Universidade Estadual de Maringá
Centro de Ciências Exatas
Departamento de Matemática
Mestrado Profissional em Matemática - Profmat

Roberto Luiz Spenthof

Primos: da aleatoriedade ao padrão

Maringá-Pr
2013

ROBERTO LUIZ SPENTHOF

PRIMOS: DA ALEATORIEDADE AO PADRÃO

Dissertação apresentada ao Curso de Mestrado Profissional em Matemática da Universidade Estadual de Maringá, como requisito parcial para obtenção do Grau de Mestre. Área de Concentração: Matemática.

Orientador: Prof. Dr. JOSINEY ALVES DE SOUZA

Maringá-Pr

2013

Dados Internacionais de Catalogação-na-Publicação (CIP)
Ficha catalográfica elaborada por Jeanine da Silva Barros CRB-9/1362

S729p Spenthof, Roberto Luiz
Primos: da aleatoriedade ao padrão / Roberto Luiz Spenthof.— Maringá, PR: UEM, 2013.
40 f.

Orientador: Prof. Dr. Josiney Alves de Souza
Dissertação (Mestrado) – Universidade Estadual de Maringá.
Programa de Pós-Graduação *Stricto Sensu* – Mestrado Profissional em Matemática em Rede Nacional, área de concentração: Matemática.
Bibliografia.

1. Números primos – Histórico - Teorias. 2. Matemática. I. Souza, Josiney Alves de. II. Universidade Estadual de Maringá. III. Título.

CDD 21.ed. 510.7

ROBERTO LUIZ SPENTHOF

PRIMOS: DA ALEATORIEDADE AO PADRÃO

Trabalho de Conclusão de Curso, apresentada ao Programa de Mestrado Profissional em Matemática em Rede Nacional do Departamento de Matemática, Centro de Ciências Exatas da Universidade Estadual de Maringá, como parte dos requisitos necessários para a obtenção do título de Mestre em Matemática tendo a Comissão Julgadora composta pelos membros:

COMISSÃO JULGADORA:

Josiney Alves de Souza

Prof. Dr. Josiney Alves de Souza
DMA/Universidade Estadual de Maringá (Presidente)

Jair da Silva

Prof. Dr. Jair da Silva
Universidade Federal do Mato Grosso do Sul – Campo Grande - MS

Wesley Vagner Inês Shirabayashi

Prof. Dr. Wesley Vagner Inês Shirabayashi
DMA/Universidade Estadual de Maringá

Aprovada em: 12 de março de 2013.
Local de defesa: Auditório do DMA, Bloco F67, campus da Universidade Estadual de Maringá.

Dedico este trabalho a professora de matemática Daniele, minha esposa, pela paciência e apoio durante todos os momentos em que a dedicação ao mestrado impossibilitou que estivéssemos juntos. Sei que estava sempre comigo nos cerca de 40.000 Km desta caminhada.

Agradecimentos

Agradeço a minha esposa Daniele e a meu filho Davi, pelo amor, carinho, paciência e por todo o apoio que me deram nestes últimos dois anos. A minha filha Helena, nascida há poucos dias, me dando uma motivação a mais.

Agradeço aos meus colegas de curso, especialmente o Amarildo, a Cleonice, a Priscila e o Ronaldo. Nossa amizade permitiu que as dificuldades fossem superadas com mais tranquilidade e aproveitamento.

Agradeço, por fim, aos meus professores, por cada explicação, conselho, incentivo e cobrança. Em especial, ao Prof. Josiney, meu orientador, pela aceitação do convite, pela disponibilidade, e pelas valorosas contribuições que possibilitaram a produção deste trabalho.

Lista de Figuras

Lista de Tabelas

Sumário

Resumo

Na busca por disseminar o assunto entre estudantes de matemática, neste trabalho, apresenta-se o histórico do estudo dos números primos. Demonstra-se os resultados fundamentais, como a infinitude e o Teorema Fundamental da Aritmética. Apresenta-se e compara-se as estimativas de Gauss, Legendre e Riemann para a função $\pi(x)$ chamada de *função de contagem dos números primos*. Parte-se da aparente aleatoriedade e segue-se os passos desses matemáticos até a obtenção do padrão que rege a sequência dos números primos. Conclui-se com uma exposição sucinta da Hipótese de Riemann, a contribuição de Euler, e discute-se sobre as consequências de uma possível demonstração para a matemática e para a segurança da internet.

Palavras-chave: números primos, contagem, estimativa, conjetura.

Abstract

Attempting to spread the subject among mathematics students, in this work, the history of the study of prime numbers is presented. Fundamental results, such as infinity and the Fundamental Theorem of Arithmetic are demonstrated. The estimates of Gauss, Legendre and Riemann for the function $\pi(x)$ called the *counting function of primes* are presented and compared. It starts with the apparent randomness and follows the steps of these mathematicians to obtain the pattern that governs the sequence of the prime numbers. It is concluded with a brief statement of the Riemann's Hypothesis, the contribution of Euler, and a discussion about the consequences of a possible demonstration for mathematics and for internet security.

Key-words: prime numbers, counting, estimate, conjecture.

Introdução

- *Um conjunto de números com um nome diferente.*

Essa é a noção de números primos com que muitos de nossos estudantes, egressos do Ensino Médio, ou, o que é pior, de cursos de graduação na área de Ciências Exatas, mantém. Não se pode, contudo, culpá-los. Quantos de nós, estudantes de matemática, quando ainda na educação básica, podem afirmar que tiveram acesso menos superficial ao assunto do que simplesmente uma definição (quase sempre incompleta) e alguns algoritmos (sem nenhuma fundamentação teórica)? Quantos pelo menos "ouviram falar" que os primos são a estrutura de um dos ramos mais férteis da matemática? Quantos sabiam da existência de alguma aplicação prática da teoria desenvolvida, como por exemplo, na segurança do contemporâneo comércio eletrônico? O fato é que esse assunto não recebe a devida importância nos programas curriculares. Tentaremos, então, diminuir essas carências nas linhas a seguir. Exemplos de atividades que podem ser aplicadas no ensino básico estão apresentadas no Apêndice deste trabalho.

Definição 1. *Um número inteiro n ($n > 1$) possuindo somente dois divisores positivos, a saber,* 1 *e n, é chamado* primo. *Se $n > 1$ não é primo, dizemos que n é* composto.

A primeira vista, esta definição não parece indicar a grandiosidade das consequências, resultados e problemas, alguns ainda não resolvidos, que advém do seu estudo mais aprofundado. O fato é que a Teoria dos Números, campo da matemática que abrange, entre outros, o estudo dos números primos, mantém-se sempre entre as mais fascinantes, durante toda a história. Grandes matemáticos como Euclides de Alexandria (360 a.C - 295 a.C.), Pierre de Fermat (1601 - 1665), Leonhard Euler (1707 - 1783), Carl Friedrich Gauss (1777 - 1855) e Georg Friedrich Bernhard Riemann (1826 - 1866), entre outros, ocuparam-se com pesquisas envolvendo os números primos. Seus trabalhos acabaram por estruturar esse ramo da matemática e por influenciar várias outras áreas, sendo respon-

sáveis pela ocupação de muitos pesquisadores desde então.

Os gregos foram os primeiros a perceber que os números primos eram os "átomos", os blocos básicos, com os quais se poderia construir todos os números naturais, exceto o 1, pela multiplicação. Eram, assim, de certo modo, "indivisíveis". Os pitagóricos, em sua veneração pelos números, também já os conheciam.

Contudo, foi somente nos Livros VII, VIII e IX, da obra *Os Elementos* de Euclides, dedicados a teoria dos números, que os primos se revelaram formalmente. Conforme consta em ([2], p. 79):

> "O Livro IX, o último dos três sobre teoria dos números, contém vários teoremas interessantes. Desses, o mais célebre é a Proposição 20: 'Números primos são mais do que qualquer quantidade fixada de números primos.' Isto é, Euclides dá aqui a prova elementar bem conhecida do fato de que há infinitos números primos. A prova é indireta, pois mostra-se que a hipótese de haver somente um número finito de primos leva a uma contradição".

