UNIVERSIDADE FEDERAL DO ESTADO DO RIO DE JANEIRO

CENTRO DE CIÊNCIAS EXATAS E TECNOLOGIA

PROFMAT – Mestrado Profissional em Matemática em Rede Nacional

O ÚLTIMO TEOREMA DE FERMAT PARA $n = 3$

AUTOR – Salvador da Silva Bruno

RIO DE JANEIRO / RJ

2014

Salvador da Silva Bruno

O Último Teorema de Fermat para $n = 3$

Trabalho de Conclusão de Curso apresentado ao Programa de Pós-graduação em Matemática PROFMAT da UNIRIO, como requisito para a obtenção do grau de MESTRE em Matemática.

Orientador: Silas Fantin
Doutor em Matemática pela USP

Rio de Janeiro – RJ
agosto de 2014

Bruno, Salvador da Silva

O Último Teorema de Fermat para $n = 3$ / Salvador da Silva Bruno – 2014

86.p

1.Matemática 2. Álgebra. I. Título

CDU 536.21

Salvador da Silva Bruno

O Último Teorema de Fermat para $n = 3$

Trabalho Final de Curso apresentado à Coordenação de Pós-Graduação *Stricto-sensu* da Universidade Federal do Estado do Rio de Janeiro, como requisito parcial para a obtenção do título de Mestre em Matemática pelo Programa PROFMAT.

Aprovada em 21 de agosto de 2014.

BANCA EXAMINADORA

Dr. Silas Fantin – UNIRIO – Orientador

Dr. Fabio Xavier Penna - UNIRIO

Dra. Miriam Abdon – UFF

Dedicatória

Dedico esse trabalho especialmente à minha esposa Simara, o grande amor da minha vida. *Aos meus pais Natale Bruno (em memória) e Maria Helena, ao meu maravilhoso e amado filho Matheus e ao meu Padrinho Wilson*.

"Para o mundo, você talvez seja só uma pessoa; mas, para uma pessoa você talvez seja o mundo".

-Josephine Bilings

Resumo

O objetivo deste trabalho é apresentar o caso $n = 3$ do Último Teorema de Fermat que afirma que: **"Não existe uma solução não trivial de três números inteiros x, y, z satisfazendo a equação $x^n + y^n = z^n$ para $n > 2$"**. Este resultado foi enunciado sem demonstração em 1637 por Fermat às margens do livro de Aritmética de Diofante. Foi preciso mais de 350 anos para ser conhecida uma prova definitiva deste resultado, conhecido como o Monte Everest da Teoria dos Números apresentada por Andrew Wiles em 1995 com versão preliminar em 1993. O primeiro avanço na direção da prova do Último Teorema de Fermat foi apresentado por Leonard Euler em 1770, após 133 anos do enunciado de Fermat, onde prova o caso $n = 3$.

A abordagem desse trabalho foi feita de forma a facilitar a compreensão do conteúdo de um aluno em nível de ensino médio e foi evitada a utilização de conhecimentos específicos que vão além da sua grade curricular, e devido a isso, houve uma grande preocupação com o uso da linguagem utilizada. No final do trabalho propomos algumas atividades que devem ser desenvolvidas em sala de aula.

Palavras-chaves: Fermat, Diofante, Pitágoras, Euler, Wiles.

Abstract

The objective of this final paper is to present the case of $n = 3$ of the last Fermat Theorem, which states that "there are no 3 integer numbers x, y, z satisfying the equation $x^n + y^n = z^n$ for $n > 2$" This result was released without demonstration in 1637 by Fermat on the Arithmetics book of Diofante It took more than 350 years for the final proof of this result being known. Named as the Mount Everest of the theory of numbers, it was presented by Andrew Wiles in 1995 but having its first version in 1993. The first step forward to the proof of Fermat last theorem was introduced by Leonard Euler in 1770 after 133 years of Fermat proof of $n = 3$.

The approach of this work was done in order to facilitate understanding of the content of a student at the high school level and has avoided the use of specific knowledge that goes beyond your curriculum, and because of this, there was great concern about the use the language used. At the end of the paper, we propose some activities to be developed in the classroom.

Keywords: Fermat, Diofante, Pitágoras, Euler, Wiles.

Agradecimentos

Gostaria de agradecer a Deus que sempre esteve ao meu lado me dando forças para superar todas as dificuldades, por ter me dado saúde para que eu pudesse chegar ao final dessa jornada e também a todos que, de alguma forma, contribuíram para que esse trabalho se concretizasse. Em especial gostaria de destacar:

- A minha mãe que sempre esteve ao meu lado orando muito por mim.
- A pessoa que me ensinou a ser um Homem forte, ético e de caráter. Que me ensinou a ser um chefe de família. Muito obrigado meu Pai onde o Sr estiver dedico todas essas conquistas ao Senhor
- A minha linda e amada esposa Simara pelo apoio, pelo suporte emocional e principalmente por superar a minha ausência em muitos finais de semana.
- Ao meu amado filho Matheus que me encanta todos os dias.
- Aos meus adorados irmãos Jorge, Wilson e Mauricio.
- Aos meus melhores amigos e mentores Cataldo, João Jorge (JJ) e Brener por todos os ensinamentos.
- Aos amigos Marcos, Felipe e João pelos finais de semana que estudamos juntos, que foram fundamentais para o término do curso.
- Ao Sensei Karmelito pelos ensinamentos da filosofia do Karatê.
- A minha querida turma de mestrado que simplesmente foi maravilhosa;
- Ao professor e orientador Silas Fantin.
- Aos ilustres professores da UNIRIO que acolheram nossa a turma 2012 do profmat com muita dedicação.
- Agradeço aos professores Fabio Xavier Penna e Miriam Abdon por terem aceito participar da banca Examinadora e pelas sugestões para aprimoramento do texto.
- A CAPES, pelo suporte financeiro, que permitiu a realização deste trabalho

Sumário

INTRODUÇÃO

"Os padrões criados pelos matemáticos, como os do pintor ou do poeta, devem ser belos; as ideias, como as cores ou as palavras, devem se encaixar de um modo harmonioso. A beleza é o primeiro desafio: não existe lugar permanente no mundo para a matemática feia."

G.H.Hardy

Nesta monografia abordaremos um caso particular do Último Teorema de Fermat enunciado sem demonstração em 1637 às margens do livro de Aritmética Diofante pelo matemático francês Pierre de Fermat que iria confundir e frustrar os matemáticos mais brilhantes do mundo por mais de 350 anos em busca de uma demonstração. A beleza deste teorema está no fato de que o problema em si é bem simples de entender e pode ser enunciado em termos familiares a qualquer estudante do ensino fundamental. Apesar disso, vidas inteiras foram devotadas à busca de uma demonstração para um problema aparentemente simples, e o mesmo ficou conhecido como o Monte Everest da Teoria dos números.

Geralmente, grande parte da dificuldade de um problema de matemática consiste em entender bem o enunciado, mas esse não é o caso do Último Teorema de Fermat que diz que: "***Não existe uma solução não trivial de três números inteiros*** x, y ***e*** z ***satisfazendo a equação*** $x^n + y^n = z^n$ ***para*** n ***maior do que*** 2".

As origens do último teorema de Fermat encontram-se na Grécia antiga, dois mil anos antes de Pierre de Fermat criar o problema na forma que conhecemos hoje. Portanto, ele liga os fundamentos da matemática criada por Pitágoras, as ideias mais sofisticadas da matemática moderna, e veremos que o Teorema de Pitágoras é o ancestral direto do Último Teorema de Fermat.

Apresentaremos agora uma descrição sucinta de cada capitulo, onde a bibliografia principal para a parte histórica é o livro do Simon Singh, dada pela referência [1].

No primeiro capítulo apresentaremos o protagonista principal de nosso trabalho que enunciou um dos problemas de aparência mais simples e familiar, pois é inspirado no

teorema de Pitágoras, e que desafiou as maiores mentes de matemática da história atrás de um prova por vários anos.

No segundo capítulo, apresentaremos o conceito de solução primitiva para a equação pitagórica e uma correspondência com pares de inteiros. Além disso, apresentaremos a prova do Último de Teorema de Fermat nos casos especiais $n = 4$ feita por Fermat e o caso $n = 3$ feita por Euler.

No terceiro capítulo, apresentaremos alguns ilustres matemáticos que não mediram esforços na tentativa de demonstrar o Último Teorema de Fermat. Mesmo não tendo chegado à prova definitiva todos foram fundamentais para o avanço da demonstração. O destaque maior é para o trabalho de Andrew Wiles, o jovem obstinado que aos dez anos afirmou que provaria o Último Teorema de Fermat e que, finalmente, no ano de 1993, após anos de muita dedicação e pesquisas, apresenta uma prova do Último Teorema de Fermat que continham alguns detalhes a ser aprimorada, sendo concluída em 1995.

Finalmente, no quarto capítulo, iremos propor algumas atividades que podem ser desenvolvidas em sala de aula a fim de enriquecer ainda mais o conhecimento dos alunos. Elas estão relacionadas com a abordagem que foi feita no decorrer deste trabalho.

CAPÍTULO 1

"A história do Último Teorema de Fermat está ligada profundamente à história da matemática, tocando em todos os temas da teoria dos números. Ela proporciona uma visão única do que impulsiona a matemática e, talvez ainda mais importante, o que inspira os matemáticos. O último Teorema é o coração de uma saga de coragem, fraudes, astúcia e tragédia, envolvendo todos os grandes heróis da matemática."

Simon Singh

Neste capítulo narraremos um pouco da vida de Pierre de Fermat, que viveu no século XVII, onde os profissionais calculistas da época inventavam métodos para fazer cálculos, fazendo todo o possível para mantê-los secretos, de modo a proteger sua reputação de serem os únicos capazes de resolver certos problemas. Fermat ficava plenamente satisfeito em criar novos teoremas sem ser perturbado, cuja publicação e o reconhecimento público nada significavam para Fermat.

