Os Três Séculos do Último Teorema de Fermat

Talita Bogler Souza

[1]Acadêmica do Curso de Matemática - Centro de Ciências Exatas e Tecnológicas da Universidade Estadual do Oeste do Paraná
Caixa Postal 711 - 85819-110 - Cascavel - PR - Brasil

talitabogler@hotmail.com

Resumo. *O objetivo deste artigo é apresentar os aspectos históricos do Último Teorema Fermat durante os três séculos desde sua origem, mostrando as diversas tentativas de solução ao longo do tempo, até chegar à história do Professor Andrew Wiles, que dedicou sua vida na demonstração do teorema. Descreveremos um pouco do trabalho de grandes matemáticos que contribuíram com a resolução do Último Teorema de Fermat durante os séculos XVIII, XIX e no século XX, como Euler, Sophie Germain, Gabriel Lamé, Augustin Louis Cauchy, Ernest Kummer, Taniyama e Shimura, Gerhard Frey e Ken Ribet.*

Palavras Chaves. *Último Teorema de Fermat, Curvas Elípticas e Formas Modulares.*

1. Introdução

Foi enquanto estudava o Livro *Aritmética* de Diofanto (séc. III d.C.), em 1637, que Pierre de Fermat, um matemático amador, encontrou uma série de observações, problemas e soluções relacionadas ao teorema de Pitágoras e os trios pitagóricos. Brincando com a equação de Pitágoras, Fermat criou uma equação que não tinha solução. Na margem do livro Fermat escreveu:

> *Cubem autem in duos cubos, aut quadratoquadratum in duos quadratoquadratos, et generaliter nullam in infinitum ultra quadratum potestatem in duos eiusdem nominis fas est dividere. Cuius rei demonstrationem mirabilem sane detexi hanc marginis exiguitas non caperet.*
>
> É impossível para um cubo ser escrito como a soma de dois cubos ou uma quarta potência ser escrita como uma soma de dois números elevados a quatro, ou, em geral, para qualquer número que seja elevado a uma potência maior do que dois ser escrito como a soma de duas potências semelhantes. Eu tenho uma demonstração realmente maravilhosa para esta proposição, mas esta margem é muito estreita para contê-la. (SINGH, 2010)

De acordo com Fermat não exite um trio de números que satisfaça a equação:

$x^n + y^n = z^n$, para x, y e $z \in \mathbb{Z}$ e $n \geq 3$.

Estava lançado o desafio que iria confundir e frustrar os matemáticos mais brilhantes do mundo por mais de três séculos, que ficou conhecido como o Último Teorema de Fermat. Este problema instigou a imaginação de muitos matemáticos e as tentativas infrutíferas de demonstração levaram a grandes avanços no conhecimento da Matemática, especialmente na teoria dos números.

2. O Nascimento do Enigma

A *Aritmética* que inspirou Fermat era uma tradução para o latim, feita por Claude Gaspar Bachet de Méziriac, que se dizia ser o homem mais culto de toda França. A *Aritmética* continha mais de cem problemas, e para cada um Diofante dava uma solução detalhada. Enquanto estudava esses problemas e suas soluções Fermat era levado a pensar em outras questões mais sutis e enfrentá-las. Mas limitava-se a escrever o que achava necessário para convencer a si mesmo de que tinha uma solução e então não se importava em registrar o resto da demonstração.

Seu filho mais velho, Clément-Smuel, passou cinco anos reunindo as cartas e anotações de seu pai nas margens de sua cópia da Aritmética, e então resolveu publicar estas anotações em uma edição especial. Em 1670, 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, estava quarenta e oito observações feitas por Fermat. (SINGH, 2010)

À medida que os séculos passavam, todas as observações foram demonstradas, uma por uma, mas o Último Teorema de Fermat se recusava a revelar seu mistério. De fato, ele é conhecido como o "último"teorema porque ficou sendo a última observação ainda por ser demonstrada. Ao longo dos anos o problema foi ficando famoso, tanto que ganhou a distinção de ser o problema matemático com maior número de demonstrações incorretas publicadas.