Tal demonstração está apresentada, em detalhes, no próximo capítulo.

Eratóstenes de Alexandria, no século III a.C., foi o primeiro a criar uma tabela de números primos. Seu método, conhecido como *crivo de Eratóstenes*, poderia encontrar todos os números primos até um certo número N estipulado. Após escrever todos os números de 2 até N, ele riscava todos os múltiplos de 2, exceto o próprio 2. O próximo número não riscado da sequência é 3 que é primo. Em seguida, riscava todos os múltiplos de 3, exceto o próprio 3. Assim, o próximo número não riscado da sequência é o 5, que é primo. Continuando assim, até o final da sua lista finita de números, somente os números primos não estariam riscados. De fato, os números não riscados só podem ser primos, pois se não fossem, então seriam múltiplos de algum número menor, e portanto, teriam sido riscados, o que é uma contradição.

Durante a Idade Média, o desenvolvimento da teoria dos números primos ficou estagnada, assim como praticamente todas as outras áreas do conhecimento. Somente no século XVII, após estudar a *Arithmetica* de Diofanto (escrita provavelmente no século III

d.C), Pierre de Fermat ressuscitou a questão, e é considerado o fundador da moderna teoria dos números. Fermat não era matemático profissional. Mesmo assim, encontrava tempo para se dedicar a matemática. Algumas de suas conjeturas posteriormente provaram-se falsas, como a de que seria primo todo número da forma $F_n = 2^{2^n} + 1$, os quais ficaram conhecidos como *números de Fermat*, que ele fez baseado na observação de que $F_0 = 3$, $F_1 = 5$, $F_2 = 17$, $F_3 = 257$ e $F_4 = 65.537$ são primos. Segundo ([7], p. 98), "Em 1732, Leonhard Euler mostrou que $F_5 = 2^{2^5} + 1 = 4.294.967.297 = 641 \cdot 6.700.417$, portanto, composto, desmentindo assim a afirmação de Fermat". Outra conjetura, hoje conhecida como *Pequeno Teorema de Fermat*, revelou-se verdadeira e diz que se p é primo, e a e p são *primos entre si* (dizemos que dois números a e p são *primos entre si* quando seu único divisor comum é o 1), então $a^{p-1} - 1$ é divisível por p. Utilizando esse teorema, podemos concluir, por exemplo, que $2^{100} - 1$ é divisível por 101, sem termos que calcular o valor desse número astronomicamente grande.

Euler, desta vez, demonstrou sua veracidade, e percebeu, inclusive, que este teorema na verdade é um corolário de um teorema mais geral, que diz que se a e m são números naturais maiores do que 1, primos entre si, então $a^{\varphi(m)} - 1$ é divisível por m (onde φ é a *função fi de Euler*, e $\varphi(m)$ corresponde à quantidade de números naturais entre 0 e $m - 1$ que são primos com m). Uma prova detalhada de tal teorema pode ser encontrada em ([7], p. 132).

Euler, como bem se sabe, foi extremamente ativo na sua produção científica. Durante sua vida publicou mais de 500 artigos em quase todas as áreas da matemática. Entre suas contribuições, que depois tiveram consequências na história dos números primos, está o estudo da função ζ, conhecida como *função zeta de Euler*.

Contudo, até então ninguém havia conseguido ver um padrão na distribuição dos números primos. Essa distribuição, aparentemente aleatória, ensejou a questão de saber se era possível prever a localização precisa do próximo número primo. Foi Gauss quem deu o primeiro e decisivo passo nesse sentido, aos quinze anos de idade. A tabela de números primos contida na contracapa de seu livro de logaritmos parece ter sido a responsável por esse passo. Conforme consta em ([5], p. 56):

> "O grande avanço de Gauss foi fazer uma pergunta diferente. Em vez de tentar prever a localização precisa do próximo primo, ele buscou ao menos descobrir quantos primos haveria entre os primeiros 100 números, os primeiros 1.000 e assim por diante. Se tomássemos o número N, haveria alguma maneira de estimar quantos primos encontraríamos entre os números 1 e N?"

Ao se perguntar quantos primos existiam entre 1 e N, isto é, qual é o valor da função $\pi(n)$ para $n = N$, Gauss percebeu que parecia existir uma relação entre esse valor e os logaritmos. Assim, parecia haver uma conexão entre a função logarítmica e a distribuição dos números primos, que o levou, por fim, até a descoberta da "integral logarítmica".

Gauss, de fato, foi um dos grandes propulsores da Teoria dos Números. Em 1798, aos 21 anos, produziu uma das obras-primas da matemática, o livro *Disquisitiones Arithmeticae*, publicado em 1801, onde, entre outras novidades, introduziu o conceito de congruência, que consiste em uma aritmética com os restos da divisão euclidiana por um número fixado, e que acabou por ter sua utilidade prática descoberta somente após cerca de 200 anos.

Analisando os estudos de Gauss, e estudando a função *zeta* de Euler, estendendo-a para números complexos, Riemann se deparou com algo que parecia acabar com a impossibilidade de prever a localização exata dos números primos. Ele visualizou uma relação entre os zeros "não-triviais" da função *zeta* e a localização dos números primos. Tal relação teve como consequência uma conjetura, até hoje não provada, conhecida como a *Hipótese de Riemann*. "Riemann havia finalmente descoberto o padrão misterioso que os matemáticos haviam almejado ao olharem para os primos ao longo dos séculos" ([5], p. 110). Se sua conjetura estivesse correta, a estimativa de Gauss sobre a distribuição dos números primos seria cada vez mais precisa à medida que se avançasse na contagem.

Capítulo 1

Alguns resultados envolvendo números primos

Euclides foi o primeiro a demonstrar que os números primos são infinitos. Sua demonstração é considerada, por muitos, a mais elegante da matemática.

Teorema 1.1 (Infinitude dos Números Primos)**.** *Existem infinitos números primos.*

Demonstração (Euclides). Suponhamos que exista somente um número finito r de números primos, a saber p_1, p_2, ..., p_r. Consideremos agora o número $N = p_1 \cdot p_2 \cdots p_r + 1$. Se N for primo, então temos uma contradição, já que supomos existir somente r números primos e N evidentemente não é um deles. Se N não for primo, então existe um número primo p que divide N. Mas esse número primo p não pode ser nenhum dos números p_i $(i = 1, \ldots, r)$, pois se fosse, dividiria o produto $p_1 \cdot p_2 \cdots p_r$, e portanto dividiria o número 1, o que é um absurdo. Em ambos os casos, conclui-se a existência de mais números primos do que a quantidade suposta inicialmente. Logo, a suposição de que existe um número finito de números primos é falsa. □

Uma outra demonstração bem conhecida desse teorema se encontra numa carta de Christian Goldbach (1690 - 1764) a Euler. Ela se baseia na busca de uma sequência infinita $a_1 < a_2 < a_3 < \ldots$ de números naturais, dois a dois primos entre si. Assim, dois termos quaisquer dessa sequência não possuem fatores primos em comum. Se tal sequência pode ser construída, então existem infinitos números primos, já que cada elemento da sequência deve trazer pelo menos um fator primo diferente daqueles que compõem os

números anteriores. Uma sequência assim poderia ser, por exemplo, 3, 7, 10, 11,...

Já era conhecido na época que, apesar de os *números de Fermat* $F_n = 2^{2^n}+1$ (para $n \geq 0$) não serem todos primos, como seu criador havia suposto, eles eram todos, dois a dois, primos entre si. Verifiquemos inicialmente dois lemas necessários à demonstração de Goldbach.