1.1. O criador de enigmas e a evolução da teoria dos números

Pierre de Fermat nasceu em 20 de agosto de 1601, na cidade de Beaumont-de-Lomagne, no sudoeste da França, e teve a sorte de receber uma educação privilegiada em virtude das condições financeiras de sua família.

Não existe nenhum registro de que o jovem Fermat mostrasse qualquer talento especial para matemática.

Estudou no monastério franciscano, freqüentou a Universidade de Toulouse e se formou em direito na Universidade de Orléans. Devido às pressões familiares, foi para o serviço público, tornando-se Juiz Supremo na Corte Soberana do Parlamento.

Fermat teve uma ascensão rápida em sua carreira de servidor público. Em 1631, Fermat foi nomeado Conselheiro do Parlamento de Toulouse e Conselheiro na Câmara dos requerimentos. Se algum cidadão local quisesse fazer um requerimento ao Rei, sobre qualquer assunto, primeiro ele tinha que convencer Fermat e seus colegas da importância do pedido.

Por volta de 1652, Fermat ficou seriamente doente, em virtude de uma praga que estava devastando toda a Europa, e devido ao seu temperamento, evitava chamar as atenções sobre si. Após uma piora em seu estado de saúde, um de seus amigos anunciou a sua morte, sendo corrigida em seguida através de cartas aos amigos.

Além dos perigos para saúde na França do século XVII, Fermat tinha que sobreviver aos riscos da política. Sua nomeação para o Parlamento de Toulouse tinha sido três anos depois de o Cardeal Richelieu ser apontando primeiro ministro da França. Aquela era uma época de intrigas e tramas e todos os que estavam envolvidos no governo, mesmo no governo das províncias, tinham que tomar cuidado para não serem envolvidos nas armações maquiavélicas do cardeal.

Fermat adotou a estratégia de cumprir com suas obrigações de modo eficiente, mas sem chamar atenção para si mesmo. Ele não tinha grandes ambições políticas e fez o melhor que podia para evitar as disputas no parlamento. Na função de Juiz certa vez lavrou uma sentença que causou grande comoção, mandando queimar na fogueira um sacerdote que abusou de suas funções. Nas horas vagas, dedicava toda a energia que lhe sobrava à matemática, que se tornara seu hobby.

Fermat se correspondia regularmente com alguns intelectuais, através de cartas, *frequentemente não amigáveis*, e elas forneciam indícios sobre a vida diária de Fermat, incluindo seu trabalho acadêmico. Por ser de temperamento pacato e tentar evitar chamar as atenções sobre si, adotou a estratégia de ficar a maior parte do seu tempo recolhido em casa, onde se entretinha com a literatura clássica e com o estudo da Matemática.

Marin Mersenne (1588-1648), um grande amigo de Fermat, foi um grande impulsionador da Matemática, servindo como centro de distribuição de informação, através da correspondência trocada com outros matemáticos, pois gostava de espalhar as últimas descobertas e era contra a atmosfera de segredo tradicional. Mersenne parece ter sido o seu principal contato regular com matemáticos.

Mersenne uma vez escreveu-lhe perguntando se o número - muito grande - 100.895.598.169 era primo ou não. Tais questões geralmente levavam anos a serem resolvidas, mas Fermat replicou sem hesitação que o número era produto de 112.303 e 898.423, e que cada um desses fatores era primo. Mersenne encorajava Fermat a publicar os seus trabalhos e as suas demonstrações, mas este recusava sempre. *Para ele, a publicação e o reconhecimento público nada significavam*. Ficava plenamente satisfeito com o simples prazer de criar novos teoremas sem ser perturbado.

Fermat se comunicava com outros matemáticos unicamente para apresentar suas mais recentes descobertas, através de teoremas, ***sem fornecer a demonstração***, e desafiava seus correspondentes a apresentar uma demonstração para os resultados apresentados. Esconder a solução tinha motivações práticas, pois significava que ele não teria que perder tempo desenvolvendo seus métodos, podendo prosseguir diretamente para a próxima conquista. Desta forma, não é de se estranhar que a sua obra tenha ficado quase toda registrada na sua numerosa correspondência com os outros matemáticos da época, em textos não publicados, em notas marginais e em comentários escritos nos seus livros.

Fermat em conjunto com o matemático Blaise Pascal, descobriram as primeiras provas para a teoria da probabilidade, um assunto intrinsecamente incerto. Fermat também esteve envolvido na fundação de outra área da Matemática, o cálculo infinitesimal. As consequências do seu trabalho ajudaram a revolucionar a ciência, permitindo aos cientistas compreender melhor o conceito de velocidade e a sua relação com a aceleração. O próprio Newton (1642-1727), que foi quem desenvolveu e aprofundou esta área da matemática, baseou a sua teoria no método de traçar tangentes de Fermat.

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 da Matemática, a teoria dos números. Fermat era obcecado em entender as propriedades e as relações entre os números. Esta é a forma mais pura e antiga de Matemática, e Fermat estava ampliando um conhecimento que fora deixado por Pitágoras.

Depois da morte de Pitágoras, a ideia de demonstração matemática se espalhou rapidamente pelo mundo civilizado. No ano de 332 a.C., depois de conquistar a Grécia, a Ásia Menor e o Egito, Alexandre, o grande, decidiu construir uma capital que seria a

cidade mais importante do mundo. Alexandria foi de fato uma metrópole espetacular, mas só depois se tornaria um centro de estudos.

Somente quando Alexandre morreu e Ptolomeu I subiu ao trono do Egito é que Alexandria se tornou o lar da primeira universidade do mundo. Matemáticos e outros intelectuais emigraram para a cidade, e embora eles fossem certamente atraídos pela reputação da universidade, a atração principal era a Biblioteca de Alexandria que continha cerca de 600 mil livros. Os matemáticos podiam absorver todo o conhecimento do mundo estudando em Alexandria, e lá, para ensiná-los, estavam os mais famosos professores. O primeiro diretor do departamento de Matemática foi ninguém menos do que Euclides.

Euclides nasceu em 330 a.C. Como Pitágoras ele acreditava na busca da verdade matemática pura e não buscava aplicações para o seu trabalho. Uma história conta de um estudante que indagou ao mestre sobre a utilidade da Matemática que estava aprendendo. Depois de terminar a aula, Euclides virou para um de seus assessores e disse: "*De uma moeda ao rapaz, já que ele deseja ter lucros com tudo o que apreende e depois o dispense do curso*".

Euclides dedicou boa parte de sua vida ao trabalho de escrever *os Elementos*, escrita em 13 volumes e abrangendo grande parte da matemática da época. Euclides explorava uma arma lógica em sua obra conhecida como ***redução ao absurdo***, ou ***prova por contradição***. Sua abordagem envolve a ideia de provar que um teorema é verdadeiro, presumindo primeiro que a tese seja falsa. Explorando as consequências lógicas do teorema ser falso, obtêm se uma contradição de algum fato que sabemos ser verdade, e, portanto concluímos que o teorema original não pode ser falso, ou seja, o teorema deve ser verdadeiro.

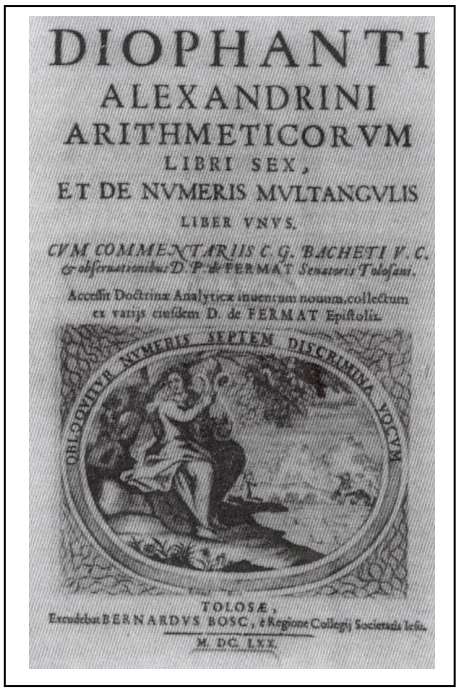
O matemático inglês G.H.Hardy resumiu o espírito da redução ao absurdo em seu livro *Apologia do matemático* da seguinte maneira: "Redução ao absurdo, que Euclides tanto amava, é uma das melhores armas do matemático. É um desafio muito maior do que qualquer jogo de xadrez pode praticar. O jogador de xadrez pode oferecer o sacrifício de um peão ou de uma peça mais importante, mas o matemático oferece o jogo inteiro.".

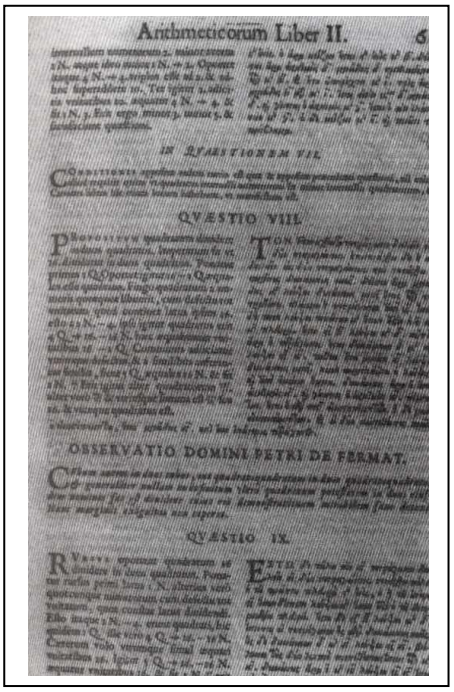
O matemático que escreveu um livro equivalente, sobre teoria dos números, foi Diofante de Alexandria, o último herói da tradição matemática grega. Embora as realizações de Diofante na teoria dos números estejam bem documentadas, quase nada se conhece sobre este matemático formidável. Presume-se que Diofante deve ter vivido antes

do ano 364 de nossa era, e uma data em torno de 250, é geralmente aceita como sendo a estimativa mais provável.

