UNIVERSIDADE FEDERAL DO PARÁ

CAMPUS UNIVERSITÁRIO DE ABAETETUBA

FACULDADE DE CIÊNCIAS EXATAS E TECNOLOGICAS

CURSO DE LICENCIATURA EM MATEMÁTICA

ELBI JESUS DOS SANTOS

TESTE DE LUCAS–LEHMER PARA PRIMOS DE MERSENNE

Tomé-Açu - Pará

2022

ELBI JESUS DOS SANTOS

TESTE DE LUCAS–LEHMER PARA PRIMOS DE MERSENNE

Trabalho de Conclusão de Curso apresentado a Faculdade de Ciência Exatas e Tecnologia da Universidade Federal do Pará, Campus Universitário de Abaetetuba, como requisito final para obtenção do grau de Licenciatura em Matemática, sob orientação do Prof. Me. Manoel Lima Corrêa.

Tomé-Açu – Pará

2022

Dados Internacionais de Catalogação na Publicação (CIP) de acordo com ISBD
Sistema de Bibliotecas da Universidade Federal do Pará
Gerada automaticamente pelo módulo Ficat, mediante os dados fornecidos pelo(a) autor(a)

S237t Santos, Elbi Jesus dos.
Teste de Lucas-Lehmer para primos de Mersenne / Elbi Jesus dos Santos. — 2022.
xiii, 52 f. : il. color.

Orientador(a): Prof. Me. Manoel Lima Corrêa
Trabalho de Conclusão de Curso (Graduação) - Universidade Federal do Pará, Campus Universitário de Abaetetuba, Curso de Matemática, Abaetetuba, 2022.

1. Primos de Mersenne. 2. Teoria dos Números. 3. Números Naturais. 4. Teste de Lucas-Lehmer. 5. Números Perfeitos. I. Título.

CDD 512.7

ELBI JESUS DOS SANTOS

TESTE DE LUCAS–LEHMER PARA PRIMOS DE MERSENNE

Este trabalho de conclusão de curso foi julgado e aprovado, para a obtenção do título de Licenciatura em Matemática pelo corpo docente da Faculdade de Ciências Exatas e Tecnologia da Universidade Federal do Pará, Campus Universitário de Abaetetuba.

Tomé-Açu, 11 de julho de 2022

Prof.° Me. Manoel Lima Corrêa

UFPA / Abaetetuba

Orientador

Prof.° Dr. Aubedir Seixas Costa

UFPA / Abaetetuba

Examinador

Prof. Dr. Sebastião M. S. Cordeiro

Prof.ª Dr. Sebastião Martins Siqueira Cordeiro

UFPA / Abaetetuba

Examinador

A minha família por todo incentivo e dedicação e ajuda para que esse trabalho se tornasse possível.

AGRADECIMENTOS

Agradeço imensamente a Deus, por ter me proporcionado essa dádiva de poder viver um sonho que era fazer uma graduação em nível superior, a minha família que sempre me apoiou de várias formas possíveis nessa importante fase da minha vida. Agradeço em especial minha Mãe Maria Eliana de Jesus por todo apoio e conselhos, mesmo que numa cidade longe, estava orando pela minha caminhada nesse curso e também minha Esposa Samires Cunha Sampaio dos Santos por todas as vezes que pensei em desistir estava sempre me incentivando.

Muito obrigado a todos os funcionários do polo, ao motorista do ônibus que no período das aulas estava ali, das vezes que pacientemente me esperou na parada quando estava atrasado.

Agradeço também aos meus colegas da turma de matemática 2017, os amigos que sempre me apoiaram e em especial ao Hermes Reinaldo de Oliveira, um irmão que universidade me deu, e também aos vários grupos de trabalho que pudesse participar nas aulas pedagógicas.

Agradeço aos professores da graduação por todo conhecimento repassado nesse período de grandes aprendizados, em especial ao meu orientador e Professor Manoel Lima Correa por toda atenção e disposição, todo empenho que teve no decorrer do trabalho.

Enfim, agradeço a Deus por ter me colocado ao lado de pessoas especiais que ao longo deste percurso, puder aproveitar cada momento e ultrapassar a cada obstáculo que era colocado, nas aulas ou no cotidiano.

“ Á Matemática é a rainha das ciências e a Teoria dos Números é a rainha da Matemática”

(KARL F. GAUSS)

RESUMO

O presente trabalho tem como objetivo um pequeno resumo sobre os números primos de Mersenne e por consequência os números primos, assunto que mostrou ter uma certa relevância em vista do aumento de usuários de aplicativos que usam a criptografia RSA, para proteção de seus dados, sendo que a mesma usa números primos em seus cálculos, em especial primos com um grande número de digito que é o caso dos primos de Mersenne. Abordaremos tema que são cruciais de Teoria dos Números para o entendimento deste assunto complexo, sobre os quais apresentamos algumas propriedades e definições, avanços recentes no caso das conjecturas, e o uso do teste de Lucas-Lehmer para saber se um número é primo ou composto. Citaremos a biografia de Marin Mersenne e casos particulares de primos que foram estudados, caso dos números perfeitos.

Palavra – chave: Teoria dos números, Números naturais, Números de Mersenne, Números perfeitos, Teste de Lucas-Lehmer.

ABSTRACT

The present work aims at a small summary of Mersenne's prime numbers and, consequently, prime numbers, a subject that has shown to have a certain relevance because of the increase in users of applications that use RSA encryption to protect their data, being that it uses prime numbers in its calculations, especially primes with a large digit number, which is the case with Mersenne primes. We will approach themes that are crucial in Number Theory for the understanding of this complex subject, on which we present some properties and definitions, recent advances in the case of conjectures, and the use of the Lucas-Lehmer test to know if a number is prime or composite. We will cite the biography of Marin Mersenne and particular cases of primes that have been studied, the case of perfect numbers.

Keywords: Number Theory, Natural numbers, Mersenne numbers, Perfect numbers, Lucas-Lehmer test.

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

MDC – Máximo Divisor Comum

a.C. – Antes de Cristo

d.C. – Depois de Cristo

$\mathbf{M_n}$ – Primos de Mersenne

$\mathbf{P_n}$ – n-ésimo primo

mod - módulo

GIMPS – Great Internet Mersenne Prime Search

AMD – Advanced Micro Devices – Micro Dispositivos Avançados

CPU – Central Processing Unit – Unidade Central de Processamento

USD – United States Dollar – Dólar dos Estados Unidos

RSA – Rivest, Shamir, e Adleman

PCNs – Parâmetros Curriculares Nacionais

LISTA DE SÍMBOLOS

$\mathbb{N}$ - Representa o conjunto dos números naturais

$|$ - Um inteiro a divide o inteiro b.

$\nmid$ - Um inteiro a não divide o inteiro b.

$\equiv$ - Congruência.

$\mathbb{Z}$ - Representa o conjunto dos números inteiros

$\in$ - Pertence

γ - É a constante de Euler-Mascheroni.

$\Rightarrow$ - Implica

σ – Letra Grega Sigma

φ – Letra Grega Fi

$\binom{p}{k}$ – Coeficiente binomial de p sobre k

SUMÁRIO

1 INTRODUÇÃO

Historicamente os números conhecidos como números primos, sempre fascinaram os matemáticos, tanto pelo lado místico quanto pela sua forma estruturada, vários matemáticos estudaram o assunto. Para Carl Boyer (2012), os números primos são estudados pelas civilizações mais antigas, mas, foi Euclides de Alexandria, um dos primeiros, e sendo que seus estudos foram iniciados no ano 360 a.C., que em sua obra intitulada Os elementos de Euclides, ele diz "Um número primo é aquele que é medido apenas por uma unidade", outros matemáticos também se destacam nos estudos dos números primos, um deles certamente foi Diofanto que por volta de 250 d.C., teve um destaque por sua escrita aritmética, que tratava em especial da solução de equações indeterminadas com coeficientes inteiros .

Outro matemático que teve seu destaque foi Pierre de Fermat, cujo o mesmo fez estudos sobre números primos, sendo que o Último Teorema de Fermat chamou a atenção dos matemáticos do século XVIII ao XIX, sendo que ao longo do tempo, várias fórmulas foram propostas pra sociedade, cuja as mesmas, pudessem gerar primos arbitrariamente grandes, um desses matemáticos foi Fermat que conjecturou que todo número da forma $2^{2^n} + 1$ fosse primo, vale ressaltar que a maioria dos estudiosos acredita que não exista uma fórmula que possa gerar todos os números primos.

Um dos matemáticos que se encantavam com os números primos foi Marin Mersenne, que também era um monge, que durante sua vida manteve diálogos com grandes nomes importantes para o conhecimento, embora números da forma $M_n = 2^n - 1$ já fossem conhecidos por Euclides, foi através de Mersenne (1588 – 1648) que o assunto se espalhou, pois de certa forma ele transmitia notícias do avanço dos estudos científicos em troca de mais informações, dessa forma, ele divulgava questões e solicitava contribuições, estimulando o desenvolvimento científico, através de cartas Mersenne se correspondia com vários nomes pela Europa, dos quais Fermat na França, Huygens na Holanda, Pell e Hobbes na Inglaterra, e Galileu e Torricelli na Itália, e muitos outros matemáticos e simpatizantes dos números primos., mas Mersenne sempre teve um interesse no conceito de divisibilidade, pois questionava sobre a possível factoração de alguns números.

Alguns matemáticos antigos pensavam que todo número da forma $2^n - 1$ seria primo para qualquer *p* primo considerado. Entretanto em 1536, Hudalrichus Regius apresentou a factorização de $2^{11} - 1 = 2047 = 23 \times 89$, demostrando que a conjectura era incorreta.

Conjectura-se que existam infinitos primos *p* para os quais tem-se que M_p seja primo, as questões sobre como reconhecer um número primo e, em sendo um número composto, como decompô-lo em seus fatores primos foram formuladas em tempos remotos. Karl Friedrich Gauss escreveu no artigo 329 das Disquisitiones Arithmeticae (1801): " O problema de distinguir números primos de compostos e decompor esses últimos em seus fatores primos é conhecido como sendo um dos mais importante e úteis na aritmética...A dignidade da própria ciência parece requerer que todos os meios possíveis sejam explorados para a solução de um problema tão elegante e tão celebrado" (MARTINEZ; MOREIRA; SALDANHA; TENGAN, 2011).

Atualmente os computadores fazem grande parte dos cálculos, mas em outros tempos esses cálculos eram feitos por uma sucessão recorrente indicada por Lucas (1878) e Lehmer (1930 e 1935), ressaltando que este método não permite determinar os fatores no caso de o número ser composto.