Lema 1.2. *Se F_m é o* m-ésimo *($m \geq 1$) número de Fermat, então $F_m - 2 = F_0 F_1 \dots F_{m-1}$.*

Demonstração. Vemos que:

$$F_m - 2 = F_0 F_1 \dots F_{m-1} \iff 2^{2^m} - 1 = (2^{2^0}+1)(2^{2^1}+1)\dots(2^{2^{m-1}}+1)$$

Demonstremos, por indução sobre $m \in \mathbb{N}$, a validade da proposição:

$$P(m) : 2^{2^m} - 1 = (2^{2^0}+1)(2^{2^1}+1)\dots(2^{2^{m-1}}+1)$$

i) Para $m = 1$, temos que $2^{2^1} - 1 = 2^{2^0} + 1$.

ii) Supondo $P(m)$ válida para algum $m > 1$, e multiplicando ambos os membros por $2^{2^m}+1$, temos:

$$(2^{2^0}+1)(2^{2^1}+1)\dots(2^{2^{m-1}}+1)(2^{2^m}+1) = (2^{2^m}-1)(2^{2^m}+1) = 2^{2^{m+1}} - 1$$

e assim $P(m+1)$ é válida. Logo $P(m)$ é válida para todo $m \in \mathbb{N}$. □

Lema 1.3. *Os números de Fermat $F_n = 2^{2^n}+1$ (para $n \geq 0$) são, dois a dois, primos entre si.*

Demonstração. Vimos pelo lema anterior que $F_m - 2 = F_0 F_1 \dots F_{m-1}$. Assim, se $n < m$, F_n divide $F_m - 2$. Se existisse um número primo p que dividisse simultaneamente F_n e F_m, então p dividiria $F_m - 2$ e portanto dividiria 2, logo $p = 2$, o que é impossível, já que todos os números de Fermat são ímpares. □

Agora já podemos apresentar a demonstração contida na carta de Goldbach:

Demonstração (Goldbach) do Teorema 1.1. É possível construir a seguinte sequência infinita: F_0, F_1, F_2, ..., onde todos os termos são, dois a dois, primos entre si. Então os números primos são infinitos.

□

Outro importante resultado envolvendo os primos, já conhecido desde o tempo de Euclides, apesar de não constar explicitamente em *Os Elementos*, é o de que os números primos são os blocos de construção dos números naturais, isto é, somente usando números primos como "tijolos" e a operação de multiplicação como a "massa" que os une, podemos construir todos os números naturais, exceto a unidade. De fato, esse resultado é tão importante, que recebeu o nome de *Teorema Fundamental da Aritmética*.

Teorema 1.4 (Fundamental da Aritmética)**.** *Todo número natural maior do que* 1 *ou é primo ou se escreve de modo único (exceto pela ordem dos fatores) como um produto de números primos.*

Demonstração. Inicialmente, definamos que, dados dois números naturais a e b, com $a \neq 0$, diremos que a *divide* b, escrevendo $a \mid b$, quando existir $c \in \mathbb{N}$ tal que $b = a \cdot c$. Neste caso dizemos que a é um *divisor* ou um *fator* de b e que b é um *múltiplo* de a.

O teorema afirma que a decomposição de um número natural $n > 1$ em fatores primos existe, e é única (exceto pela ordem). Temos que provar, portanto, a existência e a unicidade desta decomposição.

Existência: se n for primo, ele é sua própria decomposição, a qual, portanto, existe. Suponhamos n composto. Tomemos $p_1 > 1$ o menor dos divisores naturais de n. Temos que p_1 é primo, pois caso contrário, existiria p natural ($1 < p < p_1$), com $p \mid p_1$ e portanto $p \mid n$, contradizendo a escolha de p_1. Assim podemos escrever $n = p_1 n_1$.

Se n_1 for primo, novamente a prova está completa. Se n_1 é composto, tomemos p_2 como o menor fator de n_1. Pelo mesmo argumento, temos que p_2 é primo e portanto $n = p_1 p_2 n_2$.

Se repetirmos esse procedimento obteremos uma sequência decrescente de números naturais $n_1, n_2, \ldots, n_r$, todos maiores do que 1. Pelo *Princípio da Boa Ordem* (ver [7], p. 20), este processo não pode continuar indefinidamente. Nesse momento teremos uma sequência $p_1, p_2, \ldots, p_k$ de números primos não necessariamente distintos. Logo n terá a

forma:

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$$

que é a decomposição de n em fatores primos.

Unicidade: a unicidade é mostrada usando indução sobre n. Para $n = 2$, a afirmação é verdadeira trivialmente. Assumimos que ela se verifica para todos os naturais maiores do que 1 e menores do que n. Vamos provar que ela também é válida para n.

Se n é primo, não há nada a provar. Suponhamos n composto e que n possua duas decomposições, ou seja,

$$n = p_1 p_2 \cdots p_s = q_1 q_2 \cdots q_r$$

onde os p_i $(i = 1, \ldots, s)$ e os q_j $(j = 1, \ldots, r)$ são números primos. Temos que provar que $s = r$ e que cada p_i é igual a algum q_j. Podemos escrever

$$p_2 \cdots p_s = \frac{q_1 q_2 \cdots q_r}{p_1}$$

e como o primeiro membro é um número natural, então $p_1 \mid q_1 q_2 \cdots q_r$, o que implica que p_1 divide algum dos fatores q_j (que são todos primos). Sem perda de generalidade, podemos supor que $p_1 \mid q_1$. Como ambos são primos, isto implica que $p_1 = q_1$. Logo:

$$1 < p_2 \cdots p_s = q_2 \cdots q_r < n$$

e aqui a hipótese de indução nos diz que as duas decomposições são idênticas, isto é, $s = r$ e, exceto pela ordem, as decomposições $p_1 p_2 \cdots p_s$ e $q_1 q_2 \cdots q_r$ são iguais. □

Iremos discutir com mais profundidade a distribuição dos números primos no capítulo seguinte. Contudo, olhando para a lista dos primeiros números primos, 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97, ... e em seguida para a sequência formada pelo comprimento da cadeia de números compostos contida entre dois números primos consecutivos, 0, 1, 1, 3, 1, 3, 1, 3, 5, 1, 5, 3, 1, 3, 5, 5, 1, 5, 3, 1, 5, 3, 5, 7, ... percebemos que, em média, essas cadeias de números compostos vão ficando cada vez mais longas. Na verdade, essas cadeias de números compostos podem se tornar tão grandes quanto se queira. Em outras palavras, existem "saltos" arbitrariamente grandes na sequência de números primos. Podemos enunciar este resultado como

um teorema.

Teorema 1.5. *Para qualquer natural k existe uma cadeia de k números consecutivos todos compostos.*

Demonstração. Como $(k+1)!$ é divisível por todos os k números entre 2 e $k+1$, então a cadeia

$$(k+1)!+2, (k+1)!+3, \ldots, (k+1)!+k, (k+1)!+(k+1)$$

é constituída por k números consecutivos, e nenhum deles é primo, já que admitem como fatores próprios 2, 3, 4, ..., $k+1$, respectivamente. □

Analisando ainda a sequência formada pelos comprimentos das cadeias de números compostos contidos entre dois primos consecutivos, vemos que o número 1 aparece diversas vezes. Ele identifica os pares de números chamados de *primos gêmeos*, que são primos separados por um único número natural. Assim, são exemplos de primos gêmeos os pares 3 e 5, 5 e 7, 11 e 13, 71 e 73, etc. Em ([8], p. 280), consta que também são primos gêmeos os números $65516468355 \cdot 2^{333333} \pm 1$, que têm 100.355 dígitos cada. Conjetura-se que existam infinitos pares de primos gêmeos, e este ainda é um dos problemas em aberto na teoria dos números. O leitor interessado em se aprofundar no assunto pode consultar [8], e [11].

Apesar de existirem saltos arbitrariamente grandes na sequência de números primos, como mostramos, na verdade os números primos não estão tão "espalhados" assim. *O Postulado de Bertrand*, demonstrado pelo russo Pafnuti Tchebychev (1821-1894), afirma que, se n é um número inteiro positivo, então sempre existe um primo p tal que $n \leq p \leq 2n$. Isto quer dizer que, independentemente do ponto onde estejamos na sequência dos números naturais, nunca precisaremos andar mais do que já andamos para encontrar o próximo número primo. A demonstração do Postulado de Bertrand, além de longa, foge do escopo deste trabalho, mas pode ser encontrada completa no apêndice C de [12].

