UNIVERSIDADE FEDERAL DO NORTE DO TOCANTINS
CAMPUS DE ARAGUAÍNA
CENTRO DE CIÊNCIAS INTEGRADAS
CURSO DE GRADUAÇÃO EM LINCECIATURA EM MATEMÁTICA

RHIEL NATHAM RIBEIRO DE SOUZA

INTEIROS QUE SÃO SOMAS DE DOIS QUADRADOS:
UMA INTERFACE ENTRE PRIMOS E CONGRUÊNCIA MODULAR

Araguaína-TO
2022

RHIEL NATHAM RIBEIRO DE SOUZA

INTEIROS QUE SÃO SOMAS DE DOIS QUADRADOS:
UMA INTERFACE ENTRE PRIMOS E CONGRUÊNCIA MODULAR

Monografia foi avaliada e apresentada à UFNT – Universidade Federal do Norte do Tocantins – Campus Universitário de Araguaína, Curso de Licenciatura em Matemática para obtenção do título de Licenciado em Matemática e aprovada em sua forma final pelo Orientador e pela Banca Examinadora.

Orientador: Prof. Dr. José Carlos de Oliveira Junior

Araguaína-TO
2022

Dados Internacionais de Catalogação na Publicação (CIP)
Sistema de Bibliotecas da Universidade Federal do Tocantins

D467i De Souza, Rhiel Natham Ribeiro .

INTEIROS QUE SÃO SOMAS DE DOIS QUADRADOS: UMA INTERFACE ENTRE PRIMOS E CONGRUÊNCIA MODULAR . / Rhiel Natham Ribeiro De Souza. – Araguaína, TO, 2022.

50 f.

Monografia Graduação - Universidade Federal do Tocantins – Câmpus Universitário de Araguaína - Curso de Matemática, 2022.

Orientador: José Carlos de Oliveira Junior

1. Números Primos. 2. Quadrados Perfeitos . 3. Teoria dos Números. 4. Soma de Quadrados. I. Título

CDD 510

Elaborado pelo sistema de geração automática de ficha catalográfica da UFT com os dados fornecidos pelo(a) autor(a).

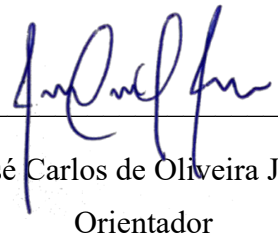
RHIEL NATHAM RIBEIRO DE SOUZA

INTEIROS QUE SÃO SOMAS DE DOIS QUADRADOS:
UMA INTERFACE ENTRE PRIMOS E CONGRUÊNCIA MODULAR

Monografia foi avaliada e apresentada à UFNT – Universidade Federal do Norte do Tocantins – Campus Universitário de Araguaína, Curso de Licenciatura em Matemática para obtenção do título de Licenciado em Matemática e aprovada em sua forma final pelo Orientador e pela Banca Examinadora.

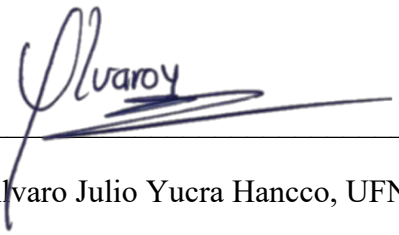
Data de aprovação: 14/12/2022

Banca Examinadora:



Prof. Dr. José Carlos de Oliveira Junior, UFNT

Orientador



Prof. Dr. Alvaro Julio Yucra Hancco, UFNT

Profa. Dra. Renata Alves da Silva, UFNT

Araguaína-TO
2022

Não importa o quão poderoso você se torne,
nunca tente fazer tudo sozinho, caso contrário
irá falhar. (Itachi Uchiha).

AGRADECIMENTOS

Agradecer a instituição Universidade Federal do Norte do Tocantins (UFNT). Agradecer aos meus familiares por todo apoio, à minha mãe, Ana Cleide de Matos Barbosa Souza, e ao meu pai, Ronipeperson Ribeiro de Souza. À minha irmã, Rhana Kimberly Matos de Souza, e ao meu irmão, Ronipeperson Ribeiro de Souza Junior.

Agradecer aos professores do meu ensino médio, Liliane Pereira Rocha e Graciano Martins, que me influenciaram a entrar em uma faculdade. Agradecer ao meu orientador, Prof. Dr. José Carlos de Oliveira Junior, e agradecer a todos os professores do curso de Licenciatura em Matemática da UFNT.

Agradecer à minha namorada, Ana Claudia Sousa Silva, por todo apoio e por ajudar nessa jornada. Agradecer a todos os meus amigos e colegas que me apoiaram e ajudaram nessa caminhada. A todos, o meu muito obrigado.

RESUMO

Este trabalho traz consigo um estudo sobre Teoria dos Números. Seu principal objetivo é provar o teorema dos quadrados perfeitos de Fermat, ou seja, estabelecer quais números inteiros podem ser escritos como a soma de dois quadrados perfeitos $x^2 + y^2$, com $x, y \in \mathbb{Z}$ e como objetivo secundário demonstrar quais não podem ser escritos de tal forma. Junto com estas demonstrações, temos como complemento a história e curiosidades sobre os teoremas e os conteúdos contidos nesta pesquisa. O trabalho é uma pesquisa qualitativa de caráter bibliográfico, onde baseamo-nos em estudos já pré-estabelecidos: livros e artigos científicos. Foram estabelecidos, ao decorrer deste trabalho, as definições e os resultados de diversos conteúdos que corroboram para a demonstração principal. Como resultado, foram apresentados de forma generalizada os números que podem e não podem ser formados pela soma de dois quadrados. Assim, conclui-se a partir das obras bibliográficas uma visão mais clara do teorema e de sua demonstração.

Palavras-chaves: Números Primos. Quadrados perfeitos. Teoria dos Números.

ABSTRACT

This work brings with it a study on Number Theory. Its main objective is to prove Fermat's perfect square theorem, that is, to establish which whole numbers can be written as the sum of two perfect squares $x^2 + y^2,\ x, y \in \mathbb{Z}$ and as a secondary objective to demonstrate which ones cannot be written in such a way. Along with these demonstrations, we have as a complement the history and curiosities about the theorems and the contents contained in this research. The work is qualitative bibliographical research, where we base ourselves on studies already pre-established: books and scientific articles. During this work, the definitions and results of several contents that corroborate the main demonstration were established. As a result, the numbers that can and cannot be formed by the sum of two squares were presented in a generalized way. Thus, a clearer view of the theorem and its demonstration can be concluded from the bibliographical works.

Keywords: Prime numbers. Perfect squares. Number theory.

LISTA DE ILUSTRAÇÕES

LISTA DE ABREVIATURAS E SIGLAS

UFNT	Universidade Federal do Norte do Tocantins
TNP	Teorema do Número Primo
TFA	Teorema Fundamental da Aritmética
RE	Relação de Equivalência

LISTA DE SÍMBOLOS

$\mathbb{Z}$	Inteiros
$\mathbb{N}$	Naturais
$\mathbb{C}$	Complexos
$\equiv$	Congruência
mod	Módulo
%	Porcentagem
log	Logaritmo
$\sum$	Somatório
$\prod$	Produtório
π(x)	Função de Euler, contagem de primos menores ou iguais a x
ζ(s)	Função Zeta aplicada em s
$\eta(s)$	Função Eta aplicada em s
$\rightarrow$	Implica, então
$\leftrightarrow$	Se, e somente se,

SUMÁRIO

1. INTRODUÇÃO

Desde muito cedo, o interesse na Matemática surgiu e junto com ele a curiosidade sobre os números e suas composições, que de certa maneira descrevem nosso mundo por meio da lógica, uma vez que, em diversas formas, os números estão presentes em nossa comunicação e em outras partes do cotidiano (tecnologia, educação, entretenimento e outros). Esse é um dos motivos para compreender Matemática em sua essência. Porém, como entendê-la sem antes entender como os próprios números se compõem? Assim, surge um dos questionamentos norteadores dessa pesquisa: Como os números inteiros se decompõem? Essa é a curiosidade que movimenta uma das engrenagens mais importantes deste trabalho.

Portanto, temos como objetivo definir e demonstrar quais números inteiros $n \in \mathbb{Z}$ podem ser escritos como a soma de dois quadrados perfeitos, ou seja, $x^2 + y^2$; $x, y \in \mathbb{Z}$. É óbvio que existem números que podem ser representados por $x^2 + y^2$:

$$2 = 1^2 + 1^2,$$
$$4 = 2^2 + 0^2,$$
$$5 = 2^2 + 1^2.$$

Esses são só alguns exemplos. Um problema pertinente é achar uma caracterização para eles. Vamos definir esse tipo de número n como um número *representável* (escrito pela soma de dois quadrados). Então, temos o seguinte: Que tipos de números inteiros n satisfazem a condição $n = x^2 + y^2$ com $x, y \in \mathbb{Z}$?

Antes de continuarmos, eis um desafio para que você, leitor, possa pensar durante sua leitura. Desafio: Dado o número $n = 270$, é possível escrevê-lo como a soma de dois quadrados $x^2 + y^2$? E o número 1764, é possível? Qual o padrão que aparece nas respostas dadas?

Esperamos que, até o final dessa monografia, você, leitor, consiga resolver esses questionamentos, mas não só isso, e sim entender de forma genérica que tipos de números podem e não podem ser representados dessa maneira.

Este trabalho tem caráter qualitativo e bibliográfico, onde baseamo-nos em estudos já pré-estabelecidos: livros e artigos científicos, tratando-se do teorema principal: "*Inteiros como Soma de Dois Quadrados"*. Suas definições, lemas e demonstrações terão como base teórica a obra de (AINGER ZIEGLER, 2018).

Para compreendermos um pouco sobre essas questões, vamos brevemente contextualizá-las. Ora, a origem do teorema ***Inteiros como Soma de Dois Quadrados***, o principal desta pesquisa, teve muitos matemáticos envolvidos que estudavam como números

podem ser representados. Euclides já considerava os números primos nos anos 300 a. C. Esses números desempenham um papel importante na caracterização dos números representáveis.

Diofanto (270 a. C.) trabalhou com uma temática muito semelhante a esse teorema. Ele afirmou que todo número $t \in \mathbb{Z}^+$ poderia ser escrito como a soma de quatro quadrados inteiros. Diversos matemáticos analisaram e trabalharam com temáticas também interligadas com este teorema como, por exemplo, em 1770, Waring (1734-1798), Lagrange (1736-1813) e outros pesquisadores famosos como Euler (1707-1783) e Hilbert (1862-1943). (EVANGELISTA, 2013. Pág. 13-14).

Aqui, daremos ênfase especial ao famigerado Pierre de Fermat (1601-1665), o mais conhecido pelo tão conhecido resultado, provado recentemente, chamado *O Último Teorema de Fermat* (SOUZA, 2019). Trataremos sobre seus resultados com mais detalhes no Capítulo 6 desta obra.

2. PRIMOS E CONGRUÊNCIA MODULAR

Trataremos de dois assuntos que serão os pilares deste trabalho: números primos e congruência modular. Falaremos primeiro dos números primos.