2.1. Fermat e o caso $n = 4$

Fermat publicou uma prova para $n = 4$, o expoente mais simples de lidar. Ele realizou isso introduzindo o *método da descida infinita*, que acabou sendo importante nas provas de muitos resultados da teoria dos números. A idéia é assumir que a equação $x^4+y^4 = z^4$ tem uma solução para alguns inteiros positivos a, b, c, e mostrar que, em seguida, tem uma solução para inteiros positivos u, v, w, com $w < c$. A repetição deste processo *ad infinitum* leva a uma contradição, uma vez que introduz uma sequência infinita decrescente de números inteiros positivos.(KLEINER, 2000) A demonstração completa pode ser vista em (EDWARDS, 2000).

O fato de que o Último Teorema de Fermat vale para $n = 4$ restringe nossa atenção ao caso em que n é um número primo ímpar. Veja que, primeiro, qualquer inteiro maior que 2 é divisível por um primo ímpar ou por 4 e, em seguida, que podemos escrever a equação

$x^{mk} + y^{mk} = z^{mk}$

como

$(x^m)^k + (y^m)^k = (z^m)^k$

Isso mostra que uma solução para o caso $n = mk$ permite obter de imediato uma solução para o caso $n = k$. Se n não for primo, nós sempre podemos escolher a fatorização de modo que k seja ou 4 ou um primo ímpar. Se já sabemos que não há solução nesses casos, não pode haver uma solução para n. Assim, o problema fica reduzido aos casos em que o expoente é primo ou é igual a quatro. (GOUVÊA, 1995)

3. Século XVIII

3.1. Euler e o caso $n = 3$

O gênio do século XVIII, Leonhard Euler, foi quem fez o primeiro avanço em direção à prova do Último Teorema de Fermat. Quando se deparou com o Último Teorema de Fermat, imaginou se não poderia provar que uma das equações não tinha solução e então generalizar o resultado para todas as outras restantes.

Euler tentou utilizar a prova do caso $n = 4$ como ponto de partida para construir uma demonstração geral para todas as outras equações. Tentou por primeiro uma demonstração para $n = 3$. Em 1753, Euler divulgou em uma correspondência que tinha adaptado o *método da descida infinita* de Fermat e conseguira demonstrar com sucesso o caso de $n = 3$. (SINGH, 2010)

Para fazer com que a prova de Fermat para o caso $n = 4$ cobrisse também o caso de $n = 3$, Euler teve de incorporar o número imaginário i, assim tapou as brechas na lógica e forçou o *método da descida infinita* a funcionar para o caso de $n = 3$. Mas fracassou ao tentar fazer seu argumento valer para os outros casos englobados pelo Último Teorema de Fermat, infelizmente. Detalhes do trabalho de Euler podem ser encontrado em (EDWARDS, 2000).

4. Século XIX

4.1. Sophie Germain

A jovem francesa revigorou a busca pela demonstração perdida do Último Teorema de Fermat. Sophie Germain (1776 - 1831) tomou conhecimento do teorema após se interessar pela teoria dos números. Trabalhou no problema durante vários anos e afinal chegou ao ponto em que acreditava ter feito uma descoberta importante.

Ela tenta fazer uma abordagem geral do problema. Seu objetivo era dizer algo sobre muitos casos de uma só vez. Tomou como base um tipo especial de número primo p de modo que $(2p + 1)$ também fosse primo. Germain desenvolveu um argumento elegante para demonstrar que provavelmente não existem soluções para $x^n + y^n = z^n$ para valores de n iguais a esses primos de Germain. Uma lista de números primos foi verificada por matemáticos da época a fim de provar que x, y ou z poderiam não ser múltiplos de n e acabaram demonstrando que para aqueles valores particulares de n não havia soluções.

