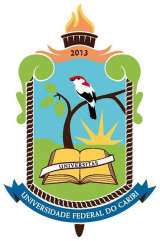

UNIVERSIDADE FEDERAL DO CARIRI
CENTRO DE CIÊNCIAS E TECNOLOGIA
PROGRAMA DE PÓS-GRADUAÇÃO EM MATEMÁTICA
EM REDE NACIONAL

JOÃO PAULO DE ARAÚJO SOUZA

ALGUNS CASOS DO ÚLTIMO TEOREMA DE FERMAT

JUAZEIRO DO NORTE
2019

JOÃO PAULO DE ARAÚJO SOUZA

ALGUNS CASOS DO ÚLTIMO TEOREMA DE FERMAT

Dissertação de Mestrado apresentada ao Programa de Pós-Graduação em Matemática em Rede Nacional, do Centro de Ciências e Tecnologia da Universidade Federal do Cariri, como requisito parcial para obtenção do Título de Mestre em Matemática. Área de concentração: Ensino de Matemática.

Orientador:
Prof. Dr. Valdinês Leite de Sousa Júnior.

JUAZEIRO DO NORTE
2019

Dados Internacionais de Catalogação na Publicação
Universidade Federal do Cariri
Sistema de Bibliotecas

S713a Souza, João Paulo de Araújo.
Alguns casos do último teorema de Fermat / João Paulo de Araújo Souza. – 2019.
52 f.: il.; color.; enc. ; 30 cm.
(Inclui bibliografia p. 50-52).

Dissertação (Mestrado) – Universidade Federal do Cariri, Centro de Ciências e Tecnologia –Programa de Pós-graduação em Matemática em Rede Nacional, Juazeiro do Norte, 2019.

Orientação: Prof. Dr. Valdinês Leite de Sousa Júnior.

1. Aritmética. 2. Equação fermatiana. 3. Sophie Germain. 4. Pitágoras. I. Título.

CDD 516.3

Bibliotecário: João Bosco Dumont do Nascimento – CRB 3/1355

MINISTÉRIO DA EDUCAÇÃO
UNIVERSIDADE FEDERAL DO CARIRI
CENTRO DE CIÊNCIAS E TECNOLOGIA
MESTRADO PROFISSIONAL EM MATEMÁTICA EM REDE NACIONAL - PROFMAT

Alguns Casos do Último Teorema de Fermat

João Paulo de Araújo Souza

Dissertação de Mestrado apresentada ao Programa de Pós-Graduação em Matemática em Rede Nacional – PROFMAT do Centro de Ciências e Tecnologia da Universidade Federal do Cariri, como requisito parcial para obtenção do Título de Mestre em Matemática. Área de concentração: Ensino de Matemática

Aprovada em 18 de março de 2019.

Banca Examinadora

Valdinês Leite de Sousa Júnior

Prof. Dr. Valdinês Leite de Sousa Júnior
Orientador

Valdir Ferreira de Paula Junior

Prof. Dr. Valdir Ferreira de Paula Junior
UFCA

Prof. Dr. Steve da Silva Vicentim
UFCA

Iza, a ti dedico mais essa canção.

AGRADECIMENTOS

À minha mãe, Cicera de Araújo Souza, por ter sido mãe e pai ao mesmo tempo e por ter feito tudo o que fosse necessário para ver qualquer um de seus filhos felizes.

Ao meu pai, José Santana de Souza, por sempre ter trabalhado mais do que qualquer pessoa conseguiria e por ser o pai mais amável do mundo.

Aos meus irmãos, por sempre cuidarem de mim e por todo o incentivo para continuar estudando.

À minha querida companheira, Iza Silva Campos, por sempre estar ao meu lado independente da situação.

Ao meu orientador, Valdinês Leite de Sousa Júnior, por ser essa pessoa tão especial e atenciosa.

A todos os colegas de curso, por toda paciência no decorrer do curso. Em especial, a Renan Fernandes de Moraes por todo o companheirismo.

A todos os professores da UFCA que participam direta ou indiretamente do PROFMAT.

A todos os professores do curso Licenciatura em Matemática do IFCE - Juazeiro do Norte, por tornarem possível meu acesso a esse Mestrado. Em especial, aos professores Mário de Assis Oliveira, Zelalber Gondim Guimarães, Leandro Barbosa Paz e Regilânia da Silva Lucena por toda atenção e incentivo.

"Dizem que o tempo resolve tudo.
A questão é: Quanto tempo?"
(Alice no País das Maravilhas)

RESUMO

A Matemática é uma das ciências mais exatas, mas que vez ou outra se torna uma caixinha de surpresas. Uma dessas situações é a quantidade de novas teorias que foram necessárias para responder um problema conhecido na literatura como o Último Teorema de Fermat, que aparentemente é tão simples por ser composto apenas de operações básicas − como soma e multiplicação − e desafiou grandes matemáticos durante 358 anos. Neste trabalho foram expostos, com a intenção de ser uma introdução, resultados que provam a validade para alguns casos especiais/particulares, como por exemplo quando n é um múltiplo de 4. Historicamente, a importância de resolver esse problema não é somente o resultado em si, mas sim o ganho substancial de propriedades e teorias que foi obtido por matemáticos na busca de tal solução. Ele está escrito, em sua maior parte, sob propriedades básicas da Matemática para que alunos interessados pelo assunto possam entendê-lo, com um pouco mais de estudo do que aquele referente ao Ensino Médio Regular. Assim como Andrew Wiles, com apenas dez anos, um dia encontrou em uma biblioteca um livro de enigmas matemáticos em que um deles se tornou o seu objetivo de vida. Esperamos que esse trabalho inspire jovens estudantes a terem esse tipo problema como um bom passatempo.

Palavras-chave: Aritmética. Equação fermatiana. Sophie Germain. Pitágoras.

ABSTRACT

Mathematics is one of the most exact sciences, but that time and again it becomes a box of surprises. One such situation is the amount of new theories that were needed to answer a problem known in the literature as Fermat's Last Theorem, which is apparently so simple because it is composed only of basic operations - such as sum and multiplication - and challenged great mathematicians for 358 years. In this work, results that prove the validity of some special cases, such as when n is a multiple of 4, have been presented with the intention of being an introduction. Historically, the importance of solving this problem is not only the result itself, but the substantial gain of properties and theories that was obtained by mathematicians in the search for such a solution. It is written, for the most part, under the basic properties of Mathematics so that students interested in the subject can understand it, with a little more study than the one referring to Regular High School. Like Andrew Wiles, at age ten, one day he found in a library a book of mathematical puzzles in which one of them became his life goal. We hope this work will inspire young students to have this kind of problem as a good hobby.

Keywords: Arithmetic. Fermat's equation. Sophie Germain. Pythagoras.

LISTA DE FIGURAS

SUMÁRIO

1 INTRODUÇÃO

Teorema 1.0.1 (Fermat) *A equação*

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

não possui solução sempre que $x, y, z \in \mathbb{Z}^*$ *e* $n \in \mathbb{N}_{>2}$.

Por mais desenvolvida que seja a Matemática usada atualmente, ainda não podemos julgar um simples problema matemático como fácil ou difícil, pois uma equação tão ingênua quanto $x^n + y^n = z^n$ composta, em sua essência, apenas por somas e multiplicações gerou um dos teoremas mais conhecidos no mundo, que é o Último Teorema de Fermat, no qual a simplicidade é inversamente proporcional a facilidade de se encontrar uma prova correta. Apesar do matemático francês Pierre de Fermat ter deixado um rascunho na margem do livro II da coletânea Aritmética de Diofanto dizendo ter encontrado uma demonstração maravilhosa, somente foi conhecido uma prova completa no ano 1995 depois de longos 358 anos após sua formulação.

Pierre de Fermat, apesar de não ser matemático profissional, contribuiu com diversas propriedades que ajudaram na criação de alguns ramos da matemática e por sua importância ficou conhecido como, Príncipe dos Amadores. Veja o que Simon Singh disse sobre as descobertas de Fermat em [14]:

> "O desenvolvimento do cálculo e da teoria da probabilidade deveria ser mais do que suficiente para dar a Fermat um lugar na galeria de honra da matemática. Mas suas maiores realizações foram em outro campo dessa ciência. Embora o cálculo tenha sido usado para enviar foguetes para a Lua e a teoria da probabilidade seja usada pelas companhias de seguros na avaliação dos riscos, a grande paixão de Fermat era por um assunto geralmente inútil – a teoria dos números. Fermat era obcecado em entender as propriedades e relações entre os números. Esta é a forma mais pura e antiga de matemática, e Fermat estava ampliando um conhecimento que lhe fora legado por Pitágoras."

Quando Simon diz "geralmente inútil" não se deve confundir com "totalmente inútil", pois para onde você olhar verá algum número e esse é o objeto de estudo da Teoria dos Números. Como aplicação, podemos citar a Criptografia que é usada na internet e pelos bancos para guardar dados de forma segura.

Nesse trabalho, iremos discutir sobre pontos interessantes pertinentes ao Último Teorema de Fermat. No primeiro capítulo, daremos uma breve nota histórica sobre o problema e falaremos sobre alguns dos matemáticos que contribuíram na busca por uma solução para o problema. Consequentemente, nos ajudará a entender melhor o contexto das demonstrações que aparecerão no segundo capítulo, e nesse provaremos a validade para

alguns casos como, por exemplo, o Teorema de Sophie Germain. Usaremos um método, inventado por Fermat, conhecido como Método da Descida Infinita para transcrever as provas propostas pelo matemático suíço Leonhard Paul Euler para os casos $n = 3$ e $n = 4$. Encerraremos o capítulo com um belo exercício no qual se propõe encontrar a probabilidade de a equação $x^n + y^n = z^n$ não ter solução para algum número natural n, sabendo, apenas, que ela não terá solução sempre que esse n for um número múltiplo de 3 ou de $4-$ que são casos que já teremos provado.

A Matemática usada nas demonstrações será, em sua maioria, básica, para que um aluno que esteja na parte final do Ensino Fundamental ou no Ensino Médio precise estudar o mínimo possível, além do que seja proposto em sua grade curricular, para entender essas anotações, mas sem deixar de ser um material que possa ser consultado por professores desses níveis de ensino que estejam interessados no assunto.

2 FERMAT E SEU ÚLTIMO TEOREMA

Considerando que a História é um dos maiores legados deixado de uma geração para outra, neste capítulo faremos um breve resumo sobre o Último Teorema de Fermat e sobre alguns personagens que tiveram grande destaque na busca de solucioná-lo, mostrando assim que a maior contribuição de Fermat para a Matemática não foi a demonstração de um único teorema em si, e sim toda a teoria que precisou ser desenvolvida durante a busca de tal solução. Os trechos aqui expostos são de forma bem resumida o que pode acarretar em falhas, como a de não citar personagens e passagens importantes. Para os leitores curiosos e mais interessados pela linda história desse teorema indica-se [14].

2.1 Fermat

Príncipe dos Amadores, assim ficou conhecido o Jurista e Magistrado Pierre de Fermat. Nascido em Beaumonte-de-Lomagne no Sul da França na primeira metade do século XVII[1], seu pai Dominique Fermat era um empresário de sucesso e sua mãe Claire de Long de uma família aristocrata. Devido a isso, acredita-se que ele tenha recebido uma educação de qualidade pois não há registros sobre esse período de sua vida. Sabemos apenas que sua mãe morreu quando ele tinha sete anos.

Em 1628, com a morte do pai, Fermat recebeu muito dinheiro de herança. Seu novo posto social não o impediu de continuar trabalhando e estudando matemática. Quando tinha cerca de 23 anos ele pagou uma grande quantia em dinheiro, estima-se que cerca de 1 milhão de dólares, por uma posição sênior no Supremo Tribunal de Toulouse. Após tornar-se um nobre, pôde usar o nome aristocrático Pierre de Fermat, ao invés de simplesmente Pierre Fermat. Nesse mesmo período, casou-se com sua prima Louise de Long com quem teve oito filhos, sendo que apenas cinco chegaram a idade adulta. Foi graças ao seu filho mais velho que sua obra foi publicada, sobre isso falaremos mais a frente.

Seu vasto conhecimento em alguns idiomas como por exemplo: espanhol, italiano, latim e grego o ajudou em um de seus interesses, a restauração de livros antigos. Uma de suas contribuições foi a reconstrução do livro Plane Loci de Apollonius de Perga (262 a.C - 190 a.C). Acredita-se que a partir daí seu interesse pela Matemática teve início.

