UNIVERSIDADE ESTADUAL DA PARAÍBA
CAMPUS I - CAMPINA GRANDE
PRÓ-REITORIA DE PÓS - GRADUAÇÃO E PESQUISA
PROGRAMA DE PÓS-GRADUAÇÃO EM MATEMÁTICA
MESTRADO PROFISSIONAL EM MATEMÁTICA EM REDE NACIONAL

EMERSON SOUZA SILVA

CONSIDERAÇÕES SOBRE O ÚLTIMO TEOREMA DE FERMAT POR MEIO DE CONCEITOS BÁSICOS

CAMPINA GRANDE - PB
2025

EMERSON SOUZA SILVA

CONSIDERAÇÕES SOBRE O ÚLTIMO TEOREMA DE FERMAT POR MEIO DE CONCEITOS BÁSICOS

Dissertação apresentada ao Programa de Pós-Graduação em Mestrado Profissional em Matemática em Rede Nacional da Universidade Estadual da Paraíba, como requisito parcial à obtenção do título de Mestre em Matemática.

Área de concentração: Matemática na Educação Básica

Orientador: Prof. Dr. Vandenberg Lopes Vieira

CAMPINA GRANDE - PB
2025

S586c Silva, Emerson Souza.

Considerações sobre o último teorema de Fermat por meio de conceitos básicos [manuscrito] / Emerson Souza Silva. - 2025.

52 p. : il. colorido.

Digitado. Dissertação (Mestrado Profissional em Matemática em Rede Nacional) - Universidade Estadual da Paraíba, Pró-Reitoria de Pós-Graduação e Pesquisa, 2025. "Orientação : Prof. Dr. Vandenberg Lopes Vieira, Departamento de Matemática - CCT. "

1. Pierre de Fermat. 2. Teoria dos números. 3. Teorema de Fermat. 4. Sophie Germain. I. Título

21. ed. CDD 510.1

Elaborada por Bruno R. F. de Lima - CRB - 15/1021 BC/UEPB

EMERSON SOUZA SILVA

CONSIDERAÇÕES SOBRE O ÚLTIMO TEOREMA DE FERMAT POR MEIO DE CONCEITOS BÁSICOS

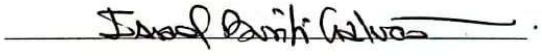
Dissertação apresentada ao Programa de Pós-Graduação em Mestrado Profissional em Matemática em Rede Nacional da Universidade Estadual da Paraíba, como requisito parcial à obtenção do título de Mestre em Matemática.

Área de concentração: Matemática na Educação Básica

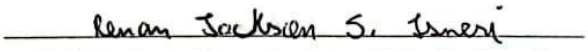
Aprovado em: 21\02\2025.

BANCA EXAMINADORA

Prof. Dr. Vandenberg Lopes Vieira (Orientador)
Universidade Estadual da Paraíba (UEPB)



Prof. Dr. Israel Burití Galvão (Membro Interno)
Universidade Estadual da Paraíba (UEPB)



Prof. Dr. Renan Jackson Soares Isneri (Membro Externo)
Universidade Federal de Campina Grande (UFCG)

Dedico esse trabalho ao meu Senhor e Salvador Jesus Cristo, Filho de Deus, por sempre ter me dado força quando muitas vezes faltaram. Também, à minha família que sempre tem me apoiado a todo o momento, em especial, à minha esposa Lucileia e minha filha Nathália de 10 anos, as quais têm me dado estima e alegria de continuar se dedicando a estudar e enfrentar as barreiras dessa vida. Aos meus pais, Maria de Lourdes e Evangelista que sempre empenharam o papel fundamental de serem o pilar em tudo em minha vida.

AGRADECIMENTOS

Agradeço em especial ao Deus Todo Poderoso, Yahweh, que por meio do seu Filho, o Senhor Jesus Cristo, tem me dado aliança eterna em minha vida, de maneira que eu sempre possa olhar para frente e, por meio do Santo Espírito, pude ter melhor compreensão da vida, do amor e da verdadeira sabedoria de existir nesse mundo.

Agradeço ao meu orientador Prof. Dr. Vandenberg Lopes Vieira, por todo apoio na dissertação.

Agradeço à minha família; sem ela, teria sido impossível em dar continuidade a esse curso, pois o seu apoio foi fundamental.

Agradeço à Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (CAPES) e à Sociedade Brasileira de Matemática (SBM) pela oportunidade de participar do Programa de Mestrado Profissional em Matemática em Rede Nacional (PROFMAT). O presente trabalho foi realizado com apoio da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - Brasil (CAPES) - Código de Financiamento 001.

“Onde há número, há beleza.” - Proclo Licio (412 – 485)

RESUMO

O Último Teorema de Fermat é um dos resultados mais famosos da matemática e um dos que mais inspiraram novas ideias e teorias matemáticas. Esse teorema tem um enunciado bastante simples, compreensível a todo leitor, o que dá a ele uma beleza à parte, porém, não foi fácil prová-lo. Tal problema atraiu a atenção de várias gerações de matemáticos, profissionais e amadores, e desafiou brilhantes matemáticos por mais de 350 anos, que foram levados a desenvolver técnicas bastante sofisticadas, criar novas teorias matemáticas, e provar resultados que, aparentemente, eram mais difíceis. Neste trabalho, analisamos o último teorema de Fermat para alguns valores específicos, sob algumas condições, por meio de conceitos básicos da Teoria Elementar dos Números.

Palavras-chave: Pierre de Fermat; teoria dos números; teorema de Fermat; Sophie Germain.

ABSTRACT

Fermat's Last Theorem is one of the most famous results in mathematics and one that has inspired new mathematical ideas and theories. This theorem has a very simple statement, understandable to every reader, which gives it a beauty of its own, but it was not easy to prove. This problem attracted the attention of several generations of mathematicians, both professional and amateur, and challenged brilliant mathematicians for more than 350 years, who were driven to develop very sophisticated techniques, create new mathematical theories, and prove results that were apparently more difficult. In this paper, we analyze Fermat's Last Theorem for some specific values, under some conditions, using basic concepts from Elementary Number Theory.

Keywords: Pierre de Fermat; number theory; Fermat's theorem; Sophie Germain.

SUMÁRIO

1 INTRODUÇÃO

"Os encantos dessa sublime ciência se revelam apenas àqueles que têm coragem de irem a fundo nela."

Carl Friedrich Gauss (1777 – 1855)

Pierre de Fermat (1601 – 1665), que muitos o consideram o pai da moderna Teoria dos Números, foi um matemático amador francês que dedicou parte de seus estudos a problemas diofantinos. Ele possuia um hábito peculiar quanto à forma de publicizar seus resultados. Quando não os guardava para si mesmo, ele os comunicava em cartas a amigos, geralmente sob uma forma bastante concisa de que possuía uma prova de cada um deles. Muitas dessas notas foram registradas na margem de sua cópia do livro Aritmética, do matemático grego Diofanto (por volta de 285 e 299), cuja tradução deve-se ao matemático francês Claude-Gaspard Bachet (1581 – 1638). Falar de Fermat quase sempre nos faz recordar da equação diofantina não linear, a equação pitagórica:

$$x^2 + y^2 = z^2,$$

conhecida desde o estudo secundário, e nos mostra a seguinte propriedade:

Num triângulo retângulo, o quadrado da hipotenusa é igual à soma dos quadrados dos catetos, ou equivalentemente, é possível separar um quadrado em dois quadrados.

Em termos algébricos, Fermat afirmou que, se $n > 2$, a equação diofnatina

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

não possui soluções nos inteiros, exceto as soluções triviais, em que pelo menos uma das variáveis é igual a zero. Esta afirmação ficou conhecida como a Conjectura de Fermat, ou, posteriormente, como o *Último Teorema de Fermat*. Em torno de 1800, todas as afirmações marginais do exemplar do livro Aritmética de Diofanto, a cópia que pertencia a Fermat, foram provadas ou refutadas, com uma importante exceção, a do último teorema, não que ele seja o último resultado escrito por ele, mas o último que restou sem ser provado ou refutado. E daí que surgiu a denominação Conjectura de Fermat.

Somente em 1995, o matemático britânico Andrew Willes, com o auxílio do matemático Richard Taylor, também britânico, demonstrou o Último Teorema de Fermat. A contribuição de Taylor foi crucial em várias etapas do trabalho de Wiles, especialmente em relação à teoria das formas modulares e curvas elípticas. Em sua demonstração, Wiles empregou conceitos e técnicas extremamente sofisticados, tornando-a uma das provas

mais complexas da história. Devido à essa complexidade, alguns historiadores sugerem que Fermat pode ter encontrado um erro em sua própria "prova", pois não há menção a ela em sua correspondência com outros matemáticos.

O presente trabalho segue a metodologia qualitativa quanto à natureza da pesquisa, em que a técnica de coleta de dados empregada foi a pesquisa bibliográfica.

No Capítulo 1, temos uma narrativa histórica do Último Teorema de Fermat e os principais matemáticos que contribuíram, significamente, com provas de alguns casos particulares, porém generalizados, para este teorema. Dentre eles, destacamos a matemática Sophie Germain, com sua demonstração para os primos da forma p e $2p + 1$, conhecidos como os *primos de Germain*. E, como não poderia deixar de ser, destacamos, também, a prova geral dada por Wiles, que se dedicou ardualmente para transformar a conjectura de Fermat no Último Teorema de Fermat.

No Capítulo 2, tratamos dos pré-requisitos, no qual sintetizamos a parte teórica sobre os conceitos elementares de Teoria dos Números, como definições e propriedades elementares da aritmética, bem como resultados imprescindíveis para o próximo capítulo. Ressaltamos que, para as propriedades referentes ao máximo divisor comum, divisiblidade e congruência, não foram feitas demonstrações. Sugerimos as referências [1], [2] e [3] para tais.

No Capítulo 3, apresentaremos a prova de Germain para o Último Teorema de Fermat e faremos as demonstrações para os casos $n = 3k$, $n = 4k$ e $n = 5k$ sob forma condicionada, por meio de conceitos básicos da Teoria Elementar dos Números.

2 CAPÍTULO I

O Último Teorema de Fermat refere-se à última conjetura não resolvida atribuída ao matemático francês Pierre de Fermat, que viveu no século XVII. Ele enunciou que não existem soluções não triviais para a equação diofantina:

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

em que n é inteiro mair do que 2, e x, y e z são incógnitas inteiras.

Fermat então escreveu a seguinte nota:

> *"É impossível para um cubo ser escrito como a soma de dois cubos ou uma quarta potência ser escrita como a soma de duas quartas potências ou, em geral, para qualquer número que é uma potência maior do que a segunda, ser escrito como a soma de duas potências com o mesmo expoente".*

Fermat disse que teria encontrado alguma solução, pois ele escreveu:

"Descobri uma demonstração maravilhosa desta proposição que, no entanto, não cabe nas margens deste livro".

Esta anotação foi descoberta pelo seu filho após alguns anos de sua morte. A partir disso, o teorema tornou-se objeto de estudo e atraiu muitos matemáticos ao longo de mais de 350 anos, os quais contribuíram para demonstrar o teorema; entretanto, para casos específicos, dentre eles podemos citar: O próprio Fermat para $n = 4$, Leonhard Euler (1770), Peter Barlow (1811), Peter Dirichlet (1825), Gabriel Lamé (1839, 1847, 1865), Peter Guthrie Tait (1872) e Carl F. Gauss (1875, póstuma), entre outros. Destacamos os matemáticos como Sophie Germain (1823), Ernst Kummer (1847) e Louis Mordell (1922) por apresentar abordagens de formas diferenciadas dos demais.

No século XX, ainda foram feitas abordagens computacionais buscando provar o teorema em faixas específicas de números. Em 1995, Wiles apresentou uma prova completa e correta do teorema, após muitos anos de trabalho intenso e inovador. Isto representou um marco significativo na história da matemática e chamou a atenção da comunidade matemática e do público em geral. A conquista de Wiles consolidou-se como um dos maiores feitos matemáticos do século XX e destacou a importância da persistência, criatividade e inovação na resolução de problemas desafiadores. A resolução desse problema emblemático também exemplifica o dinamismo contínuo da Matemática, mostrando como novas teorias e técnicas podem ser desenvolvidas para enfrentar desafios aparentemente insolúveis.

Neste capítulo, apresentaremos, resumidamente, a contribuição histórica de matemáticos que se dedicaram a provar o Último Teorema de Fermat e seus precursores, os quais forneceram contribuições para novas ferramentas matemáticas em busca de demonstrá-lo. Destacaremos os principais matemáticos e suas contribuições, que desencadearam um progresso crescente para a Teoria dos Números.

2.1 Os precursores e suas abordagens do último teorema de Fermat

Nascido na França, Fermat foi um matemático amador de grande influência no século XVIII, mas sua profissão era jurista e magistrado. Seu interesse pela matemática se iniciou com a leitura do livro de aritmética de Diofanto. Sua contribuição para a matemática foi na Teoria das Probabilidades, na Geometria Analítica e Teoria dos Números. Contudo, ele ficou mais conhecido pelo Último Teorema. Além de ter sua profissão de advogado civil, foi um matemático talentoso e brilhante para sua época e também para seus contemporâneos.

