Universidade Federal de Goiás
Instituto de Matemática e Estatística
Programa de Mestrado Profissional em
Matemática em Rede Nacional

O Mistério e a Beleza dos Números Primos

Karla Valéria Caldas Mota

Goiânia

2017

sistema de bibliotecas ufg

PRPG
PRÓ-REITORIA DE PÓS-GRADUAÇÃO

UFG

TERMO DE CIÊNCIA E DE AUTORIZAÇÃO PARA DISPONIBILIZAR VERSÕES ELETRÔNICAS DE TESES E DISSERTAÇÕES NA BIBLIOTECA DIGITAL DA UFG

Na qualidade de titular dos direitos de autor, autorizo a Universidade Federal de Goiás (UFG) a disponibilizar, gratuitamente, por meio da Biblioteca Digital de Teses e Dissertações (BDTD/UFG), regulamentada pela Resolução CEPEC nº 832/2007, sem ressarcimento dos direitos autorais, de acordo com a Lei nº 9610/98, o documento conforme permissões assinaladas abaixo, para fins de leitura, impressão e/ou *download*, a título de divulgação da produção científica brasileira, a partir desta data.

1. Identificação do material bibliográfico: **[X] Dissertação** **[ ] Tese**

2. Identificação da Tese ou Dissertação:

Nome completo do autor: Karla Valéria Caldas Mota

Título do trabalho: O Mistério e a Beleza dos Números Primos

3. Informações de acesso ao documento:

Concorda com a liberação total do documento [X] SIM [ ] NÃO[1]

Havendo concordância com a disponibilização eletrônica, torna-se imprescindível o envio do(s) arquivo(s) em formato digital PDF da tese ou dissertação.

Karla Valéria Caldas Mota
Assinatura do(a) autor(a)[2]

Ciente e de acordo:

Assinatura do(a) orientador(a)[2] Data: 14 /01 /2017

[1] Neste caso o documento será embargado por até um ano a partir da data de defesa. A extensão deste prazo suscita justificativa junto à coordenação do curso. Os dados do documento não serão disponibilizados durante o período de embargo.

Casos de embargo:

- Solicitação de registro de patente;
- Submissão de artigo em revista científica;
- Publicação como capítulo de livro;
- Publicação da dissertação/tese em livro.

Karla Valéria Caldas Mota

O Mistério e a Beleza dos Números Primos

Trabalho de Conclusão de Curso apresentado ao Instituto de Matemática e Estatística da Universidade Federal de Goiás, como parte dos requisitos para obtenção do grau de Mestre em Matemática.
Área de Concentração: Matemática do Ensino Básico.
Orientadora: Profª. Drª. Ivonildes Ribeiro Martins Dias.

Goiânia

2017

Ficha de identificação da obra elaborada pelo autor, através do
Programa de Geração Automática do Sistema de Bibliotecas da UFG.

Valéria Caldas Mota, Karla
O Mistério e a Beleza dos Números Primos [manuscrito] / Karla Valéria Caldas Mota. - 2017.
LXI, 61 f.: il.

Orientador: Profa. Dra. Ivonildes Ribeiro Martins Dias.
Dissertação (Mestrado) - Universidade Federal de Goiás, Instituto de Matemática e Estatística (IME), PROFMAT - Programa de Pós graduação em Matemática em Rede Nacional - Sociedade Brasileira de Matemática (RG), Goiânia, 2017.
Bibliografia. Anexos.
Inclui fotografias, lista de figuras.

1. Números primos. 2. hiistória. 3. importência. 4. resultados. 5. curiosidades. I. Ribeiro Martins Dias, Ivonildes, orient. II. Título.

CDU 51

Universidade Federal de Goiás - UFG
Instituto de Matemática e Estatística - IME
Mestrado Profissional em Matemática em Rede Nacional – PROFMAT/UFG
Campus Samambaia – Caixa Postal 131 – CEP: 74.001-970 – Goiânia-GO.
Fones: (62) 3521-1208 e 3521-1137 www.ime.ufg.br

Ata da reunião da banca examinadora da defesa de Trabalho de Conclusão de Curso da aluna Karla Valéria Caldas Mota – Aos catorze dias do mês de dezembro do ano de dois mil e dezessete, às 14:00 horas, reuniram-se os componentes da Banca Examinadora: Profª. Drª. Ivonildes Ribeiro Martins Dias – Orientadora, Profª. Drª. Thaynara Aryelly de Lima – Membro IME/UFG, Profª. Drª. Ticianne Proença Bueno Adorno – Membro IME/UFG, para, sob a presidência do primeiro, e em sessão pública realizada no AUDITÓRIO do IME, procederem a avaliação da defesa intitulada **"O Mistério e a Beleza dos Números Primos"**, em nível de mestrado, área de concentração Matemática do Ensino Básico, de autoria de Karla Valéria Caldas Mota, discente do Programa de Mestrado Profissional em Matemática em Rede Nacional - PROFMAT da Universidade Federal de Goiás. A sessão foi aberta pelo presidente da banca, Profª. Drª. : Ivonildes Ribeiro Martins Dias, que fez a apresentação formal dos membros da banca. A seguir, a palavra foi concedida a autora do TCC que, em 30 minutos, procedeu à apresentação de seu trabalho. Terminada a apresentação, cada membro da banca arguiu ao examinando, tendo-se adotado o sistema de diálogo sequencial. Terminada a fase de arguição, procedeu-se à avaliação da defesa. Tendo em vista o que consta na Resolução nº. 1075/2012 do Conselho de Ensino, Pesquisa, Extensão e Cultura (CEPEC), que regulamenta os Programas de Pós-Graduação da UFG, e procedidas as correções recomendadas, o Trabalho foi **APROVADO** por unanimidade, considerando-se integralmente cumprido este requisito para fins de obtenção do título de **MESTRE EM MATEMÁTICA**, na área de concentração Matemática do Ensino Básico pela Universidade Federal de Goiás. A conclusão do curso dar-se-á quando da entrega, na secretaria do IME, da versão definitiva do trabalho, com as devidas correções supervisionadas e aprovadas pelo orientador. Cumpridas as formalidades de pauta, às 16:00 horas, a presidência da mesa encerrou a sessão e, para constar, eu, Rafael Aguiar e Silva, secretário do PROFMAT/UFG, lavrei a presente ata que, após lida e aprovada, segue assinada pelos membros da Banca Examinadora em quatro vias de igual teor.

Profª. Drª. Ivonildes Ribeiro Martins Dias
Orientadora – IME/UFG

Profª. Drª. Thaynara Aryelly de Lima
Membro – IME/UFG

Profª. Drª. Ticianne Proença Bueno Adorno
Membro - IME/UFG

Karla Valéria Caldas Mota graduou-se em Licenciatura e Bacharelado em Matemática pela Universidade Católica de Goiás (Campus de Goiânia) em 2002, especializou-se em Educação Matemática pela Universidade Católica de Goiás em 2003, atualmente é professora do Ensino Básico e Médio da Secretaria Estadual de Educação de Goiás/Inhumas e no Colégio Monsenhor Angelino.

"a ferramenta mais poderosa que os homens criaram para navegar no selvagem e complexo mundo em que vivemos é a *matemática*".
Marcus Du Sautoy

Aos meus pais, Cleuza e Antonino, pelo apoio e incentivo que tiveram com os meus estudos.
Aos meus filhos, Vinícius e Arthur, pela paciência e compreensão devido a minha ausência.
Ao meu esposo, Márcio, pelo companheirismo e dedicação.

Agradecimentos

Agradeço a Deus por nunca ter me deixado só nessa missão e ter sido tão carinhoso em enviar pessoas que foram como anjos nesssa jornada, que foram solidárias e colaboraram comigo.

Em especial os meus sinceros agradecimentos a minha orientadora Profª. Drª. Ivonildes Ribeiro Martins Dias, que me acolheu com tanto carinho e foi essencial na conclusão deste curso do mestrado.

Resumo

Neste trabalho, abordamos sobre um dos assuntos mais instigantes da matemática: os números primos. O objetivo deste é apresentar a história dos números primos, suas aplicações, curiosidades e assim, estimular educadores e educandos sobre sua importância.

Palavras-chave
Números primos: história, resultados, importância e curiosidades.

Abstract

In this work, we address one of the most instigating subjects in mathematics: prime numbers. The purpose of this is present the history of prime numbers, their applications, curiosities and thus, to stimulate educators and learners about its importance.

Keywords
Prime numbers: history, results, importance and curiosities.

Lista de Figuras

Sumário

Introdução

No Brasil, o ensino de Matemática, geralmente, provoca sensações contraditórias, tanto para os professores, quanto para os alunos. Por um lado, a Matemática é uma área de conhecimento muito importante que está presente na vida cotidiana de qualquer indivíduo, sabemos que ela tem muitas aplicações e funciona como instrumento essencial para a construção de conhecimentos em outras áreas curriculares. Porém, diante dos resultados negativos obtidos com muita frequência em relação à sua aprendizagem, além da forma atual de ensino: formulaíca e sem relacionar os conceitos com a rotina do aluno, a Matemática torna-se um área temida e desprezada pelos educandos, algo que foge à sua possibilidade de compreensão, de pouca utilidade prática, gerando representações e sentimentos que afastarão e afastaram o aluno do conhecimento matemático. Assim, sabemos que existem problemas a serem enfrentados, há urgência em reformular objetivos, rever conteúdos e buscar metodologias compatíveis com a formação que a sociedade precisa. Existe uma grande necessidade de reverter um ensino centrado em procedimentos mecânicos, desprovidos de significados e aplicações para o aluno.

De acordo com a Base Nacional Curricular Comum, BNCC [7], a aprendizagem em Matemática está intrinsecamente relacionada à compreensão dos objetos matemáticos, sem deixar de lado suas aplicações. Ou seja, orienta-se pela necessidade de conhecer a aplicação de seus conceitos como aspecto que favorece o desenvolvimento do raciocínio lógico e crítico, estimula a investigação e pode ser prazeroso.

> O desenvolvimento dessas habilidades está intrinsecamente relacionado a algumas formas de organização da aprendizagem matemática, com base na análise de situações da vida cotidiana, de outras áreas do conhecimento e da própria Matemática. [7, BNCC, p.222]

Além disso, é importante que a Matemática seja reconhecida tanto no contexto

histórico como na aplicabilidade de seus conceitos e associação com as demais áreas para estimular e desenvolver o aprendizado e atrair a atenção para a mesma.

> Reconhecer que a Matemática é uma ciência humana, fruto das necessidades e preocupações de diferentes culturas, em diferentes momentos históricos, e é uma ciência viva, que contribui para solucionar problemas científicos e tecnológicos e para alicerçar descobertas e construções, inclusive com impactos no mundo do trabalho. [7, BNCC, p.223]

Portanto, o estudo histórico e a associação de alguns tópicos matemáticos com outras áreas torna-se cada vez mais necessário como fonte de estímulo para o ensino da Matemática. Pensando nisso, o objetivo deste trabalho é motivar o educador e o educando, sobre a importância do ensino dos números primos, parte central da matemática. Apresentando uma breve referência histórica e também diversas curiosidades que podem instigar o ensino e/ou aprendizagem desse conceito e todos os outros a ele relacionados.

Os Parâmetros Curriculares Nacionais, PCN [11], abrangem de forma muito superficial o estudo dos números primos no ensino fundamental e médio.

> O estudo dos números como objeto matemático também deve partir de contextos significativos para os alunos, envolvendo, por exemplo, o reconhecimento da existência de diferentes tipos de números (naturais, racionais e outros) e de suas representações e classificações (primos, compostos, pares, ímpares, etc.). [7, PCN, p.65]

Assim, educadores, que não estão habituados com a importância e necessidade desse conceito, podem não dar a devida importância para o seu estudo e introdução.

Diante disso, este trabalho tem o intuito de apresentar os números primos não apenas como uma tendência para o algebrismo, mas também como sendo um conteúdo prático e interessante. Poderá ser utilizado como uma das ferramentas para uso didático, abordando parte da teoria dos números e mostrando suas aplicações, auxiliando o docente na elaboração e preparação de assuntos que motivam os estudantes e os fazem entender que a matemática está no cotidiano e a sua fundamental importância.