Um exemplo do tipo de problema que Diofante apreciava foi gravado na lápide de seu túmulo e dizia o seguinte: "*Deus lhe concedeu a graça de ser um menino pela sexta parte de sua vida. Depois por uns doze anos, ele cobriu seu rosto com a barba. A luz do casamento iluminou-o após a sétima parte de cinco anos depois do casamento. Ele concedeu-lhe um filho. Ah! criança tardia e má, depois de viver metade da vida de seu pai o destino frio o levou. Após consultar sua mágoa em ciência dos números, por quatro anos, Diofante terminou sua vida.*" O desafio é calcular quanto tempo Diofante viveu. A solução para este enigma pode ser encontrado no capitulo de atividades propostas.

Diofante viveu em Alexandria, e reuniu em seu tratado, intitulado *Aritmética*, diversos problemas bem conhecidos e criou uma série de novos problemas. Dos treze volumes que formavam a *Aritmética de Diofante*, somente seis sobreviveram e inspiraram matemáticos da renascença, incluindo Pierre de Fermat. Os outros sete livros foram perdidos numa série de acontecimentos trágicos que enviaram a Matemática de volta para a era babilônica.


DIOPHANTI
ALEXANDRINI
ARITHMETICORVM
LIBRI SEX,
ET DE NVMERIS MVLTANGVLIS
LIBER VNVS.
CVM COMMENTARIIS C. G. BACHETI V. C.
& observationibus D. P. de FERMAT Senatoris Tolosani.
Accessit Doctrinæ Analyticæ inventorum novum, collectum
ex variis ejusdem D. de FERMAT Epistolis.
OBLONGVM NVMERI SEPTEM DISCRIMINA IOCVM
TOLOSÆ,
Excudebat BERNARDVS BOSC, è Regione Collegij Societatis Iesu.
M. DC. LXX.


Arithmeticorum Liber II. 65
QVÆSTIO VIII.
OBSERVATIO DOMINI PETRI DE FERMAT.
QVÆSTIO IX.

Não há registros de que Fermat tenha adquirido o interesse pela Matemática graças à influência de algum tutor. Foi uma cópia da Aritmética que se tornou seu mestre. A aritmética tentava descrever a teoria dos números, como era no tempo de Diofante, através de uma série de problemas e soluções. Em um único livro Fermat podia encontrar todo o conhecimento dos números obtidos por gênios como Pitágoras e Euclides. A teoria dos números não progredira desde o bárbaro incêndio de Alexandria, mas agora Fermat estava pronto para retomar o estudo da mais fundamental de todas as disciplinas matemáticas.

Enquanto estudava o *Livro II da Aritmética*, Fermat encontrou toda uma série de observações, problemas e soluções relacionadas com o teorema de Pitágoras e os ternos pitagóricos. Fermat estava ciente de que Euclides conhecia infinitas ternas pitagóricas denominadas de primeiro e segundo tipo, que apresentaremos a seguir:

Observemos que podemos gerar infinitas ternas pitagóricas a partir de uma. De fato, como $3^2 + 4^2 = 5^2$ temos que $(3,4,5)$ é uma terna pitagórica, e a partir ela podemos gerar infinitas multiplicando por um inteiro positivo:

$$(3k, 4k, 5k) \overset{k \in \mathbb{N}}{\Rightarrow} \quad (6,8,10),\ (9,12,15),\ (12,16,20),\ \ldots$$

As ternas nesta lista são chamadas de NÃO primitivas porque são obtidas multiplicando $(3,4,5)$ por um número inteiro maior do que 1, enquanto $(3,4,5)$ é chamada terna pitagorica primitiva, isto é, uma terna pitagórica (a, b, c) é chamada primitiva se ela não é obtida a partir de outra multiplicando por uma constante inteira maior ou igual a 2.

Pitágoras observou que existe uma família infinita de ternas pitagóricas primitivas $(5,12,13)$, $(7,24,25)$, $(9,40,41)$, etc. Em todos os casos estudados por ele, um dos catetos e a hipotenusa são inteiros consecutivos (***chamadas de ternas pitagóricas clássicas de primeiro tipo***), isto é, ternas da forma $(a, b, b + 1)$. Para gerar uma fórmula para este tipo de ternas é suficiente observar que:

$$a^2 + b^2 = (b + 1)^2 \qquad \Rightarrow \qquad a^2 = (b + 1)^2 - b^2 = 2b + 1$$

Logo a é um número impar, isto é

$$a = 2k + 1 \ \Rightarrow \ 2b + 1 = a^2 = (2k + 1)^2 = 4k^2 + 4k + 1$$

Segue que

$$b = 2k^2 + 2k \qquad e \qquad c = b + 1 = 2k^2 + 2k + 1$$

Isto é, obtemos a família de ternas pitagóricas dadas por

$$(2k+1, 2k^2+2k, 2k^2+2k+1) \quad k \in \mathbb{N}$$

Por outro lado, Platão observou outra família de ternas primitivas em que a diferença entre a hipotenusa e um cateto é 2 (***conhecidas como ternas pitagóricas de segundo tipo***), isto é, ternas da forma $(a, b, b+2)$. Segundo o argumento anterior, temos que

$$a^2 + b^2 = (b+2)^2 \quad \Rightarrow \quad a^2 = (b+2)^2 - b^2 = 4b + 4 = 2(2b+2)$$

Assim, a é par, temos que:

$$a = 2s \quad \Rightarrow \quad 2(2b+2) = a^2 = 4s^2 \quad \Rightarrow \quad s^2 = b+1$$

Como estamos interessados em somente ternas pitagóricas primitivas, então b não pode ser par, pois a é par, assim da equação $b = s^2 - 1$, concluímos que s não pode ser impar, logo

$$s = 2k \quad \Rightarrow \quad b = s^2 - 1 = (2k)^2 - 1 = 4k^2 - 1 \quad e \quad c = (b+2) = 4k^2 + 1$$

E neste caso obtemos a família de ternas pitagóricas dadas por

$$(4k, 4k^2 - 1, 4k^2 + 1) \quad k \in \mathbb{N}$$

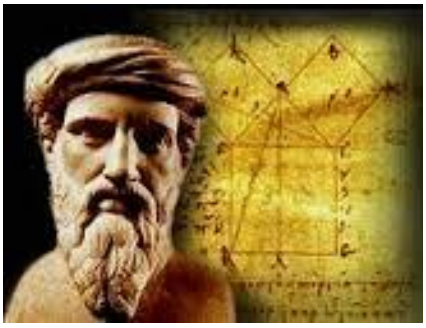
A seguinte tabela mostra as ternas obtidas a partir das equações de Pitágoras e Platão

k	$(2k+1, 2k^2+2k, 2k^2+2k+1)$	$(4k, 4k^2-1, 4k^2+1)$
1	(3,4,5)	(4,3,5)
2	(5,12,13)	(8,15,17)
3	(7,24,25)	(12,35,37)
4	(9,40,41)	(16,63,65)
5	(11,60,61)	(20,90,101)
6	(13,84,85)	(24,143,145)
7	(15,112,113)	(28,195,197)

1.2. A origem do problema

O último teorema de Fermat tem uma aparência simples e familiar porque é baseado num elemento da Matemática que todos conhecem, o teorema de Pitágoras, que afirma que: "*Num triangulo retângulo, o quadrado da hipotenusa é igual a soma dos quadrados dos catetos, em simbologia matemática,* $z^2 = x^2 + y^2$." Este resultado é bastante conhecido em virtude de ser abordado no ensino fundamental de nossas escolas, e o mesmo serviu de inspiração para um problema que desafiou as maiores mentes matemáticas da história.

No século VI a.C, Pitágoras de Samos foi uma das figuras mais influentes e, no entanto, misteriosas da Matemática. Como não existem relatos de sua vida e de seus trabalhos, Pitágoras está envolto no mito e na lenda, tornando difícil para os historiadores separar o fato da ficção. O que parece certo é que Pitágoras desenvolveu a ideia da lógica numérica e graças a sua iniciativa, os números deixaram de ser apenas coisas usadas meramente para contar e calcular, e passaram a ser apreciados por suas próprias características.



Pitágoras adquiriu suas habilidades matemáticas em suas viagens pelo mundo e por volta de 540 a.C. fundou a escola Pitagorica, reunindo muitos discípulos, que se transformou em uma sociedade secreta, regida por estranhos rituais e procedimentos.

Pitágoras observou que os egípcios e os babilônicos faziam seus cálculos na forma de uma receita que podia ser seguida cegamente. As receitas, que tinham sido passadas através de gerações, sempre produziam a resposta correta, e assim ninguém se preocupava em examinar, ou questionar, a lógica subjacente daquelas equações. O importante para essas civilizações era que os cálculos davam certo. Por que davam certo era irrelevante.

O que se sabe com certeza é que Pitágoras estabeleceu um sistema, que mudou o rumo da Matemática. A Irmandade pitagórica era realmente uma comunidade religiosa e um de seus ídolos era o número. Eles acreditavam que se entendessem as relações entre os números poderiam descobrir os segredos espirituais do universo, tornando-se assim

próximos dos deuses. De acordo com Pitágoras a perfeição numérica depende do número de divisores positivos distintos do próprio número. Por exemplo, os divisores de 12 são $\{1, 2, 3, 4, 6\}$. Quando a soma dos divisores de um número é maior do que ele, o número é chamado de "***excessivo***", e, portanto 12 é um número excessivo porque a soma de seus divisores é 16. Por outro lado, quando a soma dos divisores é menor do que o número ele é chamado "***deficiente***". É o caso de 10 porque seus divisores são $\{1, 2, 5\}$ e somam 8. Os números mais importantes e raros eram aqueles cujos divisores somados produziam ele mesmo, e estes eram chamados de números "***perfeitos***". O número 6 tem como divisores $\{1, 2, 3\}$ e somam 6 o que faz de 6 um número perfeito. O número perfeito seguinte é o 28 que possui divisores $\{1, 2, 4, 7, 14\}$.