No ano de 1629, Fermat se destacou quando apresentou o método para determinar máximo e mínimo e tangente a linhas curvas. Por causa disso, Pierre S. M. de Laplace (1749 – 1827), afirma, segundo Carl Benjamin Boyer (1906 – 1976), 1996:

"Fermat, o verdadeiro inventor do cálculo infinitesimal."

Figura 1 – Pierre de Fermat

fonte: https://www.writework.com/uploads/9/96742/portrait-pierre-fermat.png.

Fermat desenvolveu trabalhos relacionados sobre quadraturas, volumes, comprimentos de curvas e centros de gravidade, como também, um teorema para encontrar a área sob cada curva que, nos dias atuais, corresponde à integração de funções. Além disso, ele enaltece a importância da utilização dos eixos perpendiculares, a descoberta das equações da reta e da circunferência e as equações mais simples de elipse, parábola e hipérbole.

Em 1654, Fermat introduz a *Teoria das Probabilidades*, isso devido ao escritor francês Chevalier De Méré (1607 – 1684), que se dirigiu a Blaise Pascal (1623 – 1662) em busca de respostas para certos resultados em jogos de azar. Por sua vez, Pascal interessou-se

pelo assunto, mas sem obter resultados plausíveis e, dessa forma, por meio de cartas, correspondeu-se com Fermat. Sendo a probabilidade um assunto desconhecido para a época, o próprio Fermat teve que estudar certos problemas matemáticos e, a partir disso, começou a introduzir conceitos e teorias, como análise combinatória.

Entretanto, no início da sua trajetória como matemático, ficou extasiado pela obra escrita por Apolônio (262 a.C – 194 a.C), intitulada *Lugares Planos*, a qual ele fez uma nova reconstrução, levando-o, em 1636, a descobrir o princípio fundamental da Geometria Analítica. Não podemos deixar de ressaltar que Fermat era apaixonado pela Física, e uma de suas contribuições nesta área é conhecida como *princípio de Fermat em óptica*.

Ao longo da história, muitos matemáticos tentaram provar o Último Teorema de Fermat. O próprio Fermat mostrou um caso particular para $n = 4$, utilizando um método por ele demonstrado, conhecido como *"método à descida infinita"*. Este método consiste, então, no seguinte esquema (MUNIZ NETO, 2012, p. 55):

1. Supor que uma dada equação possui uma solução em inteiros não nulos.

2. Concluir daí que ela possui uma solução em inteiros positivos que seja, em algum sentido, mínima.

3. Deduzir a existência de uma solução positiva menor que a mínima, chegando a uma contradição.

Com esse método foi possível mostrar a veracidade do último teorema para os casos particulares $n = 3$ e $n = 5$. Ao longo do tempo, matemáticos brilhantes como Leonhard Euler (1707 – 1783), Adrien-Marie Legendre (1752 – 1833), Gabriel Lamé (1795 – 1870), Augustin-Louis Cauchy (1789 – 1857), Germain (1776 – 1831), Kummer (1810 – 1893), Évariste Galois (1811 – 1832), Paul Wolfskehl (1856 – 1906), Yutaka Taniyama (1927 – 1958), Goro Shimura (1930 – 2019) e Ken Ribet contribuíram de forma explícita e implícita para provar esse teorema. Tais contribuições foram bastante significativas para o avanço da matemática, pois muitos matemáticos elaboraram estratégias diferentes para mostrar casos particulares do teorema, entre essas estratégias, podemos citar a seguinte: Suponhamos que exista uma solução inteira para a equação da forma,

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

com $n > 2$. Considerando as possibilidades ao fatorar o seu lado esquerdo em um produto de elementos primos entre si, concluindo que cada um dos elementos deve ser uma $n-$ésima potência de algum outro número e, a partir disso, chegaram a uma contradição. Essa estratégia é verdadeira quando se trabalha com números inteiros na fatoração. No caso $n = 3$, Euler precisou usar números complexos da forma $a + b\sqrt{-3}$, para a e b inteiros, porém, no conjunto dos números da forma $a + b\sqrt{-3}$, não é válida a fatoração única em

irredutíveis, um resultado equivalente ao Teorema Fundamental da Aritmética sobre o conjuntos dos números inteiros. A estratégia de Euler usando esses números complexos teria que assegurar sua unicidade na fatoração, pois, sem isso, não se poderia garantir que os elementos da fatoração sejam uma $n-$ésima potência de algum outro número. Isso nos dá uma perspectiva da dificuldade que logo viria para provar o último teorema.

Em 1847, Lamé afirmou que estaria prestes a apresentar a prova do último teorema, utilizando uma fatoração no corpo dos números complexos $\mathbb{C}$, sem provar que a fatoração em irredutíveis nesse corpo é única. Na mesma época, Lamé recebeu a notícia, enviada pelo matemático Kummer, que a fatoração em $\mathbb{C}$ não é única. Ele apresentou sua prova para $n = 23$, que não só decepcionou Lamé, mas também o matemático Augustin-Louis Cauchy (1789 – 1857) que, na época, afirmava que a prova do último teorema estaria quase concluída.

Apesar disso, a ideia de fatoração feita por Lamé e sua fatoração de raízes complexas da unidade teve como início a análise do corpo $\mathbb{Q}(\zeta)$, o corpo das raízes de ζ sobre o corpo dos racionais $\mathbb{Q}$, em que ζ é uma $n-$ésima primitiva da unidade. A partir dessa ideia Kummer introduziu os chamados números *primos regulares*, e os "*números ideais*", que funcionavam para o estudo deste problema e sempre podiam ser fatorados de maneira única.

Em linguagem atual, os números ideais correspondem aos ideais de um anel, como foi introduzido por Richard Dedekind (1831 – 1916). Em 1850, Kummer provou o último teorema para os chamados números primos regulares, o qual incluíam todos os números primos menores do que 100, exceto 37, 59 e 67. A prova de Kummer, cerca de três anos após Lamé ter anunciado a sua "prova", foi o maior avanço significativo até a demonstração completa por Wiles. Entretanto, antes de tudo, Dedekind generalizou o conceito de ideal, iniciando com a fatoração de ideais primos. Tal conceito é bem mais simples do que a fatoração de elementos exposta por Lamé, o qual foi um dos pilares primordiais para a solução completa do último teorema.

2.2 Métodos apresentados em busca de solucionar o último teorema de Fermat

A demonstração do Último Teorema de Fermat inicia-se basicamente na Teoria dos Números como, por exemplo, método de descida de Fermat, para $n = 4$, até os conceitos mais avançados da Álgebra Abstrata, que incluem Teoria de Anéis e Grupos (grupos quociente, homomorfismos de anéis, corpos de frações, etc) e alguns conceitos elementares de Álgebra Linear.

Segundo relatos históricos, o filho mais velho de Fermat, Clemént-Samuel Fermat, publicou, em 1670, uma nova edição da obra Aritmética de Diofanto com todas as anotações feitas por Fermat. Uma dessas anotações continha o *método da descida infinita*.

Fermat fez a demonstração para o caso $n = 4$. Por meio deste método, ele mostra que a equação:

$$x^4 + y^4 = z^2 \tag{2.1}$$

não possui soluções inteiras positivas. Por conseguinte, a equação $x^4 + y^4 = z^4$ não possui soluções inteiras positivas. O método pressupõe a existência de uma solução (a, b, c) para a equação eq. (2.1), com c mínimo. Com essa ideia, Fermat mostrou que existe outra solução (u, v, t) para eq. (2.1), com u, v e t inteiros positivos, porém, $t < c$, uma contradição.

Com o caso $n = 4$ provado, a prova do último teorema se resumia aos casos em que n é um primo ímpar. Para esses infinitos casos, não bastavam apenas provar casos isolados. Dessa forma, os matemáticos dessa época começaram a tentar provar para infinitos casos de uma só vez. O estudo de classes de números mais amplos do que inteiros desempenhou papel central para este problema.

Entretanto, antes de Euler, vários matemáticos já haviam tentado adaptar o método da descida infinita para outros casos, porém sem sucesso. No entanto, Euler empreendeu tal abordagem ao incorporar o conceito de números imaginários à demonstração para o caso $n = 3$, pressupondo que esses números possuíssem as mesmas propriedades que os números inteiros. Contudo, a prova apresentada por Euler revelou-se incompleta. Não obstante, é digno de nota o avanço significativo promovido por Euler na direção da demonstração desse teorema.

O anel usado por Euler foi

$$\mathbb{Z} = [\sqrt{-3}] = \{a + b\sqrt{-3} : a, b \in \mathbb{Z}\},$$

uma extensão do anel dos números inteiros. Posteriormente, Joseph-Louis Lagrange (1736 – 1813) corrigiu e completou a prova de Euler, utilizando técnicas mais avançadas de teoria dos números. Lagrange mostrou que o anel considerado por Euler não era suficiente para provar o teorema e introduziu o conceito de *"formas quadráticas"* para resolver o problema. A contribuição de Lagrange foi fundamental para o desenvolvimento da Teoria dos Números e abriu caminho para futuras provas.

Para provar o caso $n = 3$, Euler utilizou o seguinte lema:

Lema 2.1. *Todas as soluções de* $s^3 = a^2 + 3b^2$ *em inteiros positivos, com* $\text{mdc}(a, b) = 1$ *e* s *é ímpar, são dadas por*

$$s = m^2 + 3n^2,\ a = m^3 - 9mn^2,\ b = 3m^2n - 3n^3,$$

com $m + n$ *ímpar e* $\text{mdc}(m, 3n) = 1$.

Com o método de descida infinita de Fermat e com resultados de números primos, ele provou que:

"A equação diofantina $x^3 + y^3 = z^3$ não possui soluções inteiras, com $xyz \neq 0$."

Euler considerou que sua prova para o caso $n = 3$ estava muito diferente da prova para o caso $n = 4$, e que a prova do caso geral parecia estar muito distante. Nos noventa anos seguintes, muitas contribuições à resolução do último teorema foram realizadas por grandes matemáticos da época, como Germain, Johann P. G. L. Dirichlet (1805 – 1859), Lamé, Legendre e Kummer.

Destacamos os casos $n = 3$ e $n = 4$ do último teorema, cujas demonstrações foram apresentadas, conforme Ribenboim (1999, pp. 15 e 33).

Figura 2 – Caso $n = 3$

Autor	Ano	Autor	Ano
Euler	1670	Krey	1909
Kausler	1795/6 (publicado 1802)	Rychilik	1910
Legendre	1823, 1830)	Stockhaus	1910
Calzolari	1855	Carmichael	1915
Lamé	1865	Van der Corput	1915
Tait	1872	Thue	1917
Günther	1878	Duarte	1944
Gambioli	1901		

Fonte: Ribenboim (1999, p. 33).

Figura 3 – Caso $n = 4$

Autor	Ano	Autor	Ano
Frénicle De Bessy	1676	Tafelmacher	1893
Euler	1738 (publicado 1747), 1771	Benda	1901
Kausle	1795/6 (publicado 1802)	Gambioli	1901
Barlow	1811	Kronecker	1901
Legendre	1823, 1830	Bang	1905
Schopis	1825	Bottari	1908
Terquem	1846	Rychlik	1910
Bertrand	1851	Nutzhorn	1912
Lebesgue	1853, 1859, 1862	Carmichae	1913
Pepin	1883	Vranceanu	1966

Fonte: Ribenboim (1999, p. 15).

Em 1823, Germain dividiu a equação $x^n + y^n = z^n$ em dois casos em que o expoente $n = p$ é um primo ímpar:

(1) Nenhum dos números x, y e z é divisível por p;

(2) Somente um dos números x, y e z é divisível por p.

Ela provou o caso (1), desde que $2p+1$ seja primo. Legendre generalizou este caso para primos ímpares p tais que $kp+1$ é primo, com k= 4, 8, 10, 14 e 16. Desta forma, as atenções foram voltadas para o caso (2) de Germain. Nesta direção, a primeira contribuição foi dada por Dirichlet e Legendre, os quais de forma independente, provaram o caso $n = 5$, utilizando a fatoração única nos Anéis de Dedekind. Lamé fez acréscimos engenhosos ao método de Germain e provou o caso $n = 7$. A sua demonstração está baseada na teoria geral das coordenadas curvilíneas pela equação:

$$\left|\frac{x}{a}\right|^n + \left|\frac{y}{b}\right|^n = 1.$$

Além disso, ele utilizou uma expressão algébrica com fatores lineares e quadráticos equivalente a $(x + y + z)^7 - (x^7 + y^7 + z^7)$.

Segundo Ribenboim (1999, p. 55), as principais demonstrações apresentadas para o caso $n = 5$ cuja prova completa se subdivide nos dois casos Germain, foram as seguintes:

Figura 4 – Caso $n = 5$

Autor	Casos	Ano
Gauss	Ambos	1863 (com publicação póstuma)
Schopis	1º Caso	1825
Lebesgue	Ambos	1843
Lamé	Ambos	1847
Gambioli	Ambos	1901 e 1903
Werebrusow	Ambos	1905
Mirimanoff	1º Caso	1909
Rychlik	Ambos	1910
Hayashi	Ambos	1911
Van Der Corput	Ambos	1915
Terjanian	Ambos	1987

Fonte: Ribenboim (1999, p. 55).