A ideia de números primos é simples, mas possui riquíssimos resultados e aplicações tanto na própria Matemática quanto em outras áreas. Por exemplo, uma compra na loja online ou mesmo uma consulta a uma conta bancária é mediada através dos

números primos que garantem o funcionamento dos sistema de segurança denominado criptografia.

Na natureza eles manifestam-se em situações surpreendentes. Duas espécies de cigarras, *Magicicada septendecim* e *Magicicada tredecim*, passam quase toda a vida enterradas, mas um pouco antes de morrerem elas emergem do solo para se reproduzirem. Elas possuem ciclos de vida de 17 e de 13 anos, respectivamente, que são ambos primos. Tal fato, supostamente, evita que coincida com o ciclo de nascimento de seus predadores naturais e garante a floresta só para uma espécie por vez. Na física quântica eles manifestam-se por meio dos níveis energéticos dos átomos.

Além disso, os números primos despertaram curiosidades e são utilizados, por alguns escritores ou autores, como ferramentas para certos mistérios em seus livros, filmes ou séries. O que é muito útil para despertar o interesse matemático dos jovens e adultos. Por exemplo, no romance clássico de Carl Sagan, *Contato*, os alienígenas usam números primos para estabelecer comunicação com a vida na terra. Ellie, heroína da estória, trabalha no programa Seti, busca por inteligência extraterrestre, escuta as crepitações do cosmo. Num determinado momento os radiotelescópios captam determinados pulsos. Dois pulsos seguidos por uma pausa, então três pulsos, cinco, sete, onze e assim por diante, seguindo por todos os números primos até 907.

> (...) Sabemos qual é a seqüência de números? Bem, podemos fazê-la de cabeça ... 59, 61, 67 ... 71... Não são todos números primos? Um murmúrio de entusiasmo percorreu a sala de controle. O rosto de Ellie revelou momentaneamente os traços de um sentimento profundo, rapidamente substituído pela sobriedade, um medo de perder o controle, uma apreensão por parecer tola, não científica. [18]

Outro exemplo é o livro *O homem que confundiu sua mulher com um chapéu* de Oliver Sacks, veja [17], que relata o caso de dois irmãos gêmeos de 26 anos de idade, John e Michael, que se comunicam através de números primos de seis algarismos.

> (...) Para mim, é difícil ouví-la e não ficar pasmo e deslumbrado com o funcionamento do cérebro, mas não sei se meus amigos não matemáticos reagem da mesma maneira. Terão eles alguma ideia da natureza bizarra e fantástica, quase sobrenatural, desse talento singular que os gêmeos manifestavam tão naturalmente? Estarão cientes de que os matemáticos têm se esforçado durante séculos para conceber um modo de fazer o que John e Michael faziam espontaneamente: gerar e reconhecer números primos? [17]

Na infinidade desses números ainda encontram-se muitos problemas em aberto, fato este que intriga e aguça a imaginação de especialistas em toda parte do mundo. Tais como: Existem infinitos números primos gêmeos? Sempre existe um número primo entre n^2 e $(n+1)^2$ para qualquer $n \in \mathbb{N}$? Para $n = 0, 1, 2, ..., 40$, tem-se que $n^2 - n + 41$ é primo. Existem infinitos números primos dessa forma? A sequência de Fibonacci $(1, 1, 2, 3, 5, 8, 13, ...)$ contém infinitos números primos?. Também, a distribuição dos números primos ainda é bastante misteriosa. Além disso, temos ainda o mais importante problema em aberto em teoria dos números: A hipótese de Riemann. Esta conjectura relaciona a distribuição dos números primos. Se provado o teorema, muitos dos mistérios que envolvem os números primos serão solucionados, deixando assim o seu realizador num renomado e destacado lugar entre os matemáticos, conhecidos por imortais da matemática, além de receber um magnífico prêmio de 1 milhão de dólares.

A busca pela compreensão dos números primos e pela resolução desses problemas levaram matemáticos ao desenvolvimento de inúmeras técnicas e hipóteses. Para eles, tais desmembramentos são mais importantes do que os próprios números primos.

Escrever sobre um assunto que não recebe a devida importância nos currículos escolares tanto para alunos quanto para alguns professores, foi um grande desafio. A motivação inicial começou quando percebi, enquanto professora, a dificuldade dos alunos de reconhecerem se um número é primo e onde utilizá-los.

Espero que os leitores deste trabalho possam usufruir das informações mostradas e quem sabe, até mesmo, desenvolverem outras pesquisas, já que os números primos possuem uma fantástica e curiosa trajetória.

No Capítulo 1 deste trabalho fizemos uma breve biografia de alguns estudiosos que dedicaram-se, direta ou indiretamente, à pesquisa dos números primos. Também, fizemos uma breve retrospectiva história sobre esses números com o intuito de trazer ferramentas simples e direta ao educador para motivar seus alunos ao introduzir o conceito de números primos.

No Capítulo 2 abordamos temas relacionados a aritmética inicial tais como divisibilidade de números inteiros, divisão euclideana, máximo divisor comum e congruência módulo m. O objetivo principal é alicerçar o conhecimento dos leitores sobre estas propriedades.

No Capítulo 3 apresentamos a definição de números primos, o Teorema Fundamental da Aritmética e outros teoremas relacionados a esses números. Além disso, apresentamos alguns testes de primalidades e alguns números primos especiais.

No Capítulo 4 colocamos algumas curiosidades e conjecturas sobre os números pri-

mos que inspiraram vários estudiosos no desenvolvimento de diversas teorias.

Capítulo 1

Retrospectiva dos números primos

Neste capítulo será abordado um pouco da origem e história dos números primos. Também traremos uma breve biografia de seus estudiosos e admiradores. Para mais detalhes o leitor pode consultar [5].

1.1 A origem dos números primos

Os números primos são estudados desde a época de antigos matemáticos filósofos, na Grécia, até os dias atuais. Suas propriedades e aplicações encantam muitos estudiosos. Receberam este nome devido aos gregos, que dividiam os números em primeiros e secundários. Daí os romanos traduziram a palavra grega para primeiro, que em latim é *primus*. De acordo com [19] o primeiro indício impreciso do momento que a humanidade se deu conta das qualidades especiais desses números é um osso datado de 6500 a.C., conhecido como *Osso de Ishango* que foi decoberto em 1960 nas montanhas da África Central Equatorial. Nele estão escritas três colunas contendo quatro séries de entalhes. Em uma dessas colunas encontramos 11,13,17 e 19 entalhes, uma lista de todos os primos entre 10 e 20.

Os números primos pertencem a uma das áreas mais fascinantes da Matemática, que estuda os números inteiros e suas propriedades: A *Teoria dos números*, considerada uma das áreas mais puras e abstratas onde se tinha poucas aplicações práticas, da qual a aritmética é a parte mais elementar.

> (...) na história da Matemática, a história da Teoria dos números tem um lugar especial. Teoria dos números é a *Rainha da Matemática*. Como nos diz Gauss no século XIX. Esse apelido não foi dado só pela razão de que a Teoria dos números é a parte mais bela da matemática, mas também pelo fato de que ela representa ao mesmo tempo a parte mais antiga e a mais jovem da matemática. Não somente no nosso tempo, mas sempre foi assim, pelo menos desde o início do tempo moderno. Teoria dos números, essa área tão antiga,tem um passado profundo, espetacular e tem um presente ativo e um futuro que deve ser julgado pelas gerações vindouras. [21]

1.2 Números primos e seus admiradores

O estudo dos números primos, transcorre através da matemática, com inúmeras influências. Compreender o mundo em que vivemos é um desafio, mas podemos contar com grandes aliados, *a matemática e seus admiradores*.

1.2.1 Pitágoras

Pitágoras (582a.C. - 497 a.C.), matemático e filósofo grego; nasceu na ilha de Samos na Grécia. Desde muito jovem impressionava seus professores com suas habilidades. Aos 16 anos foi enviado para Mileto, para estudar com Tales, o maior sábio da época.

De acordo com [5] os primeiros passos do desenvolvimento da teoria dos números e o lançamento do futuro misticismo numérico, foram dados por Pitágoras e seus seguidores movidos pela filosofia da fraternidade.

Fundou em Crótona, ao sul da Itália, uma escola filosófica. Os seus discípulos denominavam-se de pitagóricos. Pitágoras desenvolveu grandes estudos na área da matemática, astronomia, música, medicina e científica. Entre suas descobertas sobre a matemática, está a classificação dos números em primos ou compostos, pares ou ímpares.

No estudo de sons musicais, descobriu uma relação entre a altura da nota emitida e o comprimento da corda. As relações que produziam sons harmoniosos, obedeciam uma proporção dos números inteiros. Assim, Pitágoras concluiu que havia uma música que representava as relações numéricas da natureza e que constituía sua harmonia interior.

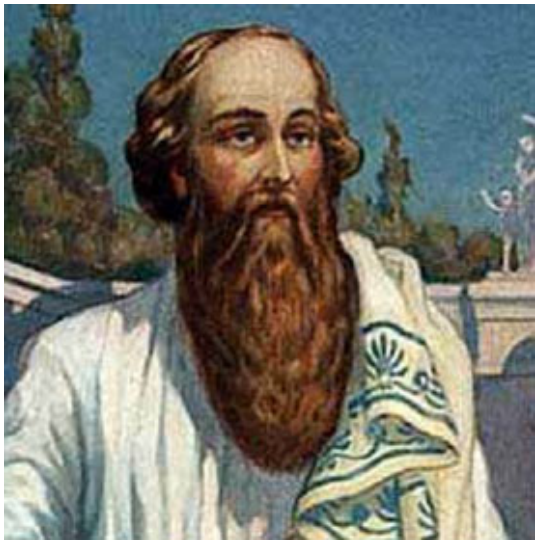

Figura 1.1: *Pitágoras (pinterest.com)*

> Como uma última e notável descoberta sobre números feita pelos pitagóricos, poderíamos mencionar a relação entre intervalos musicais e razões numéricas. Considerando cordas sujeitas a mesma tensão, eles encontraram que para a oitava os comprimentos devem ter razão 2 para 1, para a quinta 3 para 2 e para a quarta 4 para 3. Esses resultados, os primeiros fatos registrados da física e da matemática, levaram os pitagóricos a iniciar o estudo cientifico das escalas musicais. [5, EVES, pg.103].

1.2.2 Euclides

Euclides (305a.C. - 275a.C.) foi um dos mais famosos geômetras da antiguidade, sendo conhecido como o pai da Geometria. Escreveu uma obra, intitulada *Os Elementos*. Esta obra é composta de 13 volumes. O seis primeiros versam sobre Geometria Plana, os Volumes 7 a 9 tratam de Teoria dos Números; o livro X estuda a classificação dos incomensuráveis irracionais (não podem ser medidos); por fim os 3 últimos volumes abordam Geometria no Espaço. Estudou em Atenas com os sucessores de Platão, foi professor de Matemática na Escola Real de Alexandria no Egito.

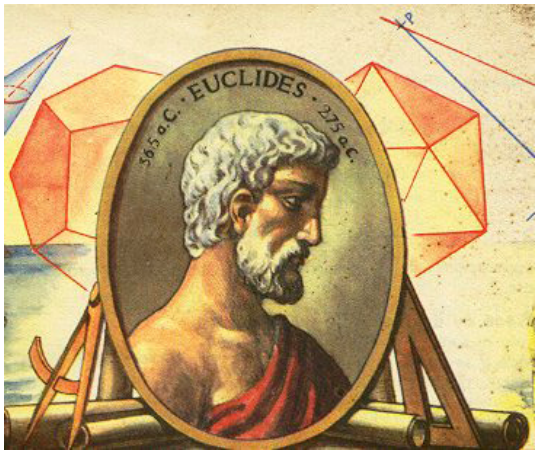

Figura 1.2: *Euclides (diariomasonico.com)*

> (...) Embora Euclides fosse autor de pelo menos dez trabalhos (textos razoavelmente completos, sendo que cinco deles chegarem até nós), sua fama repousa principalmente sobre seus *Elementos*. Parece que este trabalho notável, imediata e completamente superou todos os precedentes; de fato, nenhum vestígio restou de esforços anteriores. Tão logo o trabalho apareceu, ganhou o mais alto respeito e, dos sucessores de *Euclides* até os tempos modernos, a mera citação do número de um livro e o de uma proposição de sua obra prima é suficiente para identificar um teorema ou construção particular. Nenhum trabalho, exceto a *Bíblia*, foi tão largamente usado ou estudado e, provavelmente, nenhum exerceu influência maior no pensamento científico. [5]

Sobre números primos Euclides provou um importante resultado que caracteriza uma das principais propriedades do números primos (veja Lema 3.1.2). Uma consequência muito importante deste resultado é o "Teorema Fundamental da Aritmética" que afirma que todo número inteiro pode ser decomposto como um produto de fatores primos, ou seja, os números primos é o bloco fundamental da teria dos números.

