UNIVERSIDADE FEDERAL RURAL DE PERNAMBUCO
DEPARTAMENTO DE MATEMÁTICA
Mestrado Profissional em Matemática em Rede Nacional

Janaína Mirele de Lima Silva

O Teorema de Chebyshev e o Fascinante Mundo dos Números Primos

RECIFE
2024

UNIVERSIDADE FEDERAL RURAL DE PERNAMBUCO
DEPARTAMENTO DE MATEMÁTICA
Mestrado Profissional em Matemática em Rede Nacional

Janaína Mirele de Lima Silva

O Teorema de Chebyshev e o Fascinante Mundo dos Números Primos

Dissertação de mestrado apresentada ao Departamento de Matemática da Universidade Federal Rural de Pernambuco como requisito parcial para obtenção do título de Mestre em Matemática.

Orientador: Prof. Dr. Rodrigo Genuino Clemente

RECIFE
2024

Dados Internacionais de Catalogação na Publicação (CIP)
Sistema Integrado de Bibliotecas da UFRPE
Biblioteca Central, Recife-PE, Brasil

S586t Silva, Janaína Mirele de Lima
O Teorema de Chebyshev e o fascinante mundo dos números primos / Janaína Mirele de Lima Silva. – 2024.
64 f. : il.

Orientador: Rodrigo Genuino Clemente.
Dissertação (Mestrado) – Universidade Federal Rural de Pernambuco, Programa de Pós-Graduação Profissional em Matemática em Rede Nacional (PROFMAT), Recife, BR-PE, 2024.
Inclui bibliografia.

1. Números primos 2. Desigualdades (Matemática) 3. Chebyshev, Aproximação de I. Clemente, Rodrigo Genuino, orient. II. Título

CDD 510

JANAÍNA MIRELE DE LIMA SILVA

"O TEOREMA DE CHEBYSHEV E O FASCINANTE MUNDO DOS NÚMEROS PRIMOS."

Trabalho apresentado ao Programa de Mestrado Profissional em Matemática – PROFMAT do Departamento de Matemática da UNIVERSIDADE FEDERAL RURAL DE PERNAMBUCO, como requisito parcial para obtenção do grau de Mestre em Matemática.

Aprovado em 19/07/2024

BANCA EXAMINADORA

Rodrigo Genuino Clemente

Prof. Dr. Rodrigo Genuino Clemente (Orientador) – UFRPE

Islanita C. A. de A. Lima

Profa. Dra. Islanita Cecília Alcantara de Albuquerque Lima - UPE

Bárbara Costa da Silva

Profa. Dra. Bárbara Costa da Silva – PROFMAT/UFRPE

À minha família

Agradecimentos

Primeiramente, gostaria de expressar minha gratidão a Deus pela oportunidade e pela força concedida, especialmente nos momentos mais difíceis, que me possibilitaram a conclusão deste trabalho.

À minha família, que muitas vezes não compreendia minha ausência, mas sempre me incentivou e apoiou incondicionalmente. Em especial, agradeço à minha mãe, Maria Anunciada de Lima Silva, que sempre me incentivou a estudar e me recebia com meus jantares favoritos após cada dia cansativo na universidade; e ao meu pai, José Vieira da Silva, que nunca reclamou de acordar cedo toda sexta-feira para me levar até a rodoviária, garantindo que eu não chegasse atrasada às aulas.

Aos meus colegas de mestrado, com os quais compartilhei as frustrações e desafios ao longo dos dois anos. Especialmente a Gesica Peixoto e a Roberta Oliveira, pela companhia nos almoços e nas preparações para as provas. Estar com vocês tornava mais leve passar o dia na rural.

Às minhas amigas de graduação, Jamyle Paloma, Jéssika Pâmela e Josivânia Nair, que mesmo à distância continuam me apoiando e torcendo pelo meu sucesso.

Às minhas amigas Bianca, Dayse e Mayara pelas leituras incríveis compartilhadas nos últimos anos e por cada encontro mensal repleto de risadas, que me ajudaram a distrair quando o peso do mestrado parecia ser maior do que eu poderia carregar.

Por fim, não posso deixar de expressar minha gratidão a todos os professores que de alguma forma contribuíram para minha formação. Em especial, meu orientador, Rodrigo Clemente, pela paciência, encorajamento, disponibilidade e entusiasmo com a pesquisa. Não poderia ter pedido um orientador melhor para este trabalho.

"Cada um de nós é uma colcha de retalhos daqueles que nos amaram, daqueles que acreditaram em nosso futuro, daqueles que nos mostraram empatia e bondade ou nos disseram a verdade mesmo quando não era fácil ouví-la. Daqueles que nos disseram que poderíamos fazer algo quando não havia absolutamente nenhuma prova disso.
(Taylor Swift)

Resumo

Objeto de fascínio para matemáticos em todo o mundo, os números primos e suas propriedades são utilizados em diversos conteúdos da matemática, desde o ensino fundamental. A descoberta de números primos cada vez maiores é essencial para garantir a segurança das informações dos usuários nas redes. Mesmo com seu papel fundamental na criptografia, que utiliza o produto de primos de ordem maior ou igual a 10^{100} para proteção dos dados, e a certeza da infinitude desses números, a distribuição dos primos em relação aos números naturais ainda é um campo da teoria que continua a ser aprimorado. Como os primos não possuem um padrão que permita identificar o próximo número da sequência e devido à complexidade do Teorema do Número Primo, estudamos a distribuição dos primos a partir do Teorema de Chebyshev, cuja demonstração depende apenas de resultados elementares e conhecidos na matemática. Além disso, continuamos nossa exploração pelo mundo dos primos, apresentando características, curiosidades e resultados sobre os primos de Fermat, Mersenne e Sophie Germain. Por fim, dedicamos o último capítulo a resolver problemas presentes em competições matemáticas que utilizam propriedades dos primos discutidas neste trabalho, com o objetivo de contribuir para a preparação de estudantes que participarão das próximas edições.

Palavras-chave: Números Primos. Teorema de Chebyshev. Teorema do Número Primo.

Abstract

An object of fascination for mathematicians around the world, prime numbers and their properties are used in various mathematics content, starting in elementary school. The discovery of increasingly larger prime numbers is essential to guarantee the security of user information on networks. Even with its fundamental role in cryptography, which uses the product of primes of order greater than or equal to 10^{100} to protect data, and the certainty of the infinity of these numbers, the distribution of primes in relation to natural numbers is still a field of theory that continues to be improved. As primes do not have a pattern that allows identifying the next number in the sequence and due to the complexity of the Prime Number Theorem, we study the distribution of primes based on Chebyshev's Theorem, whose demonstration depends only on elementary results known in mathematics. Furthermore, we continue our exploration of the world of primes, presenting characteristics, curiosities and results about Fermat, Mersenne and Sophie Germain primes. Finally, we dedicate the last chapter to solving problems present in mathematical competitions that use prime properties discussed in this work, with the aim of contributing to the preparation of students who will participate in the next editions.

Keywords: Prime Numbers. Chebyshev's Theorem. Prime Number Theorem.

Lista de ilustrações

Sumário

Introdução

Os Números Primos, isto é, aqueles maiores que 1 que são divisíveis apenas por 1 e por ele mesmo, têm sido objeto de curiosidade e fascínio pelos matemáticos há muitos anos. Desde a Grécia Antiga, as propriedades místicas e numerológicas dos primos levaram os matemáticos da época a desenvolverem diversos resultados importantes, que utilizamos até os dias atuais.

Os primos e suas propriedades são utilizados em diversos resultados da matemática. Apresentados desde a educação básica, aparecem na Base Nacional Comum Curricular (BNCC) (1) entre as habilidades a serem desenvolvidas com os estudantes do sexto ano do Ensino Fundamental e, apesar de não ser citada diretamente na BNCC do Ensino Médio, a decomposição em fatores primos é utilizada nos cálculos de mínimo múltiplo comum (MMC), máximo divisor comum (MDC), para encontrar raízes n-ésimas, entre outros.

Além de sua importância para a matemática, os números primos desempenham papel fundamental na criptografia. Como a finalidade da criptografia é impedir que senhas e mensagens sejam invadidas por pessoas não autorizadas e mal-intencionadas, a dificuldade em fatorar o produto de primos grandes torna seu uso pertinente.

A possibilidade de enviar informações secretas é um problema antigo da nossa sociedade e que foi sendo aperfeiçoado com o passar dos anos. Em 1976, surgiu a ideia de criptografia com chave pública, na qual o usuário define as chaves para encifrar as mensagens que irá receber e conhece o algoritmo necessário para decifrá-las, de modo que o acesso às chaves não permite a descoberta do algoritmo para decodificar as informações (2).

O primeiro sistema empregando o conceito de chave pública surgiu apenas dois anos depois, utilizando o produto de números primos grandes, e foi denominado RSA em virtude dos sobrenomes de seus criadores: Rivest, Shamir e Adleman. Por exemplo, é fácil encontrar a fatoração do número 10.961 e descobrir que ele é decorrência do produto de 97 e 113. Porém, encontrar os primos que geram o número 2.266.784.329 se torna uma tarefa bem mais complicada.

Como a descoberta dos fatores primos multiplicados é necessária para decifrar a mensagem, a criptografia utiliza números primos da ordem maior ou igual a 10^{100}, o que torna essa tarefa humanamente impossível de ser realizada. Os valores são tão grandes que levaria anos para um computador de alto desempenho encontrar os fatores e, até lá, a informação decifrada já teria se tornado inútil, daí a busca por primos cada vez maiores.

Euclides provou que existem infinitos números primos em 300 a. C. e a demonstração

de que todo número natural é primo ou produto de primos é tão importante que conhecemos como o Teorema Fundamental da Aritmética. Entretanto, a distribuição dos primos em relação à infinitude de naturais ainda é um campo da teoria que tem sido aperfeiçoado.

Uma dificuldade no estudo da distribuição dos primos é que eles não possuem um padrão que permite identificar qual será o próximo. Observe a sequência dos primos menores que 100:

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.

Nesse pequeno intervalo analisado, note que a diferença de um primo para o próximo variou entre 1, 2, 4, 6 e 8, e não seguiu uma ordem, o que dificulta a descoberta dos próximos primos da sequência. À medida em que analisamos números muito grandes, fica ainda mais difícil identificar se é um número composto ou não, sendo necessário o uso de tecnologias digitais.

Descoberto em 2018, o maior primo conhecido atualmente é o $2^{82.589.933} - 1$, que possui mais de 24 milhões de dígitos (3). O número foi encontrado por um norte-americano utilizando o aplicativo gratuito Great Internet Mersenne Prime Search (GIMPS), software que realiza a busca por Primos de Mersenne, sendo uma recompensa em dinheiro oferecida a quem for bem sucedido em sua procura.

Desde sua criação por George Woltman em 1996, o GIMPS contribuiu para a descoberta de 17 primos de Mersenne, porém, mesmo com o uso de tecnologia, tais descobertas são raras e exigem muito tempo. Para provar que $2^{82.589.933} - 1$ é um primo, por exemplo, foram necessários 12 dias ininterruptos de teste por um computador para ter certeza que ele não é divisível por nenhum número menor que ele (3).

Assim, este trabalho tem como objetivo geral estudar a distribuição dos números primos a partir do Teorema de Chebyshev, utilizando resultados elementares e conhecidos na matemática, em especial o estudo da função $\pi(x)$, que determina todos os primos menores ou igual a x.

Como objetivos específicos temos: compreender as propriedades elementares da função $\pi(x)$; demonstrar o Teorema de Chebyshev; explorar resultados acerca dos primos de Fermat, Mersenne e Sophie Germain; e resolver problemas de competições matemáticas envolvendo números primos.

Vale ressaltar que o estudo dos números primos é um campo de estudo bastante amplo e, por isso, é praticamente impossível reuní-lo em um único documento. Dessa forma, esperamos que esse trabalho sirva de suporte para professores e estudantes que desejam expandir seus conhecimentos, bem como auxilie na elaboração de material para preparação de olimpíadas e no desenvolvimento de projetos acerca do tema.

1 Noções Introdutórias

Reservamos este capítulo para apresentar e provar as propriedades elementares da teoria dos números necessárias para a compreensão das demonstrações realizadas no decorrer deste trabalho. Para isso, utilizamos como referências os trabalhos de (4), (5) e (6).

1.1 Teorema Fundamental da Aritmética

Nesta seção, iremos explorar o teorema fundamental da aritmética, o qual trata da decomposição dos números inteiros em fatores primos.

Definição 1.1. Dados a e b inteiros, dizemos que a *divide* b, e escrevemos $a|b$, se existe $c \in \mathbb{Z}$ tal que $b = c \cdot a$. Também dizemos que a é um *fator* de b, ou ainda que b é *múltiplo* de a.

Definição 1.2. Um número natural n, com $n > 1$, é chamado de *número primo* se possui exatamente dois divisores: o um e ele próprio.

Definição 1.3. Dizemos que um número é composto se esse pode ser escrito como o produto de dois ou mais números primos.

Teorema 1.4 (Teorema Fundamental da Aritmética)**.** *Todo inteiro maior que* 1 *pode ser escrito na forma*

$$p_1{}^{\alpha_1} \cdot p_2{}^{\alpha_2} \cdot \ldots \cdot p_r{}^{\alpha_r},$$

em que os p_i *representam primos distintos e* $\alpha_i \geq 0$*, para todo* $i = 1, \ \ldots, \ r$*; essa fatoração é única.*

Demonstração. Vamos começar mostrando que todo inteiro maior que 1 pode ser escrito como produto de números primos utilizando indução matemática. Observe que 2 é primo, logo o resultado é verdadeiro para $n = 2$. Para $n > 2$ e $k \in \mathbb{Z}$, suponha que todo $1 < n \leq k$ pode ser escrito como produto de primos. Observe que $k + 1$ ou é primo ou é composto. Se $k + 1$ é primo, não há o que mostrar. Suponha então que $k + 1$ é um número composto, daí podemos escrever

$$k + 1 = a \cdot b,$$

com $1 < a < k + 1$ e $1 < b < k + 1$. Como $1 < a \leq k$ e $1 < b \leq k$, então a e b possuem fatoração em primos. Seja $a = p_1 \cdot p_2 \cdot \ldots \cdot p_s$ e $b = p'_1 \cdot p'_2 \cdot \ldots \cdot p'_t$, temos

$$k + 1 = p_1 \cdot p_2 \cdot \ldots \cdot p_s \cdot p'_1 \cdot p'_2 \cdot \ldots \cdot p'_t,$$

isto é, $k+1$ também pode ser escrito como produto de primos, o que conclui a prova por indução.Vamos agora mostrar que a fatoração em primos de um inteiro maior que 1 é única, mais uma vez por indução matemática. Para $n = 2$ é fácil ver que essa fatoração é única, pois 2 é primo. Para $n > 2$ e $k \in \mathbb{Z}$, suponha que cada $1 < n \leq k$ possui fatoração em primos única, vamos mostrar que $k+1$ também possui. Admita que $k+1$ possui duas fatorações distintas, isto é,

$$k+1 \ = \ p_1 p_2 ... p_u \ = \ p'_1 p'_2 ... p'_v,$$

em que $p_1 \leq p_2 \leq ... \leq p_u$ e $p'_1 \leq p'_2 \leq ... \leq p'_v$. Note que p'_1 divide $k+1$, então $p'_1 | p_1 p_2 ... p_u$. Logo, p'_1 divide p_i para algum i. Como p'_1 e p_i são primos, temos $p'_1 = p_i$. Analogamente podemos mostrar que $p_1 = p'_j$ para algum j. Daí, $p_1 = p_j \geq p'_1$ e $p'_1 = p_i \geq p_1$. Como $p_1 \geq p'_1 \geq p_1$, então $p_1 = p'_1$. Portanto, $(k+1)/p_1$ é um inteiro e podemos escrevê-lo como

$$\frac{k+1}{p_1} = p_2 \cdot ... \cdot p_u = p'_2 \cdot ... \cdot p'_v,$$

Entretanto, $(k+1)/p_1$ é um inteiro menor ou igual a k. Logo, pela hipótese de indução, temos $p_2 = p'_2$, ..., $p_u = p'_v$. O que conclui a demonstração da unicidade da fatoração em primos. ■

Exemplo 1.5. Observe a decomposição do número 3960.

$$\begin{aligned} 3960 &= 2 \cdot 1980 = 2 \cdot 2 \cdot 990 = 2 \cdot 2 \cdot 2 \cdot 495 \\ &= 2 \cdot 2 \cdot 2 \cdot 3 \cdot 165 = 2 \cdot 2 \cdot 2 \cdot 3 \cdot 3 \cdot 55 \\ &= 2 \cdot 2 \cdot 2 \cdot 3 \cdot 3 \cdot 5 \cdot 11 \end{aligned}$$

Ou seja, temos $3960 = 2^3 \cdot 3^2 \cdot 5 \cdot 11$.