Em 1847, Lamé anunciou que havia solucionado o Último Teorema de Fermat usando conjuntos do tipo $\mathbb{Z}[\zeta]$ (chamados de “anéis de números algébricos” ou “anéis de números

de Dirichlet", caracterizados por estenderem os números inteiros a números complexos algébricos), admitindo que esses possuíssem a propriedade chamada de *fatoração única de elementos*, a qual é encontrada no conjunto dos números inteiros, mas não é em todos os conjuntos da forma $\mathbb{Z}[\zeta] = \{a_0 + a_1\zeta + a_2\zeta^2 + ... + a_{n-1}\zeta^{n-1} | \, a_i \in \mathbb{Z}\}$, em que ζ é uma raiz complexa da unidade, isto é, $\zeta^n = 1$ para algum inteiro n. Esse foi um dos grandes problemas encontrados pelos matemáticos que buscavam provar o resultado, pois nem sempre é fácil verificar se um conjunto desse tipo apresenta a unicidade da fatoração de seus elementos. Posteriormente, em seu trabalho, Kummer provou o último teorema para casos específicos, empregando o conceito de primo regular e ideais primos em $\mathbb{Z}[\zeta]$, para estabelecer a fatoração única de ideais algébricos.

A ideia de Lamé baseou-se em introduzir a raiz $n-$ésima da unidade

$$\zeta = e^{\frac{2\pi i}{n}}$$

para fatorar a $x^n + y^n = z^n$ em termos lineares, da seguinte forma:

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

Quando $n = p$ é primo, então, $x^p + y^p = z^p$. Assim,

$$z^p = (x + y)(x + \zeta_p y)(x + {\zeta_p}^2 y) \dots (x + {\zeta_p}^{p-1} y).$$

Assim, devem existir $\varphi_0, \varphi_1, \dots, \varphi_{p-1} \in \mathbb{Z}[\zeta]$ tais que

$$\begin{aligned} x + y &= \varphi_0^p, \\ x + {\zeta_p}^1 y &= \varphi_1^p, \\ x + {\zeta_p}^2 y &= \varphi_2^p, \\ &\vdots \\ x + {\zeta_p}^{p-1} y &= \varphi_{p-1}^p. \end{aligned}$$

Dessa maneira, Lamé pretendia gerar uma descida infinita nos naturais, o que tornaria possível a demonstração do último teorema.

Entretanto, Liouville (1809 – 1882) observou que esta ideia necessitava de uma fatoração única em $\mathbb{Z}[\zeta]$ na forma:

$$a_0 + a_1\zeta + \dots + a_k\zeta^k,$$

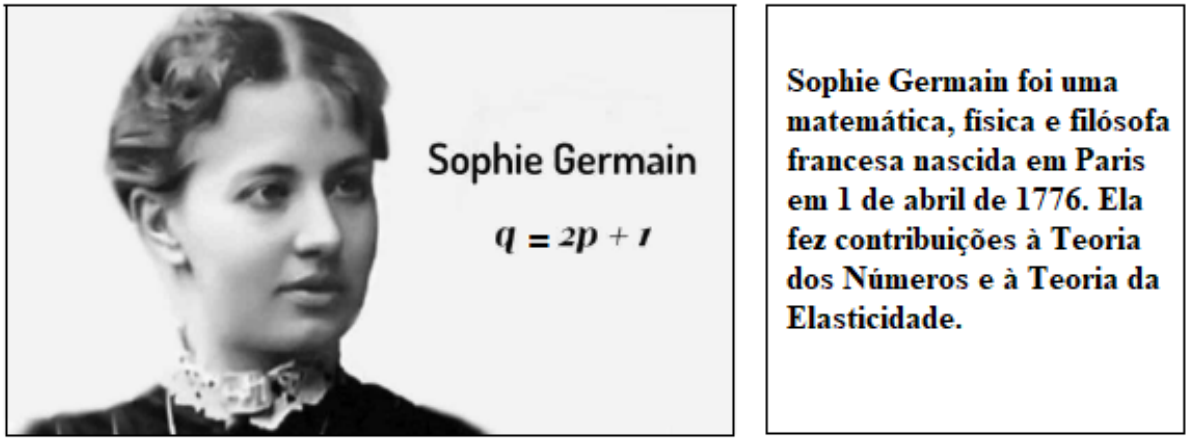
com $a_1, \dots, a_k$ números inteiros e k natural. Kummer provou que nem sempre tal fatoração é única. Com efeito, em $\mathbb{Z}[\sqrt{13}i]$, $\mathbb{Z}[\sqrt{5}i]$ e $\mathbb{Z}[\sqrt{10}i]$, temos as fatorações:

$$14 = 2 \times 7 = (1 + \sqrt{13}i)(1 - \sqrt{13}i) = (3 + \sqrt{5}i)(3 - \sqrt{5}i) = (2 + \sqrt{10}i)(2 - \sqrt{10}i),$$

ou seja, não existe fatoração única, mas escolhas de fatorações, o que constitui um erro grave na "prova" de Lamé. Kummer obteve uma prova do último teorema para todos os primos regulares. Um número primo p é *regular* se não dividir o número de classe do p–ésimo corpo ciclotômico (ou seja, o corpo de número algébrico obtido anexando a p–ésima raiz da unidade aos números racionais). Os primeiros primos regulares são: $3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 41, \ldots$. Kummer chegou a afirmar que o conjunto dos primos regulares seriam infinitos. A esperança era a de que, se os primos irregulares (que não são regulares) fossem finitos, então bastaria provar cada caso desses separadamente, mas essa abordagem se mostrou muito complicada. Com isso, tornou-se necessário criar uma nova abordagem para provar o último teorema para primos irregulares, que não surgiu antes da demonstração de Wiles.

2.3 Sophie Germain e o último teorema de Fermat

Figura 5 – Sofhie Germain



Fonte:`https://www.muhendisbeyinler.net/wp-content/uploads/2018/04/sophie-germain-eserleri.jpg`.

Germain, filha de Marie Madelaine Gruguelin e de Ambroise François, que foi um próspero comerciante de seda, iniciou sua carreira matemática aos treze anos de idade. Após ela ler um relato da morte de Arquimedes, que morreu pelas mãos de um soldado romano, decidiu se tornar uma matemática.

Germain se tornou uma ilustre apaixonada pela Teoria dos Números no início de sua carreira, porém, a presença de mulheres nas escolas não era permitida. Entretanto, ela não desistiu e começou a se corresponder com grandes matemáticos de sua época, tais como Lagrange, Legendre e Gauss. Algumas vezes sob o pseudônimo de M. Leblanc, pelo fato

da discriminação de ser mulher, o que impediria que seus trabalhos recebessem a devida atenção. Sendo assim, o próprio Lagrange, reconhecendo o brilhantismo de Germain, foi seu grande mentor, conselheiro e incentivador.

Entre 1804 e 1809, Germain correspondeu-se com Gauss a respeito dos métodos apresentados por ele em suas "Disquisitiones Arithmeticae". Nesse período, produziu alguns resultados importantes relacionados com o "*Último Teorema de Fermat*".

Gauss, reconhecendo o talento engenhoso de Germain, recomendou-a vigorosamente para um grau de doutor honorário da Universidade de Göttingen, mas ela morreu antes que essa honra lhe fosse concedida, falecendo no dia 27 de Junho de 1831. No seu pleno auge, Germain ganhou um prêmio da Academia Francesa de Ciências por sua tese na Teoria da Elasticidade, ramo na qual foi pioneira e provou a validade do último teorema, para uma classe de números primos, que ficou conhecido como *primos de Germain*.

Legendre, ao publicar "Ensaio sobre a Teoria dos Números", em 1798, faz menção ao seguinte resultado de Germain: Se $x^5 + y^5 = z^5$, então, um dos inteiros x, y ou z deve ser divisível por 5.

Vale ressaltar que Germain contribuiu enfaticamente para a Teoria dos Resíduos Quadráticos, a Lei da Reciprocidade Quadrática e a Teoria das Equações Diofantinas. Além do mais, ela introduziu ferramentas importantes envolvendo conceitos de anéis, grupos e corpos para primos que não fossem primos de Germain. Dessa forma, ela mostrou que o último teorema era válido para todos os números primos menores que 100.

Em 1831, aos 55 anos, Germain morreu devido a um câncer de mama. Ao longo de sua vida como mulher, em uma área dominada por homens, ela fez importantes contribuições para a Matemática, sendo uma das pioneiras no estudo de propriedades dos números primos e trabalhou em Mecânica Teórica, no estudo da Elasticidade dos Corpos e propôs uma Teoria de Vibração dos Corpos Sólidos.

2.4 Andrew Wiles apresenta a demonstração do último teorema de Fermat

Figura 6 – Andrew John Wiles

Andrew John Wiles é um matemático britânico, professor na Universidade de Princeton, famoso por ter demonstrado, com a colaboração de Richard Lawrence Taylor, o Teorema de Fermat, em 1994.

Fonte: `https://www.echosciences-sud.fr/uploads/article/image/attachment/1005451195/xl_20-ans-septembre-1994-andrew-wiles-triomphe-dernier-theoreme-fermat.jpg`.

"Fermat disse que ele tinha uma prova." (Andrew Wiles)

Andrew Wiles nasceu no dia 11 de abril de 1953, em Cambridge, Inglaterra. Tornou-se PhD em Matemática pela Universidade de Cambridge (1975 – 1979), sob a orientação do australiano John Coates, e foi professor em Princeton. A partir da década de 80, consagrou-se como matemático por provar, em 1995, o Último Teorema de Fermat, um dos mais famosos desafios da Matemática. As principais contribuições de Wiles à matemática:

- A demonstração do Último Teorema de Fermat, um problema que havia sido proposto por Fermat desde 1637 e que permaneceu sem solução por mais de 350 anos.
- Importantes trabalhos na Teoria dos Números, incluindo os primeiros resultados da conjectura de Birch e Swinnerton-Dyer e contribuições para a "conjectura principal" da Teoria de Iwasawa.

Por suas contribuições à matemática, Wiles recebeu importantes prêmios, tais como:

- Recebimento de vários prêmios e honrarias, incluindo o Prêmio Whitehead da London Mathematical Society, o Prêmio Rolf Schock em Matemática da Academia Real das Ciências da Suécia, o Prêmio Ostrowski da Universidade de Basel, o Prêmio Fermat e o Prêmio Wolf em Matemática.
- Agraciado, em 2016, com o Prêmio Abel por sua contribuição à Matemática.

Para demonstrar o último teorema, Wiles usou uma teoria totalmente diferente, que relacionava equações elípticas e formas modulares. Entretanto, a teoria não foi criada por ele. Os primeiros a imaginarem uma conexão entre as formas modulares e as curvas

elípticas, ou mais exatamente, um isomorfismo entre elas, foram os japoneses Yutaka Taniyama e Goro Shimura. À luz dessa conjectura, o alemão Gerhard Frey afirmou que essa conjectura implicava na prova do Último Teorema de Fermat. Tal afirmação foi provada pelo norte-americano Ken Ribet. Por fim, o último passo, provavelmente o mais difícil, foi dado por Wiles, em uma demonstração da conjectura de Taniyama-Shimura com mais de 100 páginas.

No século XX, os matemáticos Taniyama e Shimura intensificaram seus estudos nas formas modulares, assim como o matemático Martin Escher. Eles deram uma compreensão significativa para as formas modulares, pois ainda não estava claro para alguns pesquisadores da área o elo entre formas modulares e curvas elípticas. No século XIX, os matemáticos começaram a explorar as formas modulares, que despertaram interesse devido à sua simetria. No entanto, estudar essas formas era complicado e abstrato na época, dificultando sua compreensão como ferramenta matemática. Por outro lado, as equações elípticas já eram conhecidas pelos gregos desde a antiga Grécia. Por fim, não havia nenhuma equação elíptica com simetria notável.

No simpósio internacional de matemática, em 1955, realizado na Cidade de Tókio no Japão, Taniyama e Shimura anunciam um resultado central para a prova do último teorema: As formas modulares e as equações elípticas são uma coisa só, isto é, elas podem se unificar. Assim, nasce a conjectura de Taniyama e Shimura:

"Toda curva elíptica racional é modular".

Tal conjectura se tornou ainda mais forte devido ao trabalho do francês André Weil (1906 – 1998), um dos mais talentosos e respeitados matemáticos na Teoria dos Números do século XX. Ele encontrou evidências plausíveis da conjectura, inspirando em 1960, o "Programa de Langlands", cujo professor Robert Langlands da cidade de Princeton no EUA fez um projeto de pesquisa matemática, o qual investigava as relações profundas entre as diversas áreas da matemática com suas respectivas sutilezas.