Teorema 4.1. *Se n for um número ímpar primo e se $2n + 1$ é primo, então $x^n + y^n = z^n$ implica que x, y ou z é divisível por n.* (EDWARDS, 2000)

Teorema 4.2. *Seja n um número primo ímpar, se houver um número primo p auxiliar com as seguintes propriedades:*

1. $x^n + y^n = z^n \equiv 0$ *mod* p *implica que* $x \equiv 0$*, ou* $y \equiv 0$*, ou* $z \equiv 0$ *mod* p*, e*
2. $x^n \equiv n$ *mod* p *é impossivél*

se o Último Teorema de Fermat for verdadeiro para n*.* (EDWARDS, 2000)

Em 1825 Gustav Lejeune-Dirichlet e Adrien-Marie Legendre provaram que o caso $n = 5$ não tinha solução e ambos basearam sua prova e seu sucesso no trabalho de Sophie Germain. Quatorze anos depois, a França produziu outro avanço. Gabriel Lamé fez alguns acréscimos engenhosos ao método de Germain e conseguiu a demonstração para o número primo $n = 7$. (SINGH, 2010)

A descoberta de Germain para o Último Teorema de Fermat foi sua maior contribuição à matemática.

4.2. Gabriel Lamé, Louis Cauchy e Ernst Kummer

Então, 1847, Gabriel Lamé, que tinha demonstrado o caso de $n = 7$ alguns anos antes, e Augustin Louis Cauchy, outro dos melhores matemáticos de Paris, anunciaram que estavam a ponto de publicar uma demonstração completa. A expectativa aumentou em abril, quando Cauchy e Lamé publicaram detalhes vagos mas fascinantes de demonstrações no jornal da Academia.

No dia 24 de maio foi feito um anúncio que acabou com todas as especulações. Mas não foi nem Cauchy nem Lamé quem se dirigiu à Academia e sim Joseph Liouville. Liouville chocou sua audiência ao ler o conteúdo de uma carta do matemático alemão Ernest Kummer.

Kummer era um dos melhores teóricos dos números de todo o mundo. De acordo com ele, o problema fundamental era que as demonstrações de Cauchy e Lamé dependiam do uso de uma propriedade dos números conhecida como fatoração única. A fatoração única diz que só existe uma combinação de números primos que, ao serem multiplicados, produzirão determinado número. Por exemplo, a única combinação de números primos que produz o número 18 é: $2 \times 3 \times 3$

O fato de que a fatoração única é verdadeira para todos os números naturais é um elemento vital de muitas outras demonstrações e hoje é chamada de *teorema fundamental da aritmética*.

Infelizmente, ambas as demonstrações envolviam números imaginários. E embora a fatoração única seja verdadeira para os números naturais, ela pode se tornar falsa quando introduzimos os números imaginários, dizia Kummer. Em sua opinião esta era uma falha fatal. Kummer tinha mostrado que a demonstração completa do Último Teorema de Fermat encontrava-se além das abordagens da matemática da época. Era uma peça brilhante de lógica matemática, mas um golpe devastador em toda uma geração de matemáticos que tivera esperanças de resolver o mais difícil dos problemas. (SINGH, 2010)

5. Século XX

5.1. Prêmio Wolfskehl

Em 1908, o matemático Paul Wolfskehl legou um prêmio para uma prova do Último Teorema de Fermat. O prêmio, de 100 mil marcos, equivaleria a um milhão de dólares pelos padrões atuais. Este veio a ser conhecido como o Prêmio Wolfskehl. Sua condição era

que, se o prêmio não fosse concedido até 13 de setembro de 2007, nenhuma reclamação posterior seria aceita.

Parece que Wolfskehl tinha uma boa noção da dificuldade do problema, dando aos matemáticos mais 100 anos para chegar a uma prova.

5.2. O Avanço com os Computadores

Com a Segunda Guerra Mundial surgiram os primeiros computadores. Com a chegada das máquinas os casos mais difíceis do Último Teorema de Fermat podiam ser enfrentados com rapidez. Depois da Segunda Guerra Mundial, equipes de matemáticos e cientistas de computadores demonstraram o teorema para valoress de n até 500, depois para valores até 1000 e 10000. Na década de 1980, Samuel S. Wagstaff da Universidade de Illinois elevou o limite para 25000 e mais recentemente os matemáticos já podiam afirmar que o Último Teorema de Fermat é verdadeiro para todos os valores de n até 4 milhões. (SINGH, 2010)

Estas provas não usou apenas a força bruta dos computadores, mas eram uma mistura de sofisticada matemática teórica combinada com o uso de sofisticados cálculos. Entretanto, mesmo que os supercomputadores passassem décadas demonstrando um valor de n depois do outro, eles nunca poderiam demonstrar para todos os valores de n. Portanto, nunca poderiam demonstrar o teorema. Tudo o que os computadores podiam oferecer eram evidências a favor do Último Teorema de Fermat.