Uma outra conjetura famosa, que também estava contida numa carta de 1742 de Goldbach a Euler, ficou conhecida como *Conjetura de Goldbach*. Ela afirma que todo inteiro par, exceto o 2, pode ser escrito como soma de dois primos. Por exemplo, $4 = 2+2$,

$6 = 3 + 3$, $8 = 5 + 3$, ..., $20 = 17 + 3$, ..., $48 = 29 + 19$, ..., $60 = 53 + 7$, ..., $100 = 97 + 3$ e assim por diante. Segundo [6], a Conjetura de Goldbach já foi verificada para os números até 100 milhões, mas a mesma continua sem demonstração.

Existem vários outros problemas menos conhecidos, todos ainda não respondidos, como por exemplo: existem infinitos primos da forma $n^2 + 1$? Sempre existe um número primo entre n^2 e $(n+1)^2$? Existem infinitos primos de Fermat (da forma $2^{2^n} + 1$)? Como se vê, a teoria em torno dos números primos oferece uma vasta gama de opções de pesquisa.

Capítulo 2

Sobre a distribuição dos números primos

Durante gerações muitos matemáticos estiveram obcecados por prever a localização exata do próximo primo, e, entre eles, Gauss. Mas ao invés de tentar descobrir números primos, Gauss se perguntou quantos primos existiriam entre 1 e um número N qualquer. Percebeu então que parecia haver uma forte regularidade. Afirma-se que tal percepção tenha sido motivada pela leitura, por ele, de um livro de logaritmos que continha na sua contracapa uma tábua de números primos.

O que Gauss fez foi estudar uma função, que posteriormente foi denotada por $\pi(x)$, definida como o número de primos p tais que $p \leq x$, chamada de *função de contagem dos números primos*. Assim temos, por exemplo, $\pi(1) = 0$, $\pi(2) = 1$, $\pi(3) = 2$, $\pi(10) = 4$, $\pi(100) = 25$, $\pi(1000) = 168$, etc. Temos também $\pi(\sqrt{2}) = 0$, $\pi(e) = 1$, $\pi(\pi) = 2$, etc. Desse modo, a proporção de números primos entre 1 e x é dada por $\frac{\pi(x)}{x}$.

Seria muito útil se fosse possível analisar o comportamento deste quociente, mas devido a sua complexidade, Gauss buscou encontrar uma função de comportamento bem conhecido que se aproximasse de $\frac{\pi(x)}{x}$ para x suficientemente grande. Utilizando cálculos mais modernos, podemos construir a Tabela 2.1.

Uma tabela semelhante, embora não tão longa, foi construída por Gauss. Ele observou que, sempre que multiplicava seu espaço amostral por 10, a proporção de primos

x	$\pi(x)$	$\frac{x}{\pi(x)}$
10	4	2,5
100	25	4,0
1.000	168	6,0
10.000	1.229	8,1
100.000	9.592	10,4
1.000.000	78.498	12,7
10.000.000	664.579	15,0
100.000.000	5.761.455	17,4
1.000.000.000	50.847.534	19,7
10.000.000.000	455.052.511	22,0

Tabela 2.1: Proporção de primos até x

era adicionada em cerca de 2,3. Essa propriedade de transformar produtos em somas é a que caracteriza as funções logarítmicas. Pensou ele que deveria, então, haver uma base a de modo que:

$$\frac{x}{\pi(x)} = \log_a x \iff \frac{\pi(x)}{x} = \frac{1}{\log_a x}$$

Analisando tabelas, Gauss concluiu que essa base poderia ser o número e, e assim conjeturou:

$$\frac{\pi(x)}{x} \approx \frac{1}{\ln x} \iff \pi(x) \approx \frac{x}{\ln x}$$

Na Figura 2.1, temos o gráfico das duas funções no intervalo $[1, 100]$.

No gráfico vemos que parece haver uma semelhança no comportamento das duas funções no intervalo dado, apesar da característica distinta quanto a continuidade em certos pontos isolados. Mas a estimativa $\frac{x}{\ln x}$ dada por Gauss parece subestimar o verdadeiro valor de $\pi(x)$, pois o gráfico de $\frac{x}{\ln x}$ parece ficar, a partir de um certo ponto, sempre abaixo do gráfico de $\pi(x)$.

Gostaria-se de poder provar que $\pi(x)$ e $\frac{x}{\ln x}$ eram *assintoticamente iguais*, isto é, que ambas se aproximassem, relativamente, tanto quanto desejado, bastando para isso tomar x suficientemente grande. Matematicamente, conforme ([11], p. 150), dizemos que

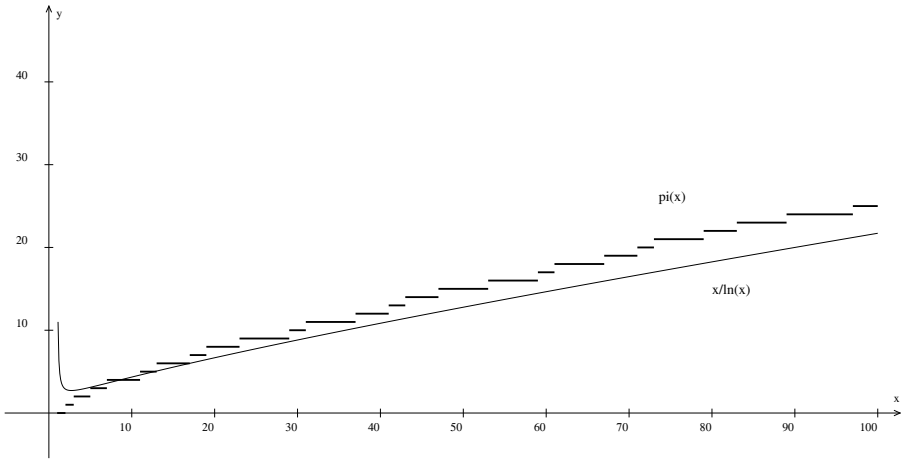

Figura 2.1: Gráfico conjunto de $\pi(x)$ e $\frac{x}{\ln x}$

duas funções $f(x)$ e $g(x)$ contínuas e positivas são assintoticamente iguais, e escrevemos $f(x) \sim g(x)$, se:

$$\lim_{x\to\infty} \frac{f(x)}{g(x)} = 1$$

Em 1896, de la Valleé Poussin e Hadamard, independentemente, demonstraram que:

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

resultado que ficou conhecido como *Teorema dos Números Primos*, provando a igualdade assintótica das duas funções. A demonstração deste teorema é bastante difícil e não será apresentada aqui, mas está no apêndice A de [8], e utiliza ferramentas de Análise Complexa. Em 1949, Selberg recebeu a Medalha Fields, o maior reconhecimento que um matemático pode ter, por ter simplificado de forma substancial a demonstração original desse teorema. Por meio dele, podemos obter uma boa aproximação para o n-ésimo número primo p_n, vendo que $p_n \approx n \ln n$.

Inconformado com a aparente incorreção da estimativa de Gauss, e analisando as tabelas de primos existentes até então, Legendre apresentou o que seria uma melhoria na estimativa. Segundo ([5], p. 63):

> "O aperfeiçoamento de Legendre consistiu em substituir a aproximação $N/ln(N)$ por
>
> $$\frac{N}{\ln N - 1,08366}$$

> introduzindo assim uma pequena correção que tinha o efeito de desviar a curva de Gauss em direção ao número verdadeiro de primos. Considerando-se os valores dessas funções situados dentro do alcance computacional [da época], era impossível distinguir os gráficos de $\pi(N)$ da estimativa de Legendre".

