101, ou seja, para resolver a seguinte progressão aritmética $1+2+3+4+5+\cdots+99+100$ basta multiplicar 50 por 101, totalizando 5050.

Aos 18 anos, Gauss descobriu como realizar a construção euclidiana de um polígono regular de 17 lados, e a partir desse momento, começou a registrar as suas produções matemáticas em seu diário, no entanto, não se preocupava em publicar suas produções. O diário matemático de Gauss só foi encontrado em 1898.

Gauss foi a primeira pessoa a demonstrar o *Teorema Fundamental da Álgebra*[11] corretamente. Essa prova foi escrita quando ele tinha 20 anos, em sua tese de doutorado. Outros grandes matemáticos como Newton, Euler, d'Alembert e Lagrange tentaram demonstrar esse teorema e falharam. Essa conquista de Gauss somada a muitas outras lhe rendeu o título de o "Príncipe dos Matemáticos".

Uma de suas publicações mais importantes é a *Disquisitiones Arithmeticae*, de grande relevância para a moderna teoria dos números. Nesse trabalho pode-se encontrar as suas construções de polígonos regulares. O intelecto de Gauss não se limitou ao ramo da Matemática, ele também contribuiu com a astronomia, geodésia e a eletricidade.

1.3 Abordagem histórica no ensino dos números primos

O ensino da matemática não é o objeto principal de estudo desta pesquisa, por isso não aprofundaremos a respeito desse assunto. No entanto, faremos uma breve análise quanto ao uso da história da matemática (HM) no ensino dos números primos.

O uso do contexto histórico no ensino dos números primos possui a pretensão de aprofundar os conhecimentos e chamar a atenção do aluno para a matemática, podendo caminhar

[11] "Uma equação polinomial complexa $f(x)=0$ de grau $n\geq 1$ tem pelo menos uma raiz complexa" (EVES, 2011, p. 477).

juntamente com a valorização do uso desses números na realidade em que o indíviduo encontra-se inserido.

Portanto, para que a história da matemática possa ser usada como um meio facilitador no ensino dos números primos ela precisa ser conhecida, e é por isso que este trabalho aborda diretamente a história dos números primos e suas aplicações. Logo, é imprescindível alertar o leitor, principalmente o docente, quanto à abordagem histórica de determinado conteúdo em sala de aula. Há professores que possuem uma ideia equivocada quanto ao uso da história no ensino da matemática, pois não basta apenas contar fatos históricos e promover um momento de descontração com os alunos. A história da matemática não pode ser considerada automotivadora, ela precisa cumprir o objetivo de levar o aluno à compreensão do conceito estudado, estimulando sua capacidade em desenvolver matemática.

Ensinar matemática não é uma tarefa fácil pois é necessário lidar com o seu estereótipo de vilã ou que o seu aprendizado é reservado apenas para aqueles que possuem aptidão. Para superar esses desafios o professor precisa buscar recursos metodológicos que consigam mostrar como a matemática é necessária à evolução do mundo e que o seu conhecimento é alcançável para qualquer estudante interessado e que tenha acesso à educação. De acordo com a Base Nacional Comum Curricular (BNCC), para o desenvolvimento das habilidades:

> [...] é importante incluir a história da Matemática como recurso que pode despertar interesse e representar um contexto significativo para aprender e ensinar Matemática. Entretanto, esses recursos e materiais precisam estar integrados a situações que propiciem a reflexão, contribuindo para a sistematização e a formalização dos conceitos matemáticos (BRASIL, 2018, p. 298).

A história da matemática permite a compreensão da evolução do conhecimento humano, desde a consciência de número às exigências linguísticas e simbólicas da matemática formal. Assim como é tratada na BNCC, ela não pode ser considerada de maneira isolada como se fosse um recurso mágico para ensinar matemática. No entanto, se for usada de maneira estratégica pode ser uma boa aliada do professor de matemática e daqueles alunos que estão abertos ao aprendizado. Embora os Parâmetros Curriculares Nacionais (PCN) do MEC não estejam mais em vigor, apresentam orientações pedagógicas pertinentes quanto ao uso da história da matemática e complementam de maneira mais específica e esclarecida do que na BNCC. Assim sendo,

> [...] essa abordagem não deve ser entendida simplesmente que o professor deva situar no tempo e no espaço cada item do programa de Matemática ou contar sempre em suas aulas trechos da história da Matemática, mas que a encare como um recurso didático com muitas possibilidades para desenvolver diversos conceitos, sem reduzi-la a fatos, datas e nomes a serem memorizados (BRASIL, 1998, p. 43).

De acordo com os PCN, conhecer a história da matemática e as heranças culturais de gerações passadas tem grande importância no aprendizado do aluno em abstrações matemáticas

e alguns porquês relacionados à construções numéricas (BRASIL, 1998). No caso dos números primos, por meio da análise da história, é possível perceber que o avanço tecnológico dependeu da evolução do estudo desses números e que a ampliação desse conhecimento está historicamente ligada à situações-problema do cotidiano, até mesmo por um simples calendário lunar.

O processo de ensino dos números primos pode ser facilitado pelo recurso à história da matemática, assim como na matemática em geral. O professor pode trabalhar com seus alunos de acordo com as circunstâncias em que se desenvolveram os primeiros conhecimentos sobre número primo. Como Magalhães (2021), "numa abordagem que trata de explorar o contexto histórico (necessidades, preocupações) no qual determinado conceito foi desenvolvido, para propor situações que levem os alunos a pensarem a respeito desses conceitos."(p. 94)

Ao usar a necessidade da época em que esses números foram descobertos ou que começaram a ser utilizados, o professor pode levar seus alunos a chegarem à conclusão sobre quem são os números primos. Podem ser propostas situações em que seja preciso dividir números naturais (dentre eles alguns primos e compostos) e, ao tentar realizar essas divisões, os educandos podem perceber que alguns números não podem ser divididos por outros além do 1 e eles mesmos. Assim sendo, a ideia da história pode contribuir para o aprendizado do conceito matemático de número primo e somente após essa descoberta, fatos históricos podem ser mostrados como curiosidade.

Outra estratégia de ensino, envolvendo a história dos números primos, que o professor pode fazer uso são as aplicações desses números (expostas na terceira parte deste trabalho). Além disso, o professor também pode trazer questionamentos, como: "o que pode ter propiciado o avanço da teoria dos números naquele determinado momento?"; ou "o que seria da nossa sociedade se esse avanço não tivesse ocorrido?". Por consequência, o professor poderá conseguir mediar uma conexão entre o aluno e o conhecimento matemático. Conforme os PCN:

> [...] ao mostrar necessidades e preocupações de diferentes culturas, em diferentes momentos históricos, ao estabelecer comparações entre os conceitos e processos matemáticos do passado e do presente, o professor cria condições para que o aluno desenvolva atitudes e valores mais favoráveis diante desse conhecimento (BRASIL, 1998, p. 42).

Como vimos anteriormente, a história da matemática pode ser utilizada de várias formas no ensino dos números primos, o mais importante é que essa estratégia seja bem pensada pelo docente. Ele deve refletir se o método a ser utilizado cumprirá o objetivo de auxiliar no aprendizado matemático significativo do aluno e não só como apresentação de fatos históricos isolados. Assim como Magalhães (2021, p. 97), "consideramos o aspecto motivador da HM não como simples artefato atrativo, mas como algo que surge de uma necessidade que leve o sujeito a agir".

Quando a ideia da história é usada em uma situação de ensino, como usar o contexto em que surgiu um determinado conteúdo para que o conceito matemático seja compreendido, ela

"pode esclarecer idéias matemáticas que estão sendo construídas pelo aluno, especialmente para dar respostas a alguns porquês e, desse modo, contribuir para a constituição de um olhar mais crítico sobre os objetos de conhecimento" (BRASIL, 1998, p. 43).

2 OS NÚMEROS PRIMOS

Os números primos podem ser considerados números simples, porém ocultam diversos mistérios que os tornam encantadores e envolventes aos olhos dos matemáticos e chegam a despertar a curiosidade até mesmo dos não-matemáticos. A maneira com que esses números são nomeados deriva-se da palavra *primus*, que em latim, significa primeiro, isso porque os antigos gregos dividiam os números em primários e secundários (compostos).

Neste capítulo discorreremos sobre os números primos de uma maneira mais formal. As definições, propriedades, demonstrações e particularidades acerca dos números primos aqui explicitadas serão expressas com base em Domingues (1991), Coutinho (2004), Sautoy (2008), Aires (2010), Spina (2014), Stewart (2014) e Burton (2016).

2.1 Múltiplos e divisores

Para que o leitor sinta-se mais familiarizado quanto ao conteúdo de números primos abordaremos, primeiramente, alguns conceitos referentes a múltiplos e divisores, que são imprescindíveis para a compreensão dos tópicos seguintes.

Definição 2.1. *Diz-se que um número natural* $\boldsymbol{a}$ *divide um número natural* $\boldsymbol{b}$ *se* $\boldsymbol{b = ac}$*, para algum* $\boldsymbol{c} \in \mathbb{N}$*. Neste caso diz-se também que* $\boldsymbol{a}$ *é divisor de* $\boldsymbol{b}$ *e que* $\boldsymbol{b}$ *é múltiplo de* $\boldsymbol{a}$*. Ou ainda que* $\boldsymbol{b}$ *é divisível por* $\boldsymbol{a}$*. Indicaremos por* $\boldsymbol{a \mid b}$ *o fato de* $\boldsymbol{a}$ *dividir* $\boldsymbol{b}$*; e se* $\boldsymbol{a}$ *não divide* $\boldsymbol{b}$*, escrevemos* $\boldsymbol{a \nmid b}$*.*

O símbolo | não deve ser confundido com o traço que representa fração, ou seja, $3 \mid 9$ é diferente de $\frac{3}{9}$ ou $\frac{9}{3}$. A fração indica um numeral e $3 \mid 9$ expressa uma relação particular entre 3 e 9 e lê-se "3 divide 9". Para que a diferença seja mais clara, podemos exemplificar $0 \mid 0$, uma relação que é verdadeira (pois $0 = 0 \cdot a, \forall a \in \mathbb{N}$), enquanto $\frac{0}{0}$ representa uma indeterminação. É válido também ressaltar que, se $b \neq 0$, então $0 \nmid b$ pois $0 \cdot c = 0 \neq b, \forall c \in \mathbb{N}$. Outro caso particular é que, se b for igual a 1, vale que $1 \mid a$ $(\forall a \in \mathbb{N})$ pois $a = 1 \cdot a$.

Exemplo 2.1. $6 \mid 18$ *pois* $18 = 6 \cdot 3 \Rightarrow 3 = 18 \div 6$*, sendo 3 chamado quociente de 18 por 6.*

Para a relação $a \mid b$ em $\mathbb{N}$ são válidas as seguintes propriedades:

I. $a \mid a, \forall a \in \mathbb{N}$, pois $a = a \cdot 1$; (reflexiva)

II. $a \mid b$ e $b \mid a \Rightarrow a = b$; (anti-simétrica)

III. $a \mid b$ e $b \mid c \Rightarrow a \mid c$; (transitiva)

IV. Se $a \mid b$ e $a \mid c$, então $a \mid (bx+cy),\ \forall x,y \in \mathbb{N}$;
Em particular: $a \mid b \Rightarrow a \mid bx, \forall x \in \mathbb{N}$;

Nota: Como consequência, temos que: $a \mid b$ e $a \mid c \Rightarrow a \mid (b+c)$.