Outra teoria é que seu interesse se deu após a leitura de um texto remanescente da famosa Biblioteca de Alexandria, queimada em 642 d.C., o texto em questão era de Aritmética de Diofanto de Alexandria (aproximadamente[2] 250 d.C), nesse havia uma

[1] Não se sabe exatamente em qual ano Fermat nasceu, mas, geralmente, é datado em 1601.

[2] Não se sabe exatamente quais foram os anos de nascimento e morte de Diofanto.

compilação de dois mil anos de conhecimentos matemáticos.

Independente do momento sabemos que Fermat interessou-se por Matemática e mesmo estando tão distante de Paris − maior abrigo de grandes matemáticos da época − e apesar de dedicar-se a Matemática apenas nas suas horas de lazer, ele foi considerado por Pascal o maior matemático de seu tempo.

O caráter amador de seus trabalhos não teve destaque diante da grandiosidade de seu legado e de suas contribuições em diversas áreas das matemáticas, sendo as principais: o Cálculo Geométrico e Infinitesimal, a Teoria dos Números e Teoria da Probabilidade. Com raras exceções, Fermat não tinha interesse em fazer publicações ou exposições sistemáticas de seus métodos ou descobertas, ele entendia a Matemática como desafios a serem vencidos.

O ramo da Matemática que Fermat mais gostava era o da Teoria dos Números e é nesse segmento que está inserido o seu mais famoso Teorema, conhecido como o Último Teorema de Fermat. Esse teorema tem um enunciado extremamente simples, contudo desafiou matemáticos do mundo inteiro.

Sua morte foi anunciada erroneamente em 1653, pois devido a um surto de praga que assolou a região no início de 1650 muitos homens de sua faixa etária chegaram a falecer, o próprio Fermat foi atingido pela doença e sua saúde ficou muito fragilizada. Pierre de Fermat morreu em 12 de janeiro de 1665 em Cartes na França, sua causa-mortis não foi anunciada, mas os registros mostram que ele estava bem e trabalhando normalmente.

2.1.1 Último teorema

Fermat que tinha tanta aversão a publicar seus resultados poderia ter passado em branco na história da Matemática, pois os únicos resultados atribuídos a ele eram os que estavam expostos em suas cartas para seus amigos matemáticos que vez ou outra ficavam intimidados pelos desafios/enigmas propostos. Mas, para nossa sorte, após a sua morte, seu filho mais velho Clément-Samuel que entendia a importância dos trabalhos matemáticos desenvolvidos por seu pai, decidiu que não iria deixar os resultados serem perdidos no tempo e com um grande esforço passou cinco anos separando e organizando as cartas e as notas feitas nas margens dos livros e publicou. Segundo Simon Singh em [14]:

> "A nota referindo-se ao Último Teorema de Fermat era apenas um dos muitos pensamentos inspirados anotados no livro. Clément-Samuel resolveu publicar essas anotações em uma edição especial da Aritmética. Em 1670, em Toulouse, ele apresentou sua Aritmética de Diofante contendo observações de P. de Fermat. Ao lado do original grego e da tradução de Bachet para o latim, estavam 48 observações feitas por Fermat."

E assim o mundo conhecia algumas das propriedades que Fermat julgava importantes ou simplesmente interessantes. Dentre a coletânea havia provas corretas, incorretas ou incompletas (muitas vezes faltando uma parte crucial no argumento) e até aquelas que ficaram sem prova. Por exemplo, a conjectura de que, para todo número natural n, o número

$$F_n = 2^{2^n} + 1$$

é um número primo estava errada, apesar de valer para $0 \leq n \leq 4$, esses foram os números testados por Fermat. A decomposição de F_5 foi dada por Euler, veja a Figura 1.

n	F_n	Primo
0	3	Sim
1	5	Sim
2	17	Sim
3	257	Sim
4	65537	Sim
5	$4294967297 = 641 \cdot 6700417$	Não

Figura 1: Valores de $F_n = 2^{2^n} + 1$ para $0 \leq n \leq 5$.

Uma propriedade que foi enunciada e demonstrada de forma completa por Fermat, foi a que todo número primo ímpar pode ser escrito de forma única como a diferença de dois quadrados.

No meio dessas notas havia uma afirmação que aparentemente era tão simples e que nenhum matemático conseguia provar, mesmo Fermat tendo escrito que sabia uma prova para tal e que não escreveria por conta da margem. Essa afirmação gerou uma comoção para provar ou refutar as alegações contidas nas notas e por incrível que pareça, a "Afirmação" ficou por último. O que a fez receber o nome de Último Teorema de Fermat, que, segundo [14], é:

> "É impossível para um cubo ser escrito como a soma de dois cubos ou uma quarta potência ser escrita como uma soma de dois números elevados a quatro, ou, em geral, para qualquer número que seja elevado a uma potência maior do que dois ser escrito como a soma de duas potências semelhantes."

O teorema se tornou o problema mais conhecido da Matemática e, segundo [14], estava acompanhado pela frase que motivou o grande interesse no desafio:

> "Eu tenho uma demonstração realmente maravilhosa para esta proposição, mas a margem é muito estreita para contê-la."

Apesar de tão maravilhosa, Fermat não quis se dar o trabalho de escrever. Vários matemáticos tentaram encontrar uma prova mesmo que não fosse a mesma de Fermat e

como não se conseguia sucesso nessa busca começaram a acreditar que a prova maravilhosa poderia estar errada ou simplesmente que Fermat não teria provado; mas, por que ele mentiria? O primeiro avanço foi dado por Leonhard Euler (1707-1783), quase cem anos após a divulgação do problema, provando o caso $n = 3$. Outro fato interessante é que a francesa Sophie Germain (1776-1831) provou um teorema que ficou conhecido como o primeiro caso do Último Teorema de Fermat.

Uma demonstração completa teve início quando o garoto de dez anos, Andrew Wiles (1953) buscando por problemas matemáticos em um biblioteca local se deparou com a história do Teorema e ficou impressionado com o tempo que passou desde que o problema havia sido publicado e como ninguém foi capaz de provar algo que parecia tão simples e prometeu a si mesmo que iria encontrar uma prova. Em 1995, com a colaboração de Richard Taylor (1962), Wiles cumpriu a sua promessa juntando ramos bem diferentes da matemática clássica e atual e entrou para a história como um dos maiores matemáticos de todos os tempos.

2.1.2 A prova

Foram necessários quase quatro séculos, 358 anos, para que enfim o mundo pudesse conhecer uma prova que foi tão cobiçada por vários matemáticos ao longo da história, mas não foi por falta de tentativas, pois como dito anteriormente, esse problema foi objeto de estudo de grandes matemáticos na história. O próprio Fermat fez um esboço para o que seria uma demonstração da conjectura com $n = 4$, usando uma técnica que ele inventou e que outros matemáticos iriam tomar posse e provar a validade para outros casos, essa técnica é conhecida como "Descida Infinita de Fermat".

Quase cem anos após a morte de Fermat, o matemático conhecido por resolver todos os problemas que lhe fossem submetidos, Leonhard Euler, depois de 7 anos tentando resolver o Último Teorema de Fermat, provou que o caso $n = 3$ era verdadeiro e para tal usou a técnica inventada por Fermat. Nesse ponto da história, já havia se passado 133 anos desde que Fermat enunciou o teorema. Contudo, ainda havia uma lacuna na demonstração de Euler, ele usou que se

$$z^3 = x^2 + 3y^2$$

para $x, y \in \mathbb{Z}$ e $\text{mdc}(x, y) = 1$, então devem existir únicos $u, v \in \mathbb{Z}$ com

$$z = u^2 + 3v^2,$$

sem, previamente, fazer uma demonstração. Vale ressaltar que tal fato é verdadeiro e Euler já havia provado isso dez anos antes de publicar essa demonstração faltando, assim, que ele estabelecesse uma relação entre as condições dos dois problemas. Com o passar do

tempo foram surgindo mais avanços como, por exemplo, Legendre (1752-1833) mostrou a validade do caso $n = 5$, Dirichlet (1805-1859) demostrou o caso $n = 14$ e o Gabriel Lamé (1795-1870) o caso $n = 7$, esses três últimos se basearam em um método criado pela matemática francesa Sophie Germain. Ela, por sua vez, também contribuiu provando o primeiro caso do Último Teorema de Fermat. Voltaremos a falar sobre ela mais a frete.

Vale ressaltar que Cauchy (1789-1857) e Lamé, dois dos melhores matemáticos franceses, travaram um duelo em busca de ser o primeiro a demonstrar o teorema. Em meio a essa disputa, desenvolveram vários métodos que ajudaram na criação de novos ramos matemáticos, mas ao que se refere ao Último Teorema de Fermat, eles não conseguiram ganhar a corrida que só foi ter um fim 150 anos depois.

Em 1957 os japoneses Yutaka Taniyama (1927-1958) e Goro Shimura (1930) formulam a Conjectura de Shimura-Taniyama - que consiste em mostrar que toda forma modular pode ser representada por uma curva elíptica - o que mudou um pouco o panorama, pois agora não era mais preciso demonstrar o famoso teorema diretamente. Bastava provar a conjectura, o que também não era tarefa fácil.

Como já foi citado, Andrew Wiles teve seu primeiro contato com Último Teorema de Fermat na sua infância e desde então assumiu o papel de tentar demonstrá-lo. Quando estava na faculdade teve que deixar o problema um pouco de lado, mas por sorte, seu orientador, sem saber que iria ajudar na futura prova, incentivou Wiles a estudar sobre as curvas elíptica, que recebem esse nome por parecerem com as funções que são usadas para calcular o comprimento de um arco da elipse e que estão diretamente ligadas a conjectura de Shimura-Taniyama. Wiles começou a tentar provar a conjectura visto que essa era a sua área de especialidade, e assim o fez, provou um caso particular que implicava na tão sonhada prova, e dessa forma, as conjecturas passaram a ser teoremas e receberam o nome de Wiles, para fazer menção de que foi ele quem demonstrou, virando "O Último Teorema de Fermat-Wiles".

Citamos mais uma vez o livro O Último Teorema de Fermat de Simon Singh:

> "Com o giz na mão, Wiles virou-se para o quadro pela última vez. Algumas linhas finais de lógica completaram a prova. Pela primeira vez, em mais de três séculos, o desafio de Fermat fora vencido. Houve mais alguns clarões de flashes tentando captar o momento histórico. Wiles terminou, voltou-se para a audiência e disse com modéstia: Acho que vou parar por aqui."

Andrew Wiles ganhou quase todos os prêmios destinados aos matemáticos que de alguma forma ficaram marcados na história por terem contribuído de forma notória para o desenvolvimento da ciência ou da humanidade. Só não ganhou a Medalha Fields, que é a maior honraria no mundo matemático, por já ter completado 40 anos quando publicou a prova o que excedeu a idade limite permitida para concorrer.

2.2 Sophie Germain

Marie-Sophie Germain nasceu no dia primeiro de abril de 1776, na França. Ela cresceu rodeada por discussões sobre política e filosofia, pois sua casa era um espaço de reuniões para esses assuntos. Possivelmente essas discussões a tenham tornado uma mulher com uma postura a frente de seu tempo. Autodidata, Sophie aprendeu latim e grego estudando sozinha e demonstrou desde muito cedo o interesse pelos números. Inicialmente, sua fascinação pelos números preocuparam seus pais, que tentaram impedir seus estudos noturnos escondendo as velas para que ela não pudesse ler Newton e Euler.

Seu interesse pela Matemática foi despertado ainda na adolescência, quando aos 13 anos de idades, estava numa biblioteca e leu um relato de um soldado romano sobre a morte de Arquimedes e ali, naquele momento, decidiu tornar-se matemática.

Por estudar em condições precárias e trabalhar em isolamento intelectual, Sophie aspirava ter a oportunidade de estudar na Escola Politécnica de Paris, mas isso não era possível pois nestas instituições apenas homens eram admitidos. Cheia de audácia, ela descobriu que um dos alunos tinha saído de Paris e por algum motivo a escola não ficou sabendo e continuou enviando as lições.

O aluno mencionado chamava-se Antoine-August Le Blanc. Sophie foi quem passou a interceptar as lições e enviar as resoluções toda semana e assinava com o nome M. Le Blanc. Joseph-Louis Lagrange, o professor da disciplina, começou a achar as mudanças nos resultados de Le Blanc muito suspeitas e pediu para que ele se apresentasse e foi assim que a verdadeira identidade de Le Blanc foi revelada. Contra todas as expectativas, Lagrange incentivou os estudos de Sophie e tornou-se seu orientador e amigo.