Muitos enxergam os primos como os átomos da Matemática pelo fato deles comporem diversos números. É uma visão justa para eles, porém preferimos dizer que os primos são análogos ao universo: são vastos e misteriosos, e entendê-los se torna essencial no mundo matemático. Então, a seguir, mostraremos desde a introdução histórica até as definições e demonstrações de resultados sobre os primos, a fim de habituar o leitor a este assunto e de bônus mostrar a grandeza deles. Em segundo lugar, falaremos a respeito de congruência módulo n, conteúdo oriundo da divisão euclidiana, a qual vamos introduzir antes de abordar congruência. Vamos usar no decorrer do trabalho o seguinte. Se p divide n, então $n = p * q$ para algum inteiro q. Nesse caso, escreveremos $\frac{n}{p} \coloneqq q$.

Vamos apresentar a definição e propriedades de congruência modular e mostrar algumas aplicações que este conteúdo tem na realidade. Temos como objetivo esclarecer e habituar o leitor ao conteúdo e ainda mostrar a importância deste conteúdo trazendo suas aplicações.

2.1 Introdução Histórica dos Números Primos

Este tópico irá tratar dos grandes estudiosos que trabalharam com os números primos. Daremos uma pequena explicação de quem foi cada um desses matemáticos e qual foi sua grande contribuição para a teoria. Desta maneira, pretendemos que você, leitor, tenha o conhecimento necessário sobre primos, para ter uma melhor leitura ao decorrer do trabalho.

Este tópico foi inteiramente baseado nas obras: (RIZEL, 2014); (FRITSCHE; SUGUIMOTO, 2015); (HISTÓRIA DOS NÚMEROS PRIMOS. BBC, 2017).

2.2 Matemáticos e os Números Primos

Euclides foi um matemático grego e escritor, nascido na antiga Alexandria por volta do ano 300 a. C. Conhecido principalmente por ser uns dos progenitores da Geometria onde ele tem mais contribuições, tendo até sua própria geometria, nomeada como Geometria Euclidiana. Se eternizou na história pela sua obra intitulada: Elementos de Euclides. Fez diversas

contribuições em outras áreas da Matemática, porém vamos nos atentar à área da teoria dos números primos.

Euclides trabalhou com os números primos no séc. III a. C. Neste período os matemáticos gregos tentavam registrar todos os números primos, a fim de eternizar seus nomes na história, mas Euclides a partir dos seus estudos demonstrou que não era possível tal feito, pois os números primos são infinitos. Escreveu essa demonstração numa das obras mais conhecidas do mundo matemático: Elementos de Euclides. Essa demonstração foi feita através de contradição, onde ele supôs que os primos são finitos e, então, demonstrou que tal afirmação fornece uma contradição. Trataremos com mais detalhes essa demonstração mais à frente.

No mesmo séc. III a. C., houve outro matemático interessado pelos números primos. Erastóstenes conhecido principalmente por ter calculado a circunferência máxima da terra, também é conhecido pela pesquisa nessa área. Seu trabalho se atentou na parte de contar e identificar estes números. Dessa forma ele construiu diversas tabelas ao longo da sua vida. Desses estudos e construções de tabelas, ele desenvolveu o famoso Crivo de Erastóstenes, que funciona da seguinte maneira: dado uma quantidade finita de números naturais, exemplo de 2 a 50, se tomarmos o primeiro primo na tabela, neste caso 2, e eliminar da tabela todos os seus múltiplos, e após isso repetir o processo para o próximo primo, em determinado momento, restarão apenas números primos. É importante destacar que isso não é uma prática viável para intervalos muito grandes, mas ainda assim é uma descoberta impressionante.

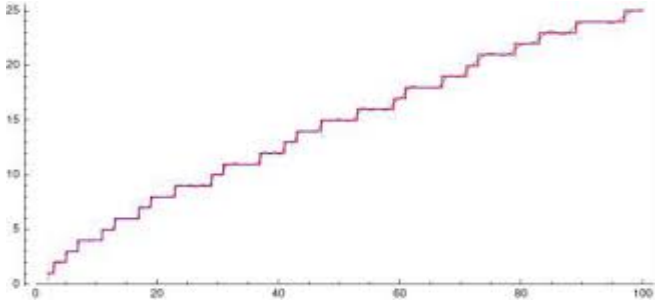
Quinze séculos depois, surgiu outro matemático que se fascinaria pelos números primos. Johann Carl Friedrich Gauss, o Príncipe da Matemática. Nascido na Alemanha em 1777, teve contribuições em diversas áreas da Matemática e em outras ciências como Astronomia. Acredita-se que Gauss teve seu primeiro interesse nesses números quando estudava tabelas de números primos em algum livro e, nesse ponto, despertou-se nele a curiosidade que nasce em geral naqueles que se debruçam sobre esses números: Como eles se comportam?

Não sabemos como eles se comportam, e Gauss sabia que não tinha como prever quando o próximo número primo ia aparecer. Portanto ele olhou tudo de uma nova perspectiva, ele começou a identificar quantos números primos existiam num intervalo de números, algo parecido com o que Erastóstenes fazia, dessa maneira ele percebeu que quanto maior o intervalo de números, menos números primos iam aparecendo.

Gauss acreditava que poderia se calcular a probabilidade de ter um número primo num intervalo numérico. Por exemplo: num bloco de 100 $(1\ a\ 100)$, teria $\frac{1}{4}$ de números primos que dá 25% de chances, então 25% dos números de $1\ a\ 100$ são primos. Ele percebeu que a cada

bloco de 10^n, ou seja, a cada $(100, 1000, 10000, \dots)$, a chance de encontrarmos primos ficam da seguinte forma: $(10^2 = 100 = \frac{1}{4}, 10^3 = 1000 = \frac{1}{6}, 10^4 = 10000 = \frac{1}{8})$; ou seja, $\frac{1}{4}$ de primos, $\frac{1}{6}$ de primos e $\frac{1}{8}$ de primos. Porém essa é uma aproximação apenas. Por exemplo, $1\ a\ 1000$, há 168 primos e a razão que Gauss deu para 1000 é $\frac{1}{6}$ que seria $16{,}666\ldots\%\ de\ 1000$ resultando em, aproximadamente, 166, dois a menos que o valor exato 168. Dessa maneira, esse comportamento graficamente se assimilava a uma escada que aumenta seus degraus a cada subida. Iremos nos referir a esse gráfico como a Escada de Gauss.

Figura 1 Gráfico da Escada de Gauss



Fonte: WILLIAN, 2015, P. 8 apud MAZUR; STEIN, 2015, p. 126

De certa maneira esse pensamento o leva a fazer uma contribuição ainda maior, onde foi possível encontra uma aproximação da função $\pi(x)$ a qual estabelecia uma quantidade de números primos em um determinando intervalo. A Figura 2 demonstra uma razão mais aproximada que a demonstrada anteriormente, que leva Gauss a perceber um certo padrão no comportamento dos primos.

Figura 2 Tabela de Primos

Tabela 1: Informações sobre $\pi(x)$

x	$\pi(x)$	$\frac{x}{\pi(x)}$	$\left(\frac{x}{\pi(x)}\right)_m - \left(\frac{x}{\pi(x)}\right)_{m-1}$
10	4	2.5	--
10^2	25	4	**1.5**
10^3	168	5.952	**1.952**
10^4	1229	8.136	**2.184**
10^5	9592	10.425	**2.288**
10^6	78498	12.739	**2.3138**
10^7	664579	15.047	**2.3079**
10^8	5761455	17.356	**2.309**
10^9	50847534	19.666	**2.309**
10^{10}	**455052511**	**21.975**	**2.308**

Fonte: WILLIAN, 2015, P. 8 apud CARNEIRO, 2014.

Ao observar a tabela da Figura 2, com intervalos 10^n, Gauss percebeu que quanto maior o primo mais próximo o valor da razão $\left(\frac{x}{\pi(x)}\right)_m$, menos razão anterior $\left(\frac{x}{\pi(x)}\right)_{m-1}$, ficava de 2,3. Usando o raciocínio anterior das porcentagens de primos num intervalo 10^n, ele concluiu a seguinte fórmula.

$$\frac{10^n}{2{,}3n} = \frac{10^n}{log10^n}.$$

A partir desse resultado, Gauss conjectura o famoso e impressionante TNP, o Teorema do Número Primo, que diz o seguinte. Dado $x \in \mathbb{Z}$, defina a função $\pi(x)$ que é a quantidade de primos no intervalo $[1,x]$. Então, uma fórmula que se aproxima de $\pi(x)$:

$$\pi(x) \sim \frac{x}{logx}.$$

Mais tarde, esse resultado foi demonstrado pelos matemáticos Hadamard e la Vallée Poussin, com demonstrações feitas separadamente - mais informações sobre esse teorema podem ser vistas no livro **Teoria dos Números**: um passeio com primos e outros números familiares pelo mundo inteiro. (MARTINEZ *et al.*, s.d).

O mais brilhante discípulo de Gauss, Georg Friedrich Bernhard Riemann, nascido na Alemanha em 1826, assim como Gauss, Riemann se encantou pelos números primos quando leu sobre eles em um livro. Em 1859, ele teve uma brilhante descoberta que se tornaria a maior de todas para a teoria dos números primos.

Ao estudar a função Zeta $\zeta(k) = \sum_{k=1}^{\infty} \frac{1}{p^k}$ com p primo e um k fixo, que é uma sequência infinita de razão de $1/p < 1$, que surgiu primeiramente por Euler quando trabalhava com números primos e posteriormente pelo próprio Riemann, quando começou a trabalhar com variáveis complexas ao invés de reais como Euler. Dessa maneira, surgiu a função Zeta de Riemann: $\zeta(s) = \sum_{n=1}^{\infty} 1/n^s$ com n sendo os Naturais e o s um complexo fixo.

Ele percebeu que os zeros não triviais dessa função se relacionavam de alguma maneira aos primos, e isso levava a uma correção da hipótese de Gauss sobre TNP. Riemann percebeu que os dez primeiros zeros dessa função estavam na mesma linha e, por conta disso, ele afirmou que todos os infinitos zeros dessa função estão na mesma linha. Caso isso seja provado, a Hipótese de Gauss terá uma validade maior, porém ninguém a demonstrou ainda. Trataremos com mais detalhes no Capítulo 7.

2.3 Definição de Primos

Definição 1: Dado $n \neq \pm 1$ pertencente aos inteiros, tal que n é divisível por 1, -1 e por n e -n e somente por esses quatro divisores $(1, -1, n, -n)$, então dizemos que n é um número primo

É importante destacar que por conta dessas condições o número 1 não é primo.

E aqueles que não são primos, o que eles são? Bem, esses são os chamados de números compostos.

Definição 2: Se $n \in \mathbb{Z}$ e d é número de divisores de n, com $d > 4$, então n será chamado de número composto.

