UNIVERSIDADE ESTADUAL DO CEARÁ

CENTRO DE CIÊNCIAS E TECNOLOGIA

PROGRAMA DE PÓS-GRADUAÇÃO EM MATEMÁTICA

MESTRADO PROFISSIONAL EM MATEMÁTICA EM REDE NACIONAL

MARDNEY FERREIRA DE CASTRO

O ESTUDO DA PROFICUIDADE DOS NÚMEROS PRIMOS DE SOPHIE GERMAIN

FORTALEZA – CEARÁ

2023

MARDNEY FERREIRA DE CASTRO

O ESTUDO DA PROFICUIDADE DOS NÚMEROS PRIMOS DE SOPHIE GERMAIN

Dissertação apresentada ao Curso de Mestrado Profissional em Matemática em Rede Nacional do Programa de Pós-Graduação em Matemática do Centro de Ciências e Tecnologia da Universidade Estadual do Ceará, como requisito parcial à obtenção do título de mestre em Matemática em Rede Nacional. Área de Concentração: Matemática.

Orientador: Prof. Dr. Léo Ivo da Silva Souza

FORTALEZA – CEARÁ

2023

Dados Internacionais de Catalogação na Publicação
Universidade Estadual do Ceará
Sistema de Bibliotecas
Gerada automaticamente pelo SidUECE, mediante os dados fornecidos pelo(a)

Castro, Mardney Ferreira de.
O estudo da proficuidade dos números primos de Sophie Germain [recurso eletrônico] / Mardney Ferreira de Castro. - 2023.
57 f. : il.

Dissertação (mestrado profissional) - Universidade Estadual do Ceará, Centro de Ciências e Tecnologia, Curso de Mestrado Profissional Em Matemática Rede Nacional - Profissional, Fortaleza, 2023.
Orientação: Prof. Dr. Leo Ivo da Silva Souza.
1. números primos. 2. Sophie Germain. 3. teorema de Fermat.. I. Título.

MARDNEY FERREIRA DE CASTRO

O ESTUDO DA PROFICUIDADE DOS NÚMEROS PRIMOS DE SOPHIE GERMAIN

Dissertação apresentada ao Curso de Mestrado Profissional em Matemática do Programa de Pós-Graduação em Matemática do Centro de Ciências e Tecnologia da Universidade Estadual do Ceará, como requisito parcial à obtenção do título de mestre em Matemática em Rede Nacional. Área de Concentração: Matemática.

Aprovada em: 27 de julho de 2023.

BANCA EXAMINADORA

Léo Ivo da Silva Souza

Prof. Dr. Léo Ivo de Silva Souza (Orientador)

Universidade Estadual do Ceará – UECE

Prof. Dr. Marcos Ferreira de Melo

Universidade Federal do Ceará – UFC

Prof. Dr. Diego Sousa Rodrigues

Instituto Federal de Educação, Ciência e Tecnologia do Ceará – IFCE

A Deus que é fiel para cumprir os Seus propósitos em minha vida.

AGRADECIMENTOS

A Deus que me ajudou a escrever este trabalho.

À minha família, meus pais e irmãos, que contribuíram mesmo que indiretamente para a conclusão deste trabalho.

Aos meus melhores amigos, que estão sempre me apoiando e incentivando.

Ao meu professor orientador, Dr. Léo Ivo da Silva Souza pela orientação e empenho.

Aos membros da banca examinadora, Prof. Dr. Marcos Ferreira de Melo e Prof. Dr. Diego Sousa Rodrigues, pelas valiosas colaborações e sugestões.

Aos professores do curso Prof. Dr. Nicolas Alcântara de Andrade e Prof. Dr. Tiago Caúla Ribeiro por todo o conhecimento compartilhado durante esses dois anos de curso.

Aos meus colegas da turma PROFMAT UECE – 2021: Artur Teixeira, Danilo Magalhães, Felipe Guimarães, Rafael Abreu, Rafael Mendonça, Sérgio Augusto, Tiago Nobre e Wellington Sampaio, por todos os momentos e risadas. Vencemos esta etapa!

À Universidade Estadual do Ceará por ser responsável pela minha formação acadêmica.

Obrigado a todos!

“Pouco importa quem chega primeiro a uma ideia, o que importa é o quão longe você pode levar essa ideia”.

(Sophie Germain)

RESUMO

Sophie Germain foi uma notável matemática francesa que fez descobertas interessantes nos ramos da Matemática e da Física, que serviram de base para que outros matemáticos pudessem utilizá-las com o passar dos anos. O presente trabalho tem como objetivo apresentar um pequeno resumo sobre os números primos de Sophie Germain e sua aplicabilidade em diferentes áreas da matemática, um assunto que tem atraído muitos matemáticos desde o princípio, e ainda hoje apresenta muitos desafios. E como objetivos específicos apresentar a importância dos números primos de Sophie Germain para história dos números; elencar sua aplicabilidade dentro da Matemática; e salientar sua significância no contexto pedagógico dos números primos. Nesse estudo apresenta-se uma breve descrição histórica dos números primos, assim como um pouco da vida de Sophie Germain. Relata também os conceitos fundamentais, demonstrações clássicas da integração de números primos de Sophie Germain, teoremas e suas relações de verossimilhanças com os números primos de Sophie Germain, e um pequeno relato histórico dos estudos sobre a sua distribuição e sua aplicabilidade, como também a relação entre os números primos de Sophie Germain e o Último Teorema de Fermat. Para tanto a metodologia aplicada foi a pesquisa qualitativa, baseando-se em livros, artigos, dissertações entre outros. Buscando assim o entendimento para essa pesquisa.

Palavras-chave: números primos; Sophie Germain; teorema de Fermat.

ABSTRACT

Sophie Germain was a remarkable French mathematician who made interesting discoveries in the fields of Mathematics and Physics, which served as a basis for other mathematicians to use over the years. The present paper aims to present a short summary about Sophie Germain's prime numbers and their applicability in different areas of mathematics, a subject that has attracted many mathematicians from the beginning, and still today presents many challenges. And as specific objectives to present the importance of Sophie Germain's prime numbers for the history of numbers; list its applicability within Mathematics; and highlight its significance in the pedagogical context of prime numbers. This study presents a brief historical description of prime numbers, as well as a bit of Sophie Germain's life. It also reports the fundamental concepts, classic demonstrations of Sophie Germain's integration of prime numbers, theorems and their likelihood relations with Sophie Germain's prime numbers, and a short historical account of studies on their distribution and applicability, as well as the relationship between Sophie Germain's prime numbers and Fermat's Last Theorem. Therefore, the applied methodology was qualitative research, based on books, articles, dissertations, among others. Thus seeking understanding for this research.

Keywords: prime numbers; Sophie Germain; Fermat's theorem.

LISTA DE FIGURAS

Figura 1 – O abacista versus o alegorista..... 17
Figura 2 – Evolução dos números indo-arábico..... 18
Figura 3 – Osso de Ishango..... 19
Figura 4 – Representação gráfica do Osso de Ishango..... 20
Figura 5 – Crivo de Eratóstenes de 1 a 100..... 21
Figura 6 – Quadrinho Primos Gêmeos..... 23
Figura 7 – Imagem de Sophie Germain..... 27
Figura 8 – A história da matemática de Jean-Étienne Montucla..... 28
Figura 9 – Pintura "*La Mort d'Archimède*"..... 28
Figura 10 – Livro *Cours de mathématiques*, 1798 de Étienne Bézout..... 29
Figura 11 – Os vinte primeiros primos de Sophie Germain..... 31

LISTA DE TABELAS

Tabela 1 – Maiores pares de primos gêmeos conhecidos..... 24
Tabela 2 – Os trinta menores pares de primos gêmeos..... 25
Tabela 3 – $S_{2,1}(x)$ dos números primos de Sophie Germain inferiores a x... 32
Tabela 4 – Os dez maiores números primos de Sophie Germain..... 33

LISTA DE ABREVIATURAS E SIGLAS

DIP	Domínio de Ideais Principais
DFU	Domínio de Fatoração Única
UTF	Último Teorema de Fermat
SCR	Sistema Completo de Resíduos
SRR	Sistema Reduzido de Resíduos
TSG	Teorema de Sophie Germain

LISTA DE SÍMBOLOS

$\mathbb{N}$	Conjunto dos números Naturais
$\mathbb{Z}$	Conjunto dos números Inteiros
$\mathbb{Q}$	Conjunto dos números Racionais
$\in$	Pertence
$>$	Maior que
$<$	Menor que
$\leq$	Menor que ou igual a
$\geq$	Maior que ou igual a
$=$	Igual a
$\neq$	Diferente de
$\lvert\ \rvert$	Módulo
$\equiv$	Congruente a
$\sum$	Somatório
$\nmid$	Não divide
$\mid$	Divide
$\subset$	Está contido
$\cap$	Intersecção
$\emptyset$	Conjunto vazio

SUMÁRIO

1 INTRODUÇÃO..... 14
2 UM VISLUMBRE DA HISTÓRIA DA MATEMÁTICA..... 16
2.1 Números primos..... 18
2.1.1 O crivo de Eratóstenes..... 20
2.1.2 Teorema Fundamental da Aritmética..... 22
2.1.3 Números primos gêmeos..... 23
2.1.3.1 Brun e os primos gêmeos..... 25
3 SOPHIE GERMAIN, A MATEMÁTICA FRANCESA..... 27
3.1 Números primos de Sophie Germain..... 31
3.2 Identidade de Sophie Germain..... 34
3.3 O Teorema de Sophie Germain e o Teorema de Fermat..... 35
3.4 Teoria dos Resíduos Quadráticos..... 37
3.5 Equações diofantinas..... 39
4 METODOLOGIA..... 41
4.1 Delineamento da pesquisa..... 42
5 RESULTADO E DISCUSSÕES..... 44
5.1 Contribuição de Sophie Germain para a resolução do Último Teorema de Fermat..... 44
5.2 Equações diofantinas e aplicabilidade..... 45
5.3 A Teoria dos Resíduos Quadráticos com os primos de Sophie Germain..... 46
5.4 Primos gêmeos e primos de Sophie Germain..... 47
5.5 Aplicabilidade dos primos de Sophie Germain no meio avaliativo 48
6 CONSIDERAÇÕES FINAIS..... 52
REFERÊNCIAS..... 53

1 INTRODUÇÃO

Os números primos são importantes em muitos ramos da matemática e das ciências em geral. Algumas das razões pelas quais os números primos são importantes estão ligadas a base da teoria dos números. Na verdade, os matemáticos têm se interessado por números primos desde os tempos antigos, e o estudo dos números primos levou a alguns dos maiores avanços da matemática.

Hoje, os números primos são essenciais na criptografia, pois são usados para gerar chaves criptográficas, já que devido fatorar números grandes em primos é muito difícil portanto, os números primos são uma ferramenta importante na segurança das comunicações modernas.

Os números primos também são importantes na teoria da computação, pois são usados em algoritmos para encontrar números primos, fatorar números grandes e gerar números aleatórios. Além de aparecer na física, por exemplo, na teoria da relatividade de Einstein e na teoria das cordas.

Este trabalho tem como objetivo apresentar um pequeno resumo sobre os números primos de Sophie Germain e sua aplicabilidade em diferentes áreas da matemática. E como objetivos específicos apresentar a importância dos números primos de Sophie Germain para história dos números; elencar sua aplicabilidade dentro da Matemática; e salientar sua significância no contexto pedagógico dos números primos.

Os primos de Sophie Germain são encontrados através da fórmula “2p + 1”, onde p é um número primo, caso o resultado seja outro número primo então p é chamado de primo de Sophie Germain. Esses números foram nomeados em homenagem a Sophie Germain, uma matemática francesa do século XVIII que fez importantes contribuições para a teoria dos números.

Os primos de Sophie Germain são interessantes porque eles estão relacionados com a conjectura de Goldbach, que afirma que todo número par maior que 2 pode ser escrito como a soma de dois números primos. Se essa conjectura for verdadeira, então todo número ímpar maior que 5 pode ser escrito como a soma de três números primos, no qual um desses primos pode ser de Sophie Germain.

Os primos de Sophie Germain também têm aplicações na criptografia de chave pública, onde são usados na construção de chaves seguras. Eles são

particularmente úteis na construção de chaves RSA seguras, pois permitem que a chave privada seja mantida secreta, mesmo se a chave pública for conhecida.

Este trabalho segue a metodologia qualitativa quanto a natureza da pesquisa, assim como quanto aos objetivos da pesquisa exploratória, onde a técnica de coleta de dados empregada foi a pesquisa bibliográfica.