Em 1985, Frey propôs uma nova abordagem para o Último Teorema de Fermat, fundamentada na noção de *modularidade*. Frey conjecturou se (A, B, C) fosse uma solução hipotética da equação $x^n + y^n = z^n$, isto é, $A^n + B^n = C^n$, com certas manobras e séries complicadas, conseguiu modular a equação original de Fermat com sua solução hipotética para criar a equação elíptica:

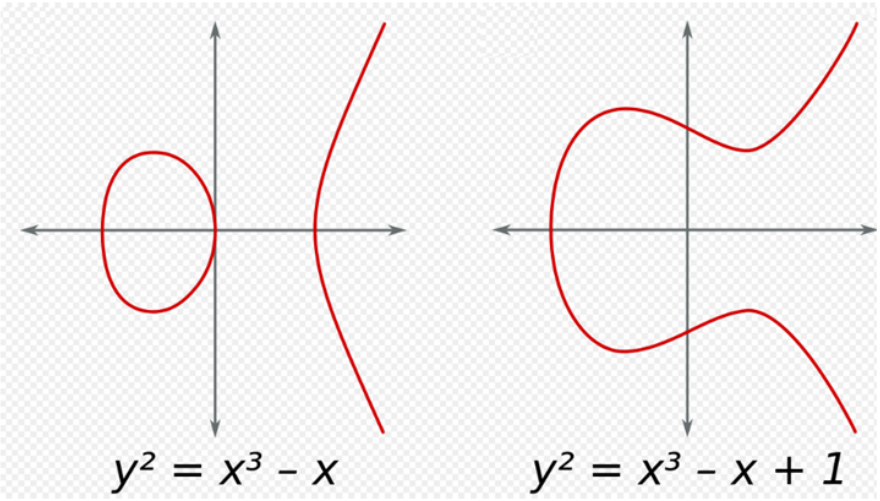
$$y^2 = x^3 + (A^n - B^n)x^2 + A^n B^n.$$

Está equação elíptica gera uma curva **elíptica semi-estável**, conhecida como Curva de Frey. Posteriormente, Frey afirmou que a prova dessa conjectura implicaria na prova do Último Teorema de Fermat.

Uma equação elíptica possui a seguinte forma:

$$y^2 = x^3 + ax^2 + bx + c, \text{ com } a, b \text{ e } c \text{ números inteiros.}$$

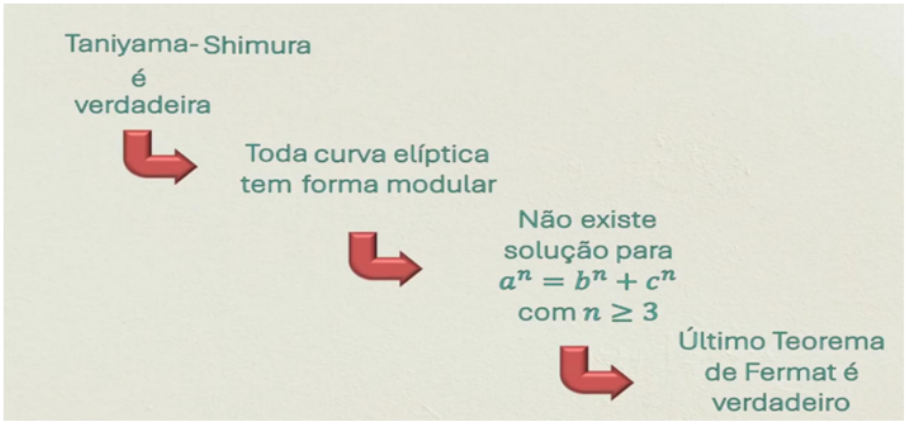
Figura 7 – Exemplos de Curvas Elípticas



Fonte:https://marcoce281.wordpress.com/2009/04/16/criptografia-de-curvas-elipticas/.

O matemático francês Jean-Pierre Serre, do Collège de France, refinou mais ainda essa ideia de Frey, que foi desenvolvida pelo matemático estadunidense Kenneth Ribet, da Universidade da Califórnia em Berkeley. Ribet demonstrou que se a conjectura relativa à modularidade fosse verdadeira, então se seguiria o Último teorema de Fermat, ou seja, ele mostrou que se toda curva elíptica semi-estável é modular, então o Último Teorema de Fermat é verdadeiro.

Figura 8 – Conjectura (Frey – Jean-Pierre – Ribet)



Fonte: Elaborado pelo autor, 2025.

Frey – Jean-Pierre – Ribet chegaram à conclusão que, para demonstrar o último teorema, deveria demonstrar a conjectura de Taniyama-Shimura. Porém, tal conjectura seria um dos problemas mais difíceis de encarar devido à complexidade matemática inerente. Entretanto, Wiles usou sua maior arma matemática que ele tinha como domínio,

a Teoria dos Grupos. Enquanto os grupos de Galois eram formados a partir de soluções de equações do quinto grau, Wiles formou seus grupos por meio de certa quantidade de equações elípticas; ele utilizou seus grupos elípticos, após longos meses de dedicação e estudo, para igualar cada uma de suas equações elípticas nas suas respectivas formas modulares, pois, fazendo isso, poderia estudar expressivamente a conjectura de Taniyama-Shimura. Contudo, algo faltava a Wiles para dar um ponto final na conjectura. Ele resolveu desenvolver um novo método que envolvia a análise de equações elípticas após ver o trabalho de Kolyvagin-Flach, mas isso tomaria meses e meses de sua vida dedicada a esse desenvolvimento, o qual conseguira com grande êxito. Com essa nova técnica, após seis anos de sua vida, Wiles provou que as novas famílias de curvas eram modulares unindo sua nova técnica de Kolyvagin-Flach com o método de Iwasawa (tal método serve para analisar as equações elípticas), finalizando um momento crucial da história do último teorema, que chegara à sua demonstração final, um momento o qual Wiles passou anos esperando e acreditando no seu brilhantismo, que de fato se tornou memorável para sua vida e para a história da matemática, onde a conjectura de Taniyama-Shimura foi provada e, por conseguinte, o último teorema.

Após sete anos de estudos árduos e secretos, Wiles anunciou, em 1993, que havia provado o teorema de Fermat. No entanto, infelizmente, o momento ainda não havia chegado, pois sua prova continha uma falha. A comissão avaliadora propôs que o matemático Taylor ajudasse Wiles a corrigir essa falha. Assim, em outubro de 1994, a demonstração definitiva foi entregue para análise e publicada em maio de 1995, em dois artigos que juntos totalizam mais de 120 páginas.

Wiles demonstrou a importância de olhar para o mesmo problema com uma visão diferente. Inicialmente, ele utilizou desde os conhecimentos básicos da Teoria dos Números até os mais profundos e inovadores objetos matemáticos, contribuindo significativamente para a história da Matemática.

3 CAPÍTULO II

"*Matemática é a rainha da ciência, e aritmética a rainha da matemática.*"

Carl Friedrich Gauss (1777 – 1855)

Neste capítulo, destacaremos o conceito de divisibilidade no conjunto dos números inteiros, destacando, especialmente, o Algoritmo da Divisão e máximo divisor comum de inteiros. Consideramos, também, propriedades inerentes aos números primos. Por fim, apresentaremos proposições relevantes para capítulo subsequente e introduziremos o conceito de congruências modulares, uma ferramenta eficaz para investigar propriedades de divisibilidade.

3.1 Divisibilidade

O conceito de divisibilidade é central na Teoria dos Números, pois muitos problemas dessa teoria estão relacionadas com questões intrínsecas a este conceito. Os resultados básicos considerados neste capítulo podem ser verificados em [1].

Definição 3.1 (**Divisibilidade**)**.** Sejam a e b inteiros. Diremos que b *divide* a, em símbolos $b \mid a$, quando existir um inteiro c tal que $a = bc$. Caso contrário, diremos que b não divide a, em símbolos, $b \nmid a$.

Definição 3.2 (**Números Primos**)**.** Um número inteiro $p > 1$ diz-se *primo* quando possui somente dois divisores positivos, 1 e o próprio p.

Exemplo 3.1. Notemos que: $4 \mid 84$, pois $84 = 4 \times 21$. Por outro lado, $3 \nmid 46$, pois $46 = 3 \times 15 + 1$, ou seja, a divisão não é exata.

Os números primos são conhecidos desde a Grécia antiga. No livro de Euclides, "*Os elementos*", o próprio Euclides faz uma demonstração sobre a infinidade desses números.

É relevante destacar que os números primos têm despertado grande fascínio entre matemáticos e estudiosos de outras eras, devido à sua complexidade e relevância no contexto contemporâneo. Por exemplo, eles desempenham um papel significativo em áreas como Criptografia, Matemática Computacional e na Teoria dos Códigos, áreas extremamente importantes para o desenvolvimento científico.

Vejamos alguns teoremas relacionados aos números primos e alguns primos especiais, os quais desempenham um papel crucial na Teoria dos Números, em outras aplicações práticas:

(1) **(Infinitude)** Existe um número infinito de números primos. Este fato foi provado pela primeira vez por Euclides, em seu Livro IX, Proposição 20, dos "Elementos"de Euclides.

(2) **(Teorema Fundamental da Aritmética – TFA)** Este teorema estabelece que todo número natural maior do que 1 pode ser representado, de forma única, como um produto de números primos, a menos da ordem dos fatores e multiplicidade de cada fator.

(3) **(Função Número de Primos)** Existem funções específicas na Teoria dos Números, como a função $\pi(x)$ que conta o número de primos menores ou iguais a x, e a função $\Psi(x)$ que fornece a soma dos logaritmos naturais de todos os números primos menores ou iguais a x.

(4) **(Primos de Mersenne)** São primos da forma $2^p - 1$, com p primo. Esses primos são essenciais para encontrar números perfeitos, que são números iguais à soma de seus divisores próprios positivos, exceto ele próprio.

(5) (**Primos de Fermat)** São números primos da forma $2^{2^n} + 1$. Esses primos testam primalidade.

(6) **(Teorema dos Números Primos)** Este teorema estabelece que a quantidade de números primos é assintoticamente equivalente a $x/ln(x)$, em que x é um número relativamente grande. Em outras palavras, a densidade de números primos entre os números naturais diminui à medida que os números aumentam, mas ainda assim há um número infinito deles.

(7) **(Distribuição Aleatória)** Apesar da aparente imprevisibilidade na distribuição dos números primos, eles exibem certas propriedades estatísticas interessantes quando observados em grandes conjuntos.

(8) **(Primos de Sophie Germain)** São primos p tais que $2p + 1$ também é primo. Germain provou o Último Teorema de Fermat para tais primos.

(9) **(Primos de Newman - Shanks - Williams – NSW)** São primos que seguem uma determinada forma recursiva. Esses primos têm aplicações em Teoria dos

Números e em algoritmos (algoritmos de criptografia, como o algoritmo de Diffie-Hellman, e em testes de primalidade). Exemplos de primos NSW:

$$107 + 9270 \times 10^{3503}, \quad 101 + 9520 \times 10^{3511} \quad \text{e} \quad 103 + 9550 \times 10^{3514}.$$

(10) **(Primos de Wieferich)** São primos p tais que $2^{p-1} \equiv 1 \pmod{p^2}$; esses primos estabelecem importantes conexões na Teoria dos Números.

3.1.1 *Propriedades da divisibilidade*

Em Matemática, a *divisibilidade* é um conceito essencial que descreve a relação entre dois números inteiros, em que um número pode ser dividido pelo outro sem deixar resto. Além do mais, trata-se de um tema fundamental e central, não apenas para a Teoria Elementar, mas também para diversos outros ramos da Teoria dos Números.

As três primeiras propriedades básicas da divisibilidade que destacaremos são seguintes: dados inteiros a, b, c e d, então:

(1) $a \mid b$ e $b \mid c \;\Rightarrow\; a \mid c$

(2) $a \mid b$ e $c \mid d \;\Rightarrow\; ac \mid bd$

(3) $a \mid b$ e $a \mid c \;\Rightarrow\; a \mid (bn + cm)$, para todo inteiro m e n.

A propriedade (3) anterior pode ser generalizada da seguinte forma:

Se $a_1, a_2, \ldots, a_n$ são inteiros divisíveis por a, então,

$$a \mid (a_1x_1 + a_2x_2 + \ldots + a_nx_n),$$

para quaisquer inteiros $x_1, x_2, \ldots, x_n$.

3.2 Máximo divisor comum

O conceito de *máximo divisor comum* (mdc) de dois inteiros é um dos principais e mais básicos na Teoria do Números. Numa linguagem mais técnica, faz-se o seguinte: consideremos a e b inteiros, com a ou b não nulos, e sejam $D(a)$ e $D(b)$ os conjuntos dos divisores positivos de a e b , respectivamente, isto é,

$$D(a) = \{n \in \mathbb{N} : n \mid a\} \quad \text{e} \quad D(b) = \{n \in \mathbb{N} : n \mid b\}.$$

Nestas condições, $D(a) \cap D(b) \neq \varnothing$, pois $1 \mid a$ e $1 \mid b$. Além do mais, o conjunto $D(a) \cap D(b)$ é finito e, por isso, possui um maior elemento, chamado máximo divisor comum de a e b, denotado por $\text{mdc}\,(a, b)$. Formalmente, temos a seguinte definição:

Definição 3.3 (**Máximo Divisor Comum**)**.** Sejam $a, b \in \mathbb{Z}$, com $a \neq 0$ ou $b \neq 0$. Dizemos que $d \in \mathbb{N}$ é o *máximo divisor comum* de a e b quando as seguintes condições são satisfeitas:

1. $d \mid a \quad$ e $\quad d \mid b$;
2. $\forall c \in \mathbb{Z}, \quad$ se $\quad c \mid a \quad$ e $\quad c \mid b, \quad$ então, $\quad c \mid d$.