Vale ressaltar que ela continuou usando o pseudônimo Le Blanc para manter contato com outros cientistas pois ela tinha receio de que se soubessem que ela era uma mulher não seria levada a sério. Não há registros de que ela tenha casado ou trabalhado, sendo assim, é especulado que seus pais mesmo sem aceitar/entender o seu interesse por este ramo no qual as mulheres não eram bem-vindas, sustentaram-a durante toda a sua vida.

Carl Friedrich Gauss (1777-1855) indicou um dos trabalhos de Sophie para ser reconhecido como tese de doutorado na Alemanha mas ela morreu antes de receber a honra.

Marie-Sophie Germain morreu de câncer de mama, em 27 de junho de 1831, no seu atestado de óbito, não consta que ela foi uma matemática ou cientista, mas que tinha como meio de vida o aluguel de propriedades.

3 SOLUÇÕES PARA ALGUNS CASOS

O famoso comentário de Fermat em forma de teorema deixado nas margens de um dos treze livros da coleção "Arithmetica" de Diofanto, continuava sem solução. Mesmo depois de tantas tentativas, parecia que ele relutava em não ser provado. Para inflamar ainda mais o ego de alguns e/ou ferir o orgulho de outros, o problema se tornou um desafio ainda mais interessante por estar acompanhado da seguinte frase escrita por Fermat, "Descobri uma demonstração maravilhosa desta proposição que, no entanto, não cabe nas margens deste livro." Dando trabalho a várias gerações de matemáticos no decorrer de quase quatro séculos - que foi o tempo necessário para demonstrá-lo - gerando diversos resultados interessantes e que alguns desses iremos expor a seguir.

Neste capítulo, iremos apresentar soluções de alguns casos do Último Teorema de Fermat, são eles: o Teorema de Sophie Germain, o caso $n = 3$ ($x^3 + y^3 = z^3$) e o caso $n = 4$ ($x^4 + y^4 = z^4$). O que mostrará a validade da afirmação feita por Fermat para qualquer número natural que seja múltiplo de 3 ou 4. De fato, uma vez que sabemos que as equações $x^3 + y^3 = z^3$ e $x^4 + y^4 = z^4$ não têm soluções inteiras não triviais, teremos que as equações

$$x^{3k} + y^{3k} = z^{3k} \Leftrightarrow (x^k)^3 + (y^k)^3 = (z^k)^3$$

e

$$x^{4k} + y^{4k} = z^{4k} \Leftrightarrow (x^k)^4 + (y^k)^4 = (z^k)^4$$

também não terão soluções sempre que $x, y, z \in \mathbb{Z}^*$ e $k \in \mathbb{N}$.

Ao se questionar qual deveria ser uma boa estratégia para demonstrar a generalidade do problema, um caminho óbvio seria mostrar que vale para todos os números primos o que teria como consequência a validade para todo número composto. Mas, como veremos, isso não é uma tarefa fácil. Veja a fala do professor Paulo Ribenboim, que é especialista em Teoria dos Números, numa entrevista dada a Revista Matemática Universitária (veja [12]) quando questionado sobre a demonstração do Último Teorema de Fermat:

> "...Eu estava vendo que para o expoente 3 não era tão fácil mas não era tão difícil. Mas era muito mais difícil para 5, ainda mais para 7, e ainda mais para 11, e não podia continuar com esse aumento de dificuldade, se você quisesse fazer para cada expoente. Tinha que ser algum método que não envolvesse os primos, tinha que ser alguma coisa completamente diferente. E foi assim que foi feito."

Como já vimos, uma demonstração completa foi dada por Andrew Wiles e tal demonstração foge totalmente da proposta desse trabalho por sua sofisticação técnica que torna suas quase duzentas páginas incompreensíveis para a maioria das pessoas, deixando

vago um lugar na história para aquele que conseguir demonstrá-la usando um método maravilhoso − entenda como razoavelmente simples − e que possa ocupar um pouco mais do que a margem da folha de um livro.
Também discutiremos um pouco sobre a equação do tipo

$$x^2 + y^2 = z^2, \tag{3.1}$$

que é conhecida como equação pitagórica ou quadrática, onde tal equação possui o maior expoente para o qual a equação

$$x^n + y^n = z^n, \tag{3.2}$$

onde $n \in \mathbb{N}$, possui solução inteira não trivial.

A equação pitagórica possui uma grande aplicabilidade nas geometrias em geral. Por exemplo, temos na Geometria Euclidiana o Teorema de Pitágoras que na Geometria Analítica é usado para encontrar uma fórmula que determina a distância entre dois pontos no espaço.

3.1 Teorema de Sophie Germain

Se um número p primo é de tal forma que $2p + 1$ também é primo, então p é um número de Sophie Germain e recebe esse nome porque a matemática francesa Sophie Germain provou o chamado "primeiro caso do Último Teorema de Fermat". Um fato interessante é que ainda não se sabe provar se existem ou não infinitos números de Sophie Germain. Entre 1 e 10^4 existem 190 números de Sophie Germain, que é uma quantidade considerada grande, visto que o conjunto dos primos de Sophie Germain é um subconjunto dos números primos, que por sua vez é infinito, mas que fica cada vez mais escasso quando estamos próximos de números suficientemente grandes.

Alguns exemplos de números de Sophie Germain são 2, 3, 5, 11, 23, 83 e 1601 com seus respectivos representantes sendo 5, 7, 11, 23, 47, 167 e 3203. Vale relembrar que 1601 é um dos possíveis anos em que Fermat pode ter nascido.

O número $p = 2$ é interessante, veja:

$$2 \text{ é primo}$$

$$2 \cdot 2 + 1 = 5 \text{ é primo}$$

$$2 \cdot 5 + 1 = 11 \text{ é primo}$$

$$2 \cdot 11 + 1 = 23 \text{ é primo}$$

$$2 \cdot 23 + 1 = 47 \text{ é primo}$$

$$2 \cdot 47 + 1 = 95 \text{ é composto.}$$

E assim acaba nossa sequência.
Você consegue pensar em uma sequência desse tipo com mais de 4 números de Sophie Germain?

Seguem três teoremas e três definições que são muito importantes para os resultados que virão. As demonstrações dos teoremas fogem um pouco da proposta deste trabalho mas podem ser consultadas nas referências [5], [7], [8] ou [10].

Definição 1 (Congruência) *Sejam a, b e n inteiros dados, sendo $n > 1$. Dizemos que a é **congruente** a b, módulo n, e denotamos $a \equiv b\,(mod\ n)$, se $n \mid (a - b)$. Se a não for congruente a b módulo n, denotamos $a \not\equiv b\,(mod\ n)$.*

Teorema 3.1.2 (PTF - Pequeno Teorema de Fermat) *Sejam $a \in \mathbb{Z}$ e p um número primo tais que* $\text{mdc}(a, p) = 1$. *Tem-se que*

$$a^{p-1} \equiv 1(mod\ p).$$

Veja [10, Proposição 5.14, página 133].

Definição 2 *Sejam $b, m \in \mathbb{Z}$, com $m > 1$ e* $\text{mdc}(b, m) = 1$, *diremos que b é um resíduo quadrático módulo m se a congruência*

$$x^2 \equiv b(mod\ m)$$

possuir pelo menos uma solução inteira x. Caso contrário, b é dito um não resíduo quadrático módulo m.

Definição 3 *Se $a, p \in \mathbb{Z}$, com p primo, definimos o símbolo de Legendre $\left[\frac{a}{p}\right]$ por:*

$$\left[\frac{a}{p}\right] = \begin{cases} 1, & \text{se } a \text{ for resíduo quadrático módulo } p \\ -1, & \text{se } a \text{ não for resíduo quadrático módulo } p \\ 0, & \text{se } p \mid a \end{cases}.$$

Teorema 3.1.3 *Se p é um número primo e $a, b \in \mathbb{Z}$, o símbolo de Legendre possui as seguintes propriedades:*

1. *Se $a \equiv b(mod\ p)$ então $\left[\frac{a}{p}\right] = \left[\frac{b}{p}\right]$.*

2. $\left[\frac{a^2}{p}\right] = 1$ *se $p \nmid a$.*

3. $\left[\frac{ab}{p}\right] = \left[\frac{a}{p}\right]\left[\frac{b}{p}\right]$.

Veja [10, Proposição 7.23, página 191].

Teorema 3.1.4 (Lei da reciprocidade quadrática de Gauss) *Se p e q são números primos ímpares e distintos, então*

$$\left[\frac{p}{q}\right]\left[\frac{q}{p}\right] = (-1)^{\left(\frac{p-1}{2}\right)\left(\frac{q-1}{2}\right)}.$$

Veja [10, Proposição 7.28, página 196].

De posse destes resultados, podemos enunciar e demonstrar o Teorema de Sophie Germain e os que seguem.

Teorema 3.1.5 (Sophie Germain) *Se p e $2p+1$ são primos com $p > 2$, então não existem inteiros x, y, z com $mdc(x, y, z) = 1$ e $p \nmid xyz$ tais que $x^p + y^p + z^p = 0$.*

Demonstração: Iremos fazer a demonstração por redução ao absurdo. Observe inicialmente que

$$(2p+1) \mid xyz$$

Pois, caso contrário, pelo Pequeno Teorema de Fermat,

$$x^{2p} \equiv 1 (\mathrm{mod}\, 2p+1),$$

o que equivale a

$$(x^p - 1)(x^p + 1) \equiv 0 (\mathrm{mod}\, 2p+1).$$

Como $2p+1$ é primo deve dividir um dos dois fatores, logo

$$x^p \equiv \pm 1 (\mathrm{mod}\, 2p+1)$$

e, analogamente,

$$y^p \equiv \pm 1 (\mathrm{mod}\, 2p+1)$$

e

$$z^p \equiv \pm 1 (\mathrm{mod}\, 2p+1).$$

Consequentemente,

$$0 = x^p + y^p + z^p \equiv \pm 1 \pm 1 \pm 1 \not\equiv 0 (\mathrm{mod}\, 2p+1)$$

um absurdo.

Por outro lado, temos

$$\begin{aligned} x^p + y^p + z^p = 0 &\Leftrightarrow y^p + z^p = -x^p \\ &\Leftrightarrow (-x)^p = y^p + z^p \\ &\Leftrightarrow (-x)^p = (y+z)(y^{p-1} - y^{p-2}z + \cdots - yz^{p-2} + z^{p-1}) \end{aligned}$$

Mostraremos que os dois fatores da direita são coprimos.
De fato, se $q > 1$ é um primo que divide ambos os termos, então $y \equiv -z (\text{mod } q)$, portanto

$$0 \equiv y^{p-1} - y^{p-2}z + \cdots - yz^{p-2} + z^{p-1} \equiv \underbrace{y^{p-1} + \cdots + y^{p-1}}_{p \text{ vezes}} \equiv py^{p-1} (\text{mod } q).$$

Perceba que $q \neq p$, pois $q \,|\, x$. Assim, $mdc(p, q) = 1$ e $q \,|\, y$. Consequentemente, $q \,|\, z$ e $q \,|\, mdc(x, y, z)$. O que contraria a hipótese de $mdc(x, y, z) = 1$.

Como temos o produto de números coprimos dando uma potência p-ésima, devem existir números inteiros a e d tais que

$$a^p = y + z \text{ e } d^p = y^{p-1} - y^{p-2}z + \cdots - yz^{p-2} + z^{p-1}.$$

Analogamente, ao considerarmos as equações

$$(-y)^p = x^p + z^p \tag{3.3}$$

e,

$$(-z)^p = x^p + y^p \tag{3.4}$$

devem existem b, c, e e f números inteiros tais que

$$b^p = x + z,\ e^p = x^{p-1} - x^{p-2}z + \cdots - xz^{p-2} + z^{p-1},$$

$$c^p = x + y \text{ e } f^p = x^{p-1} - x^{p-2}y + \cdots - xy^{p-2} + y^{p-1}.$$

Como $(2p+1) \,|\, xyz$, podemos supor sem perda de generalidade que $(2p+1) \,|\, x$.
Uma vez que,

$$b^p + c^p - a^p = (x+z) + (x+y) - (y+z) = 2x,$$

temos que $(2p+1) \,|\, (b^p + c^p - a^p)$ e o mesmo argumento do início da demonstração mostra que devemos ter $(2p+1) \,|\, abc$. Agora, temos dois casos.

Caso 1. Se

$$(2p+1) \,|\, b \text{ ou } (2p+1) \,|\, c,$$

de sorte,

$$(2p+1) \,|\, b^p = x + z \text{ ou } (2p+1) \,|\, c^p = x + y,$$

como já temos que $(2p+1) \mid x$ e $x^p + y^p + z^p = 0$ nos dá que $(2p+1) \mid y$ e $(2p+1)|z$. Consequentemente, $(2p+1) \mid \text{mdc}(x, y, z) = 1$, um absurdo.