Exemplo 1:

Note que $4 \in \mathbb{Z}$ tem 6 divisores, 4/1 = 4; 4/2 = 2; 4/4 = 1; 4/ -1 = -4; 4/ -2 = -2; 4/ -4 = -1. Outro fator mais direto que exclui o 4 de ser primo é o fato dele ser par diferente de 2, pois o único primo par é 2, e todos os demais serão números pares, assim, não cumprem as condições que caracterizam um número como primo.

2.3.1 Infinitude dos primos

O maior número primo registrado é $2^{82,589,933}$-1 (IMPA, 2019), e foi descoberto usando a fórmula de Merdenne que é escrita da seguinte maneira $2^n - 1$ com n Natural, usando-a e a tecnologia de computadores de ponta foi possível chegar neste número. Ora, Euclides demonstrou que os Números Primos são infinitos e, então, como pode existir o maior primo? De fato, ele demonstrou, e este número não é o maior primo, mas sim é apenas o maior primo descoberto. Como temos muito pouco conhecimento sobre o comportamento de crescimento desses números intrigantes e onde está o próximo primo, usamos destes métodos para achar primos muito grandes e daqui alguns anos um novo primo será o "Maior Primo" registrado.

Como posso garantir que o conjunto dos primos é infinito? Bem, iremos trazer duas demonstrações que garantem este fato: a de Euclides e a de Euler, mas antes explicaremos o TFA (Teorema Fundamental da Aritmética), que será utilizado na demonstração.

Teorema 1: ***Teorema Fundamental da Aritmética (TFA)***. Seja $n \geq 2$ um número natural. Podemos escrever n de uma única forma como um produto de primos (MARTINEZ *et al.*, s.d).

Acredita-se que o berço do TFA foi em "*Os Elementos",* obra de Euclides, que apesar de não ter escrito o TFA, traz duas proposições que se assemelham ao TFA, a saber, a Proposições VII.30; VII.31. Mas foi Gauss que fez a primeira prova do TFA em 1801 (FONSECA; MONTEIRO; FONSECA, 2021).

2.3.2 Demonstração de Euclides da infinitude dos primos

Teorema da Infinitude dos primos (Euclides): Existem infinitos números primos.

A demonstração de Euclides é feita por absurdo. Quando se demonstra um resultado desta forma, supõe-se o inverso da tese, nesse caso, em vez de dizer que os primos são infinitos, vamos supor que sejam finitos.

Teremos, então, uma sequência finita com todos os primos, digamos que sejam *n* primos da forma $P = (2, 3, 5, \ldots, P_n)$, no caso P_n será o maior primo.

Existirá um número composto pelo produto de todos os primos, vamos chamá-lo de $K = 2 * 3 * 5 * \ldots * P_n + 1$. Dado esse número nessa forma, ele não é divisível por nenhum primo, pois sempre deixa resto igual a 1. Portanto, pelo Teorema Fundamental da Aritmética (HEFEZ, 2015) K é um novo primo fora da sequência *P*, pois é maior que qualquer primo dentro dela. Isso chega a um absurdo, pois como teria um novo primo ou um fator primo fora de *P* se em *P* estão todos os primos? Então, conclui-se que o conjunto dos primos só pode ser infinito. ■

2.3.3 Demonstração de Euler

Matemático Leonhard Paul Euler (1707-1783) propõe outra demonstração para afirmar o fato de que os primos são infinitos. Ele demonstra a construção de um postulado e a partir dele basear a sua demonstração. Sua demonstração se dá da seguinte maneira.

Temos um número primo qualquer denotado de p, portanto existe uma razão da forma $\frac{1}{p} < 1$. Considere a série geométrica infinita de razão *1/p* com o primeiro termo igual a 1 da forma:

$$\sum_{k=0}^{\infty} \frac{1}{p^k} = \frac{1}{1 - p^{-1}}.$$

Vale também para outro primo denotado de q, da seguinte forma:

$$\sum_{k=0}^{\infty} \frac{1}{q^k} = \frac{1}{1 - q^{-1}}.$$

Vamos multiplicar esses dois resultados, obtemos

$$1 + \frac{1}{p} + \frac{1}{q} + \frac{1}{p^2} + \frac{1}{pq} + \frac{1}{q^2} + \cdots = \sum_{k=0}^{\infty} \frac{1}{q^k} \cdot \sum_{k=0}^{\infty} \frac{1}{p^k} = \frac{1}{1 - q^{-1}} \cdot \frac{1}{1 - p^{-1}}.$$

Demonstrando esse resultado, podemos partir para demonstração de Euler, ele usa contradição. Supondo que exista uma sequência finita de primos $p_1, p_2, p_3, \dots, p_r$. Para cada primo dessa sequência, teremos o mesmo resultado feito antes:

$$\sum_{k=0}^{\infty} \frac{1}{p_i^k} = \frac{1}{1 - p_i^{-1}}$$

com $i = 1,2,3, \cdots, r$. Fazendo a multiplicação dessas séries infinitas para que índice i, temos

$$\prod_{i=1}^{r} \left(\sum_{k=0}^{\infty} \frac{1}{p_i^k} \right) = \prod_{i=1}^{r} \frac{1}{1 - p_i^{-1}},$$

que é um número finito, pois é um produto de finitos números. Por outro lado, qualquer número da forma $\frac{1}{n}$ está nesse produtório. Por exemplo, o número $\frac{1}{30}$ é igual a $\frac{1}{2 \cdot 3 \cdot 5}$ e esse último aparece em alguma parcela quando multiplicamos as séries $\sum_{k=0}^{\infty} \frac{1}{2^k}$, $\sum_{k=0}^{\infty} \frac{1}{3^k}$ e $\sum_{k=0}^{\infty} \frac{1}{5^k}$, ou seja, o produtório acima nada mais é do que

$$\prod_{i=1}^{r} \left(\sum_{k=0}^{\infty} \frac{1}{p_i^k} \right) = \sum_{k=0}^{\infty} \frac{1}{n} = \infty,$$

uma contradição. Dessa maneira, a sequência de todos os primos não pode ser finita. ■

2.4 Congruência Modular

Vamos introduzir congruência modular, apresentando sua definição e suas propriedades e demonstrando algumas delas. Antes de partirmos diretamente para congruência módulo *n*, é essencial entender divisão euclidiana. Daremos um prelúdio do que é divisão euclidiana para que você, leitor, consiga absorver o máximo sobre congruência modular.

Todo este tópico será baseado nas seguintes obras: (CAIXETA, 2016); (IEZZI, 2003); (SILVA, 2021).

2.4.1 Divisão Euclidiana

Divisão é algo comum a todos que já estudaram matemática. Com o passar do tempo, se torna algo natural de se fazer, tanto na própria matemática quanto no dia a dia. Mas qual é a estrutura de uma divisão?

Teorema 2: Divisão Euclidiana.

Sejam $a\ e\ b\ \in \mathbb{Z}$, com $b \neq 0$. Então, existem $r\ e\ q$ únicos tais que $a = bq + r, 0 \leq r < |b|$. (IEZZI, 2003).

A seguir, usaremos a notação: $\frac{a}{b}$ para representar o quociente da divisão do número a pelo número b.

Exemplo 2: Dados $a = 4, b = 3 \rightarrow \frac{a}{b} = \frac{4}{3} \rightarrow q = 1\ e\ r = 1$.

$$a = 4 = 3 * 1 + 1.$$

Exemplo 3: Dados $a = 100, b = 10 \rightarrow \frac{a}{b} = \frac{100}{10} \rightarrow q = 10\ e\ r = 0$.

$$a = 100 = 10 * 10 + 0.$$

2.4.2 Aspectos Históricos da Congruência Módulo *n*

Congruência modular é uma área de origem na Aritmética. Temos registro de Aritmética desde Euclides, nos Elementos de Euclides. Como é umas das principais áreas da Matemática, foi uma fonte essencial de pesquisa de diversos matemáticos como Pierre de Fermat (1601-1665), Leonhard Euler (1707-1783), Josefh Louis Lagrange (1736-1813), Adrien Marie Legendre (1752), John Wilsone Carl Friedrich Gauss (1777-1855). Vamos apresentar contribuições na aritmética modular de Pierre de Fermat e Friedrich Gauss.

O pequeno teorema de Fermat: a^{p-1} deixa resto 1 na divisão por p, primo, foi a maior contribuição feita por Fermat, que teve sua publicação por volta de 1640 e 1641. Sabe-se que esse resultado tem origem numa descoberta feita por matemáticos chineses há 50 anos a. C.

Gauss foi responsável pela introdução do termo congruência na aritmética modular, pois na época eram comum expressões do tipo *a divisão de a pôr n deixa o mesmo resto da divisão de b por n*. Ao analisar tais expressões (no formato matemático), Gauss denotou $a \equiv b\ (mod\ n)$, pois a e b possuem o mesmo resto na divisão pelo inteiro n (OLIVEIRA, 2016, p.15).

Ao nosso ver, estes dois matemáticos são os grandes progenitores da Aritmética Modular, pois suas contribuições são as colunas sustentadoras dessa área até os dias de hoje.

Após essa breve introdução histórica, vamos partir para a própria congruência modular e ver algumas de suas propriedades importantes.

2.4.3 Definição e Propriedade da Congruência Modular

Definição 3: Congruência Módulo *n*. Segundo IEZZI (2003):

Sejam $a, b \in \mathbb{Z}$ quaisquer e m um inteiro estritamente positivo. Diz-se que a é côngruo a b módulo m se $\frac{a-b}{m}$, isto é, se $a - b = mq$ para um conveniente inteiro q. Para indicar que a é côngruo a b, módulo m, usa-se a notação:

$$a \equiv b(mod\ n).$$

Propriedades

Sejam $a, b, c \in Z$. Então:

p_1 Reflexiva: $a \equiv a\ (mod\ n)$, isto é, todo $a \in Z$ é congruente a si mesmo.

$p_2)$ Simétrica: $a \equiv b\ (mod\ n)$ implica $b \equiv a\ (mod\ n)$.

$p_3)$ Transitiva: $a \equiv b\ (mod\ n),\ b \equiv c\ (mod\ n) \rightarrow a \equiv c\ (mod\ n)$.

$p_4)$ $a \equiv b\ (mod\ n), 0 \leq b < n \rightarrow b = r$ da divisão de $\frac{a}{n}$.

$p_5)$ $a \equiv b\ (mod\ n) \leftrightarrow a\ e\ b$ tem o mesmo resto na divisão por n.

$P_6)$ $a \equiv b\ (mod\ n) \leftrightarrow a \pm c \equiv b \pm c\ (mod\ n)$.

$p_7)$ $a \equiv b\ (mod\ n)\ e\ c \equiv d\ (mod\ n) \rightarrow a + c \equiv b + d\ (mod\ n)$.

$p_8)$ $a \equiv b\ (mod\ n) \rightarrow ac \equiv bc\ (mod\ n)$.

$p_9)$ $a \equiv b\ (mod\ n)\ e\ c \equiv d\ (mod\ n) \rightarrow ac \equiv bd\ (mod\ n)$.