Em outras palavras, o máximo divisor comum de a e b é um número natural que os divide e é divisível por todo divisor comum de a e b.

3.2.1 *Propriedades de máximo divisor comum*

No que segue, destacaremos algumas propriedades do mdc. Sejam a, b e c números inteiros. Então, são válidas as propriedades:

(1) $\text{mdc}\,(a, 0) = |a|$.

(2) $\text{mdc}\,(a, 1) = 1$.

(3) $\text{mdc}\,(a, a) = |a|$.

(4) $\text{mdc}\,(a, b) = \text{mdc}\,(b, a)$.

(5) $\text{mdc}\,(a, b) = \text{mdc}\,(-a, b) = \text{mdc}\,(a, -b) = \text{mdc}\,(-a, -b)$.

A propriedade (5) nos diz que, para determinar o máximo divisor comum de dois inteiros, basta considerá-los positivos. Quando $\text{mdc}\,(a, b) = 1$, dizemos que os inteiros a e b *são primos entre si* ou *relativamente primos*.

3.3 Algoritmo da divisão

Historicamente, o Algoritmo da Divisão tem suas raízes na antiguidade, com evidências de sua utilização pelos egípcios e babilônios. Contudo, foi apenas no século XIX que o algoritmo foi formalmente estabelecido e generalizado para números inteiros.

Teorema 3.1 (**Algoritmo da divisão**). *Sejam a e b inteiros, com $b > 0$. Então, existem únicos inteiros q e r, tais que*

$$a = bq + r,$$

em que $0 \leq r \leq b - 1$. Os inteiros q e r são chamados, respectivamente, quociente e resto da divisão de a por b.

Demonstração: Há duas coisas a serem provadas: uma é a existência de q e r, e a outra é a unicidade destes inteiros.

(Existência) Considere o conjunto

$$S = \{a - bk : a - bk \geq 0 \quad \text{e} \quad k \in \mathbb{Z}\}.$$

Primeiramente $S \neq \varnothing$, pois, para $a \geq 0$, temos $a = a - b \times 0 \geq 0$, e para $a < 0$, $a - ba = a(1 - b) \geq 0$, já que $1 - b \leq 0$. Como $S \neq \varnothing$, então pelo princípio da Boa Ordem, ele possui um menor elemento. Digamos que $r = \min\ S$. Assim, existe $q \in \mathbb{Z}$ tal que $r = a - bq$ para algum inteiro q.

Mostremos que de r é o resto desejado. Para isto, precisamos mostrar que $0 \leq r < b$. Vejamos:

1. $r \geq 0$, pois escolhemos r como o menor elemento de S.

2. $r < b$. Suponhamos, por contradição, $r \geq b$. Assim,

$$r = a - bq = b \geq 0 \Rightarrow\ a - b(q + 1) \geq 0 \Rightarrow a - b(q + 1) \in S,$$

mas $r = \min S$, logo $r \leq a - b(q + 1)$, isto é, $a - bq \leq a - b(q + 1) \Rightarrow q + 1 \leq q$, um absurdo! Portanto, $r < b$.

(Unicidade) Suponhamos que existam inteiros, r_1, r_2, q_1 e q_2 tais que

$$a = bq_1 + r_1 = bq_2 + r_2,$$

com $0 \leq r_1,\ r_2 \leq b - 1$. Assim,

$$0 = bq_1 + r_1 - (bq_2 + r_2) = b(q_1 - q_2) + (r_1 - r_2)\ \Rightarrow\ b(q_1 - q_2) = r_2 - r_1\ \Rightarrow\ b \mid (r_2 - r_1).$$

Com $r_2 - r_1 < r_2 < b$, então, necessariamente, $r_2 - r_1 = 0$, ou melhor, $r_2 = r_1$. Por conseguinte, $q_1 = q_2$. □

3.4 Proposições

Teorema 3.2 (Bachet-Bézout)**.** *Para quaisquer que sejam a e b inteiros, existem inteiros m e n tais que*

$$am + bn = \text{mdc}\,(a, b).$$

O Teorema de Bézout ou Identidade de Bézout é um resultado fundamental na Teoria dos Números e tem grande importância em várias áreas da Matemática. Ele estabelece uma relação entre os números inteiros e o máximo divisor comum deles. Esse teorema é nomeado em homenagem ao matemático francês Étienne Bézout (1730 – 1783), que contribuiu significativamente para os campos da Álgebra, Geometria, Topologia, Criptografia e Teoria dos Códigos. Vale destacar que este teorema estabelece uma relação entre os números inteiros e equações diofantinas, que são equações polinomiais com incógnitas inteiras e, além disso, fornece uma justificativa teórica para os critérios de divisibilidade. Em síntese, ele é uma forte ferramenta para o estudo das propriedades aritméticas dos inteiros.

Proposição 3.1. *Sejam a, b e c inteiros positivos, com* $\text{mdc}\,(a, b) = 1$*. Se $a \mid bc$, então, $a \mid c$.*

Demonstração: Sendo $\text{mdc}\,(a, b) = 1$, então, pelo teorema de Bachet-Bézout, existem inteiros m e n tais que $am + bn = 1$. Multiplicando essa expressão em ambos os membros por c, tem-se, $acm + bcn = c$. Logo, $a \mid c$, pois $a \mid bc$. □

Corolário 3.1. *Se é p primo e $p \mid ab$, então, $p \mid a$ ou $p \mid b$.*

Demonstração: Suponhamos que $p \nmid a$. Logo, $\text{mdc}\,(a, p) = 1$. Daí, a partir da Proposição 3.1, $p \mid b$. □

Corolário 3.2. *Sejam n um número natural e p primo. Se $p \mid a^n$, então $p \mid a$.*

A proposição a seguir é bastante conhecida em textos matemáticos devido à relação entre números primos e coeficientes binomiais de Newton, com implicações significativas em Teoria dos Números, Combinatoria e Criptografia. A prova pode ser encontrada em [1].

Proposição 3.2. *Sejam p um primo e k um número inteiro, com $0 < k < p$. Então*

$$p \mid \binom{p}{k}.$$

Proposição 3.3. *Seja x e y inteiros distintos e p primo. Então, $p(x-y)$ divide $x^p - y^p - (x-y)^p$.*

DEMONSTRAÇÃO: Como $x^p = (x-y+y)^p$, então, por meio do Binômio de Newton obtemos:

$$[(x-y)+y]^p = (x-y)^p + \sum_{i=1}^{p-1}\binom{p}{i}(x-y)^{p-i}y^i + y^p.$$

Consequentemente,

$$x^p = (x-y)^p + \sum_{i=1}^{p-1}\binom{p}{i}(x-y)^{p-i}y^i + y^p \Rightarrow x^p - y^p - (x-y)^p = \sum_{i=1}^{p-1}\binom{p}{i}(x-y)^{p-i}y^i.$$

Visto que $p \geq 2$ e $1 \leq i \leq p-1$, então $(x-y)$ divide $(x-y)^{p-i}$ e, além disso, pela Proposição 3.2, temos $p \mid \binom{p}{i}$.

Portanto,

$$\sum_{i=1}^{p-1}\binom{p}{i}(x-y)^{p-i}y^i$$

é um múltiplo de $p(x-y)$, isso implica que $p(x-y)$ divide $x^p - y^p - (x-y)^p$. □

Um resultado substancial e que será usado mais adiante é dado pela proposição seguinte:

Proposição 3.4. *Se p é primo e divide $x^p - y^p$, então, p^2 divide $x^p - y^p$.*

DEMONSTRAÇÃO: Como $p \mid (x^p - y^p)$, existe um inteiro k tal que

$$x^p - y^p = pk. \tag{3.1}$$

Pela Proposição 3.3,

$$p(x-y) \mid [x^p - y^p - (x-y)^p].$$

Logo, existe um inteiro t tal que $x^p - y^p - (x-y)^p = tp(x-y)$. Assim,

$$(x-y)^p = x^p - y^p - tp(x-y). \tag{3.2}$$

Substituindo (3.1) em (3.2), obtemos:

$$(x-y)^p = pk - tp(x-y) = p(k - t(x-y)).$$

Dessa forma, $p \mid (x-y)^p$, e já que p é primo, então, do Corolário 3.2, $p \mid (x-y)$. Por conseguinte,

1. $(x-y)^p$ é um múltiplo de p^p e $p^p = p^2 \cdot p^{p-2}$ é múltiplo de p^2. Portanto, $(x-y)^p$ é um múltiplo de p^2.
2. $tp(x-y)$ é um múltiplo de p^2.

Logo, por (3.2),

$$x^p - y^p = (x-y)^p + tp(x-y)$$

é multiplo de p^2, ou seja, $p^2 \mid (x^p - y^p)$. □

3.5 Congruências

O conceito de congruências é central para estudar mais substancialmente as propriedades de divisibilidade, indispensáveis para a Aritmética Moderna. A Teoria das Congruências foi introduzida e estudada por Gauss em seu famoso trabalho "*Disquisitiones Arithmeticae*" (*Investigações Aritméticas*), publicado em 1801, quando Gauss tinha apenas 24 anos de idade.

Definição 3.4. (Congruência) Sejam a e b inteiros quaisquer e m um inteiro positivo. Dizemos que a é *congruente* a b módulo m se $m \mid (a-b)$. Denotamos isto por $a \equiv b \pmod{m}$. O número m é chamado o módulo de congruência.

Quando m não divide $a-b$, então dizemos que a não é *congruente* b módulo m ou que a é *incongruente* a b de módulo m. Neste caso, escrevemos $a \not\equiv b \pmod{m}$.

3.5.1 *Propriedades de congruência*

Vamos destacar as principais propriedades básicas das congruências. Sejam a, b, c e d inteiros quaisquer. Então, são válidas as seguintes propriedades:

(1) $a \equiv a \pmod{m}$.

(2) $a \equiv b \pmod{m} \Rightarrow b \equiv a \pmod{m}$.

(3) $a \equiv b \pmod{m}$ e $b \equiv c \pmod{m} \Rightarrow a \equiv c \pmod{m}$.

(4) $a \equiv b \pmod{m} \Rightarrow a \pm c \equiv b \pm c \pmod{m}$.

(5) $a \equiv b \pmod{m} \Rightarrow ac \equiv bc \pmod{m}$.

(6) $a \equiv b \pmod{m}$ e $c \equiv d \pmod{m} \Rightarrow a \pm c \equiv b \pm d \pmod{m}$.

(7) $a \equiv b \pmod{m}$ e $c \equiv d \pmod{m} \Rightarrow ac \equiv bd \pmod{m}$.

(8) $a \equiv b \pmod{m} \Rightarrow a^n \equiv b^n \pmod{m}$ para todo n natural.

(9) Se $a \equiv r \pmod{m}$, $0 \leq r < m$ e $m \geq 2$, então r é o resto da divisão de a por m.

As propriedades (1), (2) e (3) asseguram que a relação de congruência de módulo m, " $\equiv \pmod{m}$", é de equivalência. Este fato é de extrema importância para a Teoria dos Números, porque, além de outras coisas, obtém-se, por meio desta relação, o conjunto quociente de $\mathbb{Z}$ por $\equiv \pmod{m}$, denotado por $\mathbb{Z}_m$. Por meio do algoritmo da divisão, pode-se mostrar que $\mathbb{Z}_m$ tem exatamente m elementos, ou seja,

$$\mathbb{Z}_m = \{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{m-1}\}.$$

Um elemento $\overline{a}$ em $\mathbb{Z}_m$ diz-se a *classe de congruência* de módulo m que contém todos os números inteiros congruentes com a módulo m.

No exemplo que segue, veremos como as propriedades supracitadas são ótimas para a aritmética modular.

Exemplo 3.2. Calcular o resto da divisão de 2^{71} por 15.

Solução: Vamos usar o item (9) das propriedades de congruência, ou seja, devemos determinar um inteiro r tal que

$$2^{71} \equiv r \pmod{15},$$

com $0 \leq r \leq 14$. É importante destacar que

$$2^4 \equiv 1 \pmod{15}.$$

Pelo item (8),

$$(2^4)^{17} \equiv 1^{17} \pmod{15} \Rightarrow 2^{68} \equiv 1 \pmod{15}.$$

Pelo item (5),

$$2^{68} \cdot 2^3 \equiv 1 \cdot 2^3 \pmod{15} \Rightarrow 2^{71} \equiv 8 \pmod{15}.$$

Portanto, o resto é 8.

Neste exemplo seria incoveniente desenvolver a potência 2^{71}, pois possui 22 dígitos, o que tornaria o cálculo enfadonho. No entanto, com o uso das propriedades de congruência, conseguimos encontrar o resultado de forma simples.

4 CAPÍTULO III

"Os ideais que iluminam meu caminho e me deram coragem para enfrentar a vida com alegria são a gentileza, a beleza e a verdade."

