

CONCEITOS INICIAIS PARA A DEMONSTRAÇÃO DO ÚLTIMO TEOREMA DE FERMAT

Mateus Vinicius Fernandes Kojunski
Suellen Aparecida Greatti Vieira

Resumo

Pierre de Fermat foi um jurista francês que viveu no século XVII e, mesmo não sendo matemático de formação ou profissão, contribuiu significativamente para a ciência moderna, legando avanços na Teoria dos Números, na Teoria da Probabilidade e em fundamentos que auxiliaram na posterior criação do Cálculo Diferencial e Integral. Dentre suas contribuições, uma anotação informal nas bordas de um livro tornou-se célebre, culminando em uma busca de mais de três séculos por respostas: o enunciado do Último Teorema de Fermat. Nesse contexto, esta pesquisa se propõe a analisar e expor os conceitos iniciais da demonstração desse teorema, desenvolvida por Andrew Wiles e com contribuições de Richard Taylor, explorando os aspectos históricos e matemáticos do período em que o problema permaneceu sem solução, além de destacar seu impacto no desenvolvimento da matemática até a sua publicação em 1995. Desse modo, o trabalho busca compreender tópicos essenciais de Álgebra Moderna necessários para a introdução da estrutura da prova de Wiles-Taylor, concentrando-se no estudo de noções fundamentais de grupos, anéis e corpos.

Palavras-chave: Último Teorema de Fermat. História da Matemática. Estruturas Algébricas. Álgebra Moderna.

1. INTRODUÇÃO

No decorrer da história da matemática, houve muitos nomes que se destacaram, seja por grandes descobertas e formulações ou até mesmo pela proposição de desafios intrigantes. Um deles foi Pierre de Fermat e seu teorema conhecido como o “Último Teorema de Fermat”, que movimentou a comunidade acadêmica durante mais de três séculos.

Fermat foi um magistrado e matemático francês que viveu no século XVII. Ele ficou conhecido como o “Príncipe dos Amadores” pois, apesar de seu exímio conhecimento matemático, não exercia tal atividade como profissão. Filho de um rico mercador de peles, Fermat teve acesso a uma educação privilegiada no monastério franciscano de Grandselve, e logo após, estudou na Universidade de Toulouse.

Ele trabalhou em vários campos da matemática, como na criação da Teoria da Probabilidade, juntamente com Pascal, e formulando as bases que foram utilizadas por Isaac Newton para o desenvolvimento do Cálculo Diferencial e Integral. No entanto, o que realmente chamava a atenção de Fermat era a Teoria dos Números (TN). Ele dedicou bastante tempo de seus estudos a essa área,

sendo considerado um dos fundadores da Teoria dos Números Moderna.

Durante suas sessões de estudo sobre a TN, utilizando o livro “Aritmética” do matemático Diofanto de Alexandria, ele fundamentou uma conjectura derivada do conhecido Teorema de Pitágoras, deixando uma pequena anotação nas bordas de uma das páginas do livro, onde em latim dizia:

É impossível decompor um cubo em dois cubos, um biquadrado em dois biquadrados e, de um modo geral, qualquer potência acima de dois na soma de duas potências de igual expoente. Para isso, eu descobri uma demonstração verdadeiramente maravilhosa, mas a margem é pequena demais para contê-la (Cardoso, 2020, p. 13).

Com este texto, ele afirma que não existem inteiros não nulos a , b , e c que satisfaçam a equação $a^n + b^n = c^n$ para qualquer inteiro $n \geq 3$, cuja afirmação é conhecida como Último Teorema de Fermat.

Infelizmente, ele faleceu em 1665, sem apresentar sua demonstração e, mesmo após sua morte, ela não foi encontrada em nenhuma das anotações e documentos do acervo de Fermat. Com tal problema, que tem um enunciado considerado de fácil entendimento, Fermat desafiou as maiores mentes matemáticas do mundo, criando uma verdadeira corrida - onde a linha de chegada era a demonstração final do teorema - que somente foi alcançada em 1995 pelo matemático Andrew Wiles com colaboração de Richard Taylor.

Figura 1 - Pierre de Fermat, 1601-1665



Fonte: Imagem retirada da internet

No decorrer desse trajeto para chegar até a obtenção da prova final, a conjectura impulsionou expressivamente a construção e evolução da matemática, fazendo com que fossem descobertas, criadas e desenvolvidas muitas áreas, como a própria Teoria dos Números, a Álgebra Moderna e até mesmo os primeiros usos da unidade imaginária, $i^2 = -1$. Este trabalho busca adentrar os aspectos matemáticos da demonstração Wiles-Taylor para o UTF, focando em fundamentos da Álgebra Moderna. Espera-se compreender definições e proposições que são necessárias ao entendimento do teorema proposto por Pierre de Fermat, concentrando-se, neste momento, nas estruturas de grupos, anéis e corpos.

2. REFERENCIAL TEÓRICO

A demonstração do UTF trouxe bastante notoriedade para a Matemática. Sobre sua importância, destaca-se que:

A exposição desta conjectura proporcionou uma maior atratividade à matemática, visto que o enunciado dado por Fermat é pequeno e de simples compreensão. Todavia, a apresentação de uma prova geral ou de um contraexemplo para o enunciado cada vez mais se estabelecia como uma tarefa bastante árdua e de grande complexidade (Cardoso, 2020, p.14).

Cardoso (2020) ainda traça uma linha do tempo destacando os principais nomes envolvidos nas provas das “Equações Fermatianas”, como segue:

Fermat enunciou a conjectura em 1637 e, por volta de 1640, esboçou a prova para o caso do expoente $n = 4$, apresentando uma importante técnica de demonstração por contradição, conhecida, na literatura, como Método da Descida Infinita de Fermat, que consiste em uma “descida infinita” de soluções naturais. Pode ser aplicada também nos casos $n = 3$ e 5 .

Samuel de Fermat publicou, por volta de 1670, uma edição do livro Aritmética de Diofanto com as anotações do seu pai.

Apenas em 1770, foi publicado o trabalho de Leonhard Euler do caso $n = 3$ (Equação Fermatiana Cúbica), no qual se aplicou o conceito do número imaginário $i = \sqrt{-1}$ na fatoração. Para o aprofundamento da prova, estudaram-se os Anéis Eisenstein. Destaca-se ainda que Euler verificou “algumas pistas” nas anotações de Fermat sobre a ideia da “descida infinita”, método que não era de fácil extrapolação.