No capítulo 1 tem-se uma narrativa da importância dos números primos para a sociedade e as primeiras contribuições de Sophie Germain. O capítulo 2 trata dos fatos históricos, faz-se uma síntese da História da Matemática envolvendo números primos, crivo de Eratóstenes, Teorema Fundamental da Aritmética e números primos gêmeos nos quais esses assuntos foram suporte ao entendimento das demonstrações apresentadas e à realização das atividades propostas.

O capítulo 3 centra-se na história e teorias de Sophie Germain, a matemática francesa. Logo depois, apresentam-se, detalhadamente, as etapas da demonstração, a fim de que, idealmente, o leitor possa refazê-las sozinho. Levantam-se ainda aspectos histórico-matemáticos, que abrangem a conjectura inicial, a elaboração das primeiras provas e a demonstração final. O capítulo 4 apresenta a metodologia da pesquisa com um resumo de todos os caminhos percorridos até chegar aos resultados finais.

O capítulo 5, Resultados e Discussões, mostra exemplos e atividades que desempenham um papel complementar ao resto do texto, servindo para ampliar alguns exemplos da teoria e também para reforçar certos pontos abordados na demonstração principal. E por fim, não menos a importante, as Considerações Finais a qual aborda as ponderações da aplicabilidade dos objetivos da pesquisa.

2 UM VISLUMBRE DA HISTÓRIA DA MATEMÁTICA

Quando se faz um relato cronológico de onde a Matemática surgiu, uma questão de por onde devemos começar nos é imposta. Começamos pelos gregos? Pelos egípcios? Ou ainda pelos sumérios? O esforço desses povos para o desenvolvimento da Matemática tem um grande significado em sua história. Afinal todo o conhecimento matemático produzido por eles até hoje é estudado nas escolas, universidades, grupos de pesquisa e outros.

Usualmente, atribui-se o surgimento da Matemática ainda nos tempos dos homens primitivos que usavam o senso numérico, pois devemos admitir que eles reconheciam quando se acrescentavam ou se retiravam alguns dos seus objetos de uma pequena coleção, ou seja, o conceito de mais e menos já era utilizado de maneira inata.

Contagem e senso numérico são totalmente distintos dentro do campo matemático. Entende-se por contagem como sendo o ato de contar ou enumerar. Já o senso numérico é a capacidade de reconhecer e comparar pequenas quantidades em um determinado espaço. Existe uma grande variedade de estudos que comprovam que vários animais detêm o senso numérico. Podemos citar como exemplo os pássaros, pois se retirarmos dois ou mais ovos do ninho, os pássaros abandonarão esse ninho, pois verão que a quantidade de ovos diminuiu. Outro exemplo bastante significativo nos é apresentado por Silveira (2001):

> Mais impressionante ainda é o caso da vespa solitária, Genus Numenus, uma espécie em que a fêmea é maior do que o macho. Quando uma vespa mãe bota seus ovos, ela o faz colocando cada ovo em uma célula diferente e junto de cada ovo ela deixa, para futuro alimento de seu "bebê", algumas larvas de inseto. O notável é que, de alguma maneira, a mãe sabe se um dado ovo originará uma vespa macho ou fêmea e deixa na respectiva célula: 5 larvas de insetos se for um ovo de vespa macho e 10 se for ovo de vespa fêmea.

Para contar os animais de seu rebanho, pastores faziam riscos em pedras, nós em cordas ou entalhes em madeiras. Através desses procedimentos os pastores sabiam se estava faltando algum animal de seu aprisco. Dessa forma surgia o princípio da contagem.

Com o passar do tempo tornou-se necessário efetuar contagens mais extensas, de tal maneira que o processo de contagem teve que ser sistematizado. Várias foram as bases utilizadas como ordem de grandeza pelos povos. A base 5 foi

a primeira a ser usada de forma extensiva, principalmente pelas tribos indígenas da América do Sul. A base 20 foi escolhida pelas tribos americanas e sendo melhor desenvolvida pelos Maias. Houve também a base 60 criada pelos babilônicos, que até hoje é utilizada nas medidas de tempo e medidas de ângulos. Outras bases como 2, 3, 4 e 12 foram usadas em pequenas tribos. (EVES, 2011)

A base 10 foi constantemente escolhida pelos povos, talvez por expressar a quantidade de dedos das mãos. Com esta base os hindus criaram um sistema de numeração que foi amplamente divulgado pelo mundo por meio dos árabes. Este sistema ficou conhecido como Sistema de Numeração Indo-Arábico.

O sistema numérico hindu foi completamente descrito pelo matemático persa Al-Khowarizmi em um livro do ano 825 d.C. É por causa do nome desse matemático que se originou a palavra algarismo. Durante o século XII foi feita uma tradução latina de sua obra que se espalhou rapidamente em toda a Europa.

Para a efetivação desse sistema houve muitas discussões entre os matemáticos, pois os abacistas[1] eram totalmente contra a implantação desse sistema, enquanto os que defendiam foram chamados de algoristas. Devido a regras de computação estabelecidas na época, os abacistas foram derrotados dando lugar ao novo sistema de numeração. Abaixo uma pintura da época ilustra este fato.

Figura 1 – O abacista versus o algorista

Fonte: Matematizar.

[1] Dominavam a arte de calcular em ábacos, tinham grande prestígio e eram bem pagos pelo seu trabalho.

Durante muitos anos os números sofreram várias modificações em sua grafia, pois os livros eram copiados manualmente um a um e cada copista tinha uma caligrafia diferente. Somente com a invenção da imprensa, no século XV, foi que a grafia ficou conservada. A representação gráfica do número zero foi incorporada ao Sistema Indo-Arábico depois de quase 400 anos. A figura a seguir nos mostra essa evolução.

Figura 2 – Evolução dos números indo-arábicos

Fonte: Imenes.

O sistema criado pelos hindus possui 10 símbolos: 1, 2, 3, 4, 5, 6, 7, 8, 9 e 0. Esses símbolos, que recebem o nome de algarismos, podem ser repetidos em um mesmo número quantas vezes forem necessárias. É também um sistema posicional, ou seja, a posição que o algarismo ocupa no número é importante para denotar o seu valor.

2.1 Números primos

A noção de números primos foi, muito provavelmente, introduzida por Pitágoras, desempenhando um papel importante na matemática. De tal forma que os

pitagóricos[2] foram os primeiros a se interessarem pelas propriedades “místicas” dos números primos, as quais foram amplamente estudados. Segundo Silveira (2000), os gregos classificavam os números naturais em três classes:

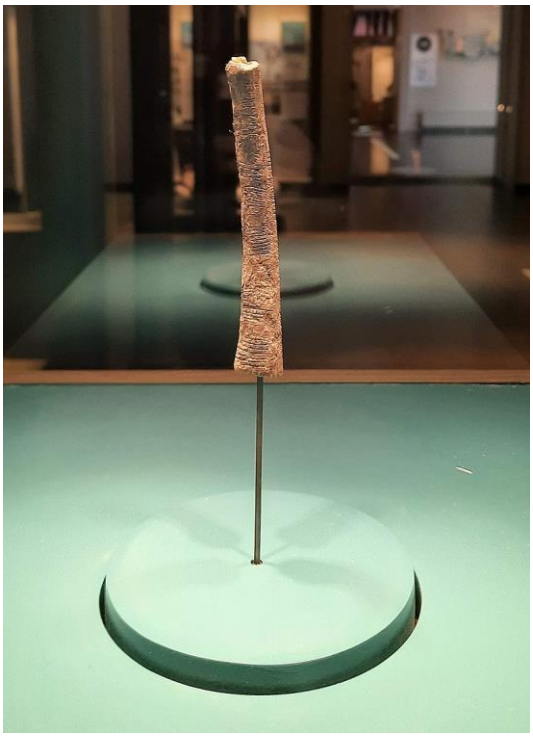
a) *monad*: a unidade (1);

b) *protói arithmói*: números primos (2, 3, 5, 7, 11, ...);

c) *deuterói arithmói*: números secundários (4, 6, 8, 9, 10, ...).

Alguns artefatos pré-históricos podem indicar uma concepção das ideias de números e operações entre os povos antigos. Um dos mais conhecidos é o Osso de Ishango ou Bastão de Ishango, que foi encontrado em uma vila de mesmo nome localizada no Congo na África Central, o qual data entre 20.000 e 18.000 a.C. Nele encontramos três colunas com várias marcações assimétricas. Em uma dessas colunas encontramos 11, 13, 17 e 19 entalhes, os quais são os números primos compreendidos entre 10 e 20. Atualmente, esse artefato encontra-se em exposição no Real Instituto Belga de Ciências Naturais em Bruxelas, Bélgica. Abaixo vemos a sua ilustração e representação gráfica.

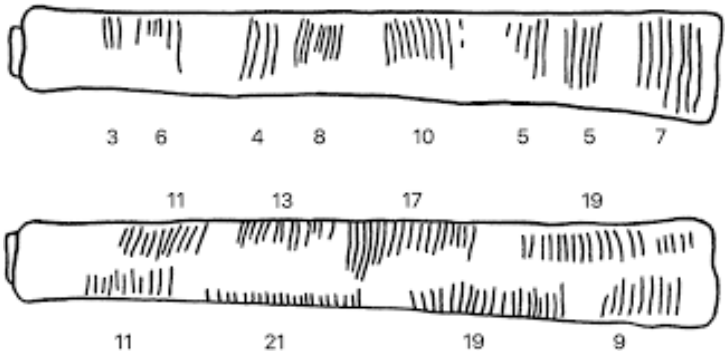
Figura 3 – Osso de Ishango



Fonte: Domingues.

[2] Pensadores gregos da corrente filosófica de Pitágoras.

Figura 4 – Representação gráfica do Osso de Ishango



Fonte: Domingues.

Por definição, um número *p* é classificado como número primo se ele satisfizer a seguinte condição: ser divisível apenas por 1 e por ele mesmo, apresentando assim, dois divisores. Desta forma, os números 0 e 1 não são números primos, pois não existe divisão de zero por zero e o número 1 possui apenas um divisor, ele mesmo. A propriedade de um número ser primo é chamada primalidade. Assim, os números que não apresentam a primalidade são chamados de números compostos, uma vez que podemos escrevê-los em forma de multiplicação de números primos.

> Desde tempos remotos, problemas concernentes a números primos têm fascinado os matemáticos. De fato, Karl Friedrich Gauß chegou a afirmar em seu Disquisitiones Arithmeticae (1801): “O problema de distinguir números primos de compostos e de decompor esses últimos em seus fatores primos é conhecido como sendo um dos mais importantes 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” (MARTÍNEZ; MOREIRA; SALDANHA; TENGAN, 2018, p. 311).

2.1.1 O Crivo de Eratóstenes

Um dos métodos mais antigos e que ainda é ensinado nas escolas de Ensino Fundamental para encontrarmos números primos até um certo número N, é o Crivo de Eratóstenes[3]. Com ele podemos determinar todos os números primos utilizando uma tabela.

Segundo o dicionário Michaelis On-line, a palavra crivo tem o significado de averiguação minuciosa. Ou seja, através do processo de averiguação desse

[3] Matemático grego que viveu entre 276 a.C. a 194 a.C. Foi diretor da famosa Biblioteca de Alexandria.

algoritmo, os números que são múltiplos de primos serão “eliminados” da tabela de tal forma que sobrem apenas os números primos. Vejamos como este algoritmo funciona.

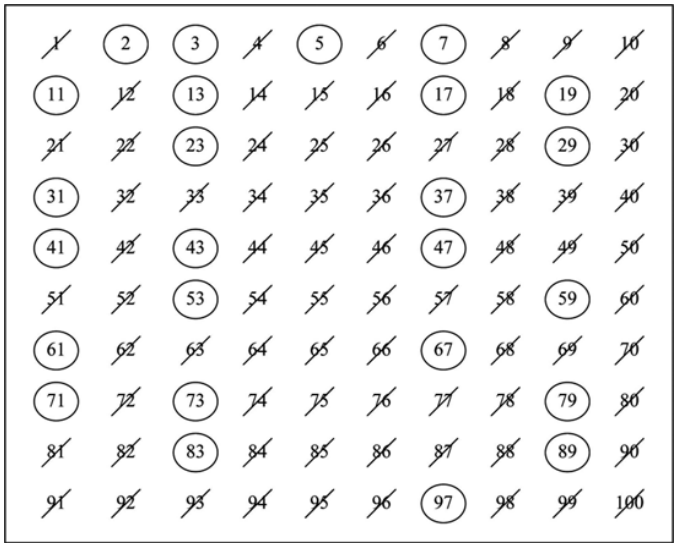
Exemplo 2.1.1: Vamos determinar todos números primos entre 1 e 100.