$p_{10})$ $ca \equiv cb\ (mod\ n)$ e $mdc\ (c, n) = d \rightarrow a \equiv b\left(mod\ \frac{n}{d}\right), d > 0$.

Dadas a definição e as propriedades, podemos ressalta que dadas as propriedades $p_1), p_2), p_3)$, temos por definição uma Relação de Equivalência. É importante destacar que, quando nos referirmos a qualquer propriedade dessas, usaremos as notações postas neste tópico.

2.4.4 Provas de algumas propriedades

Vamos tratar da demonstração de algumas propriedades que consideramos importantes para entendimento do trabalho. Essas demonstrações serão baseadas na obra (IEZZI,2003, p. 54 a 56).

Demonstração da p_3: Temos pela definição que $\frac{n}{b-a}$ e $\frac{n}{c-b}$, portanto podemos escrever da seguinte maneira:

$$\frac{n}{[(b-a)+(c-b)]}.$$

Podemos cancelar o b e, então, temos:

$$\frac{n}{c-a},$$

que, por definição, implica em $\frac{n}{c-a}$ e $\frac{n}{a-c}$. Portanto:

$$a \equiv c\ (mod\ n).$$

Assim garantimos a Transitividade.

■

Demonstração de p_4: Temos por definição que $a - b = nq, q \in \mathbb{Z}$. Dessa igualdade, temos que

$$a = nq + b,$$

e, pela definição de divisão euclidiana, como por hipótese $0 \leq b < n$, portanto $b = r$, uma vez que o resto é único. Logo, já é válida a propriedade $a \equiv b\ (mod\ n), 0 \leq b < n \rightarrow b = r$.

■

Demonstração da p_5: $(\rightarrow)$ Por hipótese $a \equiv b(mod\ n)$.

Então: $a - b = nq \rightarrow a = nq + b$, para algum q. Pelo **Teorema 2**, existe um q_1 único como quociente de a/n e r único como resto de a/n, então

$$a = nq_1 + r.$$

Portanto, podemos escrever a seguinte igualdade, $nq + b = nq_1 + r$, que implica

$$b = n(q - q_1) + r.$$

Substituindo $(q - q_1) = q_2$, segue que

$$b = nq_2 + r.$$

Logo, r é resto de $\frac{b}{n}$, e r também é resto de $\frac{a}{n}$, mostrando que b e a têm o mesmo resto na divisão por n. Primeira parte está provada. Agora falta garantir a volta.

(←) Se, por hipótese, a, b possuem restos iguais na divisão por n, então

$$a = nq_1 + r, b = nq_2 + r$$

$$\xrightarrow{(a-b)} a - b = n(q_1 - q_2).$$

Chamando $(q_1 - q_2) = k$, obtemos

$$a - b = nk,$$

que, pela **Definição 3**, garante que

$$a \equiv b \ (mod\ n).$$

Assim, segue $\boldsymbol{p_5}$. ■

Faz-se necessário definir inverso aditivo e inverso multiplicativo em $\mathbb{Z}_p$, pois são definições que serão utilizadas. Admitiremos que o leitor já está familiarizado com o conjunto das classes residuais móludo p, denotado por $\mathbb{Z}_p$. Para maiores informações, veja (IEZZI, 2003).

Definição 4: Inverso Aditivo em $\mathbb{Z}_p$: $x \in \mathbb{Z}_p$ é inverso aditivo de y se, e somente se, $x + y = 0$. Denotaremos o inverso aditivo do elemento x por $-x$.

É possível mostrar que o inverso aditivo é único.

Definição 5: Inverso multiplicativo em $\mathbb{Z}_p$: $\bar{x} \in \mathbb{Z}_p$ é inverso multiplicativo de $x \neq 0$ se, e somente se, $x * \bar{x} = 1$. Denotaremos o inverso multiplicativo do elemento x por $\bar{x}$.

É possível mostrar que o inverso multiplicativo é único. Escreveremos $\mathbb{Z}_p^*$ para nos referirmos ao conjunto $\mathbb{Z}_p \backslash \{0\}$.

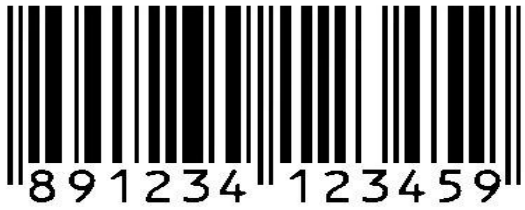
2.4.5 Aplicações de Congruência Modular

Congruência tem aplicações de grande importância e complexidade no nosso mundo. Vejamos algumas a seguir.

Primeira aplicação: Códigos de barras.

Esses códigos são usados atualmente na identificação de produtos e objetos tanto para venda quanto para controle de estoque, constituindo-se um sistema de suma importância para o mercado.

Figura 3: Código de barra



Fonte: SILVA, CLAUDEMILSON 2016, p. 22

Esses códigos em barras remetem a uma sequência de números que são gerados usando a congruência modular. A seguir daremos um exemplo baseado na OLIVEIRA (2016):

Exemplo 4: Dados os algarismos do código da Figura 3, $A = \{8, 9, 1, 2, 3, 4, 1, 2, 3, 4, 5, 9\}$, temos 12 algarismos e vamos encontrar o décimo terceiro. Para isso, existe sempre uma sequência base de multiplicação para a qual faremos uma multiplicação específica. Nesse caso, essa sequência é dada por $T = \{1,3,1,3,1,3,1,3,1,3,1,3\}$. Assim, obtemos o número $8 + 27 + 1 + 6 + 3 + 12 + 1 + 6 + 3 + 12 + 5 + 27 = 111$. O próximo algarismo é aquele que somado com 111 resulte em um múltiplo de 10, ou seja, o número 9. Portanto, o décimo terceiro algarismo é 9.

Segunda aplicação: Identificação.

Outra aplicação importante desse conteúdo é a identificação. O CPF, em parâmetro nacional, segue um padrão para gerar cada numeração. Esses números são gerados através de congruência modular. É feito da seguinte maneira: multiplicam-se os primeiros números gerados (6,5,3) por (1,2,3), e o resultado dessa multiplicação é posto em uma congruência para gerar o novo algarismo: $S - a_n \equiv 0\ (mod\ 11)$. Dessa maneira, eles criam a sequência numérica dos CPF. A seguir, daremos um exemplo baseado em OLIVEIRA (2016):

Exemplo 5: Dado o seguinte CPF: $067.390.861 - xx$ determine os dois últimos algarismos. Tome os algarismos do CPF e multiplique pela seguinte sequência base: $\{1,2,3,4,5,6,7,8,9,0\}$, isso vai gerar o seguinte resultado $0 + 12 + 21 + 12 + 45 + 0 + 56 + 48 + 9 = 203$. Agora faça $\frac{203}{11} = 18, r = 5$. O próprio resto é o próximo algarismo, CPF: $067.390.861 - 5x$, como a multiplicação do CPF com a sequência base já está gerando um múltiplo de 11, então o último algarismo é 0. Assim, CPF: $067.390.861 - 50$.

Essas aplicações são alguns exemplos dentre outros inúmeros que temos para congruência modular. Caso o leitor esteja interessado em entender mais sobre as aplicações dessa área, busque a obra: (OLIVEIRA, 2016).

3. NÚMEROS QUE PODEM SER ESCRITOS COMO SOMA DE DOIS QUADRADOS

Neste momento, introduzimos o foco do trabalho: Teorema dos dois quadrados de Fermat. E precisamos responder à seguinte questão: Que números podem ser escritos como soma de dois quadrados? Podemos listar alguns desses números, como $1 = 1^2 + 0^2; 2 = 1^2 + 1^2$, porém listar todos eles não é nada prático. Então, vamos procurar um resultado que, num certo sentido, caracterize todos esses números.

Pelo algoritmo da divisão de Euclides, todo número inteiro positivo pode ser escrito como uma destas 4 formas: $4m, 4m + 1, 4m + 2$ e $4m + 3$. Quando esse número é primo, porém, podemos restringir a apenas três: $4m + 1, 4m + 2$ e $4m + 3$. Todavia, o único primo escrito da forma $4m + 2 = 2(m + 1)$ é o número 2, quando $m = 0$. Do contrário, ele é múltiplo de 2, portanto não é primo. Os primos na forma $4m + 1$ são primos que deixam resto $r = 1$ na divisão por 4, e os na forma $4m + 3$, deixam resto $r = 3$.

3.1 Demonstração da Infinidade de Primos da forma $4m + 1$ e $4m + 3$

Vamos a um aquecimento. Anteriormente foi demonstrado por Euclides que os primos são infinitos, mas e os primos da forma $4m + 1$ e $4m + 3$, eles são infinitos?

Demonstração para o caso $4m + 3$:

Usaremos o mesmo raciocínio de demonstração por absurdo. Vamos começar essa demonstração provando que os números primos na forma *4m + 3* são infinitos. Para isso, por contradição, seja P_k o maior primo da forma $4m + 3$, e considere o número

$$N_k =: (2^2 * 3 * 5 * \ldots * P_k) - 1.$$

Como dito na introdução deste capítulo, todos os primos pertencem às três formas $P = 4m + 3, P = 4m + 1$ e $P = 2$.

Passo 1: Mostrar que N_k é da forma $4m + 3$.

Temos

$$N_k =: (2^2 * 3 * 5 * \ldots * P_k) - 1 = 4(3 * 5 * 7 * \ldots * P_k) - 1 =$$

$$4\,(3\ *\ 5\ *\ 7\ *\ldots*\ P_k) - 1\ +\ 4 - 4\ =\ 4\,(3\ *\ 5\ *\ 7\ *\ldots*\ P_k)\ +\ 3 - 4$$
$$=\ 4\,(3\ *\ 5\ *\ 7\ *\ldots*\ P_k - 1)\ +3.$$

Temos, então, $N_k := 4\bar{m}\ +\ 3$, para algum inteiro $\bar{m}$. Como estamos supondo P_k o maior primo da forma $4m + 3$, N_k não pode ser primo, pois $N_k\ >\ P_k$ *e* P_k é o maior primo escrito dessa forma.

Passo 2: Existe um primo *P* na decomposição de N_k que é da forma $4m\ +\ 3$.

Do contrário, todos os primos seriam da forma *4m + 1*. Portanto, o produto deles deixaria resto 1 (propriedades p_4 e p_9 de congruência modular) e não 3, o que é um absurdo. Assim, considere $\bar{P}\ =\ 4\bar{m}\ +\ 3$ esse primo e note que $\bar{P}$ é diferente de todos os primos p_i da sequência finita de números primos da forma $4m + 3$, pois, do contrário, se $\bar{P} = p_i$, existiria $q \in Z$ tal que

$$q\bar{P} = N_k = 2^2 * 3 * 5 * \ldots * P_k - 1,$$

o que implicaria em

$$1 = p_i(2^2 * 3 * 5 * p_{i-1} * p_{i+1} * \ldots * P_k - q),$$

o que mostra um absurdo, pois o número 1 não é dividido por nenhum primo. Assim, temos que $\bar{P}\ >\ P_k$, pois $\bar{P} \neq p_i$, ou seja, diferente de todo primo $p \leq P_k$, logo $\bar{P}$ é um número primos maior que todos os p_i, que é um absurdo já que P_k é o maior primo dessa forma. Portanto, conclui-se que os primos da forma $4m\ +\ 3$ são infinitos.■

Demonstração para o caso $4m + 1$:

Agora vamos demonstrar que os primos da forma $P = 4m + 1$ são infinitos. Usaremos a mesma linha de raciocínio da demonstração anterior.