V. Se $c \mid a,\ c \mid b$ e $a \leq b$, então $c \mid (b-a)$;

VI. Seja $a = b+c$ e suponhamos $d \mid b$. Então: $d \mid a \Longleftrightarrow d \mid c;\ (c = a-b)$

VII. Se $a \mid b$ e $b \neq 0$, então $a \leq b$.

O conjunto de múltiplos de um de número a pode ser chamado M_a. Dessa forma $M_a = \{0,\ a,\ 2a,\ 3a,\ 4a, \ldots\}$. Especialmente, se $a = 0$, então $M_0 = \{0\}$ e se $a = 1$, então $M_1 = \{\mathbb{N}\}$. Os conjuntos $M_2 = \{0,\ 2,\ 4,\ 6, \ldots\}$ e seu complementar $\mathbb{N} - M_2 = \{1,\ 3,\ 5, \ldots\}$ são, respectivamente, os "números naturais pares"e "números naturais ímpares".

2.1.1 Algoritmo de Euclides

O algoritmo da divisão de Euclides diz que "Para quaisquer $a,\ b \in \mathbb{N},\ b \neq 0$, existe um único par de números $q, r \in \mathbb{N}$, de maneira que $a = bq + r\ (0 \leq r < b)$". Por meio desse método é possível representar a divisão de dois números naturais a e b, ainda que b não seja um múltiplo de a. Os elementos a, b, q e r são chamados, respectivamente, dividendo, divisor, quociente e resto da divisão de a por b.

Exemplo 2.2. *Iremos aplicar o algoritmo nos números* $\boldsymbol{a}$ =33 *e* $\boldsymbol{b}$ = 7.

$7 \cdot 4 < 33 < 7 \cdot (4+1)$. Logo, $q = 4$ e $r = 33 - 7 \cdot 4 = 5$. Isso explica o algoritmo

$$\begin{array}{r|l} 33 & 7 \\ \cline{2-2} -\ 28 & 4 \\ \cline{1-1} 5 & \end{array}$$

Exemplo 2.3. *Vamos explicar o algoritmo usual prático da divisão utilizando o algoritmo de Euclides. Calcularemos o quociente e o resto quando* $\boldsymbol{a}$ =331 *e* $\boldsymbol{b}$ =7.

Numa primeira etapa, quando se faz

$$\begin{array}{r|l} 331 & 7 \\ -\,28 & 4 \\ \hline 5 & \end{array}$$

na verdade o 4 que aparece sob a chave não passa do algarismo das dezenas do quociente procurado, como se pode constatar abaixo:

$$33 = 7\cdot 4 + 5 \text{ (algoritmo da divisão para 33 e 7)} \Rightarrow 330 = 7\cdot 40 + 50 \Rightarrow 331 = 7\cdot 40 + 51$$

Para atender ao algoritmo de Euclides é necessário que $0 \leq r < b$, como $51 > 7$, faremos o mesmo procedimento com os números 51 e 7:

$$51 = 7\cdot 7 + 2$$

Logo,

$$331 = 7\cdot 40 + 7\cdot 7 + 2$$

$$331 = 7\cdot 47 + 2.$$

Voltando ao algoritmo usual:

$$\begin{array}{r|l} 331 & 7 \\ -\,28 & 47 \\ \hline -\,51 & \\ -\,49 & \\ \hline 2 & \end{array}$$

2.1.2 Máximo divisor comum

Definição 2.2. *Sejam* $\boldsymbol{a}$, $\boldsymbol{b} \in \mathbb{N}$. *Um número* $\boldsymbol{d} \in \mathbb{N}$ *se diz máximo divisor comum de* $\boldsymbol{a}$ *e* $\boldsymbol{b}$ *se:*

i. $\boldsymbol{d} \mid \boldsymbol{a}$ *e* $\boldsymbol{d} \mid \boldsymbol{b}$*;*

ii. Se $\boldsymbol{c}$ *é um número natural tal que* $\boldsymbol{c} \mid \boldsymbol{a}$ *e* $\boldsymbol{c} \mid \boldsymbol{b}$*, então* $\boldsymbol{c} \leq \boldsymbol{d}$.

Indicaremos o máximo divisor comum de a e b pela seguinte notação: $mdc(a,\ b) = d$. A partir da definição temos que o valor do máximo divisor comum de a e b é único e que $mdc(a,\ b) = mdc(b,\ a)$.

Exemplo 2.4. *Sejam* $\boldsymbol{a}$ **=** *12 e* $\boldsymbol{b}$ **=** *16. Calcularemos o* **mdc (a, b)** *seguindo a Definição 2.2.*

Indicaremos por D_x o conjunto dos divisores de $x \in \mathbb{N}$, então

$$D_{12} = \{1,\ 2,\ 3,\ 4,\ 6,\ 12\} \quad \text{e} \quad D_{16} = \{1,\ 2,\ 4,\ 8,\ 16\}.$$

A partir disso, temos que:

$$D_{12} \cap D_{16} = \{1,\ 2,\ 4\}.$$

De acordo com a Definição 2.2:

i. $1 \mid 12$ e $1 \mid 16$; $2 \mid 12$ e $2 \mid 16$; $4 \mid 12$ e $4 \mid 16$;

ii. Se $c \mid 12$ e $c \mid 16$, então teremos como candidatos a $mdc(a,\ b)$, $c = 1$, $c = 2$ e $c = 4$. Como 4 é o maior valor, então o máximo divisor comum de 12 e 16 é 4.

Isto é,

$$mdc(12,\ 16) = 4.$$

Proposição 2.1. *Se* $\boldsymbol{a \mid b}$*, então* $\boldsymbol{mdc\ (a,\ b) = a}$.

Demonstração. Por hipótese, $a \mid a$ e $a \mid b$. E, se $c \mid a$ e $c \mid b$, então $c \mid a$. □

Proposição 2.2. *Se* $\boldsymbol{a = bq + r}$ *e* $\boldsymbol{d = mdc(a,\ b)}$*, então* $\boldsymbol{d = mdc(b,\ r)}$*. E se* $\boldsymbol{d = mdc(b,\ r)}$*, então* $\boldsymbol{d = mdc(a,\ b)}$.

Demonstração. ($\Rightarrow$) Por hipótese $mdc(a,\ b) = d$, logo $d \mid a$ e $d \mid b$.

$$d \mid a \ \text{ e } \ d \mid b \Rightarrow d \mid bq \Rightarrow d \mid (a - bq)$$

Se $a = bq + r$, então $r = a - bq$ e $d \mid r$. Pela Propriedade IV da Seção 2.1, se $c \mid b$ e $c \mid r$, então $c \mid (bq + r)$. Como $a = bq + r$, então $c \mid a$ e $c \mid b$. Visto que $mdc(a,\ b) = d$, teremos que $c \mid d$. Pela Definição 2.2, se $d \mid b$, $d \mid r$ e se $c \in \mathbb{N}$, tal que $c \mid b$ e $c \mid r$, então $c \mid d$ e o $mdc(b,\ r) = d$.

A demonstração da volta ($\Leftarrow$) pode ser feita de maneira análoga. □

Para encontrar o máximo divisor comum entre dois números naturais a e b podemos aplicar o "processo das divisões sucessivas"que consiste em realizar divisões sucessivas a partir de a e b até que se encontre resto zero. Assim, o último divisor será o valor do $mdc(a,\ b)$.

Exemplo 2.5. *Encontremos o* $\boldsymbol{mdc}(132, 60)$ *por meio do processo de divisões sucesssivas.*

Primeiramente faremos 132 dividido por 60.

132	60	

Como $132 = 60 \cdot 2 + 12$, preencheremos o quadro da seguinte maneira:

	2	
132	60	
12		

O quociente da divisão $132 \div 60$ ficará na célula acima do 60 (o divisor) e o resto 12 abaixo do 132 (o dividendo). Como ainda não obtivemos resto zero nessa divisão, continuaremos a repetir o processo, sendo 12 o próximo dividendo, ou seja, agora faremos $60 \div 12$.

	2	
132	60	12
12		

Temos que $60 = 12 \cdot 5$, portanto o resto será zero e o processo de divisões encerra-se.

	2	5
132	60	12
12	0	

O número 12 é o último divisor obtido pelo processo de divisões sucessivas.

$$\therefore mdc(132,\ 60) = 12.$$

Exemplo 2.6. *Encontremos o* $\boldsymbol{mdc}(49, 12)$ *por meio do processo de divisões sucesssivas.*

	4	12
49	12	1
1	0	

$$\therefore mdc(49,\ 12) = 1.$$

Definição 2.3. *Dois números naturais* ***a*** *e* ***b*** *se dizem primos entre si se* ***mdc(a, b) = 1****. Neste caso diz-se também que* ***a*** *é primo com* ***b*** *ou vice-versa.*

Exemplo 2.7. *Dois números consecutivos* ***b*** *e* ***b+1*** *são sempre primos entre si.*

De imediato, pode-se concluir que $1 \mid b$ e $1 \mid (b+1)$. Se $c \mid b$ e $c \mid (b+1)$, logo $c \mid [(b+1) - b] \Rightarrow c \mid 1$.

Proposição 2.3. *Se* ***d = mdc (a, b)****, então* ***mdc (sa, sb) = sd****, para todo* $\boldsymbol{s} \in \mathbb{N}$.

Demonstração. O processo de divisões sucessivas que levam a **d**, a partir de **a** e **b**, se dá da seguinte maneira:

$$a = bq_1 + r_1\ (r_1 < b)$$

$$b = r_1q_2 + r_2\ (r_2 < r_1)$$

$$r_1 = r_2q_3 + r_3 \ (r_3 < r_2)$$
$$\vdots$$
$$r_{n-2} = r_{n-1} \cdot q_n + r_n$$
$$r_{n-1} = r_n \cdot q_{n+1}$$

Ao multiplicar cada uma das igualdades por s, temos:

$$sa = (sb) \cdot q_1 + r_1$$
$$sb = (sr_1) \cdot q_2 + r_2$$
$$\vdots$$
$$sr_{n-2} = (sr_{n-1}) \cdot q_n + r_n$$
$$sr_{n-1} = (sr_n) \cdot q_{n+1}$$

As Proposições 2.1 e 2.2 implicam então que:

$$sd = sr_n = mdc(sr_{n-1},\ sr_n) = \ldots = mdc(sb,\ sr_1) = mdc(sa,\ sb).$$

□

Corolário 2.1. *Se* $\boldsymbol{a \mid bc}$ *e* $\boldsymbol{mdc(a,\ b) = 1}$*, então* $\boldsymbol{a \mid c}$.

Demonstração. Pela hipótese $mdc(a,\ b) = 1$. Pela Proposição 2.3

$$mdc(ac,\ bc) = c.$$

Como $a \mid ac$ e, por hipótese, $a \mid bc$, então $a \mid mdc(ac,\ bc)$, isto é, $a \mid c$. □

Corolário 2.2. *Se* $\boldsymbol{a}$ *e* $\boldsymbol{b}$ *são divisores de* $\boldsymbol{c \neq 0}$ *e* $\boldsymbol{mdc(a,\ b) = 1}$*, então* $\boldsymbol{ab \mid c}$.

Demonstração. Pela Proposição 2.3:

$$mdc(a,\ b) = 1 \Rightarrow mdc(ac,\ bc) = c$$

Como $a \mid c$ e $b \mid c$, podemos dizer que $ab \mid bc$. Logo ab divide $mdc(ac, bc)$, ou seja, $ab \mid c$. □

Exemplo 2.8. *Para que um número seja divisível por 12 basta que ele seja divisível por 3 e 4, simultaneamente, pois* $\boldsymbol{mdc}(3,\ 4) = 1$.

