NÚMEROS PRIMOS E SUAS CONTRIBUIÇÕES

Ester Silva Rangel*
Unidade Acadêmica de Matemática
Universidade de Campina Grande
Campina Grande, Brasil

Taiane Barboza Silva†
Unidade Acadêmica de Matemática
Universidade de Campina Grande
Campina Grande, Brasil

Leomaques Francisco Silva Bernardo‡
Unidade Acadêmica de Matemática
Universidade de Campina Grande
Campina Grande, Brasil

Resumo

A Teoria dos Números é uma área de grande importância na Matemática e se destina a estudar os números inteiros e suas propriedades. Pode-se destacar ainda nessa Teoria o estudo dos números primos que tem diversas aplicações não somente na Matemática, mas também em diversas outras áreas, a exemplo da Criptografia que estuda métodos de codificar uma mensagem de maneira que apenas o destinatário consiga ler.

Um número primo é um número inteiro não-nulo $p \neq \pm 1$ cujo os únicos divisores são ± 1 e $\pm p$. Já um número inteiro não-nulo $n \neq \pm 1$ que não é primo chama-se composto. Tais números foram estudados em civilizações bem antigas.

Segundo Coutinho (2004, p. 19) [1] até onde se sabe, o conceito de número primo foi introduzido na Grécia Antiga. Vamos encontrá-lo, por exemplo, nos Elementos de Euclides, escrito por volta de 300 a.C. Segundo a definição 11 do Livro VII dos Elementos: "Um número primo é aquele que é medido apenas pela unidade".

Várias fórmulas já foram propostas para gerar grandes números primos, Pierre de Fermat, conjecturou que todo número da forma $2^{2^n} + 1$ seria primo, o que foi desmentido por Leonhard Euler, uma vez que $2^{2^5} + 1$ é composto. Até os dias atuais não se conhece uma fórmula simples para gerar grandes números primos. Porém existem fórmulas que geram famílias interessantes de números primos (MOREIRA; SALDANHA, 2008 p.41) [6]. Uma dessas famílias, é a dos números primos de Mersenne, ele descobriu que se um número da forma $2^n - 1$ for primo, então n é primo. Devido a essa descoberta, todo número $2^n - 1$ com n primo é chamado número primo de Mersenne, denotado por M_n.

Marin Mersenne foi um monge franciscano que viveu em um mosteiro em Paris, nasceu em 8 de setembro de 1588 na pequena cidade de Oizé, na França, e morreu em 1 de setembro de 1648, em Paris. Ficou conhecido por trocar correspondências com muitos filósofos e cientistas de sua época com o objetivo de divulgar os trabalhos que estavam sendo desenvolvidos naquele momento a fim de contribuir com o avanço da Ciência. Ao longo da sua vida ajudou muitos cientistas em potencial, orientando-os na direção certa e aconselhando alguns sobre o próximo passo a ser dado. Mersenne adoeceu após sua visita para ver René Descartes (1596-1650) em julho de 1648 e, infelizmente, sua saúde nunca melhorou (O' CONNOR; ROBERTSON, 2005) [5].

No ano de 1644, Mersenne publicou um trabalho chamado Cogitata physico-mathematica, onde ele afirma que os números M_i são primos de Mersenne para $i = 2, 3, 5, 7, 13, 17, 19, 31, 67, 127$ e 257 (O' CONNOR; ROBERTSON, 2005) [5]. Um tempo depois comprovou-se que ele se enganou com relação aos números M_{67}

*e-mail: ester1rangel@gmail.com parcialmente financiado pelo FNDE/PET
†e-mail: taianebs99@gmail.com parcialmente financiado pelo FNDE/PET
‡e-mail: leomaques@mat.ufcg.edu.br parcialmente financiado pelo FNDE/PET

e M_{257}. Apesar dos enganos cometidos, trata-se de um grande feito, tendo em vista a grandeza dos números envolvidos e poucos recursos computacionais da época.

O teste de primalidade (teste para verificar se um dado número inteiro é ou não primo) de "Lucas-Lehmer" foi criado por Fançois Edouard Lucas (1842-1891) e aperfeiçoado por Derrick Henry Lehmer (1905-1991), e apesar de ser determinístico e não depender de conjecturas sua utilização acaba sendo limitada a casos específicos, pois para se testar um número n devemos conhecer os fatores do número $n-1$ (MORIMOTO, 2014, p. 54) [7]. O teste diz: Considere a sequência (V_k) para $k = 0, 1, \ldots$ definida recursivamente por $V_0 = 4$ e $V_{k+1} = V_k^2 - 2$. Seja p um número primo ímpar. Então $M_p = 2^p - 1$ é primo se, e somente se, $V_{p-2} \equiv 0$ $(mod\ M_p)$ (CRANDALL; POMERANCE, 2005, p.183) [3].

O projeto Great Internet Mersenne Prime Search (GIMPS) foi criado em 1996 por George Woltman, formado em Ciência da Computação pelo Instituto de Tecnologia de Massachusetts (MIT), é um projeto voluntário de computação distribuída, que como o próprio nome já indica, seu objetivo é encontrar números primos conhecidos como primos de Mersenne (WOLTMAN, 1996) [4]. Para a testagem desses números que são da forma $2^p - 1$, na verdade, são os expoentes p que são testados.

O GIMPS descobriu o maior número primo conhecido até o momento, $2^{82.589.933} - 1$, com 24.862.048 dígitos. Um computador oferecido por Patrick Laroche de Ocala, Flórida, fez a descoberta em 7 de dezembro de 2018 (WOLTMAN, 1996) [4]. Tal descoberta encontra-se no site oficial do GIMPS.

Os números primos são muito relevantes na área da Criptografia RSA, método bastante usado em aplicações comerciais. Este é o método utilizado, por exemplo, no Netscape, o mais popular dos softwares de navegação da Internet (COUTINHO, 2001) [2].

Este trabalho é fruto de estudos desenvolvidos na atividade Seminários de estudo em grupo no Programa de Educação Tutorial PET-Matemática-UFCG e teve a supervisão do Prof. Tutor Leomaques Francisco Silva Bernardo.

Referências

[1] COUTINHO, S. C. *Primalidade em Tempo Polinomial: Uma introdução ao Algoritmo AKS (Coleção Iniciação Científica)*. Rio de Janeiro: IMPA, 2004.

[2] COUTINHO, S. C. *Números Inteiros e Criptografia RSA (Série Computação e Matemática)*. Rio de Janeiro: IMPA, 2001.

[3] CRANDALL, Richard; POMERANCE, Carl. *Prime Numbers: A Computational Perspective*. 2ª ed. New York: Springer, 2005.

[4] WOLTMAN, George. *GIMPS: Great Internet Mersenne Primes Search*. [S. l.], 1996. Disponível em: <https://www.mersenne.org/>. Acesso em: 6 fev. 2023.

[5] O'CONNOR, J.J.; ROBERTSON, E.F. *Marin Mersenne*. MacTutor: 2005. Disponível em: <https://mathshistory.st-andrews.ac.uk/Biographies/Mersenne/>. Acesso em: 3 fev. 2023.

[6] MOREIRA, Carlos Gustavo; SALDANHA, Nicolau. *Primos de Mersenne (e outros primos muito grandes)*. 3ª ed. Rio de Janeiro: IMPA, 2008.

[7] MORIMOTO, Ricardo Minoru. *Números Primos: Propriedades, Aplicações e Avanços*. Orientador: Dra. Carina Alves. 2014. 63 f. Dissertação (Mestrado Profissional em Matemática) - Universidade Estadual Paulista, Rio Claro, 2014.