Suponha que os primos da forma $P = 4m + 1$ sejam finitos. Portanto, é possível estabelecer um P_k como maior primo e tomar o seguinte número

$$N_k := (2 * 3 * 5 * \ldots * P_k)^2 + 1.$$

Passo 1: Mostrar que $N_k := 4m + 1$.

$$N_k := (2 * 3 * 5 * \ldots * P_k)^2 + 1$$

$$\rightarrow 2^2(3 * 5 * \ldots * P_K)^2 + 1$$

$$\rightarrow 4(3 * 5 * \ldots * P_k)^2 + 1$$

$$N_k := 4q + 1.$$

Temos que $N_k > P_k$ e, portanto, N_k não é primo por hipótese.

Passo 2: Mostrar que na decomposição por primos de N_k, existe um primo $p > P_k$ tal que $p = 4m + 1$.

Demonstração: Esse passo segue do Lema 1 que mostraremos a seguir. Voltaremos a essa demonstração após o lema.

Lema 1: Para primos $p = 4m + 1$, a equação $s^2 \equiv -1\ (mod\ p)$ tem duas soluções $s \epsilon \{1, 2, \ldots, p - 1\}$. Se $p = 2$, ela tem uma solução. E não existe solução para primos da forma $p = 4m + 3$.

Demonstração: Seja $p = 2$. Temos

$$s \epsilon \{1, 2, \ldots, p - 1\}, p = 2$$

$$\rightarrow s \in \{1\} \therefore 1^2 \equiv -1\ (mod\ 2)$$

$$\rightarrow 1^2 - (-1) = 2$$

$$2 = 2,$$

o que é verdade, mostrando que o caso $p = 2$ é verdadeiro.

Para cada elemento $x \in Z_p^* = \{1,2, \ldots, p - 1\}$, vamos associar a ele o conjunto dado por $A_x = \{x, -x, \bar{x}, -\bar{x}\}$, em que $\bar{x}$ é o inverso multiplicativo do elemento x. Agora, definimos uma relação da seguinte forma: vamos dizer que x se relaciona com y em Z_p^* se, e somente se, a igualdade $A_x = A_y$ vale. Vejamos agora algumas propriedades importantes.

Propriedade 1: $x \equiv -x\ (mod\ p)$ não pode ocorrer, para p impa.

Vamos supor que a congruência é válida. Se $x \equiv -x\ mod\ p$, então:

$$x - (-x) = p * q, q \in Z,$$

$$\rightarrow x + x = p * q,$$

$$\rightarrow 2x = p * q.$$

Isso mostra que a classe do elemento $2x$ é a classe do zero em $\mathbb{Z}_p^*$ e, como p é primo, o elemento $\overline{2}$ é inversível em $\mathbb{Z}_p^*$, garantindo que a classe do elemento x é a classe do zero, um absurdo visto que $x \in \mathbb{Z}_p^*$. Portanto, $x \equiv -x\ (mod\ p)$ é impossível. ■

Em outras palavras, a propriedade 1 diz que todo conjunto A_x tem pelo menos dois elementos.

Propriedade 2: A congruência $x \equiv \bar{x}$ equivale a $x^2 \equiv 1$. Mostremos que tal equação só tem duas soluções, a saber, $\{1, p-1\}$.

De fato, da equação equivalente $x^2 \equiv 1\ (mod\ p)$ e lembrando que Z_p é um corpo, temos que

$$x^2 \equiv 1(mod\ p) \rightarrow x = 1\ ou\ x = (p-1)$$

Para $x = 1, 1^2 \equiv 1(mod\ p) \rightarrow 1 \equiv 1$. Para $x = (p-1), (p-1)^2 \equiv 1(mod\ p) \rightarrow p^2 - 2p + 1 \equiv 1(mod\ p)$. Ora, aqueles que são múltiplos de p (p^2 e $2p$) vão se igualar a zero, pois a divisão euclidiana por p: $\frac{p^2}{p}, \frac{2p}{p}$ deixa resto zero, e conclui a demonstração da propriedade 2. ■

Propriedade 3: $x \equiv -\bar{x}$ é equivalente $x^2 \equiv -1\ (mod\ p)$. Ou essa equação tem exatamente duas soluções $(x_0, p - x_0)$ ou não possui solução.

Pela propriedade 2, temos

$$x = -\bar{x} \leftrightarrow x^2 = -1.$$

Logo, $x^2 \equiv -1$ é válida.

Agora se não houver solução, não há o que provar, mas caso tenha solução, precisamos garantir que vale para $(x_0, p - x_0)$. Por hipótese, se vale para x_0, vamos mostrar que vale para $p - x_0$. Com efeito,

$$x_0^2 \equiv -1\ (mod\ p) \rightarrow (p - x_0)^2 \equiv p^2 - 2px_0 + x_0 \equiv -1\ (mod\ p),$$

que é válido por hipótese, eliminando os termos múltiplos de p. Agora, suponha que x_1 seja outra solução da equação $x^2 \equiv -1\ (mod\ p)$. Então, pela propriedade p_3 de congruência, segue que

$$x_0^2 \equiv -1 \equiv x_1^2\ (mod\ p).$$

Logo, $(x_0 - x_1)(x_0 + x_1) = 0$. Se $x_0 \neq x_1$, então necessariamente $x_0 = -x_1$, o que mostra que $A_{x_0} = A_{x_1}$. Assim, as únicas soluções (se houver) são $(x_0, p - x_0)$. ■

Agora, considerando as propriedades dadas acima, se particionarmos o conjunto $\mathbb{Z}_p^*$ com essa relação de equivalência, com p primo da forma $4m + 1$ ou $4m + 3$, aparecerão algumas classes com quatro elementos e sempre uma ou duas classes com dois elementos. Ora, a classe $\{1, p - 1\}$ sempre aparecerá e seus elementos recaem na propriedade 2 acima. Se só houver essa classe nessa partição de $\mathbb{Z}_p^*$, então a equação do lema não haverá solução. Mas isso ocorre quando temos o valor de $p = 4m + 3$. De fato, $p = 4m + 3 \rightarrow p - 1 = 4m + 2$. Assim, dividindo o número $p - 1$ por 4, vamos obter resto igual a 2, exatamente o número de elementos da referida classe. Logo, quando $p = 4m + 3$, não há solução para a equação do lema. Quando $p = 4m + 1$, temos

$$p = 4m + 1 \rightarrow p - 1 = 4m,$$

ou seja, se particionamos em subconjuntos com quatro elementos, haverá sempre dois com dois elementos, pois senão $p - 1$ deixa de ser múltiplo de 4. Portanto, garantimos que $p = 4m + 1$ tem duas soluções, pois recaímos na propriedade 3. ■

Utilizando o lema acima, vamos demonstrar o Passo 2 da infinitude dos números da forma *4m+1*. Ora, se todos os primos na decomposição do número N_k forem da forma $4m + 3$, então existirá um primo $P = 4m + 3$ satisfazendo

$$q * P = N_k = (2 * 3 * 5 * \ldots * P_k)^2 + 1 = s^2 + 1,$$

ou seja, existe $s \in \mathbb{Z}$ satisfazendo $s^2 \equiv -1\ mod\ P$, um absurdo segundo o Lema 1. Com isso, todos os primos na decomposição de N_k são da forma $4m + 1$, mas isso gera o mesmo absurdo encontrado na demonstração para o caso $4m + 3$. ■

Daremos exemplos de primos na forma $4m + 1, 4m + 3$ em $\mathbb{Z}_p^*$ a fim de mostrar numericamente o que ocorre na demonstração do lema anterior.

Exemplo 6: Seja $p = 5 = 4 * 1 + 1$ e considere $\mathbb{Z}_5^* = \{1, 2, 3, 4\}$. Veremos seus conjuntos da forma $\{x, -x, \bar{x}, -\bar{x}\}$. Temos

$$x = 1 \rightarrow \{1, 4\}.$$

$$x = 2 \rightarrow \{2,3\}.$$

Observe que $2^2 \equiv 3^2 \equiv -1(mod\ 5)$.

Exemplo 7: Agora $\mathbb{Z}_{13}^* = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12\}$:

$$x = 1 \rightarrow \{1,12\}.$$

$$x = 2 \rightarrow \{2,11,7,6\}.$$

$$x = 3 \rightarrow \{3,10,9,4\}.$$

$$x = 5 \rightarrow \{5,8\}.$$

Observe que $5^2 \equiv 8^2 \equiv -1\ (mod\ 13)$.

Exemplo 8: $\mathbb{Z}_{17}^* = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16\}$:

$$x = 1 \rightarrow \{1,16\}.$$

$$x = 2 \rightarrow \{2,15,8,9\}.$$

$$x = 3 \rightarrow \{3,14,11,6\}.$$

$$x = 4 \rightarrow \{4,13\}.$$

$$x = 5 \rightarrow \{5,12,10,7\}.$$

Observe que $4^2 \equiv 13^2 \equiv -1\ (mod\ 17)$.

Exemplo 9: Primo da forma $p = 4m + 3$, $\mathbb{Z}_7^* = [1,2,3,4,5,6\}$:

$$x = 1 \rightarrow \{1,6\}.$$

$$x = 2 \rightarrow \{2,5,3,4\}.$$

Note que, como dito no Lema 1, não temos solução.

Exemplo 10: $\mathbb{Z}_{11}^{*} = \{1,2,3,4,5,6,7,8,9,10\}$:

$$x = 1 \rightarrow \{1,10\}.$$

$$x = 2 \rightarrow \{2,9,5,6\}.$$

$$x = 3 \rightarrow \{3,8,7,4\}.$$

Note que, como dito no Lema 1, não temos solução.

Lema 2: Nenhum número $n = 4m + 3$ é uma soma de dois quadrados $x^2 + y^2$.

Demonstração: Supomos, por contradição, que seja possível tal escrita. Então,

$$x \equiv r\ (mod\ 4) \rightarrow r = 0,1,2,3$$

$$y \equiv r_1\ (mod\ 4) \rightarrow r_1 = 0,1,2,3$$

$$x^2 \equiv r^2\ (mod\ 4) \rightarrow r = 0,1$$
$$y^2 \equiv r_1^2\ (mod\ 4) \rightarrow r_1 = 0,1.$$

Isso porque $2^2 \equiv 0\ (mod\ 4)\ e\ 3^2 \equiv 1\ (mod\ 4)$. Portanto, se somarmos tais números $x^2 + y^2$, ou essa soma vai deixar resto 0, ou resto 1 ou resto 2 na divisão por 4, gerando um absurdo, uma vez que o número $n = 4m + 3$ deixa resto 3. Portanto, $n = 4m + 3$ não pode ser escrito como a soma de dois quadrados $x^2 + y^2$. ■

Assim, conclui-se que nenhum $n = 4m + 3$ pode ser escrito como a soma de dois quadrados, portanto eliminamos os primos dessa forma. Nos restam primos da forma $p = 4m + 1$ que, com a prova do Lema 1, ficamos mais próximo de provar que esses números podem ser escritos como a soma de dois quadrados. De maneira geral, falta conferir de forma mais completa os casos em que $n = 4m, 4m + 1\ e\ 4m + 2$.