1.2 Teorema Binomial

A seguir apresentaremos a definição de coeficiente binomial, juntamente com suas propriedades e aplicações essencias para a compreensão da prova do teorema binomial. Este teorema, que permite a expansão de expressões do tipo $(a+b)^n$, será demonstrado ao final da seção.

Definição 1.6. Seja $n \in \mathbb{N}$, definimos o *fatorial* de n e escrevemos $n!$ como o produto de todos os naturais menor ou igual a n. Isto é, $n! = n \cdot (n-1) \cdot (n-2) \cdot ... \cdot 2 \cdot 1$.

Observação 1.7. Por definição, temos $0! = 1$.

Definição 1.8. O coeficiente binomial $\binom{n}{k}$ é o número de formas possíveis de escolher k elementos entre as n possibilidades. Por se tratar de uma combinação em que não importa a ordem dos fatores, pode ser calculado pela expressão

$$\binom{n}{k} = \frac{n!}{(n-k)! \cdot k!}.$$

Observação 1.9. Note que $\binom{n}{0} = \frac{n!}{(n-0)! \cdot 0!} = \frac{n!}{n! \cdot 1} = 1$ e que $\binom{n}{n}$ também é igual a 1, visto que $\binom{n}{n} = \frac{n!}{(n-n)! \cdot n!} = \frac{n!}{0! \cdot n!} = \frac{n!}{n!} = 1$.

Teorema 1.10 (Relação de Stifel)**.** *Dados n e i inteiros, com $0 \leq i \leq n$, temos*

$$\binom{n}{i} + \binom{n}{i+1} = \binom{n+1}{i+1}.$$

Demonstração. Podemos demonstrar a Relação de Stifel utilizando apenas a definição de coeficiente binomial apresentada no início da seção, colocando em evidência e simplificando os termos.

$$\begin{aligned}
\binom{n}{i} + \binom{n}{i+1} &= \frac{n!}{(n-i)!\ i!} + \frac{n!}{(n-i-1)!(i+1)!} \\
&= \frac{n!}{(n-i)(n-i-1)!\ i!} + \frac{n!}{(n-i-1)!(i+1)\ i!} \\
&= \frac{(i+1)\ n! + (n-i)\ n!}{(n-i)(n-i-1)!(i+1)\ i!} \\
&= \frac{(i+1+n-i)\ n!}{(n-i)!\ (i+1)!} \\
&= \frac{(n+1)\ n!}{(n-i)!(i+1)!} \\
&= \frac{(n+1)!}{(n-i)!(i+1)!} \\
&= \binom{n+1}{i+1}.
\end{aligned}$$

■

Teorema 1.11 (Teorema Binomial)**.** *Sejam x e y números reais e $n \in \mathbb{N}$, temos que*

$$(x+y)^n = x^n + \binom{n}{1}x^{n-1}y + \binom{n}{2}x^{n-2}y^2 + ... + \binom{n}{n-1}xy^{n-1} + y^n.$$

Demonstração. Vamos demonstrar a relação utilizando indução matemática em n. Para $n = 0$, temos $(x+y)^0 = 1 = \binom{0}{0}x^0y^0$. Logo, a relação é válida para $n = 0$. Para $n = 1$ a igualdade também é válida, pois $(x+y)^1 = \binom{1}{0}x^1y^0 + \binom{1}{1}x^0y^1 = x + y$. Agora suponha que a relação é válida para algum $n \geq 1$. Vamos mostrar que também vale para $n+1$. Note que

$$(x+y)^{n+1} = (x+y) \cdot (x+y)^n.$$

Por hipótese de indução, segue que

$$(x+y)^{n+1} = (x+y) \cdot \left[\binom{n}{0}x^n + \binom{n}{1}x^{n-1}y + ... + \binom{n}{n-1}xy^{n-1} + \binom{n}{n}y^n\right].$$

Aplicando a propriedade distributiva da adição, temos

$$(x+y)^{n+1} = x\cdot\left[\binom{n}{0}x^n + \binom{n}{1}x^{n-1}y + ... + \binom{n}{n-1}xy^{n-1} + \binom{n}{n}y^n\right] + y\cdot\left[\binom{n}{0}x^n + \binom{n}{1}x^{n-1}y + ... + \binom{n}{n-1}xy^{n-1} + \binom{n}{n}y^n\right].$$

Daí,

$$(x+y)^{n+1} = \binom{n}{0}x^{n+1} + \binom{n}{1}x^n y^1 + ... + \binom{n}{n-1}x^2y^{n-1} + \binom{n}{n}x^1y^n + \binom{n}{0}x^n y^1 + \binom{n}{1}x^{n-1}y^2 + ... + \binom{n}{n-1}x^1y^n + \binom{n}{n}y^{n+1}.$$

Organizando os termos com o mesmo fator temos

$$(x+y)^{n+1} = \binom{n}{0}x^{n+1} + \left[\binom{n}{0} + \binom{n}{1}\right]x^n y^1 + \cdots + \left[\binom{n}{n-1} + \binom{n}{n}\right]x^1y^n + \binom{n}{n}y^{n+1}.$$

Pela Relação de Stifel (1.10), segue que

$$(x+y)^{n+1} = \binom{n}{0}x^{n+1} + \binom{n+1}{1}x^n y^1 + ... + \binom{n+1}{n}x^1y^n + \binom{n}{n}y^{n+1}.$$

Por conveniência, podemos escrever $\binom{n}{0} = \binom{n+1}{0}$ e $\binom{n}{n} = \binom{n+1}{n+1}$. Logo,

$$(x+y)^{n+1} = \binom{n+1}{0}x^{n+1} + \binom{n+1}{1}x^n y^1 + ... + \binom{n+1}{n}x^1y^n + \binom{n+1}{n+1}y^{n+1}.$$

Assim, a relação é válida para $n+1$ e, consequentemente, para todo n natural.

■

Quando $y = 1$, temos um caso especial do Teorema Binomial,

$$(1+x)^n = 1 + \binom{n}{1}x + \binom{n}{2}x^2 + ... + \binom{n}{n-1}x^{n-1} + x^n.$$

Além disso, podemos escrever o binômio utilizando a notação de somatório. Assim,

$$(x+y)^n = \sum_{i=0}^{n}\binom{n}{i}x^{n-i}y^i.$$

1.3 Função Piso

Nesta seção, abordaremos a função piso, a qual associa a um número real x o maior número inteiro menor ou igual a x, bem como algumas de suas propriedades e aplicações.

Definição 1.12. Dado $x \in \mathbb{R}$, definimos o *piso* ou *parte inteira* de x pelo número inteiro que satisfaz a desigualdade $x - 1 < \lfloor x \rfloor \leq x$ ou pela equivalente $\lfloor x \rfloor \leq x < \lfloor x \rfloor + 1$.

Exemplo 1.13. Temos $\sqrt{3} \approx 1,73$. Logo, $\lfloor \sqrt{3} \rfloor = 1$.

Exemplo 1.14. Note que $\frac{21}{5} = 4,2$. Então, $\left\lfloor \frac{21}{5} \right\rfloor = 4$.

Teorema 1.15. *Dado* $\lfloor x \rfloor$*, temos* $0 \leq \lfloor 2x \rfloor - 2\lfloor x \rfloor \leq 1$.

Demonstração. Pela definição de $\lfloor x \rfloor$ temos $x - 1 < \lfloor x \rfloor \leq x$. Consequentemente,

$$2x - 1 < \lfloor 2x \rfloor \leq 2x,$$

e

$$2x - 2 < 2\lfloor x \rfloor \leq 2x.$$

Multiplicando a segunda desigualdade por (-1) e somando à primeira, segue que

$$-1 < \lfloor 2x \rfloor - 2\lfloor x \rfloor < 2.$$

Entretanto, $\lfloor 2x \rfloor - 2\lfloor x \rfloor$ é um inteiro e os únicos inteiros no intervalo $(-1, 2)$ são 0 e 1. Logo, $0 \leq \lfloor 2x \rfloor - 2\lfloor x \rfloor \leq 1$. ■

Teorema 1.16. *Se* p *é um primo, então* $\sum_{j=1}^{\infty} \left\lfloor \frac{n}{p^j} \right\rfloor$ *é o exponente de* p *que aparece na decomposição em fatores primos de* $n!$*.*

Antes de demonstrar o teorema, vamos apresentar alguns exemplos a fim de auxiliar na compreensão do resultado.

Exemplo 1.17. Para $p = 7$ e $n = 3$, temos

$$\sum_{j=1}^{\infty} \left\lfloor \frac{3}{7^j} \right\rfloor = \left\lfloor \frac{3}{7} \right\rfloor + \left\lfloor \frac{3}{7^2} \right\rfloor + \left\lfloor \frac{3}{7^3} \right\rfloor + ... = 0.$$

Logo, o expoente de 7 na decomposição de 3! é igual a 0. É claro que 7 não aparece na decomposição de 3!, pois é maior que $3! = 6$.

Exemplo 1.18. Se $p = 3$ e $n = 30$, temos

$$\sum_{j=1}^{\infty} \left\lfloor \frac{30}{3^j} \right\rfloor = \left\lfloor \frac{30}{3} \right\rfloor + \left\lfloor \frac{30}{3^2} \right\rfloor + \left\lfloor \frac{30}{3^3} \right\rfloor + \left\lfloor \frac{30}{3^4} \right\rfloor + ... = 10 + 3 + 1 + 0 = 14.$$

Então 3^{14} aparece na decomposição do número 30! e, além disso, dos inteiros $\{1, 2, ..., 30\}$ segue que $p = 3$ divide $\left\lfloor \frac{30}{3} \right\rfloor = 10$, sendo eles $\{3, 6, 9, 12, 15, 18, 21, 24, 27, 30\}$; $p^2 = 9$ divide apenas $\{9, 18, 27\}$, isto é, $\left\lfloor \frac{30}{3^2} \right\rfloor = 3$ inteiros; enquanto apenas $\left\lfloor \frac{30}{3^3} \right\rfloor = 1$ é divisível por $p^3 = 27$, o próprio 27. Observe que a partir de $\left\lfloor \frac{30}{3^4} \right\rfloor$ todos os termos do somatório são nulos, pois $3^4 = 81$ e 81 é maior que 30.

Exemplo 1.19. Encontre a quantidade de zeros que aparece no número 200!.

Note que a quantidade de zeros presente em um número depende dos expoentes de 2 e 5 que aparecem em sua decomposição, pois $2 \cdot 5 = 10$. Observe ainda que em 200! há mais múltiplos de 2 que de 5, logo a quantidade de zeros está diretamente relacionada ao expoente de 5 presente na fatoração do número 200!. Daí,

$$\sum_{j=1}^{\infty} \left\lfloor \frac{200}{5^j} \right\rfloor = \left\lfloor \frac{200}{5} \right\rfloor + \left\lfloor \frac{200}{5^2} \right\rfloor + \left\lfloor \frac{200}{5^3} \right\rfloor + \left\lfloor \frac{200}{5^4} \right\rfloor + ... = 40 + 8 + 1 + 0 = 49.$$

Logo, há 49 zeros em 200!.

Pelos exemplos podemos observar que trata-se, na verdade, de uma soma finita, visto que eventualmente temos $p^j > n$ para $j \in [1, \infty)$. A seguir apresentamos a demonstração do teorema para quaisquer p primo e n natural.

Demonstração do Teorema 1.16. Note que se $p > n$, então p não aparece na decomposição em fatores primos de $n!$ e cada termo em $\sum_{j=1}^{\infty} \left\lfloor \frac{n}{p^j} \right\rfloor$ é zero, como desejamos. Se $p \leq n$, então $\left\lfloor \frac{n}{p} \right\rfloor$ inteiros em $\{1, 2, ..., n\}$ são divisíveis por p, isto é,

$$p, 2p, 3p, ..., \left\lfloor \frac{n}{p} \right\rfloor p.$$

Desses inteiros, $\left\lfloor \frac{n}{p^2} \right\rfloor$ também são divisíveis por p:

$$p^2, 2p^2, ..., \left\lfloor \frac{n}{p^2} \right\rfloor p^2.$$

Analogamente, $\left\lfloor \frac{n}{p^3} \right\rfloor$ desses inteiros são divisíveis por p uma terceira vez:

$$p^3, 2p^3, ..., \left\lfloor \frac{n}{p^3} \right\rfloor p^3.$$

Após finitas repetições desse argumento, podemos concluir que p divide números em $\{1, 2, ..., n\}$ exatamente $\sum_{j=1}^{\infty} \left\lfloor \frac{n}{p^j} \right\rfloor$ vezes. Assim, essa soma é o expoente de p que aparece na decomposição em fatores primos de $n!$. ■

1.4 Função Logarítmica

A seguir, abordamos a definição e algumas propriedades de logarítmo fundamentais para o estudo da função $f(x) = x/\log x$, realizado ao final desta seção.

Definição 1.20. Dados os números reais positivos x e b, com $b \neq 1$, definimos o logarítmo de x na base b como a potência em que b deve ser elevada para produzir x e escrevemos $\log_b x$. Quando utilizamos a base 10, basta escrever $\log x$.

Exemplo 1.21. O $\log_2 8 = 3$, pois $2^3 = 8$.

Exemplo 1.22. Temos que $\log 100 = 2$, pois $10^2 = 100$.

Proposição 1.23. *Algumas propriedades de logarítmo.*

1. $\log_b(x \cdot y) = \log_b x + \log_b y$.
2. $\log_b \left(\frac{x}{y}\right) = \log_b x - \log_b y$.
3. $\log_b x^p = p \cdot \log_b x$.