Pitágoras percebeu que os números estavam ocultos em tudo, da harmonia da música até as órbitas dos planetas, o que o levou a proclamar que "*tudo é número*". Ao explorar o significado da Matemática, Pitágoras estava desenvolvendo uma linguagem que permitiria que ele e outros depois dele descrevessem a natureza do universo. Daí em diante cada avanço da Matemática daria aos cientistas o vocabulário de que necessitavam para explicar melhor os fenômenos que nos cercam. De fato, o desenvolvimento da Matemática iria inspirar revoluções na ciência.

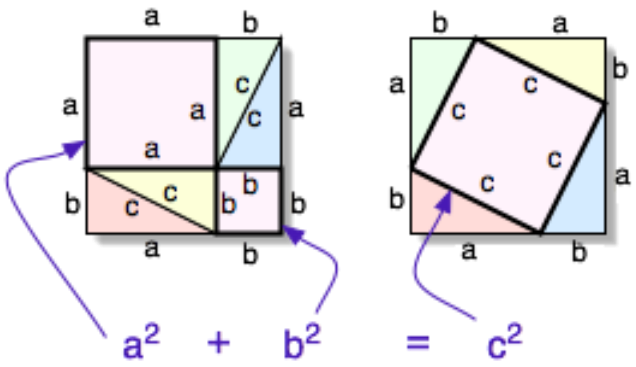
De todas as ligações entre os números e a natureza estudadas pela Irmandade, a mais importante é a relação que leva o nome de seu fundador. O teorema de Pitágoras nos fornece uma equação que é verdadeira para todos os triângulos retângulos que diz que: "***num triangulo retângulo o quadrado da hipotenusa é igual à soma dos quadrados dos catetos, em símbolos,*** $\boldsymbol{x^2 + y^2 = z^2}$."

O que é notável é que o teorema de Pitágoras é verdadeiro para todos os triângulos retângulos que puder imaginar, trata-se de uma lei universal da Matemática. Nesse ponto é importante mencionar que embora este teorema esteja eternamente associado a Pitágoras, ele já era usado pelos chineses e babilônicos mil anos antes. Contudo, estas culturas não sabiam que o teorema era verdadeiro para todos os triângulos retângulos. Era verdadeiro para os triângulos que tinham testado, mas eles não tinham meio de demonstrar que era verdadeiro para todos os triângulos que ainda não tinham testado. O motivo pelo qual o teorema leva o nome de Pitágoras é que ele foi o primeiro a demonstrar esta verdade universal. A razão para sua confiança esta no conceito de prova, ou demonstração matemática. ***A busca pela prova matemática é a busca pelo conhecimento mais absoluto do que o conhecimento acumulado por qualquer outra disciplina***.

A ideia da demonstração Matemática clássica começa com uma série de axiomas, declarações que julgamos serem verdadeiras ou que sejam verdades evidentes. Então, através da argumentação lógica, passo a passo, é possível chegar a uma conclusão. Se os axiomas estiverem corretos e a lógica for impecável, então a conclusão será inegável. Esta conclusão é o teorema.

Para Pitágoras a ideia da prova Matemática era sagrada, e foi esse tipo de demonstração que permitiu que a Irmandade descobrisse tanta coisa. A maioria das provas modernas é incrivelmente complexa e seguem uma lógica inatingível para o homem comum. Felizmente, no caso do teorema de Pitágoras, o argumento é relativamente direto e depende apenas de Matemática do nível fundamental. Apresentaremos três provas deste teorema:

Prova do Teorema de Pitágoras por Comparação de Áreas: Faça os seguintes passos:



Desenha-se um primeiro quadrado do lado esquerdo acima, de lado $(b + a)$, de modo a subdividir este quadrado em quatro retângulos, sendo dois deles quadrados de lados a e b respectivamente. Divide-se cada um destes dois retângulos não quadrados em dois triângulos retângulos, traçando-se as diagonais. Chama-se c o comprimento de cada diagonal. Concluímos que:

$$Área(■) - 4\,Área\,(◿) = a^2 + b^2 \qquad (I)$$

Desenha-se agora um segundo quadrado do lado direito acima, de lado $(b + a)$, e ao dividirmos os lados em segmentos de comprimento a e b, construímos um novo quadrado de lado c com vértices na interseção destes segmentos sobre o lado do quadrado original. Concluímos que

$$Área(■) - 4\,Área\,(◿) = c^2 \qquad (II)$$

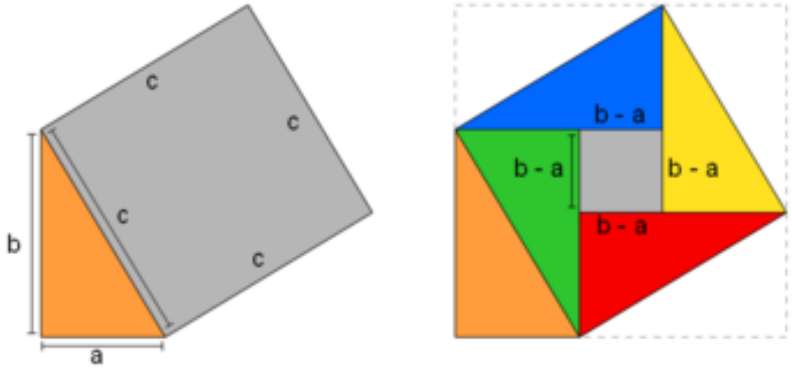
Segue de (I) e (II) que:

$$a^2 + b^2 = c^2. \quad \blacksquare$$

Prova do Pitágoras (em torno de 540 a.C.): Desenha-se um quadrado, conforme lado direito da figura acima, de lado $(b + a)$, e ao dividirmos os lados em segmentos de comprimento a e b, construímos um novo quadrado de lado c com vértice na interseção destes segmentos sobre o lado do quadrado original. Segue que

$$(a+b)^2 = 4\left(\frac{1}{2}a.b\right) + c^2 \quad \Rightarrow \quad a^2 + 2ab + b^2 = 2ab + c^2 \quad \Rightarrow \quad a^2 + b^2 = c^2 \ \blacksquare$$

Prova do Bhaskara (1114 – 1185): Faça os seguintes passos:



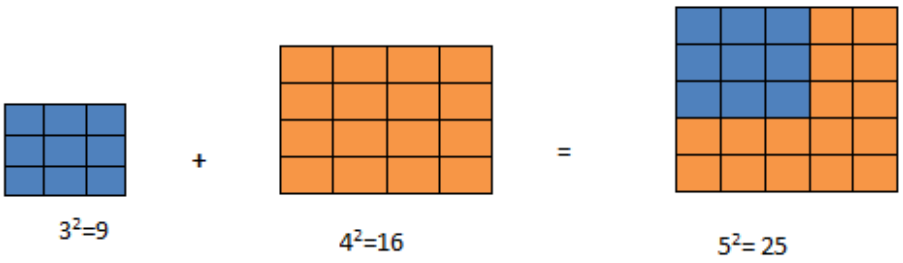
Construa um triângulo retângulo de catetos a e b, e hipotenusa c. Em seguida, construa um quadrado sobre a hipotenusa de lado c. A partir desta figura inicial com triangulo retângulo e quadrado, após fácil análise, podemos dividi-la conforme figura do lado direito acima e obtemos que:

$$c^2 = \text{Área}(\blacksquare) = 4\,\text{Área}\,(\triangle) + \text{Área}\,(\blacksquare) = 4\left(\frac{1}{2}a\,.\,b\right) + (b-a)^2$$

Segue que

$$c^2 = 2ab + b^2 - 2ab + a^2 \quad \Rightarrow \quad c^2 = a^2 + b^2\,. \ \blacksquare$$

Os ternos pitagóricos são combinações de três números inteiros que se ajustam perfeitamente a equação de Pitágoras $x^2 + y^2 = z^2$. Por exemplo, a equação de Pitágoras é verdadeira se $x = 3, y = 4$ e $z = 5$, pois $3^2 + 4^2 = 9 + 16 = 25 = 5^2$. outro modo de pensar nos ternos pitagóricos é relacioná-los ao ato de rearrumar quadrados. Têm-se um quadrado de 3 x 3 feito de 9 ladrilhos e um de 4 x 4 feito de 16 ladrilhos, então os ladrilhos podem ser rearrumados para formar um quadrado de 5 x 5 feito de 25 ladrilhos, conforme a figura a seguir:

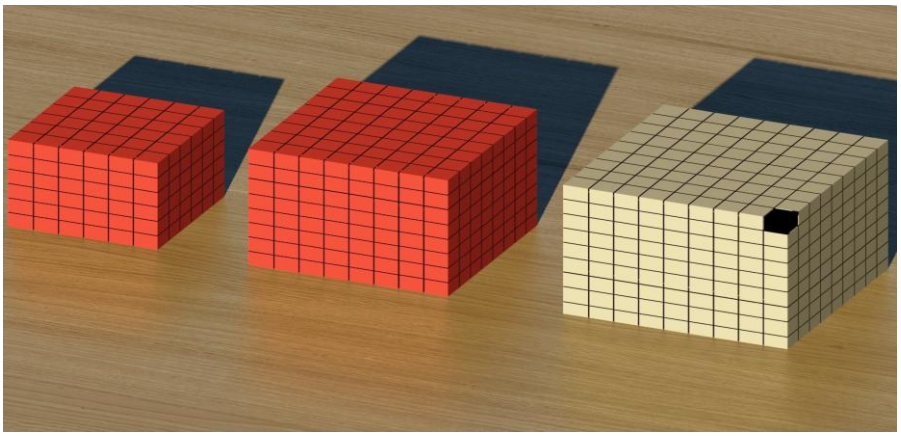


Os pitagóricos queriam encontrar outros trios pitagóricos, isto é, outros quadrados que pudessem ser somados para formar um terceiro quadrado maior. Outro trio pitagórico é $x = 5, y = 12$ e $z = 13$, pois $5^2 + 12^2 = 25 + 144 = 129 = 13^2$. Um trio pitagórico maior é $x = 99, y = 4.900$ e $z = 4901$. Os trios pitagóricos se tornam raros à medida que os números aumentar e encontrá-los se torna cada vez mais difícil. Para descobrir tantos trios pitagóricos quanto possível, os pitagóricos inventaram um método de encontrá-los e, ao fazê-lo, também demonstraram que há um número infinito deles. No capitulo de atividades propostas apresentaremos a demonstração de Euclides para a existência de infinitos trios pitagóricos.