Essa busca por fórmulas e métodos que possam gerar números primos, ficou mais atrativa devido os primos serem úteis em criptografia, pois os mesmos são utilizados na criação de senhas (chaves) para proteger dados confidencias e essa busca por números primos ou números primos de Mersenne têm-se aumentado com o tempo, pois sem esses números não seria possível efetuar compras seguras na internet.

Entretanto foi em 1951 que os computadores começaram a ser usados para o árduo trabalho de procurar números primos tão grandes, já que estudos comprovam sua infinidade, os resultados obtidos pelos computadores foram aumentando a lista dos números de Mersenne, e todos esses números foi usado o critério de Lucas-Lehmer, cujo mesmo é um algoritmo criado por Lucas e posteriormente aprimorado por Lehmer. E no final de 1995, entra George Woltman, um programador e organizador, que reuniu os bancos de dados e um programa gratuito, sendo que o mesmo é altamente otimizado para pesquisar primos de Mersenne na web, assim começou o GIMPS (o Great Internet Mersenne Prime Search).

Contudo isso, os números primos e os primos de Mersenne têm um papel importante na sociedade e, sabendo, eles podem ser abordados com mais ênfase e naturalidade no ensino, vale ressaltar que não é apenas abordar os conceitos e definições, mais também à importância histórica e aplicabilidade desses números.

Diante do exposto, este trabalho está organizado na seguinte ordem: Capítulo 1 fala sobre a Teoria dos Números; no Capítulo 2, será sobre os Primos de Mersenne e o Teste de

Lucas_Lehmer; no Capítulo 3, sobre a Tabela dos Primos de Mersenne; no Capítulo 4, sobre a Biografia de Marin Mersenne; no Capítulo 5, será sobre Números Perfeitos e algumas conjecturas; e o Capítulo 6 tem-se as conclusões e perspectivas; seguido as referências e os anexos.

2 TEORIA DOS NÚMEROS

Neste capítulo veremos tópicos básicos de teoria dos números que são importantes para o estudo dos números primos, e que são imprescindíveis que são o caso da divisibilidade, do máximo divisor comum, divisão euclidiana e o teorema fundamental da aritmética.

2.1 Números Naturais

Os números naturais formam um modelo matemático padrão, que nos possibilita uma operação de contagem, sendo que a sequência desses números é uma livre e antiga criação do espirito humano, esse processo de comparar os conjuntos de objetos com uma escala abstrata ideal, dessa forma fica mais precisa a noção de quantidade. Sabemos que os números naturais são1, 2, 3, 4, 5, · · · e a totalidade desses números formam um conjunto, que é indicado com símbolo $\mathbb{N}$, e que chamaremos de conjunto dos naturais, portanto, $\mathbb{N} = \{1, 2, 3, 4, 5, , \cdots\}$.

Figura 1 – Giussepe Peano

Fonte: https://www.liberliber.it/online/wp-contentuploads/2021/02/peano_ritratto.jpg

Giussepe Peano (1858 – 1932) fez uma constatação de que pode elaborar toda teoria dos números naturais a partir de quatro propriedades.

2.1.1 Axioma de Peano

Um matemático profissional, em sua linguagem direta e objetiva, observaria que o conjunto $\mathbb{N}$ dos números naturais é caracterizado por essas quatro propriedades:

P1 Existe uma função $s: \mathbb{N} \longrightarrow \mathbb{N}$, que associa a cada $n \in \mathbb{N}$ um elemento $s(n) \in \mathbb{N}$, chamado o sucessor de n.

P2 A função $s: \mathbb{N} \longrightarrow \mathbb{N}$ é injetiva.

P3 Existe um único elemento 1 no conjunto $\mathbb{N}$, tal que $1 \neq s(n)$ para todo $n \in \mathbb{N}$.

P4 Se um subconjunto $X \subset \mathbb{N}$ é tal que $1 \in \mathbb{N}$ e $s(X) \subset X$ (isto é, $n \in X \Rightarrow s(n) \in X$), então $X = \mathbb{N}$.

Um dos axiomas de Peano, o último, possui uma natureza mais elaborada do que os demais, ele é conhecido como axioma da indução.

2.1.2 Axioma da indução

O significado informal desse axioma é que todo número natural pode ser obtido a partir de 1 por meio de repetidas aplicações da operação de tomar o sucessor, dessa maneira, 2 é o sucessor 1, 3 é o sucessor do sucessor de 1, etc.

Vale ressaltar que não é verdade que todo número natural n pode ser obtido, a partir de 1, mediante repetidas aplicações, mas dentro de um ponto de vista estritamente matemático, pode-se reformular o axioma da indução da seguinte maneira:

Um subconjunto $X \subset \mathbb{N}$ chama-se indutivo quando $s(X) \subset X$, ou seja, quando $n \in X \Rightarrow s(n) \in X$, ou ainda, quando o sucessor de qualquer elemento X também pertence a X. Dessa forma, o axioma da indução afirma que o único subconjunto indutivo de $\mathbb{N}$ que contém o número 1 é o próprio $\mathbb{N}$, e na teoria dos números naturais o papel fundamental do axioma da indução, e mais geralmente, em toda a matemática, resulta que ele pode ser visto como método de demonstração, chamado o Método da Indução Matemática, ou Princípio da Indução Finita.

Teorema 1.1 (Princípio da Boa Ordem)

Diz que todo subconjunto não vazio de $\mathbb{N}$ possui um elemento mínimo, e este princípio é equivalente ao Princípio da indução.

2.2 Divisibilidade

Definição 1.1

Sejam $\mathbf{m, n} \in \mathbb{N}$**,** é dito que **m** divide **n**, e denota-se $\mathbf{m} \mid \mathbf{n}$, quando existir $\mathbf{q} \in \mathbb{N}$ tal que $n = m \cdot q$, Sendo assim, chamaremos **m** e **q** de divisores ou fatores de **n** e é dito que **n** é múltiplo de **m** e **q**, caso não exista **q** tal que $\mathbf{n = m \cdot q}$, é dito que **m** não divide **n** e é denotado por $m \nmid n$.

Proposição 1.1

Sejam **m**, **n** ∈ ℕ*, se **m** ∣ **n** então **m** ≤ **n**.

Demonstração

m ∣ **n** implica na existência de **q** ∈ ℕ*, tal que **n** = **m** · **q**. Como **q** ≥ **1**, temos **m** ≤ **m** · **q** = **n**.

■

Se for obtido dois inteiros a e b (com b ≠ 0), então dizemos que b divide a, ou que a é um múltiplo de b, de forma b ∣ a se e somente se a mod b = 0

2.3 Máximo Divisor Comum

Definição 1.2

Sejam m, n, d ∈ ℕ com m e n não nulos simultâneos, com as seguintes condições satisfeitas;

i) d é divisor comum de m e n
ii) todo divisor comum de m e n divide d

Dessa forma damos o nome de máximo divisor comum de m e n, ou mdc e denotamos por d = mdc (m, n), sabendo disso podemos definir outro conceito muito importante que é muito usado na demonstração de algumas propriedades do mdc.

Definição 1.3

É dito que dois números m, n ∈ ℕ são primos entre si quando mdc (m, n) = 1.

Exemplo 1.1

mdc (21, 143) = 1, note que 21 e 143 são primos entre si, mas também sabemos que eles não são primos separadamente.

Proposição 1.2

Dados a, b $\in \mathbb{Z}$ existe um único d $\in \mathbb{N}$ tal que d $\mid$ a, d $\mid$ b e, que para todo c $\in \mathbb{N}$, se c $\mid$ a e c $\mid$ b então c $\mid$ d, além disso existem x, y $\in \mathbb{Z}$ com d = ax + by.

Entre os divisores comuns de um par qualquer de números, existe um que apresenta algumas singularidades especiais.

Lema 1.1

Dados m, n, a $\in \mathbb{N}$, com m < m · a < n, mdc (m, n) = mdc (m, n – m · a).

Demonstração

Seja mdc (m, n – m · a), temos que d $\mid$ m $\rightarrow$ d $\mid$ m · a e d $\mid$ n – m · a, sendo que em particular, d $\mid$ (n – m · a + m · a) = n, portanto d é um divisor de n também, caso supormos que exista um número c que seja divisor comum de a e b, temos que c $\mid$ n – m · a, e como d = mdc(m, n – m · a), temos que c $\mid$ d, portanto d = mdc(m, n).

■

2.4 Divisão Euclidiana (Algoritmo de divisão Euclidiana)

Vale salientar que no livro VII da obra “Os Elementos” Euclides já enuncia o que hoje conhecemos como algoritmo de divisão Euclidiana, porém, sem demonstrá-lo.

Teorema 1.2 (Algoritmo de divisão geral)

Para quaisquer números a, b $\in \mathbb{Z}$ com b $\neq$ 0 existem únicos q, r $\in \mathbb{Z}$ tais que

$$a = bq + r \qquad e \qquad 0 \leq r < |b|.$$

Demonstração

Temos $|b| > 0$. Pelo teorema 2.1, existem únicos q', $r \in \mathbb{Z}$ com $a = |b| q' + r$ com $0 \leq r < |b|$.

Se $b > 0$ então $|b| = b$ e podemos considerar $q = q'$ junto com r.

Se $b < 0$ então $|b| = - b$ e podemos considerar $q = - q'$ junto com r, dessa forma obtendo,

$$a = |b| q' + r = (-b)q' + r = b(-q') + r = bq + r$$

■

Exemplo 1.1

Para $a = 100$ e $b = -7$ temos $q = -14$ e $r = 2$, pois, $100 = (-7) \cdot (-14) + 2$

Para $a = -100$ e $b = -7$ temos $q = 15$ e $r = 5$, pois, $-100 = (-7) \cdot 15 + 5$

2.5 Teorema Fundamental da Aritmética

Definição 1.4

Seja um número $p > 1$é um número **primo** se seus únicos divisores são 1 e p. Qualquer número $n > 1$ tem pelo menos um divisor primo. Se n é primo, então esse divisor primo é o próprio n. Mas se n não é primo, seja $a > 1$seu menor divisor, $n = ab$, onde $1 < a \leq b$. Se a não fosse primo, então $a = a_1a_2$ com $1 < a_1 \leq a_2 < a$ e $a_1 | n$ contradizendo a minimalidade de a.

Esse teorema diz que seja $n \geq 2$ um número natural, podemos escrever n de uma única forma como um produto

$$n = p_1 \cdot \cdot \cdot p_m$$

Onde $m \geq 1$ é um natural e $p_1 \leq \cdot \cdot \cdot \leq p_m$ são primos.