Além do mais, no século XIX havia uma grande preocupação com a aplicação prática da matemática, que deveria dar resultados mais precisos quanto possível, independentemente do método empregado, o que pesava a favor da estimativa de Legendre.

Porém, o termo 1,08366 introduzido na fórmula era um tanto "feio", totalmente artificial, o que fez com que alguns matemáticos acreditassem que deveria haver algo melhor e mais natural. Esse, na verdade, é um "exemplo de uma ideologia quase geral entre os matemáticos, segundo a qual, entre um mundo feio e outro estético, a natureza sempre escolhe o segundo" (ver [5], p. 64).

Anos mais tarde, o próprio Gauss apresentou um refinamento na sua estimativa, que ficou conhecida como a *integral logarítmica*, denotada por $Li(x)$, onde (ver [11], p. 156):

$$\pi(x) \approx Li(x) = \int_2^x \frac{dt}{\ln t}$$

Segundo ([5], p. 64), a justificativa teórica da nova estimativa de Gauss se baseava na ideia de probabilidade:

> "Como a distribuição (dos primos) parecia tão aleatória, o lançamento de uma moeda talvez fosse um bom modelo para a escolha dos primos. [...] Porém, pensou Gauss, a moeda teria que ser viciada, de modo que não caísse em cara a metade das vezes, e sim com a probabilidade de $1/ln(N)$".

Assim como, em N lançamentos de uma moeda não viciada, espera-se que o número de caras seja

$$\underbrace{\frac{1}{2} + \frac{1}{2} + \cdots + \frac{1}{2}}_{N\ termos}$$

Gauss supôs que, para a moeda viciada dos primos, o número de caras, ou seja, o número de primos até N, seria algo como

$$\frac{1}{\ln 2} + \frac{1}{\ln 3} + \frac{1}{\ln 4} + \cdots + \frac{1}{\ln N}$$

Considerando cada um destes termos como a área de um retângulo com base igual a 1 e altura igual a $\frac{1}{\ln n}$, para $n = 2, \ldots, N$, Gauss seguiu os passos naturais que o levaram até a integral logarítmica, que é a área exata sob a curva, limitada pelas retas $x = 2$, $x = N$ e o eixo-x, conforme a Figura 2.2.

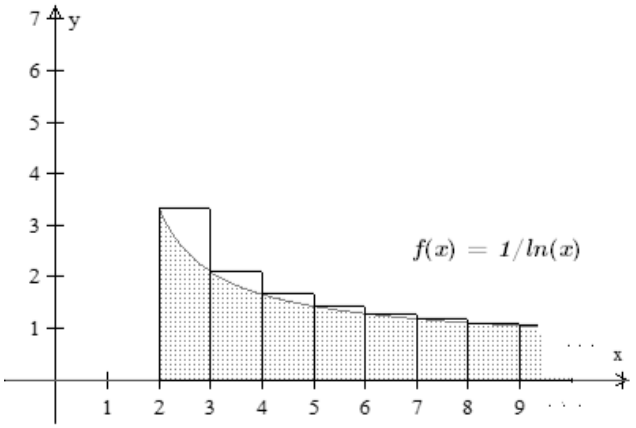

Figura 2.2: A integral logarítmica $\int_2^N \frac{1}{\ln(x)}\, dx$

Na Tabela 2.2, podemos comparar as estimativas sobre o número de primos até x.

x	Erro (%) de $\frac{x}{\ln x}$	Erro (%) de $\frac{x}{\ln x - 1{,}08366}$	Erro (%) de $\int_2^x \frac{dt}{\ln t}$
10	8,57	105,10	28,00
10^2	-13,14	13,59	16,32
10^3	-13,83	2,20	5,10
10^4	-11,65	0,12	1,31
10^5	-9,44	-0,04	0,38
10^6	-7,79	0,06	0,16
10^7	-6,64	0,08	0,05
10^8	-5,77	0,11	0,01
10^9	-5,09	0,14	0,003
10^{10}	-4,56	0,15	0,0007

Tabela 2.2: Erro (%) cometido pelas estimativas de Gauss e Legendre.

A nova estimativa de Gauss passou a ser mais precisa que a de Legendre, à medida

que as tabelas de números primos começaram a ficar mais extensas. Como consta em ([5], p. 66): "A análise teórica de Gauss havia triunfado sobre a tentativa de Legendre de manipular sua fórmula para se adequar aos dados disponíveis."

Contudo, apesar de precisa, a estimativa $Li(x)$ é uma função cujo gráfico é contínuo, suave, enquanto $\pi(x)$ se parece a uma escada. A pergunta natural que se seguiu foi: será que a porcentagem de erro entre a integral logarítmica de Gauss e o número real de primos se torna cada vez menor quanto mais avançamos na contagem? Isto é, será que os primos continuam se comportando segundo este padrão mesmo em lugares da sequência onde talvez nunca tenhamos alcance computacional suficiente para verificar?

Capítulo 3

A Hipótese de Riemann e a segurança da internet

Durante boa parte da sua vida, Euler dedicou-se ao estudo das séries infinitas. Uma das séries utilizadas para introduzir o assunto, nos cursos de Cálculo, é a série $\sum_{n=1}^{\infty} \frac{1}{n^s}$, que aprendemos ser convergente sempre que $s > 1$.

De fato, se $s > 1$, a função $f(x) = \frac{1}{x^s}$ é contínua, positiva e decrescente em $(1, \infty)$. Aplicando o teste da integral, temos:

$$\begin{aligned} \int_1^{\infty} \frac{1}{x^s}\, dx &= \lim_{t\to\infty} \int_1^t \frac{1}{x^s}\, dx \\ &= \lim_{t\to\infty} \frac{x^{-s+1}}{-s+1}\Bigg|_{x=1}^{x=t} \\ &= \lim_{t\to\infty} \frac{1}{1-s}\left(\frac{1}{t^{s-1}} - 1\right) \end{aligned}$$

Como $s > 1$, temos que $s - 1 > 0$. Logo, quando $t \to \infty$, temos $t^{s-1} \to \infty$ e $\frac{1}{t^{s-1}} \to 0$. Portanto:

$$\int_1^{\infty} \frac{1}{x^s}\, dx = \frac{1}{s-1} \qquad (s > 1)$$

Dessa forma, a integral converge, e portanto, pelo teste, a série converge.

Assim, essa série define uma função $\zeta(s)$, quando $s > 1$, isto é:

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$$

que posteriormente recebeu o nome de *função zeta de Euler*.

Entretanto, calcular os valores da função ζ para algum valor $s > 1$ é uma tarefa bastante complicada. Conforme consta em ([6], p. 498), Euler utilizou, em 1735, o procedimento descrito a seguir para o cálculo de $\zeta(2)$.

Tomemos a série de Maclaurin:

$$\operatorname{sen} x = x - \frac{x^3}{3!} + \frac{x^5}{5!} - \frac{x^7}{7!} + \dots$$

Então (após a divisão por x):

$$\operatorname{sen} x = 0 \Leftrightarrow 1 - \frac{x^2}{3!} + \frac{x^4}{5!} - \frac{x^6}{7!} + \dots = 0$$

Fazendo a substituição $y = x^2$, temos:

$$1 - \frac{y}{3!} + \frac{y^2}{5!} - \frac{y^3}{7!} + \dots = 0$$

Da teoria das equações, sabemos que a soma dos inversos das raízes da equação é igual ao oposto da razão entre o termo de primeiro grau e o termo independente, o que pode ser demonstrado utilizando as *Relações de Girard*, que são abordadas no Ensino Médio.

Como as raízes deste polinômio em x são π, 2π, 3π, ..., temos que as raízes do polinômio em y são π^2, $(2\pi)^2$, $(3\pi)^2$, ... Assim:

$$\frac{1}{\pi^2} + \frac{1}{(2\pi)^2} + \frac{1}{(3\pi)^2} + \dots = \frac{1}{6}$$

Ou seja:

$$\frac{1}{1^2} + \frac{1}{2^2} + \frac{1}{3^2} + \dots = \frac{\pi^2}{6} = \zeta(2)$$

Euler também chegou a uma fórmula para calcular o valor de ζ em todos os naturais pares, de onde se mostra, por exemplo, que $\zeta(4) = \sum_{n=1}^{\infty} \frac{1}{n^4} = \frac{\pi^4}{90}$.