4. O RESULTADO PRINCIPAL RESTRITO A PRIMOS

Apesar de usarmos apenas uma vez, o princípio a seguir é importante para a prova do teorema principal.

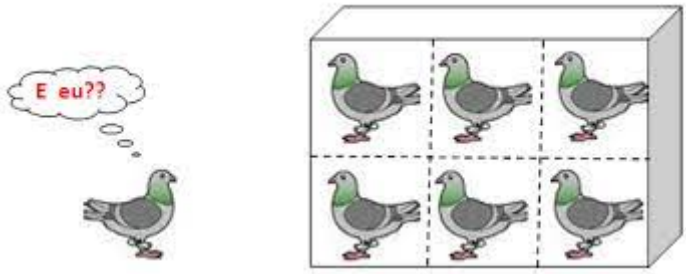
4.1 Princípio da Casa dos Pombos

Este princípio data de 1834 quando foi citado pela primeira vez, até onde temos conhecimento por *Johann Peter Gustav Lejeune Dirichlet,* porém não era denotado como o *Princípio da Casa dos Pombos* e sim por *Princípio das Gavetas de Dirichlet.* Ele diz o seguinte:

Princípio das Gavetas de Dirichlet: Se temos m gavetas e $m + 1$ objetos para guardar nessas gavetas, então ao menos uma gaveta terá dois ou mais objetos.

Princípio da Casa dos Pombos: Se temos m casas de pombos e $m + 1$ pombos, então ao menos uma casa terá dois ou mais pombos.

Figura 3: Princípio da casa dos Pombos



Fonte: Site Clube.Obmep.

Serão utilizando os seguintes conceitos: $\lfloor\sqrt{p}\rfloor$ que representar a função menor inteiro da $\sqrt{p}$. Exemplificando, se $p = 13$, $\lfloor\sqrt{13}\rfloor = 3$, então $x', y' \in \{0,1,2,3\}$. Agora, quantos pares de (x', y') podemos ter? Vão existir $\left(\lfloor\sqrt{p}\rfloor + 1\right)^2$ pares, bastando contar cada coordenada.

Exemplo 11: Se $p = 13$, vamos ter um intervalo de $\lfloor\sqrt{13}\rfloor = 3$. Assim, $x', y' \in \{0,1,2,3\}$, e os pares possíveis são $\begin{bmatrix}(0,0);(0,1);(0,2);(0,3);(1,0);(1,1);(1,2);(1,3);(2,0);\\(2,1);(2,2);(2,3);(3,0);(3,1);(3,2);(3,3)\end{bmatrix}$,

totalizando 16 pares. Em vez de listar um por um, basta usar a equação: $\{\lfloor\sqrt{13}\rfloor + 1\}^2 = \{3+1\}^2 = 4^2 = 16$ pares.

Teorema 3: Cada primo da forma *p = 4m +1* é uma soma de dois quadrados

Demonstração: Considere um par qualquer de inteiros (x', y') tais que esses valores satisfazem $0 \leq x', y' \leq \sqrt{p}$. Então, temos $x', y' \in \{0,1,2,\dots,\lfloor\sqrt{p}\rfloor\}$, e $\{\lfloor\sqrt{p}\rfloor + 1\}^2$ pares.

Feito, vamos usar o fato de que $\lfloor x\rfloor + 1 > x, \forall\, x \in \mathbb{Z}^+$. Agora note que

$$x = \sqrt{p} \rightarrow \{\lfloor\sqrt{p}\rfloor + 1\}^2 > p.$$

Portanto, para cada $s \in \mathbb{Z}$ e para cada par (x', y'), vai existir um outro par (x'', y''), diferente do primeiro, tal que

$$(x', y'), (x'', y'') \in \{0,1,2,\dots,\lfloor\sqrt{p}\rfloor\} \times \{0,1,2,\dots,\lfloor\sqrt{p}\rfloor\},$$

e a seguinte equação modular é satisfeita:

$$x' - sy' \equiv x'' - sy''(mod\ p).$$

Com efeito, existem $\{\lfloor\sqrt{p}\rfloor + 1\}^2 > p$ possíveis pares. Como existem apenas p restos possíveis na divisão de um número inteiro por p, necessariamente, vão existir esses dois pares distintos. Aqui, usamos o princípio da casa dos pombos da seguinte forma: temos p possíveis restos e $\{\lfloor\sqrt{p}\rfloor + 1\}^2$ possíveis pares, ou seja, p casas para $\{\lfloor\sqrt{p}\rfloor + 1\}^2 > p$ pombos, fornecendo o resultado. Agora, vamos voltar para a equação. Temos, para algum $q \in \mathbb{Z}$,

$$x' - sy' \equiv x'' - sy''\ (mod\ p)$$

$$\rightarrow (x' - sy') - (x'' - sy'') = p * q$$

$$\rightarrow (x' - x'') - (sy' - sy'') = p * q$$

$$\rightarrow (x' - x'') - s(y' - y'') = p * q$$

$$\rightarrow (x' - x'') \equiv s(y' - y'')\ (mod\ p).$$

Vamos definir $|x' - x''| = X\ e\ |y' - y''| = Y$; então ficamos com a seguinte expressão:

$$X \equiv \pm sY \ (mod\ p).$$

Com $X, Y \in \{1,2 \dots, \lfloor\sqrt{p}\rfloor\}$, pois, como os pares (x', y'), e (x'', y'') são distintos, nem X nem Y podem assumir o valor 0, senão os pontos seriam iguais. Pelo Lema 1, se $p = 4m + 1$, então a equação em $s^2 \equiv -1\ (mod\ p)$ tem duas soluções. Considere, então, s uma solução de $s^2 \equiv -1\ (mod\ p)$. Com isso, ficamos com nossa equação da seguinte forma, após elevá-la ao quadrado:

$$X^2 \equiv s^2Y^2 \equiv -Y^2\ (mod\ p).$$

Somando Y^2, obtemos

$$X^2 + Y^2 \equiv s^2Y^2 + Y^2 \equiv 0\ (mod\ p)$$

$$\rightarrow X^2 + Y^2 \equiv 0\ (mod\ p)$$

$$\rightarrow X^2 + Y^2 = p * q.$$

Ora, sabemos que $0 < X^2 + Y^2$, então:

$$X \in \{1,2, \dots, \lfloor\sqrt{p}\rfloor\} \rightarrow X < \sqrt{p},$$

Logo, $X^2 < p$. Também

$$Y \in \{1,2, \dots, \lfloor\sqrt{p}\rfloor\} \rightarrow Y < \sqrt{p},$$

$$Y^2 < p.$$

Então, $0 < X^2 + Y^2 < 2p$, com p sendo um inteiro. Em resumo, $X^2 + Y^2$ é um múltiplo de p e, ao mesmo tempo, é menor do que $2p$. O único múltiplo de p que satisfaz isso é o próprio p. Assim, $X^2 + Y^2 = p$, e isso finaliza a demonstração.■

5. RESULTADO PRINCIPAL

Neste momento, já garantimos que um primo da forma $4m + 1$ pode ser representável, escrito da forma $x^2 + y^2$, também eliminamos que números inteiros positivos da forma $4m + 3$ não podem ser representáveis. Resta-nos ainda números da forma $4m, 4m + 2$. Vamos demonstrar um teorema que mostra de forma mais geral quais números podem ou não ser representáveis.

Teorema 4: (AIGNER; ZIEGLER, 2018) Um número natural n pode ser representado como uma soma de dois quadrados se, e somente se, todo fator primo da forma $4m + 3$ aparece com expoente par na decomposição de n em fatores primos.

Demonstração: Vamos particionar em cinco partes. Esses cinco argumentos, quando provados, vão garantir que a afirmação do teorema é verdadeira.

1) Sabemos que existem números representáveis, $1 = 1^2 + 0^2$; $2 = 1^2 + 1^2$. Temos pela demonstração do Capítulo 4 que todo primo da forma $4m + 1$ é representável.

2) Agora vamos provar que o produto de dois números representáveis também é representável. De fato, temos $(x_i^2 + y_i^2) * (x_{ii}^2 + y_{ii}^2) = (x_i^2 x_{ii}^2 + x_i^2 y_{ii}^2 + y_i^2 x_{ii}^2 + y_i^2 y_{ii}^2) = (x_i x_{ii} + y_i y_{ii})^2 + (x_i y_{ii} - x_{ii} y_i)^2$.

3) O produto de um número n representável por z^2 é ainda representável, pois: $nz^2 = (xz)^2 + (yz)^2$.

Com esses três argumentos, procedemos da seguinte forma. Decompomos *n* em fatores primos e escrevemos:

$$n = \underbrace{2^j \prod_{i=1}^{k} (4m_i + 1) \prod_{i=1}^{q} (4r_i + 3)^{\alpha_i}}_{\text{Todos os primos da forma } 4m+1,2 \; e \; 4m+3.}.$$

Sabemos por (1) que todo número primo da forma $p = 4m + 1$ e $p = 2$ são representáveis e, por (2), sabemos que o produto de números representáveis é representável. Portanto, podemos simplificar a expressão acima e chegar a:

$$n = (z_1^2 + z_2^2)\prod_{i=1}^{q}(4r_i + 3)^{\alpha_i}.$$

Então, já podemos provar uma parte do teorema. Se os expoentes $\alpha_i's$ forem todos pares, segue que $\alpha_i = 2\beta_i$ e

$$n = (z_1^2 + z_2^2)\prod_{i=1}^{q}[(4r_i + 3)^{\beta_i}]^2,$$

e, por (3), segue que *n* é representável. Para finalizar, apresentamos os dois últimos argumentos que validarão o resultado.

4) Se temos um primo $p = 4m + 3$ e $n = x^2 + y^2$, então: Se p dividir n, então p divide $x\ e\ y$. Isso vale para p^2. De forma algébrica, seria o seguinte:

$$\frac{n}{p} \to \frac{x}{p}\ ;\ \frac{y}{p}.$$

Portanto, para p^2 ficamos:

$$\frac{n}{p^2} \to \frac{x^2}{p^2}\ ;\ \frac{y^2}{p^2}.$$

Podemos garantir isso, pois, do contrário, argumentaríamos da seguinte forma: $x \not\equiv 0\ (mod\ p)$ e isso implica que existe um $\bar{x}$ satisfazendo:

$$x * \bar{x} \equiv 1(mod\ p).$$

Portanto, multiplicando por $\bar{x}^2$ a equação $x^2 + y^2 \equiv 0$, obtemos

$$\bar{x}^2(x^2 + y^2) \to 1 + \bar{x}^2y^2 = 0$$

$$\to (\bar{x}y)^2 \equiv -1\ (mod\ p)$$

$$s^2 \equiv -1\ (mod\ p),$$

onde estamos chamando $s = \bar{x}y$. Todavia, temos pelo Lema 1 que isso é impossível, pois um número primo $p = 4m + 3$ não produz solução para a equação $s^2 \equiv -1\ (mod\ p)$. Portanto, a afirmação do argumento (4) está provada.