1.2.3 Eratóstenes de Cirene

Eratóstenes (276 a.C.,196 a.C.) foi criado em Cirene, cidade grega ao norte da África. Estudou em Alexandria, no Egito, e depois em Atenas, retornando a Alexandria em 255 a.C., onde se estabeleceu.

Escreveu sobre matemática, astronomia, geografia, história e fez críticas literárias. Conhecido como *Beta* foi escolhido para a administração da biblioteca de Alexandria,

Figura 1.3: *Eratóstenes (webquestfacil.com.br)*

cargo que aceitou em 240 a.C..

> (...) Era também conhecido como *Beta* e a respeito dessa alcunha aventaram-se algumas hipóteses. Alguns acreditam que, devido ao seu saber amplo e brilhante, era alçado a condição de segundo *Platão*. Uma explicação menos abonadora propõe que, não obstante fosse ele talentoso em muitos campos, nunca conseguiu ser o primeiro de seu tempo em campo nenhum. [5]

Umas das contribuições para os estudos da matemática foi o desenvolvimento de um procedimento, chamado de Crivo de Eratóstenes, onde desenvolveu um método para determinar, não com uma fórmula, mas com uma tabela os números inteiros primos, numerados de 0 a um determinado valor.

Porém, a dificuldade é que quanto maior for o número, mais difícil de aplicar o Crivo de Eratóstenes, pois o esforço aliado ao tempo gasto começará a aumentar e dificultará o seu desenvolvimento. Retornaremos neste assunto quando abordarmos os testes de primalidade.

1.2.4 Fermat

O matemático francês Pierre de Fermat (1601-1665) é famoso pela amplitude e excelência dos trabalhos feitos na parte de teoria dos números. Fermat nasceu na França e foi conhecido como o *Príncipe da Matemática*. Filho de um rico mercador que

lhe proporcionou educação privilegiada, tendo a advocacia como profissão, dedicava-se a matemática apenas em suas horas de lazer, considerando apenas como o seu passatempo.

Figura 1.4: *Fermat (pt.wikipedia.org)*

Os seus trabalhos apresentam caráter amador e na grande maioria não foram publicados enquanto ainda estava vivo. Uma parte do que se sabe de suas descobertas provém de anotações feitas em uma edição das obras de Diofanto. Amador mas foi considerado por Pascal como o maior matemático de sua época.

> (...) Foi graças à Fermat que conhecemos diversos conceitos pesquisados e desenvolvidos. Através da influência dos babilônios e pitagóricos Fermat conseguiu se destacar na matemática, não para se auto promover, e sim com pensamentos que visavam facilitar os complexos cálculos da época. Fermat não era ambicioso em relação as descobertas da matemática, pois, não sobrevivia disto, tinha os estudos matemáticos como hobby. [4]

1.2.5 Mersenne

Marin Mersenne (1588-1648) foi um padre e estudioso com interesses matemáticos. De acordo com [4] Mersenne lamentava o fato de não existir naquela época uma organização formal onde os estudiosos pudessem se encontrar regularmente para trocar e discutir ideias e descobertas, disponibilizando assim seu próprio quarto no convento de Minims, onde ocorreram os primeiros encontros regulares de matemáticos que decorreram continuamente até sua morte em 1648.

Figura 1.5: *Mersenne (emlo-portal.br)*

Mantinha contato com nomes importantes no domínio do conhecimento através de uma elaborada rede de correspondência que transmitiam divulgações dos avanços científicos. Deste modo, estimulou o desenvolvimento científico. Depois da sua morte, foram encontradas cartas de 78 correspondentes espalhados pela Europa, entre os quais Fermat em França, Huygens na Holanda, Pell e Hobbes na Inglaterra e Galileu e Torricelli na Itália.

Na matemática sua maior contribuição foi na teoria dos números. Mersenne tentou definir uma fórmula que descrevesse todos os números primos. Estudou música, onde desenvolveu a teoria da ressonância natural e também combinações e permutações com o objetivo de contabilizar sequências de notas musicais.

1.2.6 Euler

Leonhard Euler (1707-1783) foi o matemático mais prolífico na história. Os estudos de Euler na teoria dos números foram embasados nas obras de Pierre de Fermat. Euler desenvolveu algumas das ideias de Fermat, e refutou algumas das suas conjecturas. Foram inúmeros teoremas, demonstrações na parte de teoria dos números, contribuindo de forma bastante significativa. Suas ideias foram a base para os estudos de Carl Friederich Gauss.

Figura 1.6: *Euler (en.wikipedia.org)*

> (...) Porém, até para o grande *Euler* foi difícil encontrar uma fórmula simples que gerasse todos os primos. Em 1751, ele escreveu que: *há alguns mistérios nos quais a mente humana jamais penetrará. Para nos convecermos deste fato; basta fitarmos as tabelas de primos e percebermos que ali não reina qualquer ordem ou regra.* [19]

Euler introduziu e provocou a expansão da função zeta de Riemann, uma generalização, que mais tarde recebeu o nome de Bernhard Riemann.

1.2.7 Gauss

Carl Friedrich Gauss (1777-1855) é considerado um dos maiores matemáticos de todos os tempos. Contribuiu praticamente para todos os ramos da matemática e para a teoria dos números, área esta que lhe chamava bastante atenção.

Figura 1.7: *Gauss (pt.wikipedia.org)*

Conta-se que um professor de Matemática mandou aos alunos de sua turma que somassem de 1 a 100, como forma de castigo. Tarefa que Gauss cumpriu quase que de imediato com a utilização de um raciocínio que fascinou o professor. Sua tese de doutorado foi a primeira demonstração do teorema fundamental da álgebra.

> O problema de distinguir os números primos dos números compostos e de exprimir estes últimos à custa de seus fatores primos deve ser considerado como um dos mais importantes e úteis em Aritmética. Ele tem envolvido o esforço e a sabedoria de antigos e atuais matemáticos em tal escala que seria inútil discutir o problema detalhadamente... Apesar disso, a própria dignidade da ciência requer que todos os meios possíveis sejam explorados para a resolução de um problema tão elegante e famoso?. K.F. Gauss

1.2.8 Dirichlet

Dirichlet (1805-1859), nasceu na Alemanha onde seu pai era chefe dos correios. Foi o responsável pela definição formal de função.

Figura 1.8: *Dirichlet (pt.wikipedia.org)*

De 1828 até o ano de seu falecimento, Dirichlet trabalhou na Faculdade Militar de Berlim, no Colégio Militar e na Universidade de Gottingen, onde substituiu Gauss. Estudou os números primos em progressões aritméticas.

1.2.9 Riemann

Bernhard Riemann (1826-1866) foi um dos matemáticos que também estudou a busca pelos números primos, mesmo não sendo da área de seu interesse, a teoria dos números.

Riemann teve a ideia de definir uma função, que teve o nome de função Zeta, para todos os números complexos, de modo que tivessem a parte real maior que 1.

A hipótese de Riemann é uma afirmação matemática de que é possível decompor os números primos em música. Dizer que existe música nos primos é uma forma poética de descrever esse teorema matemático.

Figura 1.9: *Riemann (thefamouspeopli.com)*

Capítulo 2

Aritmética Inicial

Neste capítulo faremos uma breve abordagem acerca da construção e propriedades dos números inteiros, para mais detalhes veja [6, 12, 20].

2.1 Números naturais

Para estudar sobre números primos e demonstrar alguns de seus resultados é necessário um prévio conhecimento dos números inteiros e suas propriedades fundamentais. É inevitável, antes de abordar tais propriedades, uma menção ao conjunto dos números naturais. Não faremos aqui uma construção desses números, admitiremos que o leitor já conheça o conjunto dos números naturais, denotado por $\mathbb{N} = \{1, 2, 3...\}$[1], e as operações de adição e multiplicação desses números. Além disso, admitiremos que a relação de ordem "menor que" e todas as suas propriedades sejam bem conhecidas pelo leitor. Porém, não poderíamos deixar de mencionar a base da construção dos números naturais, ou seja, os *Axiomas de Peano*, escrito por Giussepe Peano (1858-1932).

Axiomas de Peano.

1. *Todo número $n \in \mathbb{N}$ possui um único sucessor $n + 1$, que também é um número que $\in \mathbb{N}$.*
2. *Números naturais diferentes têm sucessores diferentes.*
3. *Existe um único número natural, designado por 1, que não é sucessor de nenhum outro.*

[1] alguns autores consideram que $0 \in \mathbb{N}$

4. *Seja X um conjunto $\in \mathbb{N}$. Se $1 \in X$ e se, além disso, o sucessor de cada elemento de X ainda $\in X$, então $X = \mathbb{N}$.*

O item 4 dos Axiomas de Peano é a base para o *Princípio de Indução Finita* e gera uma técnica para demonstrações de afirmações sobre o conjunto dos números naturais denominada *Demonstração por Indução* que enunciamos à seguir, para mais detalhes veja [20].

Princípio de Indução. *Seja $\mathcal{P}$ uma afirmação sobre o conjunto dos números naturais. Se $\mathcal{P}(1)$ é verdadeira e, além disso, sempre que $\mathcal{P}(a)$ for verdadeira implicar que $\mathcal{P}(a+1)$ é verdadeira, então $\mathcal{P}(n)$ é verdadeira para todo $n \in \mathbb{N}$.*

2.2 Números inteiros

O conjunto dos números inteiros originou-se do conjunto dos números naturais. Sua criação teve como objetivo solucionar problemas que envolvem contagem, tais como situações relacionando lucros e prejuízos. Admitiremos que o leitor já esteja familiarizado com o conceito de números inteiros, denotado por $\mathbb{Z} = \{..., -2, -1, 0, +1, +2, ...\}$, juntamente com as operações de adição e multiplicação.

Abordaremos a seguir as propriedades das operações de adição e multiplicação dos números inteiros que são denominadas propriedades básicas da aritmética.

Propriedade 2.2.1. *Para todos $a, b, c \in \mathbb{Z}$ valem as seguintes propriedades:*

1. *$a + b = b + a$ e $ab = ba$ (Propriedade comutativa da adição e multiplicação);*
2. *$(a + b) + c = a + (b + c)$ e $(ab)c = a(bc)$ (Propriedade associativa da adição e multiplicação);*
3. *$a + 0 = a$ e $a.1 = a$ (Existência do elemento neutro 0 da adição e 1 da multiplicação);*
4. *Existe $b \in \mathbb{Z}$ tal que $a + b = 0$ (Existência do elemento simétrico da adição);*
5. *$a(b + c) = ab + ac$ (Propriedade distributiva).*

Para cada $a \in \mathbb{Z}$ o elemento simétrico de a é denotado por $-a$ e $a - b$ significa $a+(-b)$. Assim, o conjunto dos números inteiros pode ser descrito por $\mathbb{Z} = \mathbb{N} \cup \{0\} \cup -\mathbb{N}$, onde $-\mathbb{N} = \{-a | a \in \mathbb{N}\}$ é o conjunto dos simétricos dos números naturais.

O conjunto dos números naturais são denominados *positivos* e seus simétricos denominados *negativos*. Dessa forma, podemos definir no conjunto dos números inteiros a relação *menor que* conforme definição abaixo.

Definição 2.2.2. *Para $a, b \in \mathbb{Z}$ dizemos que a é menor que b, denotado por $a < b$, se $b - a \in \mathbb{N}$. Neste caso, dizemos que b é maior que a e denotamos por $b > a$.*

Dizemos que $a \leq b$ se $a < b$ ou $a = b$. De maneira análoga, $b \geq a$.

Observe que, segue da definição que $a \in \mathbb{N}$ se, e somente se, $a > 0$. E se $a \in -\mathbb{N}$ então $a < 0$. Além disso, se $x \in \mathbb{Z}$ temos que uma única das seguintes afirmações é verdadeira: $x > 0$, $x < 0$ ou $x = 0$.