5.3. As Principais Personagens

Para termos uma idéia do que permitiu a prova do Último Teorema de Fermat faremos um esboço (muito) breve de algumas definições a fim de mostrar a ligação entre as curvas elípticas e as formas modulares.

5.3.1. Curvas Elípticas

As curvas elípticas não são nem curvas, nem elipses, entretanto, receberam este nome porque no passado eram usadas para medir o perímetro de elipses e os comprimentos das órbitas dos planetas. Simplificadamente vamos definir curvas elípticas como o conjunto de pontos que satisfazem um certo tipo de equação polinomial. Considere uma equação do tipo

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

onde os a_i são números inteiros. Nós queremos considerar o conjunto dos pontos (x, y) que satisfazem esta equação. (GOUVÊA, 1995) Uma curva E pode ser definida em $\mathbb{R}$, em $\mathbb{C}$ e em $\mathbb{Q}$, denotada, respectivamente, $E(\mathbb{R})$, $E(\mathbb{C})$ e $E(\mathbb{Q})$. (FALTINGS, 1995)

Existe um polinômio $\Delta = \Delta(a_1, a_2, a_3, a_4, a_5, a_6)$ nos coeficientes a_i tal que E é uma curva elíptica se e somente se $\Delta(E) \neq 0$. O número Δ é chamado o *discriminante* da curva E. Assim podemos fazer uma definição formal.

Definição 5.1. *Seja K um corpo. Uma curva elíptica sobre K é uma curva algébrica definida por uma equação do tipo*

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

onde os a_i pertencem a K e satisfazem a condição $\Delta(a_1, a_2, a_3, a_4, a_5, a_6) \neq 0$. (GOUVÊA, 1995)

Vamos focalizar nossa atenção no caso especial em que a equação é da forma $y^2 = g(x)$, com $g(x)$ um polinômio de grau 3 (assumindo que $a_1 = a_3 = 0$). Se r_1, r_2 e r_3 são as raízes do polinômio $g(x)$, o discriminante da equação $y^2 = g(x)$ é igual a

$$\Delta = \alpha(r_1 - r_2)^2(r_1 - r_3)^2(r_2 - r_3)^2,$$

onde α é uma constante.

Precisamos ainda tornar essas curvas fechadas. Fazemos isso acrescentando um outro ponto à curva, "um ponto no infinito ", denominado ∞. Podemos agora definir uma operação no conjunto dos pontos de uma curva elíptica, isto é, uma maneira de "somar "dois pontos. Esta operação torna a curva elíptica um grupo abeliano. O elemento neutro deste grupo é o ∞ e o inverso de (x, y) é $(x, -y)$. (GOUVÊA, 1995) (FALTINGS, 1995)

O fato de que qualquer curva elíptica tem uma estrutura de grupo abeliano nos permite aprender muito sobre ele, estudando vários dos seus subgrupos. Um subgrupo interessante E é o conjunto de todos os pontos cujas coordenadas são racionais $E(\mathbb{Q})$. Um ponto $P \in E(\mathbb{Q})$ corresponde a uma solução da nossa equação cúbica em números racionais. (GOUVÊA, 1995) (FALTINGS, 1995)

5.3.2. A Conjectura de Taniyama-Shimura e as Formas Modulares

A Conjectura de Taniyama-Shimura foi formulada por Taniyama em 1955 e subsequentemente (1960), refinada por seu amigo e colega Shimura. Para expor a Conjectura de Taniyama-Shimura, precisamos primeiro definir o que é uma função modular.

Seja $H = \{x + iy | y > 0\}$ o semi-plano superior complexo, isto é, o conjunto dos números complexos cuja parte imaginária é positiva.