Em 1823, Sophie Germain propôs um teorema auxiliar ao Último Teorema de Fermat, dividido em dois casos. Relaciona a divisibilidade das ternas de inteiros a certos expoentes primos (primos de Germain). Os trabalhos de Germain foram importantes nas demonstrações dos casos $n = 5$ e 7 , entre outros casos.

Por volta de 1825, Dirichlet e Legendre provaram, de forma independente, o caso particular $n = 5$, estudando-se a fatoração única nos Anéis de Dedekind.

Dirichlet demonstrou, em 1832, o caso do expoente $n = 14$.

Já, em 1839, Lamé apresentou uma elaborada demonstração para o caso $n = 7$, aprimorando, inclusive, certos aspectos da prova original de Germain. Utilizou uma expressão algébrica com fatores lineares e quadráticos equivalente a $(X + Y + Z)^7 - (X^7 + Y^7 + Z^7)$.

Em 1847, Kummer enunciou um outro importante teorema auxiliar, também dividido em dois casos, que relaciona o Último Teorema de Fermat a uma importante classe de primos, denominados regulares, úteis em várias outras demonstrações. Assim, tendo-se um “expoente primo e regular em uma equação fermatiana,

garante-se a não existência de solução de inteiros não nulos.

Kummer trouxe ainda um importante método para os divisores complexos.

(Cardoso, 2020, p. 15-16).

Singh (2008), aborda como o teorema de Fermat não foi apenas um desafio, mas também um grande impulsionador no desenvolvimento da matemática, ampliando os seus horizontes e fazendo com que muitos campos da área se coligassem formando uma matemática sólida e unificada, e ainda fazendo com que surgissem novos campos de estudos que foram utilizados por Wiles em sua demonstração falha em 1993 e na demonstração final em 1995.

Ávila (2010) destaca a importância de que educadores apresentem demonstrações matemáticas, ou ao menos esboços delas, aos estudantes. Para o autor, essa prática é fundamental para que a Matemática não seja vista apenas como um conjunto de fórmulas e resultados aceitos sem justificativa, mas como uma ciência construída por meio de argumentos lógicos rigorosos. Nesse contexto, o estudo de demonstrações históricas, como a do Último Teorema de Fermat, constitui uma oportunidade de evidenciar a natureza investigativa da atividade matemática.

A demonstração apresentada por Wiles representou mais do que a solução de um problema histórico. Seu trabalho evidenciou profundas conexões entre diferentes áreas da Matemática, especialmente entre a Teoria dos Números, a Álgebra e a Geometria. Conceitos relacionados a curvas elípticas, formas modulares e representações de Galois desempenharam papel fundamental na estrutura da demonstração, mostrando que problemas aparentemente simples podem exigir ferramentas matemáticas extremamente sofisticadas.

Dessa forma, a compreensão da demonstração Wiles–Taylor exige o estudo prévio de diversas estruturas algébricas fundamentais. Entre elas destacam-se os grupos, os anéis e os corpos, que constituem a base para teorias mais avançadas, como a Teoria de Galois. Considerando este cenário, serão apresentados a seguir alguns conceitos introdutórios dessas estruturas, os quais servirão de fundamento para o desenvolvimento dos próximos trabalhos relacionados ao Último Teorema de Fermat.

3. MATERIAIS E MÉTODOS

A metodologia para realização desta pesquisa baseia-se em uma pesquisa bibliográfica. De acordo com Sousa, Oliveira e Alves (2021), a pesquisa bibliográfica é:

[...] o levantamento ou revisão de obras publicadas sobre a teoria que irá direcionar o trabalho científico, o que necessita uma dedicação, estudo e análise pelo pesquisador que irá executar o trabalho científico e tem como objetivo reunir e analisar textos publicados, para apoiar o trabalho científico (Sousa; Oliveira; Alves, 2021).

Utilizando a metodologia bibliográfica, realizou-se uma pesquisa nos principais documentos, livros, artigos e notícias a respeito da história de Pierre de Fermat e dos matemáticos envolvidos nas demonstrações das “Equações Fermatianas”, assim como nos campos matemáticos que surgiram nesse processo.

A principal fonte histórica foi o livro do físico Simon Singh intitulado O Último Teorema de Fermat: a história do enigma que confundiu as maiores mentes do mundo durante 358 anos, mais especificamente a 13. ed., de 2008, publicada pela editora Record.

Além da pesquisa histórica, para os aspectos matemáticos da demonstração do teorema, foram utilizados os dois artigos publicados por Andrew Wiles e Richard Taylor na revista *Annals of Mathematics*, sendo eles:

1. Modular elliptic curves and Fermat’s Last Theorem (que pode ser traduzido por Curvas elípticas modulares e o Último Teorema de Fermat), com 110 páginas.

2. Ring-Theoretic Properties of Certain Hecke Algebras (que pode ser traduzido por Propriedades da Teoria dos Anéis de Certas Álgebras de Hecke), com 20 páginas.

3.1. A DEMONSTRAÇÃO FINAL

A demonstração feita por Andrew Wiles tem início em 1954, com conjectura proposta pelos matemáticos japoneses Yutaka Taniyama e Goro Shimura. Na época os dois eram estudantes de matemática da Universidade de Tóquio, e pesquisavam de forma simultânea e independente sobre formas modulares de curvas elípticas. Por serem estudantes do mesmo *campus* eles acabaram se conhecendo e começaram a trabalhar juntos nas pesquisas sobre o tema, até chegarem na conjectura de Taniyama-Shimura.

Figura 2 - Yutaka Taniyama Figura 3 - Goro Shimura





Fonte: London Math Soc obituary portrait Fonte: London Math Soc obituary portrait

A conjectura de Taniyama-Shimura (CTS) estabelece que toda curva elíptica semistável sobre os números racionais é modular, sendo fundamental para a Teoria dos Números. O que significa que as curvas podem ser associadas a formas modulares, que são figuras que possuem um alto grau de simetria.