As seguintes propriedades não serão demonstradas, para mais detalhes veja [20].

Propriedade 2.2.3. *Para $a, b \in \mathbb{Z}$ valem as seguintes afirmações.*

1. *Seja $c \in \mathbb{Z}$, $a < b$ se, e somente se, $a + c < b + c$.*

2. *Para $c \in \mathbb{N}$, $a < b$ se, e somente se, $ac < bc$.*

3. *Se $a < b$ e $c \in -\mathbb{N}$ então $ac > bc$;*

4. *Se $a < b$ e $b < c$ então $a < c$.*

Dizemos que um subconjunto $A \subset \mathbb{Z}$ é *limitado inferiormente* se existe $x \in \mathbb{Z}$ tal que $x \leq a$ para todo $a \in A$. Um *menor elemento* do conjunto $A \subset \mathbb{Z}$ é um elemento $m \in A$ tal que $m \leq a$ para todo $a \in A$. De maneira análoga, S é *limitado superiormente* se existe $b \in \mathbb{Z}$ tal que $b \geq a$ para todo $a \in S$. Um *maior elemento* do conjunto $A \subset \mathbb{Z}$ é um elemento $M \in S$ tal que $M \geq a$ para todo $a \in A$.

Uma das principais propriedades dos números inteiros é o *Princípio da Boa Ordenação* enunciado a seguir:

Princípio da boa ordenação. *Se A é um subconjunto não vazio dos números inteiros limitado inferiormente, então A possui um menor elemento.*

Segue diretamente desse resultado que todo subconjunto dos inteiros limitado superiormente possui um maior elemento.

Proposição 2.2.4. *Não existe número inteiro n entre 0 e 1.*

Demonstração. De fato, suponha por contradição que existe $n \in \mathbb{Z}$ com $0 < n < 1$ e considere $S = \{x \in \mathbb{Z} | 0 < x < 1\}$. Como $0 \leq x$ para todo $x \in S$, S é limitado inferiormente e, pelo princípio da boa ordenação, possui um menor elemento, digamos $a \in S$. Assim, $0 < a < 1$ como $a > 0$ segue do item 2 da Proposição 2.2.3 que $0 < a^2 < a$. Ou seja, $a^2 \in S$ e $a^2 < a$, o que contraria o fato de a ser menor elemento de S. Logo não existe inteiro entre 0 e 1. □

Podemos enunciar o princípio de indução sobre o conjunto dos números inteiros da seguinte maneira:

Princípio de Indução. *Seja $\mathcal{P}$ uma afirmação sobre o conjunto dos números inteiros. Se $\mathcal{P}(a)$ é verdadeira e, além disso, sempre que $\mathcal{P}(n)$ for verdadeira implicar que $\mathcal{P}(n+1)$ é verdadeira, então $\mathcal{P}(n)$ é verdadeira para todo $n \geq a$.*

Definição 2.2.5. *Para $a, n \in \mathbb{Z}$, com $n \geq 0$, definimos a n-ésima potência de a por*

$$a^n = \begin{cases} 1, \ se \ \ n = 0 \\ a^{n-1}a, \ se \ \ n \neq 0. \end{cases} \tag{2.1}$$

As seguintes propriedades podem ser provadas por indução, para mais detalhes veja [6].

Propriedade 2.2.6. *Sejam $a, b \in \mathbb{Z}$ e $m, n \in \mathbb{N}$. Então,*

1. $a^m.a^n = a^{m+n}$;
2. $(a^m)^n = a^{mn}$;
3. $(a.b)^n = a^n.b^n$.

Definiremos também o *fatorial* de um número $n \in \mathbb{N} \cup 0$ por $1! = 1$ e $n! = n(n-1)!$. Segue, por indução, que $n! = n.(n-1)...2.1$. Assumiremos que $0! = 1$.

2.3 Divisibilidade de números inteiros

Definição 2.3.1. *Dado dois números inteiros a e b dizemos que a divide b, denotado por $a \mid b$, se existe $c \in \mathbb{Z}$ tal que $b = ac$.*

Exemplo 2.3.2. *De acordo com a definição $2 \mid 8$, pois $8 = 2.4$. Também, $2|0$ pois $0 = 2.0$. Além disso, para todo $a \in \mathbb{Z}$ temos que $a \mid a$, $1 \mid a$ e $a \mid 0$. De fato, $a = 1.a$ e $0 = 0.a$.*

Proposição 2.3.3. *Sejam $a, b, d \in \mathbb{Z}$. Se $d \mid a$ e $d \mid b$, então $d \mid (ax+by)$ para qualquer $x, y \in \mathbb{Z}$.*

Demonstração. Se $d \mid a$ e $d \mid b$ implica que existem $f, g \in \mathbb{Z}$ tais que $a = fd$ e $b = gd$. Assim, temos que

$$ax + by = x(fd) + y(gd) = d(xf) + d(yg) = d(xf + yg), \tag{2.2}$$

Logo, $d \mid (ax + by)$. □

Proposição 2.3.4. *Se $a \mid b$ e $b \mid c$ então temos que $a \mid c$, para todos $a, b, c \in \mathbb{Z}$.*

Demonstração. Se $a \mid b$ e $b \mid c$ implica que existem $f, g \in \mathbb{Z}$, de tal modo que podemos escrever $b = fa$ e $c = gb$. Assim, temos que

$$c = gb = g(fa) = (gf)a. \tag{2.3}$$

Logo, $a \mid c$. □

Considere o *módulo* ou *valor absoluto* de um número inteiro a, denotado por $|a|$, definido por $|a| = a$ se $a \geq 0$ e $|a| = -a$ se $a < 0$. Pode-se mostrar que $|ab| = |a|.|b|$, quaisquer que sejam os inteiros a e b, e $|ab| \geq |a|$ para todo $b \neq 0$.

Propriedade 2.3.5. *Se $a \mid b$ e $b \neq 0$ então temos que $|a| \leqslant |b|$.*

Demonstração. De fato, se $a \mid b$, existe $c \in \mathbb{Z}$ tal que $b = ca$. Assim, $|b| = |c||a|$. Como $b \neq 0$, temos que $c \neq 0$, logo $1 \leqslant |c|$ e, consequentemente, $|a| \leqslant |a||c| = |b|$. □

2.4 Divisão euclidiana

A divisão euclidiana, enunciada no livro *Os Elementos* para números naturais, é um resultado central da aritmética. Para sua demonstração utilizaremos a *Propriedade Ar-*

quimediana uma importante propriedade dos números inteiros que é uma consequência imediata do princípio da boa ordenação.

Propriedade 2.4.1 (Propriedade Arquimediana)**.** *Sejam $a, b \in \mathbb{Z}$, com $b \neq 0$. Então existe $x \in \mathbb{Z}$ tal que $xb > a$.*

Demonstração. De fato, como $b \neq 0$ segue que $|b| \neq 0$. Assim, pela Proposição 2.2.4, temos que $|b| \geq 1$. Agora,

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

Logo, para $b > 0$ faça $n = |a| + 1$ e para $b < 0$ faça $n = -(|a| + 1)$. □

Teorema 2.4.2 (Divisão Euclideana)**.** *Sejam a, b dois números $\in \mathbb{Z}$ com $b \neq 0$. Existem dois únicos números $q, r \in \mathbb{Z}$, chamados respectivamente de quociente e resto tais que*

$$a = bq + r, \text{ com } 0 \leqslant r \leqslant |b|. \tag{2.4}$$

Demonstração. Seja $S = \{a - by | y \in \mathbb{Z}\} \cap (\mathbb{N} \cup \{0\})$. Note que, pela Propriedade 2.4.1, S não é vazio. Além disso, S é limitado inferiormente por zero, logo S possui um menor elemento r.

Consideremos que $r = a - bq$ para certo $q \in \mathbb{Z}$. Como $r \geqslant 0$, basta mostrar que $r < |b|$. Suponhamos por absurdo que $r \geqslant |b|$. Portanto existe um $s \in \mathbb{N}$ tal que $r = |b| + s$, logo $0 \leqslant s < r$. Além disso, $s = r - |b| = a - bq - |b| = a - (q \pm 1)b \in S$, o que contradiz o fato de r ser o menor elemento do conjunto S. Logo, $r < |b|$.

Unicidade. Suponha que $a = bq + r = bq_1 + r_1$, onde $q, q_1, r, r_1 \in \mathbb{Z}, 0 \leqslant r < |b|$ e $0 \leqslant r_1 < |b|$. Suponha, sem perda de generalidade, que $r_1 > r$. Assim, $0 < r_1 - r < |b|$. Além disso, $r_1 - r = (a - bq) - (a - q_1 b) = (q_1 - q)b$, ou seja, $b | r_1 - r$ o que só é possível se $r_1 - r = 0$ isto é, $r_1 = r$ e $q_1 = q$. □

2.5 Congruência

Uma das ferramentas mais importantes em teoria dos números é a aritmética modular, que tem origem da noção de congruência.

Definição 2.5.1. *Sejam $a, b, n \in \mathbb{Z}$, com $n > 1$. Então dizemos que a é congruente a b módulo n, representado por $a \equiv b \mod n$, se $n \mid (a - b)$.*

As seguintes propriedades não serão demonstradas mas as provas podem ser encontradas em [20].

Propriedade 2.5.2. *Sejam $a, b, c, d, n \in \mathbb{Z}$, com $n > 1$. Então, as seguintes propriedades são verdadeiras:*

1. $a \equiv a \mod n$;
2. *Se* $a \equiv b \mod n$, *então* $b \equiv a \mod n$.
3. *Se* $a \equiv b \mod n$ *e* $c \equiv d \mod n$, *então* $a + c \equiv b + d \mod n$;
4. *Se* $a \equiv b \mod n$ *e* $c \equiv d \mod n$, *então* $ac \equiv bd \mod n$;
5. *Se* $a \equiv b \mod n$, *então* $ac \equiv bc \mod nc$;
6. *Se* $a \equiv b \mod n$, *então* $a^r \equiv b^r \mod n$ *para todo* $r \in \mathbb{N}$.
7. *Se* $a \equiv b \mod n$ *e* $c \mid n$, *então* $a \equiv b \mod c$.

2.6 Máximo Divisor Comum

Para $a, d \in \mathbb{Z}$, se $d|a$ dizemos que d é um *divisor* de a. O inteiro d é dito *divisor comum* entre a e b se $d|a$ e $d|b$. Definiremos agora o máximo divisor comum entre a e b.

Definição 2.6.1. *Sejam $a, b \in \mathbb{Z}$ com pelo menos um deles diferente de zero. O máximo divisor comum de a, b é um inteiro positivo d tal que:*

1. $d \mid a$ *e* $d \mid b$
2. *Se* $c \in \mathbb{Z}$ *é tal que* $c \mid a$ *e* $c \mid b$ *então* $c \mid d$.

O máximo divisor comum entre a e b é denotado por $d = mdc(a, b)$ ou por $d = (a, b)$.

Sejam $a, b \in \mathbb{Z}$ com $a \neq 0$ e $b \neq 0$. Considere $S = \{ax + by | x, y \in \mathbb{Z}\} \cap \mathbb{N}$. Então, existe um menor elemento $d \in S$. Assim, existem x_0, $y_0 \in \mathbb{Z}$ tais que $d = ax_0 + by_0$. Afirmamos que, $d = (a, b)$. De fato, pelo Teorema 2.4.2 existem $q, r \in \mathbb{Z}$ tais que

$a = dq + r$ com $0 \leq r < d$. Assim, $r = a - dq = a - (x_0 a + y_0 b)q = (1 - x_0 q)a - y_0 bq \in S$ se $r \neq 0$ mas $r < d$ então $r = 0$ e $d|a$. De modo análogo, $d|b$. Agora, se $c|a$ e $c|b$ pela Proposição 2.3.3 segue que $c|d$. Logo, se $d = (a, b)$ existem x_0, $y_0 \in \mathbb{Z}$ tais que $d = ax_0 + by_0$. Em particular, se (a, b) existem x_0, $y_0 \in \mathbb{Z}$ tais que $ax_0 + by_0 = 1$. Reciprocamente, se existem x_0, $y_0 \in \mathbb{Z}$ tais que $ax_0 + by_0 = 1$ e $d = (a, b)$ então pela Proposição 2.3.3 $d|1$ e consequentemente $d = 1$.