Para começar o algoritmo, devemos elaborar uma tabela com todos os números naturais menores ou iguais a 100.

Em seguida, riscaremos todos os números compostos da tabela, obedecendo as seguintes instruções:

- Primeiramente riscamos o número 1 que não é primo;
- Risque todos os números divisíveis por 2, e circule o número 2;
- Em seguida, risque todos os múltiplos de 3, e circule o número 3;
- O próximo número que não aparece riscado é o 5, que é primo. Risque todos os múltiplos de 5, e circule o número 5;
- Observe que o próximo número que não aparece riscado é o 7, que é primo. Risque todos os múltiplos de 7, e circule o número 7;
- Os números que estão circulados são números primos menores do que 100.

Figura 5 – Crivo de Eratóstenes de 1 a 100



Fonte: Lopes.

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

2.1.2 Teorema Fundamental da Aritmética

Enunciaremos um dos teoremas mais importantes da aritmética, o qual diz que todo número inteiro maior ou igual a 2 pode ser escrito de maneira única como um produto de números primos. Por exemplo, o número 820 é escrito de maneira única, a menos pela ordem dos fatores, como $2^2 \cdot 5 \cdot 41$. Lembramos que, pela propriedade comutativa da multiplicação, a ordem dos fatores não altera o produto.

Teorema 2.1.2 (Teorema Fundamental da Aritmética):
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 $p_1 \leq ... \leq p_m$ são números primos.

Demonstração. Mostraremos a existência da fatoração de n em números primos através do Princípio de Indução. Se n é primo não há o que provar, pois escrevemos $m = 1$ e $p_1 = n$. Se n é composto podemos escrever $n = ab$, com $a, b \in \mathbb{N}$ de modo que $1 < a < n$ e $1 < b < n$. Por hipótese de indução a e b se decompõem em produtos de números primos. Juntando as fatorações de a e b, organizando e reordenando os fatores, encontramos uma fatoração de n.

Destacando agora a unicidade da fatoração de n. Vamos supor por absurdo que n tenha duas fatorações diferentes

$$n = p_1 \cdot \cdot \cdot p_m = q_1 \cdot \cdot \cdot q_s,$$

com $p_1 \leq ... \leq p_m$, $q_1 \leq ... \leq q_s$ e que n é o mínimo com tal propriedade.

Como $p_1 \mid q_1 \cdot \cdot \cdot q_s$ temos que $p_1 \mid q_i$ para qualquer valor de i. Logo, como q_i é primo, então $p_1 = q_i$ e $p_1 \geq q_1$. Analogamente, temos que $q_1 \leq p_1$ e $q_1 = p_1$. Mas

$$n / p_1 = p_2 \cdot \cdot \cdot p_m = q_2 \cdot \cdot \cdot q_s$$

admite uma única fatoração, pela minimalidade de n, temos que $m = s$ e $p_i = q_i$ para todo i, o que contradiz o fato de n ter duas fatorações. (MARTÍNEZ; MOREIRA; SALDANHA; TENGAN)

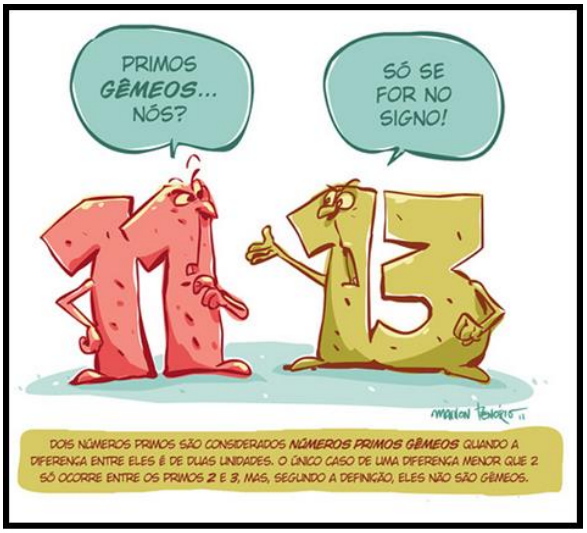
□

Assim, de acordo com o teorema sendo $n \geq 2$, com $n \in \mathbb{N}$, podemos escrevê-lo de maneira única como uma multiplicação de fatores primos.

2.1.3 Números primos gêmeos

Dois números p e q são considerados primos gêmeos quando p e q são primos e o módulo da diferença entre eles é igual a 2 ou seja, $|p - q| = 2$. De modo que os seguintes pares de primos são gêmeos: (3, 5), (5, 7), (11, 13), (17, 19), entre outros. De acordo com Viana (2018), “esta denominação foi usada pela primeira vez em 1916, pelo matemático alemão Paul Stäckel (1862-1919), mas o problema é muito mais antigo”.

Figura 6 – Quadrinho Primos Gêmeos



Fonte: Tenório.

Conjectura-se que existem infinitos pares de primos gêmeos, alguns matemáticos atribuem essa conjectura ao matemático grego Euclides de Alexandria, mas até o momento não há provas de sua autoria e/ou resolução.

No ano de 2013, o matemático Yitang Zhang[4] da Universidade de New Hampshire, em Durham, apresentou uma prova de que os números primos formam pares até o infinito. Ele conseguiu reduzir o valor do infinito para 70 milhões, ou seja, ele provou que existe um número infinito de pares de primos separados por menos de 70 milhões de unidades sem depender de conjecturas não comprovadas.

O maior par de primos gêmeos, até o momento, foi encontrado em setembro de 2016 por uma equipe de matemáticos. Cada número possui 388.342 dígitos.

Tabela 1 – Maiores pares de primos gêmeos conhecidos

Ranque	Primo	Número de dígitos	Data
1º	$2996863034895 \cdot 2^{1290000} \pm 1$	388342	Set. 2016
2º	$3756801695685 \cdot 2^{666669} \pm 1$	200700	Dez. 2011
3º	$65516468355 \cdot 2^{333333} \pm 1$	100355	Ago. 2009
4º	$160204065 \cdot 2^{262148} \pm 1$	78923	Jul. 2021
5º	$12770275971 \cdot 2^{222225} \pm 1$	66907	Jul. 2017
6º	$12599682117 \cdot 2^{211088} \pm 1$	63554	Fev. 2022
7º	$12566577633 \cdot 2^{211088} \pm 1$	63554	Fev. 2022
8º	$70965694293 \cdot 2^{200006} \pm 1$	60219	Abr. 2016
9º	$66444866235 \cdot 2^{200003} \pm 1$	60218	Abr. 2016
10º	$4884940623 \cdot 2^{198800} \pm 1$	59855	Jul. 2015

Fonte: Prime Pages.

Os primos gêmeos são de grande interesse na teoria dos números porque sua existência está relacionada a uma das questões mais antigas e importantes da teoria dos números, a conjectura dos primos gêmeos. Essa conjectura afirma que existem infinitos pares de primos gêmeos, ou seja, sempre existe outro par de primos gêmeos além de qualquer par dado.

Embora a conjectura dos primos gêmeos permaneça um problema em aberto, muitos pares de números primos gêmeos foram encontrados por meio de extensa pesquisa e aplicação de teoria avançada dos números e técnicas computacionais. A seguir temos uma tabela com os trinta menores pares de primos gêmeos.

[4] Denominado Tom Zhang, (1955) é um matemático chinês. Trabalha com teoria dos números.

Tabela 2 – Os trinta menores pares de primos gêmeos

Pares de Primos Gêmeos					
3 e 5	41 e 43	137 e 139	227 e 229	347 e 349	569 e 571
5 e 7	59 e 61	149 e 151	239 e 241	419 e 421	599 e 601
11 e 13	71 e 73	179 e 181	269 e 271	431 e 433	617 e 619
17 e 19	101 e 103	191e 193	281 e 283	461 e 463	641 e 643
29 e 31	107 e 109	197 e 199	311 e 313	521 e 523	659 e 661

Fonte: Elaborado pelo autor.

Os primos gêmeos são importantes porque estudá-los pode ajudar a melhorar nossa compreensão da distribuição dos números primos, que por sua vez podem ter aplicações importantes na criptografia e em outras áreas da computação. Além disso, a descoberta de novos pares de números primos gêmeos é uma grande conquista na teoria dos números.

2.1.3.1 Brun e os primos gêmeos

O matemático norueguês Viggo Brun provou em seu trabalho "*La série 1/5 + 1/7 + 1/11 + 1/13 + 1/17 + 1/19 + 1/29 + 1/31 + 1/41 + 1/43 + 1/59 + 1/61 + ..., où les dénominateurs sont nombres premiers jumeaux est convergente ou finie*" que existem infinitos números inteiros *n* tal que *n* e *n + 2* possuem no máximo nove fatores primos. Ele também mostrou que se *K* é um número par e suficientemente grande então ele é a soma de dois inteiros, cada um tendo no máximo nove fatores primos. Isto representa um tremendo avanço em direção à conjectura dos primos gêmeos e para a conjectura de Goldbach[5]. Como consequência do seu trabalho, ele deduziu que a soma dos recíprocos da sequência de primos gêmeos converge.

Mostrando assim que os números primos gêmeos são escassos no seguinte sentido: se

$$\pi_2(\mathrm{x}) = \#\{\mathrm{p} \leq \mathrm{x} \mid \mathrm{p} \text{ e } \mathrm{p}+2 \text{ são primos}\},$$

é o número de pares de primos gêmeos até x então existe uma constante A > 0 tal que

$$\pi_2(x) \leq A\left(\frac{(x \log\log x)^2}{(\log x)^2}\right)$$

[5] Afirma que todo número par maior que 2 pode ser escrito como a soma de primos.

Em particular, isso implica que

$$\sum_{p\ primo\ gêmeo} \frac{1}{\mathrm{p}} < +\infty,$$

na qual sabemos que a soma sobre todos os primos $\sum_{\mathrm{p\ primo}} \frac{1}{\mathrm{p}}$ diverge. (MARTÍNEZ; MOREIRA; SALDANHA; TENGAN)

3 SOPHIE GERMAIN, A MATEMÁTICA FRANCESA

Marie Sophie Germain, nasceu em 1º de abril de 1776, foi uma francesa que teve a sua infância e adolescência durante o período da Revolução Francesa. Por ser um período de terror na sociedade, as pessoas eram incentivadas a ficar em suas residências. Sua família possuía algumas posses, embora não fossem nobres. Era filha do comerciante de seda Ambroise François Germain e de sua esposa, Marie Madeleine Germain.

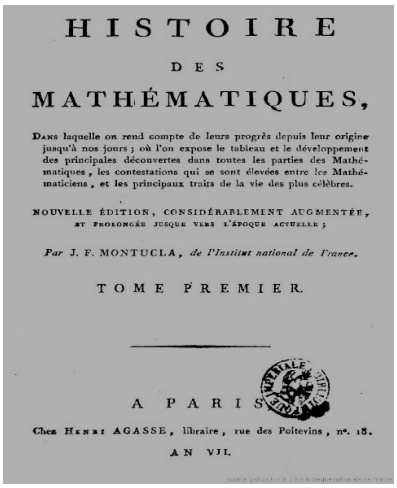
Figura 7 – Imagem de Sophie Germain

Fonte: Clubes de Matemática da OBMEP.

Sophie sempre foi interessada nos livros do seu pai, o qual tinha uma biblioteca em sua residência. Constantemente, ela pegava e estudava os livros da biblioteca, pois era autodidata.

Certo dia, pegou o livro "*A história da matemática de Jean-Étienne Montucla*" e ficou muito impressionada com a leitura. Neste momento se inicia seu interesse pela Ciência Matemática. Contudo, por ser mulher era teoricamente inapta para estudar matemática, o preconceito foi a situação em que sempre lutou contra durante toda a sua vida.

Figura 8 – A história da matemática de Jean-Étienne Montucla



HISTOIRE

DES

MATHÉMATIQUES,

Dans laquelle on rend compte de leurs progrès depuis leur origine jusqu'à nos jours ; où l'on expose le tableau et le développement des principales découvertes dans toutes les parties des Mathématiques, les contestations qui se sont élevées entre les Mathématiciens, et les principaux traits de la vie des plus célèbres.

NOUVELLE ÉDITION, CONSIDÉRABLEMENT AUGMENTÉE, ET PROLONGÉE JUSQUE VERS L'ÉPOQUE ACTUELLE ;

Par J. F. MONTUCLA, *de l'Institut national de France.*

TOME PREMIER.