Definição 5.2. *Denotamos por $\Gamma_0(N)$ o conjunto de todas as matrizes 2×2 $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ tais que:*

i) a, b, c, d são inteiros;
ii) o determinante $ad - bc = 1$;
iii) c é um múltiplo de N.

Além disso, este grupo atua no semi-plano superior tal que se $z \in H$, definimos

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot z = \frac{az + b}{cz + d}$$

Uma forma modular é uma função holomorfa $F : H \to \mathbb{C}$, que se transforma sob a ação de um dos grupos $\Gamma_o(N)$. Especificamente, exigimos que exista um inteiro positivo k tal que

$$F\left(\frac{az + b}{cz + d}\right) = (cz + d)^k F(z)$$

para toda matriz $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N)$

Uma função satisfazendo todas estas condições se chama uma *forma modular de*

peso k sobre $\Gamma_0(N)$. O número (N) é normalmente chamado o *nível* da forma modular F. (ADLER, 1994) (GOUVÊA, 1995)

Isto tudo é bem estranho e complicado, entretanto, dentro da nossa compreensão, podemos dizer que um tipo específico de forma modular se interliga com outro tipo esfecífico de curva elíptica. Essa ligação é extremamente poderosa, porque liga análise de um lado e álgebra de outro. (GOUVÊA, 1995)

Conjectura 5.3. *Conjectura Taniyama-Shimura. Dada uma curva elíptica $y^2 = Ax^3 + Bx^2 + Cx + D$ sobre $\mathbb{Q}$, existem funções modulares não constante $f(z)$, $g(z)$ do mesmo nível de N tal que*

$f(z)^2 = Ag(z)^3 + Bg(z)^2 + Cg(z) + D$. (COX, 1994)

Assim, Taniyama diz que uma curva elíptica sobre $\mathbb{Q}$ pode ser parametrizada por funções modulares. (COX, 1994)

Uma forma modular é definida por dois eixos, mas ambos os eixos são complexos, com uma parte real e uma parte imaginária, formando um espaço quadridimensional (com quatro dimensões,x_r,x_i,y_r, y_i). Este espaço quadridimensional é chamado de espaço hiperbólico, e é difícil sua visualização.

No final da década de 1960, hordas de matemáticos testaram a conjectura Taniyama-Shimura. Se a conjectura fosse verdadeira, ela permitiria que os matemáticos solucionassem problemas que tinham passado séculos sem serem resolvidos, abordando-os através do mundo modular. A grande esperança era no sentido desta unificação dos mundos elíptico e modular.(SINGH, 2010)

5.4. Gehard Frey e Ken Ribet

Em 1984, Gerhard Frey fez a afirmação extraordinária de que qualquer um que pudesse provar que a conjectura de Taniyama-Shimura era verdadeira também demonstraria imediatamente o Último Teorema de Fermat.

Frey explorou o que aconteceria se o Último Teorema de Fermat fosse falso, ou seja, se existisse pelo menos uma solução. Seja A, B, e C uma solução hipotética tais que:

$A^n + B^n = C^n$

Através de uma série hábil de complicadas manobras, Frey modelou a equação original de Fermat com sua solução hipotética para criar

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

Esta é uma curva elíptica com $a = A^n - B^n$, $b = 0$ e $c = -A^nB^n$.

Ao transformar a equação de Fermat em uma curva elíptica, Frey tinha ligado o Último Teorema de Fermat à conjectura de Taniyama-Shimura.

O argumento de Frey era o seguinte:

1. Se for verdade a conjectura de Taniyama-Shimura, então toda equação elíptica deve ser modular.
2. Se toda equação elíptica deve ser modular, então a equação de Frey não pode existir.
3. Se a equação elíptica de Frey não existe, então não podem existir soluções para a equação de Fermat.
4. Logo, o Último Teorema de Fermat é verdadeiro!