Albert Einstein (1879 – 1955)

Neste Capítulo, apresentaremos nossas contribuições ao trabalho. Especificamente, provaremos, sob certas condições, o Último Teorema de Fermat para múltiplos dos primos $p = 3$ e $p = 5$. Apresentaremos, também, a prova desse teorema dada por Germain, na qual descompactamos alguns dados técnicos que, na demonstração original, foram compactados. Por fim, abordaremos um caso para $n \geq 4$, também com restrição.

É importante ressaltar que os casos supracitados serão abordados à luz de resultados básicos da Teoria Elementar dos Números, ou seja, por meio de conceitos estudados no componente MA14 (Aritmética) do Programa PROFMAT.

Agora, chegamos à parte central do trabalho: uma prova restrita da não existência de soluções em inteiros para a equação de Fermat de ordem n,

$$x^n + y^n = z^n, \tag{4.1}$$

em que $n \geq 3$.

A equação em (4.1) generaliza a equação pitagórica,

$$x^2 + y^2 = z^2.$$

Um terno de inteiros (a, b, c) satisfazendo

$$a^2 + b^2 = c^2$$

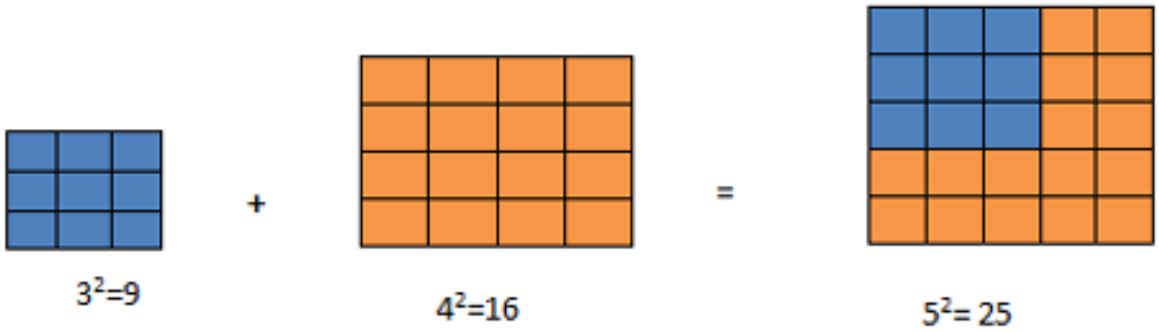
diz-se um *terno pitagórico* ou *tripla pitagórica.* Se a, b e c são inteiros tais que são dois a dois relativamente primos, isto é, $\text{mdc}\,(a, b) = 1$, $\text{mdc}\,(a, c) = 1$ e $\text{mdc}\,(b, c) = 1$, ou equivalentemente, $\text{mdc}\,(a, b, c) = 1$, então, (a, b, c) diz-se um *terno pitagórico primitivo.*

Por exemplo, $(3, 4, 5)$ e $(5, 12, 13)$ são ternos pitagóricos, ambos primitivos, pois

$$3^2 + 4^2 = 5^2 \quad \text{e} \quad 5^2 + 12^2 = 13^2,$$

com $\text{mdc}\,(3,4,5) = \text{mdc}\,(5,12,13) = 1$. Estes dois ternos são os mais familiares.

Figura 9 – Quadrados



Fonte: Bruno, Salvador da Silva (2014, p.23).

Notemos que, se (a,b,c) é um terno pitagórico, (ka,kb,kc) também o é, para qualquer inteiro k. De fato,

$$(ka)^2 + (kb)^2 = k^2(a^2+b^2) = (kc)^2.$$

Isto mostra que a equação pitagórica tem infinitas soluções inteiras. Aliás, todos os ternos pitagóricos primitivos (a,b,c), com $a>0$, $b>0$ e $c>0$, são da forma

$$a = 2mn, \quad b = m^2 - n^2, \quad c = m^2 + n^2,$$

em que $\text{mdc}\,(m,n) = 1$, $m > n > 0$ e $m+n$ ímpar. A demonstração se encontra em [1] na página 453.

Agora, vamos analisar um caso particular da equação de Fermat, com $n = 3$. Neste caso, buscamos uma de rearrumação de ladrilhos é mudarmos a potência de 2 para 3, por exemplo. Neste caso, deve-se encontrar ternos (a,b,c) tais que

$$a^3 + b^3 = c^3.$$

Gerações de matemáticos não conseguiram encontrar números não nulos que se encaixem perfeitamente na equação elevada ao cubo. Na equação original quadrada, o desafio era rearrumar os ladrilhos de dois quadrados para formar um terceiro quadrado maior. Na versão "ao cubo", o desafio é rearrumar dois cubos, feitos de tijolos, para formar um terceiro cubo maior. Aparentemente não importa que tipos de cubos sejam escolhidos como ponto de partida, quando eles são combinados, o resultado ou é um cubo completo com alguns tijolos sobrando, ou um cubo incompleto.

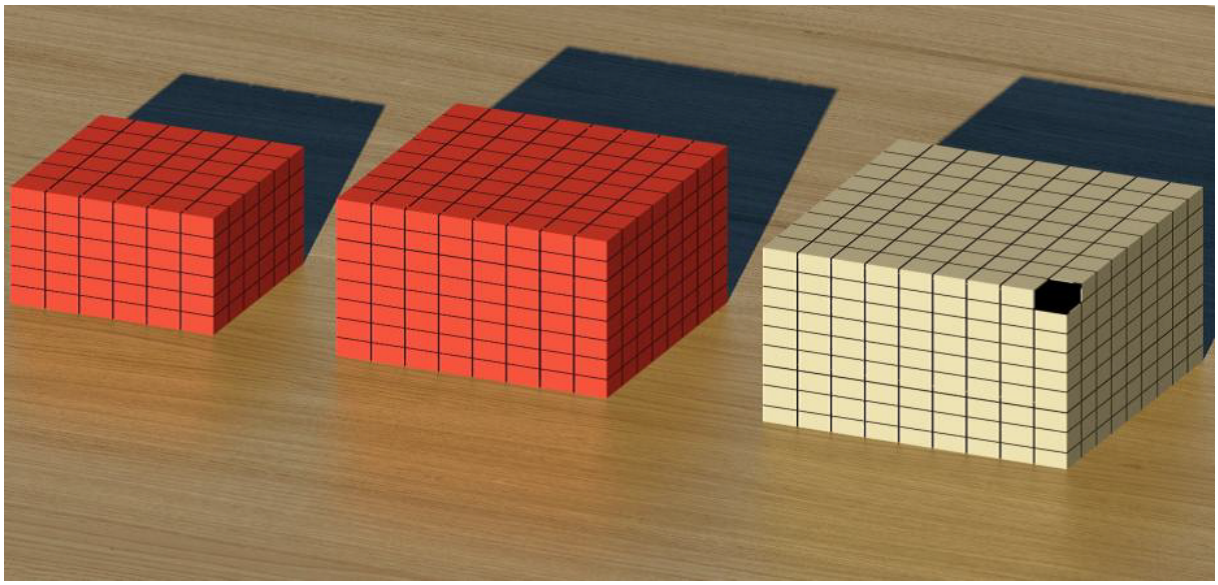
Por exemplo, se começarmos com os cubos de $6^3 = a^3$ e $8^3 = b^3$ e rearrumarmos os tijolos, então, chegaremos perto de construir um cubo, a saber $9^3 = c^3$, faltando um

cubinho para tal feito. Neste caso, temos:

$$6^3 + 8^3 = 9^3 - 1.$$

Geometricamente,

Figura 10 – Cubos



Fonte: Bruno, Salvador da Silva (2014, p.24).

Conforme já abordamos na Introdução, se a potência for mudada de 3 (cubo) para qualquer número maior, ou seja, $n = 4, 5, 6 \ldots$, então a descoberta de uma solução se torna igualmente impossível.

Definição 4.1. Um terno de inteiros (a, b, c) diz-se uma *solução* da equação em 4.1 quando

$$a^n + b^n = c^n.$$

Também chamaremos uma tal solução de um terno de Fermat de ordem n. Em particular, quando $\text{mdc}\,(a, b, c) = 1$, o terno (a, b, c) diz-se *primitivo*.

Suponhamos (a, b, c) uma solução de $x^n + y^n = z^n$ e $d = \text{mdc}\,(a, b, c)$. Assim, existem inteiros a_1, b_1 e c_1 tais que

$$a = da_1, \quad b = db_1 \quad \text{e} \quad c = dc_1.$$

Como, por hipótese, $a^n + b^n = c^n$,

$$a_1^n + b_1^n = \frac{a^n + b^n}{d^n} = \frac{c^n}{d^n} = c_1^n,$$

em que $\text{mdc}(a_1, b_1, c_1) = 1$. Em outras palavras, a_1, b_1 e c_1 formam um terno de Fermat primitivo de ordem n. Portanto, qualquer terno de Fermat pode ser obtido a partir de outro primitivo, multiplicando-o por um inteiro diferente de zero, convenientemente escolhido. Por esta razão, ao analisar as soluções da equação $x^n + y^n = z^n$, é suficiente considerar ternos primitivos. Sendo assim, se (a, b, c) é um terno de Fermat primitivo de ordem n, ou seja, $a^n + b^n = c^n$ e $\text{mdc}(a, b, c) = 1$, então,

$$\text{mdc}(a, b) = \text{mdc}(a, c) = \text{mdc}(b, c) = 1.$$

Dessa forma, não se pode ter os inteiros a, b e c todos pares. Aliás, nem exatamente dois deles, porque, se x é um inteiro par, x^n também o é, para todo inteiro positivo n, bem como a soma de dois inteiros pares é par. Portanto, dois dentre os inteiros do terno são ímpares, e o outro, par. Em resumo:

Proposição 4.1. *Se (a, b, c) é um terno de Fermat primitivo, então, um dos inteiros a e b é par, enquanto o outro é ímpar. Por conseguinte, c é ímpar.*

Por esta razão, podemos, sem perda de generalidade, supor a par e b e c ímpares,

$$a = 2k_1, \quad b = 2k_2 + 1 \quad \text{e} \quad c = 2k_3 + 1,$$

em que k_1, k_2 e k_3 são números inteiros.

É importante observar que, se a equação de Fermat for impossível para um dado expoente n, então, ela também será para todos os múltiplos de n. De fato, se $a^{kn} + b^{kn} = c^{kn}$, em que k é um inteiro positivo, então,

$$(a^k)^n + (b^k)^n = (c^k)^n.$$

Agora, para todo inteiro $n \geq 3$, temos $n = 2^k m$, com $k \geq 0$ e m ímpar. Assim, n é divisível por 4 ou por um primo ímpar. Dessa forma, a fim de provar o último teorema, basta considerar os casos $n = 4$ e $n = p$, com p primo.

4.1 Pequeno teorema de Fermat

O Teorema de Fermat, também conhecido como *Pequeno Teorema de Fermat*, é um resultado fundamental na Teoria dos Números. Ele estabelece uma congruência base importante com aplicações significativas na Aritmética Modular.

Teorema 4.1 (**Pequeno teorema de Fermat**). *Sejam p um número primo e a um*

número inteiro tal que $p \nmid a$. *Então,*

$$a^{p-1} \equiv 1 \pmod{p}.$$

Exemplo 4.1. Encontre o resto da divisão de 3^{100} por 11.

Solução: Pelo Pequeno Teorema de Fermat, temos:

$$3^{11-1} = 3^{10} \equiv 1 \pmod{11}.$$

Assim,

$$3^{100} = (3^{10})^{10} \equiv 1^{10} \equiv 1 \pmod{11}.$$

Portanto, o resto é 1.

O próximo teorema é conhecido como o *Teorema da Decomposição Prima em Potências*, um marco teórico essencial em Teoria dos Números que estabelece que números inteiros primos entre si admitem representação como potências de números primos.

Teorema 4.2. *Se* a *e* b *forem primos entre si e* $ab = c^n$, *então existem inteiros* a_1 *e* b_1 *tais que* $a = a_1^n$ *e* $b = b_1^n$.

No que segue, apresentaremos a prova condicionada, dada por Germain, para o Último Teorema de Fermat.

4.2 Teorema de Germain

Teorema 4.3 (**Germain**). *Se* p *e* $p_1 = 2p + 1$ *são primos, com* $p > 2$, *então não existe terno de Fermat primitvo* (a, b, c) *de ordem* p, *em que* p *não divide nenhum dos inteiros* a, b *e* c.