Demonstração. Considere $\log_b x = m$ e $\log_b y = n$. Pela definição de logarítmo, temos $x = b^m$ e $y = b^n$. Seja $p \in \mathbb{N}$, vamos começar provando que (3) é verdade elevando ambos os lados da equação $x = b^m$ a p. Assim, temos $x^p = (b^m)^p$. Logo, $\log_b x^p = m \cdot p$. Portanto, $\log_b x^p = p \cdot \log_b x$. Para provar (1), note que

$$\begin{aligned} \log_b(x \cdot y) &= \log_b(b^m \cdot b^n) \\ &= \log_b b^{m+n} \\ &= (m+n) \cdot \log_b b \\ &= (m+n) \\ &= \log_b x + \log_b y. \end{aligned}$$

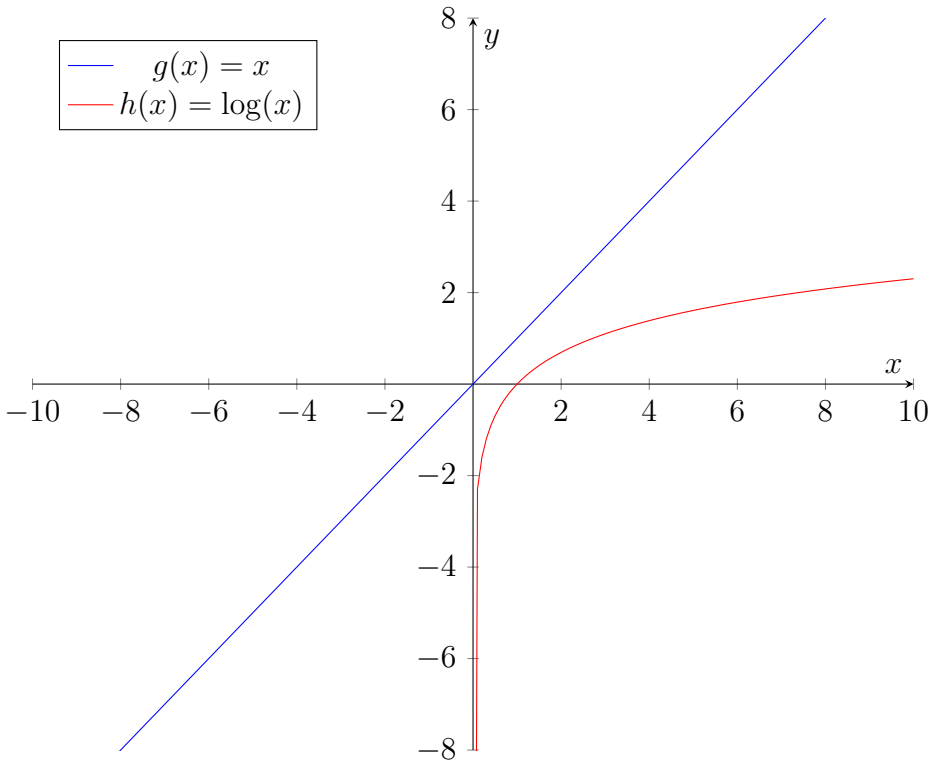
Por fim, vamos provar que (2) é verdadeira.

$$\begin{aligned} \log_b \left(\frac{x}{y}\right) &= \log_b \left(\frac{b^m}{b^n}\right) \\ &= \log_b b^{m-n} \\ &= (m-n) \cdot \log_b b \\ &= (m-n) \\ &= \log_b x - \log_b y. \end{aligned}$$

■

Para conseguir estabelecer o resultado de Chebyshev, precisamos analisar algumas propriedades elementares da função $x/\log x$. Antes disso, vamos observar o comportamento das funções $g(x) = x$ e $h(x) = \log(x)$ separadamente. Note que $g(x)$ está definida para todo $x \in \mathbb{R}$, enquanto o domínio de $h(x)$ está restrito a $x > 0$, conforme o gráfico a seguir.

Figura 1 – Gráfico das funções $g(x) = x$ e $h(x) = \log x$



Fonte: Produzido pela autora

Teorema 1.24. *Se* $f(x) = \dfrac{x}{\log x}$, *então:*

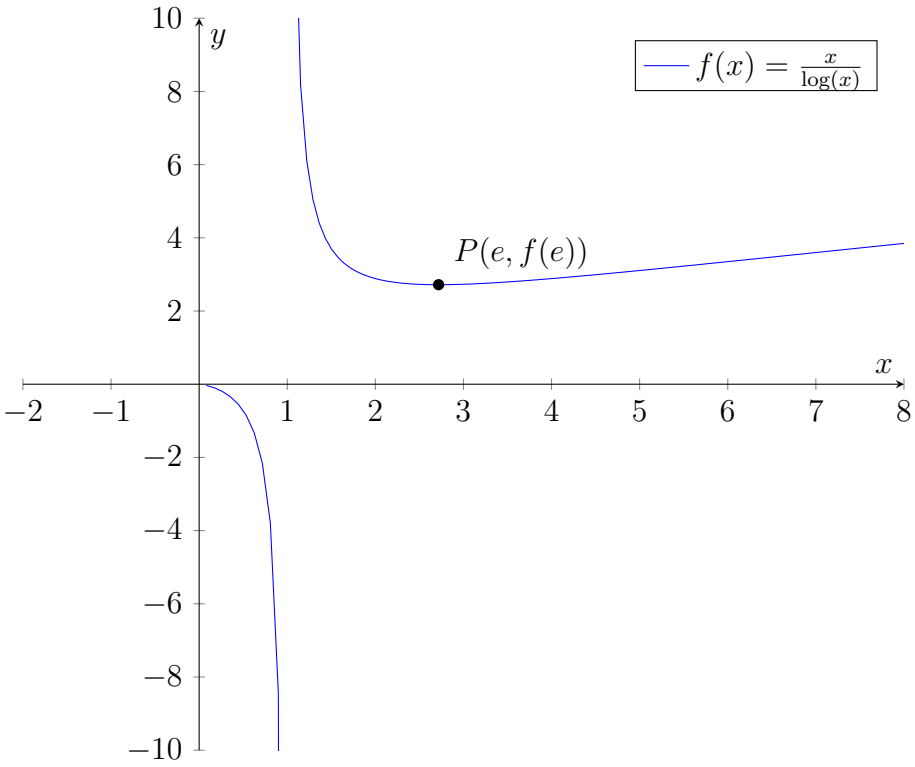
1. $f(x)$ *é crescente para* $x > e$;

2. $f(x-2) > \frac{f(x)}{2}$ *para* $x \geq 4$;

3. $f\left(\frac{x+2}{2}\right) < \frac{15f(x)}{16}$ *para todo* $x \geq 8$.

Antes de demonstrar o teorema, vamos analisar o gráfico de $f(x)$.

Figura 2 – Gráfico da função $f(x) = \frac{x}{\log x}$



Fonte: Produzido pela autora

A partir da análise gráfica, é fácil ver que a função é descrescente no intervalo $(0,1) \cup (1,e)$ e passa a ser crescente quando $x > e$, conforme demonstraremos a seguir.

Demonstração. (Teorema 1.24) Como

$$f'(x) = \frac{\log x - 1}{(\log x)^2},$$

podemos ver que $f'(x) > 0$ para $x > e$, o que prova (1). Para provar (2), note que se $x \geq 4$, então $x - 4 \geq 0$. Daí, $2x - 4 \geq x$, isto é, $x - 2 \geq x/2$. Assim,

$$f(x-2) = \frac{x-2}{\log(x-2)} \geq \frac{x}{2\log(x-2)} > \frac{x}{2\log x} = \frac{1}{2}f(x).$$

Para provar (3), observe que se $x \geq 8$, $x^3 \geq 8x^2$. Daí $(x/2)^3 \geq x^2$, isto é, $x/2 \geq x^{2/3}$. Além disso, $5x \geq 4x + 8$, logo $x + 2 \leq 5x/4$. Portanto,

$$f\left(\frac{x+2}{2}\right) = \frac{x+2}{2\log((x+2)/2)} < \frac{x+2}{2\log(x/2)} \leq \frac{x+2}{2\log x^{2/3}} \leq \frac{5x/4}{\frac{4\log x}{3}} = \frac{15}{16}f(x).$$

■

Lema 1.25. *Seja* $f(x) = \dfrac{x}{\log x}$, *para* $x \geq 5$ *temos* $f\left(2\left\lfloor \dfrac{x}{2} \right\rfloor\right) > f(x-2)$.

Demonstração. Pela definição de $\lfloor x \rfloor$, temos

$$\frac{x}{2} - 1 < \left\lfloor \frac{x}{2} \right\rfloor \leq \frac{x}{2},$$

isto é,

$$x - 2 < 2 \left\lfloor \frac{x}{2} \right\rfloor \leq x.$$

Como $f(x)$ é monótona e crescente para $x > e$, segue que $f\left(2 \left\lfloor \frac{x}{2} \right\rfloor\right) > f(x-2)$. ■

1.5 Função de Euler

Nesta seção, apresentaremos a função de Euler, que será utilizada para demonstrar as propriedades da função $\pi(x)$. Para isso, é necessário compreender o que são números relativamente primos.

Definição 1.26. Dois números inteiros a e b são considerados *relativamente primos*, *primos entre si* ou *coprimos* quando têm apenas o número 1 como maior divisor comum.

Exemplo 1.27. Note que os divisores naturais do número 5 são 1 e 5. Por outro lado, os divisores do número 12 são $1, 2, 3, 4, 6$ e 12. Logo, dizemos que 5 e 12 são primos entre si, pois o maior divisor comum entre eles é o número 1.

Definição 1.28. A *Função Totiente* ou *Função ϕ de Euler* associa a um número inteiro positivo n a quantidade de inteiros positivos menores que n que são relativamente primos com n. Denotaremos por $\phi(n)$.

Exemplo 1.29. Temos $\phi(10) = 4$, pois os números 1, 3, 7 e 9 são menores que 10 e relativamente primos com 10.

Após o estudo dessas importantes propriedades matemáticas, podemos dar início à análise da distribuição e organização dos primos para, enfim, provarmos o Teorema de Chebyshev.

2 Distribuição dos Números Primos

Neste capítulo, apresentaremos resultados elementares da matemática e a prova do Teorema de Chebyshev, utilizando o trabalho de (7) como referência.

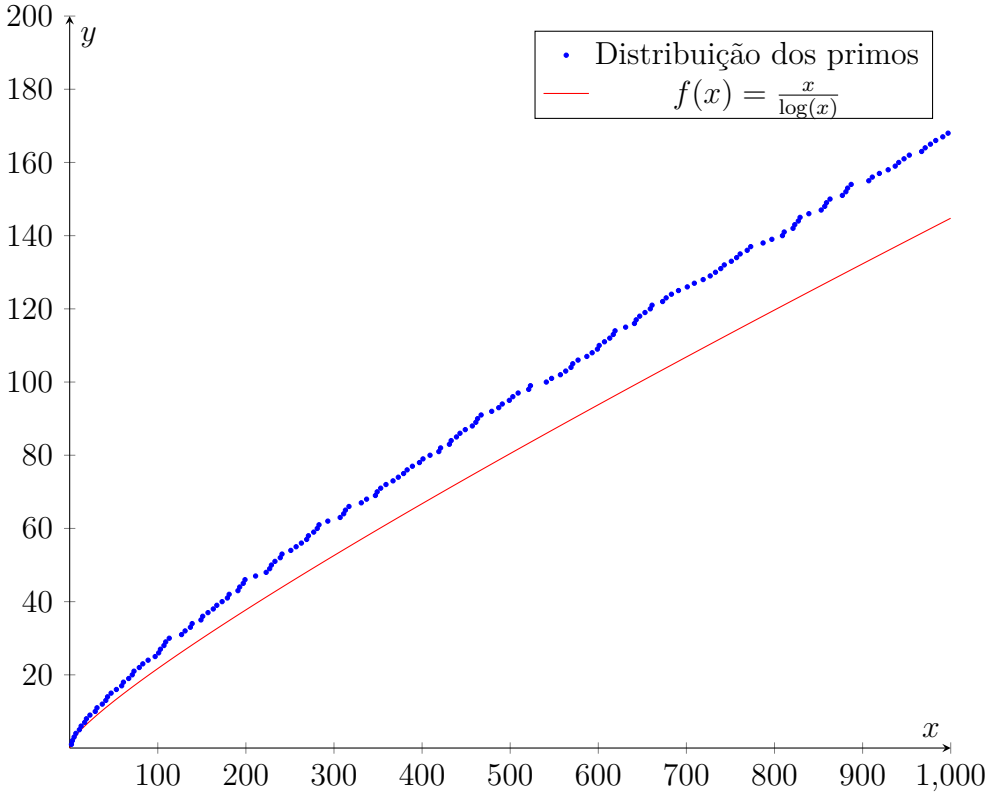
A sequência dos números primos sempre foi um tema fascinante para os matemáticos, sejam eles profissionais ou amadores. Compreender como os primos estão distribuídos entre os naturais é uma discussão que surgiu há muitos anos e ainda continua sendo objeto de interesse dos pesquisadores nos dias atuais.

Gauss foi o primeiro a dar atenção à função $\pi(x)$, o número de primos que não excede x. Ao observar que os valores de $\pi(x)$ eram dados aproximadamente por $\frac{x}{\log x}$, ele conjecturou que

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

Tal afirmação ficou conhecida como o Teorema do Número Primo e prevê como se comporta a distribuição dos primos.

Figura 3 – Comparação gráfica entre $f(x) = \frac{x}{\log x}$ e a distribuição dos primos até mil



Fonte: Produzido pela autora

A prova dessa conjectura se mostrou extremamente difícil e, apesar de muitos matemáticos tentarem, quase cem anos se passaram até conhecermos sua demonstração. A prova foi publicada em 1896, quando Hadamard e de la Vallée Poussin conseguiram demonstrar o resultado utilizando a função zeta de Riemann e outras técnicas sofisticadas da análise complexa (7).

Outras demonstrações desse teorema foram desenvolvidas ao longo dos anos, contudo ainda fazendo uso de técnicas complexas. Somente em 1949, Selberg e Erdös conseguiram demonstrar o teorema sem o uso das variáveis complexas, entretanto, essa prova é longa e de difícil compreensão, assim como todas as outras conhecidas até o momento.

Como tais demonstrações estão distantes do interesse deste trabalho, optamos por estudar a organização dos números primos por meio de um resultado semelhante, mas que pode ser provado utilizando apenas propriedades elementares da matemática: o Teorema de Chebyshev.

Chebyshev utilizou os coeficientes binomiais centrais para deduzir resultados acerca dos números primos e provou que existem constantes positivas c_1 e c_2 tais que

$$c_1 \frac{x}{\log x} < \pi(x) < c_2 \frac{x}{\log x},$$

para todo x$\geq$ 2.

Contudo, antes de demonstrar o Teorema de Chebyshev, precisamos analisar e compreender alguns resultados simples acerca de $\pi(x)$.

2.1 Propriedades Elementares de $\pi(x)$

A primeira propriedade trata da infinitude dos números primos. O famoso matemático grego Euclides provou que existem infinitos números primos utilizando a ideia de contradição, a qual apresentamos a seguir.

Teorema 2.1. $\lim_{x\to\infty} \pi(x) = +\infty$, *isto é, existem infinitos números primos.*

Demonstração. Suponha que existe um número finito de primos, p_1, p_2, ..., p_n. Considere M = $p_1 p_2 ... p_n + 1$. É fácil ver que se dividirmos M por qualquer um dos primos p_1, p_2, ..., p_n, o resto é 1. Assim, pela nossa hipótese de que há finitos números primos, deduzimos que M não possui decomposição em fatores primos. Como isso contradiz o Teorema Fundamental da Aritmética, a única conclusão possível é que há infinitos números primos. Logo, $\lim_{x\to\infty} \pi(x) = +\infty$.