Generalização: A definição de máximo divisor comum pode ser facilmente utilizada para três ou mais números. Pode -se usar a seguinte resolução para executar o cálculo do máximo divisor comum entre três números:

$$mdc(a,\ b,\ c) = mdc(mdc(a,\ b),\ c) = mdc(a,\ mdc(b,\ c)).$$

Demonstração. Vamos provar a primeira igualdade. Seja $d = mdc(a,\ b,\ c) \Rightarrow d \mid a,\ d \mid b,\ d \mid c$. Dessas duas primeiras relações temos que: $d \mid mdc(a,\ b)$. Então $d \mid mdc(a,\ b)$ e $d \mid c$. Considere k um divisor de $d_1 = mdc(a,\ b)$ e de c. Como $d_1 \mid a$ e $d_1 \mid b$, pela transitividade, segue que $k \mid a,\ k \mid b$ e $k \mid c$. Com isso, $k \mid d$ pois $d = mdc(a,\ b,\ c)$. (Considera-se a unicidade do máximo divisor comum) □

O cálculo com mais de três números dá-se, então, de maneira análoga.

Exemplo 2.9. *Encontremos o* $mdc(60,\ 132,\ 64)$.

Conforme o Exemplo 2.5, $mdc(60,\ 132) = 12$.

Temos que:

$$mdc(60,\ 132,\ 64) = mdc\ (mdc(60,\ 132),\ 64).$$

Calculando o $mdc(12,\ 64)$:

	5	3
64	12	4
4	0	

Logo,

$$mdc(12,\ 64) = 4$$

$$\therefore mdc(60,\ 132,\ 64) = 4.$$

.

2.1.3 Mínimo múltiplo comum

Definição 2.4. *Um número* $\boldsymbol{m}$ *se diz mínimo múltiplo comum de* $\boldsymbol{a}, \boldsymbol{b} \in \mathbb{N}$*, se:*

i. $\boldsymbol{a} \mid \boldsymbol{m}$ *e* $\boldsymbol{b} \mid \boldsymbol{m}$ *(*$\boldsymbol{m}$ *é múltiplo de* $\boldsymbol{a}$ *e de* $\boldsymbol{b}$*);*

ii. $\boldsymbol{a} \mid \boldsymbol{m'}$ *e* $\boldsymbol{b} \mid \boldsymbol{m'} \Rightarrow \boldsymbol{m} \mid \boldsymbol{m'}$ *(todo múltiplo de* $\boldsymbol{a}$ *e de* $\boldsymbol{b}$ *é também múltiplo de* $\boldsymbol{m}$*).*

Indicaremos o mínimo múltiplo comum de a e b pela seguinte notação: $mmc(a,\ b) = m$. A partir da definição temos que o valor do mínimo múltiplo comum de a e b é único e que $mmc(a,\ b) = mmc(b,\ a)$.

Exemplo 2.10. *Seja* $\boldsymbol{a} = 0$ *e* $\boldsymbol{b}$ *qualquer. Mostremos que* $\boldsymbol{mmc}(0,\ \boldsymbol{b}) = 0$.

- $0 \mid 0$ e $b \mid 0$ (pois $0 = b \cdot 0$)

- $0 \mid m'$ e $b \mid m' \Rightarrow 0 \mid m'$

$$\text{Logo, } mmc(0,\ b) = 0.$$

Proposição 2.4. *Pra quaisquer* $\boldsymbol{a}$, $\boldsymbol{b} \in \mathbb{N}^*$, *se* $\boldsymbol{d = mdc\ (a,\ b)}$ *então* $\boldsymbol{m = \frac{ab}{d}}$ *é o mínimo múltiplo comum de* $\boldsymbol{a}$ *e* $\boldsymbol{b}$.

Demonstração. Se $d \mid a$ e $d \mid b$ temos que $d \mid ab$, então $m \in \mathbb{N}$.

i. Como
$$\frac{ab}{d} = a \cdot \frac{b}{d} = b \cdot \frac{a}{d} = m$$
Então $a \mid m$ e $b \mid m$.

ii. Seja m' múltiplo de a e b suponha que $m' = ar$ e $m' = bs$. Logo, $ar = bs$ e:
$$\frac{a}{d} \cdot r = \frac{b}{d} \cdot s$$
Dessa forma, $\frac{a}{d} \mid \frac{b}{d}s$ e, como o $mdc\left(\frac{a}{d}, \frac{b}{d}\right) = 1$ então, pelo Corolário 2.1 e Proposição 2.3, $\frac{a}{d} \mid s$. Assim sendo,
$$s = \frac{a}{d} \cdot k$$
se $m' = bs$, para algum $k \in \mathbb{N}$, temos:
$$m' = b \cdot \frac{a}{d} \cdot k = \frac{ab}{d} \cdot k = mk$$
Então, $m \mid m'$.

□

Corolário 2.3. *Se* $\boldsymbol{a}$ *e* $\boldsymbol{b}$ *são primos entre si, então* $\boldsymbol{mmc\ (a,\ b) = ab}$.

Demonstração. De fato, como $d = mdc(a,\ b) = 1$, então $mmc(a,\ b) = \frac{ab}{1} = ab$. □

Exemplo 2.11. *Achemos o* $\boldsymbol{mmc}$*(148, 40) utilizando a proposição anterior.*

Calculando o mdc(148, 40):

	3	1	2	3
148	40	28	12	4
28	12	4	0	

Como $mdc(148,\ 40) = 4$, então:
$$mmc(148,\ 48) = \frac{148 \cdot 40}{4} = 148 \cdot 10 = 1480.$$

Exemplo 2.12. *Achemos o* $\boldsymbol{mmc}$*(4, 15) usando o mesmo procedimento.*

Calculando o $mdc(4,\ 15)$:

	3	1	3
15	4	3	1
3	1	0	

Como $mdc(4,\ 15) = 1$, então:

$$mmc(4,\ 15) = \frac{4 \cdot 15}{1} = 4 \cdot 15 = 60.$$

Generalização: A definição de mínimo múltiplo comum pode ser facilmente estendida para três ou mais números naturais. Para o caso de três números pode-se usar a seguinte propriedade:

$$mmc(a,\ b,\ c) = mmc(a,\ mmc(b,\ c)) = mmc(mmc(a,\ b),\ c).$$

Exemplo 2.13. *Achemos o* $\boldsymbol{mmc}(60,\ 132,\ 64)$.

Sabe-se que o $mdc(60,\ 132) = 12$ e $mdc(60,\ 132,\ 64) = 4$. (Exemplo 2.9)

$$mmc(60,\ 132) = \frac{\cancel{60}^{\ 5} \cdot 132}{\cancel{12}} = 5 \cdot 132 = 660$$

$$mmc(60,\ 132,\ 64) = mmc(mmc(60,\ 132),\ 64) = mmc(660,\ 64) = \frac{660 \cdot \cancel{64}^{\ 16}}{\cancel{4}} = 660 \cdot 16 = 10560$$

$$\therefore mmc(60,\ 132,\ 64) = 10560.$$

2.1.4 Congruência

A noção de congruência surgiu a partir de Gauss, que, em sua obra *Disquisitiones Arithmeticae*, concebe a ideia de aritmética modular ou finita.

Definição 2.5. *Sejam* $\boldsymbol{a}$, $\boldsymbol{b}$ *e* $\boldsymbol{m}$ *números inteiros,* $\boldsymbol{m} > 0$. *Dizemos que* $\boldsymbol{a}$ *é côngruo a* $\boldsymbol{b}$*, módulo* $\boldsymbol{m}$*, se* $\boldsymbol{m} \mid \boldsymbol{(a - b)}$.

Utilizaremos a notação $\mathbf{a} \equiv \mathbf{b}(mod\ \mathbf{m})$, a qual estabelece uma relação de congruência sobre $\mathbb{Z}$.

O módulo pode ser usado para representar relações matemáticas de ciclo, ou seja, que se reiniciem. Ao contar as horas, sempre que chegamos às 12, regressamos a 1, 2, 3,... Quando se passar mais 12 horas o ciclo irá repetir-se, ou seja, o número 12 equivale ao 0 no relógio. Por isso as horas são contadas de 0 a 11 e, dessa forma, chegam ao 0 novamente. Esse raciocínio pode levar à seguinte representação:

- Se contarmos três horas após às nove da noite teremos meia-noite;

$$9 + 3 \equiv 0 \tag{2.1}$$

- Se contarmos cinco horas após as oito da manhã teremos 1 hora da tarde.

$$8+5 \equiv 1 \tag{2.2}$$

O valor a qual a contagem sempre recomeça é 12. Quando a é côngruo a b no módulo 12 quer dizer que a diferença entre a e b é divisível por 12.

$$12-0=12 \text{ e } 13-1=12$$

Ao fazer 2.1 e 2.2 estaremos retirando o conjunto dos múltiplos M_{12}.

$$9+3=12$$

$$12-12=0$$

$$8+5=13$$

$$13-12=1$$

Isto é, respectivamente:

$$12 \equiv 0(mod\ 12)$$

$$13 \equiv 1(mod\ 12)$$

Exemplo 2.14. $4 \equiv 15(mod\ 11)$, *pois* $4-15=-11$ *e* $11 \mid (-11)$; $17 \equiv -1(mod\ 3)$, *pois* $17-(-1)=18$ *e* $3 \mid 18$.

Para $a \equiv b(mod\ m)$, conforme a Definição 2.5, são válidas as seguintes propriedades:

I. Para todo $m > 0$, a relação $\equiv$ é reflexiva, simétrica e transitiva, ou seja, é uma relação de equivalência:

   a $a \in \mathbb{Z} \Rightarrow a \equiv a(mod\ m)$

   b $a \equiv b(mod\ m) \Rightarrow b \equiv a(mod\ m)$

   c $a \equiv b(mod\ m)$ e $b \equiv c(mod\ m) \Rightarrow a \equiv c(mod\ m)$

II. Para quaisquer $a,\ b \in \mathbb{Z}:\ a \equiv (mod\ m)$ se, e somente se, a e b fornecem mesmo resto na divisão euclidiana por m.

III. Se $a \equiv b(mod\ m)$, então $a \pm c \equiv b \pm c(mod\ m)$ e $ac \equiv bc(mod\ m)$, para todo $c \in \mathbb{Z}$.

IV. Se $a \equiv b(mod\ m)$ e $c \equiv d(mod\ m)$, então $a \pm c \equiv b \pm d(mod\ m)$ e $ac \equiv bd(mod\ m)$.

V. Se $a \equiv b(mod\ m)$, então $ra \equiv rb(mod\ m)$ e $a^r \equiv b^r(mod\ m)$, para todo inteiro $r \geq 1$.

VI. Se $ca \equiv cb(mod\ m)$ e $mdc(m,\ c) = d > 0$, então:

$$a \equiv b\left(mod\ \frac{m}{d}\right)$$

Caso a e b não sejam côngruos entre si, escrevemos $a \not\equiv b(mod\ m)$ (Lê-se a é incôngruo a b módulo m).

Exemplo 2.15. *Mostre que* $2^{20} - 1$ *é divisível por 41.*

$$2 \equiv 2(mod\ 41) \equiv -39(mod\ 41)$$
$$2^2 \equiv 4(mod\ 41) \equiv -37(mod\ 41)$$
$$2^3 \equiv 8(mod\ 41) \equiv -33(mod\ 41)$$
$$2^3 \cdot 2^2 \equiv 2^5 \equiv 32(mod\ 41) \equiv -9(mod\ 41)$$
$$2^5 \cdot 2^5 \equiv (-9) \cdot (-9)(mod\ 41)$$
$$2^{10} \equiv 81(mod\ 41) \equiv -1(mod\ 41)$$
$$(2^{10})^2 \equiv (-1)^2(mod\ 41)$$
$$2^{20} \equiv 1(mod\ 41)$$
$$2^{20} - 1 \equiv 1 - 1(mod\ 41)$$
$$\therefore 2^{20} - 1 \equiv 0(mod\ 41).$$

2.2 Números primos e suas propriedades

Definição 2.6. *Um número* $\boldsymbol{p} \in \mathbb{N}$ *é chamado de primo, se:*

(i) $\boldsymbol{p} \neq 0$ *e* $\boldsymbol{p} \neq 1$*;*

(ii) Os únicos divisores de $\boldsymbol{p}$ *são 1 e* $\boldsymbol{p}$*.*

Definição 2.7. *Um número não primo* $\boldsymbol{a} \in \mathbb{N}$, $\boldsymbol{a} \neq 0$, *e* $\boldsymbol{a} \neq 1$ *é nomeado composto.*

Nota: *Um número composto sempre pode ser fatorado como* $\boldsymbol{a} = \boldsymbol{bc}$, *com* $\boldsymbol{b} \neq 1$ *e* $\boldsymbol{c} \neq 1$.