5) Seja $n = x^2 + y^2$. Se $p = 4m + 3$ divide *n,* então, por (4), p^2 divide n, x e y. Assim,

$$\frac{n}{p^2} = \frac{x^2}{p^2} + \frac{y^2}{p^2} \rightarrow \frac{n}{p^2} = \left(\frac{x}{p}\right)^2 + \left(\frac{y}{p}\right)^2,$$

o que mostra que o número $\frac{n}{p^2}$ é também representável. Logo, se p divide n e n é representável, então p^2 divide n e $\frac{n}{p^2}$ é representável. Logo, as potências que tornam n divisível por p^r são potências pares, como queríamos demonstrar. ■

Exemplo 12: Dado um $n = 18$, n pode ser representável?

Ora, a decomposição em primos de 18 é $n = 3^2 * 2$. Note que n possui na sua decomposição um primo $p = 3 = 4m + 3 = 4 * 0 + 3$, e esse p aparece com expoente par da forma $n = (4 * 0 + 3)^2 * 2$. Portanto, pelo **Teorema 4**, esse n é representável, e então $n = x^2 + y^2$. Sabe-se que $18 = 3^2 + 3^2$.

Exemplo 13: Dado um $n = 20$, n pode ser representável?

A decomposição de 20 em primos é $n = 2^2 * 5$. Note que n não possui nenhum primo da forma $p = 4m + 3$, e isso quer dizer, que temos $5 = 4 * 1 + 1, 2 = 1^2 + 1^2$. Pelo **Teorema 3** todo número primo da forma $4m + 1$ é representável e por (2) temos que produto de representáveis é representável. Ora, $n = x^2 + y^2 \rightarrow 20 = 4^2 + 2^2$.

Exemplo 14: Dado a seguinte decomposição por primos de $n = 270 = 3^3 * 2 * 5$, n pode ser representável?

Ora, pelo **Teorema 4,** sabemos que não é possível pois n possui um $p = 4m + 3 = 3$ com potência ímpar em sua decomposição. Logo, respondemos à pergunta feita na introdução deste trabalho, mostrando que 270 não pode ser escrito como soma de dois quadrados.

6. PIERRE DE FERMAT

Pierre de Fermat, sem dúvida conhecido pela maioria dos matemáticos pelos seus teoremas famosos como *O pequeno Teorema de Fermat* e o *Último Teorema de Fermat,* teve uma importância muito grande em diversas áreas da Matemática: Geometria, Probabilidade e Teoria dos Números. Chega a ser intuitivo achar que Fermat era um matemático formado, mas, na verdade, ele se formou em direito e chegou a ser juiz supremo de Toulouse.

Este capítulo foi baseado em: (OLIVEIRA, 2019); (CASTRO, 2019); (MARTINS, 2021); (O último teorema de Fermat; GUSTAVO VIEGAS, 2021).

6.1 Biografia de Fermat

Pierre de Fermat nasceu no século *XVII* por volta de 1601 em Beaumont de Lomagne na França, e teve uma vida com privilégios. Vindo de família rica, seu pai era um mercador bem-sucedido em uma época na qual riqueza significava uma boa educação e, de fato, Dominique de Fermat, pai de Pierre, proporcionou para ele uma educação de alta qualidade. Mas diferente do que se pode pensar, sua educação superior não foi em Matemática e sim em direito.

Fermat, depois de terminar seus estudos básicos, ingressou na Universidade de Toulouse, onde começou e finalizou seu curso de direito. Trabalhou como advogado público em meados de 1631 e teve muito êxito na área jurídica, pois por volta de 1652 foi declarado Juiz Supremo da Corte de Toulouse. Pierre trabalhou na área judiciária a maior parte da sua vida e teve grande sucesso nela.

Mas e a Matemática pela qual é tão conhecido? Bem, essa seria para ele, a grosso modo, um simples *hobby*. Sua paixão pelos números se mostra até onde se tem registro em livros que ele estudou e escreveu em suas páginas e cartas para conhecidos. Ali, encontram-se diversas contribuições de Fermat para o mundo matemático e muitas conjecturas que, ao passar dos anos, transformaram-se em resultados importantes.

Como citado anteriormente, Pierre contribuiu para diversas áreas da Matemática. Na Geometria analítica, alguns defendem que foi Fermat o seu pioneiro; já outros afirmam que foi René Descartes. Pierre de Fermat trabalhou desde cálculos envolvendo curvas até equações gerais da reta passando por certos pontos. Entre seus estudos, ele desenvolveu um novo método para o cálculo da reta tangente. (CASTRO, 2019).

Na Probabilidade, ele tinha contato através de cartas com Blaise Pascal, um grande matemático e físico, ao qual Pierre respondia seus problemas probabilísticos de uma maneira

não tão usual, tentando trazer uma resolução mais direta, que mostra que desenvolveu estudos também na teoria da probabilidade. (CASTRO, 2019).

E, por fim, trazemos a Teoria do Números. Como já citado, é nessa área que ele é mais conhecido por causa dos dois teoremas: *O pequeno Teorema de Fermat* e o *Último Teorema de Fermat.* Fermat estudou o livro de aritmética de Diofanto e, ao estudar suas páginas, ele concluía algum pensamento e conjecturava algum resultado que, ao passar do tempo, foram demonstrados.

6.3 Teoremas de Fermat

As próximas seções foram inteiramente baseadas nas seguintes obras: (MARTINS, 2021); (O último teorema de Fermat; GUSTAVO VIEGAS, 2021); (CASTRO, 2019); (OLIVEIRA, 2019).

6.3.1 O Último Teorema de Fermat

Ao estudar o livro de Diofanto, Pierre se depara com Teorema de Pitágoras: dado um triângulo retângulo de lados $x, y\ e\ z\ \in \mathbb{Z} \rightarrow x^2 + y^2 = z^2$. Ao observar isto, Fermat decidiu testar essa equação para expoentes maiores que dois, algo como $x^n + y^n = z^n, n > 2$ tem soluções nos $\mathbb{Z}^+$. Fermat não só afirmou que não havia soluções como disse que encontrou uma demonstração, porém não cabia na margem da página.

Isso intrigou os matemáticos, pois não é um resultado fácil de ser demonstrado. Alguns matemáticos provaram casos particulares do teorema, por exemplo, Euler demonstrou para $n = 4$. Um grande passo para este Teorema se deu pela matemática Sophia Germain.

Sophia Germain também se intrigou com o problema, porém, diferente dos demais matemáticos, ela decidiu abordar de forma geral, tentar chegar aonde Fermat afirmou ter chegado. Infelizmente, ela não conseguiu provar o resultado, todavia sua técnica de abordar o tema influenciou diversos matemáticos que adaptaram sua técnica para provar outros casos particulares. Por exemplo, Legendre provou para o caso particular $n = 5$ por volta de 1825. Outros matemáticos como Dirichlet demonstrou pra $n = 14$. Gabriel Lamé provou para $n = 7$. Assim, seguiu-se por um tempo, mas chegou um momento que Lamé tentou provar o caso geral, porém sem êxito.

Ernst Kummer também trabalhou com este teorema e apesar de não conseguir chegar numa solução geral, ele conseguiu um feito grande garantindo o teorema para os seguintes casos $3 \leq n \leq 100, n \neq 37, 59, 67$. Mesmo não sendo a forma geral, é um ponto positivo para o

teorema que estava cada vez mais próximo de ser provado. Por fim, mais recentemente, Samuel Wagstaff, com tecnologia de computadores, chegou até $3 \leq n \leq 4.000.000$.

Mas a grande chave para prova do *Último Teorema de Fermat* veio da conjectura de Taniyama e Shimura que dizia que uma curva elíptica é igual a uma função modular.

Depois de quase 300 anos de mistério sobre este teorema, em 1994, foi possível afirmar como verdadeiro através do agora Teorema Taniyama-Shimura demonstrado pelo matemático e professor Andrew Wiles e seu aluno Richard Taylor. Portanto, não existe solução para $n \geq 3$ para equação $x^n + y^n = z^n$ nos inteiros positivos.

6.3.2 O Pequeno Teorema de Fermat

O pequeno Teorema de Fermat surgiu até onde se tem registros por volta de 1640 numa carta para Frenicle, na qual de maneira geral era definido da seguinte forma: Dados $a \in \mathbb{Z}$ e p primo. Se p não divide a, então p divide $a^{p-1} - 1$. Apesar de conjecturado por Pierre de Fermat, foi Euler que o demonstrou primeiro.

Apesar de não ter uma grande história até sua demonstração, *O pequeno Teorema de Fermat* tem aplicações diversas na Teoria dos Números, principalmente na área de congruência módulo *n.* Portanto, foi um avanço que contribuiu de forma ampla para Teoria dos Números.

7. CURIOSIDADES SOBRE PRIMOS

Vamos trazer à tona novamente a temática dos números primos, mas numa abordagem diferente do Capítulo 2, no qual nós trouxemos numa forma didática. Aqui o objetivo será apresentar alguns apontamentos intrigantes sobre esses números, como criptografia, problemas sem solução e outras curiosidades. Este capítulo foi baseado nas seguintes obras (FRITSCHE; SUGUIMOTO, 2015); (RIZEL, 2014); (HISTÓRIA DOS NÚMEROS PRIMOS. BBC, 2017).

7.1 Alan Turing

Alan Turing, nascido em 1912 na cidade de Londres, foi um brilhante matemático e considerado pai da computação. Já se interessava por números primos antes dos feitos que o fizeram tão conhecido. Aplicava esses números em um dos mais famosos problemas da Matemática: a Hipótese de Riemann. Esse problema foi proposto a ele pelo matemático Godfrey Harold Hardy. Alan decidiu abordá-lo de forma diferente.

Em outro momento, um grupo de matemáticos foi designado para decodificar criptografia nas mensagens da Alemanha Nazista. Entre esses matemáticos, encontrava-se Alan Turing, que foi o grande responsável por esse feito. Até então, sua máquina que desvendaria os mistérios da Hipótese de Riemann serviu na verdade para desvendar as mensagens alemãs que foi um feito que mudou o rumo da guerra. Alan, com o auxílio da sua máquina, conseguiu mostrar que cerca de 1104 zeros estavam na mesma linha, e já foi mostrado usando computares mais modernos que cerca de 100 trilhões de zeros estão na mesma linha, porém isso não prova a hipótese, mas já é um ponto bem positivo.