Caso 2. Se

$$(2p+1) \mid a$$

de modo análogo,

$$(2p+1) \mid a^p = y + z.$$

Inicialmente, note que a hipótese $(2p+1) \mid x$ implica que,

$$f^p = x^{p-1} - x^{p-2}y + \cdots - xy^{p-2} + y^{p-1} \equiv y^{p-1} (\text{mod } 2p+1) \Rightarrow f^p \equiv y^{p-1} (\text{mod } 2p+1),$$

logo,

$$pf^p \equiv py^{p-1} (\text{mod } 2p+1).$$

Como

$$(2p+1) \mid a^p = y + z \Rightarrow z \equiv -y (\text{mod } 2p+1),$$

tem-se

$$\begin{aligned} d^p = y^{p-1} - y^{p-2}z + \cdots - yz^{p-2} + z^{p-1} &\equiv \underbrace{y^{p-1} + \cdots + y^{p-1}}_{p \text{ vezes}} \\ &\equiv py^{p-1} (\text{mod } 2p+1) \\ &\equiv pf^p (\text{mod } 2p+1). \end{aligned}$$

Além disso,

$$mdc(a, d) = mdc(a^p, d^p) = 1,$$

portanto, $(2p+1) \nmid d$, e assim, devemos ter que $(2p+1) \mid f$, pois caso contrário teríamos pelo Pequeno Teorema de Fermat, que

$$\begin{aligned} f^{2p} \equiv 1 (\text{mod } 2p+1) &\Rightarrow f^{2p} - 1 \equiv 0 (\text{mod } 2p+1) \\ &\Rightarrow (f^p - 1)(f^p + 1) \equiv 0 (\text{mod } 2p+1) \\ &\Rightarrow f^p \equiv \pm 1 (\text{mod } 2p+1) \\ &\Rightarrow pf^p \equiv \pm p (\text{mod } 2p+1). \end{aligned}$$

Como $(2p+1) \nmid d$, tem-se

$$d^p \equiv \pm 1 (\text{mod } 2p+1).$$

Ou seja,

$$\pm p \equiv pf^p \equiv py^{p-1} \equiv d^p \equiv \pm 1 (\text{mod } 2p+1) \Rightarrow \pm p \equiv \pm 1 (\text{mod } 2p+1),$$

teríamos que, a depender do sinal, $(2p+1) \mid (\pm p \mp 1)$. Conquanto,

$$|(\pm p \mp 1)| \leq p + 1 < (2p + 1)$$

e isso é um absurdo.
Mas, nesse caso, $(2p+1) \mid y$ e, consequentemente, $(2p+1) \mid z$ também, o que é impossível já que $mdc(x, y, z) = 1$, logo não existe solução inteira. ■

Exemplo 1 *Se* $5 \nmid xyz$, $11 \nmid xyz$ *e* $\text{mdc}(x, y, z) = 1$, *então as equações*

$$x^5 + y^5 = z^5 \text{ e } x^{11} + y^{11} = z^{11}$$

não têm soluções inteiras não triviais.

De fato, como $\text{mdc}(x, y, z) = 1$, 5 e 11 são primos de Sophie Germain, e $5 \nmid xyz$ pelo **Teorema 3.1.5** a primeira não terá solução inteira não trivial. Também temos que $11 \nmid xyz$ e assim por motivos análogos, vale o mesmo para a segunda equação.

Os números de Sophie Germain tem uma relação interessante com os números da forma $M_p = 2^p - 1$ que são conhecidos como números de Mersenne.

Antes de enunciar tal relação, observe que se p for um número positivo e composto teremos que M_p também será composto. Com efeito, se p é composto e positivo, existem os números $r, s, k \in \mathbb{N}$ com $p = rs$, e

$$M_p = M_{r \cdot s} = 2^{r \cdot s} - 1 = (2^r)^s - 1^s = (2^r - 1) \cdot k$$

logo, teremos que M_p é composto. Os números de Mersenne são outro exemplo que ainda não se sabe provar se há ou não infinitos números primos desta forma, mas os maiores números primos conhecidos atualmente são números Mersenne. Alguns exemplos de números primos de Mersenne estão na Figura 2.

p	$2^p - 1$	M_P
2	$2^2 - 1$	3
3	$2^3 - 1$	7
5	$2^5 - 1$	31
7	$2^7 - 1$	127
13	$2^{13} - 1$	8191
17	$2^{17} - 1$	524287

Figura 2: Alguns números primos de Mersenne.

Uma maneira de mostrar que 641 é um divisor de F_5 é perceber que

$$\begin{aligned} 641 = 2^7 \cdot 5 + 1 &\Rightarrow 2^7 \cdot 5 + 1 \equiv 0 \,(\text{mod } 641) \\ &\Rightarrow 2^7 \cdot 5 \equiv -1 \,(\text{mod } 641) \\ &\Rightarrow 2^{28} \cdot 5^4 \equiv 1 \,(\text{mod } 641). \end{aligned}$$

Além disso,

$$\begin{aligned} 641 = 2^4 + 5^4 &\Rightarrow 5^4 \equiv -2^4 \,(\text{mod } 641) \\ &\Rightarrow 1 \equiv 2^{28} \cdot 5^4 \equiv 2^{28} \cdot (-2^4) \,(\text{mod } 641) \\ &\Rightarrow 1 \equiv -2^{32} \,(\text{mod } 641) \\ &\Rightarrow 2^{32} + 1 \equiv 0 \,(\text{mod } 641) \\ &\Rightarrow 2^{2^5} + 1 \equiv 0 \,(\text{mod } 641) \\ &\Rightarrow 641 \,|\, 2^{2^5} + 1 = F_5. \end{aligned}$$

E, portanto, $F_5 = 641 \cdot k$, para algum $k \in \mathbb{N}$.

Teorema 3.1.6 *Se p e $q = 2p + 1$ são números primos (i. e. p é um primo de Sophie Germain), então $q \,|\, M_p$ ou $q \,|\, (M_p + 2)$, mas não acontecem ambos os casos.*

Demonstração: Pelo Pequeno Teorema de Fermat, temos

$$\begin{aligned} 2^{q-1} \equiv 1 \,(\text{mod } q) &\Rightarrow 2^{q-1} - 1 \equiv 0 \,(\text{mod } q) \\ &\Rightarrow (2^{\frac{q-1}{2}} - 1)(2^{\frac{q-1}{2}} + 1) \equiv 0 \,(\text{mod } q) \\ &\Rightarrow (2^p - 1)(2^p + 1) \equiv 0 \,(\text{mod } q) \\ &\Rightarrow (2^p - 1)[(2^p - 1) + 2] \equiv 0 \,(\text{mod } q) \\ &\Rightarrow M_p \cdot (M_p + 2) \equiv 0 \,(\text{mod } q). \end{aligned}$$

Como q é um número primo, devemos ter que $q \,|\, M_p$ ou $q \,|\, (M_p + 2)$. Se q dividisse ambos, teríamos

$$q \,|\, M_p \text{ e } q \,|\, (M_p + 2) \Rightarrow q \,|\, [(M_p + 2) - (M_p)] = 2 \Rightarrow q \,|\, 2.$$

O que não acontece, pois $q > 2$. ∎

Com isso, podemos observar que se p é um número composto, então M_p também será composto. Mas, se p é primo, nada poderemos dizer sobre M_p nesse sentido, pois existem alguns $p > 3$ primos de Sophie Germain com $(2p + 1) \,|\, M_p$, nos dando que M_p é composto. Veja um caso no qual isso acontece no próximo exemplo.

Exemplo 2 *Como $p = 11$ é um primo de Sophie Germain, pois, $q = 2 \cdot 11 + 1 = 23$*

também é primo. Temos:

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

Assim, M_p é composto, mesmo p sendo um número primo.

Uma reportagem publicada no site do IMPA no dia 15 de janeiro de 2019 (veja [3]), diz o seguinte:

> "O ano começou com uma boa notícia para a ciência. Matemáticos – profissionais e amadores – do projeto de pesquisa mundial Great Internet Mersenne Prime Search (GIMPS) – descobriram o maior número primo conhecido. Com 24.862.048 dígitos, mais de 1,5 milhão do que o número primo recorde descoberto em 2017, ele pode ser expresso como $2^{82.589.933} - 1$."

Esse é o 51° número primo de Mersenne encontrado.

3.2 Solução para $n = 2$

A equação $x^2 + y^2 = z^2$ é conhecida como equação pitagórica por fazer referência ao matemático grego Pitágoras. Se $x, y, z \in \mathbb{Z}$ satisfazem a relação $x^2 + y^2 = z^2$, então (x, y, z) é chamada de tripla pitagórica. Além disso, se x, y e z são coprimos dois a dois, então a tripla pitagórica (x, y, z) é dita uma solução primitiva e recebe esse nome por ser a primeira de um conjunto infinito de soluções para a equação dada. Perceba que se (x, y, z) é uma solução primitiva, então para todo $d \in \mathbb{Z}$ teremos que a tripla (dx, dy, dz) também será solução, pois:

$$\begin{aligned} x^2 + y^2 = z^2 &\Leftrightarrow d^2 \cdot (x^2 + y^2) = d^2 \cdot z^2 \\ &\Leftrightarrow d^2 \cdot x^2 + d^2 \cdot y^2 = d^2 \cdot z^2 \\ &\Leftrightarrow (dx)^2 + (dy)^2 = (dz)^2. \end{aligned}$$

Agora, nos preocuparemos apenas com as soluções primitivas.

Além disso, note que se (x, y, z) é uma solução, então todas as combinações das forma $(\pm x, \pm y, \pm z)$ também serão, veja:

$$x^2 + y^2 = z^2 \Leftrightarrow (\pm x)^2 + (\pm y)^2 = (\pm z)^2.$$

Como não traz prejuízos e simplifica o processo, iremos trabalhar apenas com soluções primitivas e positivas.

Proposição 3.1.1 *Se a tripla (a, b, c) é uma solução primitiva, então a e b tem paridades distintas e c é ímpar.*

Demonstração: Supondo que a e b sejam ambos pares, teríamos $\text{mdc}(a,b) \neq 1$, o que contrária a hipótese de serem uma solução primitiva.

Se a e b sejam ambos ímpares, ou seja, existem $r, s \in \mathbb{Z}$ com $a = 2r+1$ e $b = 2s+1$, e assim

$$\begin{aligned} c^2 &= a^2 + b^2 \\ &= (2r+1)^2 + (2s+1)^2 \\ &= (4r^2 + 4r + 1) + (4s^2 + 4s + 1) \\ &= 2[2(r^2 + r + s^2 + s) + 1] \\ &= 2(2k+1), \end{aligned}$$

para $k \in \mathbb{Z}$ e $k = r^2 + r + s^2 + s$. Como $\text{mdc}(2, 2k+1) = 1$ teríamos que 2 é um quadrado, ou seja, um absurdo.

Restando apenas a opção de terem paridades diferentes, e sem perda de generalidade iremos supor[1] a partir de agora − por ser mais conveniente − que sempre teremos a sendo um número ímpar e b é um número par.
Com efeito, dados $k, p \in \mathbb{N}$, se a tripla $(2k,\ 2p+1,\ c)$ é uma solução para $x^2 + y^2 = z^2$, então $(2p+1,\ 2k,\ c)$ também o é. Logo, existem $r, s \in \mathbb{Z}$ com $a = 2r+1$ e $b = 2s$, tais que

$$\begin{aligned} c^2 &= a^2 + b^2 \\ &= (2r+1)^2 + (2s)^2 \\ &= (4r^2 + 4r + 1) + 4s^2 \\ &= 2(2r^2 + 2r + 2s^2) + 1 \\ &= 2k + 1, \end{aligned}$$

nos dando que c^2 é ímpar e, consequentemente, c também deve ser. ■

Teorema 3.1.7 (Pitágoras) *Se (a,b,c) é uma solução primitiva de $x^2 + y^2 = z^2$, então existem números $u, v \in \mathbb{Z}$ primos entre si, com*

$$\begin{cases} a = v^2 - u^2, \\ b = 2uv, \\ c = v^2 + u^2. \end{cases}$$

Além disso, u e v têm paridades distintas.

[1] Sempre que for falado de triplas pitagóricas.