Faltava uma demonstração sólida de que isto era de fato assim. Esta conjectura foi provada por Ken Ribet, um professor da Universidade da Califórnia, em Berkeley. Depois de dezoito meses de esforços, Ribet finalmente demonstrou que a equação elíptica de Frey não é modular. Se alguém pudesse provar que toda equação elíptica é modular, isto implicaria que a equação de Fermat não teria solução e o Último Teorema estaria demonstrado. (SINGH, 2010)

Com isso podemos concluir o seguinte:
Teorema 5.4. *Suponha que a Conjectura Taniyama-Shimura seja verdadeira para toda curva elíptica semi-estável. Então o Último Teorema de Fermat é verdadeiro.* (GOUVÊA, 1995)

De fato, os matemáticos agora poderiam atacar o Último Teorema de Fermat adotando a estratégia da prova por contradição.

5.5. Andrew Wiles

Em 1975, Andrew Wiles começou sua carreira como estudante de pós-graduação na Universidade de Cambridge. Durante os três anos seguintes ele trabalhou em sua tese de Ph.D. e passou por seu aprendizado matemático.

Seu supervisor, John Coates, decidiu que Wiles deveria estudar uma área da matemática conhecida como curvas elípticas. Esta decisão se mostraria um ponto vital na carreira de Wiles e lhe daria as técnicas necessárias para uma nova abordagem do Último Teorema de Fermat.

Foi em 1986 que Wiles soube através de um amigo que Ken Ribet tinha demonstrado a ligação entre Taniyama-Shimura com o Último Teorema de Fermat.

Wiles sabia que para ter alguma esperança de encontrar uma prova ele teria que primeiro mergulhar completamente no problema. Assim, passou dezoito meses se familiarizando com cada elemento da matemática que fora usado ou que derivara das curvas elípticas e das formas modulares. Abandonou todos os trabalhos que não fossem relevantes para a demonstração do Último Teorema de Fermat e deixou de participar do circuito de conferências e colóquios, continuando apenas a ministrar aulas para os estudantes de graduação do departamento de matemática de Princeton. A partir do momento em que embarcou na busca pela demonstração, Andrew tomou a decisão de trabalhar em completo isolamento e segredo. A única pessoa que conhecia seu segredo era sua esposa, Nada. (SINGH, 2010)

Nos anos seguintes, Wiles faria uma série de descobertas extraordinárias, mas não publicou nem discutiu nenhuma delas até que sua demonstração estivesse completa.

Em 1991, diante de alguns fracassos nos seus estudos, Wiles decidiu que deveria voltar a circular de modo a ouvir os últimos boatos do mundo matemático. Numa grande conferência em Boston sobre curvas elípicas, Wiles tomou conhecimento de um estudante, chamado Matheus Flach, que estava aperfeiçoando um método criado por Kolyvagin, e parecia que este método era perfeito para o prolema. Passou a dedicar-se então ao desenvolvimento de Kolyvagin-Flach.

Depois de sete anos de esforço intenso, Wiles acreditava que o fim estava próximo. Semana após semana ele estava fazendo progresso. E foi inspirado por um trabalho de Barry Mazur, que Wiles conseguiu o que faltava para completar a sua demonstração. Por

volta de maio de 1993, Wiles tinha completado a demonstração da Conjectura Taniyama-Shimura e, consequentemente, o Último Teorema de Fermat.

No final de junho do mesmo ano, em uma conferência em Cambridge, Wiles decidiu anunciar ao resto do mundo a sua descoberta. A conferência seria realizada no Instituto Isaac Newton. O título das palestras de Wiles era "Formas Modulares, Curvas Elípticas e Representações de Galois ".

Muitos boatos circularam sobre o trabalho de Wiles e o que ele tinha para anunciar. Foram três palestras. A cada dia aumentava a audiência e a expectativa em cima do resultado. No dia 23 de junho, Andrew começou sua terceira e última palestra. Todas as pessoas que contribuíram para as idéias por trás da demonstração estavam presentes: Mazur, Ribet, Kolyvagin e muitos outros.

Ao final, após encerrar a demonstração com a declaração do Último Teorema de Fermat, Wiles disse: "Acho que vou parar por aqui ". (SINGH, 2010)

Wiles submeteu seu trabalho à revista *Inventiones Mathematicae*. Seis juízes foram selecionados para examinar seu manuscrito. Nick Katz, um dos juízes, detectou um erro, que exigiu de Wiles que reforçasse sua demonstração.