Se a e $b \in \mathbb{Z}$ tais que $(a, b) = 1$ dizemos que a e b são *primos entre si* ou *coprimos*. De acordo com a observação anterior a e b são primos entre si se, e somente se, existem x_0, $y_0 \in \mathbb{Z}$ tais que $ax_0 + by_0 = 1$.

Teorema 2.6.2 (Lema de Gauss)**.** *Sejam a, b e $c \in \mathbb{Z}$. Se $a|bc$ e $(a, b) = 1$, então $a|c$.*

Demonstração. De fato, por hipótese $a|bc$, assim existe $r \in \mathbb{Z}$ tal que $bc = ra$. Por outro lado, como $(a, b) = 1$ existem x_0, $y_0 \in \mathbb{Z}$ tais que $ax_0 + by_0 = 1$. Multiplicando por c obtemos que $c = ax_0 c + by_0 c = (x_0 c + y_0 r)a$. Logo, $a|c$. □

Capítulo 3

Números primos: definição e propriedades

Neste capítulo abordaremos algumas propriedades e teoremas sobre números primos, para mais detalhes veja [6, 20].

3.1 Definição de números primos

O conjunto dos números primos é o bloco central da matemática, conforme veremos no Teorema 3.2.1, e está relacionado a vários mistérios e problemas famosos.

Definição 3.1.1. *Um número natural maior do que 1 que só possui como divisores positivos 1 e ele mesmo é chamado de número primo.*

Logo, se p é primo e $d|p$, com $d \in \mathbb{N}$, segue que $d = 1$ ou $d = p$. Em particular, se p e q são primos tais que $q|p$ então $p = q$. Além disso, se p não divide a temos que $(a, p) = 1$.

Um número maior do que 1 e que não é primo é chamado de *número composto*. Portanto, se um número natural $n > 1$ é composto, existe um divisor natural n_1 de n tal que $1 < n_1 < n$. Logo, existirá um número natural n_2 tal que $n = n_1 n_2$, com $1 < n_1 < n$ e $1 < n_2 < n$.

O seguinte resultado é uma propriedade que caracteriza totalmente os números primos e foi demonstrada por Euclides no livro Os Elementos.

Lema 3.1.2 (Lema de Euclides)**.** *Sejam os números a, b, p pertencentes ao conjunto $\mathbb{Z}$ com p primo. Se $p \mid ab$, então $p \mid a$ ou $p \mid b$.*

Demonstração. Suponha que $p \nmid a$, então $mdc(p, a) = 1$. Assim, $p|ab$ e $mdc(a, p) = 1$, segue pelo Teorema 2.6.2, que $p \mid b$. □

Proposição 3.1.3. *Se $p > 3$ é primo, então $p = 6k + 1$ ou $p = 6k - 1$, com $k \in \mathbb{Z}$.*

Seja $p \in \mathbb{Z}$, pelo Teorema 2.4.2 existem $q, r \in \mathbb{Z}$, com $0 \leq r < 6$, tais que $p = 6q + r$. Logo, os possíveis restos da divisão de p por 6 são 0, 1, 2, 3, 4 ou 5. Suponha que $p > 3$ é primo, então $r \neq 0, 2, 3$ e 4 (já que nesses casos teríamos um inteiro $1 < s < 6$ dividindo p). Assim, $r = 1$ ou 5. Se $r = 1$, temos que $p = 6q + 1$. Agora, se $r = 5$, temos que $p = 6q + 5 = 6q + 6 - 1 = 6(q + 1) - 1 = 6k - 1$, com $k = q + 1$. O que prova a proposição sobre números primos.

3.2 Teorema fundamental da aritmética

O Teorema Fundamental da Aritmética afirma que os números primos formam um bloco para a construção dos números inteiros.

Teorema 3.2.1. *Todo número natural maior do que 1 ou é primo ou se escreve de modo único (a menos da ordem dos fatores) como um produto de números primos.*

Demonstração. Provaremos por indução sobre um número natural $n \geq 2$. O primeiro passo da indução se verifica já que 2 é primo. Agora considere $n > 2$. Se n é primo, nada temos a demonstrar. Suponhamos, então, que n seja composto. Logo, existem números inteiros naturais n_1 e n_2 tais que $n = n_1 n_2$, com $1 < n_1 < n$ e $1 < n_2 < n$. Por indução, temos que existem números primos $p_1, p_2, ..., p_r$ e $q_1, q_2, ..., q_s$ tais que $n_1 = p_1 p_2 ... p_r$ e $n_2 = q_1 q_2 ... q_s$. Portanto, $n = p_1 p_2 ... p_r q_1 q_2 ... q_s$.

Para provar a unicidade da escrita suponhamos que temos $n = p_1 p_2 ... p_r = q_1 q_2 ... q_s$; onde p_i e q_j são números primos para $1 \leq i \leq r$ e $1 \leq j \leq s$. Assim, $p_1 \mid q_1 q_2 ... q_s$ e pelo Lema 3.1.2 $p_1 | q_j$ para algum $1 \leq j \leq s$. Logo $p_i = q_j$, reordenamento os índices, se necessário, podemos supor que $p_1 = q_1$. Portanto, $p_2 ... p_r = q_2 ... q_s$ e como $p_2 ... p_r < n$, por indução, $r = s$ e $p_i = q_j$ para todos $2 \leq i \leq r$ e certos $2 \leq j \leq r$. □

De acordo com o teorema anterior qualquer que seja $n \in \mathbb{N}$ pode ser escrito (unicamente) como o produto de fatores primos, digamos $n = p_1 p_2 ... p_r$, reordenando os

primos de modo que $p_1 < p_2 < ... < p_s$ e reagrupando os termos semelhantes obtemos que $n = p_1^{\alpha_1}...p_s^{\alpha_s}$, com $1 \leq \alpha_i \leq r$. Assim, provamos o seguinte teorema.

Teorema 3.2.2. *Seja $n > 1$ um inteiro positivo. Então, existem números primos positivos $p_1 < p_2 < ... < p_s$ e $\alpha_1, \alpha_2, ..., \alpha_s$ pertencentes aos números naturais, tal que $n = p_1^{\alpha_1}...p_s^{\alpha_s}$. Além disso, essa decomposição é única.*

Observe que esse teorema pode ser estendido para um número inteiro qualquer $a \neq 0$, já que se $a < 0$ então $-a > 0$ e, pelo teorema anterior, $-a = p_1^{\alpha_1}...p_s^{\alpha_s}$ para certos primos $p_1 < p_2 < ... < p_s$ e $\alpha_i \in \mathbb{N}$. Logo $a = -p_1^{\alpha_1}...p_s^{\alpha_s}$.

3.3 Pequeno Teorema de Fermat

Primeiramente vamos determinar os coeficientes da expressão $(1 + x)^n$, onde x é uma variável e $n \in \mathbb{N}$.
Para $n = 1$ temos $(1 + x)^1 = 1 + x$;
Para $n = 2$ temos $(1 + x)^2 = (1 + x)(1 + x) = 1 + 2x + x^2$;
Para $n = 3$ temos que $(1 + x)^3 = (1 + x)^2(1 + x) = (1 + 2x + x^3) = 1 + 3x + 3x^2 + x^3$;
Assim, $(1 + x)^n = a_0 + a_1x + ... + a_nx^n$.
O termo a_i será denotado por $a_i = \binom{n}{i}$ e denominado de *número binominal*. Observe que $a_0 = 1 = a_n$, logo $\binom{n}{0} = \binom{n}{n} = 1$. Além disso, como $a_{n+r} = 0$ para todo $r \geq 1$, segue que $\binom{n}{i} = 0$ se $i > n$. Pode-se provar, por indução, que para todos $n, i \in \mathbb{N}$ com $1 \leq i \leq n$,

$$\binom{n}{i} = \frac{n!}{i!(n-i)!}. \tag{3.1}$$

Lema 3.3.1. *Para p primo e $1 \leq i \leq p - 1$, $p|\binom{p}{i}$.*

Demonstração. Se $i = 1$ pela Equação (3.1) $\binom{p}{1} = \frac{p!}{1!(p-1)!} = p$, o resultado é verdadeiro. Podemos supor então que $1 < i < p - 1$. Então pela Equação (3.1)

$$\binom{p}{i} = \frac{p!}{i!(p-i)!} = \frac{p.(p-1)...(p-(i-1))(p-i)!}{i!(p-i)!} = \frac{p.(p-1)...(p-i+1)}{i!} \in \mathbb{N}.$$

Logo, $i!|p.(p-1)...(p-i+1)$. Como $1 < i < p-1$, $(i!, p) = 1$ e $i!|(p-1)...(p-i+1)$. Portanto,

$$\binom{p}{i} = p\frac{(p-1)...(p-i+1)}{i!}.$$

□

Teorema 3.3.2 (Pequeno Teorema de Fermat)**.** *Dado um número primo p e $a \in \mathbb{Z}$ então $a^p \equiv a \mod p$.*

Demonstração. Se $p = 2$, então $a^2 - a = a(a-1)$ é um número par e $p|a^2 - a$. Suponhamos então que $p > 2$ e $a \geqslant 0$. Vamos provar por indução sobre a. Para $a = 0$, o resultado é verdadeiro pois $p|0 = a^p - a$. Suponhamos que o teorema é verdadeiro para $a > 0$. Provaremos para $a + 1$.

$$(a+1)^p - (a+1) = a^p + \binom{p}{1}a^{p-1} + ... + \binom{p}{p-1}a - a - 1 = (a^p - a) + \binom{p}{1}a^{p-1} + ... + pa.$$

Logo, utilizando a hipótese de indução e o Lema 3.3.1, o resultado é verdadeiro para $a > 0$. Agora, se $a < 0$, então $-a > 0$ e pelo passo anterior $(-a)^p = -a^p \equiv -a \mod p$, já que p é ímpar. O resultado segue da Propriedade 2.5.2 item 4. □

Observe que se p não divide a então $(a, p) = 1$. Como $p|a^p - a = a(a^{p-1} - 1)$ segue que $p|a^{p-1} - 1$. Assim, obtemos uma consequência direta do teorema anterior, também conhecida como Pequeno Teorema de Fermat.

Corolário 3.3.3 (Pequeno Teorema de Fermat)**.** *Se p é primo e $a \in \mathbb{Z}$ com $(a, p) = 1$, então $a^{p-1} \equiv 1 \mod p$.*

3.4 A infinidade de números primos

Quantos números primos existem? Essa pergunta foi respondida por Euclides no Livro 9 dos *Os Elementos*. Utilizaremos a mesma prova dada por Euclides, onde pela primeira vez se registra o uso de uma demonstração por redução ao absurdo em matemática. Essa demonstração é considerada uma das pérolas da matemática. O Teorema de Euclides é um resultado fundamental estabelecido em teoria de números que garante a existência de uma infinidade de números primos, para mais detalhes veja [6].

> (...) A prova de Euclides (o número de números primos é infinito) é considerada universalmente pelos matemáticos como um modelo de elegância matemática. Ela emprega o método indireto, ou redução ao absurdo(...) [5]

Teorema 3.4.1. *O conjunto formado pelos números primos é infinito.*

Demonstração. Suponhamos que exista somente uma quantidade finita de números primos, digamos: $p_1, p_2, p_3, \ldots, p_n$. Consideremos o número $k = p_1p_2p_3 \ldots p_n + 1$. Como k é inteiro e $k > 2$, existe um primo p tal que $p \mid k$. Segue então que $p = p_i$ para algum $1 \leq i \leq n$. Logo $p_i \mid k$. Mas $p_i | p_1p_2p_3 \ldots p_n$. Assim $p_i | k - p_1p_2p_3 \ldots p_n = 1$, o que é um absurdo. □

Como existem infinitos números primos uma pergunta importante é como eles estão distribuídos. De acordo com [6] a distribuição dos números primos é ainda bastante misteriosa e está associada a muitos problemas em aberto.

3.5 Números primos especiais

Nesta seção, abordaremos certos números naturais que possuem formas ou propriedades especiais.

3.5.1 Números primos de Fermat

Os números de Fermat são os números escritos da forma $F_n = 2^{2^n} + 1$, sendo n pertencentes aos números naturais.

De acordo com [6], Fermat, em uma das cartas que escreveu para Mersenne, disse que achava que esses números eram todos primos.