A PARIS

Chez HENRI AGASSE, libraire, rue des Poitevins, n°. 18.

AN VII.

JEAN ETIENNE MONTUCLA

de l'Institut National de France,

de l'Académie de Berlin, &c.

Fonte: Montucla.

Em um dos capítulos do livro se deparou com a história da morte de Arquimedes[6], isso chamou muito a atenção de Sophie. Arquimedes foi o homem que entendeu o princípio da alavanca, mas durante uma invasão romana, na sua cidade natal, Siracusa, o mesmo estava tão concentrado nos seus estudos de matemática, que não observou a chegada de um soldado romano para prendê-lo, o soldado enfurecido deu-lhe um golpe com uma espada e matou-o. Esta narrativa despertou em Sophie a curiosidade de identificar que assunto era esse que se chamava matemática, em que Arquimedes levou uma espadada sem nem ter visto antes o seu assassino (HALL; JONES; JONES, 2004).

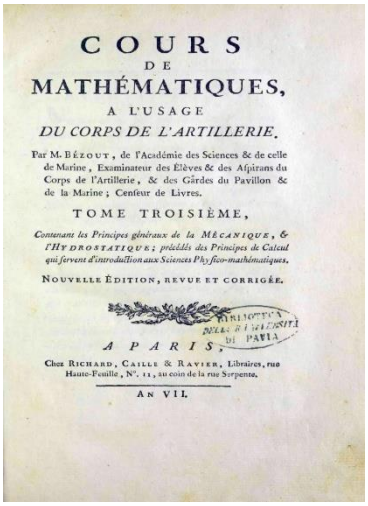
Figura 9 – Pintura "*La Mort d'Archimède*"

Fonte: Killhian.

[6] Arquimedes de Siracusa (287 a.C. – 212 a.C.) foi um matemático, físico, engenheiro, inventor e astrônomo grego. Considerado um dos maiores cientistas da Antiguidade.

Posteriormente, ela iniciou os estudos do livro “*Cours de mathématiques, a l'usage du corps de l'artillerie”*, 1798 de Étienne Bézout (1730-1783), onde o assunto da aritmética básica é apresentado para esta estudiosa.

Figura 10 – Livro *Cours de mathématiques*, 1798 de Étienne Bézout


COURS
DE
MATHÉMATIQUES,
A L'USAGE
DU CORPS DE L'ARTILLERIE.
Par M. Bézout, de l'Académie des Sciences & de celle de Marine, Examinateur des Élèves & des Aspirans du Corps de l'Artillerie, & des Gardes du Pavillon & de la Marine; Censeur de Livres.
TOME TROISIÈME,
Contenant les Principes généraux de la Mécanique, & l'Hydrostatique; précédés des Principes de Calcul qui servent d'introduction aux Sciences Physico-mathématiques.
Nouvelle Édition, revue et corrigée.
A PARIS,
Chez Richard, Caille & Ravier, Libraires, rue Haute-Feuille, N°. 11, au coin de la rue Serpente.
An VII.

Fonte: Wikipedia.

Sophie Germain após estudar o livro de Étienne Bézout, se interessou também pelas obras de Isaac Newton (1643-1727) e de Leonhard Euler (1707-1783) que estavam escritos em latim. Estes autores foram o incentivo para ela estudar e aprender latim e grego.

Naquela época não se esperava que uma mulher estudasse tanto, então o pai de Sophie percebendo que a filha estava adquirindo conhecimento retirou dela os agasalhos, alguns casacos pesados e também retirou as velas que ela utilizava para iluminar os seus estudos a noite. Todas essas atitudes só tinham uma única idealização, que era impedir Sophie de estudar. Mas, isso não foi empecilho para a determinação de Sophie, pois mesmo escondida ela continuou a sua rotina de estudos.

Em 1794 foi fundada a “*École Polytechnique*”, Escola Politécnica Francesa, cujo objetivo era que jovens não nobres tivessem acesso ao ensino superior. Por ser o período da Revolução Francesa, então se enfatizava o ideal de igualdade no acesso ao ensino superior contudo, esta escola era somente para homens. ‘‘A história das mulheres no mundo acadêmico foi excluída, esquecida por muitos séculos, tanto que a maioria dos nomes importantes citados no ensino é de homens. As mulheres eram

discriminadas” (OLIVEIRA, 2012, p. 14). Não permitindo que Sophie ingressasse no ensino superior, todavia a dificuldade não a desestimulou.

Narra-se um fato de que um aluno da Escola Politécnica Francesa, Antoine-August Le Blanc havia desistido das aulas, então Sophie percebeu uma oportunidade de utilizar os materiais desse ex-aluno para seus estudos.

A Escola Politécnica enviava listas de exercícios através de cartas, no entanto Sophie pegava as listas de exercício, que eram destinadas a esse ex-aluno, as respondiam e enviava novamente. Durante dois meses ela conseguiu fazer isso. Contudo, o professor de matemática Joseph Louis Lagrange percebeu uma disparidade em relação a resolução das atividades de Le Blanc, pois o mesmo tinha uma dificuldade intelectual e de um momento para outro, virou um grande aluno, pois aquelas respostas que Sophie enviava eram excelentes.

O professor Lagrange ficou impressionado e disse a Le Blanc que queria explicações em relação as suas atividades, neste momento Sophie teve que revelar que estava se passando por esse aluno que abandonou a Escola Politécnica. O professor ficou impressionado, mas não conseguiu matriculá-la na Escola Politécnica. Mais uma vez, a mesma era impedida pelo fato de ser uma mulher, “’por causa da fragilidade do sexo e da sua pior condição (...) não se devem intrometer nas reuniões dos homens’; não podem ser fiadoras; não podem ser testemunhas nos testamentos (ord. Fil., IV, 76); nos delitos são castigadas mais brandamente” (HESPANHA, 2010, p. 112-113).

Sophie tinha interesse em estudar então procurou alguns professores como Carl Friedrich Gauss em 1804. Após estudar um dos seus trabalhos, ela começou a se corresponder com ele, ainda utilizando o pseudônimo de Antoine-Auguste Le Blanc, já que muitos matemáticos não levavam a sério as mulheres que se dedicavam a essa área. Em 1807, Gauss descobriu a verdadeira identidade de Sophie, pois o imperador Napoleão Bonaparte invadiu a Prússia fazendo com que Sophie intervisse, por meio de um general amigo da família, e garantisse a segurança de Gauss. Então “Gauss escreve a sua protetora uma carta de agradecimento na qual externa o seu espanto pela verdadeira identidade do seu correspondente e aproveita o ensejo para elogiar a coragem e o talento de Sophie para estudar Matemática” (MORAIS FILHO, 1996).

Sophie Germain fez importantes contribuições em teoria dos números, em particular, estudando as propriedades dos números primos. Ela também trabalhou em

mecânica teórica, estudando a elasticidade dos corpos e propondo uma teoria de vibração dos corpos sólidos. Ela recebeu uma medalha da Academia de Ciências da França, em 1809, em reconhecimento ao seu trabalho em matemática com contribuições significativas para a resolução do Último Teorema de Fermat.

> O gosto pelas ciências abstratas em geral e, acima de tudo, pelos mistérios dos números, é muito raro: isto não é surpreendente, uma vez que os encantos dessa sublime ciência em toda sua beleza revelam-se somente àqueles que têm a coragem de decifrá-los. Mas, quando uma mulher, devido a seu sexo, a nossos costumes e a nossos preconceitos, encontra infinitamente mais obstáculos do que os homens em familiarizar-se com seus intricados problemas e, ainda assim, supera tais barreiras e desvenda aquilo que está mais escondido, ela sem dúvida tem a mais nobre coragem, extraordinário talento e gênero superior (GARBI, 2007, p. 21).

Sophie Germain morreu em 1831, aos 55 anos, devido a um câncer de mama. Apesar dos desafios que enfrentou como mulher em uma área dominada por homens, ela fez importantes contribuições para a matemática e é lembrada como uma das pioneiras do estudo das propriedades dos números primos.

3.1 Números primos de Sophie Germain

Um número de Sophie Germain é um número primo que, quando multiplicado por 2 e adicionado 1, resulta em outro número primo. Por exemplo, 5 é um número de Sophie Germain, pois $2 \cdot 5 + 1 = 11$ é também um número primo.

Figura 11 – Os vinte primeiros primos de Sophie Germain

Fonte: Elaborado pelo autor.

A infinitude desses números é até hoje desconhecida, sendo titulada como uma conjectura. Os primos de Sophie Germain conquistaram tamanha notoriedade, pois o Primeiro Caso do UTF é válido para n = p, onde p é um primo de Sophie Germain.

Usaremos como referência para esta seção (RIBENBOIM, 2004) e (COUTINHO, 2016).

Vamos dar agora estimativas do número de Sophie Germain inferiores a um número x ≥ 1.

Mas geralmente, sejam a e d ≥ 1 com *a, d* par e mdc (a, d) = 1. Para todo x ≥ 1, seja

$$S_{d,a}\ (x) = \#\ \{\ p\ primo \mid p \leq x, a + pd\ primo\}.$$

Se a = 1 e d = 2, $S_{2,1}\ (x)$ é igual ao número dos primos de Sophie Germain com p ≤ x conforme nos mostra na tabela 3.

Tabela 3 – $S_{2,1}\ (x)$ dos números primos de Sophie Germain inferiores a x

x	$S_{2,1}\ (x)$
10^3	37
10^4	190
10^5	1 171
10^6	7 746
10^7	56 032
10^8	423 140
10^9	3 308 859
10^{10}	26 569 515
10^{11}	218 116 524

Fonte: Ribenboim (2020).

Assim, podemos listar os maiores números de Sophie Germain encontrados até o momento, que correspondem aos maiores primos p para os quais 2p + 1 é primo. A tabela 4 faz um levantamento dos maiores números primos de Sophie Germain descobertos até o momento.

Tabela 4 – Os dez maiores números primos de Sophie Germain

Ranque	Primo	Número de dígitos	Data
1º	$2618163402417 \cdot 2^{1290000} - 1$	388342	Fev. 2016
2º	$18543637900515 \cdot 2^{666667} - 1$	200701	Abr. 2012
3º	$183027 \cdot 2^{265440} - 1$	79911	Mar. 2010
4º	$648621027630345 \cdot 2^{253824} - 1$	76424	Nov. 2009
5º	$620366307356565 \cdot 2^{253824} - 1$	76424	Nov. 2009
6º	$1068669447 \cdot 2^{211088} - 1$	63553	Maio 2020
7º	$99064503957 \cdot 2^{200008} - 1$	60220	Abr. 2016
8º	$12443794755 \cdot 2^{184516} - 1$	55555	Set. 2021
9º	$21749869755 \cdot 2^{184515} - 1$	55555	Set. 2021
10º	$14901867165 \cdot 2^{184515} - 1$	55555	Set. 2021

Fonte: Prime Pages.

Os primos de Sophie Germain não foram oficialmente demonstrados que são infinitos, nem tão pouco provado o contrário, desta afirmação, conjectura-se que existem infinitos números primos de Sophie Germain.

3.2 Identidade de Sophie Germain

A identidade não é trivial, mas pode ser facilmente demonstrada, realizando a multiplicação dos termos no lado direito da igualdade (ou, mais engenhosamente, somando e subtraindo $4a^2b^2$ no lado esquerdo).

Identidade de Sophie Germain: Sejam a e b números reais. Mostre que:

$$a^4 + 4b^4 = (a^2 + 2b^2 + 2ab) \cdot (a^2 + 2b^2 - 2ab)$$

Demonstração.

$$a^4 + 4b^4 =$$
$$= (a^2)^2 + (2b^2)^2 =$$
$$= (a^2)^2 + (2b^2)^2 + 4\,a^2\,b^2 - 4\,a^2\,b^2 =$$
$$= (a^2 + 2b^2)^2 - (2ab)^2 =$$
$$= (a^2 + 2b^2 + 2ab) \cdot (a^2 + 2b^2 - 2ab)$$

□

Exemplo 3.2: Sendo *n* um inteiro maior do que 1, mostre que $n + 4^n$ nunca é primo. Vamos dividir a demonstração em dois casos.

Caso I: Se *n* é par, então temos $n = 2k$, para *k* inteiro positivo.
Assim,

$$n^4 + 4^n = (2k)^4 + 4^{2k} = 16k^4 + 2^{4k} = 2 \cdot (8k^4 + 2^{4k-1})$$

logo $n^4 + 4^n$ não é primo, já que $(8k^4 + 2^{4k-1}) > 1$.