■

Por outro lado, é fácil ver que $\pi(x) \leq x$. Os três teoremas a seguir mostram que $\pi(x)$ é, na verdade, muito menor que x.

Teorema 2.2. *Se k é um inteiro positivo qualquer,*

$$\frac{\pi(x)}{x} \leq \frac{\phi(k)}{k} + \frac{2k}{x}.$$

Demonstração. Seja $\lfloor x \rfloor = kl + r$, com $0 \leq r < k$ e $\lfloor x \rfloor$ indicando o maior inteiro que não excede x. Podemos dividir os inteiros do intervalo $[1, x]$ em l conjuntos de k inteiros consecutivos mais um conjunto com os r inteiros restantes $kl + 1, kl + 2, ..., kl + r$. Entre os inteiros $1, 2, ..., k$ há, no máximo, k primos. Entre os inteiros $k + 1, k + 2, ..., 2k$, há no máximo $\phi(k)$ primos, visto que qualquer inteiro não relativamente primo com k tem um fator primo de k que é menor ou igual a k. Analogamente, em cada conjunto de k inteiros consecutivos restante há no máximo $\phi(k)$ primos. Por fim, no conjunto de r inteiros restante, há no máximo r primos. Consequentemente,

$$\pi(x) \leq k + (l - 1)\phi(k) + r \leq 2k + \frac{x}{k}\phi(k).$$

Daí,

$$\frac{\pi(x)}{x} \leq \frac{\phi(k)}{k} + \frac{2k}{x}.$$

■

O próximo resultado permite estimar o tamanho de $\frac{\phi(x)}{k}$.

Teorema 2.3. *Se $M > 1$ e $p_1, p_2, ..., p_s$ são todos os primos em $\{1, 2, ..., M\}$, então*

$$\sum_{n=1}^{M} \frac{1}{n} < \frac{1}{\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)...\left(1 - \frac{1}{p_s}\right)}.$$

Demonstração. Da fórmula para a soma de uma série geométrica temos, para cada primo p,

$$\frac{1}{1 - \frac{1}{p}} = 1 + \frac{1}{p} + \frac{1}{p^2} + \frac{1}{p^3} + ...$$

Consequentemente,

$$\begin{aligned}\frac{1}{\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)...\left(1 - \frac{1}{p_s}\right)} &= \left(1 + \frac{1}{p_1} + \frac{1}{{p_1}^2} + \frac{1}{{p_1}^3} + ...\right) \\ &\cdot \left(1 + \frac{1}{p_2} + \frac{1}{{p_2}^2} + \frac{1}{{p_2}^3} + ...\right)...\left(1 + \frac{1}{p_s} + \frac{1}{{p_s}^2} + \frac{1}{{p_s}^3} + ...\right) \\ &= \sum_{n \in \Lambda} \frac{1}{n} > \sum_{n \leq M} \frac{1}{n},\end{aligned}$$

em que Λ é o conjunto de todos os inteiros nos quais o maior fator primo é M. É fácil ver que a última igualdade é verdadeira, visto que multiplicando essas séries temos todos os possíveis termos da forma $\frac{1}{{p_1}^{\alpha_1}{p_2}^{\alpha_2}...{p_s}^{\alpha_s}}$, com $p_i \leq M$.

■

Teorema 2.4. *A série infinita* $\sum_{i=1}^{\infty} \frac{1}{p_i} = \frac{1}{2} + \frac{1}{3} + \frac{1}{5} + \frac{1}{7} + \frac{1}{11} + ...$ *diverge.*

A prova deste teorema não será apresentada, pois depende de propriedades que não foram demonstradas neste trabalho; no entanto, pode ser encontrada em (8).

O próximo teorema mostra que $\pi(x)$ é muito menor que x, mas ainda precisamos de mais ferramentas antes de provar o resultado de Chebyshev, que explicitamente descreve o quão pequena é $\pi(x)$.

Teorema 2.5. $\lim_{x\to\infty} \frac{\pi(x)}{x} = 0.$

Demonstração. Como $\frac{\pi(x)}{x} \geq 0$ para todo $x > 0$, precisamos mostrar que podemos fazer $\frac{\pi(x)}{x}$ arbitrariamente pequeno escolhendo x suficientemente grande. O Teorema 2.2 estabeleceu que

$$\frac{\pi(x)}{x} \leq \frac{\phi(k)}{k} + \frac{2k}{x}$$

para cada inteiro positivo k. Seja M um inteiro grande e $k = p_1 p_2 ... p_s$, em que $\{p_1, p_2, ..., p_s\}$ é o conjunto de todos os primos que não excedem M. Daí

$$\begin{aligned}\frac{\phi(k)}{k} &= \frac{k\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)...\left(1-\frac{1}{p_s}\right)}{k} \\ &= \left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)...\left(1-\frac{1}{p_s}\right) < \left(\sum_{n=1}^{M}\frac{1}{n}\right)^{-1}.\end{aligned}$$

Assim,

$$\frac{\pi(x)}{x} \leq \left(\sum_{n=1}^{M}\frac{1}{n}\right)^{-1} + \frac{2p_1p_2...p_s}{x}. \tag{2.1.1}$$

Agora basta fazer $\frac{\pi(x)}{x}$ tão pequeno quanto desejarmos. Como $\sum_{n=1}^{\infty}\frac{1}{n}$ é uma série divergente (2.4), podemos escolher M grande de modo que $\sum_{n=1}^{M}\frac{1}{n} > \frac{2}{\epsilon}$, em que $\epsilon > 0$ é um número positivo arbitrário. Daí, para $x > \frac{4p_1p_2...p_s}{\epsilon}$, temos

$$\frac{2k}{x} < \frac{2p_1p_2...p_s}{\frac{4p_1p_2...p_s}{\epsilon}} = \frac{2p_1p_2...p_s\epsilon}{4p_1p_2...p_s} = \frac{\epsilon}{2}.$$

Logo,

$$\frac{\pi(x)}{x} < \frac{\epsilon}{2} + \frac{2p_1p_2...p_s\epsilon}{4p_1p_2...p_s} = \epsilon.$$

■

Para concluir nossa seção de propriedades elementares de $\pi(x)$, vamos apresentar dois resultados adicionais para provar o Teorema de Chebyshev.

Lema 2.6. *Dado $x \geq 5$, temos $\pi(x) \geq \pi\left(2\left\lfloor \frac{x}{2} \right\rfloor\right)$.*

Demonstração. Na demonstração do Lema (1.25), mostramos que

$$x - 2 < 2\left\lfloor \frac{x}{2} \right\rfloor \leq x.$$

Como $x \geq 2\left\lfloor \frac{x}{2} \right\rfloor$ e $\pi(x)$ é monótona, segue o resultado.

■

Lema 2.7. *Para $x \geq 8$, temos*

$$\pi(x+1) \leq \pi\left(2\left\lfloor \frac{x+2}{2} \right\rfloor\right).$$

Demonstração. Pela definição de $\lfloor x \rfloor$, para x par, temos $2\left\lfloor \frac{x+2}{2} \right\rfloor = 2\left(\frac{x+2}{2}\right) = x+2$. Quando x é ímpar, temos $2\left\lfloor \frac{x+2}{2} \right\rfloor = 2\left(\frac{x+1}{2}\right) = x+1$. Daí, segue que $x+1 \leq 2\left\lfloor \frac{x+2}{2} \right\rfloor$ e, como $\pi(x)$ é monótona, segue o resultado.

■

2.2 Teorema de Chebyshev

Após o estudo das propriedades da função $\pi(x)$, estamos prontos para provar o Teorema de Chebyshev. Vale ressaltar que a demonstração apresentada a seguir é realizada utilizando apenas as propriedades matemáticas elementares já apresentadas neste trabalho.

Além disso, quanto mais próximas de 1 forem as constantes c_1 e c_2, mais técnica fica a demonstração. Assim, iremos mostrar que $c_1 = \frac{\log 2}{4}$ e $c_2 = 30(\log 2)$ funcionam.

Teorema 2.8 (Chebyshev)**.** *Para $x \geq 8$,*

$$\frac{\log 2}{4} \cdot \frac{x}{\log x} < \pi(x) < 30(\log 2)\frac{x}{\log x}.$$

Demonstração. Vamos começar provando a desigualdade do lado esquerdo. Observe o coeficiente binomial $\binom{2n}{n}$, isto é, o número de combinações de $2n$ objetos distintos tomados n a n. Pela definição 1.8, temos

$$\binom{2n}{n} = \frac{(2n!)}{(n!)(n!)} = \frac{2n(2n-1)...(n+1)}{n(n-1)...1}.$$

Agora, cada primo p no intervalo $(n, 2n]$ deve aparecer como fator do numerador de $\binom{2n}{n}$. Uma vez que não pode aparecer no denominador (porque é maior que n), podemos ver

que $p \mid \binom{2n}{n}$. Daí, multiplicando todos esses primos temos

$$P_n \mid \binom{2n}{n},$$

em que P_n denota o produto de todos os primos maiores que n que não excedem $2n$. Assim, como cada primo que aparece como fator de P_n é maior que n e como existem $\pi(2n) - \pi(n)$ fatores primos de P_n, podemos ver que

$$n^{\pi(2n)-\pi(n)} < P_n < \binom{2n}{n}. \tag{2.2.1}$$

Por outro lado, suponha que correspondente a cada primo p definimos r_p pelas desigualdades $p^{r_p} \leq 2n < p^{r_p+1}$. Usando o Toerema 1.16 para determinar a potência de p que aparece na decomposição em fatores primos de $\binom{2n}{n}$, vemos que o expoente correto é a potência de p que aparece em $(2n)!$ menos a potência de p que aparece em $(n!)(n!)$; em outras palavras, o expoente é $\sum_{j=1}^{r_p} \left(\left\lfloor \frac{2n}{p^j} \right\rfloor - 2 \left\lfloor \frac{n}{p^j} \right\rfloor \right)$. Pelo Teorema 1.15,

$$0 \leq \sum_{j=1}^{r_p} \left(\left\lfloor \frac{2n}{p^j} \right\rfloor - 2 \left\lfloor \frac{n}{p^j} \right\rfloor \right) \leq \sum_{j=1}^{r_p} 1 = r_p.$$

Daí, vemos que

$$\binom{2n}{n} \mid Q_n,$$

em que Q_n denota o produto de todos os p^{r_p}. Como cada p^{r_p} não excede $2n$ e Q_n tem $\pi(2n)$ fatores da forma p^{r_p},

$$\binom{2n}{n} \leq Q_n \leq (2n)^{\pi(2n)}. \tag{2.2.2}$$

Assim que determinarmos o tamanho de $\binom{2n}{n}$, nós podemos ver que o Teorema de Chebyshev pode ser deduzido de (2.2.1) e (2.2.2). Por outro lado, pela definição 1.8,

$$\begin{aligned}
\binom{2n}{n} &= \frac{2n}{n} \frac{(2n-1)(2n-2)}{(n-1)(n-2)} \cdots \frac{(n+1)}{1} \\
&= 2 \cdot \frac{2(2n-1)(n-1)}{(n-1)} \cdot \frac{2(2n-3)(n-2)}{(n-2)} \cdot \ldots \cdot \frac{(n+1)}{1} \\
&\geq 2 \cdot 2 \cdot 2 \cdot \ldots \cdot 2 = 2^n.
\end{aligned} \tag{2.2.3}$$

Combinando (2.2.2) e (2.2.3) temos

$$2^n \leq \binom{2n}{n} \leq (2n)^{\pi(2n)},$$

isto é,

$$2^n \leq (2n)^{\pi(2n)}. \tag{2.2.4}$$

Aplicando logaritmo de ambos os lados de (2.2.4), obtemos a desigualdade

$$\log 2^n \leq \log(2n)^{\pi(2n)},$$

logo,

$$n \log 2 \leq \pi(2n) \log 2n,$$

ou ainda,

$$\pi(2n) \geq \frac{n \cdot \log 2}{\log 2n}. \tag{2.2.5}$$

Daí, se $x \geq 5$ e $f(x) = x/\log x$, por (2.2.5), (1) e (2), segue que

$$\begin{aligned}\pi(x) &\geq \pi\left(2\left\lfloor \frac{x}{2} \right\rfloor\right) \geq \frac{\left\lfloor \frac{x}{2} \right\rfloor \log 2}{\log 2\left\lfloor \frac{x}{2} \right\rfloor} = \frac{\log 2}{2} \cdot \frac{2\left\lfloor \frac{x}{2} \right\rfloor}{\log 2\left\lfloor \frac{x}{2} \right\rfloor} \\ &= \frac{\log 2}{2} f\left(2\left\lfloor \frac{x}{2} \right\rfloor\right) > \frac{\log 2}{2} f(x-2) > \frac{\log 2}{2} \cdot \frac{1}{2} f(x) \\ &= \frac{\log 2}{4} \cdot \frac{x}{\log x},\end{aligned}$$

o que conclui a desigualdade do lado esquerdo do teorema 2.8. Pelo Teorema Binomial (1.11),

$$(1+x)^{2n} = 1 + \binom{2n}{1}x + \binom{2n}{2}x^2 + \ldots + \binom{2n}{n}x^n + \ldots + x^{2n}.$$

Por isso, com x = 1, encontramos

$$2^{2n} = 1 + \binom{2n}{1} + \binom{2n}{2} + \ldots + \binom{2n}{n} + \ldots + 1 > \binom{2n}{n}. \tag{2.2.6}$$

Para mostrar que $\pi(x) < 30 \cdot \log 2 \cdot \dfrac{x}{\log x}$, combinamos (2.2.1) e (2.2.6). Assim,

$$n^{\pi(2n)-\pi(n)} < \binom{2n}{n} < 2^{2n},$$

ou seja,

$$n^{\pi(2n)-\pi(n)} < 2^{2n}. \tag{2.2.7}$$

Aplicando logaritmo de ambos os lados de (2.2.7), encontramos que

$$\begin{aligned}[\pi(2n) - \pi(n)] \log n &< 2n \cdot \log 2 \\ \pi(2n) - \pi(n) &< \frac{n}{\log n} \cdot 2 \log 2.\end{aligned}$$

Portanto,

$$\pi(2n) < (2 \log 2)\frac{n}{\log n} + \pi(n). \tag{2.2.8}$$

Agora, por indução matemática, vamos mostrar que

$$\pi(2n) < 32(\log 2)\frac{n}{\log n}, \text{para n} > 1. \tag{2.2.9}$$

Inicialmente, note que (2.2.9) é verdade para $2 \leq n \leq 8$:

$$\begin{aligned}\pi(4) = 2 < \pi(6) = 3 < \pi(8) = \pi(10) = 4 \\ < \pi(12) = 5 < \pi(14) = \pi(16) = 6 < 64 \\ = 32 \cdot 2 = 32(\log 2)\frac{2}{\log 2}.\end{aligned}$$

Agora suponha (2.2.9) verdade para todos os inteiros $n \leq k$, com $k \geq 8$. Daí, para $k+1$, segue por (2.2.8) com $f(x) = x/\log x$ que

$$\begin{aligned}\pi(2k+2) &< 2(\log 2)f(k+1) + \pi(k+1) \\ &\leq 2(\log 2)f(k+1) + \pi\left(2\left\lfloor\frac{k+2}{2}\right\rfloor\right) \\ &< 2(\log 2)f(k+1) + 32(\log 2)f\left(\left\lfloor\frac{k+2}{2}\right\rfloor\right) \\ &\leq 2(\log 2)f(k+1) + 32(\log 2)f\left(\frac{k+2}{2}\right) \\ &< 2(\log 2)f(k+1) + 32(\log 2)\frac{15}{16}f(k+1) \text{ (por 3)} \\ &= 32(\log 2)f(k+1) \\ &= 32(\log 2)\frac{k+1}{\log(k+1)}.\end{aligned}$$

Assim, por indução matemática, temos

$$\pi(2n) < 32(\log 2)\frac{n}{\log n} \text{ para todo } n > 1.$$

Daí, para todo número real $x \geq 8$,

$$\begin{aligned}\pi(x) < \pi\left(2\left\lfloor\frac{x}{2}\right\rfloor + 2\right) &< 32(\log 2)f\left(\left\lfloor\frac{x}{2}\right\rfloor + 1\right) \\ &\leq 32(\log 2)f\left(\frac{x+2}{2}\right) \\ &< 32(\log 2)\frac{15}{16}f(x) \text{ (por 3)} \\ &= 30(\log 2)f(x) \\ &= 30(\log 2)\frac{x}{\log x},\end{aligned}$$

o que conclui a prova do Teorema de Chebyshev.