Demonstração

Mostramos a existência da fatoração por indução. Se n é primo não há o que provar, escrevemos m = 1, p_1 = n, Mas se n é composto podemos escrever n = ab, com a, b ∈ $\mathbb{N}$, 1 < a < n, 1 < b < n. Por hipótese de indução, a e b se decompõem como produtos de primos, juntando as fatorações de a e b (e organizando os fatores) obtemos uma fatoração de n.

Agora mostramos a unicidade, também por indução, suponha que

$$n = p_1 \cdot \cdot \cdot p_m = q_1 \cdot \cdot \cdot q_{m'}$$

Com $p_1 \leq \cdot \cdot \cdot \leq p_m$, $q_1 \leq \cdot \cdot \cdot \leq q_{m'}$. Como $p_1 \mid q_1 \cdot \cdot \cdot q_{m'}$ temos $p_1 \mid q_i$ para algum valor de i, donde, como qi é primo, $p_1 = q_i$ e $p_1 \geq q_i$. Analogamente temos $q_1 \leq p_1$, donde $p_1 = q_1$. Mas por hipótese de indução temos:

$$n \mid p_1 = p_2 \cdot \cdot \cdot p_m = q_2 \cdot \cdot \cdot q_{m'}$$

Admite uma única fatoração, donde m = m' e $p_i = q_i$ para todo i.

■

Com os assuntos citados, vamos abordar os números de Mersenne e o teste de primalidade de Lucas-Lehmer.

3 PRIMOS DE MERSENNE E O TESTE DE LUCAS- LEHMER

Neste capítulo será abordado algumas definições e teoremas que têm uma grande importância para o assunto exposto.

Figura 2 - Euclides de Alexandria.

Fonte: https://maestrovirtuale.com/wp-content/uploads/2019/10/5-aportaciones-de-Euclides.jpg.

3.1 Números Primos

Teorema 2.1 (Euclides)

Existem infinitos números primos.

Demonstração

Suponha por absurdo que $P_1, P_2, \cdots, Pm$ fossem todos os primos. O número $N = P_1, P_2, \cdots, P_m + 1 > 1$ não seria divisível por nenhum primo, o que contradiz o teorema fundamental da aritmética.

■

Definição 2.1

Um número n > 1 que não é primo é chamado de **composto**. Se n é um número composto, então ele tem um divisor primo menor que $\sqrt{n}$. De fato, como na definição 1.4, n = ab, onde $1 < a \leq b$ e a é o menor divisor de n, logo $n \geq a^2$, e portanto $a \leq \sqrt{n}$., vale lembrar que essa ideia pertence ao matemático Eratóstenes (250 a.C.) da Grécia antiga.

Figura 3 - Eratóstenes ensinando em Alexandria

Fonte: https://greciantiga.org/img/j/ji645.jpg.

Definição 2.2

Seja $n \in \mathbb{N}_0$ um número fixo, dois números a, b,$\in \mathbb{Z}$ chamam-se congruentes módulo n, se a – b é múltiplo de n, denotamos por $a \equiv b \bmod n$, dessa forma se,

$$a \equiv b \bmod n \Leftrightarrow n \mid a - b.$$

Exemplo 2.1

Para n = 6 $\quad 1 \equiv 7 \equiv -5 \equiv -11 \bmod 6 \quad 123 \equiv -135 \bmod 6.$

3.2 Primos de Mersenne

Durante muitos séculos vários matemáticos acreditavam que todos os números da forma $2^n - 1$ com n primo fossem primos, mas, em 1536, Hudalrichus Regius mostrou que $2^{11} - 1$ era composto, entretanto na primeira metade do século 17 Marin Mersenne publicou sua lista de primos

2, 3, 5, 7, 13, 17, 19, 31, 67, 127, 257

Para os quais acreditava que o número $2^p - 1$ seria primo, alguns anos depois outros matemáticos apontaram erros nela, como inclusão de números compostos e omissão de números primos, Somente séculos mais tarde, que a lista foi completamente verificada até o expoente 257, mas apesar dos erros, Mersenne ficou conhecido por tais números.

Definição 2.3

É dito primo de Mersenne todo número primo da forma $M_n = 2^n - 1$, onde n é um número natural.

Teorema 2.2

Se $2^n - 1$ é primo então n é primo.

Demonstração

Se n = ab, com a, b ≥ 2 então $1 < 2^a - 1 < 2^n - 1$ e $2^n - 1 = 2^{ab} - 1 = (2^a)^b - 1 \equiv 1^b - 1 = 0 \pmod{2^a - 1}$ e $2^n - 1$ é composto.

■

Exemplo 2.2

Sabe-se que desde os tempos de Mersenne, que números desta forma podem ser primo ou compostos, este são primos para isto $M_n = 2^n - 1$ com $n > 1$, temos então:

$M_2 = 3$, pois $M_2 = 2^2 - 1 = 4 - 1 = 3$

$M_3 = 7$, pois $M_3 = 2^3 - 1 = 8 - 1 = 7$

$M_5 = 31$, pois $M_5 = 2^5 - 1 = 32 - 1 = 31$

$M_7 = 127$, pois $M_7 = 2^7 - 1 = 128 - 1 = 127$

Exemplo 2.3

Entretanto, existem números desta forma que são compostos:

$M_{11} = 2047$, pois $M_{11} = 2^{11} - 1 = 2048 - 1 = 2047 = 23$ X 89, dessa forma não sendo primo;

$M_{67} = 147.573.952.589.676.412.927$ pois $M_{67} = 2^{67} - 1 = 147.573.952.589.676.412.928 - 1 = 147.573.952.589.676.412.927 = 761.838.257.287$ X 193.707.721 portanto não sendo primo.

Vale ressaltar que em 1903, em uma apresentação para a American Mathematical Society, o professor Frank Nelson Cole (1861 – 1926), foi até um quadro-negro e, em completo silêncio, realizou os cálculos, citados acima, todos à mão. E sem dizer uma palavra voltou ao seu lugar, ele foi recompensado com uma ovação de palmas com todos de pé.

Atualmente não se sabe demostrar nem que existam infinitos primos de Mersenne e nem que existem infinitos primos p para os quais M_p é composto, conjectura-se que existam infinitos primos p para os quais M_p é primo e que, se p_n é o n-ésimo primo deste tipo, temos

$$0 < A < \frac{\log Pn}{n} < B < +\infty$$

Sendo que para constantes A e B, sendo que existem algumas conjecturas um pouco mais precisas quanto ao valor de

$$\lim_{n\to\infty} \sqrt[n]{Pn},$$

Eberhart conjectura que este limite exista e seja igual a 3⁄2; Wagstaff por outro lado conjectura que o limite seja

$$2^{e^{-\gamma}} \approx 1{,}4757613971$$

onde γ é a constante de Euler-Mascheroni.

Apesar dos enganos cometidos, não podemos negar que foi um grande feito, haja vista da grandeza dos números envolvidos e dos poucos recursos computacionais da época, e o que nos mostra um problema que é determinar se um determinado número de Mersenne é primo ou não, e sendo assim, determinar seus fatores primos.

Lema 2.1

Seja p um número primo, então os números $\binom{p}{k}$, onde 0 < k < p são divisíveis por p.

Demonstração

Para k = 1, temos $\binom{p}{1} = 1$. Podemos, então supor 1 < k < p, assim, k! $\mid$ (p – 1) · · · (p – k + 1), e o resultado se segue, pois $\binom{p}{k} = p\frac{(p-1)\ldots(P-K+1)}{k!}$.

■

Teorema 2.3

Sejam a ∈ ℤ, n ∈ ℕ , n ≥ 2 e (a, n) = 1. Então n é primo se, e somente se, $(x + a)^n \equiv (x^n + a) \pmod n$).

Demonstração

Para 0 < k < n, o coeficiente de x^k em $(x + a)^n – (x^n + a)$ é $\binom{n}{k}a^{n-k}$. Supondo que n é primo, pelo Lema 2.1, temos $\binom{n}{k} = 0 \pmod n$, ou seja, todos os coeficientes são 0 (zero). Por outro lado, suponhamos que n é composto. Seja o primo p um fator de n e p^q a maior potência

de p que divide n. Assim, p^q não divide $\binom{n}{p}$ e (p^q, a^{n-p}) = 1, logo, coeficiente de x^p não é 0 (zero). Portanto, n ∤ $(x + a)^n - (x^n + a)$.

Entretanto, com um número de Mersenne em mãos, como podemos ter certeza que esse número é realmente um primo, por essa razão podemos usar o teste que veremos no decorrer do trabalho.

3.3 Primos especiais

São tipos especiais de primos dados por formulas, exemplo:

$F_n = 2^{2^n} + 1$ com n um número natural;

Existem 5 primos conhecidos (Fermat)

$M_p = 2^p - 1$ onde p é um número primo;

Existem 51 primos conhecidos (Mersenne)

3.4 Teste de primalidade de Lucas-Lehmer

Esse teste foi criado por Edouard Lucas e Aperfeiçoado por Derrick Henry Lehmer, e apesar de ser um teste determinístico e não depender de conjecturas sua utilização acaba sendo limitada a casos específicos, e para testar um número n devemos conhecer os fatores do número n – 1, dessa forma acaba sendo mais eficaz para testar números como os de Mersenne.

Figura 5 – Édouard Lucas

https://faculty.evansville.edu/ck6/bstud/elucas.jpg

Figura 4 – Derrick Lehmer

https://mathshistory.st-andrews.ac.uk/Biographies/Lehmer_

O teste de Lucas-Lehmer também pode ser estendido para inteiros arbitrários, sendo que antes do trabalho de Pratt (1975), o teste de Lucas-Lehmer era considerado como uma heurística que funcionava em grande parte do tempo (Knuth 1969).

Teorema 2.4

Seja S_k a sequência definida por $S_k = (2 + \sqrt{3})^{2^k} + (2 - \sqrt{3})^{2^k}$ para $k \in \mathbb{N}$. Seja $n > 2$, $M_n = 2^n - 1$ é primo se, e somente se, S_{n-2} é múltiplo de M_n.