Uma generalização do problema de rearrumação de ladrilhos, é mudarmos a potência de 2 para 3 na equação pitagórica, e buscarmos números inteiros positivos satisfazendo a equação cúbica $x^3 + y^3 = z^3$. Gerações de matemáticos não conseguiram encontrar números não nulos que se encaixem perfeitamente na equação elevada ao cubo. Na equação original quadrada o desafio era rearrumar os ladrilhos de dois quadrados para formar um terceiro quadrado maior. Na versão "***ao cubo***", o desafio é rearrumar dois cubos, feitos de tijolos, para formar um terceiro cubo, maior. Aparentemente não importa que tipos de cubos sejam escolhidos como ponto de partida, quando eles são combinados, o resultado ou é um cubo completo com alguns tijolos sobrando, ou um cubo incompleto. O

mais próximo de que alguém já chegou de um arranjo perfeito foi aquele em que falta um tijolo ou sobra um tijolo.

Por exemplo, se começarmos com os cubos de $6^3 = x^3$ e $8^3 = y^3$ e rearrumarmos os tijolos, então chegamos perto de construir um cubo de $9^3 = z^3$, faltando um cubinho para tal feito, conforme figura a seguir:



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

$$216 + 512 = 729 - 1$$

Além disso, se a potência for mudada de 3 (cubo) para qualquer número maior n (ou seja, $4, 5, 6, \ldots$), então a descoberta de uma solução se torna igualmente impossível. Parece não existir números inteiros para a equação mais geral:

$$x^n + y^n = z^n \quad para \quad n > 2$$

Ao meramente trocar o 2 na equação de Pitágoras por qualquer número maior, a busca por soluções para números inteiros deixa de ser um problema relativamente simples e se torna um desafio impossível.

Pierre de Fermat enquanto estudava o *Livro II de Aritmética de Diofante*, no lugar de considerar a equação pitagórica $x^2 + y^2 = z^2$ modificou a potência de 2 para 3, do quadrado para o cubo, mas sua nova equação aparentemente não tinha solução para nenhum numero inteiro. O método de tentativa e erro logo mostra a dificuldade de encontrar dois números elevados ao cubo que, ao serem somados, produzem outro número elevado ao cubo. Não dava para imaginar que uma pequena modificação na equação de

Pitágoras, que possui um número infinito de soluções, a transformasse em uma equação insolúvel, sem nenhuma solução em números inteiros não nulos.

Fermat alterou ainda mais a equação, trocando a potência para números maiores do que 3 e descobrindo que a busca de soluções para estas equações era igualmente difícil. De acordo com Fermat, parecia não existir um trio de números que se encaixasse perfeitamente na equação $x^n + y^n = z^n$ para $n > 2$. Na margem do livro de Aritmética, ao lado do problema 8, Fermat escreveu uma nota de sua observação:

> *E impossível para um cubo ser escrito como soma de dois cubos ou de uma quarta potencia ser escrita como uma soma de números elevados a quatro, ou em geral, para qualquer numero que seja elevado a uma potencia maior do que dois ser escrito como soma de duas potencias semelhantes.*

Fermat declarava que não podiam existir três números inteiros, todos não nulos, satisfazendo a "***equação fermatiana***". Era uma afirmação extraordinária, mas Fermat acreditava que poderia prová-la. Depois da primeira nota na margem, esboçando sua teoria, ele colocou um comentário adicional que iria assombrar gerações de matemáticos:

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

Este era Fermat no seu modo mais frustrante. Suas próprias palavras sugerem que ele estava particularmente satisfeito com sua demonstração "*realmente maravilhosa*", mas não se daria ao incômodo de escrevê-la em detalhe, quanto mais publicá-la. Ele nunca falou a ninguém sobre sua prova e, no entanto, apesar desta combinação de indolência e modéstia, o último teorema de Fermat, como mais tarde seria chamado, se tornaria famoso no mundo inteiro pelos séculos seguintes.

A notória descoberta de Fermat aconteceu no inicio de sua carreira como matemático, por volta de 1637, e como Fermat não era lembrado com saudade pelos seus correspondentes, havia o risco das descobertas de Fermat serem perdidas para sempre. Felizmente, seu filho mais velho, Clement-Samuel, percebia a importância do *hobby* de seu pai. Ele decidiu que aquelas descobertas não seriam esquecidas pelo mundo. É graças aos

seus esforços que sabemos alguma coisa sobre os avanços extraordinários feitos por Fermat na teoria dos números.

Depois que as observações de Fermat chegaram a uma comunidade maior, ficou claro que as cartas que ele tinha enviado aos seus colegas eram meras migalhas num banquete de descobertas. Suas notas pessoais continham uma série de teoremas. Infelizmente, ou esses teoremas não eram acompanhados por nenhuma explicação ou tinham apenas indícios da demonstração que os apoiava. Mas havia argumentos de lógica que deixaram os matemáticos na certeza de que Fermat tivera as demonstrações. A tarefa de recriá-las fora deixada como um desafio para as gerações futuras.

Os teoremas de Fermat variam daqueles que são fundamentais aos que são meramente divertidos. Os matemáticos avaliam a importância de um teorema de acordo com o seu impacto para o resto da Matemática. Em primeiro lugar, um teorema é considerado importante se contém uma verdade universal, isto é, se ele se aplica a todo um conjunto de números. No caso do teorema dos números primos, ele não é verdadeiro apenas para alguns números primos, e sim para todos. Em segundo lugar, os teoremas devem revelar alguma verdade profunda e subjacente a respeito do relacionamento entre os números. Um teorema pode ser o trampolim para a produção de todo um novo conjunto de teoremas, ou até mesmo inspirar o desenvolvimento de um novo ramo da Matemática. E, finalmente, um teorema é importante se ele resolver um problema em uma área de pesquisa anteriormente obstruída pela ausência de uma conexão lógica. Muitos matemáticos já se desesperaram sabendo que só poderiam obter um grande resultado se pudessem estabelecer um elo perdido em uma corrente lógica.

Como os matemáticos usam os teoremas como degraus para obter outros resultados, era essencial que cada um dos teoremas de Fermat fosse demonstrado. Só porque Fermat afirmava ter a prova para o teorema não podia ser aceito como verdade. Antes de poder ser usado, cada teorema tinha que ser demonstrado com rigor implacável, senão as consequências poderiam ser desastrosas. Por exemplo, imagine que os matemáticos tivessem aceitado um dos teoremas de Fermat. O teorema seria então incorporado como elemento de toda uma série de demonstrações maiores. E no devido tempo essas demonstrações passariam a fazer parte de outras, mais amplas ainda, e assim por diante. Finalmente, centenas de teoremas passariam a depender de que o teorema original, não verificado, fosse verdadeiro. Mas e se Fermat tivesse cometido um erro, e o teorema não provado estivesse errado? Todos os outros teoremas que o tivessem incorporados estariam

incorretos e grandes áreas da Matemática entrariam em colapso. Os teoremas são os alicerces da Matemática, porque uma vez que tenham sido estabelecidos como verdade, outros teoremas podem ser erguidos, em segurança, por cima deles. Ideias não fundamentada são muito menos valiosas e recebem o nome de conjecturas. Qualquer lógica que dependa de conjecturas é ela mesma, uma conjectura.

Fermat dizia ter uma demonstração para cada uma de suas observações, assim, para ele, eram teoremas. Contudo, até que a comunidade como um todo pudesse reconstruir as demonstrações para cada uma delas, as observações de Fermat seriam chamadas de conjecturas. De fato, nos últimos 350 anos, o último teorema de Fermat deveria ter sido chamado de a última conjectura de Fermat.

À medida que os séculos passavam, todas as observações foram demonstradas, uma por uma, mas o último teorema de Fermat se recusava a ceder seu segredo. De fato, ele é conhecido como o "Último" teorema porque ficou sendo a última observação ainda por ser demonstrada. Três séculos de esforços fracassados para obter uma demonstração levaram à notoriedade do mais famoso problema de Matemática. Contudo, esta reconhecida dificuldade não significa que o Último Teorema de Fermat seja um teorema importante, como descrito acima.

A fama deste teorema se deve unicamente pela enorme dificuldade em demonstrá-lo. E um estímulo extra é acrescentado, pelo fato de que Fermat dizer que podia prová-lo. Os comentários de Fermat na margem de seu exemplar da Aritmética foram lidos como um desafio para o mundo.

CAPÍTULO 2

“ Nunca perca a coragem quando seus bons propósitos não obtiverem os resultados esperados”

Santa Julia Billiart

Frequentemente o objetivo da demonstração Matemática é claro, mas o caminho pode ser bastante tortuoso e o matemático teme que cada passo possa estar levando sua argumentação na direção errada. Além disso, existe o temor de que o caminho certo não exista. Um matemático pode acreditar que uma conjectura é verdadeira, e perder anos tentando provar uma conjectura falsa.

Um dos mais importantes matemáticos proeminentes do século XVIII e de todos os tempos foi Leonhard Euler (1707 – 1783) e foi ele quem fez o primeiro avanço em direção a prova do último teorema de Fermat, provando o caso $n = 3$ que será o objetivo deste capitulo.

Euler tinha uma memória invejável e uma intuição tão incrível que se dizia que poderia fazer uma série de cálculos complexos de cabeça, sem precisar colocar a caneta no papel. Euler teve grandes contribuições em análise matemática e teoria dos números.