Depois de meses de muitas tentativas infrutíferas, Wiles convidou o professor Richard Taylor para lhe ajudar a consertar a demonstração. Juntos, trabalharam por mais de um ano até conseguirem solucionar o problema.

No dia 25 de outubro de 1994 dois manuscritos foram divulagados: "Curvas Elípticas Modulares e o Último Teorema de Fermat ", por Andrew Wiles. (WILES, 1995) E "Propriedades Teóricas de Anel em certas Álgebras de Hecke ", por Richard Taylor e Andrew Wiles. (TAYLOR; WILES, 1995)

A demonstração de Wiles para o Último Teorema de Fermat depende da verificação de uma conjectura criada na década de 1950. O argumento explora uma série de técnicas matemáticas desenvolvidas na última década, algumas inventadas pelo próprio Wiles. A demonstração é uma obra-prima da matemática moderna, o que leva a conclusão de que a demonstração de Wiles não é a mesma de Fermat, pois certamente ele não inventou as formas modulares, a conjectura Taniyama-Shimura e o método Kolyvagin-Flach séculos antes de todo mundo.

E se Fermat não tinha a demonstração de Wiles, o que é que ele tinha? Os matemáticos se dividem em dois grupos. Os céticos acreditam que o Último Teorema de Fermat foi o resultado de um raro momento de fraqueza de Fermat. Eles afirmam que, embora Fermat tenha escrito "eu tenho uma demonstração realmente maravilhosa ", ele de fato, só tinha uma demonstração equivocada. Já outros matemáticos, os otimistas românticos, acreditam que Fermat teria uma prova genuína. O que quer que tenha sido esta prova, ela teria sido baseada na matemática do século XVII, e teria um argumento tão astucioso que escapou a todos, de Euler a Wiles.

Embora Wiles tenha recorrido a métodos do século XX para resolver o enigma do século XVII, ele conquistara o desafio de acordo com as regras do comitê Wolfskehl. No dia 27 de junho de 1997, Andrew Wiles recebeu o Prêmio Wolfskehl no valos de 50 mil dólares. O Último Teorema de Fermat fora oficialmente provado.

Nas palavras de Wiles:

"Eu tive o raro privilégio de conquistar, em minha vida adulta, o que fora o sonho da minha infância. Sei que este é um privilégio raro, mas se você puder trabalhar, como adulto, com algo que significa tanto para você, isto será mais compensador do que qualquer coisa imaginável. Tendo resolvido este problema, existe um certo sentimento de perda, mas ao mesmo tempo há uma tremenda sensação de liberdade. Eu fiquei tão obcecado por este problema durante oito anos, pensava nele o tempo todo - quando acordava de manhã e quando ia dormir de noite. Isto é um tempo muito longo pensando só em uma coisa. Esta odisseia particular agora acabou. Minha mente pode repousar ". (SINGH, 2010)

Referências

ADLER, A. Fermat's last theorem: Lecture 1. July 1994.

COX, D. A. Introduction to fermat's last theorem. January 1994.

EDWARDS, H. M. *Fermat's Last Theorem, A Genetic Introduction to Algebraic Number Theory*. New York - USA: Springer-Verlag, 2000.

FALTINGS, G. The proof of fermat's last theorem by r. taylor and a. wiles. *Notices of the AMS*, v. 42, n. 7, p. 743 – 746, July 1995.

GOUVÊA, F. Q. Uma demonstração maravilhosa. *Matemática Universitária*, n. 19, p. 16–43, Dezembro 1995.

KLEINER, I. From fermat to wiles: Fermat's last theorem becomes a theorem. *Elemente der Mathematik*, v. 55, p. 19–37, 2000.

SINGH, S. *O Último Teorema de Fermat*. 17ª ediçao. ed. Rio de Janeiro: Editora Record, 2010.

TAYLOR, R.; WILES, A. Ring-theoretic properties of certain hecke algebras. *Annals of Mathematics*, n. 141, p. 553 – 572, January 1995.

WILES, A. J. Modular elliptic curves and fermat's last theorem. *Annals of Mathematics*, n. 141, p. 443 – 551, January 1995.