Como consequência imediata às Definições 2.6 e 2.7, podemos dizer que o número 1 é um caso especial, pois não é nem primo e nem composto. Outra observação a ser feita é que o número 2 é o único primo par, pois todo número inteiro par maior que 2 poderá ser dividido por ele.

Proposição 2.5. *Se* $\boldsymbol{p}$ *é primo e* $\boldsymbol{p} \mid \boldsymbol{ab}$, *então* $\boldsymbol{p} \mid \boldsymbol{a}$ *ou* $\boldsymbol{p} \mid \boldsymbol{b}$.

Demonstração. Admitindo que $p \mid ab$, suponha que $p \nmid a$ e provemos que $mdc(p,\ a) = 1$. Se $c \mid a$ e $c \mid b$, como p é primo, então $c = 1$ ou $c = p$. Visto que $p \nmid a$, então $c = 1$. Logo, pelo Corolário 2.1, temos que $p \mid b$. □

Todo número não primo pode ser decomposto em fatores primos, sendo essa fatoração única, com exceção da ordem em que se segue. Essa alegação é garantida pelo Teorema Fundamental da Aritmética.

Teorema 2.1. *(Teorema Fundamental da Aritmética) Para todo número natural* $\boldsymbol{a} > 1$ *existem números primos* $\boldsymbol{p}_1, \boldsymbol{p}_2, \ldots, \boldsymbol{p}_r$ $(\boldsymbol{r} \geq 1)$*, de maneira que* $\boldsymbol{a} = \boldsymbol{p}_1 \cdot \boldsymbol{p}_2 \cdots \boldsymbol{p}_r$*. Além disso, se também* $\boldsymbol{a} = \boldsymbol{q}_1 \cdot \boldsymbol{q}_2 \cdots \boldsymbol{q}_s$ $(\boldsymbol{s} \geq 1)$*, onde os* $\boldsymbol{q}_i$ *são igualmente primos, então* $\boldsymbol{r} = \boldsymbol{s}$ *e cada* $\boldsymbol{p}_i$ *é igual a algum dos* $\boldsymbol{q}_j$*.*

Demonstração.

a) Usaremos o segundo princípio de indução[1]. Como 2 é primo, para $a = 2$ é válido. Suponhamos que o teorema seja válido para $\forall b \in \mathbb{N}$, tal que $2 \leq b < a$, e provaremos para a. Se $a+1$ fosse primo a demonstração se encerraria. Se a não é primo existe $2 \leq a_1 < a$ que divide a, sendo $a = a_1 \cdot b$. Pela hipótese de indução temos que a_1 e b podem ser escritos por fatores de números primos.

$$a_1 = p_1 \cdot p_2 \cdots p_r \ \text{ e } \ b = q_1 \cdot q_2 \cdots q_s$$

Assim podemos escrever:

$$a = p_1 \cdot p_2 \cdots p_r \cdot q_1 \cdot q_2 \cdots q_s$$

b) Suponha por absurdo que um número possa ser escrito de duas formas diferentes, sendo elas:

$$a = p_1 \cdot p_2 \cdots p_r$$

$$a = q_1 \cdot q_2 \cdots q_s$$

Assim como no enunciado do teorema, se $p_1 \cdot p_2 \cdots p_r = q_1 \cdot q_2 \cdots q_s$, então, pela Proposição 2.5, podemos dizer que, se $p_1 \mid (q_1 \cdots q_s)$, então $p_1 \mid q_1$. Dado que q_1 é primo, seus divisores são 1 e q_1. Como $p_1 \neq 1$ chegamos a $p_1 = q_1$.
Cancelando p_1 e q_1:

$$\cancel{p_1} \cdot p_2 \cdots p_r = \cancel{q_1} \cdot q_2 \cdots q_s$$

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

Ao repetir esse processo, quantas vezes for necessário, chegaremos a unicidade.

$$\cancel{p_1} \cdot p_2 \cdots p_r = \cancel{q_1} \cdot q_2 \cdots q_s$$

[1] Ver (DOMINGUES, 1991, p. 94).

$$\cancel{p_2}\cdots p_r = \cancel{q_2}\cdots q_s$$
$$\vdots$$
$$p_r = q_s$$

É evidente que não pode acontecer algo como $1 = q_{r+1}\cdots q_s$, pois isto resultaria em $q_s \mid 1$, um absurdo, pois q_s é primo.

□

Decorre-se, do Teorema 2.1, que os números primos são geradores de todos os números naturais maiores que 1. Ou seja, os números compostos dependem dos números primos para existir, pois todo número composto pode ser escrito como a multiplicação de, no mínimo, dois números primos. Se, por exemplo, algum primo como o 3, deixasse de existir, todos os seus múltiplos $M_3 = \{6,\ 9,\ 12,\ 15,\ 18, \ldots\}$ em consequência disso, não poderiam ser formados.

Exemplo 2.16. *Decompondo em fatores primos o número 140.*

140	2
70	2
35	5
7	7
1	

$$140 = 2\cdot 2\cdot 5\cdot 7 = 2^2\cdot 5\cdot 7$$

A cargo de curiosidade podemos pensar "o que aconteceria se o número 1 fosse considerado primo?". Primeiramente, essa suposição contraria a definição de número primo. No entanto, se pensarmos mais a fundo, o número 1 como primo derrubaria o tão majestoso Teorema Fundamental da Aritmética. Os números não teriam mais uma maneira única de fatoração, por exemplo, o número 6 poderia ser escrito de infinitas formas, algumas delas: $2\cdot 3\cdot 1$, $2\cdot 3\cdot 1^2$, $2\cdot 3\cdot 1^3$, $2\cdot 3\cdot 1^4$, ...

Procedendo de $a = p_1\cdot p_2\cdots p_r$ (2.1), quando a decomposição de um número for escrita da forma $a = p_1^{\alpha_1}\cdot p_2^{\alpha_2}\cdots p_s^{\alpha_s}$, onde $1 \le s \le r,\ p_i \ne p_j$ sempre que $i \ne j$ e $\alpha_i \ge 1$ $(i = 1,\ 2,\ 3, \ldots,\ s)$, se $p_1 < p_2 < \ldots < p_s$, então teremos a decomposição canônica de a.

Ao descobrir sobre as principais características dos números primos surge o questionamento quanto a quantidade de números que obedecem a essa definição. "Será que esses números são finitos ou infinitos? E, caso forem finitos, quantos deles existem?". Todas essas perguntas já foram respondidas há aproximadamente 2300 anos atrás, por Euclides.

Goldbach[2] e Euler também demontraram a infinidade dos números primos, mas eles não foram os únicos, há dentre eles até mesmo alguns matemáticos que caíram no esquecimento.

[2] ✱ 1690 - ✝ 1764

A demonstração feita neste trabalho está de acordo com a de Euclides, entretanto, não possui o mesmo rigor matemático de sua época. Optamos por uma abordagem mais simplificada e atual, mas que possua a mesma essência.

Teorema 2.2. *O conjunto dos números primos é infinito.*

Demonstração. Suponha que o conjunto dos números primos seja finito, ou seja:

$$P = \{p_1, p_2, p_3, \ldots, p_k\}$$

Vamos construir um número natural p da seguinte forma:

$$p = p_1 \cdot p_2 \cdot p_3 \cdot \ldots \cdot p_k + 1$$

Pela forma como foi construído, podemos afirmar que p é composto. Sendo p composto, ele pode ser fatorado como produto de números primos. Logo $\exists p_j$ $(1 \leq j \leq k)$, tal que:

$$p_j \mid p \text{ e } p_j \mid (p_1 \cdot p_2 \cdot p_3 \cdot \ldots \cdot p_k)$$

$$p_j \mid p - (p_1 \cdot p_2 \cdot p_3 \cdot \ldots \cdot p_k)$$

$$\therefore p_j \mid 1$$

Se o único divisor positivo de 1 é ele mesmo e $p > 1$, chegamos a uma contradição. Logo, temos que o conjunto dos números primos é infinito. □

A demonstração do Teorema 2.2 mostra que, se os números primos fossem finitos seria sempre possível encontrar um novo primo, provando assim, que eles são infinitos.

2.3 Como reconhecer que um número é primo?

Para verificar se números pequenos são primos ou compostos é bem simples, pois basta testar os seus divisores.

Exemplo 2.17. *8 é primo ou composto?*

8 é composto, pois $2 \mid 8$ e $4 \mid 8$.

Exemplo 2.18. *7 é primo ou composto?*

7 é primo, pois $2 \nmid 7$, $3 \nmid 7$, $4 \nmid 7$, $5 \nmid 7$ e $6 \nmid 7$.

Se o número for muito grande o número de candidatos a ser testado obviamente também será. Ao seguir esse raciocínio, para testar o número 597 seria então necessário analisar os 595 números que o antecedem, tendo como exceção o 1 e ele mesmo. Sendo, então, um processo inadequado para números grandes.

Um dos métodos mais antigos para se determinar se um número é primo ou não é conhecido como *Crivo de Eratóstenes*[3], também ideal para encontrar números primos de 1 a um certo número natural não-nulo. Esse processo não envolve fórmulas, e funciona como um filtro que retém os primos e descarta os compostos. Vejamos, em detalhes, como realizar esse procedimento no Exemplo 2.21.

Proposição 2.6. *Se* $\boldsymbol{n} > 1$ *é um número composto, então há um número primo* $\boldsymbol{p}$ *tal que:*

$$\boldsymbol{p} \mid \boldsymbol{n} \ \ e \ \ \boldsymbol{p}^2 \leq \boldsymbol{n} \ (\Longleftrightarrow \boldsymbol{p} \leq \sqrt{\boldsymbol{n}}).$$

Demonstração. Pela hipótese, n é um número composto, então pode ser escrito como:

$$n = ab \ (2 \leq a \leq b < n)$$

Assim sendo, $n = ab \geq a^2$. Seja p um divisor primo de a, logo, $p^2 \mid a^2$ e $p^2 \leq a^2$. Então teremos: $p^2 \leq n \Rightarrow p \leq \sqrt{n}$. □

Como consequência direta à demonstração da Proposição 2.6, temos que, se $n > 1$ não é divisível por nenhum dos números primos $p \leq \sqrt{n}$, portanto n é primo.

Exemplo 2.19. *O número 229 é primo ou composto?*

Primeiramente, vamos definir o intervalo em que se encontra a raiz de 229.

$$15 \leq \sqrt{229} < 16$$

Os primos menores ou iguais a 15 são: $2,\ 3,\ 5,\ 7,\ 11,\ 13$.

$$229 = 2 \cdot 114 + 1$$

$$229 = 3 \cdot 76 + 1$$

$$229 = 5 \cdot 45 + 4$$

$$229 = 7 \cdot 32 + 5$$

$$229 = 11 \cdot 20 + 9$$

$$229 = 13 \cdot 17 + 8$$

Nenhum desse primos divide 229. Logo, ele é primo.

Exemplo 2.20. *O número 177 é primo ou composto?*

[3] "Eratóstenes de Cirene (aprox. 280-192 a.C.) foi um sábio de atividades várias: além de matemático foi astrônomo, geógrafo e filólogo. Quando tinha cerca de 40 anos de idade passou a dirigir a célebre biblioteca de Alexandria. É mais conhecido, provavelmente, pela medição que fez, bastante boa para a época, da circunferência da Terra" (DOMINGUES, 1991, p. 58).