Caso II: Se *n* é ímpar, então temos $n = 2k + 1$, para *k* inteiro positivo.
Assim,

$$n^4 + 4^n = (2k+1)^4 + 4^{2k+1} = (2k+1)^4 + 4 \cdot 4^{2k} = (2k+1)^4 + 4 \cdot (2^{4k})$$

Tomando $a = 2k + 1$ e $b = 2^{2k}$ pela identidade de Sophie Germain, podemos fatorar a última expressão obtendo

$$n^4 + 4^n = (a^2 + 2b^2 + 2ab) \cdot (a^2 + 2b^2 - 2ab)$$

Resta mostrar que esses fatores não são 1 e o próprio $n^4 + 4^n$.

Faremos isso mostrando que os dois fatores são maiores que 1. Como *k* é inteiro positivo, temos $k \geq 1$ e, assim,

$$b^2 = (2^k)^2 = 2^{2k} \geq 2^2 = 4;$$

logo,

$$a^2 + 2b^2 - 2ab = (a-b)^2 + b^2 \geq (a-b)^2 + 4 > 1.$$

Além disso, como $a > 0$ e $b > 0$, temos:

$$a^2 + 2b^2 + 2ab > a^2 + 2b^2 - 2ab > 1$$

Portanto, $n^4 + 4^n$ não é primo.

□

Sophie Germain não é conhecida por desenvolver um método específico de fatoração. No entanto, seu trabalho em teoria dos números, em particular o Teorema de Sophie Germain, pode ser usado em alguns casos para fatorar certos tipos de números.

3.3 O Teorema de Sophie Germain e o Teorema de Fermat

O Teorema de Sophie Germain é um resultado importante da teoria dos números que relaciona números primos e números de Sophie Germain. Foi descoberto no início do século XIX e é um dos seus principais resultados. Onde o mesmo será abordado no capítulo 5.

O Teorema de Sophie Germain tem diversas aplicações em teoria dos números e é usado em muitas demonstrações de resultados importantes, como o Último Teorema de Fermat, que foi provado por Andrew Wiles em 1994. Uma de suas realizações mais notáveis foi seu trabalho no Teorema de Fermat, pois é um dos problemas mais famosos da história da matemática.

Teorema 3.3.1 (Teorema de Sophie-Legendre) Suponha que p e q são primos ímpares, tais que
(a) Toda solução da congruência $x^p + y^p + z^p \equiv 0 \pmod q$ *satisfaz q | xyz;*
(b) A congruência $w^p \equiv p \pmod q$ *não possui solução.*
Então não existem inteiros x, y, z com mdc $(x, y, z) = 1$ *e* $p \nmid xyz$ *tais que* $x^p + y^p + z^p = 0$.

Demonstração.
Suponhamos por contradição que a equação $x^p + y^p + z^p = 0$ possui tal solução. Assim, temos que

$$(-x)^p = (y + z)\,(y^{p-1} - y^{p-2}z + \cdots - yz^{p-2} + z^{p-1}) = 0$$

Vamos mostrar que os dois fatores da direita são primos entre si.
Se l é um primo que divide ambos os termos, então $z \equiv -\mathrm{y} \pmod l$ e portanto
$0 \equiv \mathrm{y}^{\mathrm{p}-1} - \mathrm{y}^{\mathrm{p}-2}\mathrm{z} + \cdots + \mathrm{z}^{\mathrm{p}-1} + \mathrm{z}^{\mathrm{p}-1} \equiv \mathrm{p}\mathrm{y}^{\mathrm{p}-1} \pmod l$; temos $l \neq \mathrm{p}$ pois $l \mid \mathrm{x}$, assim

$l \mid \mathrm{p}\mathrm{y}^{\mathrm{p}-1} \Longrightarrow\ l \mid \mathrm{y}$, mas então $\mathrm{z} \equiv -\mathrm{y} \equiv 0\ (\mathrm{mod}\ l)$ e l dividiria simultaneamente x, y, z contrariando a hipótese mdc $(\mathrm{x}, \mathrm{y}, \mathrm{z}) = 1$.

Assim, pela fatoração única em primos existentes inteiros a, d tais que

$$\mathrm{ad} = -\mathrm{x},\ \mathrm{a}^{\mathrm{p}} = \mathrm{y} + \mathrm{z} \quad \mathrm{e} \quad \mathrm{d}^{\mathrm{p}} = \mathrm{y}^{\mathrm{p}-1} - \mathrm{y}^{\mathrm{p}-2}\mathrm{z} + \cdots - \mathrm{y}\mathrm{z}^{\mathrm{p}-2} + \mathrm{z}^{\mathrm{p}-1}$$

e analogamente,

$$\mathrm{be} = -\mathrm{y},\ \mathrm{b}^{\mathrm{p}} = \mathrm{x} + \mathrm{z} \quad \mathrm{e} \quad \mathrm{e}^{\mathrm{p}} = \mathrm{x}^{\mathrm{p}-1} - \mathrm{x}^{\mathrm{p}-2}\mathrm{z} + \cdots - \mathrm{x}\mathrm{z}^{\mathrm{p}-2} + \mathrm{z}^{\mathrm{p}-1}$$

$$\mathrm{cf} = -\mathrm{z},\ \mathrm{c}^{\mathrm{p}} = \mathrm{x} + \mathrm{y} \quad \mathrm{e} \quad \mathrm{f}^{\mathrm{p}} = \mathrm{x}^{\mathrm{p}-1} - \mathrm{x}^{\mathrm{p}-2}\mathrm{y} + \cdots - \mathrm{x}\mathrm{y}^{\mathrm{p}-2} + \mathrm{y}^{\mathrm{p}-1}$$

para *b, c, e, f* inteiros.

Como $\mathrm{q} \mid \mathrm{xyz}$ podemos supor sem perda da generalidade que $\mathrm{q} \mid \mathrm{x}$.

Assim, de $2\mathrm{x} = \mathrm{b}^{\mathrm{p}} + \mathrm{c}^{\mathrm{p}} - \mathrm{a}^{\mathrm{p}}$ temos que

$$\mathrm{q} \mid \mathrm{b}^{\mathrm{p}} + \mathrm{c}^{\mathrm{p}} - \mathrm{a}^{\mathrm{p}} = \mathrm{b}^{\mathrm{p}} + \mathrm{c}^{\mathrm{p}} + (-\mathrm{a})^{\mathrm{p}},$$

logo, pela primeira hipótese do teorema $\mathrm{q} \mid \mathrm{abc}$.

Mas se $\mathrm{q} \mid \mathrm{b}$ ou $\mathrm{q} \mid \mathrm{c}$, teríamos que $\mathrm{q} \mid \mathrm{b}^{\mathrm{p}} = \mathrm{x} + \mathrm{z}$ ou $\mathrm{q} \mid \mathrm{c}^{\mathrm{p}} = \mathrm{x} + \mathrm{y}$; como $\mathrm{q} \mid \mathrm{x}$ e $\mathrm{x}^{\mathrm{p}} + \mathrm{y}^{\mathrm{p}} + \mathrm{z}^{\mathrm{p}} = 0$, teríamos que $\mathrm{q} \mid \mathrm{mdc}(\mathrm{x}, \mathrm{y}, \mathrm{z}) = 1$, um absurdo.

Por outro lado, temos $f^p \equiv y^{p-1}$ (mod q) e, se $\mathrm{q} \mid \mathrm{a}$, então $\mathrm{q} \nmid \mathrm{d}$ (pois a e d são primos entre si) $y \equiv -z\ (\mathrm{mod}\ \mathrm{q}) \Longrightarrow d^p \equiv py^{p-1} (mod\ q)$.

Assim, $q \mid f$, pois caso contrário f teria o inverso do módulo q e $(\mathrm{df}^{-1})^{\mathrm{p}} \equiv \mathrm{p}$ (mod q), o que contradiz a segunda hipótese do teorema.

Logo, também teríamos $\mathrm{q} \mid \mathrm{z}$ e, como $\mathrm{x}^{\mathrm{p}} + \mathrm{y}^{\mathrm{p}} + \mathrm{z}^{\mathrm{p}} = 0$, $\mathrm{q} \mid \mathrm{y}$ o que é impossível já que $\mathrm{mdc}(\mathrm{x}, \mathrm{y}, \mathrm{z}) = 1$, completando a prova. (MARTÍNEZ; MOREIRA; SALDANHA; TENGAN)

□

O Último Teorema de Fermat afirma que não há soluções inteiras para a equação $x^n + y^n = z^n$ quando n é um número inteiro maior que 2. O teorema foi

proposto pelo matemático francês Pierre de Fermat em 1637, mas ele não apresentou uma prova completa de sua conjectura. Fermat afirmou ter uma prova desse teorema, mas não deixou nenhum registro dela, sendo assim, por mais de três séculos, matemáticos de todo o mundo tentaram provar o teorema sem sucesso pois não conseguiram encontrar uma demonstração geral para todos os valores de n $\in \mathbb{N}$.

Sophie Germain foi a primeira pessoa a fazer progressos significativos na demonstração do UTF. Em particular, ela se concentrou no caso especial de n = 5 e provou que se, x, y e z são números inteiros que satisfazem a equação $x^5 + y^5 = z^5$, então pelo menos um dos números x, y, ou z deve ser divisível por 5. Embora isso não tenha sido suficiente para provar o Último Teorema de Fermat em sua totalidade, ela preparou o terreno para mais trabalhos sobre o problema.

Em resumo, Sophie Germain foi uma notável matemática cujo trabalho no teorema de Fermat e outros problemas na teoria dos números e na física matemática fizeram dela uma figura importante na história da matemática.

O Teorema de Sophie Germain, que relaciona números primos e números de Germain, é um dos seus principais resultados em teoria dos números. Além disso, ela contribuiu para a teoria dos números com estudos sobre a teoria dos resíduos quadráticos, a lei da reciprocidade quadrática e a teoria das equações diofantinas.

3.4 Teoria dos Resíduos Quadráticos

A teoria dos resíduos quadráticos é um assunto importante da teoria dos números que estuda as propriedades dos números que são resíduos quadráticos módulo um número primo p. Um número inteiro a é chamado de resíduo quadrático módulo p se existe um inteiro x tal que,

$$x^2 \equiv a \pmod{p},$$

caso contrário, a é chamado de não-resíduo quadrático módulo p.

A teoria dos resíduos quadráticos tem aplicações em criptografia e em outras áreas da matemática, como a teoria dos campos finitos e a geometria algébrica.

Um resultado importante na teoria dos resíduos quadráticos é a Lei da Reciprocidade Quadrática de Euler, que estabelece uma relação entre o símbolo de Legendre e o símbolo de Jacobi. O símbolo de Legendre é definido como:

$$\begin{cases} \frac{a}{p} = 1, \text{ se p ł a é um resíduo quadrático módulo p;} \\ \frac{a}{p} = -1, \text{ se a é um não-resíduo quadrático módulo p;} \\ \frac{a}{p} = 0, \text{ se a é divisível por p.} \end{cases}$$

O símbolo de Jacobi é uma generalização do símbolo de Legendre para qualquer inteiro n é definido como o produto dos símbolos de Legendre para os fatores primos de n. A Lei da Reciprocidade Quadrática de Euler estabelece uma relação entre os símbolos de Legendre e Jacobi e pode ser usada para determinar se um número é um resíduo quadrático módulo um número primo p.

Sophie Germain contribuiu para a teoria dos resíduos quadráticos com um método para resolver equações diofantinas da forma $ax^2 + by^2 = cz^2$, onde a, b, c são inteiros e p é um número primo que não divide abc. Este método é conhecido como método da desigualdade de Sophie Germain.

O método da desigualdade de Sophie Germain é uma técnica matemática usada para provar a primalidade de um número ímpar. A ideia básica por trás da desigualdade de Sophie Germain é que, se p é um número ímpar que é primo, então é possível encontrar um número inteiro a tal que:

$$a^2 \equiv 1 \pmod{p},$$

se essa relação for verdadeira, então p divide ou a + 1 ou a – 1.

Uma vez que essa relação é estabelecida, é possível usar o método para provar que um número ímpar é primo. O método funciona da seguinte maneira:

- Escolha um número ímpar n que se deseja testar para a primalidade.
- Escolha um número inteiro a que seja relativamente primo a n, ou seja, que não tenha fatores em comum com n.
- Calcule a^2 mod n. Se $a^2 \equiv 1 \pmod{n}$, então o método falha e outro valor de a deve ser escolhido.
- Caso contrário, calcule $a^{\frac{(n-1)}{2}} \equiv \text{mod n}$.
- Se $a^{\frac{(n-1)}{2}} \equiv -1 \pmod{n}$, então n é primo. Caso contrário, n é composto e outro valor de a deve ser escolhido.