Em 1984 foi realizado um simpósio entre matemáticos que pesquisavam sobre equações elípticas, na cidade de Oberwolfach, no interior da Alemanha. Durante o evento, o matemático Gerhard Frey propôs que quem conseguisse demonstrar a conjectura de Taniyama-Shimura conseguiria também demonstrar o UTF. Para isso ele afirmou que, se existisse uma solução inteira e não trivial para a equação de Fermat (ou seja, se o teorema fosse falso) para um expoente $n > 2$, então a equação $a^n + b^n = c^n$ levaria à construção de uma curva elíptica muito particular, chamada Curva de Frey (ou curva de Hellegouarch-Frey),

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

Para concluir este pensamento Frey realizou uma manipulação algébrica da equação fermtiana mantendo sua integridade, sendo assim, se o teorema de Fermat tivesse solução, essa curva teria que existir. No entanto, de acordo com Frey, essa curva possuía uma formulação tão estranha, que seria impossível ela ser modular, o que é uma contradição da conjectura de Taniyama-Shimura, pois ela afirma que toda curva elíptica deve ser modular. Sendo assim, havia duas interpretações da argumentação de Frey,

Se, e somente se, o UTF estivesse errado, então a equação elíptica de Frey existe.

A equação elíptica de Frey é tão estranha que nunca poderia ser modular.

A conjectura de Taniyama-Shimura afirma que toda equação elíptica deve ser modular.

Portanto, a conjectura de Taniyama-Shimura é falsa.

Alternativamente, e mais importante, Frey podia inverter este argumento.

Se for verdadeira a conjectura de Taniyama-Shimura, então toda equação elíptica deve ser modular.

Se toda equação elíptica deve ser modular, então a equação de Frey não pode existir

Se a equação elíptica de Frey não existe, então não podem existir soluções para a equação de Fermat.

Portanto, o Último Teorema de Fermat é verdadeiro.

(Singh, 2008, p. 206).

Mesmo com toda essa lógica construída por Frey, ainda faltava uma peça crucial para a ligação entre a conjectura de Fermat e o de Taniyama-Shimura, pois mesmo com a afirmação da impossibilidade de que a equação (I) pudesse ser modular, não tinha sido apontada nenhuma demonstração de tal proposição. Portanto, ainda não se tinha provas de que a demonstração de uma das conjecturas implicaria que a outra também pudesse ser demonstrada.

Nesta conferência onde Frey elucubrou sua hipótese, havia uma série de matemáticos que se fascinaram com a ideia, mas tinham percebido o erro presente em sua corrente de pensamento, o que gerou uma espécie de corrida para provar que a curva de Frey não poderia ser modular. A princípio parecia ser um problema muito simples, considerado até elementar por matemáticos mais experientes, porém tal impasse se mostrou bastante complexo.

Um dos matemáticos que estavam na conferência era Ken Ribet, um professor da Universidade da Califórnia, que também tentava provar a não modularidade da curva de Frey, ele trabalhou cerca de 18 meses nessa pesquisa, conseguindo provas apenas para alguns casos específicos de modularidade. Até que, em 1986, aconteceu o Congresso Internacional de Matemática em Berkeley, nos EUA, e Ribet em conversa com outro matemático, o professor Barry Mazur, conseguiu a peça que precisava para a generalização de sua demonstração.

Assim, Ribet provou a ligação entre a equação de Fermat e a conjectura de Taniyama-Shimura, sendo um dos avanços mais significativos até a demonstração de Wiles.

Andrew Wiles é um matemático britânico que conheceu o Teorema de Fermat ainda criança e cresceu fascinado com a possibilidade de um dia conseguir prová-lo. Wiles afirma:

Por acaso, estava folheando livros na biblioteca pública da minha cidade e encontrei um livro de matemática que contava um pouco da história desse problema: alguém o havia resolvido há 300 anos, mas ninguém jamais tinha visto a demonstração. Ninguém sabia se havia uma demonstração. E desde então, as pessoas a procuravam. E ali estava um problema que eu, com dez anos de idade, conseguia entender, um problema que nenhum dos grandes matemáticos do passado havia conseguido resolver. E a partir daquele momento, é claro, eu simplesmente tentei resolvê-lo sozinho. Era um desafio e tanto, um problema tão belo. Esse problema era o Último Teorema de Fermat. (Lynch, 2016)

Ele se formou bacharel em matemática pela Universidade de Oxford em 1974 e, em seguida, ingressou no Clare College, em Cambridge, para cursar o doutorado. Em 1981, assumiu uma posição no Instituto de Estudos Avançados de Princeton, sendo nomeado professor em Princeton no ano seguinte.

E, então, em 1986 ele fica sabendo sobre a conexão das conjecturas feitas por Frey, mas sem muita esperança de que aquela afirmação pudesse resultar na real demonstração. Wiles só ficou convencido de que seria possível provar o UTF quando ele descobriu que Ribet havia conseguido provar a modularidade da Curva de Frey. Andrew afirmou

Eu estava na casa de um amigo tomando chá gelado no início da noite, quando ele mencionou casualmente, no meio da conversa: "A propósito, você soube que Ken Ribet provou a conjectura ϵ ?" Fiquei simplesmente eletrizado. Naquele instante, soube que o rumo da minha vida estava mudando, porque isso significava que, para provar o Último Teorema de Fermat, eu só precisava provar a conjectura de Taniyama - Shimura. A partir daquele momento, foi nisso que me concentrei. Eu simplesmente sabia que chegaria em casa e trabalharia na conjectura de Taniyama - Shimura (Lynch, 1997).

Depois disso, ele se dedicou a tentar resolver a conjectura de Taniyama-Shimura, com o objetivo de provar o UTF, abdicando de todas as pesquisas que estava realizando no momento e se

dedicando de forma integral à tentativa de demonstrar a CTS e ministrar suas aulas na universidade. Ele trabalhou nessa demonstração por cerca de sete anos, de forma totalmente reclusa. Wiles não quis compartilhar seu trabalho com ninguém, mantendo-o em segredo.

Para começar sua pesquisa, Wiles utilizou um conceito criado por Galois chamado Teoria dos Grupos, usando-a como ferramenta para generalizar a CTS.

O que tornava tão difícil a prova da conjectura era sua generalização infinita, pois, para afirmar com toda certeza que a proposição era válida, era preciso provar sua aplicabilidade a qualquer curva elíptica existente.

Para isso, Andrew teria que provar que cada elemento de uma série $E(E_1, E_2, E_3, \dots, E_n)$ (o que seria o equivalente às equações de curvas elípticas existentes) seria igual a cada um dos elementos da série $M(M_1, M_2, M_3, \dots, M_N)$ (que seria o equivalente às modularidades de cada uma das curvas elípticas da série E).

Para tal, ele pretendia utilizar um método de demonstração conhecido como Princípio da Indução Finita, que consiste em provar que um argumento é verídico para um caso base n de um conjunto de elementos, e após isso mostrar que esta proposição também é válida para o caso $n + 1$, assim obtendo uma generalização para qualquer elemento deste conjunto.