Primeiramente, vamos definir o intervalo em que se encontra a raiz de 177.

$$13 \leq \sqrt{177} < 14$$

Os primos menores ou iguais a 13 são: $2,\ 3,\ 5,\ 7,\ 11$

$$177 = 88 \cdot 2 + 1$$

$$177 = 59 \cdot 3$$

Como $3 \mid 177$, então ele é composto.

Exemplo 2.21. *Encontremos todos os números primos no intervalo de* 1 *a* 100 *utilizando o Crivo de Eratóstenes.*

Para $n \in \mathbb{N}$, tal que $n \leq 100$. Como $\sqrt{100} = 10$, basta trabalhar com os números primos menores que 10 $(2,\ 3,\ 5,\ 7)$.

Primeiramente, iremos cancelar todos os múltiplos de 2, exceto o próprio 2.

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

Os múltiplos de 3 que também são múltiplos de 2, já foram cancelados anteriormente. Portanto, retiraremos todos os múltiplos de 3 restantes da lista, exceto o próprio 3.

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

Em sequência, repetiremos o mesmo procedimento com os números 5 e 7, obtendo:

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

Logo, os números primos de 1 a 100 são: 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97.

O *Crivo de Eratóstenes* é um critério eficiente para determinar números primos pequenos, mas não serve para números primos muitos grandes. No entanto, na prática, o que mais importa é conseguir reconhecer números primos gigantes, pois são fundamentais em aplicações como a criptografia (assunto expresso em mais detalhes no Capítulo 3).

Os computadores fazem uso de números primos com milhares de dígitos. Portanto, é possível imaginar o quanto seria trabalhoso e demorado usar esse critério para definir se esse número é primo ou não.

Dentre os métodos mais atuais para determinar se um número é primo ou não, temos os testes de primalidade[4] usados por computadores, que podem ser determinísticos ou não-determinísticos. A diferença entre esses dois tipos de teste de primalidade é que o determinístico traz um resultado 100% confiável, ou seja, sabe-se com certeza se tal número é composto ou primo. Já o teste não-determinístico assegura que um número é primo apenas com uma certa probabilidade, controlada de acordo com a vontade do utilizador.

Os testes de primalidade mais usados são os não-determinísticos, que também podem ser chamados de probabilísticos. Pode parecer contraditório, pois um teste determinístico traria uma resposta totalmente verdadeira, no entanto, isto acontece devido ao tempo necessário para sua aplicação. Alguns testes determinísticos possuem tempo de execução exponecial [5], e isso torna-os ineficientes, já que eles só seriam economicamente consideráveis caso fossem de tempo polinomial[6].

Quando um teste de primalidade possui grande probabilidade de acerto e um certo número, mesmo sendo composto, passa nesse teste, ele é então chamado de pseudo-primo.

---

[4] "A expressão *teste de primalidade* refere-se a um algoritmo que, tendo por entrada um número positivo n, determina se n é, ou não é, primo" (COUTINHO, 2004, p. 64).

[5] Tempo de execução determinado por $f(N)$, para todo $N = e^{log\ N}$, sendo $f(X)$ um polinômio. (RIBENBOIM, 2001)

[6] "O algoritmo é chamado tempo polinomial se existir um polinômio $f(X)$, tal que, para todo N, é limitado por $f(log\ N)$" (RIBENBOIM, 2001, p. 100).

O *Pequeno Teorema de Fermat* e o *Teorema de Euler* foram fundamentais para o desenvolvimento dos testes de primalidade. Estes estão dentre os mais conhecidos: *Teste De Leibniz*, *Teste de Miller* e *Teste de Lucas*. Esses testes citados não são os únicos existentes e como este trabalho aborda esse assunto superficialmente, caso o leitor deseje apronfundar mais acerca do tema, ver Ribenboim (2001) e Coutinho (2007).

2.4 Como encontrar números primos?

Figura 2.1 – Distribuição dos números primos de 1 a 100 em uma reta numérica

Fonte: A autora (2022).

Pode-se perceber, a partir da distribuição dos primos de 1 a 100, representada na Figura 2.1, que esse números não possuem um padrão de distância entre um e outro, e que não é possível estabelecer uma regra que defina quando irá aparecer o próximo.

Como vimos anteriormente, obter a lista dos números primos entre 1 e 100 é uma tarefa fácil, porém encontrar números primos muito grandes é bem mais complicado.

As mentes matemáticas de todas as épocas têm sido atormentadas pelo questionamento acerca da fórmula que permite gerar qualquer número primo. "Depois de mais de dois mil anos de esforços, os primos parecem resistir a qualquer tentativa de encaixá-los em um padrão reconhecível" (SAUTOY, 2008, p.15). Sautoy (2008) ainda ressalta:

> Com a prova de Euclides, não havia mais como montar uma tabela periódica de todos os primos ou descobrir algo como seu genoma, codificando bilhões deles. Não existiria uma simples coleção de borboletas que nos permitisse entender esses números. Eis, novamente, o desafio máximo: o matemático, equipado com um arsenal limitado, enfrentando a extensão infinita de primos. Como poderíamos mapear um caminho por esse emaranhado caótico, encontrando algum padrão que pudesse prever seu comportamento? (p. 40)

Esses números podem ser definidos de forma simples, porém estão rodeados de enigmas não resolvidos. Dentre os principais problemas em aberto estão: a Conjectura de Golbach [7] e a Hipótese de Riemann [8].

Muitos empenharam-se em provar a existência de uma fórmula que gera primos, mas, até o momento, todos os matemáticos conhecidos falharam nessa missão. Como afirma Sautoy (2008), "O que motiva a existência de um matemático é a descoberta de padrões, para encontrar e explicar as regras subjacentes à natureza e prever o que acontecerá a seguir"(p. 28). A falta de

[7] Ver apêndice A.
[8] Ver apêndice B.

previsibilidade do conjunto dos números primos representa o caos para muitos matemáticos, e, provavelmente por essa motivação, tenham sido realizadas tantas tentativas.

2.4.1 Algumas tentativas de gerar números primos

Fermat, no ano de 1640, enviou uma a seu amigo Bernard Frenide de Bessy, declarando que todos os números escritos da forma

$$F_n = 2^{(2^n)} + 1 \ (n \geq 0)$$

(atualmente chamados *números de Fermat*) são primos . Ele confessou não ter provado tal afirmação, apenas verificou que era válido para F_0, F_1, F_2, F_3, e F_4. Mais tarde, no ano de 1732, Euler provou que Fermat estava errado, e que F_5 é divisível por 641.

Em 1772, Euler descobriu que a função polinomial quadrática $f(n) = n^2 + n + 41$ assumia uma sequência de valores primos. Ao substituir os valores $n = 0, 1, 2, 3, 4, 5, \ldots, 39.$, essa função irá gerar uma lista de primos, que pode ser observada na Tabela 1.

Tabela 1 – Lista de números primos gerada por $f(n)$

n	$f(n)$
0	41
1	43
2	47
3	53
4	61
5	71
6	83
7	97
8	113
9	131
10	151
11	173
12	197
13	223
14	251
15	281
16	313
17	347
18	383
19	421
20	461
21	503
22	547
23	593
24	641
25	691
26	743
27	797
28	853
29	911
30	971
31	1033
32	1097
33	1163
34	1231
35	1301
36	1373
37	1447
38	1523
39	1601

Fonte: Burton (2016, p. 55).

Porém, ao substituir $n = 40$ na função, obtém-se:

$$f(40) = 40^2 + 40 + 41 = 40 \cdot 40 + 41 = 40(40+1) + 41 = 40 \cdot 41 + 41 = 41(40+1) = 41^2.$$

Portanto, como $f(40)$ pode ser escrita como fator de um número primo, $f(n)$ também fornece números compostos.

Euler também considerou os polinômios $2x^2 + p$, com $p = 3,\ 5,\ 11,$ e 29 e mostrou ser válido para $x = 0,\ 1, \ldots,\ p-1$. No entanto, esse polinômio não supera o anterior quanto a quantidade de valores iniciais primos, obtidos sucessivamente.

De acordo com Ribenboim (2001, p. 125), "O polinômio quadrático $f(X) = 36X^2 - 810X + 2753$, descoberto por R. RUBY em 1990, é presentemente o que fornece a mais longa sucessão $|f(k)|$ (para $k = 0,\ 1, \ldots,\ 44$) de valores absolutos primos iniciais".

Seja p primo e p^k definido como o produto de todos os números primos menores ou iguais a p. Os números escritos como $p^k + 1$ são chamados números euclidianos e, isso, porque eles aparecem no método que Euclides usa para demonstrar a infinitude dos números primos. O curioso é que ao listar os cinco primeiros números, todos serão primos.

$$2^k + 1 = 2 + 1 = 3$$

$$3^k + 1 = 2 \cdot 3 + 1 = 7$$

$$5^k + 1 = 2 \cdot 3 \cdot 5 + 1 = 31$$

$$7^k + 1 = 2 \cdot 3 \cdot 5 \cdot 7 + 1 = 211$$

$$11^k + 1 = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 + 1 = 2311$$

Nos cinco primeiros números primos a fórmula funciona muito bem, porém nos próximos não dará certo e não se formarão números primos.

$$13^k + 1 = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 + 1 = 30031 = 59 \cdot 509$$

$$17^k + 1 = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 + 1 = 510511 = 19 \cdot 97 \cdot 277$$

$$19^k + 1 = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19 + 1 = 9699691 = 347 \cdot 27953$$

Outra questão desconhecida é que se existem infinitos primos p para os quais $p^k + 1$ também sejam primos. Até então, são conhecidos 22 primos que podem ser escritos dessa forma, o vigésimo segundo foi descoberto em 2001, usando $p = 392113$, e obtendo-se um primo de 169966 dígitos.

Essas não foram as únicas tentativas de gerar primos e, apesar de terem tido muitas outras colaborações quanto a esse problema em aberto, ninguém conseguiu ainda formular uma regra geral que forneça qualquer número primo.

2.5 Tipos de números primos e algumas curiosidades

Embora muitos enigmas que envolvam os números primos não tenham sido resolvidos, com o passar dos anos muitas particularidades acerca desses números foram descobertas, dentre elas alguns tipos de números primos especiais. Iremos, então, destacar aqui alguns desses tipos de números primos.

Definição 2.8. *Primos Gêmeos consistem em um par de números primos* p *e* $p+1$.

Exemplo 2.22. 3 *e* 5, 17 *e* 19, 59 *e* 61 *são Primos Gêmeos.*

Os Primos Gêmeos estão ligados diretamente à Conjectura dos Primos Gêmeos, mais um dos mistérios não resolvidos que envolvem os primos. Essa conjectura afirma que existem infinitos pares de números primos gêmeos.

Definição 2.9. p *é um Primo de Sophie Germain*[9] *se* $2p+1$ *é também número primo.*

Exemplo 2.23. 3, 5 *e* 11 *são Primos de Germain, pois* $2\cdot 3+1=7$, $2\cdot 5+1=11$ *e* $2\cdot 11+1=23$.

Estima-se que haja infinitos Primos de Germain, no entanto, a demonstração seria tão complexa quanto à da Conjectura de Primos Gêmeos.

Definição 2.10. *Seja* p *primo, um Primos de Mersenne são os primos que podem ser escritos da forma* 2^p-1.

Exemplo 2.24. *3 é um Primo de Mersenne*[10]*, pois* $2^2-1=3$.

Em 2006, conforme Sá (2007), o número de Primos de Mersenne descobertos era de 44, no entanto, após essa data mais números podem ter sido descobertos.