Esse método é bastante eficaz para testar a primalidade de números ímpares grandes, mas não é uma solução geral para o problema da primalidade. Existem números compostos que passam no teste de Sophie Germain para todos os valores possíveis de a, e esses são chamados de números de Carmichael[7]. No entanto, esses números são relativamente raros e o método da desigualdade de Sophie Germain ainda é amplamente utilizado na teoria dos números.

3.5 Equações diofantinas

Equações diofantinas são equações polinomiais em que as incógnitas devem assumir valores inteiros. O termo "diofantina" é uma homenagem a Diofanto de Alexandria, um matemático grego que viveu no século III d.C. e que é considerado o pai da Álgebra.

Um exemplo simples de equação diofantina é:

$$3x + 4y = 5$$

Nessa equação, as incógnitas são x e y, e os coeficientes são 3 e 4. A solução dessa equação consiste em encontrar valores inteiros para x e y que satisfaçam a equação. No caso dessa equação em particular, não existem soluções inteiras positivas.

Equações diofantinas podem ser muito mais complexas do que esse exemplo simples. Quando a equação tem duas ou mais incógnitas, ela é chamada de equação diofantina linear, podendo ser uma equação diofantina polinomial. Soluções para essas equações podem ser encontradas por meio de técnicas algébricas, como o algoritmo de Euclides.

As equações diofantinas em números primos são equações que envolvem números primos e que são resolvidas em termos de números inteiros. Estas equações são importantes em teoria dos números e têm sido estudadas por muitos matemáticos ao longo dos anos.

Um exemplo de equação diofantina em números primos é a seguinte:

$$P_1 + P_2 = n$$

[7] Postulados em 1910 pelo americano Robert Carmichael. São números compostos que passam em testes de primalidade.

onde P_1 e P_2 são números primos e n é um número inteiro. Neste caso, a equação pede que encontremos dois números primos cuja soma seja igual a n.

Outro exemplo de equação diofantina em números primos é a seguinte:

$$\frac{P_1}{P_2} = n,$$

onde P_1 e P_2 são números primos e n é um número racional. Neste caso, a equação pede que encontremos dois números primos cujo quociente seja igual a $n \in \mathbb{Q}$.

Resolver equações diofantinas em números primos pode ser um desafio, pois nem sempre há uma solução óbvia. No entanto, existem técnicas e teoremas em teoria dos números que podem ser usados para resolver essas equações em alguns casos.

4 METODOLOGIA

Selltíz *et al*. (1987) comentam que os investigadores pesquisam cientificamente para solucionar problemas como “cerne da questão a ser estudada” (RUIZ, 2006, p. 51) e que o primeiro passo na formulação da pesquisa é tornar o problema concreto e explícito. Segundo Richardson (1999), os objetivos de uma pesquisa são: resolver problemas específicos, gerar teorias ou avaliar as teorias existentes, sendo que esses três objetivos se complementam entre si.

A determinação de um estudo por parte do pesquisador é intencional. “Com a reflexão do pesquisador a respeito do tema, surge o problema como indagação necessária em busca de soluções, pois é preciso ter a ideia clara do problema a ser resolvido, da dúvida a ser superada” (RUIZ, 2006, p. 51).

Para Rudio (2007, p. 94):

> Formular o problema consiste em dizer, de maneira explícita, clara, compreensível e operacional, qual a dificuldade com a qual nos defrontamos e que pretendemos resolver, limitando o seu campo e apresentando suas características. Desta forma, o objetivo da formulação do problema da pesquisa é torná-lo individualizado, específico, inconfundível.

Frequentemente, a opção pelo problema da investigação é precedida de uma aproximação do pesquisador à temática que pode ocorrer por diversos canais e caminhos. Independentemente dos canais e caminhos, o problema é um enunciado interrogativo o qual questiona sobre a possível relação que possa haver entre duas ou mais variáveis pertinentes ao objeto de estudo investigado e passível de observação empírica (KÖCHE, 2003). Este trabalho segue a metodologia qualitativa quanto a natureza da pesquisa e quanto aos objetivos da pesquisa exploratória, no qual a técnica de coleta de dados empregada foi a pesquisa bibliográfica.

Segundo Triviños (1987) a pesquisa qualitativa é uma abordagem metodológica de investigação que busca compreender e interpretar a complexidade dos fenômenos sociais, culturais, políticos e psicológicos a partir da perspectiva dos sujeitos envolvidos. Ela se baseia em métodos que permitem a coleta e análise de dados não estruturados, como entrevistas, observações e análise de documentos, buscando uma compreensão mais profunda e detalhada do objeto de estudo.

Contudo, Gil (2008) afirma que a pesquisa qualitativa é frequentemente utilizada em áreas como sociologia, antropologia, psicologia, educação, entre outras.

Ela pode ser realizada por meio de diferentes técnicas, com análise de documentos e análise de conteúdo. Os resultados da pesquisa qualitativa são apresentados em forma de narrativas, descrições detalhadas e interpretações dos dados coletados. Eles são frequentemente utilizados para subsidiar a formulação de políticas públicas, a tomada de decisões em organizações e a produção de conhecimento em diferentes áreas.

Por ter um caráter exploratório, onde ocorre uma abordagem inicial da pesquisa que visa explorar um tema ou problema de pesquisa de forma mais ampla e abrangente. Ela é utilizada para gerar ideias e hipóteses, identificar lacunas de conhecimento, definir conceitos e variáveis, e estabelecer a viabilidade de uma pesquisa mais detalhada (AAKER, KUMAR & DAY, 2004).

No entanto, conforme Zikmund (1997) a pesquisa exploratória não tem como objetivo fornecer conclusões definitivas ou generalizações precisas, mas sim fornecer uma visão geral do tema ou problema em questão. É particularmente útil quando o tema de pesquisa é pouco conhecido ou não foi estudado anteriormente, ou quando se deseja obter uma compreensão mais profunda de um fenômeno complexo.

Desse modo, o estudo foi realizado no ambiente da pesquisa bibliográfica que é elaborada a partir de material já publicado, incluindo livros, revistas, publicações e artigos científicos, jornais, boletins, monografias, dissertações, teses, material cartográfico, internet. O pesquisador espera em contato direto com todo o material já escrito sobre o assunto da pesquisa (PRODANOV E FREITAS, 2013). Contudo a veracidade dos trabalhos foi analisada para não comprometer o andamento.

4.1 Delineamento da pesquisa

O delineamento da pesquisa refere-se ao plano geral que define como a pesquisa será conduzida e como os dados serão coletados, analisados e interpretados. É uma etapa importante na elaboração de um projeto de pesquisa, pois determina a estrutura e a estratégia que serão utilizadas para alcançar os objetivos da pesquisa. Conforme Prodanov e Freitas (2013, p. 54):

> O delineamento refere-se ao planejamento da pesquisa em sua dimensão mais ampla, envolvendo diagramação, previsão de análise e interpretação de coleta de dados, considerando o ambiente em que são coletados e as formas de controle das variáveis envolvidas. O elemento mais importante para a

> identificação de um delineamento é o procedimento adotado para a coleta de dados.

O delineamento da pesquisa deve ser escolhido com base nos objetivos da pesquisa e nas questões de pesquisa que se deseja responder. É importante que seja claro e bem definido para garantir a validade e a confiabilidade dos resultados obtidos. Por ser um estudo com o delineamento longitudinal, pois envolve a coleta de dados em diferentes momentos do tempo para examinar mudanças ao longo do tempo. Onde os dados coletados são analisados para identificar padrões e mudanças ao longo do tempo, bem como para examinar as relações entre diferentes variáveis (MARCONI; LAKATOS, 2004).

A coleta de dados que embasaram a pesquisa foi bibliográfica, como descrita anteriormente, pois consiste na revisão sistemática e crítica da literatura relevante para o tema em questão. Ela envolve a análise de fontes bibliográficas, tais como artigos científicos, livros, teses, dissertações, relatórios técnicos, entre outros. O objetivo da pesquisa bibliográfica é fornecer uma visão geral do estado atual do conhecimento sobre um determinado assunto, permitindo identificar as principais contribuições e lacunas na literatura. É importante também utilizar diversas fontes e perspectivas para garantir uma análise abrangente e imparcial do tema (PRODANOV E FREITAS, 2013).

Por esse percalço metodológico foi feito um levantamento da aplicabilidade da Identidade de Sophie Germain por diferentes áreas da matemática, sempre buscando a viabilidade da utilização dos números primos de Sophie Germain por diversas situações, tais como: no Último Teorema de Fermat; em Equações Diofantinas e na Teoria dos Resíduos Quadráticos.

5 RESULTADOS E DISCUSSÕES

Os resultados e discussões são etapas inseparáveis em qualquer projeto de pesquisa. Compreender, validar e analisar criticamente os resultados são alicerces para o conhecimento e para a tomada de decisões. Ao valorizar esse ciclo de reflexão é possível avançar de forma mais sólida e consciente. A seguir discorreremos sobre as contribuições dos números primos de Sophie Germain.

5.1 Contribuição de Sophie Germain para a resolução do Último Teorema de Fermat

Sophie Germain contribuiu para a teoria do Último Teorema de Fermat ao investigar a equação $x^n + y^n = z^n$ para o caso em que *n* é um número primo. Ela utilizou essa descoberta para provar um caso especial do Teorema de Fermat, conhecido como o "Teorema de Fermat para números primos". A demonstração completa pode ser vista em EDWARDS (2000). Este teorema afirma que, se *p* é um número primo ímpar e a, b são inteiros positivos tais que a e b não são divisíveis por p, então $a^{(p-1)} + b^{(p-1)}$ é um múltiplo de p. A equação

$$x^n + y^n = z^n,$$

para todo $n \in \mathbb{N}$ com $n > 2$, não possui soluções inteiras não-nulas.

Teorema 5.1 (Teorema de Sophie Germain) Seja n um número primo ímpar, se houver um número primo p auxiliar com as seguintes propriedades:
1. $x^n + y^n + z^n \equiv 0 \bmod p$ *implica que* $x \equiv 0$ *ou* $y \equiv 0$ *ou* $z \equiv 0 \bmod p$, *e*
2. $x^n \equiv n \bmod p$ *é impossível*,
se o Último Teorema de Fermat for verdadeiro para n, então vale o caso I do teorema de Fermat para n, isto é, se nenhum dos x, y ou z for divisível por n então a equação $x^n + y^n + z^n = 0$ não possui soluções inteiras para além da nula. (EDWARDS, 2000).

Como exemplo, suponhamos que n = 5. Se considerarmos p = 11, vemos que a primeira condição do teorema é satisfeita, uma vez que, módulo 11, as quintas

potências são congruentes a 0, 1 ou –1. Então, para $x^5 + y^5 + z^5 \equiv 0 \bmod p$, uma das quantidades tem de ser divisível por 11. Note-se que, pelo pequeno teorema de Fermat, a décima potência de um número qualquer módulo 11 é sempre congruente a 1 se esse número não for divisível por 11.

A nota de Fermat dizia o seguinte em latim, com tradução para o português citado por Singh (2008, p. 80):

> É impossível para um cubo ser escrito como a soma de dois cubos ou uma quarta potência ser escrita como uma soma de dois números elevados a quatro, ou, em geral, para qualquer número que seja elevado a uma potência maior do que dois ser escrito como a soma de duas potências semelhantes. Eu tenho uma demonstração realmente maravilhosa para esta proposição, mas a margem é muito estreita para contê-la.

Sophie Germain provou esse teorema usando a relação que ela descobriu entre os números primos e as formas quadráticas. Ela mostrou que a equação $a^{(p-1)} + b^{(p-1)}$ é equivalente a uma forma quadrática e que essa forma quadrática é congruente a 0 módulo p, o que significa que é um múltiplo de p.

Embora Sophie Germain não tenha conseguido provar o Último Teorema de Fermat em si, suas contribuições para a teoria dos números primos e sua relação com as formas quadráticas foram fundamentais para o desenvolvimento da teoria moderna dos números.

5.2 Equações diofantinas e aplicabilidade

Uma equação Diofantina é uma equação polinomial onde as soluções desejadas são números inteiros. Um exemplo de equação Diofantina que envolve números primos de Sophie Germain é a seguinte:

$$(p - q)(p + q) + 4q^2 = n^2$$

Nessa equação, p e q são primos de Sophie Germain, e n é um número inteiro desconhecido que buscamos encontrar. A equação relaciona a diferença e o produto de p e q, juntamente com um termo quadrático, a um quadrado perfeito n^2.