■

Exemplo 2.9. Sabemos que $\pi(10) = 4$, pois apenas 2, 3, 5 e 7 são primos e menores que 10. Pelo Teorema de Chebyshev, quando $x = 10$ temos

$$\frac{\log 2}{4} \cdot \frac{10}{\log 10} \approx 0,75.$$

O que nos diz que há pelo menos 1 primo que não excede o valor de 10. Já pela estimativa do lado direito, há no máximo 90 primos, pois

$$30(\log 2)\frac{10}{\log 10} \approx 90,31.$$

Logo, $\pi(10) \in [1, 90]$.

Exemplo 2.10. Vamos utilizar o Teorema de Chebyshev para analisar o valor de $\pi(1000)$. Para $x = 1000$, temos

$$\frac{\log 2}{4} \cdot \frac{1000}{\log 1000} \approx 25,08.$$

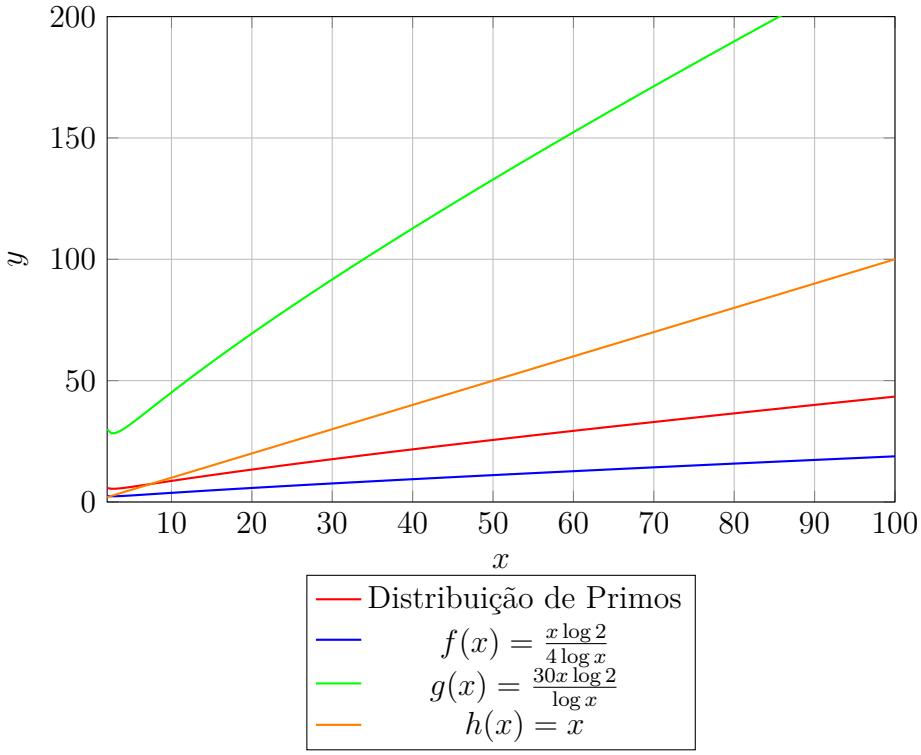
Isto significa que existem pelo menos 26 primos menores que 1000. Enquanto,

$$30(\log 2)\frac{1000}{\log 1000} \approx 3010,3.$$

O resultado de Chebyshev nos mostra que $26 \leq \pi(1000) \leq 3010$. De fato, conforme o gráfico (3), existem 168 números primos menores que 1000, isto é, $\pi(1000) = 168$.

É claro que o valor de $\pi(x)$ deve ser menor (ou igual) que x e por isso a estimativa inferior é o resultado mais interessante deste teorema, pois nos permite estipular o número mínimo de primos que não excedem determinado x, como podemos ver no gráfico a seguir.

Figura 4 – Representação gráfica do Teorema de Chebyshev



Fonte: Produzido pela autora

Podemos observar, por meio da representação gráfica do Teorema de Chebychev (2.8), que, de fato, a função $\pi(x)$ está situada entre as funções $f(x) = \dfrac{\log 2}{4} \cdot \dfrac{x}{\log x}$ e $g(x) = 30 \log 2 \cdot \dfrac{x}{\log x}$ e que se aproxima mais da estimativa inferior. Isso acontece pois $\dfrac{\log 2}{4} \approx 0,075$ está mais próximo de 1 que $30(\log 2) \approx 9,031$ e quanto mais próximo de 1 forem as constantes c_1 e c_2, mais próximas do valor de $\pi(x)$ serão as estimativas do teorema.

Além disso, notamos que a estimativa superior excede o valor de x no domínio apresentado. Entretanto, em determinado ponto, elas se cruzam e o valor de x passa a ser maior que $g(x)$. De fato, observe que, para encontrar o valor de x onde as funções $g(x)$ e $h(x)$ se encontram, basta igualar as duas funções. Assim,

$$x = \frac{30x \log 2}{\log x}.$$

Como estamos analisando as funções para $x > 0$, podemos simplificar ambos os lados da equação por x. Daí,

$$1 = \frac{30 \log 2}{\log x}.$$

Logo,

$$\log x = 30 \log 2.$$

Resolvendo o logaritmo, temos que as funções se cruzam em $x = 2^{30} = 1.073.741.824$. A partir desse ponto, a função $g(x)$ passa a ser menor que x, tornando a estimativa de Chebyshev interessante para números primos maiores que 2^{30}.

3 Primos Especiais e Curiosidades

Neste capítulo, vamos apresentar e explorar alguns resultados relacionados aos chamados primos especiais por suas características únicas, incluindo os primos de Mersenne, Sophie Germain e Fermat. Além disso, discutiremos alguns problemas não resolvidos envolvendo números primos, como a conjectura de Goldbach.

3.1 Os Primos de Mersenne

Marin Mersenne (1588 - 1648) foi um monge e matemático francês que contribuiu para o desenvolvimento de importantes resultados da teoria dos números, ficou conhecido por sua conjectura acerca dos números primos que seriam batizados em seu nome.

Definição 3.1. É considerado um número de Mersenne, e indicado por M_n, todo número da forma $2^n - 1$ com $n \in \mathbb{N}$. Se $2^n - 1$ é primo, então M_n é um Primo de Mersenne.

Em 1644, Mersenne publicou em seu livro *Cogita physico mathematics* (9) a seguinte conjectura: os números da forma $2^n - 1$ são primos para $n = 2$, 3, 5, 7, 13, 17, 19, 31, 67, 127, 257 e composto para os demais inteiros do intervalo $2 \leq n \leq 257$.

Teorema 3.2. *Seja $n \in \mathbb{N}$. Se $2^n - 1$ é um primo de Mersenne, então n é primo.*

Demonstração. Suponha que n não é primo. Logo, n é composto e pode ser escrito como o produto de dois inteiros positivos a e b. Desse modo, temos

$$\begin{aligned} 2^n - 1 &= 2^{a \cdot b} - 1 \\ &= (2^a)^b - 1 \\ &= (2^a - 1) \cdot [(2^a)^{b-1} + (2^a)^{b-2} + ... + (2^a)^1 + (2^a)^0] \\ &= (2^a - 1) \cdot [(2^a)^{b-1} + (2^a)^{b-2} + ... + (2^a)^1 + 1]. \end{aligned}$$

Analogamente,

$$\begin{aligned} 2^n - 1 &= 2^{a \cdot b} - 1 \\ &= (2^b)^a - 1 \\ &= (2^b - 1) \cdot [(2^b)^{a-1} + (2^b)^{a-2} + ... + (2^b)^1 + (2^b)^0] \\ &= (2^b - 1) \cdot [(2^b)^{a-1} + (2^b)^{a-2} + ... + (2^b)^1 + 1]. \end{aligned}$$

Assim, para n composto, temos que $2^n - 1$ também é composto.

■

Inicialmente, acreditava-se que $2^p - 1$ era primo se, e somente, p era primo. Entretanto, em 1563, o matemático Hudalricus Regius mostrou que para $n = 11$ temos que $2^{11} - 1 = 2047 = 23 \cdot 89$ não é primo.

Temos que se $2^n - 1$ é primo, então n é primo, mas n ser primo não é condição suficiente para que $2^n - 1$ também o seja, conforme o contraexemplo visto acima.

Mersenne não conseguiu provar sua teoria e, durante séculos, muitos matemáticos se dedicaram a estudar os números $2^n - 1$ e descobrir se eram primos ou compostos. Por quase dois séculos, o maior número primo de Mersenne conhecido era o $M_{19} = 2^{19} - 1 = 524.287$, encontrado pelo italiano Pietro Cataldi em 1603.

Quase três séculos se passaram até que os matemáticos conseguissem testar todos os números da conjectura de Mersenne. O mais impressionante é que ele tenha cometido apenas cinco erros em sua lista: a inclusão dos primos $n = 67, 257$, que geram números compostos; e a ausência de $n = 61, 89, 107$.

Para Tanner É. Lucas, Mersenne criou sua lista considerando como condição suficiente os primos até 257 que podiam ser escritos como $2^{2n} + 1$, $2^{2n} \pm 3$ ou $2^{2n+1} - 1$, com $n \in \mathbb{N}$ (9).

De fato, ao calcular os primos $2 < p < 258$ que podem ser escritos por uma das fórmulas acima, podemos observar que

- Para $p = 2^{2n} + 1$, temos $5, 17, 257$;
- Para $p = 2^{2n} - 3$, temos $13, 61$;
- Para $p = 2^{2n} + 3$, temos $7, 19, 67$;
- Para $p = 2^{2n+1} - 1$, temos $7, 31, 127$.

Colocando em ordem crescente, encontramos uma lista de primos quase idêntica à da conjectura,

$$5, 7, 13, 17, 19, 31, 61, 67, 127, 257.$$

Sendo a diferença o número 61, que não estava incluso na lista de Mersenne. Além disso, há um erro na limitação dos valores, visto que para $p = 3$ temos $2^3 - 1 = 7$ primo, porém 3 não pode ser escrito em nenhuma das formas acima.

Tanner provou que apesar de $p = 67$ ser primo, o número $2^{67} - 1$ é composto. Logo, p ser escrito em uma dessas formas não é condição suficiente para que $2^p - 1$ seja primo.

Os números $257, 1021$ e 8191 são outros exemplos de que essa condição não é suficiente. Além disso, o número $2^{89} - 1$ é primo, mas $p = 89$ não pode ser escrito em nenhuma das formas apresentadas.

Os primos de Mersenne são raros e ainda não se sabe se há infinitos ou não. Atualmente conhecemos apenas 51 deles e, desde 1997, todos os M_p encontrados foram por meio do GIMPS, que une esforços de amadores e profissionais. Outra curiosidade sobre os primos de Mersenne é sua relação com os números perfeitos.

Definição 3.3. Um número N é considerado um *número perfeito* se a soma de seus divisores naturais é igual a $2N$.

O menor número perfeito é o 6. Note que os divisores naturais de 6 são 1, 2, 3 e 6, logo $1 + 2 + 3 + 6 = 12 = 2 \cdot 6$.

O segundo número perfeito é o 28, cujos divisores positivos geram a soma $1 + 2 + 4 + 7 + 14 + 28 = 56 = 2 \cdot 28$.

Ao todo são conhecidos 51 números perfeitos e ainda não sabemos se há infinitos ou não. Isso mesmo, hoje conhecemos 51 primos de Mersenne e 51 números perfeitos. Coincidência? Não! Euclides provou que $2^{p-1}(2^p - 1)$ é um número perfeito sempre que $2^p - 1$ é primo. Assim, a busca por primos de Mersenne é também uma busca por números perfeitos.

Muito anos depois, o matemático Alhazen conjecturou que a volta também era verdadeira, isto é, sempre que $2^p - 1$ é primo temos que $2^{p-1}(2^p - 1)$ é um número par [1] perfeito. De fato, quando $p = 2$, temos $2^{2-1}(2^2 - 1) = 2 \cdot 3 = 6$. Para $p = 3$, temos $2^{3-1}(2^3 - 1) = 4 \cdot 7 = 28$.

Os próximos números perfeitos são 496, 8.128 e 33.550.336, encontrados quando p é igual a 5, 7 e 13, respectivamente. Entretanto, a prova dessa conjectura só foi feita séculos depois por Euler, no que ficou conhecido como o Teorema Euclides-Euler.

Teorema 3.4 (Teorema Euclides-Euler)**.** *O número $2^{p-1}(2^p - 1)$ é um número par perfeito se, e somente se, $2^p - 1$ é primo.*

Antes de demonstrar o teorema, precisamos conhecer algumas propriedades da função soma de divisores positivos de um número, representada por $\sigma(n)$. Para isso, utilizamos os trabalhos (10) e (11).

Proposição 3.5. *Algumas propriedades da função $\sigma(n)$.*

1. *Seja p um número primo, $\sigma(p) = p + 1$.*
2. *Para $k \in \mathbb{Z}$, temos $\sigma(p^k) = \dfrac{p^{k+1} - 1}{p - 1}$.*
3. *A função $\sigma(n)$ é uma função multiplicativa, pois, dados $m, n \in \mathbb{N}$ com $mdc(m, n) = 1$, temos $\sigma(m \cdot n) = \sigma(m) \cdot \sigma(n)$.*

[1] Até o momento nenhum número perfeito ímpar foi descoberto e sua existência permanece uma incógnita.

Demonstração. A propriedade (1) é consequência direta da definição de número primo: ter apenas dois divisores naturais, o 1 e ele mesmo. Para demonstrar (2), observe que os divisores de p^k são $1, p, p^2, p^3, ..., p^k$, isto é, trata-se de uma progressão geométrica de razão p. Logo,

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

Por fim, vamos provar a propriedade (3). Como $mdc(m, n) = 1$, temos que m e n são primos entre si, logo, não possuem divisores em comum. Assim, seja $a_1, a_2, ..., a_r$ os divisores de m e $b_1, b_2, ..., b_s$ os divisores de n, podemos escrever cada divisor de $m \cdot n$ de forma única como $a_i b_j$, com $1 \leq i \leq r$ e $1 \leq j \leq s$. Daí, cada termo de $\sigma(m \cdot n)$ aparece uma única vez na soma $\sigma(m) \cdot \sigma(n)$. Note que cada $a_i b_j$ é um divisor de $m \cdot n$, então a soma tem que ser igual. Logo,

$$\sigma(m \cdot n) = \sum_{i,j} a_i b_j = (a_1 + ... + a_r) \cdot (b_1 + ... + b_j) = \sigma(m) \cdot \sigma(n).$$

■

Agora estamos prontos para demonstrar o Teorema Euclides-Euler, fundamentado em (12).