Demonstração: Veja que,

$$a^2 + b^2 = c^2 \Leftrightarrow b^2 = c^2 - a^2 \Leftrightarrow b^2 = (c-a)(c+a).$$

Pondo $d = \text{mdc}(c-a, c+a)$ teremos que

$$d \,|\, (c-a) \text{ e } d \,|\, (c+a),$$

e assim,

$$d \,|\, [(c-a)+(c+a)] = 2c \text{ e } d \,|\, [(c+a)-(c-a)] = 2a,$$

nos dando que

$$d \,|\, \text{mdc}(2a, 2b) = 2 \cdot \text{mdc}(a, b) = 2$$

pois estamos trabalhando com uma solução primitiva e $\text{mdc}(a, b) = 1$. Como $(c-a)$ e $(c+a)$ são pares por serem diferença e soma de dois ímpares respectivamente, nos resta $d = 2$.
Como b é um número par, podemos dividí-lo por 2. Daí,

$$b^2 = (c-a)(c+a) \Leftrightarrow \left(\frac{b}{2}\right)^2 = \left(\frac{c-a}{2}\right) \cdot \left(\frac{c+a}{2}\right).$$

Tem-se que o $\text{mdc}\left(\frac{c-a}{2}, \frac{c+a}{2}\right) = 1$, pois $\text{mdc}(c-a, c+a) = 2$. Portanto, os números $\left(\frac{c-a}{2}\right)$ e $\left(\frac{c+a}{2}\right)$ são quadrados perfeitos. Ou seja, existem $u, v \in \mathbb{Z}$ com $\text{mdc}(u, v) = 1$ tais que $c - a = 2u^2$ e $c + a = 2v^2$. Note que, neste caso, temos $v > u$. Resolvendo em função de c e a, encontramos:

$$c = u^2 + v^2 \text{ e } a = v^2 - u^2.$$

Aqui, já temos que u e v devem ter paridades distintas, pois caso contrário teríamos que c é par, mas sabemos que c deve ser ímpar. Substituindo as novas representações de a e c na equação inicial, temos:

$$\begin{aligned} a^2 + b^2 = c^2 &\Leftrightarrow (v^2 - u^2)^2 + b^2 = (u^2 + v^2) \\ &\Leftrightarrow (v^4 - 2u^2v^2 + u^4) + b^2 = (v^4 + 2u^2v^2 + u^4) \\ &\Leftrightarrow b^2 = (2uv)^2 \\ &\Leftrightarrow b = \pm 2uv. \end{aligned}$$

Teremos que $(v^2 - u^2,\ 2uv,\ v^2 + u^2)$ é uma solução para a equação $x^2 + y^2 = z^2$. ∎

De posse desse teorema, temos que para encontrar uma infinidade de soluções para

a equação de inteiros $x^2 + y^2 = z^2$ basta atribuir valores inteiros a u e v com $u < v$ de forma que sejam primos entre si e de paridades distintas e aplicar em $(v^2-u^2, 2uv, v^2+u^2)$. Encontrando assim uma solução primitiva e para a infinidade basta multiplicar por $d \in \mathbb{Z}$ cada uma das entradas. Por exemplo, fazendo $u = 1$ e $v = 2$, temos a solução primitiva

$$(v^2 - u^2, 2uv, v^2 + u^2) = (2^2 - 1^2, 2 \cdot 1 \cdot 2, 2^2 + 1^2) = (3, 4, 5)$$

para a equação $x^2 + y^2 = z^2$, pois, mdc$(3, 4, 5) = 1$ e $3^2 + 4^2 = 5^2$. Para uma infinidade de soluções basta incluir o d, ficando com $(3d, 4d, 5d)$ que como já vimos também será solução, independente do valor de d.

Um fato interessante sobre a tripla pitagórica é o seguinte:

Proposição 3.1.2 *A única tripla pitagórica de elementos positivos que estão numa sequência de valores consecutivos é* $(3, 4, 5)$.

Demonstração: Como já vimos, $(3, 4, 5)$ é uma tripla pitagórica, faltando mostrar apenas que é a única.

Faremos uma redução ao absurdo. Suponha que exista outra tripla com os elementos em sequência, ou seja, existe $(n, n+1, n+2)$ com $n \in \mathbb{N}$ e $n \neq 3$, que seja solução de $x^2 + y^2 = z^2$, logo

$$\begin{aligned} n^2 + (n+1)^2 = (n+2)^2 &\Leftrightarrow n^2 + (n^2 + 2n + 1) = n^2 + 4n + 4 \\ &\Leftrightarrow (2n^2 - n^2) + (2n - 4n) + (1 - 4) = 0 \\ &\Leftrightarrow n^2 - 2n - 3 = 0 \\ &\Leftrightarrow (n-3)(n+1) = 0 \Leftrightarrow n = 3 \text{ ou } n = -1. \end{aligned}$$

Um absurdo, pois, devemos ter $n \neq 3$ o que anula a primeira alternativa e $n > 0$ o que anula a segunda alternativa. Ou seja, não existe tal n. Mostrando que (3,4,5) é única. ■

Pitágoras mostrou que se (a, b, c) são as medidas dos lados de um triângulo retângulo com c sendo o comprimento da hipotenusa, então devemos ter $a^2 + b^2 = c^2$. Existem várias demonstrações para esse fato. Veja a seguir, uma dessas demonstrações.

Proposição 3.1.3 *Em todo triângulo retângulo cujas medidas dos catetos são a e b e a medida da hipotenusa é c, teremos que (a, b, c) é uma tripla pitagórica, ou seja, devemos ter $a^2 + b^2 = c^2$.*

Demonstração: Seja $\triangle ABC$, um triângulo retângulo com catetos $\overline{AB} = a$, $\overline{AC} = b$ e hipotenusa $\overline{BC} = c$. E seja $AMNK$ um quadrado de lados,

$$\overline{AK} = \overline{AM} = \overline{MN} = \overline{KN} = a + b.$$

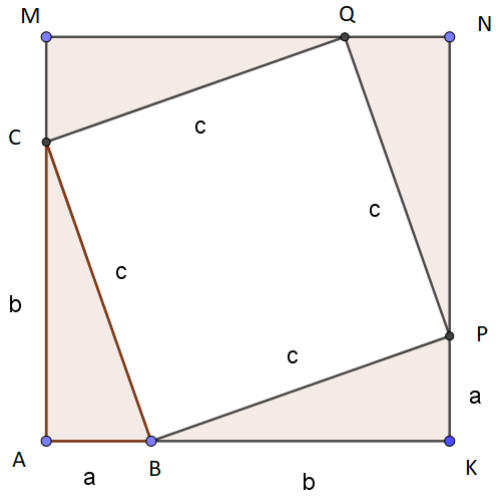

Figura 3: Quadrado usado como auxílio na demonstração do Teorema de Pitágoras.

Note que,

$$\begin{cases} \overline{BK} = \overline{AK} - \overline{AB} = (a+b) - a = b, \\ \overline{MC} = \overline{AM} - \overline{AC} = (a+b) - b = a. \end{cases}$$

E sejam $Q \in \overline{MN}$ e $P \in \overline{KN}$, tais que

$$\begin{cases} \overline{MQ} = a \text{ e } \overline{NQ} = b, \\ \overline{NP} = b \text{ e } \overline{KP} = a. \end{cases}$$

Como $AMNK$ é um quadrado, temos

$$\text{med}(\widehat{MAK}) = \text{med}(\widehat{AMN}) = \text{med}(\widehat{MNK}) = \text{med}(\widehat{NKA}) = 90°.$$

Pelo caso de congruência LAL, tem-se que $\triangle ABC$, $\triangle CMQ$, $\triangle NPQ$ e $\triangle BKP$ são congruentes. Além disso,

$$\text{med}(\widehat{PBK}) = \text{med}(\widehat{ACB}). \tag{3.5}$$

Pela soma dos ângulos internos de um triângulo, temos

$$\text{med}(\widehat{ABC}) + \text{med}(\widehat{ACB}) + \text{med}(\widehat{BAC}) = 180° \Rightarrow \text{med}(\widehat{ABC}) + \text{med}(\widehat{ACB}) = 90°.$$

Como um ângulo raso mede 180°, temos

$$\text{med}(\widehat{ABC}) + \text{med}(\widehat{PBK}) + \text{med}(\widehat{CBP}) = 180°.$$

Pela Equação 3.5,

$$\underbrace{\text{med}(\widehat{ABC}) + \text{med}(\widehat{ACB})}_{=90^\circ} + \text{med}(\widehat{CBP}) = 180^\circ.$$

Ou seja, $\text{med}(\widehat{CBP}) = 90^\circ$.
Logo, o quadrilátero $BPQC$ tem todos os lados iguais a c, e, pelo menos, um ângulo reto ($\widehat{CBP}$). Consequentemente, $BPCQ$ é um quadrado. E sua área é,

$$A_m = \text{ Área de } BPQC = c^2.$$

E por ABC ser retângulo:

$$A_T = \text{ Área do triângulo } ABC = \frac{a \cdot b}{2}.$$

Por outro lado, o quadrado $AMNK$ é a união do quadrado $BPQC$ com quatro triângulo de áreas iguais a $\frac{a \cdot b}{2}$. Onde

$$A_M = \text{ Área de } AMNK = (a+b)^2.$$

Por fim,

$$\begin{aligned} A_M = A_m + 4 \cdot A_T &\Leftrightarrow (a+b)^2 = c^2 + 4 \cdot \frac{ab}{2} \\ &\Leftrightarrow a^2 + 2ab + b^2 = c^2 + 2ab \\ &\Leftrightarrow a^2 + b^2 = c^2. \end{aligned}$$

■

Exemplo 3 *O Teorema de Sophie Germain diz que se p é um primo com $2p+1$ também primo e o $\text{mdc}(x,y,z) = 1$ e $p \nmid xyz$, então a equação,*

$$x^p + y^p = z^p$$

não terá solução inteira não trivial. O caso $n = 2$, equação pitagórica, não contradiz tal teorema. De fato, mesmo 2 sendo um primo de Sophie Germain a equação $a^2+b^2 = c^2$ com $\text{mdc}(a,b,c) = 1$, tem infinitas soluções como vimos em no Teorema 3.1.7. Um exemplo é a tripla $(3,4,5)$. E, isso não contradiz o teorema de Sophie Germain, por $2 \mid abc$. Vale salientar que, esse caso já é excluído no enunciado do teorema ao pedir $p > 2$.

3.3 Solução para $n = 3$

Agora, usaremos um processo criado por Fermat para mostrar a validade do caso $n = 3$. Esse processo é conhecido como *Método da Descida Infinita de Fermat*, que muitas vezes é bem útil para resolver equações nas quais as variáveis devem assumir apenas valores inteiros − equações diofantinas.

Para mostrar que a equação

$$x^3 + y^3 = z^3$$

não possui solução inteira não nula, usaremos uma demonstração publicada por Euler em 1770, em que ele usou as ideias deixadas por Fermat ao resolver um problema para saber se a área de um triângulo retângulo pode ser um quadrado de um número inteiro.

De acordo com [10] a esquematização desse processo consiste em:

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

ii. Concluir, a partir daí, que ela possui uma solução em inteiros não nulos que seja, em algum sentido, mínima.

iii. Deduzir a existência de uma solução em inteiros não nulos menor que a mínima (no sentido do item ii.), chegando, assim, a uma contradição.

Como na equação pitagórica podemos trabalhar apenas com o caso em que (x, y, z) é uma solução primitiva, ou seja, são coprimos dois a dois, pois se (a, b, c) é uma solução com $\text{mdc}(a, b, c) = d$, então

$$x^3 + y^3 = z^3 \Leftrightarrow \left(\frac{a}{d}\right)^3 + \left(\frac{b}{d}\right)^3 = \left(\frac{c}{d}\right)^3.$$

Logo, $\left(\frac{a}{d}, \frac{b}{d}, \frac{c}{d}\right)$ também seria uma solução. Assim, nos preocuparemos apenas com as soluções primitivas.

Além disso, os valores de $x, y, z \in \mathbb{Z}$ são diferentes, pois caso contrário:

Caso 1. Supondo $x = y$ teríamos

$$x^3 + y^3 = z^3 \Leftrightarrow 2x^3 = z^3 \Leftrightarrow 2 = m^3 \text{ para algum } m \in \mathbb{Z},$$

um absurdo.

Caso 2. Supondo $x = z$ teríamos

$$x^3 + y^3 = z^3 \Rightarrow z^3 + y^3 = z^3 \Rightarrow y^3 = 0 \Rightarrow y = 0.$$

E deveríamos ter, $y \neq 0$.

Os números $x, y, z \in \mathbb{Z}$ não podem ser todos pares pois, por hipótese, $\text{mdc}(x, y, z) = 1$.