Demonstração

Suponha, por absurdo, que $M_n \mid (2 + \sqrt{3})^{2^{n-2}} + (2 - \sqrt{3})^{2^{n-2}}$ e M_n seja composto, com um fator primo p tal que $p^2 \leq M_n$ Assim, teremos:

$(2 + \sqrt{\mathbf{3}})^{\mathbf{2^{n-2}}} + (2 - \sqrt{\mathbf{3}})^{\mathbf{2^{n-2}}} \equiv 0 \pmod p \Leftrightarrow (2 + \sqrt{\mathbf{3}})^{\mathbf{2^{n-2}}} \equiv -(2 - \sqrt{\mathbf{3}})^{\mathbf{2^{n-2}}} \pmod p$, como $(2 + \sqrt{3}) \cdot (2 - \sqrt{3}) = 1$, ou seja $2 - \sqrt{3} = (2 + \sqrt{3})^{-1}$ dessa forma podemos reescrever a equação $(2 + \sqrt{\mathbf{3}})^{\mathbf{2^{n-2}}} \equiv - \frac{\mathbf{1}}{(\mathbf{2 + \sqrt{3}})^{\mathbf{2^{n-2}}}} \pmod p \Leftrightarrow (2 + \sqrt{\mathbf{3}})^{\mathbf{2^{n-1}}} \equiv -1 \pmod p$, o que significa que a ordem de $2 + \sqrt{3}$ é igual a 2^n. Absurdo, pois o valor máximo de $\boldsymbol{\varphi}(M_n) = p^2 - 1 < 2^n$, logo, se S_{n-2} é múltiplo de M_n então M_n é primo.

Supondo M_n primo, pelo Teorema 2.3 temos:

$(1 + \sqrt{3})^{Mn} \equiv 1 + (\sqrt{3})^{Mn} \equiv 1 + 3^{\frac{Mn-1}{2}}\sqrt{3} \equiv 1 \left(\frac{3}{Mn}\right)\sqrt{3} \equiv 1 - \sqrt{3} \pmod{M_n}$, já que pela reciprocidade quadrática $\left(\frac{3}{Mn}\right) = -\left(\frac{Mn}{3}\right) = -\left(\frac{-2}{3}\right) = -1$.

Note ainda que $(1 + \sqrt{3})^2 = 2(2 + \sqrt{3})$. Assim, temos:

$[(1 + \sqrt{3})^2]^{2^{n-1}} = 2^{2^{n-1}}(2 + \sqrt{3})^{2^{n-1}} \Leftrightarrow (1 + \sqrt{3})^{2^n} = 2^{2^{n-1}}(2 + \sqrt{3})^{2^{n-1}}$

$(1 + \sqrt{3})^{Mn+1} = 2.2^{\frac{Mn-1}{2}}(2 + \sqrt{3})^{2^{n-1}} \Leftrightarrow -2 \equiv 2\left(\frac{2}{M_2}\right)(2 + \sqrt{3})^{2^{n-1}} \pmod{M_n}$

$-1 \equiv \left(\frac{2}{Mn}\right)(2 + \sqrt{3})^{2^{n-1}} \pmod{M_n} \Leftrightarrow -1 \equiv (2 + \sqrt{3})^{2^{n-1}} \pmod{M_n}$,

Sendo que $\left(\frac{2}{Mn}\right) = (-1)^{\frac{Mn^2-1}{8}} = 1$. Dessa forma usamos novamente a igualdade $(2 + \sqrt{3}) \cdot (2 - \sqrt{3}) = 1$ concluímos que:

$(2 + \sqrt{3})^{2^{n-1}} \cdot (2 - \sqrt{3})^{2^{n-2}} \equiv -(2 + \sqrt{3})^{2^{n-2}} \pmod{M_n}$

$(2 + \sqrt{3})^{2^{n-1}} \cdot \frac{1}{(2 + \sqrt{3})^{2^{n-2}}} \equiv -(2 + \sqrt{3})^{2^{n-2}} \pmod{M_n}$

$(2 + \sqrt{3})^{2^{n-2}} \equiv -(2 - \sqrt{3})^{2^{n-2}} \pmod{M_n}$

$(2 + \sqrt{3})^{2^{n-2}} + (2 - \sqrt{3})^{2^{n-2}} \equiv 0 \pmod{M_n}$

Portanto, $M_n \mid (2+\sqrt{3})^{2^{n-2}} + (2-\sqrt{3})^{2^{n-1}}$, ou seja, S_{n-2} é múltiplo de M_n.

Proposição 2.1

Seja a sequência $S_k = (2+\sqrt{\mathbf{3}})^{\mathbf{2^k}} + (2-\sqrt{\mathbf{3}})^{\mathbf{2^k}}$, S_k de forma recursiva é dada por: $S_o = 4$ e $\boldsymbol{S_k^2} - 2$.

Demonstração

Para k = 0, teremos $S_0 = (2+\sqrt{\mathbf{3}})^{\mathbf{2^0}} + (2-\sqrt{\mathbf{3}})^{\mathbf{2^0}} \Leftrightarrow S_0 = 2 + \sqrt{3} + 2 - \sqrt{3} \Leftrightarrow S_0 = 4$.

De modo análogo, escrevemos S_{k+1} em função de S_k, portanto:

$S_{k+1} = (2+\sqrt{\mathbf{3}})^{\mathbf{2^{k+1}}} + (2-\sqrt{\mathbf{3}})^{\mathbf{2^{k+1}}} = (2+\sqrt{\mathbf{3}})^{\mathbf{2^k \cdot 2}} + (2-\sqrt{\mathbf{3}})^{\mathbf{2^k \cdot 2}}$

$= [(2+\sqrt{\mathbf{3}})^{\mathbf{2^k}}]^2 + [(2-\sqrt{\mathbf{3}})^{\mathbf{2^k}}]^2 + 2(2+\sqrt{\mathbf{3}})^{\mathbf{2^k}}(2-\sqrt{\mathbf{3}})^{\mathbf{2^k}} - 2(2+\sqrt{\mathbf{3}})^{\mathbf{2^k}}(2-\sqrt{\mathbf{3}})^{\mathbf{2^k}}$

$= [(2+\sqrt{\mathbf{3}})^{\mathbf{2^k}} + (2-\sqrt{\mathbf{3}})^{\mathbf{2^k}}]^2 - 2[(2+\sqrt{3})(2-\sqrt{\mathbf{3}})]^{\mathbf{2^k}}$

$= [(2+\sqrt{\mathbf{3}})^{\mathbf{2^k}} + (2-\sqrt{\mathbf{3}})^{\mathbf{2^k}}]^2 - 2 \cdot \mathbf{1^{2^k}} = [(2+\sqrt{\mathbf{3}})^{\mathbf{2^k}} + (2-\sqrt{\mathbf{3}})^{\mathbf{2^k}}]^2 - 2 = \boldsymbol{S_k^2} - 2$

■

Exemplo 2.4

Através do teste de Lucas-Lehmer vamos verificar a primalidade de $M_5 = 2^5 - 1 = 32 - 1 = 31$

Tomando $S_0 = 4$, vamos atualizar o valor da expressão ($S_k^2 - 2$) (mod M_5) 3 vezes:

$S_1 \equiv S_0^2 - 2 (\text{mod } 31)$; $S_0^2 - 2 = 4^2 - 2 = 14$. Logo $S_1 \equiv 14 \text{ (mod } 31)$

$S_2 \equiv S_1^2 - 2 (\text{mod } 31)$; $S_1^2 - 2 = 14^2 - 2 = 194$. Mas $194 \equiv 8 \text{ (mod } 31)$. Logo:

$S_2 \equiv 8 \text{ mod } 31$

$S_3 \equiv S_2^2 - 2 \text{ (mod } 31)$; $S_2^2 - 2 = 194^2 - 2 = 37.634$. Mas $37.634 \equiv 0 \text{ (mod } 31)$

Assim $S_3 \equiv 0 \text{ mod } 31$, ou seja, S_3 é múltiplo de M_5

Portanto M_5 é primo.

Exemplo 2.5

M_{11} = 2^{11} – 1 = 2048 – 1 = 2047, usando o teste de Lucas-Lehmer.

Tomando S_0= 4, atualizando 11 – 2 = 9 vezes a expressão $(S_k^2 - 2)$ (mod M_{11}).

$S_1 \equiv S_0^2 - 2$(mod 2047); S_0^2 - 2 = 4^2 - 2 = 14

$S_2 \equiv S_1^2$ - 2(mod 2047); S_1^2 - 2 = 14^2 - 2 = 194

$S_3 \equiv S_2^2 - 2$(mod 2047); S_2^2 - 2 = 194^2 - 2 = 37.634. Mas 37.634 ≡ 788 (mod 2047). Logo :

$S_3 \equiv$ 788 mod 2047

$S_4 \equiv S_3^2 - 2$(mod 2047); S_3^2 - 2 = 788^2 - 2 = 620.942. Mas 620.942 ≡ 701 (mod 2047). Logo :

$S_4 \equiv$ 701 mod 2047

$S_5 \equiv S_4^2 - 2$(mod 2047); S_4^2 - 2 = 701^2 - 2 = 491.399. Mas 491.399 ≡ 119 (mod 2047). Logo :

$S_5 \equiv$ 119 mod 2047

$S_6 \equiv S_5^2 - 2$(mod 2047); S_5^2 - 2 = 119^2 - 2 = 14.159. Mas 14.159 ≡ 1877 (mod 2047). Logo :

$S_6 \equiv$ 1877 mod 2047

$S_7 \equiv S_6^2 - 2$(mod 2047); S_6^2 - 2 = 1877^2 - 2 = 3.523.127. Mas 3.523.127 ≡ 240 (mod 2047). Logo : $S_7 \equiv$ 240 mod 2047

$S_8 \equiv S_7^2 - 2$(mod 2047); S_7^2 - 2 = 240^2 - 2 = 57.598. Mas 57.598 ≡ 282 (mod 2047). Logo :

$S_8 \equiv$ 282 mod 2047

$S_9 \equiv S_8^2 - 2$(mod 31); S_8^2 - 2 = 282^2 - 2 = 79.522. Mas 79.522 ≡ 1736 (mod 2047). Logo :

$S_9 \equiv$ 1736 mod 2047

Sendo assim, S_9 não é múltiplo de M_{11}

Portanto, o M_{11}não é primo.

Usando esse teste, Lucas mostrou em 1876 que M_{127} é um número primo e M_{67} é composto e alguns anos mais tarde, Pervushin mostrou que M_{61} é primo, e em 1927, Lehmer mostrou que M_{257} é composto

3.5 Números de Mersenne Composto

Uma pergunta que surge é quanto aos números de Mersenne compostos existem?

Teorema 2.4

Sejam $2 \leq a, k \in \mathbb{N}$.

Se $a^k - 1$ for primo, então $a = 2$ e k é primo.

Demonstração

Dessa forma temos:

$$a^k - 1 = (a - 1) \cdot (1 + a + a^2 + \cdots + a^{k-1}),$$

Com $(1 + a + a^2 + \cdots + a^{k-1}) > 1$, pois $k \geq 2$. Ora, se a^{k-1} fôr primo, concluímos $a - 1 = 1$, ou seja, $a = 2$.