Assim, através desses artifícios matemáticos, em alguns meses Wiles já conseguia igualar as curvas elípticas a sua forma modular, dividindo-as nos grupos propostos por Galois. Além disso, nesse momento ele também já conseguia igualar os primeiros termos das séries E e M ($E_1 = M_1$).

Agora o grande desafio de Wiles era provar que ao igualar os primeiros elementos dessas séries, ele poderia fazer a generalização utilizando a argumentação da indução finita.

Enquanto ele trabalhava para conseguir essa demonstração, em 1988 outro matemático chamado Yoichi Miyaoka, da Universidade Metropolitana de Tóquio, anunciava que havia conseguido provar o UTF, porém utilizando um caminho diferente de Wiles. Miyaoka construiu sua prova utilizando a geometria diferencial ligada à Teoria dos Números. Porém, durante as duas semanas após o seu anúncio, sua pesquisa foi submetida a um rigoroso processo de verificação, e, para a infelicidade de Yoichi, havia um erro lógico na sua construção, sendo assim o UTF permanecia intacto.

Depois da tentativa frustrada de Yoichi, Wiles deu prosseguimento em suas pesquisas. Mesmo com os avanços obtidos sob o viés da teoria de Galois, ele ainda não havia conseguido dar continuidade em sua argumentação indutiva finita, resolvendo, então, utilizar um método que aprendeu durante o seu doutorado em Cambridge, denominado Teoria de Iwasawa. A Teoria de

Iwasawa é uma área da Teoria dos Números que estuda como certos objetos aritméticos se comportam em sequências infinitas de corpos numéricos, no entanto ela ainda não se encaixava na demonstração, mas Wiles acreditava que poderia adaptá-la para alcançar seu objetivo.

Mesmo realizando uma série de adaptações, a Teoria de Iwasawa não se mostrou eficiente, forçando Wiles a buscar outro meio para conseguir generalizações. Ele já não conseguia encontrar nenhum artifício que pudesse ser útil em seu cálculo, então resolveu voltar-se à comunidade de matemáticos novamente para buscar algo que lhe fosse útil.

Em 1991, Wiles participou de uma convenção sobre equações elípticas realizada em Boston, onde encontrou John Coates, um matemático que havia sido seu orientador de doutorado. Enquanto os dois conversavam, Wiles fez questão de não exprimir nenhuma pista sobre o que estava trabalhando e, no decorrer da conversa, ficou sabendo de um estudante chamado Matheus Flach, que estava aprimorando um certo método de análises de curvas elípticas criado por Victor Kolyvagin.

Wiles se interessou bastante pelo método Kolyvagin-Flach (MKF) e acreditava que conseguiria utilizá-lo para os seus cálculos, ele então se dedicou a aprender o método, mas teve uma certa dificuldade, pois era uma matemática totalmente nova e complexa. Voltando à sua pequena sala na Universidade de Princeton ele conseguiu ao longo de meses se familiarizar com MKF, e já conseguia demonstrar a modularidade de algumas curvas elípticas.

Um dos grandes obstáculos do uso do MKF, era que o método não funcionava com todas as equações elípticas existentes, então Wiles precisou fazer um grande esforço para conseguir adaptá-lo, a fim de conseguir uma generalização que tornaria possível sua prova por indução. No decorrer de suas pesquisas Wiles percebeu que as equações elípticas poderiam ser agrupadas em determinados grupos que tinham características distintas entre si.

Ele foi progredindo de forma linear em demonstrar a modularidade de cada um desses grupos que ele projetou, um trabalho que durou cerca de 2 anos. Mesmo com o progresso alcançado, Wiles tinha dúvidas sobre seu uso do método Kolyvagin-Flach, e decidiu que precisava de ajuda de alguém que fosse especialista no campo em que ele trabalhava:

Durante aquele ano eu trabalhei muito duramente tentando fazer o método Kolyvagin-Flach funcionar, mas isso envolvia ferramentas sofisticadas com as quais eu não estava familiarizado. Havia um bocado de álgebra complexa que exigia que eu aprendesse muita matemática nova. Então, em janeiro de 1993, eu decidi que precisava de um conselho de alguém que fosse especialista no tipo de técnicas geométricas que eu estava invocando na demonstração. Eu tinha que escolher com cuidado para quem contaria meu segredo, porque ele teria que ser mantido em sigilo. Resolvi falar com Nick Katz (Singh, 2008, p. 245-246).

Nicholas Katz, assim como Wiles, era professor na Universidade de Princeton, ele realizava pesquisas em Teoria dos Números e Geometria Algébrica Aritmética. Andrew procurou Katz em uma tarde como todas as outras e pediu que ele fosse até o seu escritório. Quando Katz chegou lá, ficou maravilhado com a ideia de Wiles de provar a conjectura de Taniyama-Shimura.

Durante essa pequena reunião, Wiles explicou uma boa parte de sua corrente de raciocínio, no entanto, havia muitos cálculos que precisavam ser revisados, e essas pequenas reuniões não seriam suficientes para que isso fosse possível. Katz afirmou:

O que Andrew tinha que me explicar era tão grande e longo que não daria certo tentar mostrar-me em seu escritório, durante conversas informais. Para algo tão grandioso, nós precisávamos montar uma estrutura formal de aulas semanais; de outro modo, a coisa iria se degenerar. E assim decidimos criar um curso com várias aulas (Singh, 2008, p. 246-247).

Então para que isso fosse possível, Andrew anunciou uma série de palestras intituladas ‘Cálculos em Curvas Elípticas’, que seriam abertas à comunidade acadêmica de Princeton e que Katz estaria na plateia. Sendo assim, Wiles ia explicar toda sua demonstração e os outros estudantes que não sabiam do que se tratava não iriam perceber que todo aquele cálculo era uma possível demonstração da conjectura de Taniyama-Shimura.

No início o curso chamou atenção de uma boa parte dos estudantes, mas com o passar das aulas as cadeiras foram ficando vazias até que ficasse apenas Nick, que cuidadosamente analisava cada passo da demonstração de Wiles. Quando o curso terminou não havia mais dúvidas de que MKF funcionava perfeitamente, assim Wiles deu continuidade a sua demonstração.

Em uma tarde no final de maio de 1993, Andrew estava trabalhando em sua conjectura e se deparou com um trabalho de Barry Mazur, e viu uma frase que lhe chamou atenção, ela falava sobre a teoria da deformação de representações de Galois, uma técnica desenvolvida no século XIX. Ele então viu ali uma maneira de fazer com que o método Kolyvagin-Flach funcionasse para o último grupo de equações elípticas que faltava.