> Estou quase persuadido de que todos os números da forma $2^{2^n} + 1$, são números primos... Não tenho uma demonstração exacta disto, mas excluí uma tão grande quantidade de divisores através de demonstrações infalíveis, e tenho umas tão grandes luzes que fundamentaram o meu pensamento,que teria dificuldade em me desdizer. [9]

Não sabemos ao certo se haveria algum motivo para que Fermat afirmasse com tamanha certeza. Talvez pelo fato que $F_0 = 3$, $F_1 = 5$, $F_2 = 17$, $F_3 = 257$ e $F_4 = 65537$ são todos números primos. Porém em 1732, Leonhard Euler, provou que $F_5 = 2^{2^5} + 1 = 4294967297 = 641 \times 6700417$ era um número composto, contrariando a afirmação de Fermat.

Os números de Fermat que são primos são conhecidos como os *Primos de Fermat*. Até hoje, não sabemos se existem outros primos de Fermat além dos cinco primeiros. Existe uma conjectura que os números primos de Fermat são em número finitos.

3.5.2 Números primos de Mersenne

Mersenne tinha interesse sobre divisibilidade, entre suas correspondências havia algumas com Fermat onde questionava sobre a possível fatoração de alguns números. Também, estava interessado em descobrir a existência, ou não, de um número perfeito de vinte ou vinte e um algarismos.

Um número natural n é dito *perfeito* se n é igual a soma de seus divisores positivos menores que n. Por exemplo, $6 = 1 + 2 + 3$ é perfeito. Em Os Elementos, Euclides não só define número perfeito, como também enuncia e demonstra um método para os calcular esses números. Para mais detalhes veja [4].

Os números de Mersenne são os números da forma $M_p = 2^p - 1$, com p sendo um número primo. Os números de Mersenne que são primos são denominados *Primos de Mersenne*. Temos os seguintes primos de Mersenne no intervalo $2 \leqslant p \leqslant 5000$: M_2, M_3, M_5, M_7, M_{13}, M_{19}, M_{31}, M_{61}, M_{89}, M_{107}, M_{127}, M_{521}, M_{607}, M_{1279}, M_{2203}, M_{2281}, M_{3217}, M_{4253} e M_{4423}.

Com a chegada da era informática, a busca de primos de Mersenne, e por consequência, de novos números perfeitos, tem sido efetuada com recurso a computadores. Em 1996 foi fundado o projeto GIMPS (Great Internet Mersenne Prime Search), que partilha a busca por milhões de computadores pessoais de todo o mundo. Deste modo, foram descobertos até hoje 49 primos de Mersenne, sendo o maior e mais recente encontrado em Janeiro de 2016 pelo professor Curtis Cooper da University of Central Missouri, o número é $M_{274207281} = 2^{274.207.281} - 1$. Ele possui 22.338.618 dígitos - quase cinco milhões de dígitos a mais que o antigo recordista de maior número primo conhecido (para mais detalhes veja [10]). Vale ressaltar que os maiores números primos encontrados nos últimos anos são os primos de Mersenne.

Figura 3.1: *Maior primo de Mersenne (folha.uol.com.br)*

3.5.3 Primos gêmeos

Os *números primos gêmeos* são dois números primos cuja diferença é igual a dois. Portanto, os seguintes pares de números primos: $(3, 5)$, $(5, 7)$, $(11, 13)$ são exemplos de primos gêmeos. Acredita-se que existem infinitos pares de primos gêmeos essa é uma famosa conjectura que está em aberto, poucos avanços foram dados em busca de sua solução e é um dos temas centrais da moderna teoria analítica dos números.

Conforme [13] são conhecidos pares de primos gêmeos bastante grandes, tais como $65516468355.2^{333333} \pm 1$, que têm 100355 dígitos cada.

3.6 Teste de primalidade

Os números primos são considerados muito importantes na área da teoria dos números em matemática, de tal forma que há um grande interesse em estudar sua teoria e suas propriedades. Principalmente aquelas que determinam se dado um qualquer, se ele é primo ou não.

Existem métodos, algoritmos, que determinam a primalidade do número. Tais algoritmos são considerados como Testes de Primalidade. Os testes de primalidade podem ser classificados como determinísticos ou probabilísticos.

Os testes de primalidade determinísticos determinam com certeza se um número inteiro é primo ou composto. Mas este teste só é prático para números inteiros pequenos ou inteiros que sejam divisíveis por um número primo pequeno.

Os testes de primalidade probabilísticos são testes que podem provar que um número é composto, porém, apenas indicam a probabilidade de que um número inteiro primo. O testes probabilísticos ainda são mais usados que os testes determinístico, pois são

mais rápidos e eficientes.

3.6.1 Crivo de Eratóstenes

O *Crivo de Eratóstenes* é um dos métodos determinísticos mais antigos. Com ele podemos determinar todos os números primos até um certo número inteiro específico, utilizando apenas uma tabela.

A palavra crivo significa *peneira*. Ou seja, o algoritmo vai peneirar ou números de uma determinada tabela de tal forma que separe os múltiplos dos números primos. Este processo será feito sucessivamente, deixando somente os que não são divisíveis por estes primos. Porém, esse algoritmo terá fim quando o último números a ser avaliado não exceder a raiz quadrada do número inteiro dado (conforme Lema 3.6.1), mas não é muito eficiente para ordens muito elevadas.

Lema 3.6.1 (Lema de Eratóstenes)**.** *Se um número natural $n > 1$ não é divisível por nenhum número primo p tal que $p^2 \leqslant n$, então ele é primo.*

Demonstração. Suponhamos, por absurdo, que n não seja divisível por nenhum número primo p tal que $p^2 \leqslant n$ e que n não seja primo. Seja q o menor número primo que divide n, então, $n = qn_1$, com $q \leqslant n_1$. Daí temos que $q^2 \leqslant qn_1 = n$. Logo, n é divisível por um número primo q tal que $q^2 \leqslant n$, o que seria um absurdo. □

Assim, para verificar se um dado número n é primo, basta verificar que n não é divisível por nenhum primo p que não supere $\sqrt{n}$.

Exemplo 3.6.2. *Por exemplo,vamos determinar todos números primos entre 1 e 100. Para começar o algoritmo, devemos elaborar uma tabela com todos os números naturais menores que 100. Em seguida, riscaremos todos os números compostos da tabela, obedecendo as seguintes instruções:*

1. *Primeiramente riscamos o número 1 que não é primo;*
2. *Risque todos os números divisíveis por 2, diferente de 2;*
3. *Em seguida, todos os múltiplos*[1] *de 3, exceto o 3;*
4. *O terceiro número não riscado que aparece é o 5, que é primo. Risque todos os múltiplos de 5, diferentes de 5;*

[1] Dizemos que c é múltiplo de a se $a|c$

5. *O próximo número não riscado que aparece é o 7, que é primo. Risque todos os seus múltiplos, exceto o 7.*

Observe que, de acordo com o Lema 3.6.1 precisamos repetir este procedimento apenas até o número 7, pois o próximo primo é 11, cujo quadrado é 121 e supera 100.

Figura 3.2: *Crivo de Eratóstenes (portaldoprofessor.mec.gov.br)*

Assim, os números primos menores que 100 são: 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89 e 97, conforme a figura 3.6.2.

3.6.2 Teste de primalidade de Fermat

O Pequeno Teorema de Fermat 3.3.3 dá a origem a um teste de primalidade, conhecido por Teste de Fermat. Ele é um teste de primalidade probabilístico.

Seja $a > 1$ com a pertencentes aos números inteiros positivos. Tomemos um $p > 1$ qualquer, também pertencente aos inteiros, e calculemos $a^{(p-1)} mod(p)$.

Caso o resultado encontrado não seja $1 \mod p$, então temos que p é um número composto.

Caso o resultado encontrado seja $1 \mod p$, então p pode ser um número primo. Neste caso ele recebe o nome de primo vovável na base a ou pseudoprimo na base a.

A existência de pseudoprimos, nos certifica de o teste de primalidade não é determinístico. Nota-se que podemos aumentar a eficácia do Teste de Fermat, fazendo os cálculos repetitivamente e mudanças de base.

Capítulo 4

Números primos e curiosidades

Neste capítulo abordaremos algumas curiosidades sobre os números primos. Para leitores mais interessados veja [19].

4.1 A música dos números primos

Por centenas de séculos matemáticos sabiam que os números primos formavam uma harmonia musical, mas percebiam apenas ruídos desorganizados. Esses números representavam notas aleatórias rabiscadas e desorganizadas, sem um determinado e compreensível tom.

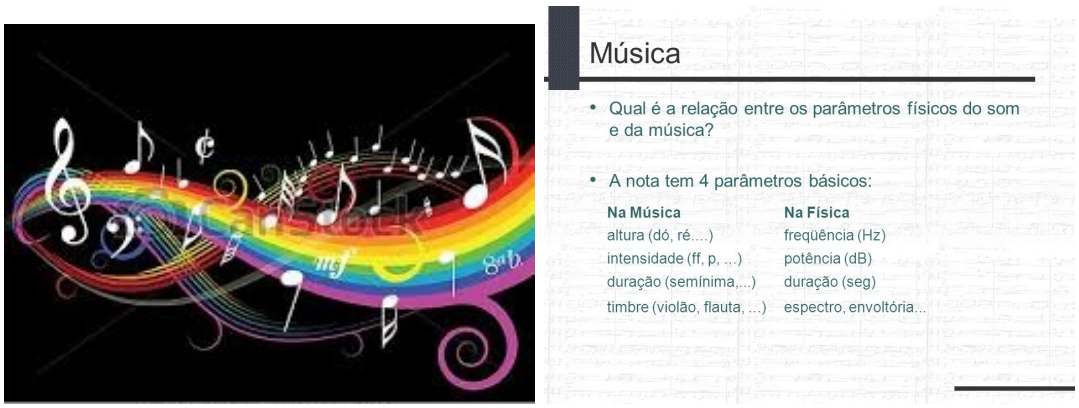

Figura 4.1: *Música, física e números primos (slideplayer.com.br)*

Pitágoras descobriu a harmonia musical escondida em uma sequência de frações. Mersenne e Euler desenvolveram a teoria matemática dos harmônicos. Mas nenhum

deles imaginava que existia uma relação entre a música e os números primos.

> O estudo da história da matemática deveria ser semelhante à análise musical de uma sinfonia. Temos diversos temas. Podemos observar o momento aproximado em que um tema surge pela primeira vez. Este, então, se mistura aos demais temas, e a arte do compositor está em lidar com todos eles simultaneamente. Às vezes, o violino toca um tema, a flauta outro, então se alternam, e a música prossegue. A história da matemática corre da mesma forma. [19]

Riemann, porém, descobriu uma nova forma de escutar esses tons misteriosos, utilizando as ondas senoides, criadas a partir dos zeros de sua *Função Zeta*[1], onde mostravam uma estrutura harmônica oculta.

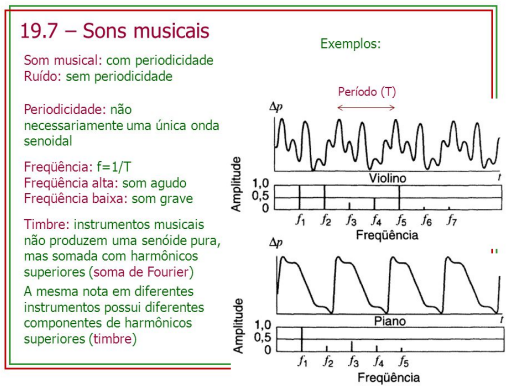

Figura 4.2: *Sons musicais (slideplayer.com.br)*

Segundo Riemann, as ondas simples juntas, podiam reproduzir as mais belas harmonias dos números primos. Ele entendeu que a natureza dos gráficos representavam os fenômenos físicos ou uma onda sonora. Ele sabia que o som podia ser representado por um gráfico no qual o eixo horizontal representa o tempo e o eixo vertical controla o volume e a altura do som a cada instante.

Começando com gráficos que representam o som mais simples, percebeu que a imagem da onda sonora resultante, se tratava de uma onda senoide. Expandindo através de combinações dessas ondas senoides, encontrou sons mais complicados.