Definição 2.11. *O número* p *é chamado Primo de Wilson quando* $(p-1)!\equiv -1(mod\ p^2)$.

Exemplo 2.25. *5 é Primo de Wilson, pois*

$$(5-1)!\equiv -1(mod\ 5^2)$$

$$4!\equiv -1(mod\ 25)$$

$$24\equiv -1(mod\ 25).$$

[9] Sophie Germain (1776-1831), por ser mulher, não conseguiu matricular-se na Escola Politécnica, mas conseguiu material de vários professores por meio de trabalhos escritos, submetidos sob o pseudônimo masculino de M. Leblanc. Trocava correspondências matemáticas com Gauss, por quem foi muito elogiada, porém, só depois de um tempo Gauss foi descobrir seu verdadeiro nome (EVES, 2011).

[10] "Marin Mersenne (1558-1648) foi um frei franciscano francês que dedicou boa parte de sua vida ao estudo da matemática, escrevendo livros e contribuindo para o desenvolvimento de teorias através de sua correspondência com Fermat e outros matemáticos de sua época"(SÁ, 2007, p. 78).

Ainda não foi provado que existem infinitos números Primos de Wilson. Até o momento são conhecidos 3 números primos nessa condição, 563 foi o último a ser descoberto, no ano de 1953, "[...] obtido como uma das primeiras pesquisas feitas com computadores eletrônicos" (RIBENBOIM, 2001, p. 195). Já foram feitos cálculos até $5 \cdot 10^8$ e nenhum outro Primo de Wilson foi achado.

As particularidades dos números primos estendem-se além de seus tipos ou da dificuldade de prever quando o próximo irá aparecer. Portanto, apresentaremos algumas das curiosidades sobre esses números:

- Os únicos números primos consecutivos são 2 e 3;
- Existem mais números primos entre 1 e 100 do que entre 101 e 200 (SÁ, 2007, p. 75);
- O único trio de números Primos Gêmeos são 3, 5 e 7;
- O número 5 é o único primo terminado com o algarismo 5;
- Entre 1 e 1000 existem somente 168 números primos;
- "O maior número primo conhecido cujo algarismos são primos $(2,\ 3,\ 5,\ 7)$ é

$$72323252323272325252 \times \frac{10^{3120}-1}{10^{20}-1} + 1$$

  Ele tem 3120 algarismos" (RIBENBOIM, 2001, p. 106);
- Os maiores números primos conhecidos com algarismo inicial d (não múltiplo de 3), seguido de n algarismos iguais a 9, são descritos na tabela a seguir:

Tabela 2 – Maiores números primos com algarismo inicial d, seguido de n algarismos 9

d	n
1	15749
2	9439
4	16131
5	4332
7	2846
8	8415

Fonte: Ribenboim (2001, p. 107).

- O maior número primo conhecido cujos algarismos são todos ímpares é aquele indicado na tabela 2, com algarismo inicial 5, seguido de 4332 algarismos iguais a 9;
- "Enfim, o menor número primo com 1000 algarismos (definitivamente) é $10^{999} + 7$" (RIBENBOIM, 2001, p. 107).

3 APLICAÇÕES DE NÚMEROS PRIMOS

Neste capítulo apresentaremos duas aplicações de números primos. Falaremos sobre a criptografia, sua origem e importância. Além disso, explicaremos um método criptográfico que utiliza números primos grandes para garantir o compartilhamento de informações em segredo. Posteriormente, com o intuito de evidenciar a importância dos primos em nosso mundo, falaremos sobre as cigarras periódicas, insetos que dependem desses números para sua sobrevivência.

3.1 Criptografia

O termo criptografia origina-se do grego *kryptos* (escondido) + *grafia* (escrita); e quer dizer arte ou ciência dos códigos secretos, isto é, consiste em um conjunto de métodos que possibilitam tornar uma mensagem incompreensível, de maneira que, idealmente, somente o destinatário consiga interpretá-la (SÁ, 2007).

Acredita-se que a criptografia surgiu da necessidade que o ser humano sente, desde os tempos antigos, de transmitir mensagens em segredo, sejam essas informações pessoais, comerciais, políticas ou militares. Ela "[...] é tão antiga quanto a própria escrita, já estava presente no sistema de escrita hieroglífica dos egípcios. Os romanos utilizavam códigos secretos para comunicar planos de batalha" (SÁ, 2007, p. 98). De acordo com Stewart (2016, p.81):

> Um código é uma maneira de transformar uma mensagem dada em outra mensagem. Mas como qualquer mensagem é um número, um código pode ser pensado como uma maneira de transformar um dado número em outro número. A essa altura, entra em jogo a matemática, e ideias da teoria dos números podem ser usadas para criar códigos.

Na Antiguidade, a criptografia não era exatamente uma ciência, mas já existiam várias maneiras de compartilhar informações secretas: "Foram usadas tatuagens nos corpos de escravos, invenção de sinais, linguagens secretas, pinturas, conversas em particular, troca de sinais, etc" (SHOKRANIAN, 2005).

"Para impedir que informações importantes caíssem nas mãos erradas, nossos ancestrais inventaram maneiras cada vez mais perspicazes de dissimular o conteúdo de uma mensagem" (SAUTOY, 2008, p. 186). A cítala foi um dos primeiros métodos utilizados para transmitir mensagens escondidas. Esse artifício foi pensado pelo exército espartano, por volta de 2500 anos atrás, e funcionava da seguinte forma: assim como o emissor da mensagem, o receptor também possuía em mãos um cilindro com medidas idênticas. Para que a mensagem fizesse sentido era necessário enrolar a faixa de pergaminho em volta da cítala, portanto, sem estar enrolada ao cilindro o conteúdo tornava-se ininteligível (SAUTOY, 2008).

Outro tipo de aplicação criptográfica rudimentar é a *Cifra de César*, inventada pelo imperador romano Júlio César, com o objetivo de trocar mensagens com seus generais. Esse método criptográfico consiste em trocar as letras do alfabeto de acordo com a chave escolhida, por exemplo, se a chave fosse 3, cada letra passaria a ser equivalente à terceira letra anterior a ela no alfabeto. Portanto, quem tivesse posse da chave ou simplesmente conhecesse a regra utilizada, conseguiria descriptografar a mensagem (SÁ, 2007).

Exemplo 3.1. *Usando a chave 5 da Cifra de César, vamos encriptografar a seguinte mensagem:*

"O fascinante mundo dos números primos"

A	B	C	D	E	F	G	H	I	J	K	L	M
V	W	X	Y	Z	A	B	C	D	E	F	G	H
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
I	J	K	L	M	N	O	P	Q	R	S	T	U

Fazendo as substituições, temos:

"J AVNXDIVIOZ HPIYJ YJN IPHZMJN KMDHJN".

Infelizmente, códigos como a *Cifra de César* não são tão eficazes, pois são muito simples de decifrar (COUTINHO, 2007).

> Na verdade, qualquer código que envolva substituir cada letra sistematicamente por outro símbolo qualquer sofre do mesmo problema. Isto se deve ao fato de que a freqüencia média com que cada letra é usada em uma língua é mais ou menos constante. Por exemplo, na língua portuguesa:
> • As vogais são mais frequentes que as consoantes;
> • A vogal mais frequente é o A;
> • Se um monossílabo tem uma única letra, então esta letra é uma vogal;
> • Consoantes como S e M são mais freqüentes que as outras (COUTINHO, 2007, p. 1-2).

Segundo Sautoy (2008), até 1977, se alguém quisesse comunicar-se sem que outros tivessem conhecimento da mensagem, as partes envolvidas (emissor e receptor) precisariam encontrar-se para decidir o método de codificação a ser usado. No caso da cítala, eles teriam que estabelecer quais as suas dimensões. Mesmo durante a Segunda Guerra Mundial, com a máquina Enigma, era necessário que Berlim enviasse para os capitães e comandantes as informações referentes a configuração diária da máquina. Logo, se algum adversário tivesse acesso aos códigos, as mensagens poderiam ser facilmente decodificadas.

Desde então, os métodos critográficos foram cada vez mais aprimorados. Esse avanço está diretamente ligado à teoria dos números, uma das principais responsáveis pela tecnologia presente nos computadores atualmente. "O mais interessante é que a tecnologia de criptografia demorou até a metade do século passado para sofrer algum tipo de mudança" (SÁ, 2007, p. 98).

O advento dos computadores tornou impossível o uso de códigos que podem ser decifrados por contagem de frequência, ou seja, qualquer um que envolva substituição de letras. Aliás, a criação dos primeiros computadores está intimamente relacionada à necessidade de quebrar códigos, como aconteceu na Segunda Guerra Mundial, com a construção da máquina de Turing, que tinha por objetivo vencer a Enigma (COUTINHO, 2007).

Atualmente, o ser humano depende da internet para uma série de tarefas cotidianas, desde comunicar-se pelo *Whatsapp* com outras pessoas a realizar compras online ou até mesmo fazer transferências bancárias com um clique. O compartilhamento massivo de informações exigiu da criptografia métodos mais sofisticados, que tornasse mais complicada, cada vez mais, a quebra de códigos.

> Assim como ocorreu em Bletchley Park na decifração do Enigma durante a guerra, os matemáticos seriam outra vez os responsáveis pelo invento de uma nova geração de códigos que tirariam a criptografia dos romances de espionagem e a levariam para a aldeia global (SAUTOY, 2008, p. 186).

A partir disso, foram criados códigos matemáticos que deram origem à criptografia de chave pública. Antes era possível encriptografar e descriptografar uma mensagem utilizando uma mesma chave. Agora, com esse outro método, é usada uma chave pública para a encifração e uma chave privada para decifração. Além disso, o acesso a chave pública não garante a chegada à chave privada.

Sautoy (2008) imagina como seria um mundo virtual sem a criptografia de chave pública:

> Antes que pudéssemos enviar nossos dados bancários com segurança, teríamos de receber cartas confidenciais da empresa que organiza cada página virtual em que quiséssemos fazer compras, dizendo-nos como codificar os detalhes. Dado o enorme tráfego da internet, haveria uma grande chance de que muitas dessas cartas fossem interceptadas (p. 186).

A vantagem neste tipo de criptografia torna-se evidente, já que o emissor e o receptor da mensagem não precisarão mais encontrar-se para compartilhar a chave. Não é necessário nem mesmo que o receptor conheça a chave de decodificação (BURTON, 2016).

3.1.1 Criptografia RSA

O processo de funcionamento do método RSA descrito neste trabalho é fundamentado em Coutinho (2007), Burton (2016) e Stewart (2016).

Segundo Coutinho (2007), o sistema de criptografia de chave pública mais popular é o RSA, criado no ano de 1978. Seu nome é formado pelas iniciais de seus inventores: Ted Rivest, Adi Shamir e Leonard Adleman. Existem vários outros códigos, mas, na atualidade, esse é o mais usado em aplicações comerciais.

Esse sistema começa escolhendo dois números primos grandes p e q, que podemos encontrar em um teste de primalidade feito por um computador. Para o processo de codificação é suficiente conhecer o produto desses dois números primos ($n = p \cdot q$). Porém, para a decodificação é necessário conhecer os dois números primos (p e q). A chave pública n pode ser conhecida por todos, mas a chave privada formada por p e q deve ser mantida em segredo. Caso contrário, o código poderá ser quebrado.

Para codificar uma mensagem, primeiramente ela é convertida em um código e um cálculo baseado na multiplicação desses números primos p e q é realizado. É calculado $n = p \cdot q$ e $s = (p-1)(q-1)$, depois é escolhido um número e entre 1 e s que não tenha nenhum fator comum com s. O par $(n,\ e)$ será então a chave de decodificação.

Para decodificar essa mesma mensagem é necessário calcular um número d, de forma que

$$d \cdot e \equiv 1 (mod\ s).$$

Portanto, o par $(n,\ d)$ será a chave de decodificação.