Tal como não existe uma solução onde os três são ímpares, pois, se x e y forem ímpares os seus cubos também serão e a soma de ímpares é sempre um número par, o que é uma contradição. Se dois deles forem pares, a equação $x^3 + y^3 = z^3$ garante que o terceiro também deve ser par, e como já vimos isso não é possível para soluções primitivas. Restando a única opção onde dois deles serão ímpares e o terceiro será par. Sem perda de generalidade, podemos supor que x e y são ímpares e z é par.

Para evitar a lacuna deixada por Euler na demonstração original, devemos provar algumas propriedades pertinentes aos números p em que

$$p^3 = a^2 + 3b^2,$$

onde $a, b \in \mathbb{Z}$ com $\text{mdc}(a, b) = 1$.

Vale ressaltar a *Identidade de Fibonacci*, que para qualquer $N \in \mathbb{Z}$ temos

$$(a^2 + Nb^2)(c^2 + Nd^2) = (ac \pm Nbd)^2 + N(ad \mp bc)^2.$$

Particularmente, destacaremos o caso $N = 3$, como segue

$$(a^2 + 3b^2)(c^2 + 3d^2) = (ac \pm 3bd)^2 + 3(ad \mp bc)^2.$$

Note que o conjunto dos números da forma $a^2 + 3b^2$ é fechado para a multiplicação.

Lema 1 *Todo número primo p da forma $3k + 1$ divide algum inteiro da forma $a^2 + 3b^2$ com $\text{mdc}(a, b) = 1$.*

Demonstração: Tomemos a forma equivalente,

$$u^2 + uv + v^3,$$

com $u = b + a$ e $v = b - a$, pois

$$\begin{aligned} u^2 + uv + v^3 &= (b + a)^2 + (b + a)(b - a) + (b - a)^2 \\ &= (b^2 + 2ab + a^2) + (b^2 - a^2) + (b^2 - 2ab + a^2) \\ &= a^2 + 3b^2. \end{aligned}$$

Basta mostrar que $p = 3k + 1$ divide essa nova representação com $\text{mdc}(u, v) = 1$. Perceba que

$$u^{3k} - v^{3k} = (u^k - v^k)(u^{2k} + u^k v^k + v^{2k}).$$

Fazendo $v = 1$ garantimos que $\text{mdc}(u, v) = 1$ e teremos

$$u^{3k} - 1 = (u^k - 1)(u^{2k} + u^k + 1).$$

Pelo Pequeno Teorema de Fermat $p \mid (u^{p-1}-1) = (u^{3k}-1)$ sempre que $\text{mdc}(p,u) = 1$. Para que $p \nmid (u^{2k}+u^k+1)$ para cada um desses valores de u, é necessário que $p \mid (u^k-1)$ para todo $u \in \{1,2,3,\cdots,p-1\}$. No entanto a congruência

$$u^k = u^{\frac{p-1}{3}} \equiv 1(\text{mod p})$$

pode ter no máximo $\frac{p-1}{3}$ raízes distintas, ou seja, a congruência não é valida para os $\frac{2}{3}$ restantes e para cada um desses valores que $p \nmid (u^k-1)$. Devemos ter que $p \mid (u^{2k}+u^k+1)$ que é mais da metade dos valores de 1 até $p-1$. Assim, podemos escolher um número u, ímpar, e fazer,

$$a = \left(\frac{u-1}{2}\right) \text{ e } b = \left(\frac{u+1}{2}\right).$$

E com esses valores teremos que $\text{mdc}(a,b) = 1$ e que $p \mid (a^2+3b^2)$, encerrando a prova.

■

Lema 2 *Se um inteiro N é da forma a^2+3b^2 e se o número primo $p = c^2+3d^2$ divide N, então existem $u, v \in \mathbb{Z}$ com $N = p\cdot(u^2+3v^2) = (c^2+3d^2)(u^2+3v^2)$ e a representação de N pode ser dada aplicando a Identidade de Fibonacci.*

Demonstração: Como p divide N, então p também dividirá Nd^2-pb^2. Além disso,

$$\begin{aligned} Nd^2-pb^2 &= (a^2+3b^2)\cdot d^2-(c^2+3d^2)\cdot b^2 \\ &= a^2d^2+3b^2d^2-b^2c^2-3b^2d^2 \\ &= a^2d^2-b^2c^2 \\ &= (ad+bc)(ad-bc). \end{aligned}$$

Logo, p deve dividir $ad+bc$ ou $ad-bc$. Aplicando a Identidade de Fibonacci temos,

$$\begin{aligned} Np &= (a^2+3b^2)(c^2+3d^2) \\ &= (ac\pm 3bd)^2+3(ad\mp bc)^2. \end{aligned}$$

Dependendo se p dividir $ad+bc$ ou $ad-bc$ podemos escolher o sinal conveniente para que $p \mid (ad\mp bc)$ e como $p \mid Np$ também deve dividir $(ac\pm 3bd)^2$, logo

$$\frac{N}{p} = \left(\frac{ac\pm 3bd}{p}\right)^2 + 3\left(\frac{ad\mp bc}{p}\right)^2.$$

Fazendo

$$u = \frac{ac\pm 3bd}{p} \text{ e } v = \frac{ad\mp bc}{p},$$

teremos que $\frac{N}{p} = u^2 + 3v^2$. De sorte que,

$$\begin{aligned} uc + 3dv &= c \cdot \left(\frac{ac \pm 3bd}{p}\right) + 3d \cdot \left(\frac{ad \mp bc}{p}\right) \\ &= \left(\frac{ac^2 \pm 3bcd}{p}\right) + \left(\frac{3ad^2 \mp 3bcd}{p}\right) \\ &= \left(\frac{ac^2 \pm 3bcd + 3ad^2 \mp 3bcd}{p}\right) \\ &= \left(\frac{ac^2 + 3ad^2}{p}\right) \\ &= a \cdot \left(\frac{c^2 + 3d^2}{p}\right) \\ &= a \cdot \left(\frac{p}{p}\right) \\ &= a \end{aligned}$$

e

$$\begin{aligned} \pm(du - cv) &= \pm\left[d \cdot \left(\frac{ac \pm 3bd}{p}\right) - c \cdot \left(\frac{ad \mp bc}{p}\right)\right] \\ &= \pm\left[\left(\frac{acd \pm 3bd^2}{p}\right) - \left(\frac{acd \mp bc^2}{p}\right)\right] \\ &= \pm\left(\frac{acd \pm 3bd^2 - acd \pm bc^2}{p}\right) \\ &= \pm\left(\frac{\pm 3bd^2 \pm bc^2}{p}\right) \\ &= \pm(\pm b)\left(\frac{c^2 + 3d^2}{p}\right) \\ &= b \cdot \left(\frac{p}{p}\right) \\ &= b. \end{aligned}$$

Ou seja,

$$\begin{cases} a = uc + 3dv, \\ b = \pm(du - cv). \end{cases}$$

Temos assim, que a representação de N é dada pela aplicação da Identidade de Fibonacci na multiplicação

$$N = p \cdot \frac{N}{p} = (c^2 + 3d^2)(u^2 + 3v^2),$$

o que encerra a prova. ■

Lema 3 *Se um número inteiro N pode ser representado na forma $a^2 + 3b^2$ com $a, b \in \mathbb{Z}$ e $\text{mdc}(a, b) = 1$, então os fatores primos ímpares de N são da forma $p = 3k + 1$.*

Demonstração: Se $p \mid (a^2 + 3b^2)$, então devemos ter que, $a^2 \equiv -3b^2 (\text{mod } p)$. Além disso, $p \nmid a$ e $p \nmid b$, pois $\text{mdc}(a, b) = 1$. Pelas propriedades do símbolo de Legendre, temos:

1. $\left[\frac{a^2}{p}\right] = \left[\frac{-3b^2}{p}\right]$;
2. $\left[\frac{a^2}{p}\right] = 1$;
3. $\left[\frac{b^2}{p}\right] = 1$;
4. $\left[\frac{-3b^2}{p}\right] = \left[\frac{-3}{p}\right]\left[\frac{b^2}{p}\right]$.

Consequentemente,

$$\left[\frac{-3}{p}\right] = 1.$$

Implicando que -3 é um resíduo quadrático módulo p. Como

$$\left[\frac{-1}{p}\right] = (-1)^{(p-1)/2},$$

e pela teorema da reciprocidade quadrática temos,

$$\left[\frac{3}{p}\right]\left[\frac{p}{3}\right] = (-1)^{(p-1)/2} \Rightarrow \left[\frac{3}{p}\right] = \left[\frac{p}{3}\right](-1)^{(p-1)/2}.$$

Portanto,

$$1 = \left[\frac{-3}{p}\right] = \left[\frac{3}{p}\right]\left[\frac{-1}{p}\right] = \left[\frac{p}{3}\right] = \left[\frac{1}{3}\right],$$

nos dando, $p \equiv 1 (\text{mod } 3)$, ou seja, $p = 3k + 1$. ■

Lema 4 *Todo número primo p da forma $3k+1$ pode ser expresso na forma $a^2 + 3b^2$ com $\text{mdc}(a, b) = 1$ de uma única maneira.*

Demonstração: Pelo Lema 1, sabemos que p divide algum número da forma $a^2 + 3b^2$ e substituindo a e b pelos seus respectivos restos módulo p, o resultado ainda será divisível por p, mas agora cada um é menor ou igual a $\frac{p-1}{2}$ e assim,

$$a^2 + 3b^2 \leq \left(\frac{p-1}{2}\right)^2 + 3\left(\frac{p-1}{2}\right)^2 = 4 \cdot \frac{(p-1)^2}{4} = (p-1)^2 < p^2.$$

Portanto, todos os divisores de $a^3 + 3b^2$ são estritamente menores do que p exceto o p. Pelo Lema 3 todos esses divisores são da forma $3k + 1$. Como, cada divisor deve ser da forma $u^2 + 3v^2$, podemos aplicar o Lema 2 para cada um desses pequenos divisores primos e retornar, formando um quociente único da forma $a^2 + 3b^2$ até chegar ao p, completando a prova. ■

Lema 5 *Todas as soluções inteiras e primitivas da equação*

$$x^2 + 3y^2 = N^3,$$

para N ímpar e $\text{mdc}(x, y) = 1$*, são dadas por*

$$\begin{cases} x = u(u^2 - 9v^2), \\ y = 3v(u^2 - v^2), \\ N = u^2 + 3v^2. \end{cases}$$

com u e v com paridades distintas e $\text{mdc}(u, v) = 1$.

Demonstração: Todos os divisores p primos de $x^2 + 3y^2 = N^3$ devem ser ímpares, já que N é ímpar. Logo, pelo Lema 3 são todos da forma $p = 3k + 1$ com $k \in \mathbb{N}$. Pelo Lema 4, esses representantes são escritos de forma única como $p = r^2 + 3s^2$, para $r, s \in \mathbb{Z}$ e $\text{mdc}(r, s) = 1$. Assim, basta fazer $x^2 + 3y^2 = N^3 = (u^2 + 3v^2)^3$ e encontrar os valores de x e y. Aplicando a identidade de Fibonacci, temos:

$$\begin{aligned} x^2 + 3y^2 &= N^3 \\ &= [(u^2 + 3v^2) \cdot (u^2 + 3v^2)] \cdot (u^2 + 3v^2) \\ &= [(u^2 - 3v^2)^2 + 3(uv)^2] \cdot (u^2 + 3v^2) \\ &= [u(u^2 - 3v^2) - 3v(2uv)]^2 + 3[u \cdot 2uv + v(u^2 - 3v^2)]^2 \\ &= [u^3 - 3uv^2 - 6uv^2]^2 + 3[2u^2v + u^2v - 3v^3]^2 \\ &= [\underbrace{u(u^2 - 9v^2)}_{x}]^2 + 3[\underbrace{3v(u^2 - v^2)}_{y}]^2. \end{aligned}$$

Ou seja,

$$\begin{cases} x = u(u^2 - 9v^2), \\ y = 3v(u^2 - v^2). \end{cases}$$

Note que, se u e v tivessem a mesma paridade, $N = u^2 + 3v^2$ seria um número par, um absurdo. Se $\text{mdc}(u, v) = d$, temos que,

$$d \mid u \text{ e } d \mid v \Rightarrow d \mid x \text{ e } d \mid y \Rightarrow d \mid \text{mdc}(x, y) = 1 \Rightarrow \text{mdc}(u, v) = 1.$$

Concluindo a demostração. ■

Agora temos ferramentas suficientes para resolver nosso equação fermatiana de grau 3.

Proposição 3.1.4 (Euler) *A equação*

$$x^3 + y^3 = z^3$$

não possui solução inteira não trivial.