Assim, após sete anos de trabalho Wiles finalmente acreditava ter encontrado a demonstração para o tão grandioso Último Teorema de Fermat.

Wiles então resolveu apresentar sua demonstração em uma conferência sobre Teoria dos Números, que aconteceu por volta de maio de 1993 em Cambridge, Intitulada “Funções *Le Aritmética*”. Esse evento tinha sido organizado por John Coates, que, como já citado anteriormente, tinha sido o orientador de doutorado de Andrew, que o convidou para ministrar duas palestras.

Wiles tinha informado a Coates que tinha algo grande para suas palestras, então John decidiu

disponibilizar um de seus próprios horários de palestra para que Andrew pudesse apresentar seu trabalho, mesmo sem saber sobre o que se tratava.

Nas três palestras ministradas, Wiles desenvolveu sua demonstração deixando todos os matemáticos que estavam presentes entusiasmados e maravilhados com tudo o que estava sendo apresentado. Uma matemática totalmente nova estava sendo exibida, instigando a curiosidade de todos presentes.

Após essa série de palestras, Wiles recebeu um gigantesco destaque da mídia, sendo a primeira página dos principais jornais da época, estampando páginas de revista onde foi eleito como uma das vinte e cinco pessoas mais interessantes do mundo e sendo ainda convidado para fazer parte da propaganda de uma marca de vestuário que pretendia lançar uma coleção de roupas masculinas.

Assim, tendo todos os olhos da comunidade acadêmica voltados ao seu trabalho, os manuscritos de Wiles foram submetidos a um rigoroso processo de revisão pela revista a que foi submetido, chamada *Inventiones Mathematicae*. Os trabalhos acadêmicos submetidos em revistas costumam passar por um pequeno grupo de até três revisores, no entanto o editor da revista, o matemático Barry Mazur, decidiu que o trabalho de Wiles precisava de uma equipe maior. Assim foi formada uma equipe de seis revisores, sendo eles:

Nicholas Katz (especialista em curvas elípticas)

Barry Mazur (especialista em curvas elípticas e formas modulares)

John Coates (orientador de doutorado de Wiles e especialista em funções L_p -ádicas)

Ken Ribet (matemático cujo trabalho – o Teorema de Ribet – foi crucial para a abordagem de Wiles, pois conectou de forma definitiva a conjectura de Taniyama-Shimura e o UTF)

Richard Taylor (ex-aluno de Wiles, que mais tarde colaborou com ele para corrigir a falha na prova original e foi coautor do segundo artigo complementar)

Os meses após o anúncio da prova da conjectura de Taniyama-Shimura foram de espera pela correção da equipe revisora. As 200 páginas do trabalho de Wiles foram divididas em seções, que foram distribuídas aos seis matemáticos.

3.1.1. ERRO FUNDAMENTAL

Wiles já esperava que houvesse muitas dúvidas e correções feitas pelos revisores, que aos poucos foram sendo sanadas e ajustadas através de e-mails entre ele e a banca. Durante a correção de sua seção, Katz teve uma dúvida a respeito de uma ligação lógica no uso do método Kolyvagin-Flach e como de costume enviou um e-mail a Wiles, que após muitas dúvidas acreditava ser apenas mais uma correção de simples solução.

Katz insistiu bastante nesse trecho, o que fez com que Wiles o revisse com bastante atenção e, nesse momento, ele percebe um erro fundamental em sua demonstração. O problema encontrado consistia na ideia de que a afirmação feita por Wiles de que o método Kolyvagin-Flach funcionava para todas as equações elípticas estava equivocada.

O método desenvolvido por Kolyvagin funcionava para determinadas equações elípticas em situações específicas e Wiles havia o adaptado para funcionar em sua demonstração, no entanto a ideia estava errada. A generalização feita por Wiles estava incorreta e devido a este erro a sequência lógica de prova por indução de que ele desenvolveu não funcionava mais.

Devido a confidencialidade do processo de correção da pesquisa este assunto não foi a público, sendo assim Wiles iniciou uma corrida contra o tempo para tentar encontrar uma maneira de corrigir este erro.

Ele passou todo o restante do ano de 1993 tentando resolver esse problema sem obter sucesso em sua busca.

3.1.2. BUSCANDO UMA SOLUÇÃO

Nos meses que se seguiram após o encontro do erro, a comunidade acadêmica começava a desacreditar que Wiles havia realmente provado a conjectura de Taniyama-Shimura. O manuscrito com a prova ainda permanecia confidencial sendo de conhecimento apenas da banca de correção e de Andrew Wiles, o que alimentava ainda mais a ideia de que ele não provaria o teorema.

Wiles continuou a sua procura por uma solução para o seu problema conectivo lógico. Já havia se passado todo o inverno do final de 1993 e ele ainda não havia encontrado nenhuma solução para o seu obstáculo. Já estava prestes a desistir e publicar toda a sua demonstração, mesmo que de forma incompleta.

Durante todo esse período em que ele buscava uma solução para o problema, Wiles se isolou do mundo, mesmo com toda a repercussão sobre sua demonstração e os boatos sobre a incompletude dela. Uma das únicas pessoas com quem Wiles compartilhava sobre seu trabalho era Peter Sarnak, um amigo e também professor do departamento de matemática de Princeton, que entrou na universidade no mesmo momento que Andrew.

Sarnak aconselha o amigo a procurar alguém para lhe ajudar com seus cálculos, uma pessoa que revisasse o que ele vinha desenvolvendo para ter uma visão externa no problema. Wiles pensou bastante no conselho do amigo e decidiu convidar Richard Taylor, um de seus ex-alunos e revisor de sua demonstração. Taylor morava na Inglaterra e foi passar uma temporada na Universidade de Princeton para trabalhar no teorema com Wiles.

Juntos, Wiles e Taylor, começaram a revisar os manuscritos do capítulo 3 da demonstração, onde estava o problema. Eles passaram todo o mês de janeiro de 1994 revisando os cálculos utilizando o método Kolyvagin-Flach, e mesmo assim ainda não conseguiram pensar em nenhuma saída para o problema.

No mês de abril de 1994, um matemático chamado Noam Elkies, anunciou que havia encontrado um contraexemplo para o Último Teorema de Fermat. Elkies já havia ficado famoso por ter encontrado um contraexemplo para a conjectura de Euler, e agora afirmava ter encontrado uma solução para a equação fermatiana envolvendo um expoente primo incrivelmente grande (Maior que 10^{20}).