Demonstração. (Teorema 3.4) Seja $2^p - 1$ um número primo, vamos mostrar que $N = 2^{p-1}(2^p - 1)$ é um número par perfeito. Pelas propriedades da função $\sigma(n)$ vistas acima, temos que $\sigma(2^{p-1}) = 2^p + 1 - 1 = 2^p$. Além disso, como $2^p - 1$ é primo, então $2^p - 1$ e 2^{p-1} são primos entre si. Calculando $\sigma(N)$, temos

$$\sigma(N) = (2^p - 1) \cdot \sigma(2^p - 1) = (2^p - 1) \cdot 2^p = 2 \cdot 2^{p-1}(2^p - 1) = 2N.$$

Assim, se $2^p - 1$ é primo, então $N = 2^{p-1}(2^p - 1)$ é um número par perfeito. Agora vamos assumir que N é um número par perfeito e mostrar que $2^p - 1$ é primo. Seja $N = 2^{p-1} \cdot m$ perfeito, com m ímpar. Como $2 \nmid m$, então 2^{p-1} e m são primos entre si. Logo,

$$\sigma(N) = \sigma(2^{p-1}) \cdot \sigma(m) = (2^p - 1) \cdot \sigma(m). \tag{3.1.1}$$

Por hipótese, N é perfeito, então

$$\sigma(N) = 2N = 2^p \cdot m. \tag{3.1.2}$$

De (3.1.1) e (3.1.2) temos $(2^p - 1) \cdot \sigma(m) = 2^p \cdot m$. Daí,

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

Observe que $\sigma(m)$ e m são números inteiros, então $d = m/(2^p - 1)$ também é inteiro. Portanto, $2^p - 1 \mid m$ e, consequentemente, $d \mid m$. Além disso, $\sigma(m) = m + m/(2^p - 1) = m + d$ é a soma de todos os divisores de m. Então, obrigatoriamente d é igual a 1 ou teríamos $\sigma(m) = m + d + 1$, o que seria uma contradição. Assim, $m = 2^p - 1$ e, como m tem apenas dois divisores naturais, segue que m é primo.

■

3.2 Os Primos de Sophie Germain

Sophie Germain (1776 - 1831) foi uma matemática autoditada francesa, que ficou conhecida por suas contribuições para a demonstração do Último Teorema de Fermat.

Definição 3.6. Dizemos que p é um primo de Sophie Germain se $2p+1$ também é primo, sendo este chamado de Primo Seguro.

Exemplo 3.7. O menor primo de Sophie Germain é o 2, pois $2 \cdot 2 + 1 = 5$ é primo.

A sequência dos primos de Sophie Germain é

$$2, 3, 5, 11, 23, 29, 41, 53, 83, 89, 113, 131, 173, 179, 191, 233, 239, 251, 281, 293, ...$$

E, assim como os primos de Mersenne, ainda não foi provado se há infinitos primos de Sophie Germain.

Definição 3.8. Uma Cadeia de Cunningham de primos de Sophie Germain é definida pela sequência $\{p,\ 2p+1,\ 2(2p+1)+1, ...\}$.

Exemplo 3.9. A sequência $\{2, 5, 11, 23\}$ é uma Cadeia de Cunningham de primos de Sophie Germain. Note que esta cadeia termina em 23, pois o próximo número seria $23 \cdot 2 + 1 = 47$, que não é um primo de Sophie Germain.

Em 1750, Euler anunciou um teorema relacionando os primos de Sophie Germain com os números compostos de Mersenne, que só foi provado 25 anos depois por Lagrange.

Teorema 3.10. *Se p é primo diferente de 3 e da forma $4k+3$ com $k \in \mathbb{Z}$, então $2p+1$ é primo se, e somente se, $2p+1$ divide $M_p = 2^p - 1$. Nesse caso, p é um primo de Sophie Germain.*

Exemplo 3.11. Observe que $p = 11 = 4 \cdot 2 + 3$. Além disso, temos $2p + 1 = 23$ e $M_{11} = 2048 - 1 = 2047 = 23 \cdot 89$. Logo, $2p + 1 \mid M_p$. Portanto, 23 é primo e 11 é um primo de Sophie Germain.

A demonstração deste teorema não será apresentada neste trabalho, pois requer uma compreensão sobre resíduos quadráticos e outros resultados da aritmética modular que ultrapassam o âmbito de nossa pesquisa. O leitor pode encontrar a demonstração em (13).

A relevância dos primos de Sophie Germain para a matemática está relacionada com o Último Teorema de Fermat, no qual o matemático afirma que $x^n + y^n = z^n$ não possui solução inteira para $n > 2$.

Enquanto Fermat provou para $n = 4$ e Euler fez uma prova não muito rigorosa para $n = 3$, Germain foi uma das primeiras pessoas a tentar provar o teorema de forma

geral e não apenas para valores pequenos (14). Para isso, ela dividiu o problema em dois casos:

- Caso 1: Dados x, y, z primos entre si e $p \nmid xyz$;
- Caso 2: Dados x, y, z primos entre si e $p \mid xyz$;

E então provou o primeiro caso para todos os primos $p \leq 197$. A prova detalhada desta demonstração pode ser encontrada em (15).

3.3 Os Primos de Fermat

Pierre de Fermat (1601 - 1665) foi um advogado e matemático francês que ficou conhecido por seus trabalhos na Teoria dos Números, em especial, pelo Pequeno Teorema de Fermat.

Teorema 3.12 (Pequeno Teorema de Fermat)**.** *Se p é primo e a é um inteiro coprimo com p, então $a^{p-1} \equiv 1 \pmod{p}$.*

Demonstração. Vamos mostrar, utilizando indução em a, que $a^p \equiv a \pmod{p}$, obtida multiplicando ambos os lados da congruência acima por a. Para $a = 1$, temos $1^p \equiv 1 \pmod{p}$, que é verdade para todo primo p, uma vez que $p \nmid 1$. Suponha que $a^p \equiv a \pmod{p}$ para algum $a \in \mathbb{Z}$. Vamos mostrar que $(a+1)^p \equiv a+1 \pmod{p}$. Para isso, precisamos expandir $(a+1)^p$ utilizando o Teorema Binomial (1.11):

$$(a+1)^p = a^p + \binom{p}{1}a^{p-1} + \binom{p}{2}a^{p-2} + ... + \binom{p}{p-1}a + 1.$$

Mas, p é primo, então $p \mid \binom{p}{k}$ para todo $0 < k < p$. Assim, $(a+1)^p \equiv a^p + 1 \pmod{p}$. O que conclui nossa prova por indução. Note que $p \nmid a$, logo o teorema pode ser obtido simplificando ambos os lados da congruência por a (9).

■

A seguir apresentaremos a definição e alguns resultados envolvendo os primos de Fermat.

Definição 3.13. Um número da forma $F_n = 2^{2^n} + 1$ com $n \geq 0$ é chamado de *número de Fermat*. Se F_n é primo, dizemos que se trata de um *Primo de Fermat*.

Os cinco primeiros números de Fermat são primos:

$$F_0 = 3, F_1 = 5, F_2 = 17, F_3 = 257 \text{ e } F_4 = 65537.$$

Fermat conjecturou que todos os números da forma $2^{2^n}+1$ são primos para $n \geq 0$. Entretanto, em 1732, Euler provou que a conjectura de Fermat é falsa mostrando que F_5 é um número composto divisível por 641, pois

$$F_5 = 2^{2^5}+1 = 4.294.967.297 = 641 \cdot 6.700.417.$$

Até maio de 2024, o maior primo de Fermat conhecido é o $F_4 = 65537$ e ainda não sabemos se há infinitos primos de Fermat. Enquanto o maior número composto de Fermat conhecido é o $F_{18.233.954}$, cujo fator primo $7 \cdot 2^{18.233.956}+1$ só foi encontrado em outubro de 2020.

Já foi provado que F_n é composto para todo $5 \leq n \leq 32$, porém, a fatoração completa dos números de Fermat só foi encontrada para $n \leq 11$.

Teorema 3.14. *Para $n > 0$, temos $F_n - 2 = F_0 \cdot F_1 \cdot \ldots \cdot F_{n-1}$.*

Demonstração. Vamos provar o teorema por indução. Note que $F_0 = 3$ e $F_1 = 5$. Como $F_1 - 2 = 5 - 2 = 3 = F_0$, o resultado é verdade para $n = 1$. Agora suponha que $F_n - 2 = F_0 \cdot F_1 \cdot \ldots \cdot F_{n-1}$ para algum $n > 0$. Vamos provar que é verdade para $n+1$. De fato, por hipótese, temos $F_0 \cdot F_1 \cdot \ldots \cdot F_{n-1} \cdot F_n = (F_n - 2) \cdot F_n$. Daí,

$$\begin{aligned}(F_n - 2) \cdot F_n &= (2^{2^n} + 1 - 2) \cdot (2^{2^n} + 1) \\ &= (2^{2^n} - 1) \cdot (2^{2^n} + 1) \\ &= 2^{2 \cdot 2^n} - 1 \\ &= 2^{2^{n+1}} - 1 \\ &= 2^{2^{n+1}} + 1 - 2 \\ &= F_{n+1} - 2.\end{aligned}$$

Logo, o resultado também é verdade para $n+1$, o que conclui a prova do teorema.

■

Teorema 3.15. *Se $m \neq n$, então $(F_m, F_n) = 1$.*

Demonstração. Suponha, sem perda de generalidade, que $m < n$. Suponha ainda que existe um número primo p tal que $p \mid F_m$ e $p \mid F_n$. Observe que F_m é um dos fatores do produto $F_0 \cdot F_1 \cdot \ldots \cdot F_{n-1}$, pois $m < n$. Portanto, $p \mid F_0 \cdot F_1 \cdot \ldots \cdot F_{n-1}$. Pelo Teorema 3.14, temos

$$2 = F_n - F_0 \cdot F_1 \cdot \ldots \cdot F_{n-1}.$$

Como $p \mid F_n$ e $p \mid F_0 \cdot F_1 \cdot \ldots \cdot F_{n-1}$, então $p \mid 2$. Mas, isto é um absurdo, pois todo F_n é um número ímpar. Assim, não existe primo que divide F_m e F_n ao mesmo tempo. Logo, $(F_m, F_n) = 1$.

■

3.4 Alguns Problemas Não Resolvidos Sobre Primos

Apesar de ser um tema abordado desde a educação básica, ainda existem problemas elementares sobre os números primos que até hoje não foram provados. Apresentaremos a seguir dois desses problemas que, apesar da dificuldade em prová-los, podem ser facilmente compreendidos por estudantes do ensino médio e abordados nas salas de aula.

Um dos problemas mais antigos e sem solução da teoria dos números é a conjectura de Goldbach: *todo número par maior que dois é a soma de 2 primos*. Apesar de ser facilmente compreendida e verificada para números pequenos, como $4 = 2 + 2$, $6 = 3 + 3$, $8 = 3 + 5$, $10 = 3 + 7 = 5 + 5$,..., não é uma combinação trivial de ser encontrada quando observamos números muito grandes. Na verdade, para números maiores é possível fazer mais de uma combinação de primos; por exemplo,

$$118 = 5 + 113 = 11 + 107 = 17 + 101 = 29 + 89 = 47 + 71 = 59 + 59.$$

Goldbach não conseguiu provar sua afirmação para todos os números pares. Por meio de uma carta em 1742, pediu ajuda de Euler para demonstrar o resultado, mas este também não obteve sucesso (7). Quase 300 anos depois de ser proposto, esse problema continua sem solução, mas já houve avanços que podem contribuir para a demonstração do resultado. O matemático russo I. M. Vinogradov provou que todos os grandes inteiros ímpares são a soma de três primos utilizando a teoria das variáveis complexas; já Nils Pipping provou que a afirmação Goldbach é verdadeira para todos os pares até 100.000; mas se é verdade para *todo* par maior que 2 ainda não sabemos.

Outro não resolvido é o famoso Problema dos Primos Gêmeos. No século XIX, o matemático alemão Paul Stäckel chamou de primos gêmeos um par de primos p tal que $p + 2$ também é primo. Mais uma vez, é fácil ver que existem vários pares quando analisamos números pequenos; por exemplo, 3 e 5, 5 e 7, 11 e 13, 17 e 19, 29 e 31 e assim por diante.

Mas será que existem *infinitos* primos gêmeos? Para Euclides, a resposta é *sim*! Responsável pela elegante prova de que há infinitos números primos apresentada no início do capítulo, a Euclides também é atribuída a infinitude dos primos gêmeos. Porém, até os dias atuais, nenhum matemático conseguiu provar essa afirmação.

Alguns outros problemas sobre primos, como a hipótese de Riemann, requer uma base de conhecimentos matemáticos considerável até mesmo para a compreensão das afirmações, o que está além do objetitvo deste trabalho e por isso não serão abordados.

4 Competições Matemáticas e Os Números Primos

Neste capítulo, apresentaremos alguns problemas sobre números primos presentes em competições matemáticas, com o intuito de auxiliar professores e estudantes que estão se preparando para as próximas edições.

Delimitamos nossa pesquisa nas Olimpíada Brasileira de Matemática (OBM), Internacional Mathematical Olympiad (IMO), Olimpíada Pernambucana de Matemática (OPEMAT), Olimpíada Íbero-americana de Matemática (OIM) e na American Invitational Mathematics Examination (AIME), que, apesar de não ser uma olimpíada, é uma competição voltada para estudantes do ensino médio que estão se preparando para representar seu país nas competições internacionais.

Realizamos a busca pela palavra *primo* (ou *prime* nas provas em inglês) nas edições anteriores das competições e mostraremos a seguir alguns desses problemas e suas respectivas soluções. Ao final do capítulo, preparamos uma seção com problemas para que o leitor possa praticar.

4.1 Olimpíada Brasileira de Matemática (OBM)

A OBM é uma competição voltada para estudantes brasileiros de instituições públicas e privadas (16), sendo dividida em três níveis: anos finais do ensino fundamental (níveis 1 e 2), ensino médio (nível 3) e universitário (OBMU).

Esta olimpíada, que teve sua primeira edição em 1979, tem como objetivos a melhoraria no ensino da matemática no Brasil por meio do estímulo a professores e estudantes pela participação em competições, descobrir jovens com habilidades matemáticas e propiciar a oportunidade de seguir carreira de pesquisador em instituições de pesquisa de alto nível, além de selecionar os representantes brasileiros nas olimpíadas internacionais.

Limitamos nossa busca às edições das provas de nível 3 e universitário e selecionamos dois problemas para apresentar nesta seção.

Exercício 4.1. (OBM 2014 - Nível 3 - 1ª Fase - Q. 1) Para descobrir a quantidade de divisores positivos de um número inteiro positivo n, basta tomar sua fatoração em primos e calcular o produto dos expoentes dos primos adicionados de 1. Por exemplo, $2800 = 2^4 \cdot 5^2 \cdot 7$ possui $(4+1)(2+1)(1+1) = 30$ divisores positivos. Qual é o menor inteiro positivo com 2014 divisores positivos?