Exemplo 3.2. *Usando o método RSA, codificaremos a seguinte mensagem:*

"Matemática é legal"

Esta primeira etapa será chamada de pré-codificação. Converteremos a mensagem em um código usando a tabela de conversão abaixo:

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

Usaremos o número 99 para o espaço entre as palavras. Portanto, a mensagem convertida em número é:

$$22102914221029181210991499211416102 1$$

Calculando n para $p = 11$ e $q = 13$:

$$n = p \cdot q$$

$$n = 11 \cdot 13$$

$$n = 143$$

Após a conversão, dividiremos a mensagem em blocos, de maneira que cada um seja menor que n e nenhum se inicie com 0.

$$2 - 2 - 102 - 91 - 42 - 2 - 102 - 91 - 81 - 2 - 109 - 91 - 49 - 92 - 11 - 41 - 6 - 102 - 1$$

Os blocos em que a mensagem foi quebrada diferenciam-se das unidades linguísticas. Isso é ideal, pois torna a decodificação por contagem essencialmente impossível.

Calculando s para $p = 11$ e $q = 13$:

$$s = (p-1)\cdot(q-1)$$

$$s = (11-1)\cdot(13-1)$$

$$s = 10\cdot 12$$

$$s = 120$$

Precisamos escolher e de modo que $mdc(e,s) = 1$. O menor valor possível para e é 7, pois é o menor primo que não divide 120. Logo, a chave de codificação é $(n,e) = (143,7)$.

Iremos chamar o bloco codificado de $C(b)$ e calcularemos usando a seguinte fórmula:

$$C(b) = \text{resto da divisão de } b^e \text{ por } n$$

Isto é:

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

Calcularemos para 2, 102, 91, 42, 81, 109, 49, 92, 11, 41, 6 e 1.

$$2^7 \equiv 128(mod 143)$$

$$102^7 \equiv 102^2\cdot 102^2\cdot 102^2\cdot 102(mod 143)$$
$$102^7 \equiv 108\cdot 108\cdot 108\cdot 102(mod 143)$$
$$102^7 \equiv 81\cdot 5(mod 143)$$
$$102^7 \equiv 119(mod 143)$$

$$91^7 \equiv 91^2\cdot 91^2\cdot 91^2\cdot 91(mod 143)$$
$$91^7 \equiv 130\cdot 130\cdot 130\cdot 91(mod 143)$$
$$91^7 \equiv 26\cdot 104(mod 143)$$
$$91^7 \equiv 130(mod 143)$$

$$42^7 \equiv 42^2\cdot 42^2\cdot 42^2\cdot 42(mod 143)$$
$$42^7 \equiv 48\cdot 48\cdot 48\cdot 42(mod 143)$$

$$42^7 \equiv 16 \cdot 14 (mod 143)$$

$$42^7 \equiv 81 (mod 143)$$

$$81^7 \equiv 81^3 \cdot 81^3 \cdot 81 (mod 143)$$

$$81^7 \equiv 53 \cdot 53 \cdot 81 (mod 143)$$

$$81^7 \equiv 16 (mod 143)$$

$$109^7 \equiv 109^3 \cdot 109^3 \cdot 109 (mod 143)$$

$$109^7 \equiv 21 \cdot 21 \cdot 109 (mod 143)$$

$$109^7 \equiv 21 (mod 143)$$

$$49^7 \equiv 49^3 \cdot 49^3 \cdot 49 (mod 143)$$

$$49^7 \equiv 103 \cdot 103 \cdot 49 (mod 143)$$

$$49^7 \equiv 36 (mod 143)$$

$$92^7 \equiv 92^3 \cdot 92^3 \cdot 92 (mod 143)$$

$$92^7 \equiv 53 \cdot 53 \cdot 92 (mod 143)$$

$$92^7 \equiv 27 (mod 143)$$

$$11^7 \equiv 11^3 \cdot 11^3 \cdot 11 (mod 143)$$

$$11^7 \equiv 44 \cdot 44 \cdot 11 (mod 143)$$

$$11^7 \equiv 132 (mod 143)$$

$$41^7 \equiv 41^3 \cdot 41^3 \cdot 41 (mod 143)$$

$$41^7 \equiv 138 \cdot 138 \cdot 41 (mod 143)$$

$$41^7 \equiv 24 (mod 143)$$

$$6^7 \equiv 85 (mod 143)$$

$$1^7 \equiv 1 (mod\ 143)$$

Ao codificar toda a mensagem obtemos os seguintes blocos:

$$128-128-119-130-81-128-119-130-16-128-21-130-36-27-132-24-85-119-1.$$

Para decodificar a mensagem do Exemplo 3.2 é necessário duas informações: n e o inverso de e em s, que chamaremos de d. Logo, (n, d) será a chave de decodificação. A fórmula utilizada para o processo de decodificação é:

$$D(a) = \text{resto da divisão de } a^d \text{ por } n.$$

É possível observar que para calcular d é preciso saber quem são os números primos p e q. Ao imaginar esse processo de decodificação usando p e q com mais de 100 dígitos torna-se ainda mais perceptível a dificuldade da resolução desse problema.

No Exemplo 3.2 temos que $n = 143$ e $e = 7$. Sabendo que $s(143) = 120$, aplicaremos o algoritmo euclidiano da seguinte maneira:

$$120 = 7 \cdot 17 + 1$$

$$1 = 120 + (-17) \cdot 7.$$

Portanto, segue que o inverso de 7 módulo 120 é -17. Para d positivo, teremos $d = 120 - 17 = 103$. A partir desta etapa os cálculos feitos à mão não são mais suficientes. Por exemplo, para decodificar o bloco 109, é necessário fazer o seguinte cálculo:

$$109^{103} \equiv D(a)(mod\ 143).$$

Esses códigos são chamados de *códigos de alçapão*, pois são fáceis de codificá-los, no entanto, a saída é bem mais difícil de ser encontrada. Para tomar conhecimento do número d seria necessário a fatoração de números muito grandes e ainda não foi descoberta nenhuma forma rápida de se fazer isso. Logo, o problema matemático da fatoração de números muitos grandes gerou uma solução para a criptografia.

> Fatorar é computacionalmente mais difícil do que a distinguir primos e compostos. Atualmente, nos computadores mais rápidos, o teste de primalidade de um número de 200 dígitos leva menos de 20 segundos, enquanto o tempo de funcionamento necessário para decompor um número composto do mesmo tamanho é incalculável (BURTON, 2016, p. 204).

Em consequência, quanto maiores os primos p e q aplicados nesse método criptográfico, mais segura será a transmissão de informações.

A Tabela 3 representa o tempo médio gasto para quebrar o código RSA. "Se houvesse tempo ilimitado de computação e algum algoritmo de fatoração inimaginavelmente eficiente, o sistema de criptografia RSA poderia ser quebrado, mas para o presente ele parece ser bastante seguro" (BURTON, 2016, p. 204).

Tabela 3 – Tempo médio para quebrar o código RSA

Nº de algarismos de n	Tempo necessário para "quebrar"o RSA
50	$3,9$ horas
75	104 dias
100	74 anos
200	$3,8 \cdot 10^7$ séculos
300	$4,9 \cdot 10^{13}$ séculos
500	$4,2 \cdot 10^{23}$ séculos

Fonte: Carvalho (2013, p. 35).

Os criadores do RSA, para provar a eficiência de seu método, lançaram um desafio na revista *Scientific American*, valendo 100 dólares. Segundo eles seria preciso aproximadamente 40 quadrilhões de anos para decifrar o RSA 129[1]. No entanto, dezessete anos depois o número foi decifrado.

Dezessete anos é tempo suficiente para que um cartão de crédito fique seguro, pois nesse período ele já terá perdido a validade e sido renovado. "Contudo, resta a dúvida de quanto tempo passará até que surja um matemático com idéias que transformarão esses dezessete anos em dezessete minutos" (SAUTOY, 2008, p. 194).

A criação de novos algoritmos de fatoração implica na descoberta de números primos p e q progressivamente maiores. Portanto, até quando esse método será inquestionável e seguro - um dos maiores questionamentos em relação à criptografia.

3.2 As cigarras periódicas

"As cigarras são insetos alados que evoluíram cerca de 1,8 milhões de anos atrás durante a época do Pleistoceno, quando as geleiras avançaram e recuaram na América do Norte[2]" (PICKOVER, 2009, p. 22, tradução nossa). As cigarras do gênero *Magicicada* permanecem a maior parte de suas vidas no subsolo e, após um certo período de tempo, emergem para a reprodução e logo morrem.

Segundo Pickover (2009), existem 1500 espécies de cigarras desse mesmo gênero, porém uma pequena parte delas apresentam um comportamento surpreendente. Essas cigarras, em particular, são chamadas cigarras periódicas.

As cigarras periódicas sempre surgem em grande quantidade para terem uma maior chance de sobreviver aos predadores. "Às vezes, mais de 15 milhões de indivíduos emergem em um único acre dentro de um curto intervalo de tempo[3]" (PICKOVER, 2009, p. 22, tradução

[1] "[..] módulo de cifragem de 129 dígitos que foi o produto de dois números primos de aproximadamente a mesma magnitude" (BURTON, 2016, p. 204).

[2] Cicadas are winged insects that evolved around 1.8 million years ago during the Pleistocene epoch, when glaciers advanced and retreated across North America.

[3] Sometimes more than 15 million individuals emerge in a single acre within a short interval of time.

nossa).

A eclosão, geralmente, ocorre em tempos diferentes de outros grupos para que não haja cruzamento entre as espécies, pois suas crias teriam períodos irregulares, o que prejudicaria sua sobrevivência. Elas possuem ciclos de vida primos, porque dessa forma o encontro de espécies coincidirá um menor número de vezes.

Exemplo 3.3. *Sabendo que duas cigarras de espécies diferentes eclodem a cada 7 e 13 anos. Encontremos quando os ciclos irão coincidir-se. Como* 7 *e* 13 *são números primos:*

$$mmc(7,\ 13) = 7 \cdot 13 = 91.$$

Logo, as duas espécies de cigarras irão eclodir simultaneamente a cada 91 *anos .*

Exemplo 3.4. *Sabendo que duas cigarras de espécies diferentes eclodem a cada 13 e 17 anos. Encontremos quando os ciclos irão coincidir-se. Como* 13 *e* 17 *são números primos:*

$$mmc(13,\ 17) = 13 \cdot 17 = 221.$$

Logo, as duas espécies de cigarras irão eclodir simultaneamente a cada 221 *anos .*

Figura 3.1 – Ciclo de vida de cigarras periódicas de 7 e 13 anos

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

Fonte: A autora (2022).

A Figura 3.1 representa visualmente o Exemplo 3.3. Dessa forma, torna-se bem mais fácil visualizar a coincidência dos ciclos, que é exatamente no ano cujo valor é representado pelo

mínimo múltiplo comum entre os períodos. Ou seja, essas espécies se encontrariam apenas uma vez a cada cem anos.

De fato, as cigarras costumam emergir, respectivamente, a cada 13 e 17 anos (como no Exemplo 3.4), no entanto, como afirma Pickover (2009), não se sabe ao certo o que há de especial nesse par de números primos.

Sabe-se que se não fossem utilizados números primos, haveria muito mais eclosões coincidentes. Como o $mmc(a_1,\ b_1) = a_1 \cdot b_1$, se a_1 e b_1 são primos entre si e $mmc(a_2,\ b_2) = \dfrac{a_2 \cdot b_2}{mdc(a_2,\ b_2)}$ se $mdc(a_2,\ b_2) \neq 1$, fica evidente que as cigarras garantem mais a sua sobrevivência ao escolher ciclos com períodos primos.