7.2 Problemas não Resolvidos

As próximas seções foram baseadas nas seguintes obras: (FRITSCHE; SUGUIMOTO, 2015); (RIZEL, 2014); (HISTÓRIA DOS NÚMEROS PRIMOS. BBC, 2017); (BITENCOURT, 2018).

7.2.1 Primos Gêmeos

Antes de enunciar esse problema, vamos definir o que são primos gêmeos. Dados primos r e t, dizemos que são gêmeos caso $|r - t| = 2$. Por exemplo, 3 e 5 são gêmeos e 11 e 13 são gêmeos. Um problema atual que rodeia os primos gêmeos é garantir sua infinidade, ou seja, se existem infinitos pares de primos gêmeos. Ao contrário de números primos, em geral, que teve

sua infinidade provada por Euclides, os gêmeos ainda não foram demonstrados por ninguém e se mantém como uns dos problemas mais intrigantes da Matemática.

7.2.2 Conjecture de Goldbach

Essa conjectura foi feita pelo matemático Christian Goldbach, nascido na antiga Prússia. Ela se desenvolveu a partir de cartas com o outro matemático chamado Euler. Christian já havia escrito para Euler uma conjectura similar: Todo número $n \in \mathbb{Z}, n > 6$, é soma de três primos. Com continuidade da conversa com Euler, surgiu a tão famosa conjectura de Goldbach. (BITENCOURT, 2018). A saber:

Todo inteiro $n = 2k, n \in \mathbb{Z}, n > 2$, pode ser escrito como a soma de dois primos $n = p + q$. Foi conjecturado por volta de 1742 e até hoje não foi provada. Muitos tomam como verdadeira, porém sem demonstração. Podemos apenas dar alguns exemplos para situar como funciona.

$$20 = 7 + 13$$

$$22 = 11 + 11$$

$$42 = 23 + 17.$$

Esses são só alguns exemplos de números pares que podem ser formados pela soma de dois primos.

Alguns matemáticos trabalharam com essa conjectura. Georg Cantor, por exemplo, conseguiu garantir a validade até 10^3. A. Aubry garantiu até $n < 2000$; o matemático R. Hauser conseguiu para $n < 5000$. N. Pipping chegou até $n < 10^5$, e, por fim, até onde sabemos o último resultado foi para $n < 4 * 10^{17}$ feito por Tomas Oliveira em 2013.

7.2.3 Hipótese de Riemann

Antes de abordar diretamente a Hipótese de Riemann, é necessário introduzir a função Zeta. Essa surgiu por meio de Euler, que utilizou para demonstrar por contradição que primos são infinitos. A função Zeta de Euler é dada por:

$$\zeta(k) = \sum_{n=1}^{\infty} {}^{1}/_{n^k} \text{ com } k > 1.$$

Riemann reescreveu essa função Zeta, só que agora ao invés de k temos $s \in \mathbb{C}$. Dessa maneira, surge a Função Zeta de Riemann, dada por:

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

Após isso, Riemann trabalhou com a função Zeta junto com a função *Eta de Dirichlet* $\eta(s)$, dada por:

$$\sum_{n=1}^{\infty} \frac{(-1)^{n-1}}{n^s} = (1 - 2^{1-s})\zeta(s)$$

$$\rightarrow \zeta(s) = \frac{1}{1 - s^{1-s}} \sum_{n=1}^{\infty} \frac{(-1)^{n-1}}{n^s}, R(s) > 0.$$

Após isso, Riemann faz uma sequência de cálculos complexos, mudando as restrições da reta crítica $R(s)$ da função Zeta, faz cálculos para $R(s) \leq 0; R(s) < 0; R(s) > 1; R(s) = 0$. Depois de todos os cálculos, Riemann percebe um certo comportamento nessa reta crítica, onde os zeros não triviais eram da seguinte forma $w = \frac{1}{2} + it$. Riemann, por conta desse fato, conjectura em 1859 o seguinte. (FRITSCHE; SUGUIMOTO, 2015).

Hipótese de Riemann: Todos os zeros não triviais da função $\zeta(s)$ pertencem à reta crítica $R(s)$. (FRITSCHE; SUGUIMOTO, 2015).

Após essa conjectura, Riemann a considera verdadeira e faz uma sequência de cálculos que levam algumas conclusões, as quais serão citadas de forma superficial por conta da sua complexidade. Riemann chegou num termo de aproximação para $\pi(x)$, a função que conta números primos até *x.* Esse termo é denotado por $R(x) = \sum_w R(x^w)$ e se aproxima de $\pi(x)$. Por conta dos zeros não triviais de $\zeta(s)$, caso a hipótese de Riemann seja verdadeira, $R(x)$ deixa de ser uma aproximação e traz um padrão para números de primos, o que seria fantástico.

7.3 Primos e suas Formas

Existem diversas fórmulas que permitem determinar muitos primos. Mesmo que não exista uma que determine todos (pelo menos, até então), existem algumas que tentam abranger

o máximo de primos até determinado valor. A seguir, veremos um pouco sobre algumas dessas formas.

Formulação de Mersenne é da forma $2^n - 1$, como já vimos anteriormente ela é utilizada para encontrar primos muito grandes, apesar de nem sempre gerar primos. Os primos de Mersenne foram úteis em sua época e ainda são utilizados. Também existem os primos de Sophia Germain da forma $2n + 1$, mas não são conhecidos quantos números dessa forma existem e ainda não foi provada a sua infinidade.

7.4 Primos e a Criptografia

Pelo fato de não sabemos como os números primos são gerados e como eles se dispõem, eles são usados atualmente em criptografia, ou seja, segurança de cartões de crédito, em mensagens de celular, etc. Um exemplo de como são usados: Multiplicam-se dois primos muito grandes para gerar um número composto maior ainda e, como não se sabe ao certo como primos se comportam, é extremante difícil desvendar quais primos foram multiplicados.

8. CONSIDERAÇÕES FINAIS

O Teorema sobre Inteiros que são soma de dois quadrados é algo baseado em outros três resultados escritos por Pierre de Fermat, que nesse trabalho tiveram sua notação como **Lema 2**: $n = 4m + 3$, não pode ser escrito como a soma de dois quadrados $x^2 + y^2$; **Teorema 3**: Cada primo da forma p = 4m +1 é uma soma de dois quadrados. $x^2 + y^2 = 4m + 1; x, y \in \mathbb{N}$; **Teorema 4**: Um número natural n pode ser representado como uma soma de dois quadrados se, e somente se, todo fator primo da forma $4m + 3$ aparece com expoente par na decomposição de n em fatores primos.

Estes são os três teoremas que respondem à pergunta inicial "quais números $n \in \mathbb{Z}$ podem ser escritos como a soma de dois quadrados perfeitos?" Dessa maneira, foram determinados quais podem e não podem ser soma de dois quadrados, cumprindo com o objetivo do trabalho.

Porém, esse estudo abrangeu além da prova final. Nosso outro objetivo era trazer ao leitor aquilo que compunha o tema principal. Por conta disso, acreditamos que cumprimos esse objetivo ao trazer desde a história dos números primos à biografia de Pierre de Fermat, autor dos três teoremas que sustentaram este trabalho.

Concluímos dizendo que este trabalho é um estudo na teoria dos números, voltado para a formação específica de certos números, mas também com uma breve passagem na história da matemática, a fim de contextualizar e justificar o estudo proposto. Por fim, queremos saber se você, caro leitor, conseguiu resolver nosso desafio inicial. Esperamos que sim.

REFÊNCIAS

AIGNER, Martin; M. ZIEGLER, Gunter. Lines in the plane and decompositions of graphs: Question for solution. In: **PROOFS from THE BOOK**. Sixth Edition. ed. [S. l.]: Springer, 2018.

BITENCOURT, Carolina da Silva. **A Conjectura de Goldbach e a intuição matemática**. 2018. 42 f. Dissertação (Mestrado) - Curso de Matemática, Profmat, Ufba, Salvador, 2018.

IEZZI, Hygino H. Domingues Gelson. **Álgebra Mordena**. 4. ed. São Paulo: Atual Editora, 2003. 371 p.

CAIXETA, Susiane Bezerra. **Algoritmo da divisão de Euclides**. 2016. 80 f. Dissertação (Mestrado) - Curso de Matemática, Profmat, Unb, Brasília, 2016.

SANTOS, João Evangelista Cabral do. **Números inteiros como a soma de quadrados**. 2013. 70 f. Dissertação (Mestrado) - Curso de Matemática, Profmat, Ufpa, João Pessoa, 2013.

OLIVEIRA, Claudemilson da Silva. **CONGRUÊNCIA MODULAR E APLICAÇÕES**. 2016. 48 f. TCC (Graduação) - Curso de Licenciatura em Matemática, Demat, Ufsj, Ão João Del-Rei, 2016.

BARROS, Francisco Vlademir Dedes da Cruz. **O método de Minkowski e a representação de um inteiro como soma de quadrados**. 2020. 79 f. Dissertação (Mestrado) - Curso de Matemática, Profmat, Urca, Juazeiro do Norte, 2020.

SILVA, Draytonn Lincoln Ferreira da. **TEOREMA DE EULER - ARITMÉTICA MODULAR**. 2021. 44 f. TCC (Graduação) - Curso de Licenciatura em Matemática, Ufal, Arapiraca, 2021

FRITSCHE, Willian Cleyson; SUGUIMOTO, Alexandre Shuji. **OS NÚMEROS PRIMOS E A HIPÓTESE DE RIEMANN.** 2015. 9 p.

RIZEL, Ary Camargo. **Números Primos**. 2014. 60 f. TCC (Graduação) - Curso de Matemática, Icex, Ufmg, Belo Horizonte, 2014.

OLIVEIRA, Francisco Erilson Freire de. **SOBRE VÁRIAS DEMONSTRAÇÕES DO PEQUENO TEOREMA DE FERMAT E AS INTER-RELAÇÕES ENTRE AS ÁREAS DA MATEMÁTICA**. 2019. 61 f. Dissertação (Mestrado) - Curso de Matemática, Ufc, Fortaleza, 2019.

CASTRO, Isabela Souza. **O Último teorema de Fermat nos Ensinos Fundamental e Médio**. 2019. 61 f. Dissertação (Doutorado) - Curso de Matemática, Ufv, Minas Gerais, 2019.

DOCUMENTARIOCIENCIA. **A HISTÓRIA DOS NÚMEROS PRIMOS - Documentário (2007).** Youtube. 2013. Disponível em: https://www.youtube.com/watch?v=eHp0cQy-2S4&t=3153s

TODA A MATEMÁTICA. **O último teorema de Fermat.** Youtube. 2021. Disponível em: https://www.youtube.com/watch?v=Kl9wFtKrFtY&t=9s

MATINEZ, Fabio E. Brochero. MOREIRA, Carlos Gustavo T. de A. SALDANHA, Nicolau C. TENGAN, Eduardo. **TEORIA DOS NÚMEROS:** um passeio com primos e outros números familiares pelo mundo inteiro. [S.D]. 510 P.