Solução. Realizando a fatoração em números primos, temos $2014 = 2 \cdot 19 \cdot 53$. Logo, o menor inteiro que estamos procurando possui, no máximo, três fatores primos. Como buscamos o menor inteiro positivo, os três possíveis fatores devem ser os três menores primos, isto é, $2, 3$ e 5. Observe que a quantidade de divisores é calculada a partir do produto dos expoentes dos primos acrescidos de 1, logo:

- Se o número possuir apenas um fator primo, o expoente será igual a 2013, pois $2013 + 1 = 2014$;
- Se o número possuir dois fatores primos, as possíveis combinações dos expoentes são: 1 e 1006, 37 e 52 ou 105 e 18;
- Se o número possuir três fatores primos, os expoentes serão iguais a 1, 18 e 52.

Para obter o menor número, note que os menores primos devem ter os maiores expoentes. Portanto, as possíveis soluções são: 2^{2013}, $2^{1006} \cdot 3$, $2^{52} \cdot 3^{37}$, $2^{105} \cdot 3^{18}$ e $2^{52} \cdot 3^{18} \cdot 5$. Sendo o menor número inteiro positivo o $2^{52} \cdot 3^{18} \cdot 5$.

■

Exercício 4.2. (OBMU 2018 - 1ª Fase - Q. 23) Para quantos números primos p o número $p^3 - 4p + 9$ é um quadrado perfeito?

Solução. O número $p^3 - 4p + 9$ é um quadrado perfeito quando podemos escrever $p^3 - 4p + 9 = a^2$, com $a \in \mathbb{N}$. Note que $p^3 - 4p + 9 \equiv 9 \pmod{p}$, logo $a^2 \equiv 9 \pmod{p}$. Daí, $a \equiv 3 \pmod{p}$ ou $a \equiv -3 \pmod{p}$. Logo, $a = n \cdot p \pm 3$, com $n \in \mathbb{Z}$. Assim,

$$\begin{aligned} a^2 &= n^2p^2 \pm 6np + 9 \\ p^3 - 4p + 9 &= n^2p^2 \pm 6np + 9 \\ p^3 - 4p &= n^2p^2 \pm 6np \\ p \cdot (p^2 - 4) &= p \cdot (n^2p \pm 6n) \\ p^2 - 4 &= n^2p \pm 6n \\ p^2 - n^2p &= \pm 6n + 4 \\ p \cdot (p - n^2) &= 2 \cdot (\pm 3n + 2) \end{aligned}$$

Portanto, $p \mid 2$ ou $p \mid (\pm 3n + 2)$. Se $p \mid 2$ e é primo, então $p = 2$. Como $2^3 - 4 \cdot 2 + 9 = 9 = 3^2$, segue que $p = 2$ é uma das soluções do problema. Suponha, então, que $p \nmid 2$, logo $p \mid (\pm 3n + 2)$. Daí, $p \leq 3n + 2$, isto é,

$$\begin{aligned} \frac{p-2}{3} &\leq n \\ \left(\frac{p-2}{3}\right) \cdot p &\leq np \\ \frac{p^2 - 2p}{3} &\leq np. \end{aligned} \tag{4.1.1}$$

Como $a = n \cdot p \pm 3$, então $a \geq np - 3$. Assim, $np \leq a + 3$ e, de (4.1.1), segue que

$$\begin{aligned}
\frac{p^2 - 2p}{3} &\leq a + 3 \\
\frac{p^2 - 2p}{3} - 3 &\leq a \\
\frac{(p^2 - 2p - 9)^2}{9} &\leq a^2 \\
\frac{p^4 - 4p^3 - 14p^2 + 36p + 81}{9} &\leq p^3 - 4p + 9 \\
p^4 - 4p^3 - 14p^2 + 36p + 81 &\leq 9p^3 - 36p + 81 \\
p^4 - 13p^3 - 14p^2 + 72p &\leq 0 \\
p \cdot (p^3 - 13p^2 - 14p + 72) &\leq 0.
\end{aligned}$$

Como vimos anteriormente, $p = 2$ é uma solução, então $(p - 2)$ é fator do polinômio encontrado. Logo, podemos reescrevê-lo da seguinte maneira:

$$p \cdot (p - 2) \cdot (p^2 - 11p - 36) \leq 0.$$

Vamos analisar para quais valores de p o fator $(p^2 - 11p - 36)$ é nulo. Observe que $\Delta = (-11)^2 - 4 \cdot 1 \cdot (-36) = 265$. Portanto,

$$p = \frac{11 \pm \sqrt{265}}{2}.$$

Assim,

$$\frac{11 - \sqrt{265}}{2} \leq p \leq \frac{11 + \sqrt{265}}{2}.$$

Como $\sqrt{265} \approx 16,28$, temos $-2,64 \leq p \leq 13,64$ e os únicos primos desse intervalo são $2, 3, 5, 7$ e 11. Já provamos que 2 é solução, então basta analisarmos para quais desses primos ímpares o número $p^3 - 4p + 9$ é um quadrado perfeito.

- Para $p = 3$, temos $3^3 - 4 \cdot 3 + 9 = 24$;
- Para $p = 5$, temos $5^3 - 4 \cdot 5 + 9 = 114$;
- Para $p = 7$, temos $7^3 - 4 \cdot 7 + 9 = 324 = 18^2$;
- Para $p = 11$, temos $11^3 - 4 \cdot 11 + 9 = 1296 = 36^2$.

Portanto, o número $p^3 - 4p + 9$ é um quadrado perfeito apenas para três números primos: $2, 7$ e 11.

■

4.2 Internacional Mathematical Olympiad (IMO)

A Olimpíada Internacional de Matemática (IMO) é uma competição mundial para estudantes do ensino médio que acontece anualmente desde 1959 (17). Nesta seção, vamos resolver um problema envolvendo a distribuição dos números primos presente na edição de 1989 da IMO.

Exercício 4.3. (IMO 1989 - Q. 5) Prove que para todo n natural podemos encontrar um conjunto de n inteiros consecutivos tal que nenhum deles é uma potência de um número primo.

Solução. Para solucionar este problema, note que o conjunto

$$\{(n+1)!+2, (n+1)!+3, ..., (n+1)!+n+1\}$$

para $n \geq 1$, é um conjunto com n inteiros consecutivos tal que nenhum elemento é primo (18). Como estamos buscando um conjunto de números que possuem dois divisores, observe que na decomposição de $(2n)! = 2n \cdot (2n-1) \cdot (2n-2) \cdot ... \cdot 2 \cdot 1$ encontramos dois fatores de qualquer número k para $2 \leq k \leq n$. Desse modo, analisando $(2n-2)!+k$, podemos mostrar que este número é divisível por k, mas ao fatorá-lo encontramos um termo que deixa resto 1 ao ser dividido por k. Assim, o conjunto

$$\{(2n+2)!+2, (2n+2)!+3, ..., (2n+2)!+n+1\}$$

satisfaz o problema. Observe que

$$(2n+2)!+2 = 2\left[\frac{(2n+2)!+2}{2}+1\right].$$

Como $n \geq 1$, note que $(2n+2)!+2$ possui, pelo menos, dois fatores pares, assim,

$$\frac{(2n+2)!+2}{2} = \frac{(2n+2)\cdot(2n+1)\cdot ... \cdot 2 \cdot 1}{2} \equiv 0 \pmod 2.$$

Daí, $\dfrac{(2n+2)!+2}{2}+1 \equiv 1 \pmod 2$. Portanto, $(2n+2)!+2$ não pode ser potência de um número primo, pois possui um fator par e outro ímpar. Agora, note que

$$(2n+2)!+k = k\left[\frac{(2n+2)!+2}{k}+1\right].$$

Como $2 \leq k \leq n+1$, devemos ter $(2n+2)! \equiv 0 \pmod{k^2}$ ou $\dfrac{(2n+2)!}{k} \equiv 0 \pmod k$. Logo, $\dfrac{(2n+2)!}{k}+1 \equiv 1 \pmod k$. Entretanto, como $(2n+2)!+k$ é divisível por k, este deve ser uma potência perfeita de k. Mas, como $\dfrac{(2n+2)!}{k}+1$ não é uma potência de k, segue que $(2n+2)!+k$ não é potência de um primo.

■

4.3 Olimpíada Pernambucana de Matemática (OPEMAT)

A OPEMAT é uma competição destinada a estudantes de escolas públicas e privadas, abrangendo do 6º ao 9º ano do Ensino Fundamental e o Ensino Médio. Nas edições de 2015 a 2019 as provas eram realizadas em fase única, mas a partir de 2021 passaram a ser aplicadas em duas fases (19). A seguir, apresentaremos um problema presente na edição de 2018 que envolve a distribuição dos números primos.

Exercício 4.4. (OPEMAT 2018 - Nível 3 - Q. 5) Alice e Clarinha estavam estudando para as olimpíadas de matemática e encontraram o seguinte problema: "Dado $n \in \mathbb{N}$ com $n \geq 2$, existe uma lista formada por n inteiros positivos consecutivos contendo apenas um único número primo?" Elas perguntaram para tio Dk: "É verdade isso?" Tio Dk respondeu: "Vamos ver! Para $n = 2$ é fácil encontrar exemplos disso. Se p é primo, então "$p,\ p+1$" ou "$p-1,\ p$" formam listas de $n = 2$ números inteiros positivos e consecutivos com apenas um primo. Analogamente, se $n = 3$ e p é um primo maior do que 3, então "$p-1,\ p,\ p+1$" é uma lista com $n = 3$ inteiros positivos consecutivos com apenas um número primo". Depois disso, tio Dk propôs:

a) Exibam uma lista com 13 inteiros consecutivos contendo apenas um número primo.

b) Agora verifiquem se é verdade que para todo $n \in \mathbb{N}$ com $n \geq 2$, existe uma lista formada por n inteiros positivos consecutivos contendo apenas um único número primo.

Faça o que tio DK propôs!

Solução. A solução para o item (a) é facilmente obtida ao analisar a sequência dos primos menores que 100 apresentada no início deste trabalho. Basta observar que do número 84 ao 96 temos uma lista com exatamente 13 inteiros consecutivos positivos com um único número primo, o 89. Assim, a sequência $\{84, 85, 86, 87, 88, 89, 90, 91, 92, 93, 94, 95, 96\}$ é solução para este problema. Para resolver o item (b), dado $n \geq 2$, considere a lista de $n-1$ inteiros consecutivos

$$n! + 2,\ n! + 3,\ n! + 4,\ ...,\ n! + n.$$

Observe que para cada $2 \leq i \leq n$, temos

$$\begin{aligned} n! + i &= 1 \cdot 2 \cdot ... \cdot (i-1) \cdot i \cdot (i+1) \cdot ... \cdot n \ + \ i \\ &= i \cdot [2 \cdot ... \cdot (i-1) \cdot (i+1) \cdot ... \cdot n + 1]. \end{aligned}$$

Logo, $n! + i$ é composto para todo $2 \leq i \leq n$. Dessa forma, a lista

$$n! + 2,\ n! + 3,\ n! + 4,\ ...,\ n! + n$$

é formada por $n-1$ inteiros consecutivos e compostos. Seja p o maior primo que satisfaz $p \leq n! + 1$. Pela maximalidade de p, temos que

$$p+1, p+2, p+3, ..., p+n-1,$$

é uma lista com $n-1$ inteiros consecutivos e compostos. Logo,

$$p, p+1, p+2, p+3, ..., p+n-1,$$

é uma lista com n inteiros positivos consecutivos com um único primo, o p.

■

4.4 Olimpíada Ibero-americana de Matemática (OIM)

A OIM é uma competição internacional na qual podem participar estudantes da América Latina, Espanha e Portugal (20). Anualmente, desde 1985, os países são representados por uma equipe de até quatro estudantes, que não tenham feito 18 anos em 31 de dezembro do ano imediatamente anterior à aplicação da prova e que não tenham participado de duas edições anteriores da olimpíada. A seguir, apresentaremos dois problemas envolvendo números primos presentes nas provas da OIM.

Exercício 4.5. (OIM 2016 - Q. 1) Determine todos os números primos positivos p, q, r, k tais que $pq + qr + rp = 12k + 1$.

Solução. Suponha que p, q e r são primos ímpares. Logo, podemos escrevê-los na forma $p = 2m + 1$, $q = 2n + 1$ e $r = 2t + 1$, com $m, n, t \in \mathbb{N}$. Daí,

$$(p+q) \cdot (p+r) = (2m + 2n + 2) \cdot (2m + 2t + 2) = 4 \cdot (m + n + 1) \cdot (m + t + 1).$$

Isto é, $(p+q) \cdot (p+r)$ é um múltiplo de 4. Entretanto, isto é um absurdo, pois

$$\begin{aligned}(p+q) \cdot (p+r) &= p^2 + pq + qr + rp \\ &= p^2 + 12k + 1 \\ &\equiv p^2 + 1 \pmod 4 \\ &\equiv 4m^2 + 4m + 2 \pmod 4 \\ &\equiv 2 \pmod 4.\end{aligned}$$

Assim, pelo menos um deles é par. Suponha, sem perda de generalidade, que $p = 2$. Daí, temos $(2+q) \cdot (2+r) = 4 + 12k + 1 = 12k + 5 \equiv 2 \pmod 3$. Assim, ao ser divididos por 3, os restos deixados por $2+q$ e $2+r$ são 1 e 2, não necessariamente nessa ordem. Suponha,

então, que $2+q \equiv 2 \pmod 3$. Assim, $q \equiv 0 \pmod 3$ e, como q é primo, temos $q = 3$. Mas, se $p = 2$ e $q = 3$, então

$$\begin{aligned} pq + qr + rp = 12k + 1 &\Rightarrow 2 \cdot 3 + 3r + 2r = 12k + 1 \\ &\Rightarrow 6 + 5r = 12k + 1 \\ &\Rightarrow 5 + 5r = 12k \\ &\Rightarrow 5 \cdot (1 + r) = 12k. \end{aligned}$$

Mas, $5 \nmid 12$, então $5 \mid k$. Como k é primo, temos $k = 5$. Assim,

$$5 + 5r = 12 \cdot 5 \Rightarrow 5r = 55 \Rightarrow r = 11.$$

Note que os valores de p, q e r encontrados podem ser permutados, logo, há seis soluções do tipo (p, q, r, k), sendo elas: $(2, 3, 11, 5)$, $(2, 11, 3, 5)$, $(11, 2, 3, 5)$, $(11, 3, 2, 5)$, $(3, 2, 11, 5)$ e $(3, 11, 2, 5)$.

■

Exercício 4.6. (OIM 1999 - Q. 4) Seja B um inteiro maior que 10 tal que cada um dos seus dígitos pertence ao conjunto $1, 3, 7, 9$. Demonstre que B tem fator primo maior ou igual a 11.