Contudo, para um argumento ímpar, a dificuldade é ainda maior. Sobre o valor de $\zeta(3)$ consta em ([6], p. 499): "...não se sabe nem mesmo se a soma dos inversos dos cubos dos inteiros positivos é um múltiplo racional de π^3".

Euler também descobriu uma relação fundamental para o tema entre a função ζ e os números primos, por meio do *Produto de Euler*, conforme segue:

Teorema 3.1. *Se $s > 1$, então*

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_{p\,primo} \frac{1}{1 - \frac{1}{p^s}}$$

onde a expressão à direita é o produto de Euler.

Demonstração. Se $|x| < 1$, sabemos que (soma da progressão geométrica infinita):

$$\frac{1}{1-x} = 1 + x + x^2 + \dots$$

Como $\left|\frac{1}{p}\right| < 1$ para todo primo p, temos que:

$$\frac{1}{1 - \frac{1}{p^s}} = 1 + \frac{1}{p^s} + \frac{1}{p^{2s}} + \dots$$

Multiplicando essas séries para todos os primos p, e lembrando que, pelo teorema 2.4, todo inteiro $n > 1$ é expresso de modo único como produto de potências de diferentes primos, então:

$$\begin{aligned} \prod_{p\,primo} \frac{1}{1 - \frac{1}{p^s}} &= \prod_{p\,primo} \left(1 + \frac{1}{p^s} + \frac{1}{p^{2s}} + \dots\right) \\ &= 1 + \frac{1}{2^s} + \frac{1}{3^s} + \dots + \frac{1}{n^s} + \dots \\ &= \sum_{n=1}^{\infty} \frac{1}{n^s} \end{aligned}$$

□

Este teorema nos mostra que existe uma relação entre a função ζ e os números primos. Usando essa série, Euler construiu uma outra demonstração para a infinitude dos primos (Teorema 1.1).

Demonstração (De Euler para a infinitude dos números primos). Pelo teorema 3.1:

$$\sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_{p\,primo} \frac{1}{1-\frac{1}{p^s}}$$

Se houvesse um número finito de primos, então o produto no segundo membro da expressão seria finito para todo $s > 0$, em particular para $s = 1$. Entretanto, para $s = 1$, o valor da primeiro membro é a série harmônica $1 + \frac{1}{2} + \frac{1}{3} + \ldots$, que sabemos ser divergente, o que contradiz o fato de que o produto à direita é finito. Logo, existem infinitos números primos. □

Mas o papel da função ζ sobre a teoria dos números ainda estava apenas começando. Anos mais tarde, enquanto se dedicava a explorar o recém-definido plano complexo, Riemann teve a ideia de estender o domínio da função ζ para todos os números complexos cuja parte real fosse superior a 1. Assim, definiu uma nova função:

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}, \quad para\ \Re(s) > 1$$

que ficou conhecida como *função zeta de Riemann.*

Mas o grande avanço que Riemann obteve foi quando conseguiu prolongar analiticamente a função ζ para todo o plano complexo, particularmente para regiões à esquerda da reta $\Re(s) = 1$.

Em 1859, Riemann encontrou a equação funcional para a função zeta (ver [1], p. 40):

$$\zeta(s) = 2(2\pi)^{s-1}\zeta(1-s)\Gamma(1-s)\,\mathrm{sen}\left(\frac{\pi s}{2}\right)$$

onde

$$\Gamma(s) = \int_0^{\infty} e^{-u}u^{s-1}\,du$$

é a *função gama de Euler*, que é uma extensão da função fatorial para números complexos (ver [10], p. 77-90).

Em seguida, apresentou a hoje conhecida como *função de Riemann* (ver [11], p. 160):

$$R(x) = \sum_{n=1}^{\infty} \frac{\mu(n)}{n} Li(x^{\frac{1}{n}})$$

onde $\mu(n)$ é a *função de Möbius* (ver [12], p. 75), definida por:

$$\mu(n) = \begin{cases} 1 & se \quad n = 1 \\ 0 & se \quad a^2|n \text{ para algum } a > 1 \\ (-1)^k & se \quad n \text{ é o produto de } k \text{ primos distintos} \end{cases}$$

Riemann obteve então a seguinte fórmula (exata!) para $\pi(x)$ ([11], p. 160):

$$\pi(x) = R(x) - \sum_{\rho} R(x^{\rho})$$

onde o somatório é extendido a todos os zeros ρ *não-triviais* de $\zeta(s)$, cada um contado com a sua multiplicidade. Nesta fórmula, $R(x)$ é uma excelente estimativa para $\pi(x)$, enquanto que o somatório representa o erro desta estimativa, funcionando como uma parcela de correção, fazendo com que a expressão seja uma equação. A função de Riemann $R(x)$ é uma aproximação ainda melhor do que $Li(x)$ para $\pi(x)$.

Assim, percebeu-se que o caminho para melhorar a estimativa era estudar a localização dos zeros da função ζ. Estes são de dois tipos:

a) *zeros triviais*: -2, -4, -6, ..., $-2n$, ... ($n \in \mathbb{N}$)

De fato, se $\Re(s) > 1$, pelo Produto de Euler $\zeta(s) \neq 0$, isto é, não há raízes nessa porção do plano complexo. Se $\Re(s) < 0$, a própria equação funcional nos dá os zeros triviais.

b) *zeros não-triviais*: zeros contidos no conjunto dos números complexos s tais que $0 \leq \Re(s) \leq 1$. A fórmula de $\pi(x)$ apresentada por Riemann requer o conhecimento da localização dos zeros nessa faixa do plano, que ficou conhecida como *domínio crítico* da função ζ. Um estudo aprofundado, em português, sobre a função zeta de Riemann, pode

ser encontrado em [1].

Em 1859, Riemann fez uma afirmação que resiste à demonstração até hoje. Ele conjeturou que todos os zeros da função ζ, no domínio crítico, encontram-se sobre a reta $\Re(s) = \frac{1}{2}$. Isto é, ele afirmou que os zeros não-triviais da função zeta são da forma $\frac{1}{2} + it$. Tal conjetura ficou universalmente conhecida como "A Hipótese de Riemann". A validade deste resultado implica que não há surpresas no comportamento da sequência dos números primos, ou seja, o padrão de regularidade que eles mantêm, e que pode ser expresso pela integral logarítmica de Gauss, não se altera jamais, por mais que avancemos na contagem até valores incomputáveis. A validade da Hipótese de Riemann significa, então, que os primos são "bem comportados", e não fazem nada "inesperado" em locais onde nossa vista não alcança.

Uma das mais importantes aplicações atuais das propriedades dos números primos é na segurança da informação que trafega pela internet. Já vimos, pelo Teorema 1.4, que todo número natural pode ser decomposto de modo único como produto de primos. Contudo, encontrar esta decomposição costuma não ser uma tarefa fácil. Por exemplo, tente com o número composto 5.063, relativamente pequeno. Leva um bom tempo para decompor este número sem ajuda de algum meio eletrônico. Esta característica é o segredo da chamada "criptografia RSA".

Em 1978, os matemáticos Ron Rivest, Adi Shamir e Leonard Adleman, do Instituto de Tecnologia de Massachusetts (MIT), criaram este sistema de criptografia, que foi batizada com as iniciais dos seus sobrenomes, e que atualmente domina o campo da segurança na internet.

Mas o que é criptografia? Segundo ([3], p. 1):

> "Em grego, *cryptos* significa secreto, oculto. A criptografia estuda os métodos para codificar uma mensagem de modo que só seu destinatário legítimo consiga interpretá-la. É a arte dos códigos secretos [...]. Naturalmente, todo código vem acompanhado de duas receitas: uma para codificar uma mensagem; outra para decodificar uma mensagem codificada."