Seja $k = rs$ composto com $1 < s \leq r < k$. Então temos a decomposição:

$$2^k - 1 = (2^r - 1) \cdot (1 + 2^r + 2^{2r} + + \cdots + 2^{(8-1)r})$$

Na qual $2^k - 1 > 1$ e $1 + 2^r + 2^{2r} + + \cdots + 2^{(8-1)r} > 1$, pois, $s > 1$. Logo $2^k - 1$ não é primo quando k é composto.

■

Exemplo 2.6

$M_{11} = 2^{11} - 1 = 2048 - 1 = 2047 = 23 \cdot 89$.

Não é primo, apesar de k = 11 é primo.

Sendo assim, podemos construir a tabela com os números primos de Mersenne encontrados desde os antigos gregos até os dias atuais.

4 TABELAS DOS PRIMOS DE MERSENNE

Neste capítulo será abordado todos os números de Mersenne conhecido e seus descobridores, e a história do GIMPS.

4.1 Lista dos Mersenne Conhecidos

Tabela 1 - Listas dos Primos Mersenne e seus descobridores

(continua)

#	$2^p - 1$	Dígitos Em M_p	Ano	Descobridor
1	$2^2 - 1$	**1**	**. . . .**	**. . . .**
2	$2^3 - 1$	**1**	**. . . .**	**. . . .**
3	$2^5 - 1$	**2**	**. . . .**	**. . . .**
4	$2^7 - 1$	**3**	**. . . .**	**. . . .**
5	$2^{13} - 1$	**4**	**1456**	Anônimo
6	$2^{17} - 1$	**6**	**1588**	Cataldi
7	$2^{19} - 1$	**6**	**1588**	Cataldi

Tabela 1 - Listas dos Primos Mersenne e seus descobridores.

(continuação)

8	$\mathbf{2^{31} - 1}$	**10**	**1772**	Euler
9	$\mathbf{2^{61} - 1}$	**19**	**1883**	Pervushin
10	$\mathbf{2^{89} - 1}$	**27**	**1911**	Poderes
11	$\mathbf{2^{107} - 1}$	**33**	**1914**	Poderes
12	$\mathbf{2^{127} - 1}$	**39**	**1876**	Lucas
13	$\mathbf{2^{521} - 1}$	**157**	**1952**	Robinson
14	$\mathbf{2^{607} - 1}$	**183**	**1952**	Robinson
14	$\mathbf{2^{1.279} - 1}$	**386**	**1952**	Robinson
16	$\mathbf{2^{2.203} - 1}$	**664**	**1952**	Robinson
17	$\mathbf{2^{2.281} - 1}$	**687**	**1952**	Robinson
18	$\mathbf{2^{3.217} - 1}$	**969**	**1957**	Gotejar
19	$\mathbf{2^{4.253} - 1}$	**1.281**	**1961**	Hurwitz
20	$\mathbf{2^{4.423} - 1}$	**1.332**	**1961**	Hurwitz
21	$\mathbf{2^{9.689} - 1}$	**2.917**	**1963**	Gillies
22	$\mathbf{2^{9.941} - 1}$	**2.993**	**1963**	Gillies
23	$\mathbf{2^{11.213} - 1}$	**3.376**	**1963**	Gillies
24	$\mathbf{2^{19.937} - 1}$	**6.002**	**1971**	Tuckerman
25	$\mathbf{2^{21.701} - 1}$	**6.533**	**1978**	Noll e Níquel

Tabela 1 - Listas dos Primos Mersenne e seus descobridores.

(continuação)

26	$\mathbf{2^{23.209} - 1}$	**6.987**	**1979**	Noll
27	$\mathbf{2^{44.497} - 1}$	**13.395**	**1979**	Nelson e Slowinski
28	$\mathbf{2^{86.243} - 1}$	**25.962**	**1982**	Esloveno
29	$\mathbf{2^{110.503} - 1}$	**33.265**	**1988**	Colquitt e Welsh
30	$\mathbf{2^{132.049} - 1}$	**39.751**	**1983**	Esloveno
31	$\mathbf{2^{216.091} - 1}$	**65.050**	**1985**	Esloveno
32	$\mathbf{2^{756.839} - 1}$	**227.832**	**1992**	Slowinski e Gage et al.
33	$\mathbf{2^{859.433} - 1}$	**258.716**	**1994**	Slowinski e Gage
34	$\mathbf{2^{1.257.787} - 1}$	**378.632**	**1996**	Slowinski e Gage
35	$\mathbf{2^{1.398.269} - 1}$	**420.921**	**1996**	Armengaud, Woltman, et al (GIMPS).
36	$\mathbf{2^{2.976.221} - 1}$	**895.932**	**1997**	Spence, Woltman, et al (GIMPS).
37	$\mathbf{2^{3.021.377} - 1}$	**909.526**	**1998**	Clarkson, Woltman, Kurowski et al (GIMPS, PrimeNet).
38	$\mathbf{2^{6.972.593} - 1}$	**2.098.960**	**1999**	Hajratwala, Woltman, Kurowski et al (GIMPS, PrimeNet).

Tabela 1 - Listas dos Primos Mersenne e seus descobridores.

(continuação)

39	$\mathbf{2^{13.466.917} - 1}$	**4.053.946**	**2001**	Cameron, Woltman, Kurowski et al (GIMPS, PrimeNet).
40	$\mathbf{2^{20.996.011} - 1}$	**6.320.430**	**2003**	Shafer, Woltman, Kurowski et al (GIMPS, PrimeNet).
41	$\mathbf{2^{24.036.583} - 1}$	**7.235.733**	**2004**	Findley, Woltman, Kurowski et al (GIMPS, PrimeNet).
42	$\mathbf{2^{25.964.951} - 1}$	**7.816.230**	**2005**	Nowak, Woltman, Kurowski et al (GIMPS, PrimeNet).
43	$\mathbf{2^{30.402.457} - 1}$	**9.152.052**	**2005**	Cooper, Boone, Woltman, Kurowski et al (GIMPS, PrimeNet).
44	$\mathbf{2^{32.582.657} - 1}$	**9.808.358**	**2006**	Cooper, Boone, Woltman, Kurowski et al (GIMPS, PrimeNet).
45	$\mathbf{2^{37.156.667} - 1}$	**11.185.272**	**2008**	Elvenich, Woltman, Kurowski et al (GIMPS, PrimeNet).
46	$\mathbf{2^{42.643.801} - 1}$	**12.837.064**	**2009**	Strindmo, Woltman, Kurowski et al (GIMPS, PrimeNet).

Tabela 1 - Listas dos Primos Mersenne e seus descobridores.

(conclusão)

47	$\mathbf{2^{43.112.609} - 1}$	**12.978.189**	**2008**	Smith, Woltman, Kurowski et al (GIMPS, PrimeNet).
48	$\mathbf{2^{57.885.161} - 1}$	**17.425.170**	**2013**	Cooper, Woltman, Kurowski et al (GIMPS, PrimeNet).
49*	$\mathbf{2^{74.207.281} - 1}$	**22.338.618**	**2016**	Cooper, Woltman (prime95), Kurowski e Blosser (PrimeNet), GIMPS et al.
50*	$\mathbf{2^{77.232.917} - 1}$	**23.249.425**	**2017**	Pace, Woltman (prime95), Kurowski e Blosser (PrimeNet), GIMPS et al.
51*	$\mathbf{2^{82.589.933} - 1}$	**24.862.048**	**2018**	Laroche, Woltman (prime95), Blosser (PrimeNet), GIMPS et al.

Fonte: Great Internet Mersenne Prime Search – GIMPS

Dados: Classificação provisória, pois nem todos os candidatos entre M57.885.161 e M82.589.933 foram eliminados

4.2 História do GIMPS

Desde sua fundação em 1996, por George Woltman, o projeto GIMPS – Great Internet Mersenne Prime Search, já descobriu 17 primos de Mersenne, o software que foi executado em sistemas Intel i386 usando código de montagem e ajustados à mão para os cálculos críticos, que tiveram como resultado o código Lucas-Lehmer altamente otimizado.

Com esse código não demorou para o GIMPS ter sua primeira descoberta no mesmo ano, mostrando a eficácia da computação, um esforço coordenado para aproveitar os ciclos de computadores sobressalentes.

Por mais que fosse eficiente o próprio software, nos anos iniciais do GIMPS existia um processo manual que usava e-mails para solicitar atribuições de trabalho e enviar os resultados de volta, porém a medida que o projeto crescia, foi necessário um sistema mais eficiente e então Scott Kurowski com a introdução do PrimeNet por meio de uma empresa chamada Entropia, pioneira nos primeiros dias de projetos de computação distribuída, e sem a contribuição de Scott, que tinha uma capacidade de gerenciar milhares de pessoas por todas as partes do globo terrestre, não teria sido possível.

Com o PrimeNet deu-se um grande avanço para o futuro do projeto como um todo, com a base sólida do PrimeNet, George continuou em melhorar os cálculos básicos do Prime95, entretanto os processadores da Intel e AMD foram introduzidos, George teve que trabalhar com os novos conjuntos de instruções para aumentar o desempenho, dessa forma o núcleo do programa ficou capaz de se otimizar com eficiência máxima em todas as CPUs modernas. Todavia também sendo possível encontrar um lar em muitos sistemas mais antigos.

O projeto sempre faz boletins informativos detalhando todos os trabalhos realizado por seus voluntários espalhados por vários países, caso alguém encontre um primo de Mersenne maior que 100,000,000 dígitos ganha um prêmio de 50,000(USD), existem também outros prêmios que o projeto fornece caso encontre novos primos de Mersenne.

O próximo capitulo é destacado á Marin Mersenne, sua biografia, como ele se destacou numa sociedade, e dentre vários estudiosos da matemática.

5 BIOGRAFIA DE MARIN MERSENNE

Figura 6 – Marin Mersenne

Fonte: https://mathshistory.st-andrews.ac.uk/Biographies/Mersenne/Mersenne_3.jpeg.

Marin Mersenne nasceu em uma pequena cidade de Oizé, em 8 de setembro de 1588, na província de Maine, sua família era descendente de uma classe trabalhadora e foi batizado no mesmo dia, desde muito cedo mostrou-se sinais de devoção e vontade de estudar, mesmo com a situação financeira da família desfavorecida, seus pais o enviaram para o Collége du Mans, onde aprendeu gramática, aos 16 anos, Mersenne pediu para ir pro recém criado Colégio Jesuíta em La Fléche, lugar que também estava matriculado Descartes, que era oito anos mais novo, embora fossem se tornar amigos tempo mais tarde.