Na época de Fermat os matemáticos eram considerados calculistas amadores, mas no século XVIII eles já eram tratados como solucionadores profissionais de problemas. A cultura dos números tinha mudado, dramaticamente, e isto era em parte uma consequência dos cálculos científicos de ***Sir Isaac Newton***. Newton acreditava que os matemáticos estavam perdendo tempo desafiando uns aos outros com enigmas sem sentido. Ele queria aplicar a Matemática ao mundo físico, calculando tudo, das órbitas dos planetas as

trajetórias das balas de canhão. Quando Newton morreu em 1727, a Europa tinha passado por uma revolução cientifica e no mesmo ano, Euler publicou seu primeiro trabalho. Embora a publicação apresentasse uma Matemática elegante e inovadora seu objetivo era descrever uma solução para um problema relacionado a rastreamento de navios.

Euler adquiriu a reputação de ser capaz de resolver qualquer problema que lhe fosse apresentado, um talento que parecia se estender além dos campos da ciência. Quando Euler encontrou o último teorema de Fermat, ele deve ter-lhe parecido tão simples que ele deve ter pensado em resolvê-lo adaptando uma estratégia igualmente direta. Lembre que Fermat declarou que não existem soluções com números inteiros não nulos para a seguinte equação: $x^n + y^n = z^n$ para $n = 3, 4, 5, 6, 7, \ldots$. Euler imaginou se não poderia provar que uma das equações não tinha solução e então extrapolar o resultado para todas as outras restantes.

O trabalho de Euler recebeu um empurrão quando descobriu uma pista oculta nas anotações de Fermat. Embora Fermat nunca tenha escrito uma demonstração do seu último teorema, ele descreveu disfarçadamente, uma prova para o caso especifico $n = 4$ em outra parte do livro de Aritmética de Diofante, e a incorporou na demonstração de um problema totalmente diferente. Embora este fosse o cálculo mais completo que ele jamais colocou num papel, os detalhes eram vagos e incompletos. Fermat conclui a demonstração dizendo que a falta de tempo e de papel o impedia de apresentar uma explicação completa. Mas apesar da falta de detalhes nos escritos de Fermat, eles claramente ilustram uma prova por contradição conhecida como ***método de descida infinita***.

De modo a provar que não existem soluções para a equação $x^4 + y^4 = z^4$, Fermat começou presumindo que existe uma solução hipotética $x = x_1$, $y = y_1$ e $z = z_1$. Examinando as propriedades da trinca de inteiros (x_1, y_1, z_1), Fermat poderia demonstrar que se esta solução hipotética existisse, então existiria uma solução ainda menor (x_2, y_2, z_2) num certo sentido. E, ao analisar esta segunda solução, Fermat poderia mostrar a existência de outra solução ainda menor (x_3, y_3, z_3) e assim por diante.

Fermat tinha descoberto uma escadaria descendente de soluções que teoricamente, poderia continuar gerando números cada vez menores. Contudo se um destes números $x_i, y_i \; e \; z_i$ for sempre um inteiro positivo, teríamos que a escadaria infinita é impossível, porque entre um número inteiro positivo e o número zero existe somente uma quantidade finita de possibilidades. Esta contradição prova que a hipótese inicial que existe uma

solução (x_1, y_1, z_1) deve ser falsa. Usando o método da descida infinita, Fermat tinha demonstrado que a equação com $n = 4$ não pode ter nenhuma solução.

Euler tentou usar isso como ponto de partida para construir uma prova geral para todas as outras equações. Além de criar para todas as possibilidades possíveis ele teria que criar uma para n = 3, e foi este o primeiro degrau que tentou. No dia 4 de agosto de 1753, Euler divulgou em uma carta enviada ao matemático Prussiano Christian Goldbach, que tinha adaptado o método da descida infinita de Fermat e conseguira provar com sucesso o caso $n = 3$. Depois de 100 anos esta era a primeira vez que alguém conseguiu fazer algum progresso na direção de solucionar o desafio de Fermat.

Euler adaptou a prova de Fermat do caso $n = 4$ para o caso $n = 3$, utilizando um conceito pouco conhecido para a época, que hoje conhecemos por ***números imaginários***, uma entidade que fora descoberta pelos matemáticos europeus do século XVI. É estranho pensar em novos números sendo descobertos, mas isso é porque estamos tão acostumados com os números que usamos no dia a dia que esquecemos que houve uma época em que estes números não eram conhecidos.

No passado outros matemáticos tentaram adaptar o método de descida infinita de Fermat para resolver outros casos, alem de $n = 4$, mas cada uma dessas tentativas de estender a prova levava a brechas na lógica. Euler mostrou que, incorporando-se o número imaginário i em sua prova, ele poderia tapar os buracos na demonstração e forçar o método da descida infinita a funcionar para o caso $n = 3$.

Foi uma realização extraordinária, mas uma realização que não se pode repetir para os outros casos englobados pelo último teorema de Fermat. Infelizmente todas as tentativas de Euler de fazer seu argumento valer para outros casos de n, terminaram em fracasso.

Um século depois da morte de Fermat existiam demonstrações para apenas dois casos específicos do último teorema de Fermat deixou aos matemáticos uma boa pista com sua demonstração de que não existem soluções em inteiros não nulos para a equação $x^4 + y^4 = z^4$. Euler tinha adaptado a demonstração para provar que não existem soluções em inteiros não nulos para a equação $x^3 + y^3 = z^3$. Embora o progresso feito pelos matemáticos fosse muito lento, a situação não era tão ruim quanto podia parecer à primeira vista. A prova para o caso $n = 4$ também serve de demonstração para os casos de $n = 8, 12, 16, \ldots$, pois se a primeira equação $x^8 + y^8 = z^8$ têm solução, ao reescrevermos como $(x^2)^4 + (y^2)^4 = (z^2)^4$, renomeando, podemos afirmar que a equação dada por

$X^4 + Y^4 = Z^4$ tem solução, gerando uma contradição. De maneira análoga, a prova de Euler para $n = 3$ prova os casos para $n = 6, 9, 12, ...$

Subitamente duas famílias de números estavam comprovando o último teorema de Fermat e o mesmo parecia vulnerável. A demonstração para o caso $n = 3$ é particularmente significativa, porque 3 é um exemplo de número primo. Um número positivo é primo se seus únicos divisores positivos são 1 e ele mesmo for inteiro maior do que 1 e somente é divisível por 1 e ele mesmo. Os números primos são considerados os alicerces da teoria dos números. Para demonstrar o último teorema de Fermat para todos os valores de n, basta demonstrá-lo para valores primos de n. Todos os outros casos serão então meramente múltiplos dos casos primos e serão demonstrados implicitamente. Intuitivamente isto deveria simplificar bastante o problema, pois agora é possível ignorar as equações que envolvem um valor de n que não seja número primo e a quantidade de equações que resta se reduz imensamente, mas ainda existe uma infinidade de casos a serem comprovados.

A demonstração que existe uma infinidade de números primos vem da época de Euclides (330 a 260 a.C.), e constituiu uma das argumentações clássicas da Matemática. Inicialmente, Euclides supôs que a sucessão $p_1 = 2, p_2 = 3, \ldots, p_r$ dos r números primos seja finita. Façamos $P = p_1 . p_2 \ldots p_r + 1$ e seja p um numero primo que divide P. Esse número não pode ser igual a qualquer um dos números $p_1, p_2, \ldots, p_r$ porque então ele dividiria a diferença $P - p_1 . p_2 \ldots p_r = 1$, o que é impossível. Assim p é um número primo que não pertence à sucessão e, por conseqüência, $p_1, p_2, \ldots, p_r$ não podem formar o conjunto de todos os números primos.

Apresentaremos 2 (duas) novas provas para a afirmação que: "*Existe uma infinidade de números primos.*"

Prova 1: Em 1878, o matemático alemão Ernst Kummer (1810-1893) deu a seguinte variante da demonstração de Euclides:

Suponha por absurdo que exista somente um número finito n de números primos, isto é, digamos que:

$$(p_1 = 2) < p_2 < \cdots < p_n$$

e seja N o produto de todos os primos, isto é, $N = p_1 . p_2 \ldots p_n > 2$.

Como o número $(N-1)$ é inteiro, ao olharmos para sua fatoração em números primos, temos que $(N-1)$ teria um fator primo p_i, .e p_i também é um fator primo do N. Assim este fator p_i dividiria $1 = N-(N-1)$, o que é absurdo. ■

Prova 2: A demonstração de Métrod de 1917 é igualmente muito simples.

Suponha por absurdo que exista somente um número finito n de números primos, isto é, digamos que:

$$(p_1 = 2) < p_2 < \cdots < p_n$$

e seja N o produto de todos os primos, isto é, $N = p_1.p_2 \ldots p_n > 2$.

Para cada $i = 1,\ldots,n$, defina $Q_i = \frac{N}{p_i}$ e $S = Q_1 + \cdots + Q_n$. Claramente temos que p_j divide todos os Q_i se $(j \neq i)$ e p_j não divide Q_j . Assim nenhum p_j pode dividir S, pois senão p_j dividiria $S - \left(Q_1 + \cdots + \widehat{Q_j} + \cdots Q_n\right) = Q_j$. Como o número S é inteiro, ao olharmos para sua fatoração em números, existiria um primo $q \neq p_j$ para todo $j = 1,\ldots,n,$. o que gera um absurdo pois assumimos que somente existem os primos $p_1,\ldots,p_n$. ■

2.1. Solução primitiva

Nesta seção, apresentaremos os conceitos preliminares, para abordamos a demonstração do caso $n = 3$ do último teorema de Fermat, onde estudaremos brevemente a equação pitagórica.

$$X^2 + Y^2 = Z^2 \qquad (2.1)$$

Uma terna (x,y,z) de inteiros positivos satisfazendo a equação (2.1) tais que $x^2 + y^2 = z^2$ é chamado de "terna pitagórica". Por exemplo, $(3,4,5)$ é uma terna pitagórica visto que $3^2 + 4^2 = 5^2$. Se x,y,z são inteiros não nulos satisfazendo (1.1) tais que $x^2 + y^2 = z^2$ então $|x|,|y|,|z|$ também satisfazem a mesma equação. Note que x e y não podem ser ambos ímpares, pois caso contrário $z^2 = 4k + 2$, o que é impossível analisando $z = 4k + r$ com $r \in \{0,1,2,3\}$. Além disso, se $d = mdc\,(x,y,z)$ então $x/d, y/d, z/d$ também satisfazem a equação. Diremos que a terna (x,y,z) de inteiros é uma ***solução primitiva*** de $X^2 + Y^2 = Z^2$, se $x > 0$, $y > 0$, $z > 0$, x é par, $mdc\,(x,y,z) = 1$ e, portanto y e z são ímpares.