Para interpretar uma mensagem codificada, temos duas formas: decodificá-la ou decifrá-la. Qual é a diferença? Decifrar significa interpretar uma mensagem codificada sem possuir a receita de decodificação. Obviamente, esta opção é utilizada por quem não é o destinatário legítimo da mensagem. Assim, o objetivo dos criadores de códigos criptográficos é dificultar ao máximo o trabalho dos decifradores.

O RSA funciona da seguinte forma (ver [3], p. 4):

1. Escolhemos dois números primos p e q.
2. Para codificar uma mensagem, utilizamos o número $n = p \cdot q$.
3. Para decodificar uma mensagem, precisamos conhecer p e q.

Como já foi dito, a segurança do método reside na dificuldade de fatorar n, ou seja, na dificuldade de se obter p e q, mesmo possuindo n. Isto, é claro, quando se está falando de números grandes, com centenas de algarismos, como os que são usados atualmente para a segurança da internet pela criptografia RSA. Números como $5.063 = 61 \cdot 83$, apesar de apresentarem algum trabalho para um ser humano, são decompostos instantaneamente por qualquer microcomputador moderno.

Outra pergunta que surge é a de como obter primos grandes como p e q? Teríamos que escolher dois números grandes quaisquer, e tentar fatorá-los, para assim descobrir se eles são primos? Se assim fosse, enfrentaríamos o mesmo tipo de dificuldade que atribui segurança ao método RSA, e este seria tão difícil de implementar quanto é de decifrar. Felizmente, para o sucesso do RSA, existem testes que permitem verificar se um número grande é primo ou composto, sem fatorá-lo. Para mais detalhes sobre estes métodos e também sobre Criptografia RSA, consultar [3].

Os matemáticos têm desenvolvido métodos poderosos de fatoração, e que continuamente são aprimorados. Segundo ([4], p. 74):

> "Estes métodos fazem uso de muito do que se sabe sobre os números primos e cada vez que há um avanço em nosso conhecimento sobre estes números, existe uma possibilidade de que isto leve a um novo método de fatoração.

> Uma vez que a Hipótese de Riemann nos diz tanto a respeito dos primos, uma prova dessa conjetura poderia perfeitamente levar a um grande progresso nas técnicas de fatoração".

Em 1900, no Congresso Internacional de Matemáticos em Paris, David Hilbert (1862 - 1943) apresentou sua lista de 23 problemas a serem "atacados" pelos matemáticos no novo século que se iniciava, e a Hipótese de Riemann já constava entre eles. 100 anos após, em 2000, o Clay Mathematics Institute ofereceu um prêmio de 1 milhão de dólares a quem provasse um dos "Sete Problemas do Milênio", e entre eles novamente se encontrava a Hipótese de Riemann. Segundo ([4], p. 74): "com a segurança da internet e grande parte da matemática contemporânea pesando na balança, tem muito mais em jogo no Problema de Riemann do que o Prêmio do Milênio de 1 milhão de dólares".

A conjetura de Riemann recebeu o nome de "hipótese", por causa de inúmeros outros resultados obtidos posteriormente, por outros matemáticos, utilizando-se da conjetura, e que, portanto, dependem de sua veracidade.

Na época de Riemann, os recursos computacionais praticamente inexistiam, e assim, os indícios descobertos por ele não pareciam ser suficientes para uma generalização. Esta foi baseada principalmente na própria intuição de Riemann e na crença que ele, assim como a maioria dos matemáticos, possuía na estética da natureza.

Até 1920, haviam sido localizados apenas 138 zeros não triviais da função zeta, todos eles sobre a linha crítica. Apesar de G. H. Hardy (1877 - 1947) ter demonstrado que haviam infinitos zeros sobre a linha crítica, isto não significava que não existisse algum zero fora dela.

Com o desenvolvimento dos recursos computacionais, abriu-se uma nova perspectiva em relação à Hipótese de Riemann: a de refutá-la. Bastava para isso encontrar um único zero fora da linha crítica.

Em 1956, as máquinas de Derrick Lehmer verificaram que os primeiros 25.000 zeros estavam sobre a linha. Em 1969, Rosser, Yohe e Schoenfeld determinaram que os primei-

ros 3.500.000 zeros estavam de acordo com a conjetura de Riemann. Em 2004, Gourdon e Demichel determinaram que os 10^{13} primeiros zeros não-triviais da função zeta estavam sobre a reta crítica.

Um exemplo de que estes resultados, em matemática, não significam nada, é o caso da *Conjetura de Mertens*, que recebeu este nome em homenagem ao matemático alemão Franz Mertens (1840 - 1927). A função de Mertens, muito usada em teoria dos números, é definida como:

$$M(n) = \sum_{k=1}^{n} \mu(k)$$

onde $\mu(k)$ é a já mencionada função de Möbius.

Como $\mu(k)$ só assume os valores -1, 0 e 1, temos obviamente que $M(n) \leq n$, $\forall n \in \mathbb{N}$. Mertens foi além, e conjeturou que $M(n) \leq \sqrt{n}$, $\forall n \in \mathbb{N}$.

Segundo ([5], p. 239), "em 1917, Mertens produziu tabelas de cálculo até $n = 10.000$ para dar apoio a sua conjetura. Nos anos 1970, as observações experimentais já haviam chegado a um bilhão". Somente em 1985, Odlyzko e Te Riele refutaram a conjetura, por meio de um experimento computacional envolvendo o cálculo dos primeiros 2.000 zeros da função ζ, até 100 casas decimais, o que era equivalente a verificar a conjetura para $n > 10^{30}$. Ou seja, somente para um número n absurdamente grande, encontramos um contraexemplo para a conjetura. Se tivéssemos nos deixado levar pelos dados obtidos anteriormente, teríamos erroneamente a considerado como verdadeira.

Enquanto isso, a Hipótese de Riemann continua sem demonstração, o que significa, simplesmente, que não sabemos se ela é verdadeira.

Conclusão

A motivação inicial era abordar um assunto, que em nossa concepção, não recebe a devida importância nos programas curriculares, e dessa forma, fomentar sua disseminação e aprendizado por alunos e professores de matemática.

Agora sabemos que os primos são infinitos, e que, junto com a operação de multiplicação, constroem todos os naturais, exceto a unidade. Sabemos também que, mesmo existindo saltos arbitrariamente grandes na sequência dos primos, sempre haverá um primo entre um natural qualquer e seu dobro.

Para chegar a essas conclusões, usamos probabilidades, logaritmos, calculamos séries infinitas, aplicamos várias funções especiais, observamos padrões e proferimos conjeturas. Fizemos demonstrações, diretas, indiretas, de existência e unicidade. Enfim, mantivemos contato com diversas áreas da matemática, somente para escrever sobre os números primos. Tudo isso acaba por reforçar nossa ideia de que tal assunto é pouco aproveitado pelos educadores, visto que possibilita enorme integração entre conceitos e áreas distintas da matemática.

Tivemos contato com a natureza estética da matemática, que preferiu a estimativa de Gauss a de Legendre. Sempre poderemos inserir termos de correção artificiais em nossos modelos, assim como fez Legendre, de modo que os mesmos convirjam perfeitamente para os dados existentes. Mas devemos, como Gauss, buscar entender profundamente a natureza do problema e da realidade, de modo que nossos modelos não precisem destes termos de correção, de modo que continuem convergindo mesmo para os novos dados que surgirão no futuro.

A estética da matemática se apresentou também a Riemann. Somente confiando nela ele pôde, em uma época onde os recursos computacionais eram inexistentes, conjeturar que havia um padrão nos zeros da função ζ. Ele provavelmente tenha calculado somente alguns poucos destes infinitos zeros, e sua intuição contribuiu com o restante.