Por exemplo, se um violino[2] tocar a mesma nota utilizando um diapasão[3] o som é

[1] não entraremos em detalhes sobre essa função, leitores interessados veja [22]

[2] instrumento musical de cordas friccionado

[3] instrumento metálico em forma de forquilha que serve para afinar instrumentos e vozes através da vibração de um som musical de determinada altura

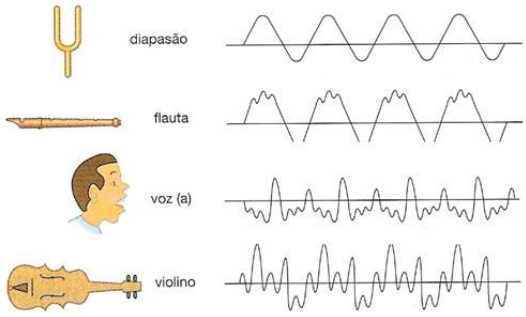

Figura 4.3: *ondas sonoras (ebah.com.br)*

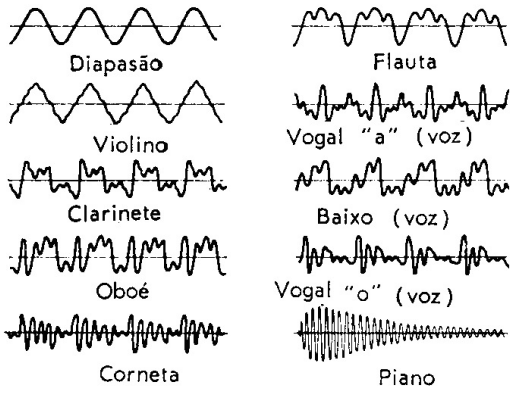

Figura 4.4: *Ondas (slideshare.net)*

muito diferente. Pois a corda do violino não vibra somente na frequência fundamental, determinada por seu comprimento.

Existem notas adicionais, os harmônicos, que correspondem a frações simples do comprimento da corda. Os gráficos de todas essas notas adicionais também são ondas senoides, porém de frequências mais elevadas.

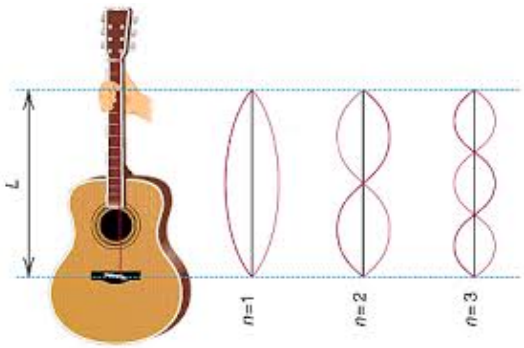

Figura 4.5: *Violino (musicaeadoracao.com.br)*

Agora imagine uma clarineta[4] e um piano. O gráfico da onda sonora criada pela clarineta se parece a uma função de onda quadrada, ao invés do gráfico espiculado do piano. Essa diferença ocorre porque a clarineta é aberta em uma das extremidades, enquanto a corda do piano é fixa nas duas pontas. Assim, os harmônicos produzidos pela clarineta são distintos dos do piano, portanto o gráfico que representa seu som é formado por ondas senoides que oscilam em frequências diferentes.

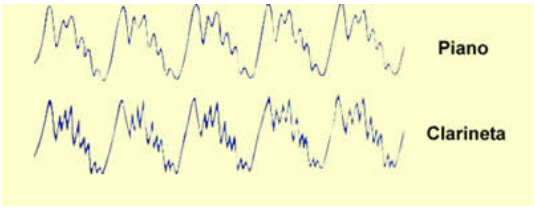

Figura 4.6: *Clarineta e piano (educacao.uol.com.br*

Esse princípio é utilizado na codificação do som em um CD, sendo que o CD instrui os alto falantes sobre o modo como devem vibrar para criar todas as ondas senoides que constituem o som da música. Essa combinação de ondas senoides nos transmite a sensação de uma orquestra ou uma banda tocando ao vivo.

> A hipótese de Riemann é a afirmação matemática de que é possível decompor os primos em música. Dizer que existe música nos primos é uma forma poética de descrever esse teorema matemático. Contudo, é uma música extremamente pós-moderna. [19]

Riemann demonstrou que uma escolha apropriada de ondas senoides, oscilando em diferentes frequências, poderia ser usada para criar uma grande gama de gráficos complicados. Ao somar as alturas das ondas senoides, reproduziu as formas desses gráficos, da mesma maneira que um CD combina os tons puros de diapasões para reproduzir sons musicais complexos. Assim, Riemann conseguiu explicar em seu artigo de dez páginas.

Ele reproduziu o gráfico escalonado que contava a quantidade de números primos exatamente da mesma forma, somando as alturas das funções de onda que derivou dos zeros da função zeta.

As ondas que Riemann criou a partir dos zeros da função, eram como os sons de diapasões, notas claras e simples, sem harmônicos. Quando tocadas simultaneamente,

[4]instrumento musical de sopro

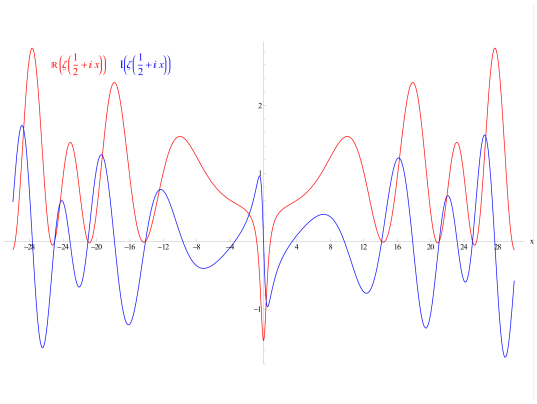

Figura 4.7: *Música e complexos (noosfera.com.br)*

essas ondas básicas reproduziam o som dos números primos. Esse som complexo é representado pelo gráfico escalonado.

Se as frequências das notas de Riemann estiverem em extensão contínua, os números primos formariam ruídos brancos. Mas, se as frequências forem notas isoladas, o som dos números primos se pareceria à música de uma orquestra.

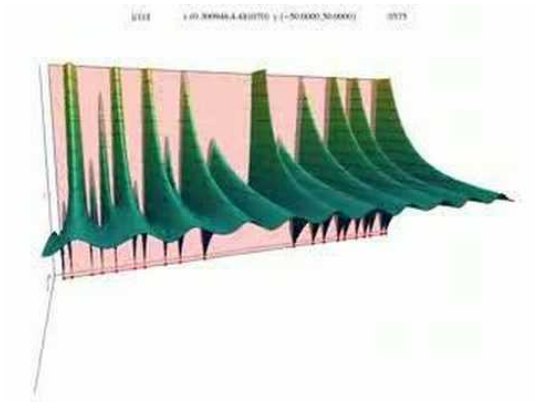

Figura 4.8: *Senoides (youtube.com)*

Dada a aleatoriedade dos primos, podemos esperar que a combinação das notas tocadas pelos zeros da função de Riemann não passasse de ruído branco. A coordenada vertical de cada zero determina a altura de sua nota. Se o som dos primos realmente fosse ruído branco, deveria haver uma concentração de zeros na função zeta.

Podemos então nos perguntar: Será que a natureza havia escondido nos números primos a música de uma orquestra matemática?

Em especial, temos o livro *A música e os números primos*, [19], que numa narrativa rica e abrangente conta a história de um dos maiores problemas da matemática: Seria possível haver harmonia entre os números primos semelhante a uma harmonia musical?

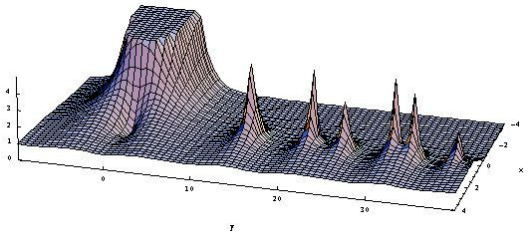

Figura 4.9: *Função zeta(mudancasabruptas.com.br)*

4.2 A criptografia e os números primos

Atualmente a criptografia é uma aplicação muito usada e importante para os números primos. Criptografia, em grego vem de *cryptos* que significa secreto ou oculto, é a ciência capaz de escrever mensagens ocultas ou codificadas. É o estudo das técnicas pelas quais a informação pode ser transformada da sua forma original para outra forma de linguagem, para que possa ser conhecida apenas por seu destinatário.

> A criptografia pode ser entendida como um conjunto de métodos e técnicas para cifrar ou codificar informações legíveis por meio de um algoritmo, convertendo um texto original em um texto ilegível, sendo possível mediante o processo inverso recuperar as informações originais. [14]

Uma aplicação muito importante na teoria dos números foi a codificação de mensagens enviadas por linhas telefônicas, principalmente no contexto bancário e comercial. Surgiram, então, os diversos métodos de criptografia e a teoria de criptografia moderna foi desenvolvida por volta dos anos 70 do século XX.

Figura 4.10: *Criptografia (estudopratico.com.br)*

O uso da criptografia tem aplicações variadas. Por exemplo, em assuntos ligados à guerra, com a finalidade de que o inimigo não descubra as estratégias do emissor da

mensagem. Em assuntos diplomáticos, com a finalidade de que facções rivais não estraguem os planos de acordos feitos. Até mesmo em assuntos amorosos, com finalidade de que segredos não sejam descobertos ou em uma simples troca de e-mails nos dias atuais.

A evolução e a popularização dos computadores, através da facilidade de conexão com as redes mundiais contribuíram imensamente com a criptografia.

Há dois tipos de criptografia: simétrica e assimétrica. Na criptografia simétrica todos os participantes compartilham um segredo. Esta não faz uso de números primos, geralmente utilizam a *Probabilidade Discreta*. Enquanto que, na criptografia assimétrica um dos participantes tem um segredo que o outro não possui. Esta sim faz uso extensivo de números primos, pois é baseada na teoria dos números.

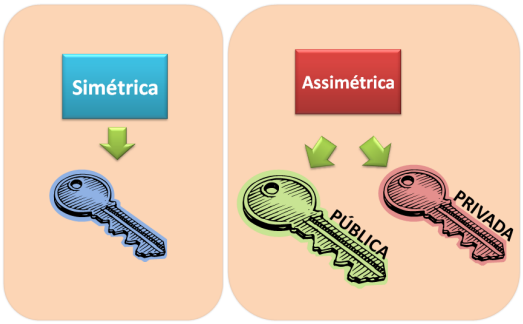

Figura 4.11: *Chave do segredo (pt.linkedin.com)*

Podemos até brincar imaginando que os números primos sabem guardar segredos, já que estão relacionados a processos de codificação na Internet.

4.3 Conjectura de Goldbach

Uma conjectura matemática é uma proposição que muitos matemáticos acham que deve ser verdadeira, mas ainda não conseguiram prová-la. Para que uma conjectura torne-se um teorema, é necessário que alguém determine uma prova, ou seja, uma função que assegure sua veracidade.

A conjectura de Goldbach diz que todo número par, maior que três é igual a soma de dois números primos. Porém para que a conjectura se torne um teorema, é necessário que qualquer um dos infinitos números pares seja escrito como uma soma de dois números primos.

Numa correspondência do matemático prussiano para o famoso matemático suíço Leonhard Euler (1707-1783), foi formulada a questão (1742): Todo número inteiro par maior que 2 pode ser representado como a soma de dois números primos. Hoje, mais de 250 anos depois, a Conjectura de Goldbach tornou-se um dos problemas mais intrigantes da Matemática. Mesmo já tendo sido testada, ninguém jamais conseguiu provar que a afirmação é válida para todos os números inteiros pares maiores que 2. [8]

Figura 4.12: *Carta de 7 de junho de 1742(pt.wikipedia.org)*

Encontramos uma outra conjectura relacionada com a de Goldbach, chamada de *Conjectura fraca de Goldbach*. No ano de 2015 a Conjectura fraca de Goldbach, foi demonstrada por um peruano, Harald Andrés Helfgott, que tem 35 anos e vive em Paris, onde trabalha para o Centro Nacional de Pesquisa Científica. A conjectura afirma:

Teorema 4.3.1. *Todo número ímpar $n > 5$ pode ser escrito como soma de três números primos.*

Em 2015, Helfgott tornou-se o primeiro latino-americano e também o cientista mais jovem a ganhar o Prêmio de Pesquisa Humboldt, concedido pela Fundação Alexander von Humboldt, da Alemanha. Ele recebeu 3,9 milhões de dólares por ter respondido uma pergunta que vinha desafiando matemáticos do mundo inteiro há quase trezentos anos... [8]

Considerações finais

A intenção deste trabalho foi de contribuir para uma abordagem mais ampla sobre o ensino dos números primos. A escolha do tema, se deve ao fato de que os números primos são muito importantes e, infelizmente, pouco explorados em sala de aula por professores e até mesmo em livros adotados. Limitam-se apenas em regras de divisibilidade, sem contextualizar com o cotidiano do aluno, como é cobrado através dos PCNs.