A próxima proposição estabelece uma correspondência entre o conjunto dos pares de inteiros positivos (a, b), primos entre si e de paridades distintas, com o conjunto das soluções primitivas (x, y, z) da equação pitagórica.

Proposição 2.1: *Se a, b são inteiros tal que $a > b > 0$ com $mdc\,(a, b) = 1$, onde a e b possuem paridades distintas se, e somente se, a terna (x, y, z) é uma solução primitiva da equação $X^2 + Y^2 = Z^2$ é dada por:*

$$\begin{cases} x = 2ab \\ y = a^2 - b^2 \\ z = a^2 + b^2 \end{cases}.$$

Prova: Se a, b são inteiros tal que $a > b > 0$ com $mdc\,(a, b) = 1$, seja x, y, z definido como indicado. Então

$$x^2 + y^2 = (2ab)^2 + (a^2 - b^2)^2 = 4a^2 b^2 + (a^2)^2 - 2a^2 b^2 + (b^2)^2 = (a^2 + b^2)^2 = z^2$$

Claramente $x > 0, y > 0\ e\ z > 0, x$ é par e $mdc\,(x, y, z) = 1$ porque se d divide $x, y\ e\ z$ então d divide $(y + z) = 2a^2\ e\ (z - y) = 2b^2$, assim $d = 1\ ou\ d = 2$, pois $mdc\,(a, b) = 1$, mas $d \neq 2$, pois y é ímpar visto que a e b tem paridades diferentes. Observamos que pares diferentes (a, b) dão ternas diferentes (x, y, z).

Reciprocamente, seja (x, y, z) uma solução primitiva de (1.1), assim $x^2 + y^2 = z^2$. Do $mdc\,(x, y, z) = 1$ temos que $mdc\,(x, z) = 1$, visto que x é par então z é impar e, portanto $mdc\,(z - x, z + x) = 1$. Como

$$y^2 = z^2 - x^2 = (z - x).(z + x),$$

Segue de sua decomposição em números primos que $(z - x)\ e\ (z + x)$ são quadrados de inteiros, isto e $(z + x) = t^2$ e $(z - x) = u^2$ onde $t\ e\ u$ são inteiros positivos impares com $t > u > 0$. Sejam a, b inteiros tais que:

$$\begin{cases} 2a = t + u \\ 2b = t - u \end{cases} \Rightarrow \begin{cases} t = a + b \\ u = a - b \end{cases} \quad \text{com} \quad a > b > 0$$

Assim

$$\begin{cases} x = \frac{1}{2}[t^2 + u^2] = \frac{1}{2}[(a+b)^2 - (a-b)^2] = 2ab \;\Rightarrow\; x = 2ab \\ y^2 = u^2\,t^2 = (a-b)^2\,.\,(a+b)^2 = \left(a^2 - b^2\right)^2 \;\Rightarrow\; y = a^2 - b^2 \\ z = \frac{1}{2}[t^2 - u^2] = \frac{1}{2}[(a+b)^2 + (a-b)^2] = a^2 + b^2 \;\Rightarrow\; z = a^2 + b^2 \end{cases}$$

Notamos que $mdc\,(a,b) = 1$ porque $mdc\,(z-x, z+x) = 1$ e finalmente $a+b = t$ é ímpar, assim a, b não são ambos ímpares. ■

Por exemplo, as menores soluções primitivas para (2.1), ordenadas em ordem crescente para valores de z, são as seguintes:

(3,4,5)	(12,5,13)	(8,15,17)	(24,7,25)
(20,21,29)	(12,35,37)	(40,9,41)	(28,45,53)
(60,11,61)	(56,33,65)	(16,63,65)	(48,55,73)

Em vista da Proposição 2.1, para encontramos as soluções primitivas da equação (2.1), basta determinarmos quais são os inteiros positivos impares que são somas de dois quadrados, e em cada caso, escrever todas estas representações.

Claramente todos os números primos podem se encaixados em duas categorias: aqueles que são iguais a $(4n+1)$ e aqueles que são iguais a $(4n-1)$, onde n é igual a algum número inteiro não nulo. Assim, 13 pertence ao primeiro grupo $(4x3+1)$, enquanto 19 pertence ao segundo grupo $(4x5-1)$.

Um resultado que Fermat conhecia:

[Um numero primo p é soma de 2 quadrados] $\Leftrightarrow$ [$p = 2$ *ou* $p = 4k+1$]

Observe que se um número primo p é soma de 2 quadrados, podemos escrever $p = a^2 + b^2$ então a e b não podem ser ambos pares, caso contrário, 4 divide p. Se a, b são ambos impares então $p = (2r+1)^2 + (2s+1)^2 = 4k+2$ então $p = 2$ pois é primo. Se a é par e b é impar então $p = (2r)^2 + (2s+1)^2 = 4k+1$.

Por exemplo, $13 = 2^2 + 3^2$, e o segundo tipo jamais pode ser escrito desse modo. Esta propriedade de números primos é bem simples, mas tentar provar que ela é verdadeira para cada um dos numerosos primos se torna muito difícil. Para Fermat era apenas uma de suas muitas demonstrações secretas. O desafio para Euler era reconstruir esta demonstração. Finalmente, em 1749, depois de sete anos de trabalho e quase um século depois da morte de Fermat, Euler teve sucesso, obtendo a prova para este teorema dos números primos.

2.2. A equação fermatiana biquadrática

Nesta seção estudaremos o caso $n = 4$. Ao investigar este caso, Femat estudou o problema de se a área de um triângulo pitagórico de lados (a, b, c) satisfazendo a equação $a^2 + b^2 = c^2$ pode ser o quadrado de um número inteiro, isto é, $Área\ (\triangle) = \frac{1}{2}\ a.b = d^2$, ou seja, $a.b = 2\ d^2$, observe que isso é falso para o triangulo pitagórico de lados (3,4,5). Fermat foi levado a estudar a equações do tipo $X^4 - Y^4 = Z^2$ e concluiu o seguinte:

Proposição 2.2*. As equações do tipo*

$$X^4 - Y^4 = Z^2$$

não possuem solução nos inteiros não nulos.

Prova: Se a afirmação é falsa, então considere (x, y, z) uma trinca de inteiros positivos com x o menor possível tal que $x^4 - y^4 = z^2$. Então o $mdc\ (x, y) = 1$, porque se um primo p divide x e y simultaneamente, então p^4 divide z^2 e, portanto p^2 divide z. Desta forma, fazendo $x = p.x_1$, $y = p.y_1$ e $z = p^2\ z_1$ temos que:

$$(px_1)^4 - (py_1)^2 = (p^2\ z_1)^2 \quad \Rightarrow \quad x_1^4 - y_1^4 = z_1^2$$

com $0 < x_1 < x,$ o que contradiz a hipótese para escolha inicial de x. Temos que

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

e o $mdc\,(x^2+y^2, x^2-y^2) = 1\ ou\ 2$, como pode ser visto facilmente, porque o $mdc\,(x,y) = 1$,

Caso 1: $mdc\,(x^2+y^2, x^2-y^2) = 1$

Visto que o produto de (x^2+y^2) e (x^2-y^2) é um quadrado então (x^2+y^2) e (x^2-y^2) são quadrados, mais precisamente, existem inteiros positivos s,t com $mdc\,(s,t) = 1$ tal que

$$\begin{cases} x^2+y^2 = s^2 \\ x^2-y^2 = t^2 \end{cases}$$

Segue que s,t devem ser ambos impares, visto que $2x^2 = s^2+t^2$ então s e t tem a mesma paridade e eles não podem ser ambos pares pois o $mdc\,(s,t) = 1$. Assim existem inteiros positivos u,v tais que

$$\begin{cases} u = \dfrac{1}{2}\,(s+t) \\ \\ v = \dfrac{1}{2}\,(s-t) \end{cases}$$

e necessariamente $mdc\,(u,v) = 1$ porque s e t são ambos impares. Temos que

$$u.v = \frac{1}{4}\,(s^2-t^2) = \frac{1}{2}\,y^2 \quad \Rightarrow \quad y^2 = 2uv$$

Como $mdc\,(u,v) = 1$ então existem inteiros positivos l,m tais que

$$\begin{cases} u = 2l^2 \\ v = m^2 \end{cases} \quad ou \quad \begin{cases} u = l^2 \\ v = 2m^2 \end{cases}$$

Iremos considerar a primeira alternativa, a outra é feita de maneira análoga. Deste modo, u é par, o $mdc\,(u,v,x) = 1$ e

$$u^2+v^2 = \frac{1}{4}(s+t)^2 + \frac{1}{4}(s-t)^2 = \frac{s^2+t^2}{2} = \frac{2x^2}{2} = x^2$$

Como $x^2 = u^2 + v^2$, segue da Proposição 2.1, que existem inteiros positivos a,b, com $0 < b < a$ com $mdc\,(a,b) = 1$ onde $u = 2l^2$ e $v = m^2$ tal que

$$\begin{cases} u = 2ab \\ v = a^2-b^2 \\ x = a^2+b^2 \end{cases}$$

Portanto $u = 2l^2 = 2ab$ segue que $l^2 = ab$. Como $mdc\,(a,b) = 1$, existem inteiros positivos c, d com $mdc\,(c,d) = 1$, tais que

$$\begin{cases} a = c^2 \\ b = d^2 \end{cases}$$

e assim $m^2 = v = a^2 - b^2 = c^4 - d^4$. Note que $0 < c < a < x$ e a trinca de inteiros positivos (c, d, m) seria uma solução da equação $X^4 - Y^4 = Z^2$, com $0 < c < x$, o que contradiz novamente a hipótese para escolha inicial de x como sendo o menor possível satisfazendo a equação.