As soluções dessa equação Diofantina são encontradas quando valores inteiros adequados para p, q e n satisfazem a equação. No entanto, a dificuldade está em encontrar esses valores que sejam soluções válidas.

A equação Diofantina mencionada acima pode ser explorada para estudar as propriedades dos primos de Sophie Germain e suas relações com quadrados perfeitos. A resolução completa e a obtenção das soluções específicas exigiriam um estudo mais aprofundado e técnicas específicas de resolução de equações Diofantinas.

5.3 A Teoria dos Resíduos Quadráticos com os primos de Sophie Germain

A teoria dos resíduos quadráticos é uma área importante em teoria dos números que estuda as propriedades dos resíduos quadráticos é o módulo um número inteiro. Um dos resultados interessantes desta teoria é a relação entre os primos de Sophie Germain e os resíduos quadráticos.

A relação entre os primos de Sophie Germain e os resíduos quadráticos é dada pelo Teorema de Quadrados de Euler, que afirma que se p é um número primo ímpar, então:

$$a^{\frac{(p-1)}{2}} \equiv \pm 1 \pmod{p}$$

para todo a que é um resíduo quadrático módulo p (isto é, a tem uma raiz quadrada módulo p) e a ≠ 0, e:

$$a^{\frac{(p-1)}{2}} \equiv \pm i \pmod{p}$$

para todo a que é um não-resíduo quadrático módulo p (isto é, a não tem uma raiz quadrada módulo p) e a≠0, onde i é a unidade imaginária.

Exemplo 5.3 Utilizaremos os primos de Sophie Germain (11, 23)

Para determinar se 11 e 23 são resíduos quadráticos módulo um certo primo p, podemos aplicar o Teorema do Quadrado de Euler.

Se o valor da expressão acima for +1, então a é um resíduo quadrático módulo p. Se for –1, então a não é um resíduo quadrático módulo p.

Vamos considerar o caso em que p = 13

Para a = 11 temos:

$11^6 \equiv 12 \pmod{13} \equiv -1 \pmod{13}$

Assim, 11 não é um resíduo quadrático módulo 13.

Para a = 23 temos:

$23^6 \equiv 1 \pmod{13}$

Assim, 23 é um resíduo quadrático módulo 13.

5.4 Primos gêmeos e primos de Sophie Germain

Os números primos gêmeos e os números primos de Sophie Germain estão relacionados através de uma propriedade especial entre eles. Para entender essa relação, é importante entender a definição de cada um desses conceitos.

Os números primos gêmeos são pares de números primos consecutivos que diferem em 2. Em outras palavras, são números primos que possuem uma diferença de dois entre eles. Alguns exemplos de números primos gêmeos são (3, 5), (5, 7), (11, 13), (17, 19), entre outros.

Por outro lado, podemos ter pares de números primos da forma (p, 2p + 1), onde p é um número primo de Sophie Germain e 2p + 1 também é um número primo. Alguns exemplos de pares de números primos onde o primeiro número é primo de Sophie Germain são (2, 5), (3, 7), (5, 11), (11, 23), entre outros.

A relação entre esses dois conceitos é que um par de números primos gêmeos também pode ser considerado um par de números primos de Sophie Germain. Isso ocorre no seguinte par de números primos gêmeos (3, 5) pois 3 é um número primo e $2 \cdot 3 + 1 = 7$ também é primo; assim como, 5 é um número primo e $2 \cdot 5 + 1 = 11$ também é primo, satisfazendo o critério de Sophie Germain.

Vale ressaltar que os primos de Sophie Germain são importantes na criptografia de chave pública, uma vez que são usados em algoritmos criptográficos

como o RSA[8] (COUTINHO, 2014) e a assinatura de DSA[9] (STALLINGS, 2017; STINSON; PATERSON, 2019). Esses algoritmos são baseados na dificuldade de fatorar números grandes em seus fatores primos. Os primos de Sophie Germain são usados nesses algoritmos porque eles têm propriedades matemáticas que os tornam difíceis de fatorar.

Enquanto os primos gêmeos também têm implicações importantes na teoria dos números e na criptografia. Eles são usados em algoritmos criptográficos como o Goldwasser-Micali[10], que é baseado na dificuldade de determinar se um número é primo ou composto. Os primos gêmeos têm sido objeto de estudo há séculos, e sua distribuição é um problema em aberto na teoria dos números.

5.5 Aplicabilidade dos primos de Sophie Germain no meio avaliativo

No contexto específico do meio avaliativo, pode haver várias aplicações dos primos de Sophie Germain. As questões sobre os primos de Sophie Germain podem ser incluídas em provas e avaliações em diferentes níveis de ensino, dependendo do objetivo pedagógico e do nível de conhecimento dos estudantes.

Também podem ser úteis em preparação para provas de matemática, pois elas frequentemente aparecem em exames e competições de nível avançado. Ao resolver essas questões, os estudantes podem melhorar suas habilidades em resolução de problemas, raciocínio lógico e dedução matemática.

O objetivo de compreender a matemática desde seus primórdios e fornecer uma justificativa para o ensino é estudar sua história, não apenas para expressar suas origens, evolução ou aplicações na vida cotidiana dos alunos, mas também para expandir suas visões de mundo e desafiar o *status* que, está permitindo para maior interação e intervenção em sua realidade. Isso transcende aspectos teóricos e práticos, evocando a matemática inerente que os humanos seguem desde as

[8] O algoritmo RSA foi descrito no final da década de 70 e o acrônimo RSA é composto pelas letras iniciais dos sobrenomes dos criadores Ron Rivest, Adi Shamir e Leonard Adleman.
[9] Um algoritmo de assinatura digital (DSA) refere-se a um padrão para assinaturas digitais. Foi introduzido em 1991 pelo Instituto Nacional de Padrões e Tecnologia (NIST) como o melhor método de criação de assinaturas digitais.
[10] O sistema criptográfico Goldwasser-Micali é um algoritmo de criptografia de chave assimétrica desenvolvido por Shafi Goldwasser e Silvio Micali em 1982. A GM tem a distinção de ser o primeiro esquema probabilístico de criptografia de chave pública que é comprovadamente seguro sob suposições criptográficas padrão.

cavernas. Os raciocínios elementares os transformam em indivíduos capazes de gerar pensamento criativo e resolver problemas cotidianos.

> A matemática não é uma superprodução onde os atores principais são gênios – mesmo que a genialidade esteja presente nos processos de criação –, que fizeram tudo individualmente, do começo ao fim de cada teoria. Na maioria, homens sem falhas e sem dúvidas. E é com este enredo que a história deve contar para procurar atuar na melhoria das atitudes dos alunos – e professores – frente à matemática. Penso que o contato com a história é imprescindível para oferecer uma visão dinâmica da disciplina, de sua evolução e desenvolvimento e, desta forma, dar significação aos seus conceitos. (PETERS, 2005, p. 9).

As questões podem ser mais simples e concentrar-se na definição dos primos de Sophie Germain e em propriedades básicas dos números primos, quando se atribui a devida significação aos seus conceitos e os utiliza em níveis mais básicos. Por exemplo, uma questão pode pedir aos alunos para identificar um número que é um primo de Sophie Germain ou pedir-lhes para explicar por que determinado número não pode ser um primo de Sophie Germain.

Exemplo 5.5.1

(Universidade Federal Fluminense – UFF 2005) Sophie Germain introduziu em seus cálculos matemáticos um tipo especial de número primo descrito abaixo. Se p é um número primo e se 2p + 1 também é um número primo, então o número primo p é denominado primo de Germain. Pode-se afirmar que é primo de Germain o número:

Sophie Germain (1776-1831)

Alternativas:

A) 7

B) 17

C) 18

D) 19

E) 41

RESPOSTA: item E

Em níveis mais avançados, as questões sobre os primos de Sophie Germain podem ser usadas para avaliar a compreensão dos alunos sobre a Teoria dos Números e suas aplicações em áreas como criptografia e testes de primalidade. As questões podem envolver a identificação de pares de números primos de Sophie Germain, a resolução de problemas que dependem da propriedade desses números, ou a aplicação de algoritmos que usam números primos para resolver problemas específicos.

Exemplo 5.5.2

(Universidade Estadual de Londrina – UEL 2022) Em um mundo predominantemente masculino, mulheres foram, sistematicamente, impedidas de fazer parte do universo da pesquisa. Sem jamais ter perdido a esperança, último dos predicados da Caixa de Pandora, a matemática Sophie Germain (1776-1831) lutava e sofria com tais preconceitos, chegando, até mesmo, a apresentar-se com o pseudônimo masculino Monsier Le Blanc.

Adaptado de: FLOOD, Raymond e WILSON, Robin. Os grandes matemáticos. São Paulo: M. Books do Brasil, 2013. p.126

Sophie Germain é conhecida por provar, matematicamente, que se *x, y, z, n* são inteiros positivos e satisfazem às seguintes condições simultaneamente

i) x, y, z são diferentes de 0;
ii) mdc(x, y) = mdc(y, z) = mdc(z, x) = 1;
iii) n é um número primo maior que 2;
iv) 2n + 1 é um número primo;
v) $x \cdot y \cdot z$ não é múltiplo de n,

então $x^n + y^n \neq z^n$. Por outro lado, se x, y, z, n não satisfazem simultaneamente as condições dadas, deve-se checar, por outro método, se $x^n + y^n \neq z^n$ ou $x^n + y^n = z^n$.

Com base no enunciado e nos conhecimentos matemáticos, atribua V (verdadeiro) ou F (falso) às afirmativas a seguir.

( ) $1^{11} + 23^{11} = 24^{11}$
( ) $3^2 + 4^2 = 5^2$
( ) $67^5 + 71^5 \neq 79^5$
( ) $\{n \in \mathbb{N}$ tal que n é um número primo$\} \subset \{n \in \mathbb{N}$ tal que 2n + 1 é um número primo$\}$
( ) $\{n \in \mathbb{N}$ tal que n é um número primo$\} \cap \{n \in \mathbb{N}$ tal que 2n + 1 é um número primo$\} \neq \emptyset$

Assinale a alternativa que contém, de cima para baixo, a sequência correta.

A) V, V, F, V, F.
B) V, F, F, F, V.
C) F, V, V, F, V.
D) F, V, F, V, V.
E) F, F, V, F, V.

RESPOSTA: item C

A importância pedagógica das questões dos primos de Sophie Germain reside no fato de que elas incentivam os estudantes a explorar a relação entre números primos e a desenvolver habilidades em Teoria dos Números. Além disso, elas também podem ajudar a desenvolver habilidades em Álgebra e manipulação de expressões matemáticas.

É importante notar que o Teorema de Sophie Germain não é uma ferramenta infalível para resolver questões envolvendo números primos. Existem números primos que não podem ser escritos na forma $a^2 + 2b^2$, e existem números que podem ser escritos dessa forma, mas ainda assim não são primos. No entanto, em muitos casos, o teorema pode ser uma ferramenta útil para simplificar a resolução de problemas envolvendo números primos.

6 CONSIDERAÇÕES FINAIS

O critério de Sophie Germain é uma condição necessária para que um número ímpar p seja primo. A condição é que, se existir um número inteiro q primo satisfazendo a equação 2p + 1 = q, então p é primo de Sophie Germain.

O critério de Sophie Germain é importante na teoria dos números porque fornece uma maneira de verificar se um número ímpar pode ser um primo de Sophie Germain sem a necessidade de testar explicitamente se ele é primo. Isso é útil porque testar explicitamente se um número é primo pode ser uma tarefa muito demorada e difícil, especialmente quando se lida com números grandes. Além disso, o critério de Germain é um exemplo da habilidade de Sophie Germain em encontrar condições importantes para a primalidade de um número.

Contudo, os primos de Sophie Germain têm aplicações importantes na criptografia, uma vez que são usados em algoritmos criptográficos como o RSA e a assinatura de DSA. Esses algoritmos são baseados na dificuldade de fatorar números grandes em seus fatores primos. Os primos de Sophie Germain são úteis nesses algoritmos porque eles têm propriedades matemáticas que os tornam difíceis de fatorar.

Através do legado de Sophie Germain e dos esforços contínuos de matemáticos e pesquisadores, esses números primos continuam a inspirar descobertas e explorar os mistérios dos números primos, contribuindo para o avanço do conhecimento e a beleza intrínseca da matemática. Ao abraçar essa rica área de estudo, perpetuamos o impacto duradouro de Sophie Germain e continuamos a desvendar os enigmas dos números primos na busca incessante pelo entendimento mais profundo de nosso universo matemático.