Demonstração: Suponhamos, por contradição, que (a, b, c) seja um terno de Fermat de ordem p, em que p não divide nenhum dos inteiros do terno. Assim, por definição,

$$a^p + b^p = c^p,$$

com $\text{mdc}\,(a, b, c) = 1$. Em primeiro lugar, notemos que:

$$p_1 \mid abc. \tag{4.2}$$

Com efeito, senão, neste caso, $\text{mdc}\,(a, p_1) = 1$, de maneira que, pelo Pequeno Teorema de Fermat, $a^{p_1-1} \equiv 1 \pmod{p_1} \Rightarrow a^{2p} \equiv 1 \pmod{p_1}$, ou melhor,

$$(a^p + 1)(a^p - 1) \equiv 0 \pmod{p_1}.$$

Por isso,

$$a^p \equiv \pm 1 \pmod{p_1}.$$

Da mesma forma, como $\text{mdc}\,(b, p_1) = \text{mdc}\,(c, p_1) = 1$,

$$b^p \equiv \pm 1 \pmod{p_1} \qquad \text{e} \qquad c^p \equiv \pm 1 \pmod{p_1}.$$

Observe que:

$$\pm 1 \pm 1 = \begin{cases} 2, & \text{se } (+1) + (+1). \\ 0, & \text{se } (+1) + (-1) \text{ ou } (-1) + (+1). \\ -2, & \text{se } (-1) + (-1). \end{cases}$$

Portanto, $a^p + b^p \equiv 0,\ -2$ ou $2 \pmod{p_1}$. Em qualquer um dos casos, obtemos uma contradição, já que $c^p = a^p + b^p$ e p é um primo ímpar. Isto prova a afirmação.

Visto que $a^p = c^p - b^p$,

$$a^p = (c - b)(c^{p-1} + c^{p-2}b + \cdots + b^{p-1}). \tag{4.3}$$

Nestas condições,

$$\lambda_1 = c - b \qquad \text{e} \qquad \lambda_2 = c^{p-1} + c^{p-2}b + \cdots + b^{p-1}$$

são primos entre si. De fato, se $\text{mdc}\,(\lambda_1, \lambda_2) > 1$, então, existe um primo q que divide λ_1 e λ_2. Daí,

$$c^{p-1} + c^{p-2}b + \cdots + b^{p-1} \equiv 0 \pmod{q}, \tag{4.4}$$

e como $c \equiv b \pmod{q}$, segue, de (4.4), que

$$b^{p-1} + b^{p-2}b + \cdots + b^{p-1} \equiv 0 \pmod{q} \Rightarrow \underbrace{b^{p-1} + b^{p-1} + \cdots + b^{p-1}}_{p \text{ termos}} \equiv 0 \pmod{q},$$

ou melhor, $pb^{p-1} \equiv 0 \pmod{q}$. Com isto, $p \neq q$, senão, de (4.3), $p \mid a^p$, isto é, $p \mid a$, uma contradição. Portanto, $p \neq q$ e, assim, $\text{mdc}\,(p, q) = 1$. Daí,

$$pb^{p-1} \equiv 0 \pmod{q} \;\Rightarrow\; q \mid b^{p-1} \;\Rightarrow\; q \mid b,$$

pois q é primo. Agora, como $c \equiv b \pmod{q}$, temos $q \mid c$. Por isso, por (4.3), $q \mid a$. Por conseguinte, $\text{mdc}(a,b,c) \geq q > 1$, uma contradição, pois, por hipótese, $\text{mdc}(a,b,c) = 1$.

Portanto, conforme o Teorema 4.2, existem inteiros α_1 e k_1 tais que

$$c - b = \alpha_1^p \qquad \text{e} \qquad c^{p-1} + c^{p-2}b + \cdots + b^{p-1} = k_1^p. \tag{4.5}$$

Da mesma forma, sendo $b^p = c^p - a^p$, pode-se mostrar que existem inteiros α_2 e k_2 para os quais

$$c - a = \alpha_2^p \qquad \text{e} \qquad c^{p-1} + c^{p-2}a + \cdots + a^{p-1} = k_2^p. \tag{4.6}$$

Sendo $c^p = a^p + b^p$ e p ímpar, então

$$a^p + b^p = (a+b) \times \sum_{i=0}^{p-1} (a)^{p-1-i}(-b)^i = (a+b) \times (a^{p-1} - a^{p-2}b + \cdots + b^{p-1}),$$

também existem inteiros α_3 e k_3, com

$$a + b = \alpha_3^p \qquad \text{e} \qquad a^{p-1} - a^{p-2}b + \cdots + b^{p-1} = k_3^p. \tag{4.7}$$

Por, (4.5), (4.6) e (4.7), temos:

$$2a = \alpha_1^p + \alpha_3^p - \alpha_2^p, \quad 2b = \alpha_3^p + \alpha_2^p - \alpha_1^p \quad \text{e} \quad 2c = \alpha_1^p + \alpha_2^p + \alpha_3^p.$$

Por (4.2), $p_1 \mid abc$. Assim, como p_1 é primo, podemos, sem perda de generalidade, supor $p_1 \mid c$, $2c = \alpha_1^p + \alpha_2^p + \alpha_3^p$ e, então,

$$p_1 \mid \alpha_1^p + \alpha_2^p + \alpha_3^p.$$

Analogamente, mostra-se que

$$p_1 \mid \alpha_1\alpha_2\alpha_3.$$

De fato, se $p_1 \nmid \alpha_1\alpha_2\alpha_3$, então $p_1 \nmid \alpha_1$, $p_1 \nmid \alpha_2$ e $p_1 \nmid \alpha_3$. Segue pelo Pequeno Teorema de Fermat que

$$\alpha_1^p \equiv \pm 1 \pmod{p_1}, \quad \alpha_2^p \equiv \pm 1 \pmod{p_1} \quad \text{e} \quad \alpha_3^p \equiv \pm 1 \pmod{p_1}.$$

Daí,

$$\pm 1 \pm 1 \pm 1 = \begin{cases} +3, & \text{se } (+1)+(+1)+(+1). \\ +1, & \text{se } (+1)+(+1)+(-1) \text{ ou } (+1)+(-1)+(+1) \text{ ou } (-1)+(+1)+(+1). \\ -1, & \text{se } (+1)+(-1)+(-1) \text{ ou } (-1)+(+1)+(-1) \text{ ou } (-1)+(-1)+(+1). \\ -3, & \text{se } (-1)+(-1)+(-1). \end{cases}$$

Portanto, $\alpha_1^p + \alpha_2^p + \alpha_3^p \equiv \pm 1$ ou $\pm 3 \pmod{p_1}$, um absurdo! Logo, $p_1 \mid \alpha_1\alpha_2\alpha_3$.

Analisemos os seguintes casos:

CASO 1: Se $p_1 \mid \alpha_1$, então, $p_1 \mid \alpha_1^p = c - b$ e, por isso, $p_1 \mid b$, já que $p_1 \mid c$. Assim, como $a^p = c^p - b^p$, temos $p_1 \mid a$. Por conseguinte,

$$\text{mdc}\,(a, b, c) \geq p_1,$$

uma contradição.

CASO 2: Se $p_1 \mid \alpha_2$, então, $p_1 \mid \alpha_2^p = c - a$. Daí, $p_1 \mid \alpha_2^p$ e, com isto, $p_1 \mid a$. Portanto, $p_1 \mid c$, ou seja,

$$\text{mdc}\,(a, b, c) \geq p_1,$$

uma impossibilidade.

CASO 3: Está suposição, $p_1 \mid \alpha_3$, requer um pouco mais de detalhes. Como $p_1 \mid c$, segue, de (4.5), que

$$k_1^p \equiv b^{p-1} \pmod{p_1}. \tag{4.8}$$

Como $p_1 \mid \alpha_3$, então $p_1 \mid \alpha_3^p$. Segue de (4.7), que $a \equiv -b \pmod{p_1}$ e, por isso,

$$k_3^p \equiv pb^{p-1} \pmod{p_1}. \tag{4.9}$$

Note que $p_1 \nmid k_3^p$. Pois, caso contrário, se $p_1 \mid k_3^p$, segue de 4.9 e do $\text{mdc}\,(p_1, p) = 1$, que

$$p_1 \mid pb^{p-1} \Rightarrow p_1 \mid b^{p-1} \Rightarrow p_1 \mid b.$$

De $a \equiv -b \pmod{p_1}$ e $p_1 \mid b$, temos $p_1 \mid a$. Por conseguinte, $\text{mdc}\,(a, b, c) \geq p_1 > 1$, o que é impossível.

Também, $p_1 \nmid k_1^p$. Pois, caso contrário, de (4.8), $p_1 \mid b^{p-1} \Rightarrow p_1 \mid b$, de forma análoga

anterior, o $\text{mdc}\,(a,b,c) \geq p_1 > 1$, um absurdo.

Nestas condições, como $p_1 \nmid k_3^p$ e $p_1 \nmid k_1^p$, então $p_1 \nmid k_3$ e $p_1 \nmid k_1$. Pelo Pequeno Teorema de Fermat:

$$k_3^{p_1-1} \equiv 1 \pmod{p_1} \quad \text{e} \quad k_1^{p_1-1} \equiv 1 \pmod{p_1}.$$

Ou seja,

$$k_3^p \equiv \pm 1 \pmod{p_1} \quad \text{e} \quad k_1^p \equiv \pm 1 \pmod{p_1}.$$

Assim, de (4.8), $b^{p-1} \equiv \pm 1 \pmod{p_1}$ e, consequentemente, de (4.9),

$$\pm 1 \equiv k_3^p \equiv pb^{p-1} \equiv \pm p \pmod{p_1} \Rightarrow \mp p \pm 1 \equiv 0 \pmod{p_1} \Rightarrow p_1 = (2p+1) \mid (\mp p \pm 1),$$ é impossível.

Pois, $2p+1 > \mp p \pm 1 = p+1, p-1, -p+1$ ou $-p-1$, com p um primo ímpar. Isto finalmente conclui a prova. □

Os primos p e $2p+1$ são chamados *primos de Germain*. Conjecturou-se que esses primos fossem infinitos, no entanto, até o presente momento, não se tem nenhuma prova disto.

O resultado de Germain foi estendido por Legendre e, após, por Peter Dénes (1930 – 2019), em 1951 e, mais recentemente, por George Fee (1929 – 2011) e André Grandville (1932 – 2019), em 1991.

4.3 Teorema de Sophie – Legendre

Teorema 4.4 (**Teorema de Sophie – Legendre**). *Sejam p e q primos ímpares, tais que:*

(i) Toda solução da congruência $x^p + y^p + z^p \equiv 0 \pmod{q}$ satisfaz $q \mid xyz$.

(ii) $w^p \equiv p \pmod{q}$ não possui solução em w.

Então, não existem inteiros x, y e z, com $\text{mdc}\,(x,y,z) = 1$ e $p \nmid xyz$, tais que $x^p + y^p + z^p = 0$.

A demonstração desse teorema é bastante semelhante com à do teorema de Germain. Como ilustrado, consideremos os primos $p = 5$, $q = 11$ e w um inteiro. Assim,

$$w^5 \equiv 0, 1 \text{ ou } -1 \pmod{11}.$$

Consequentemente, para que $x^5 + y^5 + z^5 \equiv 0 \pmod{11}$, devemos ter x, y ou z múltiplo de 11. Logo, o caso (i) é satisfeito. Claramente, $w^5 \equiv 5 \pmod{11}$ não possui solução. Isso mostrar que o Último Teorema de Fermat é verdadeiro para o caso $n = 5$, desde que $5 \nmid xyz$ e que $\text{mdc}(x, y, z) = 1$.

Passamos a apresentar, a seguir, demonstrações condicionadas para o Último Teorema de Fermat, especificamente para os casos $n = 3$, $n = 4$ e $n = 5$.

4.4 O último teorema de Fermat: caso $n = 3$ com restrições

Teorema 4.5 (**Fermat − Caso** $n = 3$)**.** *Não existe um terno de Fermat* (x, y, z) *de ordem* 3*, em que* $3 \nmid xyz$.

Demonstração: Suponhamos que exista um terno de Fermat (x, y, z) de ordem 3, com $3 \nmid xyz$. Dessa forma,

$$x^3 + y^3 = z^3, \text{ em que } 3 \nmid xyz. \tag{4.10}$$

Assim, podemos reescrever esta equação da seguinte maneira:

$$x^3 + y^3 = (x + y)^3 - 3(x + y)xy = z^3. \tag{4.11}$$

Considerando $a = x + y$ e $b = xy$ e substituindo em (4.11), temos:

$$a^3 - 3ab = z^3. \tag{4.12}$$

Daí,

$$a^3 - z^3 = 3ab \Rightarrow 3 \mid (a^3 - z^3).$$

Como $3 \mid (a^3 - z^3)$ segue, da Proposição 3.4, que

$$3^2 \mid (a^3 - z^3) \Rightarrow 3^2 \mid 3ab \Rightarrow 3 \mid ab.$$

Assim, pelo Corolário 3.1, $3 \mid a$ ou $3 \mid b$. Analisemos estes casos.

Se $3 \mid a$, então, de (4.12), $3 \mid z^3$ e, assim, $3 \mid z$, uma contradição. Daí, pela Proposição 3.1, temos $3 \mid b$, e como $b = xy$, então, $3 \mid xyz$, um absurdo. isto finaliza a prova. □

Corolário 4.1. *Não existe um terno de Fermat* (x, y, z) *tal que:*

$$x^{3k} + y^{3k} = z^{3k},$$

para todo k *em* $\mathbb{N}$, *com* $3 \nmid xyz$.

Demonstração: De fato, como $x^{3k} + y^{3k} = z^{3k}$, então, $(x^k)^3 + (y^k)^3 = (z^k)^3$. Logo, (x^k, y^k, z^k) é uma solução para $x^3 + y^3 = z^3$, o que, pelo Teorema 4.5, é impossível. □

4.5 O último teorema de Fermat: caso $n = 5$ com restrições

Teorema 4.6 (**Fermat − Caso** $n = 5$)**.** *Não existe um terno de Fermat* (x, y, z) *de ordem 5, em que* $5 \nmid xyz$.