A notícia dessa solução se espalhou rapidamente, o que deixou Wiles extremamente abalado com a ideia de que sua demonstração era totalmente falsa. Depois de toda a repercussão foi constatado que a notícia não passava de uma brincadeira feita por Elkies, pois o e-mail afirmando que ele encontrou a contraprova foi enviado dia 1 de abril (data que o ocidente considera o dia da mentira).

Após a confirmação de que a contraprova encontrada por Elkies era apenas uma brincadeira de 1 de abril, Wiles continuou a sua procura por uma solução para o seu problema conectivo lógico. Com a chegada do final de 1994, Wiles ainda não havia superado o obstáculo que comprometia sua demonstração. Depois de meses dedicados à busca por uma solução, passou a considerar a possibilidade de divulgar o trabalho desenvolvido até aquele momento, mesmo que a prova permanecesse incompleta.

Faltava apenas um mês para que Taylor retornasse à Inglaterra e ele convenceu Wiles a continuar tentando nesse último mês antes de desistir de resolver o problema.

Enquanto Taylor explorava novos métodos para resolver o problema, Wiles decidiu revisar todo o método Kolyvagin-Flach para pelo menos encontrar o motivo pelo qual o seu trabalho havia fracassado. E foi durante essa busca pela origem de seu erro que Wiles encontrou a solução para seu problema, que de acordo com suas palavras:

Eu estava sentado diante de minha escrivaninha, na manhã da segunda-feira, 19 de setembro, examinando o método Kolyvagin-Flach. Não é que eu achasse que poderia fazê-lo funcionar, mas achava que pelo menos poderia explicar por que não funcionava. Achava que estava me agarrando nos últimos fios de esperança, mas queria me tranquilizar. Subitamente, de um modo totalmente inesperado, eu tive esta incrível revelação. Eu percebi que, embora o método Kolyvagin-Flach não estivesse funcionando completamente, ele era tudo que eu precisava para fazer a minha teoria original Iwasawa funcionar. Percebi que tinha o suficiente do método Kolyvagin-Flach para construir minha abordagem original do problema nos

primeiros três anos de trabalho. Assim, das cinzas de Kolyvagin-Flach, parecia surgir a verdadeira resposta para o problema (Singh, 2008, p.277).

E assim, depois de 7 anos de trabalho, Wiles finalmente havia encontrado a solução para o Último Teorema de Fermat, criando essa conexão entre os métodos de Kolyvagin-Flach e a Teoria de Iwasawa. De forma separada essas abordagens não funcionavam para demonstrar o UTF, mas juntas os seus resultados se complementavam. Ele fez isso trabalhando com a hipótese de que certas álgebras de Hecke são interseções locais completas.

Depois de resolvido totalmente o teorema, Wiles publicou seus dois artigos contendo a demonstração, o primeiro sendo o manuscrito das palestras em que ele apresentou a sua primeira demonstração e o segundo que ele publicou juntamente com Richard Taylor que continha a conexão entre os métodos que ele utilizou.

3.3.3. GRUPOS, ANÉIS E CORPOS

A estratégia utilizada por Wiles e Taylor para demonstrar o Último Teorema de Fermat envolve ferramentas sofisticadas da Álgebra Moderna. Entre elas destacam-se a Teoria de Galois e o estudo de representações associadas a grupos de Galois. Dessa forma, torna-se necessário compreender inicialmente algumas estruturas algébricas fundamentais, como grupos, anéis e corpos, que constituem a base teórica para os tópicos que serão abordados nos próximos estágios desta pesquisa.

Nesta seção serão apresentados conceitos e definições de autores como Domingues e Iezzi (2018), Vieira (2015), Martin (2010) e Yartey (2017).

Definição 3.1 - Um grupo consiste num conjunto não vazio G munido de uma operação binária, denotada por,

$$\square : G \times G \rightarrow G$$

$$(a, b) \square a \square b$$

que satisfaz os seguintes axiomas:

$$(a \square b) \square c = a \square (b \square c), \forall a, b, c \in G \text{ (G1)}$$

$$\exists e \in G, \text{ tal que } e \square a = a \square e = a, \forall a \in G \text{ (G2)}$$

$$\forall a \in G, \exists a' \in G, \text{ tal que } a \square a' = a' \square a = e \text{ (G3)}$$

Se, além disso, ainda se cumprir o axioma da comutatividade,

$$a \square b = b \square a, \forall a, b \in G, (G4)$$

o grupo recebe o nome de grupo *comutativo* ou *abeliano*.

No decorrer do trabalho será usado a notação $(G, \square)$ para representar grupos quaisquer.

Definição 3.2 - Seja $(G, \square)$ um grupo. Um subconjunto $H \subset G$ é um subgrupo de G se:

$$H \neq \square$$

H é fechado para a operação de G , ou seja,

$$a \square b \in H, \forall a, b \in H$$

$(H, \square)$ também é um grupo

Usaremos a notação $H < G$ para quando H for um subgrupo de G .

Definição 3.3 - Seja $(G, \square)$ um grupo. Um subgrupo H de G é chamado de subgrupo normal, e denotado por $H \triangleleft G$, quando

$$a \square h \square a' \in H, \forall a \in G, \forall h \in H.$$

Definição 3.4 - Um Homomorfismo de um grupo $(G, \square)$ em um grupo $(J, \cdot)$ é uma aplicação $f : G \rightarrow J$ tal que

$$f(a \square b) = f(a) \cdot f(b), \forall a, b \in G.$$

Definição 3.5 - Seja $(G, \square)$ e $(J, \cdot)$ dois grupos e $f : G \rightarrow J$ um homomorfismo entre eles. O núcleo de f é o subconjunto de G , denotado por $N(f)$, definido por

$$N(f) = \{a \in G | f(a) = e_j\}$$

sendo e_j o elemento neutro do grupo J .

Definição 3.6 - Seja $f : G \rightarrow J$ um homomorfismo.

Se f é injetora, dizemos que ela é um monomorfismo.

Se f é sobrejetora, dizemos que ela é um epimorfismo.

Se f é bijetora, dizemos que ela é um isomorfismo.

Se f é um isomorfismo e $G = J$, dizemos que f é um automorfismo

Definição 3.7 - Sejam $(G, \square)$ um grupo e H um subgrupo normal de G ($H \triangleleft G$). Denotamos por,

$$G/H = \{aH | a \in G\}$$

o conjunto das classes laterais à esquerda com respeito a H .