REFERÊNCIAS

A PERFEIÇÃO DO SISTEMA INDO-ARÁBICO. **Matematizar**, 18 jul. 2012. Disponível em: http://matematizare.blogspot.com/2012/07/a-perfeicao-do-sistema-de-numeracao.html. Acesso em: 15 dez. 2022.

AAKER, David A.; KUMAR, V.; DAY, George S. **Pesquisa de marketing**. São Paulo: Atlas, 2004. 745 p.

CLUBES DE MATEMÁTICA DA OBMEP. **Marie Sophie Germain**. Disponível em: http://clubes.obmep.org.br/blog/b_marie-sophie-germain/. Acesso em: 12 abr. 2023.

CLUBES DE MATEMÁTICA DA OBMEP. **Problemão**: Outro produto notável. Disponível em: http://clubes.obmep.org.br/blog/problemao-outro-produto-notavel/. Acesso em: 22 abr. 2023.

COPS – Coordenadoria de Processos Seletivos. **Vestibular UEL 2022**. Disponível em: https://www.cops.uel.br/v2/download.php?Acesso=NTc0NTQyMzZjZTU3Mzg2MDZkNzAwMjMyMmVmZjA2MjJiM2EzNjg5NDhlYTY1NGM5NGU3N2Q0NGNkYTM2NTUzZjYwMTYyNmQzY2M5MWFlNDg5M2Q3YTM5MzE0MjJiOWRjOTc0Y2E1YmFiN2RlZDIyZGM4ZjNhN2Q4NjllNjY0MzBlOGM2MmQxNzA3Y2ExOGVjYmQ1MDc5ZjU0Yjc4ZTk0Zg==. Acesso em: 20 jun. 2023.

COUTINHO, Severino Collier. **Números Inteiros e Criptografia RSA**. 2. ed. Rio de Janeiro: IMPA, 2014. 226 p.

COUTINHO, Severino Collier. **Criptografia**. Rio de Janeiro: IMPA, 2015. 217 p.

CRIVO. Dicionário Michaelis On-line, 11 jan. 2023. Disponível em: http://michaelis.uol.com.br/. Acesso em: 11 jan. 2023.

CURSOS PREPARATÓRIOS PARA O ENEM E VESTIBULARES – ESTRATÉGIA VESTIBULARES. **Questão Sophie Germain introduziu em seus cálculos matemáticos um tipo especial de número primo descrito abaixo. Se p ...** Disponível em: https://vestibulares.estrategia.com/public/questoes/Sophie-Germain501ea285ab/. Acesso em: 20 jun. 2023.

DOMINGUES, Joelza Ester. **Osso de Ishango**: os primórdios da Matemática na África Paleolítica. Ensinar História - Joelza Ester Domingues, 26 mar. 2022. Disponível em: https://ensinarhistoria.com.br/osso-de-ishango-primordios-da-matematica-na-africa-paleolitica/. Acesso em: 21 dez. 2022.

EDWARDS, Harold M. **Fermat's last theorem**: a genetic introduction to algebraic number theory. 1. softcover printing ed. New York: Springer, 2000. 407 p.

EVES, Howard. **Introdução à história da matemática**. 5. ed. Campinas: Editora da UNICAMP, 2011. 843 p. Tradução de Hygino H. Domingues.

GARBI, Gilberto Geraldo. **A rainha das ciências**: um passeio histórico pelo maravilhoso mundo da matemática. 5. ed. São Paulo: Editora Livraria da Física, 2007. 450 p.

GIL, Antonio Carlos. **Métodos e técnicas de pesquisa social**. 6. ed. São Paulo: Atlas, 2008. 200 p.

GOUVÊA, Fernando Quadros. **Uma demonstração maravilhosa**. Revista Matemática Universitária, n. 19, p. 16-43, dezembro de 1995. Disponível em: https://rmu.sbm.org.br/wp-content/uploads/sites/27/2018/03/n19_Artigo03.pdf. Acesso em: 21 maio 2023.

HALL, Natascha; JONES, Mary; JONES, Gareth. A Vida e o Trabalho de Sophie Germain. **Gazeta de Matemática**, Portugal, nº 146, p. 32-35, janeiro de 2004. Disponível em: http://gazeta.spm.pt/getArtigo?gid=89. Acesso em: 08 maio 2023.

HESPANHA, António Manuel. **Imbecilitas**: as bem-aventuranças da inferioridade nas sociedades de Antigo Regime. São Paulo: Annablume, 2010. 294 p.

IMENES, Luiz Márcio. **A numeração indo-arábica**. 7. ed. São Paulo: Scipione,1995. 48 p. (Coleção Vivendo a Matemática).

KILHIAN, Kleber. **O Corpus Arquimediano.**, [s.d.]. Disponível em: https://www.obaricentrodamente.com/2011/04/o-corpus-arquimediano.html. Acesso em: 14 abr. 2023.

KÖCHE, José Carlos. **Fundamentos de metodologia científica**: Teoria da ciência e iniciação à pesquisa. 21. ed. Petrópolis: Vozes, 2003. 184 p.

LOPES, Frederico. **Eratóstenes**: seu crivo e a circunferência da Terra. Disponível em: https://fredlopes.com.br/eratostenes-seu-crivo-e-a-circunferencia-da-terra/. Acesso em: 05 jan. 2023.

MARCONI, Maria de Andrade; LAKATOS, Eva Maria. **Metodologia científica**. São Paulo: Editora Atlas, 2004. 392 p.

MARTÍNEZ, Fábio Brochero; MOREIRA Carlos Gustavo; SALDANHA, Nicolau; TENGAN, Eduardo. **Teoria dos Números**: um passeio com primos e outros números familiares pelo mundo inteiro. 4. ed. Rio de Janeiro: IMPA, 2018.

MORAIS FILHO, Daniel Cordeiro de. **As mulheres na matemática**. Revista do professor de matemática. n. 30, 1996. Disponível em: https://rpm.org.br/cdrpm/30/2.htm. Acesso em: 12 abr. 2023.

MONTUCLA, Jean-Étienne. (1725-1799). **Histoire des mathématiques. T. 1 /, dans laquelle on rend compte de leurs progrès depuis leur origine jusqu'à nos jours... Nouvelle édition... par J.-F. Montucla,...** [s.l: s.n.]. Disponível em: https://gallica.bnf.fr/ark:/12148/bpt6k1076512.texteImage. Acesso em: 12 abr. 2023.

OLIVEIRA, Cristiane Monteiro de. **A presença das mulheres nas ciências exatas**. 2012. 71 f. Trabalho de conclusão de curso (Graduação em licenciatura em Matemática) – Faculdade de Engenharia, Universidade Estadual Paulista, Guaratinguetá, 2012. Disponível em: http://hdl.handle.net/11449/120256. Acesso em: 13 abr. 2023.

PETERS, José Roberto. **A História da Matemática no Ensino Fundamental**: uma análise de livros didáticos e artigos sobre história. 2005. 144 f. Dissertação (Mestrado em Educação Científica e Tecnológica) – Programa de Pós-graduação, Centro de Ciências Físicas e Matemáticas, Centro de Ciências da Educação, Centro de Ciências Biológicas, Universidade Federal de Santa Catarina, Florianópolis, 2005. Disponível em: https://repositorio.ufsc.br/bitstream/handle/123456789/102559/221350.pdf. Acesso em: 21 jun. 2023.

PRODANOV, Cleber Cristiano; FREITAS, Ernani César de. **Metodologia do trabalho científico**: métodos e técnicas da pesquisa e do trabalho acadêmico. 2. ed. Novo Hamburgo: Feevale, 2013. 276 p.

PROFESSOR SE APROXIMA DE PROVA SOBRE NÚMEROS PRIMOS. **Folha de São Paulo**, São Paulo, 11 jun. 2013. Ciência. Disponível em: https://m.folha.uol.com.br/ciencia/2013/06/1292713-professor-se-aproxima-de-prova-sobre-numeros-primos.shtml. Acesso em: 15 jan. 2023.

RIBENBOIM, Paulo. **Números primos**: Velhos mistérios e novos recordes. Rio de Janeiro: IMPA, 2020. 280 p.

RIBENBOIM, Paulo. **The Little Book of Bigger Primes**. 2. ed. New York: Springer, 2004. 356 p.

RICHARDSON, Roberto Jarry. **Pesquisa social**: métodos e técnicas. 3 ed. São Paulo: Atlas, 1999. 424 p.

RUDIO, Franz Victor. **Introdução ao projeto de pesquisa científica**. 34. ed. Petrópolis: Vozes, 2007. 144 p.

RUIZ, João Álvaro. **Metodologia científica**: guia para eficiência nos estudos. 6. ed. São Paulo: Atlas, 2006. 184 p.

SELLTÍZ, Claire; WRIGHTSMAN, Samuel Lawrence; COOK, Stuart Wellford; KIDDER, Louise H. **Métodos de pesquisa nas relações sociais**. 2. ed. São Paulo: EPU, 1987. 136 p. Tradução de Maria Martha Hubner d'Oliveira e Miriam Marinotti del Rey.

SILVEIRA, José Francisco Porto da. **Por que o nome primos para os números primos?** Disponível em: http://www.mat.ufrgs.br/~portosil/pqprimo.html. Acesso em: 04 jan. 2023.

SILVEIRA, José Francisco Porto da. **Senso numérico: a concepção intuitiva de número**. Disponível em: http://www.mat.ufrgs.br/~portosil/senso.html. Acesso em: 04 jan. 2023.

SINGH, Simon. **O Último Teorema de Fermat**: A história do enigma que confundiu as maiores mentes do mundo durante 358 anos. 13. ed. Rio de Janeiro: Record, 2008. 328 p. Tradução Jorge Luiz Calife.

SOPHIE GERMAIN (P). **PrimePages: prime number research records and results**. Disponível em: https://t5k.org/top20/page.php?id=2. Acesso em: 21 fev. 2023.

STALLINGS, William. **Cryptography and network security**: principles and practice. 7. ed. New York: Person, 2017. 766 p.

STINSON, Douglas Robert; PATERSON, Maura B. **Cryptography**: theory and practice. 4. ed. Boca Raton: CRC Press, Taylor & Francis Group, 2019. 580 p.

TENÓRIO. Marlon. **Número primo**. Disponível em: https://marlontenorio.wordpress.com/tag/numero-primo/. Acesso em: 12 jan. 2023.

THE LARGEST KNOWN PRIMES (DATABASE SUMARY). **PrimePages: prime number research records and results**. Disponível em: https://primes.utm.edu/largest.html. Acesso em: 10 jan. 2023.

TRIVIÑOS, Augusto Nibaldo Silva. **Introdução à pesquisa em ciências sociais**: a pesquisa qualitativa em educação. São Paulo: Atlas, 1987. 175 p.

UNIVERSIDADE ESTADUAL DO CEARÁ. Sistema de Bibliotecas. **Guia de normalização de trabalhos acadêmicos**. 4. ed. Fortaleza, CE, 2022. 170 p. Disponível em: https://www.uece.br/biblioteca/wpcontent/uploads/sites/27/2022/12/GUIA-UECE-2022__Atualizado-13.12.2022.pdf. Acesso em: 28 dez. 2022

VIANA, Marcelo. Primos gêmeos constituem um dos mistérios mais intrigantes. **Folha de São Paulo**, São Paulo, 16 mar. 2018. Opinião. Disponível em: https://www1.folha.uol.com.br/colunas/marceloviana/2018/03/primos-gemeos-constituem-um-dos-misterios-mais-intrigantes-da-aritmetica.shtml. Acesso em: 08 jan. 2023.

VIANA, Marcelo. Sophie Germain mostrou que uma mulher pode ser cientista. **Folha de São Paulo**, São Paulo, 25 maio 2022. Opinião. Disponível em: https://www1.folha.uol.com.br/colunas/marceloviana/2022/05/sophie-germain-mostrou-que-uma-mulher-pode-ser-cientista.shtml. Acesso em: 08 jan. 2023.

WIKIPEDIA. **Ficheiro:Bézout, Étienne – Cours de mathématiques, a l'usage du corps de l'artillerie, 1798 – BEIC 12049846.jpg – Wikipédia, a enciclopédia livre**. Disponível em: https://commons.wikimedia.org/wiki/File:B%C3%A9zout,_%C3%89tienne_%E2%80

%93_Cours_de_math%C3%A9matiques,_a_l%27usage_du_corps_de_l%27artillerie,_1798_%E2%80%93_BEIC_12049846.jpg. Acesso em: 12 abr. 2023.

ZIKMUND, William G. **Business research methods**. 5. ed. Fort Worth: Dryden, 1997. 829 p.