No decorrer do trabalho, escrevi sobre a história dos números primos, seus estudiosos, teoremas, teste de primalidades, aplicações e curiosidades. Mostrei que os números primos é um assunto de grande importância e aplicado ao nosso cotidiano. Com o intuito de contribuir com um material, de fácil entendimento, que proporcionasse um maior conhecimento aos assuntos relacionados a esses números, que estão presentes em diversas áreas da ciência.

Espero que este trabalho possa ajudar os leitores e em especial professores e alunos. Além disso, despertar o interesse para um estudo mais aprofundado sobre as curiosidades apresentadas.

Referências Bibliográficas

[1] Arbietro, A., *Aspectos Ergódicos da Teoria dos Números*, Editora IMPA, 2007.

[2] Artoni, G., *Monografia: História do último teorema de Fermat*, Unicamp, 2014.

[3] Changeux, J. P.; Connes, A., *Conversations on mind, Matter and Mathematics*, Princeton University Press December 7, 1998

[4] Costa, T. J. M. B. da, *Dissertação de Mestrado: Os números perfeitos e os primos de Mersenne*, Universidade de Lisboa, 2015.

[5] Eves, H., *Introdução à História da Matemática* Editora Unicamp, 1997 .

[6] Hefez, A., *Aritmética* , SBM Coleção PROFMAT, Volume único, 1ª edição, 2ª impressão, Rio de Janeiro, 2014.

[7] http://basenacionalcomum.mec.gov.br/images/BNCC_publicacao.pdf acesso em 27/09/2017

[8] http://www.dec.ufcg.edu.br/biografias/ChrstiaG.html acesso em 24/10/2017

[9] http://www.fermatsearch.org.br acesso em 24/10/2017

[10] https://olhardigital.com.br/noticia/projeto-descobre-maior-numero-primo-conhecido-ate-hoje/54532 acesso em 21/11/2017.

[11] http://portal.mec.gov.br/seb/arquivos/pdf/livro03.pdf acesso em 27/09/2017

[12] Lima, E. L., *Números e Funções Reais*, SBM, Coleção PROFMAT, Volume único, 1ª Edição, Rio de Janeiro, 2013.

[13] Moreira, C. G; Martínez, F. E. B. M. , *Primos gêmeos, primos de Sophie Germain e o Teorema de Brun*, Revista Universitária, nº 48/49 pg. 92-101.

[14] Moreno, E. D., *Criptografia em Software e Hardware* Editora Novatec.

[15] de Oliveira, C. N. C.; Fugita, F.; Fernandes, M. A. M. *Para viver juntos: matemática. Ensino Fundamental* Edições SM, São Paulo, 3ª edição, 2014.

[16] Alvaro-Prada,L. Ed. *Formação continuada de professores: alguns conceitos, interesses, necessidades e propostas* Rev. Diálogo Educ., Curitiba, v. 10, n. 30, pg. 367–387, 2010.

[17] Sacks, O., *O homem que confundiu sua mulher com um chapéu*, Editora companhia das letras,1997 1ª edição.

[18] Sagan, C., *Contato*, Editora Companhia de Bolso

[19] Sautoy, M. Du, *A música dos números primos* Editora Zahar, volume único, 1ª edição 2008.

[20] Silva, V. V. da, *Números, construção e propriedades*, Goiânia , Editora da UFG, 2003, Coleção Didática.

[21] Shokranian, S., *Uma Introdução à Teoria dos Números*, Editora Ciência Moderna.

[22] Voloch, J. F., *A distribuição dos números primos*, Revista Universitária, nº 06 pg. 71-82, 1987.

Anexo

Neste anexo apresentamos a abordagem feita sobre números primos no livro didático do ensino fundamental "Para viver juntos: Matemática." Nesse livro, veja [15], os autores apresentam curiosidades matemáticas acerca de temas relacionados ao conteúdo estudado pelo aluno, entre elas encontramos curiosidades sobre a importância da matemática na música e sobre criptografia. Além disso, anexamos a abordagem dos números primos. Para mais detalhes veja [15].

Número primo

Veja alguns números e seus divisores naturais.

Número	2	3	4	5	6	7	8	9	10	11	12	13
Divisores	1 e 2	1 e 3	1, 2 e 4	1 e 5	1, 2, 3 e 6	1 e 7	1, 2, 4 e 8	1, 3 e 9	1, 2, 5 e 10	1 e 11	1, 2, 3, 4, 6 e 12	1 e 13

Qualquer número natural não nulo é divisível por 1 e por ele mesmo. Além disso, observando a tabela percebe-se que os números 2, 3, 5, 7, 11 e 13 têm apenas dois divisores.

Definição

Número primo é todo número natural maior do que 1 que tem apenas dois divisores naturais diferentes: o número 1 e ele mesmo.

Assim, 2, 3, 5, 7, 11 e 13 são números primos.

Quando um número natural tem mais do que dois divisores, é denominado **número composto**.

Como saber se um número é primo

Para verificar se um número é primo, basta dividi-lo pelos números primos menores do que ele até obter resto 0 – nesse caso o dividendo não é um número primo – ou um quociente menor do que ou igual ao divisor e resto diferente de zero – nesse caso o dividendo é um número primo. Veja como exemplo o número 149.

$$\begin{array}{r|l} 149 & 2 \\ 09 & 74 \\ 1 & \end{array} \qquad \begin{array}{r|l} 149 & 3 \\ 29 & 49 \\ 2 & \end{array} \qquad \begin{array}{r|l} 149 & 5 \\ 49 & 29 \\ 4 & \end{array}$$

$$\begin{array}{r|l} 149 & 7 \\ 09 & 21 \\ 2 & \end{array} \qquad \begin{array}{r|l} 149 & 11 \\ 39 & 13 \\ 6 & \end{array} \qquad \begin{array}{r|l} 149 & 13 \\ 19 & 11 \\ 6 & \end{array}$$

Em 3 minutos

Usando os critérios de divisibilidade, responda: é preciso calcular as divisões 149 por 2, 149 por 3 e 149 por 5 para saber se elas são exatas?

A divisão foi efetuada até o número 13, porque todas as divisões anteriores não foram exatas e em 149 : 13 o quociente 11 é menor do que 13 e o resto é diferente de zero. Logo, o número 149 é primo.

ATIVIDADES

■ **69.** Verifique quais dos números a seguir são primos. Justifique.

a) 47
b) 79
c) 91
d) 101
e) 122
f) 169

■ **70.** Há vários pares de números primos que diferem em apenas duas unidades. Por exemplo: 3 e 5; 5 e 7. Pares assim são denominados primos gêmeos. Escreva outros dois pares de números primos gêmeos.

■ **71.** Siga os passos a seguir.

I. Faça um quadro com os números naturais de 2 até 100, incluindo esses números.
II. Risque os números maiores do que 2 que sejam divisíveis por ele.
III. Risque os números maiores do que 3, 5 e 7 que sejam divisíveis por um deles.

Em seguida, identifique todos os números primos menores do que 100.

Pesquise quantos algarismos o maior número primo conhecido tem.

Boxe – Em 3 minutos

Não. Pelos critérios de divisibilidade:

- o último algarismo de 149 é 9, um número ímpar, portanto não é divisível por 2;
- a soma dos algarismos 1, 4 e 9 é igual a 14, portanto 149 não é divisível por 3;
- o número 149 não termina em 0 ou 5, portanto não é divisível por 5.

69. a) 47 : 2 = 23 e resto 1
47 : 3 = 15 e resto 2
47 : 5 = 9 e resto 2
47 : 7 = 6 e resto 5
Como nenhuma dessas divisões é exata e o quociente 6 é menor do que o divisor 7, 47 é primo.

b) 79 : 2 = 39 e resto 1
79 : 3 = 26 e resto 1
79 : 5 = 15 e resto 4
79 : 7 = 11 e resto 2
79 : 11 = 7 e resto 2
Como nenhuma das divisões é exata e o quociente 7 é menor do que o divisor 11, 79 é primo.

c) 91 : 2 = 45 e resto 1
91 : 3 = 30 e resto 1
91 : 5 = 18 e resto 1
91 : 7 = 13 e resto 0
Como a última divisão acima é exata, 91 não é primo.

d) 101 : 2 = 50 e resto 1
101 : 3 = 33 e resto 2
101 : 5 = 20 e resto 1
101 : 7 = 14 e resto 3
101 : 11 = 9 e resto 2
Como nenhuma das divisões é exata e $9 < 11$, 101 é primo.

e) 122 : 2 = 61 e resto 0
Como a divisão acima é exata, 122 não é primo.

f) 169 : 2 = 84 e resto 1
169 : 3 = 56 e resto 1
169 : 5 = 33 e resto 4
169 : 7 = 24 e resto 1
169 : 11 = 15 e resto 4
169 : 13 = 13 e resto 0
Como a divisão acima é exata, 169 não é primo.

Fatoração

Todos os números naturais, exceto o número 1, podem ser escritos como o produto de dois ou mais números naturais distintos. Veja, como exemplo, as decomposições do número 12.

$12 = 1 \cdot 12$ $\quad 12 = 2 \cdot 6$ $\quad 12 = 3 \cdot 4$ $\quad 12 = 2 \cdot 2 \cdot 3$

Observe que uma dessas decomposições tem apenas fatores primos, $12 = 2 \cdot 2 \cdot 3$. Por isso, ela é denominada **decomposição em fatores primos**.

Todo número natural composto pode ser decomposto em fatores primos. Essa decomposição é única e existem dois modos de efetuá-la: por decomposições sucessivas e pelo dispositivo prático.

1º modo: decomposições sucessivas

Fazemos decomposições sucessivas até obter apenas números primos. Veja um exemplo.

$60 = 6 \cdot 10$ ou $60 = 4 \cdot 15$

$60 = 2 \cdot 3 \cdot 2 \cdot 5$ $\qquad 60 = 2 \cdot 2 \cdot 3 \cdot 5$

Logo: $60 = 2^2 \cdot 3 \cdot 5$

2º modo: usando o dispositivo prático

I Começamos a dividir o número 60 pelo menor número primo divisor de 60, nesse caso o 2. Escrevemos o quociente 30 da divisão abaixo do número 60.

60	2	← divisor primo
30		

quociente →

II Dividimos o número 30 pelo menor número primo divisor de 30, que também é 2. Escrevemos o quociente 15 da divisão abaixo do número 30.

60	2
30	2 ← divisor primo
15	

quociente →

III Dividimos o número 15 pelo menor número primo divisor de 15, que é o número 3. Escrevemos o quociente 5 da divisão abaixo do número 15.

60	2
30	2
15	3 ← divisor primo
5	

quociente →

IV Por fim, dividimos 5 por 5, pois 5 é um número primo. Escrevemos o quociente 1 da divisão abaixo do número 5.

60	2
30	2
15	3 } fatores primos de 60
5	5
1	

$60 = 2^2 \cdot 3 \cdot 5$

Assim como no 1º modo, concluímos que $60 = 2^2 \cdot 3 \cdot 5$.

Em 3 minutos

Por que não decompomos em fatores primos os números primos?

Orientações didáticas

Fatoração

Escreva no quadro "fatoração" e pergunte aos alunos o que essa palavra lembra. Estimule-os a perceber que lembra "fator", uma nomenclatura que eles já conhecem, do estudo dos termos de uma multiplicação.

Com isso, os alunos podem perceber que o conteúdo visto em outros momentos é retomado e utilizado em novos conteúdos.

Continuação das respostas da página 130

70. Respostas possíveis: 11 e 13, 17 e 19.

71.

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~~

Boxe – Em 3 minutos

Porque não existem dois números primos distintos que multiplicados resultem em um número natural primo. Por exemplo, o número primo 13 só pode ser decomposto em $1 \cdot 1^3$, e 1 não é número primo; assim, não é possível decompor 13 em fatores primos.