Solução. Observe que o último dígito de B é ímpar, logo B é ímpar. Além disso, temos que 5 não pode ser fator de B, pois este não termina em 0 ou 5. Logo, se B não possui fator primo maior ou igual a 11, os únicos fatores primos possíveis de B são os números 3 e 7. Vamos mostrar que todo número natural que possui apenas os fatores primos 3 e 7 são da forma $a = 20k + n$, com $k \in \mathbb{N}$ e $n \in \{1, 3, 7, 9\}$. Isto é, o dígito das dezenas de a é par e não pertence ao conjunto $\{1, 3, 7, 9\}$ ou todos os dígitos de a pertencem ao conjunto, porém $a < 10$. De fato, se $k = 0$, temos $20 \cdot 0 + 1 = 1$. Além disso,

- Se $a = 20k + 1$, temos $3a = 20 \cdot (3k) + 3$ e $7a = 20 \cdot (7k) + 7$;
- Se $a = 20k + 3$, temos $3a = 20 \cdot (3k) + 9$ e $7a = 20 \cdot (7k + 1) + 1$;
- Se $a = 20k + 7$, temos $3a = 20 \cdot (3k + 1) + 1$ e $7a = 20 \cdot (7k + 2) + 9$;
- Se $a = 20k + 3$, temos $3a = 20 \cdot (3k + 1) + 7$ e $7a = 20 \cdot (7k + 3) + 3$.

Logo, B possui um fator primo maior ou igual a 11.

■

4.5 American Invitational Mathematics Examination (AIME)

Estudantes do ensino médio que se destacam na American Mathematics Competition 10/12 (AMC 10/12) são convidados a participar da AIME (21). Aqueles com as maiores notas seguem para a USA Mathematical Olympiad (USAMO), sendo os melhores selecionados para o Mathematical Olympiad Program (MOP), uma preparação durante o verão norte-americano para representar os Estados Unidos na IMO.

Sua primeira edição ocorreu em 1983, mas a partir de 2000 houve uma alteração em seu formato, no qual as provas passaram a ser aplicadas em dois níveis: sendo o AIME I para estudantes do ensino fundamental e o AIME II para os estudantes do ensino médio. Para esta seção, selecionamos três problemas da AIME envolvendo números primos para apresentar e solucionar.

Exercício 4.7. (AIME I 2019 - Q. 14) Encontre o menor primo ímpar fator de $2019^8 + 1$.

Solução. Como p é ímpar, temos $p > 2$ tal que $p \mid 2019^8 + 1$. Logo, $2019^8 + 1 \equiv 0 \pmod{p}$, isto é, $2019^8 \equiv -1 \pmod{p}$. Elevando ambos os lados da congruência ao quadrado temos $2019^{16} \equiv 1 \pmod{p}$. Se $2019^n \equiv 1 \pmod{p}$ para algum $0 < n < 16$, então $2019^{mdc(n,16)} \equiv 1 \pmod{p}$. Note que $mdc\,(n, 16) \in \{1, 2, 4, 8, 16\}$, mas $mdc\,(n, 16) \nmid 8$, pois teríamos $2019^8 \equiv 1 \pmod{p}$, que contradiz o enunciado do problema. Logo, $mdc\,(n, 16) = 16$. Portanto, 2019^{16} é a menor potência positiva congruente a 1 módulo p. Pelo Pequeno Teorema de Fermat (3.12), segue que $2019^{p-1} \equiv 1 \pmod{p}$. Portanto, $p - 1 = 16k$, com $k \in \mathbb{Z}$. Assim, $p = 16k + 1$, ou ainda, $p \equiv 1 \pmod{16}$. O menor primo que satisfaz a congruência é o número 17, porém, para $p = 17$, temos:

$$\begin{aligned} 2019 &\equiv 13 \pmod{17} \\ 2019^2 &\equiv 169 \equiv -1 \pmod{17} \\ 2019^8 &\equiv 1 \pmod{17}. \end{aligned}$$

Logo, $p = 17$ não é solução do problema. O segundo menor primo que satisfaz a congruência acima é 97 e $p = 97$ implica que:

$$\begin{aligned} 2019 &\equiv 79 \pmod{97} \\ 2019^2 &\equiv 33 \pmod{97} \\ 2019^4 &\equiv 22 \pmod{97} \\ 2019^8 &\equiv 484 \equiv -1 \pmod{97}. \end{aligned}$$

Logo, $p = 97$ é a solução do problema.

■

Exercício 4.8. (AIME I 2015 - Q. 3) Existe um número primo p tal que $16p+1$ é o cubo de um inteiro positivo. Encontre p.

Solução. Se $p = 2$, temos $16 \cdot 2 + 1 = 33$, que não é o cubo de um inteiro. Logo, p é ímpar. Buscamos p tal que $16p + 1 = a^3$, com $a \in \mathbb{N}$. Portanto,

$$\begin{aligned} 16p &= a^3 - 1 \\ 16p &= a^3 - 1^3 \\ 16p &= (a-1) \cdot (a^2 + a + 1). \end{aligned}$$

Como $p \neq 2$, o máximo divisor comum entre p e 16 é 1. Note que a é ímpar, pois $16 + 1$ é ímpar. Assim, $a - 1$ é par e $a^2 + a + 1$ é ímpar. Logo, $p = a - 1$ ou $p = a^2 + a + 1$. Se $p = a - 1$, então $a^2 + a + 1 = 16 \Rightarrow a^2 + a - 15 = 0$. Note que $\Delta = 1 - 4 \cdot 1 \cdot (-15) = 61$ e $\sqrt{61} \notin \mathbb{Z} \Rightarrow a \notin \mathbb{Z}$. Mas, a é um inteiro positivo. Portanto, $p = a^2 + a + 1$. Daí, $a - 1 = 16 \Rightarrow a = 17$. Logo, $p = 17^2 + 17 + 1 = 307$.

■

Exercício 4.9. (AIME 1983 - Q. 8) Qual é o maior fator primo de dois dígitos do inteiro $n = \binom{200}{100}$?

Solução. Pela definição do coeficiente binomial, temos

$$\binom{200}{100} = \frac{200!}{100!\ 100!}.$$

Como estamos procurando um primo p com dois dígitos, temos $p < 100$. Logo, p aparece duas vezes no denominador. Assim, para que p seja fator de $\binom{200}{100}$, é necessário que p apareça pelo menos três vezes no numerador. Dessa forma, pelo teorema 1.16, queremos $\left\lfloor \frac{200}{p} \right\rfloor > 3$. Daí, $p < \frac{200}{3} \approx 66,6$. Logo, $p = 61$.

■

4.6 Outros Problemas

Nesta seção, apresentaremos problemas de competições matemáticas que necessitam de propriedades dos números primos para serem resolvidos, ficando suas resoluções a cargo do leitor.

Exercício 4.10. (OIM 2021 - Q. 1) Seja $P = p_1, p_2, ..., p_{10}$ um conjunto de 10 primos distintos e seja A o conjunto de todos os inteiros maiores que 1 tais que em sua decomposição em fatores primos aparecem apenas primos de P. Os elementos de A são coloridos de tal forma que:

a) cada elemento de P tem uma cor distinta,

b) se $m, n \in A$, então mn tem a mesma cor que m ou n,

c) para qualquer par de cores distintas R e S, não existem $j, k, m, n \in A$ (não necessariamente distintos), com j, k da cor R e m, n da cor S, tais que j divide m e n divide k.

Prove que existe um primo de P tal que todos os seus múltiplos em A tem a mesma cor.

Exercício 4.11. (IMO 2022 - Q. 3) Seja k um inteiro positivo e seja S um conjunto finito de números primos ímpares. Prove que existe no máximo uma forma (a menos de rotação e reflexão) de colocar os elementos de S ao redor de uma circunferência de modo que o produto de quaisquer dois vizinhos é da forma $x^2 + x + k$ para algum inteiro positivo x.

Exercício 4.12. (IMO 2022 - Q. 5) Encontre todas as triplas (a, b, p) de inteiros positivos tais que p é primo e

$$a^p = b! + p.$$

Exercício 4.13. (IMO 2008 - Q. 3) Prove que existe um número infinito de inteiros positivos n tais que $n^2 + 1$ tem um divisor primo maior que $2n + \sqrt{2n}$.

Exercício 4.14. (AIME I - 2004 - Q. 15) Para todos os inteiros positivos x, seja

$$f(x) = \begin{cases} 1, & \text{se } x = 1 \\ \dfrac{x}{10} & \text{se } x \text{ é divisível por 10} \\ x + 1 & \text{para os demais valores de } x \end{cases}$$

e defina uma sequência tal que: $x_1 = x$ e $x_{n+1} = f(x_n)$ para todos os inteiros positivos n. Seja $d(x)$ o menor n tal que $x_n = 1$. (Por exemplo, $d(100) = 3$ e $d(87) = 7$.) Seja m o número de inteiros positivos x tais que $d(x) = 20$. Encontre a soma dos fatores primos distintos de m.

Exercício 4.15. (AIME I 2024 - Q. 13) Seja p o menor número primo para o qual existe um inteiro positivo n tal que $n^4 + 1$ é divisível por p^2. Encontre o menor inteiro positivo m tal que $m^4 + 1$ é divisível por p^2.

Exercício 4.16. (AIME 1999 - Q. 8) Encontre o menor primo que é o quinto elemento de uma progressão aritmética crescente, com todos os quatro termos anteriores também primos.

Exercício 4.17. (OBMU 2022 - Fase Única - 2º dia - Q. 3) Seja $p \equiv 3 \pmod 4$ um número primo, e seja θ um ângulo tal que $tan(\theta)$ é racional. Prove que $tan((p+1)\theta)$ é um número racional cujo numerador é múltiplo de p, ou seja, $tan((p+1)\theta) = \frac{u}{v}$ com $u, v \in Z, v > 0, mdc(u, v) = 1$ e $u \equiv 0 \pmod p$.

Conclusão

O objetivo deste trabalho é explorar o universo dos números primos, analisando sua distribuição entre os números naturais através do teorema de Chebyshev. Para tanto, realizamos um estudo aprofundado de resultados elementares da matemática, apresentando e demonstrando propriedades fundamentais da teoria dos números, como o teorema fundamental da aritmética e o teorema binomial.

Apresentamos o teorema de Chebyshev, que permite estimar o valor da função $\pi(x)$, a qual retorna a quantidade de números primos menores ou iguais a x. Este enfoque permite uma compreensão mais ampla e acessível dos conceitos envolvidos, visto que utiliza resultados básicos em sua demonstração.

Devido à amplitude do tema, acreditamos que este trabalho possa inspirar professores a explorar o fascinante mundo dos números primos com seus alunos, especialmente no ensino médio. Primos especiais como os de Mersenne, Sophie Germain e Fermat, bem como os problemas não resolvidos apresentados, trazem resultados intrigantes que podem despertar o interesse dos estudantes.

Desejamos que este trabalho desperte o interesse pela participação em competições matemáticas, estimulando o raciocínio lógico dos alunos e seu engajamento em atividades desafiadoras, sendo este material útil para a preparação de professores e estudantes interessados.

Por fim, considerando as mudanças trazidas pelo Novo Ensino Médio e a inclusão de itinerários formativos pela BNCC (1), sugerimos a criação de uma disciplina eletiva dedicada à apresentação e exploração de curiosidades sobre os números primos. Essa abordagem pode estimular a curiosidade e o interesse dos estudantes pela matemática, tornando o aprendizado mais envolvente e motivador.

Referências

1 BRASIL. Ministério da Educação. **Base Nacional Comum Curricular**. Brasília: MEC, 2018.

2 LEMOS, Manoel. **Criptografia, Números Primos e Algoritmos**. 4 ed. Rio de Janeiro: IMPA, 2010.

3 **Mersenne Prime Discovery - $2^{82589933} - 1$ is Prime!**. Disponível em: <https://www.mersenne.org/primes/?press=M82589933>. Acesso em: 15 maio 2024.

4 HEFEZ, Abramo. **Aritmética**. 3. ed. Rio de Janeiro: Sociedade Brasileira de Matemática, 2022.

5 WANG, Xingbo. Frequently-Used Properties of the Floor Function. **International Journal of Applied Physics and Mathematics**, v. 10, p. 135-142, 2020. 10.17706/ijamp.2020.10.4.135-142.

6 OLIVEIRA, Marcílio Souza Rodrigues de. **Do binômio de Newton ao polinômio de Leibniz, demonstrações e aplicações**. 2021. 55 f. Trabalho de Conclusão de Curso (Licenciatura em Matemática) - Departamento de Matemática, Universidade Federal Rural de Pernambuco, Recife, 2021.

7 ANDREWS, George E. **Number Theory**. Philadelphia: W. B. Saunders Company, 1971.

8 LITT, Daniel. **Prime Reciprocals and Primes in Arithmetic Progression.** [s.l: s.n.]. Disponível em: <https://static1.squarespace.com/static/57bf2a6de3df281593b7f57d/t/57bf68b26a49636398ee2dce/1472161971095/primes1mod4.pdf>. Acesso em: 24 jul. 2024.

9 DEZA, Elena. **Mersenne numbers and Fermat numbers**. Hackensack, NJ: World Scientific Publishing Co. Pte. Ltd., 2022.

10 VOIGHT, John. **Perfect numbers: An elementary introduction**. Berkeley: Department of Mathematics, University of California, 1998. Disponível em: <https://math.dartmouth.edu/~jvoight/notes/perfelem.pdf>.Acesso em: 20 maio 2024.

11 COOPER, Christopher Donald Huntington. **Multiplactive Functions**. Macquarie University, 2022. Disponível em: <https://coopersnotes.net/docs/numbers/CHAP08%20Multiplicative%20Functions.pdf>. Acesso em: 11 jun. 2024.

12 BROWNING, Thomas. **Perfect Numbers, Mersenne Primes and the Euclid-Euler Theorem**. Disponível em: <https://sites.math.washington.edu/~mathcircle/circle/2015-16/first/2016s-week6-ws.pdf>. Acesso em: 11 jun. 2024.

13 CALDWELL, Chris. **Euler and Lagrange on Mersenne Divisors**. Disponível em: <https://t5k.org/notes/proofs/MerDiv2.html>. Acesso em: 11 jun. 2024.

14 ALKALAY-HOULIHAN, Colleen. **Sophie Germain and Special Cases of Fermat's Last Theorem**. Disponível em: <https://www.math.mcgill.ca/darmon/courses/12-13/nt/projects/Colleen-Alkalay-Houlihan.pdf>. Acesso em: 16 jun. 2024.

15 **6 Sophie Germain and Fermat's Last Theorem**. [s.l: s.n.]. Disponível em: <https://www.math.uci.edu/~ndonalds/math180b/6germain.pdf>. Acesso em: 15 maio 2024.

16 **OBM - Olimpíada Brasileira de Matemática**. Disponível em: <https://www.obm.org.br/>. Acesso em: 8 jun. 2024.

17 **International Mathematical Olympiad**. Disponível em: <https://www.imo-official.org/>. Acesso em: 8 jun. 2024.

18 STEVENS, Justin. **Olympiad Number Theory Through Challenging Problems**. [s.l: s.n.]. Disponível em: <https://s3.amazonaws.com/aops-cdn.artofproblemsolving.com/resources/articles/olympiad-number-theory.pdf>. Acesso em: 8 jun. 2024.

19 **Olimpíada Pernambucana de Matemática**. Disponível em: <https://www.opemat.com.br/>. Acesso em: 20 jun. 2024.

20 **Olimpíada Íbero-Americana de Matemática**. Disponível em: <https://www.obm.org.br/olimpiada-ibero-americana-de-matematica/>. Acesso em: 8 jun. 2024.

21 **American Invitational Mathematics Examination - AIME | Mathematical Association of America**. Disponível em: <https://maa.org/math-competitions/american-invitational-mathematics-examination-aime>. Acesso em: 8 jun. 2024.