Proposição 3.8 - Se definirmos a seguinte operação binária no conjunto das classes laterais G/H ,

$$\square : G/H \times G/H \rightarrow G/H$$

$$((aH), (bH)) \square (a \square b)H$$

ela está bem definida.

Demonstração: Suponha que $a, a', b, b' \in G$ tais que $aH = a'H$ e $bH = b'H$. Então $a' = a \square h_1$ e $b' = b \square h_2$ para algum $h_1, h_2 \in H$. Então por definição,

$$\square (a'H, b'H) = (a' \square b')H$$

$$= ((a \square h_1) \square (b \square h_2))H$$

$$= (a \square h_1 \square b)H \text{ pois } h_2 \in H$$

$$= (a \square h_1)Hb \text{ pois } H \text{ é normal}$$

$$= aHb \text{ pois } h_1 \in H$$

$$= (a \square b)H \text{ pois } H \text{ é normal}$$

Portanto $\square$ é bem definida.

Teorema 3.9 - Se $(G, \square)$ é um grupo e $H \trianglelefteq G$, então G/H é um grupo munido da operação, $aH \square bH = (a \square b)H$,

o qual é chamado de grupo quociente de G módulo H .

Demonstração:

(i) Sejam $aH, bH, cH \in G/H$. Como G é um grupo, vale que $a(bc) = (ab)c$, temos que,

$$(aH \square bH) \square cH = (a \square b)H \square cH$$

$$= ((a \square b) \square c)H$$

$$= (a \square (b \square c))H$$

$$= aH \square (b \square c)H$$

$$= aH \square (bH \square cH)$$

(ii) Como G é um grupo, sabemos que ele possui um elemento neutro e , portanto, $H = eH$.
Temos,

$$aH \square H = aH \square eH$$

$$= (a \square e)H$$

$$= aH$$

$$= (e \square a)H$$

$$= eH \square aH$$

$$= H \square aH, \forall a \in G$$

Logo H é o elemento neutro de $\square$.

(iii) Como G é um grupo, todo $a \in G$ possui elemento inverso $a' \in G$. Temos,

$$aH \square a'H = (a \square a')H$$

$$= eH$$

$$= (a' \square a)H$$

$$= a'H \square aH$$

Logo, $a'H$ é o elemento inverso aH para operação $\square$.

Portanto de (i), (ii) e (iii) concluímos que $(G/H, \square)$ é um grupo.

Teorema 3.10 (Fundamental do Homomorfismo) - Seja $f : G \rightarrow J$ um homomorfismo de grupos. Então,

$$G/N(f) \square \text{Im}(f).$$

Esse resultado estabelece uma relação fundamental entre os conceitos de homomorfismo, núcleo e grupo quociente, mostrando que a imagem de um homomorfismo pode ser descrita, a menos de isomorfismo, pelo quociente do grupo domínio pelo seu núcleo.

Outras estruturas que serão apresentadas a seguir são os anéis e corpos, que são muito importantes visto que eles podem ser compreendidos como ampliações do conceito de grupos, adicionando novas propriedades operatórias.

Definição 3.11 - Um anel é uma terna $(A, \square, \cdot)$ que consiste num conjunto não vazio A e um par de operações sobre A , respectivamente uma adição ($\square$) e uma multiplicação ($\cdot$),

$$(a, b) \in A \times A \square a \square b \in A$$

$$(a, b) \in A \times A \square a \cdot b \in A$$

satisfazendo os seguintes axiomas:

$(A, \square)$ é um grupo abeliano, ou seja:

$$a \square (b \square c) = (a \square b) \square c, \forall a, b, c \in A;$$

$$a \square b = b \square a, \forall a, b \in A;$$

$$\exists 0_A \in A, \text{ tal que } a \square 0_A = 0_A \square a = a, \forall a \in A;$$

$$\forall a \in A, \exists a' \in A, \text{ tal que } a \square a' = a' \square a = 0_A;$$

A operação $\cdot$ atende a propriedade associativa, isto é:

$$a \cdot (b \cdot c) = (a \cdot b) \cdot c, \forall a, b, c \in A.$$

A operação $\cdot$ é distributiva em relação à $\square$:

$$a \cdot (b \square c) = a \cdot b \square a \cdot c, \forall a, b, c \in A.$$

$$(a \square b) \cdot c = a \cdot c \square b \cdot c, \forall a, b, c \in A.$$

Definição 3.12 - Seja $(A, \square, \cdot)$ um anel. Diz-se que um subconjunto $L \subset A$ é um subanel

de A se:

$$L \neq \emptyset$$

L é fechado para a operação de A , ou seja,

$$a \square b \in L, \forall a, b \in L$$

$$a \cdot b \in L, \forall a, b \in L$$

$(L, \square, \cdot)$ também é um anel

Definição 3.13 - Seja $(A, \square, \cdot)$ um anel. Se a operação $\cdot$ satisfaz a comutatividade, isto é,

$$a \cdot b = b \cdot a, \forall a, b \in A,$$

então dizemos que A é um anel comutativo.

Definição 3.14 - Seja $(A, \square, \cdot)$ um anel. Se a operação $\cdot$ possui um elemento neutro, isto é,

$$\exists 1_A \in A, 1_A \neq 0, \text{ tal que } a \cdot 1_A = 1_A \cdot a = a, \forall a \in A,$$

então se diz que 1_A é a unidade de A e que A é um anel com unidade.

Definição 3.15 - Seja $(A, \square, \cdot)$ um anel comutativo com unidade. Se para esse anel vale a lei do anulamento do produto, ou seja, se uma igualdade do tipo

$$a \cdot b = 0_A,$$

em que $a, b \in A$, só for possível para

$$a = 0_A \text{ ou } b = 0_A,$$

então se diz que A é um anel de integridade ou um domínio de integridade.

Definição 3.16 - Um homomorfismo de um anel $(A, \square, \cdot)$ em um anel $(B, \square, \cdot)$ é uma aplicação $f : A \rightarrow B$, tal que, para quaisquer $a, b \in A$,

$$f(a \square b) = f(a) \square f(b)$$

$$f(a \cdot b) = f(a) \cdot f(b).$$

Definição 3.17 - Seja $f : A \rightarrow B$ um homomorfismo de anéis e seja 0_B o elemento neutro da primeira operação do anel B . Chamamos de núcleo do homomorfismo f , denotado por $I(f)$, o subconjunto de A definido por,

$$I(f) = \{a \in A \mid f(a) = 0_B\}$$

Definição 3.18 - Seja $f : A \rightarrow B$ um homomorfismo.