O pai de Mersenne desejava que seu filho tivesse uma carreira na igreja, no entanto, Mersenne dedicava-se aos estudos, que adorava, e mostrava-se pronto para as responsabilidades do mundo, então decidiu continuar seus estudos em Paris, partindo para o convento dos Mínimos, essa experiência lhe inspirou de tal maneira, que ele concordou em se juntar à Ordem. Chegando em Paris, frequentou aulas de teologia na Sorbone, onde obteve o grau de Magister Atrium em Filosofia, terminando seus estudos em 1611, foi então que percebeu que estava pronto para a vida calma e estudiosa de um mosteiro.

Depois de dois anos ensinando, foi eleito superior do mosteiro Place Royale em Paris, lugar que permaneceu, exceto por breves viagens, até sua morte em 1648, desde muito cedo ele teve ligações com importantes estudiosos de Paris. Em 1623 ele publicou seus dois primeiros trabalhos consistindo em estudos contra o ateísmo e o ceticismo na França; L’usage de la raison e Análise da vida espiritual.

A matemática foi a área que ele estudou com maior profundidade, e a partir de 1623, ele fez uma seleção cuidadosa de sábios que se reuniam em seu convento ou se correspondiam com ele de toda a Europa e até de lugares tão distantes quanto Constantinopla e Transilvânia.

Seus visitantes regulares ou correspondentes incluíam Peiresc, Gassendi, Descartes, Roberval, Beeckman, Fermat, JB van Helmont, Hobbes, Étienne Pascal e seu filho Blaise Pascal, fez encontros acadêmicos de toda a Europa, durante os quais liam e revisavam artigos científicos, nacionais e internacionais. Esta veio a ser conhecida como Académie Parisiensis e as vezes entre amigos como Académie Mersenne, foi um centro de pesquisa mais engenhosos da época, mesmo com sua saúde debilitada, ele não hesitou em viajar para reuniões com estudiosos de toda a Europa.

Ao longo de sua vida, ele ajudou muitos cientistas em potencial, se tornando um modelo para Huygens, a quem Mersenne tomou sob sua asa e, através de suas cartas, inspirou a Teoria da Música de Huygens, sendo que Mersenne e Huygens nunca se encontraram.

E foi pela insistência de Mersenne, para que Galileu publica-se seu trabalho, dessa forma tornando seu trabalho tão conhecido, outro que deve ser grato pelos conselhos de Mersenne é Pierre Trichet, pois teve sua marca conhecida por todos, o qual teve sucesso na vida científica em Bordeaux e Guyenne, em 1647 Mersenne retornou a Paris.

Mersenne estava ciente de toda a ciência que estava acontecendo, o que todos os cientistas estavam fazendo, Ele estudou a cicloide por vários anos citando sua pesquisa em Quaestiones in Genesim (1623), ele tentou encontrar a área sob a curva por integração, mas falhou, então colocou a questão para Roberval, que em 1638, anunciou que Roberval havia de fato encontrado a área sob a ciclóide.

Entretanto, o nome de Mersenne é mais lembrado pelos primos de Mersenne, já que ele tentou encontrar uma fórmula que representasse todos os primos, embora tenha falhado, seu trabalho com números da forma $2^p - 1$, melhor tive sido de interesse contínuo na investigação de grandes primos. Em 1644 Mersenne afirmou que n é primo se p = 2, 3, 5, 7, 13, 17, 19, 67, 127 e 257, mas composto para os outros 44 primos p menor que 257, mas ao longo dos anos, descobriu que Mersenne estava errado sobre 5 dos primos da forma $2^p - 1$, Drake (1971) tentou entender a fonte e também do trabalho de Mersenne sobre esses primos, e tentar determinar a regra que estava sendo usada, sugerindo que Frenicle de Bessy pode ser a fonte e também sugere que os erros podem ser erros de impressão da impressora.

Em alguns de seus trabalhos não matemáticos, Mersenne analisa permutações e combinações, estabelecendo regras práticas para calcular o número das mesmas, porém sua principal razão para estudar análise combinatória era para otimizar a composição musical como ele explica em O livro da arte de cantar bem, que é o Livro Seis deHarmonia Universal (1636).

Os últimos quatro anos de sua vida, passou muito tempo investigando o barômetro, Pascal já havia provado que o ar não era sem peso, mas foi Mersenne quem descobriu que a densidade do ar era aproximadamente $\frac{1}{19}^{\circ}$ da água, foram feitos vários experimentos que Mersenne estava presente.

Uma questão interessante é como Mersenne conseguiu perseguir livremente suas idéias científicas em sua época, já que a igreja, cujo o mesmo era membro devoto, tinha movido para evitar tais discussão. Segundo Hine (1973 apud O'CONNOR; ROBERTSON,2005).

> Durante a primeira metade do século XVII, o debate sobre a hipótese copernicana se espalhou além das fileiras dos astrônomos e provocou tanta controvérsia que a Igreja decidiu intervir. Em 1616, um corpo de exame teológico concluiu que a idéia do movimento da Terra era filosoficamente falsa e em conflito com as Escrituras, e suspendeu o livro de Copérnico até ser corrigido. Os historiadores geralmente assumem que esta decisão e a subsequente condenação de Galileu teve um efeito tão devastador que o processo científico nos países católicos foi muito retardado. No entanto, a atitude de Mersenne, que era um fiel membro de uma ordem religiosa e uma figura central no desenvolvimento da ciência francesa, não suporta tal conclusão. Um exame da reação de Mersenne ao copernicanismo indica que, por mais perturbadora que fosse a decisão da Igreja, ainda era possível, pelo menos na França, estudar as idéias copernicanas e acha-las úteis, apesar de algumas reservas. Mersenne foi afetado por tais decisões da Igreja, mas menos do que se poderia supor.

Ele nunca desistiu de seu desejo ao longo da vida de avançar a ciência, pois menos após sua morte, em seu testamento, pediu que seu corpo fosse usado para pesquisas biológicas.

O próximo capitulo fala sobre a relação dos primos de Mersenne e os números perfeitos, e os duplos Mersenne.

6 NÚMEROS PERFEITOS E ALGUMAS CONJECTURAS

Parte do interesse em primos de Mersenne deve-se a sua relação com os números perfeitos.

6.1 Números Perfeitos

Muitas culturas antigas dotaram certos números inteiros com significado religioso e mágico especial exemplo são os números perfeitos, que são aqueles inteiros que a soma de seus divisores próprio positivos. O estudioso cristão Agostinho explicou que Deus poderia ter criado o mundo em um instante, mas escolheu fazê-lo em um número perfeito de dias.

Os primeiros comentaristas judeus achavam que a perfeição do universo era demostrada pelo período lunar de 28 dias, enquanto Pierre de Fermat procurava por números perfeitos, ele descobriu o Pequeno Teorema de Fermat.

Definição 5.1

Dados n ∈ ℕ* definimos σ(n) = $\sum_{d \mid n} d$, a soma dos divisores (positivos) de n.

Proposição 5.1

Se M_P é um primo de Mersenne então $2^{p-1}M_p$ é perfeito. Além disso, todo número perfeito par é da forma $2^{p-1}M_p$ para algum primo p, sendo M_p um primo de Mersenne.

Demonstração 5.1

Se M_p é primo então

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

Por outro lado seja $n = 2^k b$, com $k > 0$ e b ímpar, um número perfeito par. Temos:

$\sigma(n) = 2n = \sigma(2^k)\,\sigma(b)$ donde $2^{k+1}b = (2^{k+1} - 1)\sigma(b) \geq (2^{k+1} - 1) \cdot (b + 1)$, valendo a igualdade apenas se b for primo. Desta desigualdade temos $b \leq (2^{k+1} - 1) \mid b$ e $2^{k+1} - 1 \leq b$.

Assim $b = 2^{k+1} - 1$ e $(2^{k+1} - 1)\sigma(b) = \sigma(n) = 2n = 2^{k+1}b = (2^{k+1} - 1) \cdot (b + 1)$, donde $\sigma(b) = (b + 1)$, e portanto b é primo. Como $p = K + 1$ é primo, $b = M_p$ e $n = 2^{p-1}M_p$.

■

Exemplo 5.1

Os três primeiros números perfeitos são:

$6 = 1 + 2 + 3$,

$28 = 1 + 2 + 4 + 7 + 14$, e

$496 = 1 + 2 + 4 + 8 + 16 + 31 + 62 + 124 + 248$

Por outro lado, um dos problemas em aberto mais antigos da matemática é o da existência de números perfeitos ímpares, acredita-se apenas que um número perfeito ímpar, se existir, deve ser muito grande (com mais de 300 algarismos) e satisfaz simultaneamente várias condições complicadas.

6.1.1. Outros Perfeitos

Tabela 2 – Todos os números perfeitos encontrados.

(continua)

##	$2^{p-1}M_p$	##	$2^{p-1}M_p$	##	$2^{p-1}M_p$
1	$2^1 \cdot (2^2 - 1)$	**8**	$2^{30} \cdot (2^{31} - 1)$	**15**	$2^{1.278} \cdot (2^{1.279} - 1)$
2	$2^2 \cdot (2^3 - 1)$	**9**	$2^{60} \cdot (2^{61} - 1)$	**16**	$2^{2.202} \cdot (2^{2.203} - 1)$
3	$2^4 \cdot (2^5 - 1)$	**10**	$2^{88} \cdot (2^{89} - 1)$	**17**	$2^{2.280} \cdot (2^{2.281} - 1)$
4	$2^6 \cdot (2^7 - 1)$	**11**	$2^{106} \cdot (2^{107} - 1)$	**18**	$2^{3.217} \cdot (2^{3.217} - 1)$
5	$2^{12} \cdot (2^{13} - 1)$	**12**	$2^{126} \cdot (2^{127} - 1)$	**19**	$2^{4.452} \cdot (2^{4.453} - 1)$
6	$2^{16} \cdot (2^{17} - 1)$	**13**	$2^{520} \cdot (2^{521} - 1)$	**20**	$2^{4.422} \cdot (2^{4.423} - 1)$
7	$2^{18} \cdot (2^{19} - 1)$	**14**	$2^{606} \cdot (2^{607} - 1)$	**21**	$2^{9.688} \cdot (2^{9.689} - 1)$

Tabela 2 – Todos os números perfeitos encontrados.