Para exemplificar essa afirmação, podemos observar, na Figura 3.2, que o período de tempo para que ocorresse o encontro entre essas cigarras com ciclos de 6 e 12 anos, supostamente, aconteceria a cada 12 anos, pois $mmc(6,\ 12) = 12$.

Figura 3.2 – Ciclo de vida de cigarras periódicas de 6 e 12 anos

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

Fonte: A autora (2022).

De acordo com Pickover (2009), esses encontros mais frequentes seriam prejudiciais à sobrevivência dessas cigarras. Hipoteticamente, se uma espécie tivesse um ciclo de vida de 12 anos, possivelmente, ela correria mais riscos de encontrar predadores com ciclos de vida de 2, 3, 4 ou 6 anos.

> Mario Markus, do Instituto Max Planck de Fisiologia Molecular em Dortmund, Alemanha, e seus colegas descobriram que esses tipos de ciclos de números primos surgem naturalmente de modelos matemáticos evolutivos de interações

> entre predador e presa. Para experimentar, eles primeiro atribuíram durações aleatórias do ciclo de vida às suas populações simuladas por computador. Depois de algum tempo, uma sequência de mutações sempre prendeu as cigarras sintéticas em um ciclo estável de números primos [4] (PICKOVER, 2009, p. 22, tradução nossa).

Os números primos, além de misteriosos, também são fascinantes, podendo ser aplicáveis a situações fundamentais para o cotidiano, como a criptografia (Seção 3.1), e ainda serem participantes ativos da natureza.

[4] Mario Markus of the Max Planck Institute for Molecular Physiology in Dortmund, Germany, and his coworkers discovered that these kinds of prime-number cycles arise naturally from evolutionary mathematical models of interactions between predator and prey. In order to experiment, they first assigned random life-cycle durations to their computer-simulated populations. After some time, a sequence of mutations always locked the synthetic cicadas into a stable prime-number cycle.

CONSIDERAÇÕES FINAIS

Este trabalho buscou evidenciar o surgimento da matemática, os primeiros indícios de uso dos números primos, retratou as principais descobertas dos matemáticos precursores da teoria dos números, além de realizar uma breve análise acerca da abordagem histórica como recurso no ensino dos números primos.

Para cumprir o objetivo de enfatizar a importância dos números primos na vida do ser humano, após a contextualização histórica, apresentamos definições, propriedades, descobertas, características e curiosidades sobre esses números. Esses conhecimentos matemáticos específicos, além de sanar dúvidas quanto ao conteúdo, serviram de base para o entendimento das aplicações aqui explanadas.

Analisar a evolução dos números primos, desde a época do Osso de Ishango até a atualidade, mostra como o desenvolvimento da matemática está intrinsecamente relacionado à evolução de outras ciências. Quem poderia imaginar que a teoria dos números, tão abstrata no tempo de Euclides, poderia originar uma aplicação tão presente e relevante na vida do ser humano como a criptografia?

É incrível a possibilidade de aplicar os números primos no cotidiano, entretanto, podemos dizer que é magnífico saber que a natureza também é diretamente influenciada, com espécies de cigarras que dependem desses números pra sobreviver.

Atualmente, a maior parte das pessoas beneficiam-se do que os conhecimentos avançados de teoria dos números propiciam, por exemplo, enquanto fazem compras *online*, jogam na internet, realizam transferências por PIX, enviam mensagens pelo *Whatsapp*, etc. Em atividades cotidianas como essas, o ser humano está depositando a sua confiança na criptografia, lembrando que o método RSA garante a segurança no compartilhamento de informações por meio de números primos gigantes.

Esperamos que as informações obtidas, por meio desta pesquisa, possam levar o leitor a reconhecer o valor da matemática, que por muitas vezes é subestimado. Esse método utilizado para codificar informações só será seguro enquanto não houverem descobertas significativas na fatoração de números grandes. A cargo de curiosidade, o leitor poderá pesquisar sobre a computação quântica, que, se concretizada, mudará totalmento o rumo da criptografia.

Por fim, consideramos importante ressaltar que a evolução do estudo da teoria dos números está relacionada à resolução dos problemas que podem surgir na criptografia.

REFERÊNCIAS

AIRES, L. M. *Uma História da Matemática - Dos Primeiros Agricultores a Alan Turing, dos Números ao Computador*. 1. ed. Lisboa: Edições Sílabo, 2010.

BOYER, C. B. *História da Matemática*. 1. ed. São Paulo: Edgard Blucher, 1974.

BOYER, C. B. *História da Matemática*. 3. ed. São Paulo: Edgard Blucher, 2012.

BRASIL. Ministério da educação. Secretaria de educação. *Parâmetros Curriculares Nacionais: Matemática*, Brasília, MEC/SEF - Terceiro e quarto ciclos, 1998.

BRASIL. Ministério da educação. *Base Nacional Comum Curricular*, Brasília, 2018.

BURTON, D. M. *Teoria Elementar dos Números*: tradução Gabriela dos Santos Barbosa. 7. ed. Lisboa: LTC, 2016.

CARVALHO, G. C. A. D. *Números Primos*: Pequenos tópicos. Dissertação (Mestrado) — Universidade Federal de Goiás, Instituto de Matemática e Estatística, Goiânia, 2013.

COUTINHO, S. C. *Primalidade em Tempo Polinomial*: Uma introdução ao algoritmo AKS. Rio de Janeiro: Sociedade Brasileira de Matemática, 2004.

COUTINHO, S. C. *Número Inteiros e Criptografia RSA*. 2. ed. Rio de Janeiro: Associação Instituto Nacional de Matemática Pura e Aplicada - IMPA, 2007.

DOMINGUES, H. H. *Fundamentos de Aritmética*. Rio de Janeiro: Atual, 1991.

EVES, H. *Introdução à história da matemática*: tradução Hygino H. Domingues. 5. ed. Campinas, São Paulo: Editora da Unicamp, 2011.

MAGALHÃES, A. P. de A. S. *O Processo de Significação Atribuído à História Da Matemática Por Estudantes De Um Curso De Licenciatura Em Matemática*. Tese (Doutorado) — Universidade Federal de Goiás, 2021.

PEJLARE, J.; BRÄTING, K. Writing the history of mathematics: Interpretations of the mathematics of the past and its relation to the mathematics today. *Sriraman B. (eds) Handbook of the Mathematics of the Arts and Sciences*, Springer, Cham, 2019.

PICKOVER, C. A. *The Math Book*: From Pythagoras to the 57th dimension, 250 milestones in the history of mathematics. New York: Sterling, 2009.

RIBENBOIM, P. *Número primos: mistérios e recordes*. Rio de Janeiro: Associação Instituto Nacional de Matemática Pura e Aplicada - IMPA, 2001.

SÁ, I. P. de. *A Magia da "Matemática"*: Atividades Investigativas, Curiosidades e História da Matemática. Rio de Janeiro: Editora Ciência Moderna, 2007.

SANTOS, C. Os números primos de Ishango. *Revista Brasileira Multidisciplinar*, v. 22, n. 2, p. 120 – 130, 2019.

SAUTOY, M. D. *A música dos números primos*: A história de um problema não resolvido na matemática. Rio de Janeiro: Zahar, 2008.

SHOKRANIAN, S. *Criptografia para iniciantes*. Brasília: Editora Universidade de Brasília, 2005.

SPINA, A. V. *Números Primos E Criptografia*. Dissertação (Mestrado) — Universidade Estadual de Campinas, Campinas, 2014.

STEWART, I. *Em busca do infinito*: Uma história da matemática dos primeiros números a teoria do caos. 1. ed. Rio de Janeiro: Zahar, 2014.

STEWART, I. *O fantástico mundo dos números*: A matemática do zero ao infinito. Rio de Janeiro: Zahar, 2016.

Apêndices

APÊNDICE A – CONJECTURA DE GOLDBACH

Em uma carta a Euler, no ano de 1742, o matemático russo Christian Goldbach conjecturou que todo número inteiro maior que 5 pode ser expresso como a soma de três números primos. Como exemplo: $23 = 11 + 7 + 5$ (PICKOVER, 2009).

De acordo com Pickover (2009), a seguinte afirmação, reexpressa por Euler, é denominada conjectura "forte"de Golbach, que diz que todo inteiro par, exceto o 2, pode ser escrito como a soma de dois números primos. Por exemplo: $4 = 2 + 2$; $6 = 3 + 3$; $8 = 5 + 3; \ldots$; $16 = 13 + 3$; $18 = 11 + 7; \ldots$; $48 = 29 + 19; \ldots$; $100 = 97 + 3$; e assim por diante.

Foi oferecido um prêmio pela *Faber and Faber* no valor de 1 milhão de dólares para quem resolvesse a Conjectura de Goldbach, mas até o presente momento ninguém conseguiu resolver esse problema em aberto (PICKOVER, 2009).

"Em 2008, Tomás Oliveira e Silva, investigador da Univerdade de Aveiro, Portugal, realizou uma pesquisa informática distribuída que verificou a conjectura até $12 \cdot 10^{17}$" (PICKOVER, 2009, p. 178)[1]. Entretanto, ainda se espera uma prova que demonstre a conjectura válida para cada número.

[1] In 2008, Tomás Oliveira e Silva, a reseacher at the University of Aveiro, Portugal, ran a distributed computer search that has verified the conjecture up to $12 \cdot 10^{17}$.

APÊNDICE B – HIPÓTESE DE RIEMANN

Esta conjectura foi proposta por Georg Bernhard Riemann, em 1859, e até o momento ninguém conseguiu solucioná-la. "A hipótese de Riemann permanece um dos mais desconcertantes e irritantes enigmas de toda a matemática. Sua resolução seria um dos acontecimentos mais dramáticos na história da matemática" (STEWART, 2016, p. 133).

A partir de uma observação de Gauss acerca do comportamento dos números primos, conforme Santos (2019), Riemann propôs que a função $\zeta(s) = 1 + \frac{1}{2^s} + \frac{1}{3^s} + \frac{1}{4^s} + \ldots$ está intimamente relacionada aos números primos. "A “Hipótese de Riemann” afirma que todas as soluções da equação $\zeta(s) = 0$, no plano complexo, descrevem uma linha vertical" (SANTOS, 2019, p. 126).

De acordo com Stewart (2016), seja $\zeta(z)$, tal que z seja um número complexo. Alguns zeros dessa função podem ser facilmente encontrados, como: $z = -2,\ -4,\ -6,\ -8, \ldots$. Mas Riemann conseguiu mostrar que existem outros infinitos zeros. Após encontrar seis deles,

$$\frac{1}{2} \pm 14,135i \ \ \frac{1}{2} \pm 21,022i \ \ \frac{1}{2} \pm 25,011i$$

Riemann conjecturou que todos os zeros da função zeta, com exceção dos inteiros pares negativos, podem ser escritos da forma $\frac{1}{2} + iy$ (parte real igual a y).

Stewart (2016) conta que essa afirmação de Riemann foi provada para os primeiros 10 trilhões de zeros, entretanto, isso não quer dizer que todos os zeros não triviais estejam sobre a linha crítica. Uma única exceção que, supostamente, ainda não teria sido calculada, é suficiente para destruí-la.

Se essa hipótese revelar-se verdadeira, muitos questionamentos sobre os números primos podem ser respondidos. Como afirma Stewart (2016, p. 134)

> Se soubermos o suficiente sobre os zeros da função zeta, poderemos deduzir um bocado de informação nova sobre os primos a partir da fórmula de Riemann. Informação sobre as partes reais dos zeros, em particular, nos permitirá deduzir propriedades estatísticas dos primos: quantos deles há até um determinado valor, como estão espalhados entre os outros inteiros, e assim por diante.

Além disso, maneiras mais rápidas de encontrar primos também podem ser descobertas.

Santos (2019) declara que a demontração dessa conjectura pode render um prêmio de 1 milhão de dólares, pago pelo *Clay Mathematics Institute*.