Se f é injetora, dizemos que ela é um monomorfismo de anéis

Se f é sobrejetora, dizemos que ela é um epimorfismo de anéis.

Se f é bijetora, dizemos que ela é um isomorfismo de anéis. Neste caso, dizemos que os anéis A e B são isomorfos e denotamos por $A \cong B$.

Se f é um isomorfismo e $A = B$, dizemos que f é um automorfismo de anéis.

Definição 3.19 - Seja $(A, +, \cdot)$ um anel. Um subconjunto não vazio $I \subset A$, é chamado de ideal de A se satisfazer as seguintes propriedades:

$$a + (-b) \in I, \forall a, b \in I$$

$$a \cdot b \in I \text{ e } b \cdot a \in I, \forall a \in A, \forall b \in I$$

Definição 3.20 - Um anel comutativo com unidade $(K, +, \cdot)$ é chamado de corpo se todo elemento não nulo possui inverso multiplicativo.

Definição 3.21 - Seja $(K, +, \cdot)$ um corpo. Diz-se que um subconjunto $F \subset K$ é um subcorpo de K se:

$$F \neq \emptyset$$

F é fechado para as operações de K , ou seja,

$$a + b \in F, \forall a, b \in F$$

$$a \cdot b \in F, \forall a, b \in F$$

$(F, +, \cdot)$ também é um corpo.

Definição 3.22 - Seja K um corpo qualquer. Um polinômio sobre K em uma variável x é uma soma infinita formal

$$f(x) = \sum_{i=0}^{\infty} a_i x^i = a_0 + a_1 x + a_2 x^2 + \dots + a_n x^n + \dots,$$

em que $a_i \in K$, para todo $i \in \cup \{0\}$ e $a_i \neq 0$ apenas para um número finito de valores de i ou seja, existe $m \in \mathbb{N}$ tal que $a_j = 0$ para qualquer $j \geq m$. O conjunto de todos estes polinômios, sob as operações usuais de adição e multiplicação de polinômios, é denotado por $K[X]$ e chamado de anel de polinômios sobre K .

O estudo das extensões de corpos está intimamente relacionado ao estudo de polinômios. Uma das ideias centrais da Teoria de Galois consiste em investigar as simetrias existentes em extensões de corpos obtidas a partir das raízes de determinados polinômios. Essas simetrias são descritas pelos automorfismos de corpos e dão origem aos chamados grupos de Galois.

Definição 3.23 - Sejam K e F dois corpos tais que F é um subcorpo de K . Dizemos que K é uma extensão de corpo (ou simplesmente uma extensão) de F , denotada por $K: F$. O corpo F é chamado de corpo de base da extensão.

Definição 3.24 - Um homomorfismo de um corpo $(K, +, \cdot)$ em um corpo $(F, +, \cdot)$ é uma aplicação $f: K \rightarrow F$ tal que, para quaisquer $a, b \in K$,

$$f(a + b) = f(a) + f(b)$$

$$f(a \cdot b) = f(a) \cdot f(b)$$

$$f(1_K) = 1_F$$

Definição 3.25 - Seja $f: K \rightarrow F$ um homomorfismo de corpos.

Se f é injetora, dizemos que ela é um monomorfismo de corpos.

Se f é sobrejetora, dizemos que ela é um epimorfismo de corpo.

Se f é bijetora, dizemos que ela é um isomorfismo de corpos.

Se f é um isomorfismo e $K = F$, dizemos que f é um automorfismo de corpo.

O conjunto de todos os automorfismos de um corpo K é denotado por $\text{Aut}(K)$.

Os conceitos apresentados nesta seção constituem o ponto de partida para o estudo da Teoria de Galois, tema que desempenha papel central na matemática utilizada por Wiles e Taylor na demonstração do Último Teorema de Fermat.

4. RESULTADOS ESPERADOS

Espera-se apresentar aspectos iniciais da demonstração desenvolvida por Andrew Wiles e Richard Taylor, analisando seus aspectos teóricos e estabelecendo o escopo matemático utilizado, abordando como foi feita a ligação entre a conjectura de Taniyama-Shimura e o Último Teorema de Fermat.

REFERÊNCIAS

- ÁVILA, G. **Várias faces da matemática: tópicos para licenciatura e leitura geral**. 2. ed. São Paulo: Blucher, 2010.
- CARDOSO, S. O. **O Último Teorema de Fermat para $n = 5$** . Dissertação (Mestrado em Matemática) – Universidade Federal do Estado do Rio de Janeiro, Centro de Ciências Exatas e Tecnologia, Rio de Janeiro, 2020.
- DOMINGUES, H. H.; IEZZI, G. **Álgebra moderna**. 5. ed. São Paulo: Saraiva, 2018.
- LYNCH, J. **The Proof**. Coprodução da BBC TV/WGBH Boston, 28 out. 1997. NOVA | Transcripts | The Proof | PBS.
- LYNCH, P. **Andrew Wiles ganha a Medalha Abel com uma prova que levou 350 anos para ser feita**. The Irish Times, 19 maio 2016.
- MARTIN, P. A. **Grupos, corpos e teoria de Galois**. São Paulo: Editora Livraria da Física, 2010. (Coleção de Textos Universitários do IME-USP).
- SINGH, S. **O Último Teorema de Fermat: a história do enigma que confundiu as maiores mentes do mundo durante 358 anos**. 13. ed. Rio de Janeiro: Record, 2008.
- SOUSA, A. S.; OLIVEIRA, G. S.; ALVES, L. H. A pesquisa bibliográfica: princípios e fundamentos. **Cadernos da Fucamp**, v. 20, n. 43, p. 68-83, 2021.
- TAYLOR, R.; WILES, A. Ring-Theoretic Properties of Certain Hecke Algebras. **Annals of Mathematics**, v. 141, n. 3, p. 553-572, 1995. JSTOR.
- VIEIRA, V. L. **Álgebra abstrata para licenciatura**. 2. ed. Campina Grande: EDUEPB; Livraria da Física, 2015.
- WILES, A. Modular Elliptic Curves and Fermat's Last Theorem. **Annals of Mathematics**, v. 141, n. 3, p. 443-551, 1995.
- YARTEY, J. N. A. **Álgebra II**. Salvador: UFBA, Instituto de Matemática e Estatística; Superintendência de Educação a Distância, 2017. 244 p.: il.