Com a ampliação dos recursos computacionais nos nossos dias, pôde-se calcular muitos mais destes zeros, e todos obedecem a conjetura de Riemann. Isto seria mais do que suficiente em qualquer outra área do conhecimento, mas na matemática, não significa quase nada. Mesmo havendo infinitos zeros sobre a linha crítica, não poderemos afirmar que todos estão, o que é o anseio dos matemáticos. No máximo, isto serve para manter as esperanças na veracidade da conjetura e na existência de uma demonstração para a mesma.

Mas, poderíamos nos perguntar: se ela for verdadeira, então certamente há uma demonstração (que ainda não descobrimos)? Não necessariamente. O lógico-matemático austríaco Kurt Gödel (1906 - 1978) demonstrou, em seus conhecidos *Teoremas da Incompletude*, que qualquer sistema axiomático suficiente para incluir a aritmética dos números inteiros não pode ser simultaneamente completo e consistente. Isto significa que, admitindo a consistência de um sistema axiomático, ou seja, que não haja contradições entre os resultados deduzidos de seus axiomas, então sempre haverá proposições verdadeiras que não poderão ser provadas dentro do referido sistema. Dessa forma, é possível que a Hipótese de Riemann seja verdadeira sem que seja possível prová-la com os axiomas do sistema formal em que ela é enunciada: a matemática. Curiosamente, Gödel utilizou números primos e o teorema fundamental da aritmética na demonstração destes teoremas.

Essa demonstração, tão buscada, entretanto, não tem tanta importância em si mesma, já que muitos trabalhos posteriores já utilizam a conjetura como hipótese. Na verdade, a grande maioria dos matemáticos acham que ela é verdadeira. A importância está na matemática nova que continuamente é criada na busca por esta demonstração.

Quase toda a teoria dos números foi desenvolvida sem um fim prático imediato. Mesmo assim, a criptografia RSA, por exemplo, está aí para mostrar mais uma vez que o trabalho dos matemáticos puros não é em vão. Uma pergunta muito comum após a

exposição de um assunto novo, em uma típica aula de matemática, é: Para quê serve isto? Essa pergunta nem sempre é oportuna. De fato, o que teria sido da teoria dos números (e da nossa tão prezada internet) se Gauss tivesse desistido de suas ideias pelo simples fato de não vislumbrar uma aplicação prática imediata?

Enfim, viajamos desde a aleatoriedade aparente dos números primos até o padrão descoberto por Gauss e ratificado por Riemann.

Esperamos ter, com este trabalho, aprimorado a visão do assunto que o leitor previamente possuía, preenchendo algumas lacunas, mas principalmente, criando novas, estimulando a curiosidade que deve acompanhar sempre todo estudante de matemática.

Apêndice

De acordo com a conveniência (o professor deve selecioná-las de acordo com a maturidade matemática de sua turma), as seguintes atividades podem ser utilizadas no ensino básico. Estes exercícios são apenas alguns exemplos, para ilustrar a possibilidade de aprofundamento no assunto proposta neste trabalho.

1) Utilizando o *Crivo de Eratóstenes*, encontre todos os números primos entre 2 e 200 (utilize a tabela abaixo).

	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32
33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48
49	50	51	52	53	54	55	56	57	58	59	60	61	62	63	64
65	66	67	68	69	70	71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90	91	92	93	94	95	96
97	98	99	100	101	102	103	104	105	106	107	108	109	110	111	112
113	114	115	116	117	118	119	120	121	122	123	124	125	126	127	128
129	130	131	132	133	134	135	136	137	138	139	140	141	142	143	144
145	146	147	148	149	150	151	152	153	154	155	156	157	158	159	160
161	162	163	164	165	166	167	168	169	170	171	172	173	174	175	176
177	178	179	180	181	182	183	184	185	186	187	188	189	190	191	192
193	194	195	196	197	198	199	200								

a) Você percebeu que a partir de um certo momento não foi mais preciso riscar nenhum número, porque todos os números a serem riscados já haviam sido riscados anteriormente? Qual foi o último número primo que teve algum múltiplo riscado? Porquê?

b) Para saber se um número n é primo, é necessário e suficiente verificar que n não é divísivel por todos os primos p tais que:

( ) $p \leq n-1$ ( ) $p \leq \sqrt{n}$ ( ) $p \leq \sqrt[3]{n}$ ( ) $p \leq \frac{n}{2}$ ( ) $p \leq \frac{n}{3}$

c) Discuta com seus colegas a conclusão acima.

2) Escreva a decomposição em fatores primos para os seguintes números:

a) 73 b) 30 c) 40 d) 221 e) 361

3) Calcule os *Números de Fermat* $F_n = 2^{2^n} + 1$ para $n = 0, 1, 2, 3$ e 4. Verifique que estes números são primos (sugestão: utilize uma calculadora). Podemos afirmar que os Números de Fermat são primos para todo $n \in \mathbb{N}$?

4) Utilizando a tabela construída no exercício 1, encontre todos os pares de *primos gêmeos* (primos separados por um único número natural) menores que 200. Obs.: ainda não se sabe se os primos gêmeos são infinitos.

5) Escreva todos os números pares entre 4 e 50 como soma de dois primos. Obs.: ainda não se sabe se todos os números pares, exceto o 2, podem ser escritos como soma de dois primos (Conjetura de Goldbach).

$4 = 2 + 2$, $6 = 3 + 3$, $8 = 5 + 3$, ...

6) Construa uma sequência de 7 números consecutivos, todos compostos. Existe alguma outra sequência como esta formada por números menores?

7) Complete a seguinte tabela usando uma calculadora científica e esboce o gráfico conjunto (gráfico de pontos) de p_n (n-ésimo primo) em azul e de $n \ln n$ em vermelho para n entre 1 e 20, em uma cartolina. O que podemos dizer a respeito deste gráfico?

n	p_n	$n \ln n$
1	2	0
2	3	$1,4$
3	5	$3,3$
4	7	$5,5$
5	11	$8,0$
6		
7		
8		
9		
10		
11		
12		
13		
14		
15		
16		
17		
18		
19		
20		

Para complementar: uma lista com 15 atividades relacionadas aos números primos podem ser encontradas em [9].

Referências Bibliográficas

[1] AGUILERA-NAVARRO, Maria Cecilia K.; et al. *A função zeta de Riemann*, Revista Ciências Exatas e Naturais - UNICENTRO/PR - Guarapuava, v. 1, n. 1, p. 23-47, 1999.

[2] BOYER, Carl B. *História da matemática*, 2a. ed. - São Paulo: Edgard Blücher, 1996.

[3] COUTINHO, S. C. *Números inteiros e criptografia RSA*. - Rio de Janeiro: IMPA, 2011.

[4] DEVLIN, Keith J. *Os problemas do milênio*, 2a. ed. - Rio de Janeiro: Record, 2008.

[5] DU SAUTOY, Marcus. *A música dos números primos: a história de um problema não resolvido na matemática*. - Rio de Janeiro: Zahar, 2007.

[6] EVES, Howard. *Introdução à história da matemática*, tradução: Hygino H. Domingues. 5a. ed. - Campinas, SP: Editora da UNICAMP, 2011.

[7] HEFEZ, Abramo. *Elementos de aritmética*, 2a. ed. - Rio de Janeiro: SBM, 2011.

[8] MARTINEZ, Fabio Brochero; et al. *Teoria dos números: um passeio com primos e outros números familiares pelo mundo inteiro*, 2a. ed. - Rio de Janeiro: IMPA, 2011.

[9] NERI, Chico; POSSANI, Claudio. *Os primos esquecidos*, Revista do Professor de Matemática - SBM - n. 47, p. 16-20, 2001.

[10] OLIVEIRA, E. Capelas de. *Funções especiais com aplicações*, 1a. ed. - São Paulo: Editora Livraria da Física, 2005.

[11] RIBENBOIM, Paulo. *Números primos. Velhos mistérios e novos recordes*, 1a. ed. - Rio de Janeiro: IMPA, 2012.

[12] SANTOS, José Plínio de Oliveira. *Introdução à teoria dos números*, 3a. ed. - Rio de Janeiro: IMPA, 2010.