Demonstração: Suponhamos que existe um terno de Fermat (x, y, z) com

$$x^5 + y^5 = z^5,$$

em que $5 \nmid xyz$. Desenvolvendo $(x + y)^5$, obtemos:

$$(x + y)^5 = x^5 + 5x^4y + 10x^3y^2 + 10x^2y^3 + 5xy^4 + y^5,$$

ou melhor,

$$(x + y)^5 - (5x^4y + 10x^3y^2 + 10x^2y^3 + 5xy^4) = x^5 + y^5.$$

Agora,

$5x^4y + 10x^3y^2 + 10x^2y^3 + 5xy^4 = 5xy(x^3 + 2x^2y + 2xy^2 + y^3) =$

$= 5xy[(x + y)^3 - x^2y - xy^2] = 5xy[(x + y)^3 - xy(x + y)] =$

$= 5xy[(x + y)^3 - 5(xy)^2(x + y)].$

Portanto,

$$(x + y)^5 - 5xy(x + y)^3 + 5(x + y)(xy)^2 = x^5 + y^5.$$

Substituindo $x + y = a$, $b = xy$ e $x^5 + y^5 = z^5$, nesta última expressão, temos:

$$a^5 - 5ba^3 + 5ab^2 = z^5. \tag{4.13}$$

Daí,

$$a^5 - 5ba^3 + 5ab^2 = z^5 \;\Rightarrow\; a^5 - z^5 = 5(ba^3 - ab^2) \;\Rightarrow\; 5 \mid (a^5 - z^5).$$

Da Proposição 3.4, temos $5^2 \mid (a^5 - z^5)$. Assim,

$$5^2 \mid 5(ba^3 - ab^2) \;\Rightarrow\; 5 \mid (ba^3 - ab^2) \;\Rightarrow\; 5 \mid ab(a^2 - b).$$

Do Corolário 3.1, $5 \mid a$ ou $5 \mid b$ ou $5 \mid (a^2 - b)$. Analisemos estes casos:

(i) Se $5 \mid a$, então, de (4.13), temos $5 \mid z^5$ e, pelo Corolário 3.2, $5 \mid z$, o que é impossível, segundo à hipótese.

(ii) Se $5 \mid b$, então, como $b = xy$, temos $5 \mid xyz$, uma impossibilidade.

(iii) Finalmente, se $5 \mid (a^2 - b)$, então, já que $a = x + y$ e $b = xy$,

$$a^2 - b = x^2 + y^2 + xy. \tag{4.14}$$

Por hipótese, $5 \nmid x$ e $5 \nmid y$. Os possíveis restos de x na divisão por 5 são:
$x \equiv 1, 2, 3$ ou $4 \pmod 5$. Das propriedades de congruência:

$$x^2 \equiv 1^2, 2^2, 3^2 \text{ ou } 4^2 \pmod 5.$$

Logo,

$$x^2 \equiv 1 \text{ ou } 4 \pmod 5.$$

No caso $y \equiv x \pmod 5$, temos, por (4.14),

$$a^2 - b \equiv x^2 + x^2 + x^2 \equiv 3x^2 \equiv 2 \text{ ou } 3 \pmod 5 \;\Rightarrow\; 5 \nmid (a^2 - b).$$

Agora, notemos que, tanto o par (x, y) quanto o par (y, x) representam a mesma solução para (4.14). Dessa forma, podemos construir uma tabela de congruência de $\pmod 5$ em que o par $(x, y) = (y, x)$; $x \not\equiv y \pmod 5$ e $5 \nmid a = (x + y)$. Daí,

Tabela 4.1 – **Congruência Módulo 5**

(x, y)	$x^2 + y^2$	xy	$a^2 - b$
$(1, 2)$	0	2	2
$(1, 3)$	0	3	3
$(2, 4)$	0	3	3
$(3, 4)$	0	2	2

Elaborado pelo autor, 2025.

De acordo esta tabela, verificamos que $5 \nmid (a^2 - b)$. Isto prova o resultado. □

Corolário 4.2. *Não existe um terno de Fermat de ordem $5k$, em que $5 \nmid xyz$.*

Demonstração: Suponha que (x, y, z) seja um terno de Fermat de ordem $5k$. Assim,

$$x^{5k} + y^{5k} = z^{5k},$$

em que $5 \nmid xyz$ para todo $k \in \mathbb{N}$. Logo, (x^k, y^k, z^k) é uma solução para $x^5 + y^5 = z^5$, porém, conforme o Teorema 4.6, é impossível. □

4.6 O último teorema de Fermat: caso n par com restrições

Teorema 4.7 (**Fermat– Caso n par com restrição**)**.** *Seja $n \geq 4$ um inteiro par. Então, não existe nenhum terno de Fermat (x, y, z) de ordem n, em que x, y e z são positivos e*

$$\operatorname{mdc}(x + y + z, x + z) = 1 \iff \operatorname{mdc}(x + z, y) = 1,$$

sendo x par e y e z ímpares.

Demonstração: Sejam a e b números inteiros. Então, para cada $n \in \mathbb{N}$,

$$a^n - b^n = (a - b) \sum_{i=0}^{n-1} a^{n+1-i}\, b^i,$$

então,

$$(a - b) \mid (a^n - b^n). \tag{4.15}$$

Uma vez que

$$a^{2n} - b^{2n} = (a^2)^n - (b^2)^n \quad \text{e} \quad (a^2 - b^2) = (a + b)(a - b),$$

então, de (4.15),

$$(a+b) \mid (a^{2n} - b^{2n}). \tag{4.16}$$

Suponhamos que (x, y, z) seja um terno de Fermat primitivo de ordem n, sendo x, y e z todos positivos, com x par e y e z ímpares, dessa forma,

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

De (4.15), considerando $a = x + y + z$ e $b = y$, temos $(x + z)$ divide $(x + y + z)^n - y^n$. Por esta razão,

$$(x + y + z)^n - y^n = (x + z)k,$$

para algum inteiro k. Dessa forma, sendo $y^n = z^n - x^n$, temos

$$(x + y + z)^n = (x + z)k + z^n - x^n. \tag{4.17}$$

Agora, como n é par, segue, de (4.16), que $(z + x)$ divide $(z^n - x^n)$. Daí,

$$z^n - x^n = (z + x)t,$$

para algum inteiro t. Daí, por (4.17),

$$(x + y + z)^n = (x + z)s,$$

em que $s = k + t \in \mathbb{Z}$. Portanto,

$$(x + z) \mid (x + y + z)^n. \tag{4.18}$$

Sendo x e z são inteiros positivos, temos $x + z > 1$. Por outro lado, pelo Teorema Fundamental da Aritmética, existe um q primo tal que $q \mid (x + z)$. Por (4.18), $q \mid (x + y + z)^n$ e do Corolário 3.2, $q \mid (x + y + z)$. Consequentemente,

$$q \mid \operatorname{mdc}((x + y + z), x + z).$$

visto que, por hipótese, $\operatorname{mdc}(x + y + z, x + z) = 1$, então $q = 1$, uma contradição, pois q é

primo. Isto prova o resultado. □

Corolário 4.3. *Não existe um terno de Fermat* (x, y, z) *tal que*

$$x^{4k} + y^{4k} = z^{4k},$$

para todo inteiro positivo k*, em que*

$$\text{mdc}\,(x + y + z, x + z) = 1 \iff \text{mdc}\,(x + z, y) = 1,$$

sendo x *par e* y *e* z *ímpares.*

Demonstração: De fato, pois $x^{4k} + y^{4k} = z^{4k} \Rightarrow (x^k)^4 + (y^k)^4 = (z^k)^4$. Logo,

(x^k, y^k, z^k) é uma solução para $x^4 + y^4 = z^4$, em que $\text{mdc}\,(x + z, y) = 1$. O que, conforme o Teorema 4.7, é impossível. □

5 CONCLUSÃO

Poucos resultados na Teoria dos Números aguçaram tanto a curiosidade de teóricos dos números quanto o Último Teorema de Fermat, que é certamente um dos resultados que mais inspiraram o desenvolvimento de novas ideias na aritmética; seu enunciado, fácil de ser entendido até por leigos, torna-o um resultado especial, não apenas pelo resultado em si, mas pelo desafio o que ele impôs a notáveis matemáticos por mais de 350 anos. Neste trabalho, à luz de conceitos básicos da Teoria Elementar dos Números, provamos, sob determinadas restrições, a não existência de solução para a equação de Fermat $x^n + y^n = z^n$, para alguns valores específicos de n.

Por fim, espero que este trabalho possa contribuir como estímulo e fonte de referência aos possíveis leitores interessados no campo da Teoria dos Números, inspirando novas pesquisas e descobertas que possam avançar ainda mais o conhecimento nessa área fascinante.

REFERÊNCIAS

[1] VIEIRA, V. L. **Um Curso Básico em Teoria dos Números** (2ª edição). Textuniversitários, Editora Livraria da Física, São Paulo, 2020.

[2] SANTOS, J.P.O. **Introdução à Teoria dos Números** (2ª impressão). Associação Instituto Nacional de Matemática Pura e Aplicada, 198pp. Coleção Matemática Universitária, Rio de Janeiro, 2003.

[3] SAMPAIO, J.C.; CAETANO, P.A. **Introdução à Teoria dos Números – um curso breve**. Editora Edufscar, coleção Matemática, São Paulo, 2014.

[4] MARTINEZ, F. B.; MOREIRA, C.G.; SALDANHA, N.; TENGAN, E. **Teoria dos Números: um passeio com primos e outros números familiares pelo mundo inteiro**. Instituto de Matemática Pura e Aplicada, Projeto Euclides, Rio de Janeiro, 2015.

[5] SINGH, S. **O Último Teorema de Fermat: a história do enigma que confundiu as maiores mentes do mundo durante 358 anos**. Record, Rio de Janeiro, 2011.

[6] RIBENBOIM, P. **Fermat's Last Theorem for Amateurs**. Springer Verlag, New York, 2000.

[7] NETO, A.C.M. **Tópicos de Matemática Elementar –Volume 1: Introdução à Análise**. SBM, Rio de Janeiro, 2012.

[8] BRUNO, S.S. **O Último Teorema de Fermat para** $n = 3$. Trabalho de Conclusão de Pós-graduação em Matemática PROFMAT para a obtenção do grau de MESTRE em Matemática. Universidade Federal do Estado do Rio de Janeiro (UNIRIO), 2014. Disponível em: `https://sca.profmat-sbm.org.br/profmat_tcc.php?id1=1344&id2=1396`. Acesso em: 15 Nov. 2023.

[9] SILVA, F.C. **O Último Teorema de Fermat: Casos Especiais**. Juiz de Fora, 2018. Trabalho de Conclusão de Curso (Bacharelado em Matemática). Departamento de Matemática, Universidade Federal de Juiz de Fora (UFJF). Disponível em: `https://www.professores.uff.br/rsalomao/wp-content/uploads/sites/93/2017/08/danielcunha.pdf`. Acesso em: 01 Nov. 2023.

[10] SILVA, D. S. **O Último Teorema de Fermat**. Rio de Janeiro, 2010. Trabalho de Conclusão de Curso. Instituto de Matemática e Estatística da Universidade do Estado do Rio de Janeiro (UERJ). Disponível em: https://www.professores.uff.br/rsalomao/wp-content/uploads/sites/93/2017/08/danielcunha.pdf. Acesso em: 05 Dez. 2023.

[11] RIZE, A.C. **Números Primos**. Belo Horizonte, 2014. Requisito parcial à obtenção do título de especialização Latu Senso para professores com ênfase em cálculo. Departamento de Matemática do Instituto de Ciências Exatas (ICEX), Universidade Federal de Minas Gerais Instituto de Ciências Exatas(UFMJ). Disponível em: https://repositorio.ufmg.br/bitstream/1843/EABA-9REL7B/1/monografia_ary.pdf. Acesso em: 01 Nov. 2023.

[12] CARDOSO, S. O. **O Último Teorema de Fermat para** $n = 5$. Rio de Janeiro, 2020.Trabalho de Conclusão de Pós-graduação em Matemática PROFMAT para a obtenção do grau de MESTRE em Matemática. Universidade Federal do Estado do Rio de Janeiro Centro de Ciências Exatas e Tecnologia (UNIRIO). Disponível em: https://sca.profmat-sbm.org.br/profmat_tcc.php?id1=5461&id2=170480121. Acesso em: 05 Jan. 2024.

[13] CASTRO, F.C. **O Estudo da Proficuidade dos Números Primos de Sophie Germain**. Trabalho de Conclusão de Pós-graduação em Matemática PROFMAT para a obtenção do grau de MESTRE em Matemática. do Centro de Ciências e Tecnologia da Universidade Estadual do Ceará, (UFC), 2023. Disponível em: https://sca.profmat-sbm.org.br/profmat_tcc.php?id1=7234&id2=171057180. Acesso em: 10 Jan. 2024.