(conclusão)

##	$2^{p-1}M_p$	##	$2^{p-1}M_p$	##	$2^{p-1}M_p$
22	$2^{9.940} \cdot (2^{9.941} - 1)$	**32**	$2^{756.838} \cdot (2^{756.839} - 1)$	**42**	$2^{25.964.950} \cdot (2^{25.964.951} - 1)$
23	$2^{11.212} \cdot (2^{11.213} - 1)$	**33**	$2^{859.432} \cdot (2^{859.433} - 1)$	**43**	$2^{30.402.456} \cdot (2^{30.402.457} - 1)$
24	$2^{19.936} \cdot (2^{19.937} - 1)$	**34**	$2^{1.257.786} \cdot (2^{1.257.787} - 1)$	**44**	$2^{32.582.656} \cdot (2^{32.582.657} - 1)$
25	$2^{21.700} \cdot (2^{21.701} - 1)$	**35**	$2^{1.398.268} \cdot (2^{1.398.269} - 1)$	**45**	$2^{37.156.666} \cdot (2^{37.156.667} - 1)$
26	$2^{23.208} \cdot (2^{23.209} - 1)$	**36**	$2^{2.976.220} \cdot (2^{2.976.221} - 1)$	**46**	$2^{42.643.800} \cdot (2^{42.643.801} - 1)$
27	$2^{44.498} \cdot (2^{44.497} - 1)$	**37**	$2^{3.021.376} \cdot (2^{3.021.377} - 1)$	**47**	$2^{43.112.608} \cdot (2^{43.112.609} - 1)$
28	$2^{86.242} \cdot (2^{86.243} - 1)$	**38**	$2^{6.972.592} \cdot (2^{6.972.593} - 1)$	**48**	$2^{57.885.160} \cdot (2^{57.885.161} - 1)$
29	$2^{110.502} \cdot (2^{110.503} - 1)$	**39**	$2^{13.466.916} \cdot (2^{13.466.917} - 1)$	**49**	$2^{74.207.280} \cdot (2^{74.207.281} - 1)$
30	$2^{132.048} \cdot (2^{132.049} - 1)$	**40**	$2^{20.996.010} \cdot (2^{20.996.011} - 1)$	**50**	$2^{77.232.916} \cdot (2^{77.232.917} - 1)$
31	$2^{261.090} \cdot (2^{216.091} - 1)$	**41**	$2^{24.036.582} \cdot (2^{24.036.583} - 1)$	**51**	$2^{82.589.932} \cdot (2^{82.589.933} - 1)$

Fonte: Great Internet Mersenne Prime Search – GIMPS

6.1.2. Números Multiperfeitos

Devido ao estudo dos números perfeitos, outros estudos se iniciaram, sendo o caso dos números Multiperfeitos, um número n é k-multiperfeito (também chamado de k-multiplicado número perfeito ou k-multiperfeito número) se

$\sigma(n) = k \cdot n$

Para algum inteiro k> 2, onde σ(n) é a função divisora. O valor de k é chamado de classe. O caso especial k = 2 corresponde aos números perfeitos P_2. O número 120 já era conhecido há muito tempo por ser 3-multiplicado perfeito (P_3).

$$\sigma(120) = 3 \cdot 120$$

6.1.3. Número Duplo Mersenne

Um número de Mersenne duplo é um número da forma

$$M_{M_n} = 2^{2^n-1} - 1,$$

onde M_n é um número de Mersenne, os primeiros duplos de Mersenne são 7, 127, 32767 e outros. Os números de Double Mersenne são primos para n = 2, 3, 5, 7. O status de todos os números duplos de Mersenne é desconhecido, M_{M61} sendo o menor caso não resolvido, pois esse número tem 694.127.911.065.419.642 dígitos, é muito grande para que o teste usual de Lucas-Lehmer seja prático, o único método possível de determinar o status desse número é encontrar divisores pequenos. T. Forbes organizou uma pesquisa distribuída, mas, nenhum fator foi encontrado.

6.2 Conjecturas

6.2.1 Conjectura

Não existe nenhum número perfeito ímpar.

6.2.2 Conjectura dos Números Primos Gêmeos

A conjectura dos números primos gêmeos, veio de uma fonte totalmente inesperada, um matemático sino-americano, professor da Universidade de New Hampshire, um especialista no ramo da Teoria dos números, ele submeteu seu artigo a uma revista, alegando ter dado um importante passo em direção a solução da conjectura, vale lembrar que damos o nome de primos gêmeos ao par de números primos que diferem de apenas 2 unidades. Sabendo disso conjectura-se que eles sejam infinitos, entretanto a demonstração para isso ainda não foi alcançada. O trabalho de Yitang-Zhang mostrou domínio sobre o assunto, e diante de um auditório lotado em Harvard, ele mostrou seu trabalho, ele não havia chagado a demostrar a conjectura dos números

primos gêmeos, mas conseguiu provar que existe uma quantidade infinita de primos que diferem de no máximo 70 milhões.

Ressaltando que o trabalho que o professor demostrou, não era um método totalmente novo, e apenas tinha insistido em métodos que já haviam sido testados, mas com mais persistência do que seus predecessores.

6.2.3 Conjectura de Goldbach

O matemático prussiano Christin Goldbach fez uma afirmação, “Parece... que todo número maior do que 2 é a soma de três números primos”, em uma de suas cartas destinadas a Euler, no ano 1742, sendo que Euler respondeu: “... todo inteiro par a é uma soma de dois primos. Eu tenho isso como certamente um teorema, embora não possa prova-lo”.

Através dessas trocas de cartas surgiu um dos maiores mistérios da teoria dos números, a conjectura de Goldbach, que foi testada e verificada verdadeira para todo

$$n \leq 4 \cdot 10^{18},$$

mas para a qual ainda não existe solução definitiva.

Exemplo 5. 2

$6 = 3 + 3$; $8 = 3 + 5$; $10 = 3 + 7$; $12 = 5 + 7$; $14 = 7 + 7$; $16 = 5 + 11$; $\cdots$; $200 = 3 + 197 = 7 + 193 = 19 + 181 = 37 + 163 = 43 + 157 = 61 + 139 = 73 + 127 = 97 + 103$; $\cdots$

Para Goldbach o número 1 era considerado primo, logo não havia problema para provar sua afirmação para os números 3, 4 e 5. Mas com a exclusão do número 1 como número primo acabou fazendo com que a conjectura fosse a ser conhecida em duas versões, sendo elas uma forte e uma fraca:

A versão fraca diz: Todo inteiro ímpar maior do que 5 pode ser escrito como a soma de 3 primos;

A versão forte diz: Todo número par maior do que 2 pode ser escrito como a soma de dois primos.

Mas devido essa diferença, acontece que uma vez provada a versão forte, a fraca resulta como um corolário, enquanto que o contrário não é verdade.

6.2.4 A música dos números primos

A conjectura proposta por Riemann diz que todos os zeros não triviais da função zeta têm parte real igual $\frac{1}{2}$, e é hoje conhecida como hipótese de Riemann. Essa afirmação parece não ter relação alguma com números primos, mas uma outra descoberta de Riemann foi de uma função R(x), que estima a quantidade de primos menores que x, sendo ainda melhor que a integral logarítmica de Gauss, e que poderia ser melhorada até a perfeição caso se todos os zeros da função zeta fossem conhecidos.

Riemann descobriu que, quando calculada em seus zeros, a função zeta gera ondas senoidais semelhantes a notas musicais, e que a função R(x) se torna cada vez mais próxima de π(x) conforme somamos mais e mais as senoides geradas pelos zeros.

Caso se prove a hipótese de Riemann, a tarefa de encontrar todos os zeros da função zeta se torna um pouco mais fácil, gerando assim um avanço significativo em direção a função π(x).

6.3 Criptografia RSA

O conceito de sistema de criptografia com chave pública (ou criptografia assimétrica) foi uma proposta para solucionar um problema, que veio com o crescimento da computação e da internet, sendo que o sistema é composto por duas chaves, uma inversa da outra. Dessa forma deixando inviável computacionalmente a determinação de uma chave a partir da outra, uma das chaves é disponibilizada ao público (chave pública) e a outra fica em segredo (chave privada), para que não exista risco à segurança do código.

Com o conceito de sistema de criptografia com chave pública, era necessário um método de criptografia assimétrica que fosse computacionalmente mais rígido. Rivest, Shamir e Adleman que desenvolveram um método de criptografia, chamado de criptografia RSA, que utiliza a teoria dos números inteiros desenvolvidas por grandes matemáticos como Fermat, Euler, Gauss.

Na criptografia RSA a chave pública e a chave privada são compostas por dois números naturais cada (e, n) e (d, n), onde n é o produto de dois primos, e d, e satisfazem determinadas relações. Portanto para obter a chave privada a partir da pública basta que fatoremos o número natural n, o que torna inviável tentar decodificar mensagens criptografas e através desse sistema pode-se garantir o sigilo da mensagem.

6.3.1 A matemática por trás da criptografia RSA

No primeiro momento são escolhidos valores para os caracteres, em seguida, selecionamos dois números primos p e q. Dessa forma obtemos n = pq, esse n é o tamanho do conjunto, pois é necessário um conjunto finito de valores para fazer o caminho inverso quando for realizado a cifrar da mensagem.

Deve-se calcular a função totiente, ou $\varphi(x)$ de Euler, ela revela a quantidade de Co-primos de um número que são menores que ele mesmo, ressaltando que Co-primos ou Números primos entre si, é quando dois números são primos entre si, ou seja, o máximo divisor comum (MDC) entre eles é 1, dessa forma temos:

$$\varphi(x) = (p - 1) \cdot (q - 1),$$

Dessa forma podemos calcular a chave pública que deve ser um número e em que 1< e < $\varphi(x)$, sendo que e seja Co-primo de $\varphi(x)$, ou seja, que seja um MDC ($\varphi(x)$, e) = 1, com e > 1.

Utilizando-se da aritmética modular, é aplicado uma formula,

$$c = m \wedge e \bmod n,$$

Onde e é a chave pública e m é o valor numérico da letra e c é o valor numérico da letra cifrada e para calcular a chave privada, é necessário encontrar o inverso multiplicativo do número e, podendo utilizar o algoritmo de Euclides estendido, e para decifrar basta aplicar uma exponenciação modular para o valor de cada letra, dessa forma obtemos a seguinte fórmula:

$$m = c \wedge d \bmod n,$$

Onde d é a chave privada, n é o tamanho do conjunto e c é o valor numérico da letra cifrada.

Por todos esses cálculos envolvidos, fica claro que a criptografia em segurança virtual é uma forma de proteger informações privadas de serem roubadas ou comprometidas, e nos dias atuais ela tem sido fundamental em criptografar dados que ficam em sistemas de nuvem, pois cada vez usuários e organizações utilizam dessa tecnologia.