Demonstração: Suponhamos que exista alguma solução e que essa seja mínima no sentido que $|z|$ é o menor possível. Como x e y são ímpares, existem $u, v \in \mathbb{Z}$ com paridades distintas e $\text{mdc}(u, v) = 1$ e

$$\begin{cases} x = u + v, \\ y = u - v. \end{cases}$$

Fazendo a substituição, temos

$$\begin{aligned} z^3 &= x^3 + y^3 \\ &= (u+v)^3 + (u-v)^3 \\ &= (u^3 + 3u^2v + 3uv^2 + v^3) + (u^3 - 3u^2v + 3uv^2 - v^3) \\ &= 2u^3 + 6uv^2 \\ &= (2u)(u^2 + 3v^2). \end{aligned}$$

Aqui já começa a fazer sentido o motivo de tanto estudo sobre os número da forma a^2+3b^2.

Uma vez que z é par, teremos que u deve ser par e v deve ser ímpar.
Perceba que se $\text{mdc}(2u, u^2 + 3v^2) = d$, como $d \mid (u^2 + 3v^2)$ teremos que $\text{mdc}(2, d) = 1$. Por outro lado, $d \mid 2u$ e isso implica que $d \mid u$, ou seja, $d \mid 3v^2$ temos assim, dois casos a considerar:

Caso i) Se tivermos que $d \mid v$, teremos que

$$d \mid \text{mdc}(u, v) = 1 \Rightarrow d = 1.$$

Caso ii) Se tivermos que $d \nmid v$, nos resta que

$$d \mid 3 \Rightarrow d = 1 \text{ ou } d = 3.$$

Concluímos que as únicas opções são $d = 1$ ou $d = 3$. Vamos analisar esses casos de forma isolada:

Caso 1: $\text{mdc}(2u, u^2 + 3v^2) = 1$
Como o produto deles resulta em um cubo (z^3), então cada um também deve ser um

cubo, ou seja, existem números $m, n \in \mathbb{Z}$ com

$$\begin{cases} u = 4m^3, \\ u^2 + 3v^2 = n^3. \end{cases}$$

Como n^3 é ímpar, n também deve ser. Pelo Lema 5, devem existir números inteiros r, s com

$$\begin{cases} u = r(r^2 - 9s^2) = r(r - 3s)(r + 3s), \\ v = 3s(r^2 - s^2) = 3s(r - s)(r + s). \end{cases}$$

Onde r e s têm paridades distintas e $\text{mdc}(r, s) = 1$. Como v é ímpar e u é par, devemos ter que s é ímpar e r é par. Como $u = 4m^3$ e $(r - 3s)$ e $(r + 3s)$ são ambos ímpares e primos entre si, devem existir inteiros não nulos A, B e C. Com,

$$\begin{cases} r = 4A^3, \\ r - 3s = B^3, \\ r + s = C^3. \end{cases}$$

Além disso,

$$2r = (r - 3s) + (r + 3s) \Rightarrow 2 \cdot 4A^3 = B^3 + C^3 \Rightarrow (2A)^3 = B^3 + C^3.$$

Logo, $(B, C, 2A)$ também é uma solução para a equação inicial, mas por outro lado aplicando o modulo em ambos os membros de $z^3 = 2u(u^2 + 3v^2)$, temos,

$$\begin{aligned} |z^3| &= |2u(u^2 + 3v^2)| \\ &= |2r(r^2 - 9s^2)(u^2 + 3v^2)| \\ &= |2r(r - 3s)(r + 3s)(u^2 + 3v^2)| \\ &= |(2A)^3| \cdot |\underbrace{B^3C^3}_{>1}| \cdot |\underbrace{(u^2 + 3v^2)}_{>1}| \\ &> |(2A)^3|. \end{aligned}$$

E assim, teríamos que $|z| > |2A|$, um absurdo por contrariar a hipótese de $|z|$ ser mínimo, o que implica pela Método da Descida Infinita de Fermat que se $\text{mdc}(2u, u^2 + 3v^2) = 1$ não teremos soluções inteiras não nulas.

Caso 2: $\text{mdc}(2u, u^2 + 3v^2) = 3$.

Nesse caso temos que $3 \mid z$ e $3 \mid u$, mas $3 \nmid v$ (se dividisse o $\text{mdc}(2u, u^2 + 3v^2)$ seria 9),

logo:

$$\begin{aligned} z^3 &= 2u(u^2+3v^3) \\ &= 6u\left[3\left(\frac{u}{3}\right)^2+v^2\right]. \end{aligned}$$

Como mdc $\left(6u, 3\left(\frac{u}{3}\right)^2+v^2\right)=1$, devem existir $m,n\in\mathbb{Z}$ com

$$\begin{cases} u = 36m^3, \\ 3\left(\frac{u}{3}\right)^2+v^2 = n^3. \end{cases}$$

Como n é ímpar, pelo Lema 5 existem $r,s\in\mathbb{Z}$ primos entre si e com s um número par, com

$$\begin{cases} v = r(r^2-9s^2) = r(r-3s)(r+3s), \\ \frac{u}{3} = 3s(r^2-s^2) = 3s(r+s)(r-s). \end{cases}$$

Temos que,

$$\begin{aligned} \frac{u}{3} = 3s(r+s)(r-s) &\Rightarrow u = 9s(r+s)(r-s) \\ &\Rightarrow 36m^3 = 9s(r+s)(r-s) \\ &\Rightarrow 4m^3 = s(r+s)(r-s). \end{aligned}$$

Consequentemente, devem existir $A,B,C\in\mathbb{Z}$ não nulos com,

$$\begin{cases} s = 4A^3, \\ r+s = B^3, \\ r-s = C^3. \end{cases}$$

Assim,

$$(2s)+(r-s)=(r+s)\Rightarrow(2\cdot 4A^3)+C^3=B^3\Rightarrow(2A)^3+C^3=B^3.$$

Teríamos que, $(2A,C,B)$ é uma solução para a equação com,

$$\begin{aligned} |z^3| &= |2u(u^2+3v^2)| \\ &= |18s(r+s)(r-s)(u^2+3v^2)| \\ &= |18\cdot 4A^3\cdot B^3\cdot C^3(u^2+3v^2)| \\ &= |B^3|\cdot\underbrace{|18\cdot 4A^3\cdot C^3|}_{>1}\cdot\underbrace{|(u^2+3v^2)|}_{>1} \\ &= |B^3|. \end{aligned}$$

Consequentemente, temos que, $|z| > |B|$, um absurdo por contrariar a hipótese de $|z|$ ser mínimo, o que implica pelo Método da Descida Infinita de Fermat que se $\text{mdc}(2u, u^2 + 3v^2) = 3$, não teremos soluções inteiras não nulas.

Como os únicos dois casos possíveis não tem solução inteira não nula, nos resta que a equação geral não têm solução inteira não nula, encerrando a prova.

■

Devemos observar o seguinte,

$$x^{3k} + y^{3k} = z^{3k} \Leftrightarrow (x^k)^3 + (y^k)^3 = (z^k)^3.$$

Para todo $k \in \mathbb{N}$, como mostramos que a equação depois da equivalência não tem solução inteira não nula, então tem-se que a equação antes da equivalência também não terá. E finalmente, podemos afirmar que para todo $n = 3k$ com $k \in \mathbb{N}$ a equação

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

não tem solução inteira não nula. Encerrando assim o caso $n = 3$.

3.4 Solução para $n = 4$

Agora, iremos mostrar, usando o mesmo Método da Descida Infinita de Fermat, que ele estava certo ao afirmar que a equação

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

não tem solução não trivial sempre que esse n é um múltiplo de 4, ou seja, $n = 4k$ onde $k \in \mathbb{N}$. Apresentaremos mais uma prova que é de autoria de Euler e que foi publicada pela primeira vez em 1747.

Inicialmente perceba que, para não ter solução inteira para qualquer expoente múltiplo de 4 é necessário e suficiente mostrar apenas o caso $n = 4$. Veja, se $k \in \mathbb{N}$ e

$$x^4 + y^4 = z^4$$

não tem solução inteira não trivial, então

$$x^{4k} + y^{4k} = z^{4k} \Leftrightarrow (x^k)^4 + (y^k)^4 = (z^k)^4$$

também não terá. Reciprocamente, se a equação não tem solução inteira não trivial para todos os múltiplos de 4, então em particular não terá para o próprio 4 já que todo número é múltiplo dele mesmo. Para tal, provaremos inicialmente um lema em que o

nosso problema será uma consequência imediata.

Lema 6 (Euler) *A equação*

$$x^4 + y^4 = z^2$$

não possui solução inteira não trivial.

Demonstração: Suponhamos que a equação tenha alguma solução inteira não trivial, ou seja, existem $a, b, c \in \mathbb{N}$ tais que

$$a^4 + b^4 = c^2,$$

Para usar o Método da Descida Infinita devemos supor que (a, b, c) é uma solução mínima em algum sentido, assim podemos supor que (a, b, c) é uma solução tal que c seja mínimo. Como c é mínimo, podemos supor que $\text{mdc}(a, b) = 1$ e, consequentemente teremos $\text{mdc}(a^2, b^2) = 1$. Pois, caso contrário existiria um $d \in \mathbb{N}$ com $\text{mdc}(a, b) = d \neq 1$ e isso nos daria que

$$\begin{aligned} d \mid a \text{ e } d \mid b &\Rightarrow d^4 \mid a^4 \text{ e } d^4 \mid b^4 \\ &\Rightarrow d^4 \mid (a^4 + b^4) = c^2 \\ &\Rightarrow d^4 \mid c^2 \\ &\Rightarrow d^2 \mid c. \end{aligned}$$

Assim,

$$\left(\frac{a}{d}\right)^4 + \left(\frac{b}{d}\right)^4 = \left(\frac{c}{d^2}\right)^2.$$

Logo a tripla $\left(\frac{a}{d}, \frac{b}{d}, \frac{c}{d^2}\right)$ seria uma solução para a equação dada com

$$\frac{c}{d^2} < c,$$

gerando um absurdo por contrariar a minimalidade de c. Consequentemente, devemos ter $\text{mdc}(a^2, b^2) = 1$. Além disso,

$$(a^2)^2 + (b^2)^2 = c^2,$$

mostrando que (a^2, b^2, c) é uma tripla pitágorica primitiva e pelo Teorema 3.1.7, temos que existem $u, v \in \mathbb{Z}$ com $\text{mdc}(u, v) = 1$ e de paridades distintas, tais que

$$\begin{cases} a^2 = v^2 - u^2, \\ b^2 = 2uv, \\ c = v^2 + u^2. \end{cases}$$

Como $a^2 + u^2 = v^2$, novamente pelo Teorema 3.1.7, existem $j, p \in \mathbb{Z}$ com $\text{mdc}(j, p) = 1$ e de paridades distintas, tais que

$$\begin{cases} a = p^2 - j^2, \\ u = 2jp, \\ v = p^2 + j^2. \end{cases}$$

Ou seja,

$$b^2 = 2uv = 4jp(p^2 + j^2).$$

Como o $\text{mdc}(j, p) = 1$, temos que $\text{mdc}(j, j^2 + p^2) = 1$ e $\text{mdc}(p, j^2 + p^2) = 1$ implicando que $\text{mdc}(jp, j^2 + p^2) = 1$. Devemos ter que j, p e $j^2 + p^2$ devem ser quadrados perfeitos, ou seja, devem existir $l, m, n \in \mathbb{Z}$, tais que

$$\begin{cases} j = l^2, \\ p = m^2, \\ j^2 + p^2 = n^2. \end{cases}$$

E assim,

$$l^4 + m^4 = (l^2)^2 + (m^2)^2 = j^2 + p^2 = n^2,$$

com

$$n \leq n^2 = j^2 + p^2 = v < v^2 + u^2 = c \Rightarrow n < c.$$

Como (l, m, n) seria uma solução para $x^4 + y^4 = z^2$ com $n < c$, temos um absurdo.

Portanto concluímos que a equação $x^4 + y^4 = z^2$ não pode ter solução inteira não nula. ■

Teorema 3.1.8 (Fermat/Euler) *A equação*

$$x^4 + y^4 = z^4$$

não possui solução inteira não trivial.

Demonstração: Note que,

$$x^4 + y^4 = z^4 \Leftrightarrow x^4 + y^4 = (z^2)^2.$$

Como a segunda não tem solução inteira não trivial, implica que a primeira também não tem. Encerrando a demonstração. ■

Corolário 3.1.1 *A equação*

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

não possui solução inteira não trivial sempre que $n = 4k$ para algum $k \in \mathbb{N}$.