Diante deste trabalho faço minhas conclusões e perspectivas, evidenciando alguns pontos de extrema importância para o tema abordado até aqui.

7 CONCLUSÕES E PERSPECTIVAS

Considerando que a matemática desempenha um papel importante na formação do cidadão, na inserção do indivíduo no mundo do trabalho, da relação social e cultural (PCNs 2001, p. 29), e diante da complexidade do tema abordado mesmo que de uma forma superficial, visando as origens e definições dos números primos e por consequência dos primos de Mersenne, é notável o fascínio provocado por estes números tão misteriosos, que há séculos vem desafiando matemáticos e apaixonados pela ciência, ao ponto de movimentar a sociedade em qual vivia, que foi o caso de Marin Mersenne.

A realização deste trabalho mostrou-se de grande interesse, devido que esse assunto abordado sempre foi um tópico que tive uma grande vontade de explorar, assim como grandes matemáticos e estudiosos que vieram antes de mim. Trabalhar com números de Mersenne e o Teste de Lucas-Lehmer me fez revisar assuntos e conceitos dentro da Teoria dos números.

Todavia, é necessário um conhecimento de matemática avançada para ter um maior aprofundamento, nos assuntos que envolvem números primos, mesmo com algumas tentativas de simplificar o tema em questão, para que fique mais compreensível aos alunos de forma em geral.

Dessa forma fica evidente o interesse em fazer uma atividade de aperfeiçoamento com professores, afim de agregar novos conhecimentos para os mesmos e estimular a discussão sobre novas formas de desenvolver o assunto exposto, visto que antes os números primos não tinham uma aplicação imediata, e nos dias atuais com o desenvolvimento das tecnologias, houve a necessidade de proteger os dados dos usuários, através da criptografia RSA, e como foi visto ela usa números primos, e como foi mencionado quanto maior for o número primo, mais eficiente é a criptografia, dessa maneira fica evidente a busca por números primos de Mersenne.

REFERÊNCIAS

ANDRADE, Doherty. **Números Primos e Números de Mersenne**. Disponível em http://www.dma.uem.br/kit/jeepema-1/art3_1801.pdf. Acesso em 23 novembro 2021.

ANDRADE, Ricardo Pereira de. **Testes de Primalidade:** Uma Análise Matemática dos Algoritmos Determinísticos e Probabilístico. 2017. 52 f. Dissertação (Curso de Mestrado Profissional de Pós-Graduação em Matemática – PROFMAT). Universidade Federal do Ceará, Fortaleza, 2017.

ARAÚJO, Gabriel; BERNARDI, Matheus; GOMES, Daniel; GOMES, Lucas; GOUVEIA, Maico, **Primos de Fermat, Primos de Mersenne, Números Perfeitos e O Fatorial**. São Paulo: IMECC, 2017. 9 p.

BATEMAN, P. T., et al. "**The Editor's Corner: The New Mersenne Conjecture**" The American Mathematical Monthly, vol. 96, no. 2, 1989, pp. 125–28. JSTOR, Disponível em https://www.jstor.org/stable/2323195?read-now=1&refreqid=excelsior%3Ab7fb5cc336fdd8893a7c732f52785861&seq=1. Acesso em 26 Maio. 2022.

BRASIL, **Parâmetros Curriculares Nacionais: Matemática/Ministério da Educação**. Secretaria da Educação Fundamental. 3. Ed. Brasília: A Secretaria, 2001. 142 p.

BOYER, C. B, MERZBACH, U. C. **História da Matemática**; Tradução de Helena Castro. São Paulo: Blucher, 2012.

CALDWELL, C. K., **The Largest Known Primes**: A summary, 1994. Disponível em https://primes.utm.edu/largest.html. Acesso em 10 outubro 2021.

GUSMÃO, Gustavo. Porque a descoberta do maior número primo da história importa? **Exame.com**, São Paulo, 20 Jan 2019. Disponível em https://exame.com/ciencia/por-que-a-descoberta-do-maior-numero-primo-da-historia-importa. Acesso em 23 novembro 2021.

Great Internet Mersenne Prime Search - PrimeNet. Mersenne.org. Disponível em: https://www.mersenne.org/. Acesso em: 03 outubro. 2021.

KARPERSKY. **O que é criptografia de dados? Definição e explicação.** Disponível em https://www.kaspersky.com.br/resource-center/definitions/encryption. Acesso em 20 junho 2022.

LIMA, Elon Lages. O Princípio da Indução. **Universidade de Coimbra – Departamento de Matemática.** Rio de Janeiro, 1987. Disponível em http://www.mat.uc.pt/~mat0829/A.Peano.htm. Acesso em 30 junho 2022

MARTINEZ, Fábio; MOREIRA, Carlos; SALDANHA, Nicolau; TENGAN, Eduardo; **Teoria dos Números**: Um passeio com primos e outros números familiares pelo mundo inteiro. 2ª ed. Rio de Janeiro: IMPA, 2010. 450 p.

MAIER, Rudolf. **TEORIA DOS NÚMEROS: Texto de aula Versão atualizada 2005.** UNIVERSIDADE DE BRASÍLIA DEPARTAMENTO DE MATEMÁTICA -IE. Brasília, 2005. Disponível em: https://www.mat.unb.br/~maierr/tnotas.pdf. Acesso em 30 junho 2022

MORIMOTO, Ricardo. **Números Primos**: Propriedades, Aplicações e Avanços. 2014. 65 f. Dissertação (Programa de Pós-Graduação – Mestrado Profissional em Matemática) – Universidade Estadual Paulista " Júlio de Mesquita Filho", Rio Claro, 2014.

O'CONNOR, J. J., ROBERTSON, E. F., **Marin Mersenne - Biography**. Maths History. Disponível em https://mathshistory.st-andrews.ac.uk/Biographies/Mersenne/ Acesso em 15 maio 2022.

OLIVEIRA, Fernando. Entendendo (de verdade) a criptografia RSA, **Lambda3.com**, São Paulo, 10 dezembro 2012. Disponível em https://www.lambda3.com.br//2012/12/entendendo-de-verdade-a-criptografia-rsa. Acesso em 12 junho 2022.

PEREIRA, Ledina Lentz. **Primalidade e Polinômios de Chebyshev**. 2000. 108 f. Dissertação (Programa de Pós-Graduação em Matemática Aplicada – Mestre em Matemática Aplicada) – Universidade Federal do Rio Grande do Sul, Porto Alegre,2000.

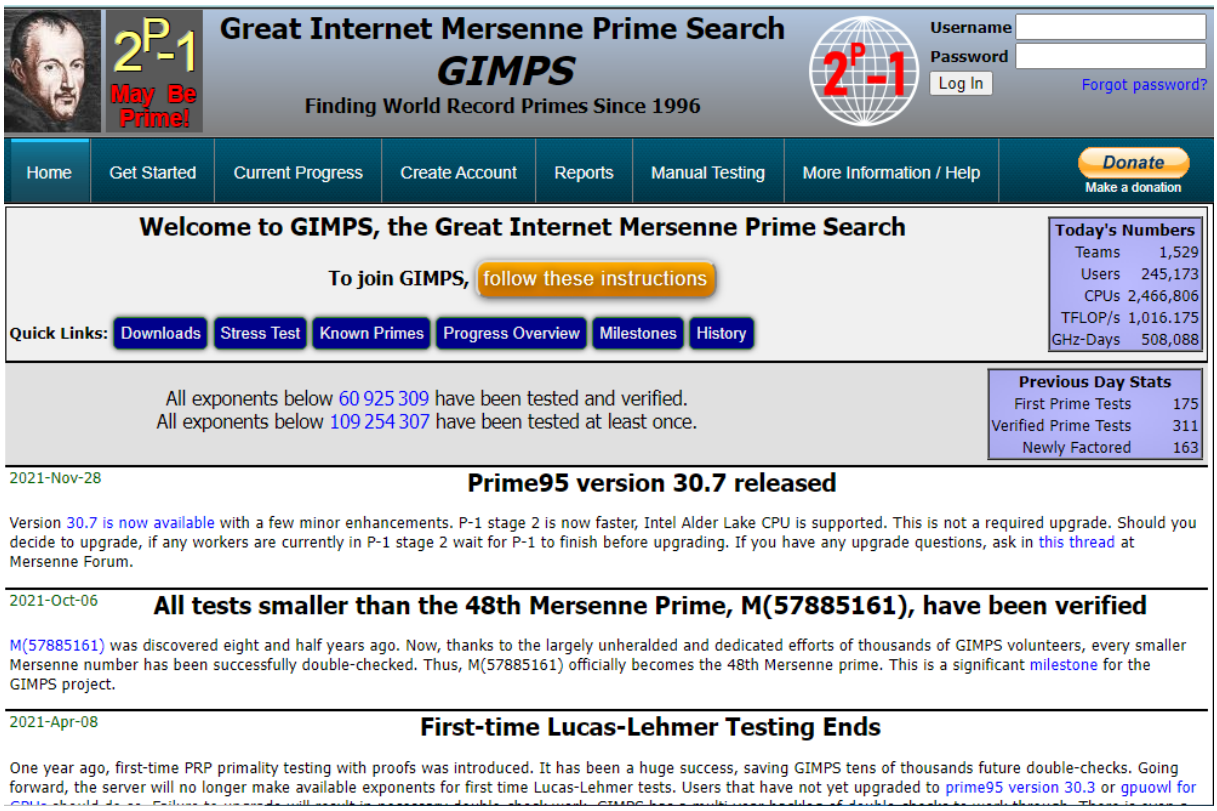
RIZEL, Ary Camargo; **Números Primos**. Belo Horizonte: ICEX da Universidade Federal de Minas Gerais, 2014. 60 p., Disponível em https://repositorio.ufmg.br/bitstream/1843/EABA-9REL7B/1/monografia_ary.pdf. Acesso em 09 abril 2022

WEISSTEIN, Eric W., **Teste Lucas-Lehmer**, De MathWorld – Um recurso da web da wolfram. Disponível em https://mathworld.wolfram.com/Lucas-LehmerTest.html. Acesso em 22 novembro 2021.

ANEXO A – O GIMPS

O GIMPS - Great Internet Mersenne Prime Search é um site bem intuitivo, mostra os avanços desde sua criação em 1996, explica como podemos fazer parte do projeto e esclarece todas as dúvidas que são geradas, e também fornece os valores que cada pessoa ganhará caso encontre novos primos de Mersenne. Desde sua criação o site sempre passa por novas atualizações, vale lembrar que todo esse projeto com toda sua estrutura está operando em nível mundial.

Figura A1 – Interface do site do GIMPS



Fonte: Autoria própria