Demonstração: De fato, a falta de solução inteira não trivial para essa equação com expoente múltiplo de 4 é uma consequência direta do caso $n = 4$ que foi provado no Teorema 3.1.8. ■

Um problema interessante é sobre a irracionalidade de $\sqrt[n]{2}$. Mas como só provamos a validade do Último Teorema de Fermat para os casos n é um múltiplo de 3 ou de 4, vamos nos limitar a eles.

Problema 1 *Mostre que $\sqrt[n]{2}$ sempre é um número irracional quando n for um múltiplo de 3 ou 4.*

Solução: Comecemos supondo que $\sqrt[n]{2}$ seja um número racional, ou seja, existem $r, s \in \mathbb{Z}$ com $s \neq 0$ tais que

$$\sqrt[n]{2} = \frac{r}{s},$$

assim,

$$\left(\frac{r}{s}\right)^n = 2 \Leftrightarrow r^n = 2s^n \Leftrightarrow r^n = s^n + s^n.$$

E como já sabemos, a última equação não tem solução, consequentemente a primeira também não pode ter, implicando que não existem tais $r, s \in \mathbb{Z}$. Ou seja, $\sqrt[n]{2}$ é irracional para todo n múltiplo de 3 ou 4. ◇

3.5 Uma pequena aposta

Sabendo sobre o Último Teorema de Fermat apenas o que foi exposto aqui, você se arriscaria em uma aposta sobre a validade ou não da celebre afirmação de Fermat?

Para encerrar o Capítulo, mostraremos que, de acordo com o que vimos, a probabilidade de Fermat estar certo é maior do que 50%, ou seja, mais do que um para dois. O que é muito animador, visto que só provamos o primeiro caso (Sophie Germain) e os casos $n = 3$ e $n = 4$, mas não devemos esquecer que na Matemática uma coisa só é verdade depois que forem provados todos os casos. Como na analogia feita na "historinha" de Ian Stewart no livro Conceitos de Matemática Moderna:

> "Um astrônomo, um físico e um matemático estavam passando férias na Escócia. Olhando pela janela do trem eles avistaram uma ovelha preta no meio de um campo. 'Que interessante', observou o astrônomo, 'na Escócia todas as ovelhas são pretas.' Ao que o físico respondeu: 'Não, nada disso! Algumas ovelhas escocesas são pretas.' O matemático olhou para cima em desespero e disse: 'Na Escócia existe pelo menos um campo, contendo pelo menos uma ovelha e pelo menos um lado dela é preto.' "

Para dar início a nossa questão de probabilidade devemos, primeiramente, responder algumas perguntas que irão nos auxiliar na busca pelas respostas procuradas.

Exemplo 4 *Qual a probabilidade de ao escolhermos um número natural, ao acaso, e ele ser um múltiplo de 3?*

Solução: Devemos pensar inicialmente em dividir os números naturais em três grupos que iremos chamar de caixas, veja a figura 4:

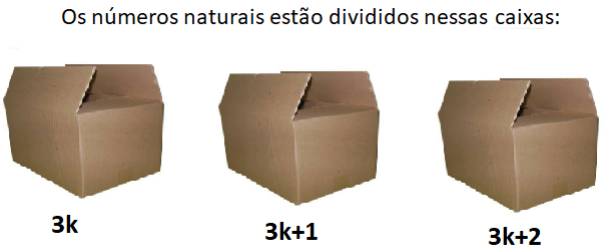

Figura 4: Dividir em três caixas.

Se os números naturais podem ser divididos entre os números que são da forma ou $3k$ ou $3k+1$ ou $3k+2$, onde a interseção é vazia, pois não existe um número que seja múltiplo de três (da forma $3k$) e que não seja (das formas $3k+1$ ou $3k+2$) ao mesmo tempo. De posso disso, a probabilidade pedida dever ser um terço visto que dos três casos apenas um é do nosso interesse, assim

$$P(A) = \frac{1}{3}.$$

onde $A = \{x \in \mathbb{N}; x = 3k, k \in \mathbb{N}\}$.

◇

Exemplo 5 *Qual a probabilidade de ao escolhermos um número natural, ao acaso, e ele ser um múltiplo de 4?*

Solução: De modo análogo ao caso anterior, mostra-se que

$$P(B) = \frac{1}{4}.$$

onde $B = \{x \in \mathbb{N}; x = 4q, q \in \mathbb{N}\}$. ◇

Exemplo 6 *Qual a probabilidade de ao escolhermos um número natural, ao acaso, e ele ser um múltiplo de 12?*

Solução: Como $\text{mdc}(3, 4) = 1$, temos que para um número ser múltiplo de 12 ele deve

ser múltiplo de 3 e de 4 ao mesmo tempo e por serem eventos independentes, temos

$$\begin{aligned} P(C) &= P(A \cap B) \\ &= P(A) \cdot P(B) \\ &= \left(\frac{1}{3}\right) \cdot \left(\frac{1}{4}\right) \\ &= \frac{1}{12}. \end{aligned}$$

Onde $C = \{x \in \mathbb{N}; x = 12p, p \in \mathbb{N}\}$. ◇

Agora, podemos responder qual a probabilidade de Fermat estar certo sabendo apenas os casos $n = 3$ e $n = 4$.

Problema 2 *Sabendo a validade do Último Teorema de Fermat para os múltiplos de 3 e para os múltiplos de 4, qual a probabilidade de escolher um número natural ao acaso e o teorema ser valido para esse número?*

Solução:

Para que o teorema seja válido teremos que escolher um número que seja múltiplo de 3 ou de 4, e essa probabilidade é:

$$\begin{aligned} P(D) &= P(A \cup B) \\ &= P(A) + P(B) - P(A \cap B) \\ &= \left(\frac{1}{3}\right) + \left(\frac{1}{4}\right) - \left(\frac{1}{12}\right) \\ &= \left(\frac{4}{12}\right) + \left(\frac{3}{12}\right) - \left(\frac{1}{12}\right) \\ &= \left(\frac{6}{12}\right) = \frac{1}{2}. \end{aligned}$$

Ou seja, a probabilidade é 50 %. ◇

A Figura 5 nos dá a ideia de que realmente deveremos ter metade dos números sendo múltiplos de 3 ou 4. Observe que o padrão exposto nela continuará por todo o conjunto dos números naturais.

1	2	3	4	5	6	7	8	9	10	11	12
13	14	15	16	17	18	19	20	21	22	23	24
25	26	27	28	29	30	31	32	33	34	35	36
37	38	39	40	41	42	43	44	45	46	47	48
49	50	51	52	53	54	55	56	57	58	59	60

Figura 5: Múltiplos positivos de 3 ou 4 menores do que 61.

Fermat poderia facilmente saber disso, já que Probabilidade era um dos ramos que ele gostava de trabalhar em seus estudos. Um pouco além disso, ainda mostramos que o teorema de Sophie Germain vale para alguns casos especiais de primos, e como os múltiplos de 3 e de 4 são sempre compostos, com exceção do 3 que é o único primo. Podemos finalizar dizendo que a probabilidade de Fermat estar certo é maior do que 50%.

"Acho que vou parar por aqui."

4 CONSIDERAÇÕES FINAIS

Neste trabalho, foi contada uma breve história sobre o Último Teorema de Fermat e sobre alguns personagens que se empenharam em descobrir uma demonstração para o que até então era uma "simples" conjectura, o que nos possibilitou entender um pouco do contexto e das limitações que esses matemáticos tiveram que enfrentar. Em seguida, provamos o Teorema de Sophie Germain, conhecido como "o primeiro caso", nos dando algumas situações em que o teorema é verdadeiro e relacionamos os números de Sophie Germain com os números de Mersenne. Mostramos propriedades algébricas e geométricas da equação

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

Também foi provado a validade do Último Teorema de Fermat para os expoentes que são múltiplos de 3 ou de 4. Por fim, usamos propriedades de Probabilidade em conjuntos infinitos para mostrar que Fermat, só com esses três casos, teria mais de 50% de chance de estar certo.

Todo esse trabalho nos faz perceber que mesmo os problemas mais simples podem nos trazer surpresas ao tentar desvendá-los e ao buscar resolvê-los. Perceba que a equação

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

é tão simples em sua composição e que não foi fácil conseguir resultados suficientes para garantir que a mesma não terá solução no conjunto dos números inteiros positivos, mesmo que, às vezes, tenhamos usado algumas ferramentas um pouco mais avançadas de Teoria dos Números.

Apesar de termos provado que a probabilidade de Fermat estar certo ao afirmar que não teremos soluções sempre que $n \in \mathbb{N}_{>2}$ é maior do que 50%, mostrar a validade de mais alguns outros casos é uma sugestão para pesquisas futuras. Como, por exemplo, quando n é um múltiplo de 5 ou de qualquer outro número primo maior do que 3. Vale ressaltar que haverá um ganho substancial na complexidade de tal demonstração, principalmente, nas ferramentas necessárias para chegar ao objetivo.

O que não poderíamos deixar de sugerir como uma continuação da pesquisa é a busca por uma solução simples e maravilhosa para o problema central deste trabalho e mesmo que não caiba na margem de uma folha, que seja simples. Fazendo com que a celebre frase de Fermat continue seu legado.

Neste trabalho, ao mostrarmos alguns casos do Último Teorema de Fermat, tentamos fazê-lo da forma mais básica possível para introduzir algumas propriedades interessantes com o intuito de que possam servir como fonte de pesquisa para professores e alunos do Ensino Médio. Esperamos que quando os alunos, que venham ter contato com

esse texto, consigam entendê-lo e possam perceber que a Matemática não é apenas números e repetições, mas também anseia por tempo, ideias e pensamentos. Com isso, venha ser um cartão de visitas a essa ciência tão maravilhosa, e que acabe gerando interesses pela busca de novos conhecimentos.

Encerramos este trabalho, com a plena certeza de que disponibilizamos um material plausível de ser consultado por todos aqueles interessados em conhecer uma breve apresentação sobre o Último Teorema de Fermat e sua importância para a história da Matemática.

REFERÊNCIAS

[1] BRUNO, S. S. **O Último Teorema de Fermat para n=3**. 2014. 86 p. Dissertação (Mestrado em Ensino de Matemática) - PROFMAT, UNIRIO, Rio de Janeiro.

[2] COSTA, T. J. M. B. **Os Números Perfeitos e os Primos de Mersenne**. 2015. 65 p. Dissertação (Mestrado em Matemática para Professores) - Universidade de Lisboa, Lisboa.

[3] **Descoberto número primo com quase 25 milhões de dígitos**. IMPA. Diponível em: https://impa.br/page-noticias/descoberto-numero-primo-com-quase-25-milhoes-de-digitos/. Acesso em: 19 fev. 2019.

[4] **Fermat's Last Theorem for Cubes**. Math Pages. Diponível em: https://www.mathpages.com/home/kmath009/kmath009.htm. Acesso em: 19 fev. 2019.

[5] HEFEZ, A. **Aritmética**. Coleção PROFMAT. SBM, 2016.

[6] LIMA, E. L. et al. **A matemática do ensino médio** vol. 2. 6^a edição Rio de janeiro: SBM, 2006.

[7] MARTINEZ, F. B. et al. **Teoria dos Números: Um passeio com primos e outros números familiares pelo mundo inteiro**. 4^a edição. Rio de Janeiro: IMPA, 2015.

[8] MOREIRA, C. G. T. de A et al. . **Tópicos de teoria dos números**. Coleção PROFMAT. 1 ed. Rio de Janeiro: SBM, 2012.

[9] MORGADO, A. C. et al. **Análise combinatória e probabilidade**. 9^a edição Rio de Janeiro: SBM, 2006.

[10] NETO, A. C. M. **Tópicos de Matemática Elementar**, Vol. 5. 1^a edição. Sociedade Brasileira de Matemática, 2012.

[11] RIBENBOIM, P. **Números Primos. Velhos mistérios e novos recordes**. 1^a edição. Rio de Janeiro: IMPA, 2014.

[12] RIBENBOIM, P. **Seis Décadas de Matemática**. Matemática Universitária, n. 45, p 20-43, 18 ago. 2009. Entrevista cedida a Alberto de Azevedo (UnB), Eduardo Colli (IME/USP) e Severino Toscano Melo (IME/USP). Disponível em: https://rmu.sbm.org.br/wp-content/uploads/sites/27/2018/03/n45_Entrevista.pdf. Acesso em: 19 fev. 2019.

[13] SHOUP, V. **A Computational Introduction to Number Theory and Algebra**. 2^a edição. Cambridge University Press, 2008. Disponível em: https://shoup.net/ntb/ntb-v2.pdf. Acesso em: 19 fev. 2019.

[14] SINGH, S. **O Último Teorema de Fermat**. Record, 2014.