Caso 2: $mdc\,(x^2 + y^2, x^2 - y^2) = 2$

Neste caso temos que x, e y são ambos impares e z é par. Como $x^4 - y^4 = z^2$ temos que $(z)^2 + (y^2)^2 = (x^2)^2$ e segue da Proposição 3.1, que existem inteiros positivos a, b com $0 < b < a,\ e\ mdc\,(a,b) = 1$ tal que

$$\begin{cases} z = 2ab \\ y^2 = a^2 - b^2 \\ x^2 = a^2 + b^2 \end{cases}$$

Portanto $(xy)^2 = x^2y^2 = (a^2 + b^2)(a^2 - b^2) = a^4 - b^4$ com $0 < a < x$ o que contradiz novamente a hipótese para escolha inicial de x como sendo o menor possível satisfazendo a equação. . ■

O argumento acima é chamado o ***método da descida infinita*** e foi inventado por Fermat e pode ser formulado da seguinte maneira: Se assumirmos que (x_0, y_0, z_0) é uma solução em inteiros positivos da equação $X^2 - Y^2 = Z^2$ então obteríamos uma nova solução em inteiros positivos (x_1, y_1, z_1) com a propriedade que $x_1 < x_0$. Repetindo este procedimento, iremos produzir uma sequência decrescente infinita de inteiros positivos

$$x_0 > x_1 > x_2 > \cdots$$

o que não é possível.

Como corolário da Proposição 2.2, obtemos a declaração original de Fermat, proposto como um problema a Marin Mersenne.

Corolário 2.3 (caso $n = 4$) *Não existe uma solução não trivial de inteiros, todos diferentes de zero, para a equação:*

$$X^4 + Y^4 = Z^4$$

Prova: Se x, y, z são inteiros não nulos tais que $x^4 + y^4 = z^4$ então $z^4 - y^4 = (x^2)^2$, o que contradiz a Proposição 2.2 ■

Como aplicação da Proposição 2.2 podemos concluir também o seguinte resultado.

Proposição 2.4 *A Área de um triângulo pitagórico nunca pode ser o quadrado de um número inteiro.*

Prova: Seja a, b, c os lados de um triângulo pitagórico, onde c é a hipotenusa. Assim $c^2 = a^2 + b^2$. Assuma que a área é um quadrado de um inteiro d, isto é,

$$área\ (\triangle) = \frac{1}{2}\, a\,.\, b = d^2 \quad \Rightarrow \quad ab = 2\, d^2$$

Então:

$$\begin{cases} (a+b)^2 = a^2 + 2ab + b^2 = c^2 + 4d^2 \\ (a-b)^2 = a^2 - 2ab + b^2 = c^2 - 4d^2 \end{cases}$$

Portanto

$$(a^2 - b^2)^2 = a^4 - 2a^2b^2 + b^4 = \underbrace{a^4 + 2a^2\, b^2 + b^4}_{c^4} - 4a^2b^2 = c^4 - (2d)^4$$

seria uma solução não trivial em inteiros para a equação $X^4 - Y^4 = Z^2$, contradizendo a Proposição 2.2. ■

Os resultados apresentados acima foram reproduzidos por Euler (1770) e Legendre (1808, 1830). Um resultado similar ao apresentado na Proposição 2.2 foi dado por Euler em 1770 que afirma o seguinte:

Proposição 2.5 (provada por Euler) *As equações do tipo*

$$X^4 + Y^4 = Z^2$$

não possuem solução nos inteiros não nulos.

Prova: Se a afirmação é falsa, então considere (x, y, z) uma trinca de inteiros positivos, com z o menor possível tal que $x^4 + y^4 = z^2$. Como na Proposição 2.2, podemos assumir que $mdc\ (x, y) = 1$. Observamos também que x, y não podem ser ambos impares, pois caso contrário $z^2 = x^4 + y^4 = 4k + 2$ e isto é impossível. Deste modo, por exemplo, podemos assumir que x é par.

De $(x^2)^2 + (y^2)^2 = z^2$ segue que (x^2, y^2, z) é uma solução primitiva da equação $X^2 + Y^2 = Z^2$. Pela Proposição 2.1 existem inteiros a, b tais que $a > b > 0$ com $mdc\ (a, b) = 1$, $a\ e\ b$ não são ambos impares onde

$$\begin{cases} x^2 = 2ab \\ y^2 = a^2 - b^2 \\ z = a^2 + b^2 \end{cases}.$$

Além disso, b deve ser par, pois se b é impar então a é par e $y^2 = a^2 - b^2$ podemos escrever $y^2 = 4k + 1$ o que é impossível.

Agora consideremos a relação $y^2 + b^2 = a^2$ onde y, b, a são inteiros positivos, b é par e $mdc\ (b, y, a) = 1$. Pela proposição 2.1, existem inteiros c, d tais que $c > d > 0, mdc\ (c, d) = 1$, c, d de paridades distintas onde

$$\begin{cases} b = 2cd \\ y = c^2 - d^2 \\ a = c^2 + d^2 \end{cases}$$

Portanto

$$x^2 = 2ab = 2.(c^2 + d^2).(2cd) = 4\ cd\ (c^2 + d^2)$$

mas $c, d, c^2 + d^2$ são dois a dois relativamente primos entre si.

Na decomposição de x^2 em fatores primos, concluímos que $c, d, c^2 + d^2$ são quadrados de inteiros positivos, digamos que

$$\begin{cases} c = p^2 \\ d = q^2 \\ c^2 + d^2 = r^2 \end{cases}$$

Portanto $p^4 + q^4 = c^2 + d^2 = r^2$, isto é, a trinca (p, q, r) é solução da equação $X^4 + Y^4 = Z^2$. Mas

$$z = a^2 + b^2 = (c^2 + d^2)^2 + (2cd)^2 = r^4 + 4c^2d^2 > r^4 > r \quad pois \ r > 1$$

o que contradiz a hipótese para escolha inicial de z como sendo o menor possível satisfazendo a equação $X^4 + Y^4 = Z^2$. ■

Corolário 2.6 (Conclusão do Euler para o caso $n = 4$) *Não existe uma solução não trivial de inteiros, todos diferentes de zero, para a equação:*

$$X^4 + Y^4 = Z^4$$

Prova: Se x, y, z são inteiros não nulos tais que $x^4 + y^4 = z^4$ então $x^4 + y^4 = (z^2)^2$, o que contradiz a Proposição 2.5 ■

Na tabela abaixo, citaremos alguns autores que apresentaram outras provas do Ultimo Teorema de Fermat para o expoente $n = 4$.

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

2.3. A equação fermatiana cúbica

Pierre de Fermat (1601-1665) em cartas a alguns matemáticos com quem se relacionava entre os quais destacamos: Mersenne (1640), Digby (1658) e Carcavi (1659), propôs o problema de mostrar que um cubo não pode ser igual à soma de dois cubos diferentes de zero.

Leonhard Euler (1707-1783) foi o primeiro a apresentar uma prova para o problema proposto por Fermat para o caso $n = 3$ do Ultimo Teorema de Fermat. Euler utilizou o método de descida infinita criado por Fermat e a prova deste resultado apareceu em seu livro de Álgebra, publicado em São Petersburgo em 1770, traduzido para o alemão em 1802 e para o inglês em 1822. Um estudo crítico da prova de Euler descobriu que não foi apresentado um passo importante, sobre as propriedades de divisibilidade de números inteiros da forma $a^2 + 3b^2$. No artigo de 1760, Euler já havia provado rigorosamente que se um número primo impar p divide $a^2 + 3b^2$ onde a e b são inteiros não nulos e primos entre si, então existem inteiros u, v tal que $p = u^2 + 3v^2$. No entanto, Euler não estabeleceu plenamente os passos que são exigidos na prova. Legendre reproduziu a prova de Euler, em seu livro de (1808, 1830) sem completar os detalhes.

Em 1875, Pepin publicou um longo artigo sobre números da forma $a + b\sqrt{-c}$ apontando os argumentos que tinham sido insuficientemente justificados por Euler referentes números da forma $a^2 + cb^2$, especialmente para $c = 1,2,3,4,7$. Schumacher (1894) observou explicitamente o elo que faltava na prova. Em 1901, Landau ofereceu uma prova rigorosa; isto foi mais uma vez objeto de estudo no artigo de Holden (1906), e outra vez em 1915, onde uma prova detalhada apareceu no livro de Carmichael. Em 1966, Bergmann publicou um artigo com considerações históricas e uma análise aprofundada da prova de Euler. Mais uma vez, em 1972, R. Legendre ressaltou que a prova de Euler não era perfeita e Edwards em 1977 discutiu também em seu livro esta prova.

Teorema 2.7 (Caso $n = 3$) *Não existe uma solução de inteiros não nulos para a equação:*

$$X^3 + Y^3 + Z^3 = 0$$

Prova: Assuma que x, y *e* z são números inteiros não nulos, primos entre si dois a dois, tais que $x^3 + y^3 + z^3 = 0$. Então eles devem ser distintos (porque 2 não é um cubo), e exatamente um destes inteiros é par, digamos que x e y são impares e z é par. Entre todas as soluções com as propriedades acima escolhemos uma para o qual |z| é a menor escolha possível.

Vamos encontrar inteiros p, m, n primos entre si dois a dois, satisfazendo a equação $p^3 + m^3 + n^3 = 0$, onde n é par e $|z| > |n|$. Isto irá gerar uma contradição, pois teremos uma sequência infinita descendente de inteiros positivos.

Visto que x *e* y são impares, $(x + y)$ *e* $(x - y)$ são pares, então existe inteiros a *e* b tal que $(x + y) = 2a$ *e* $(x - y) = 2b$. Assim $x = (a + b)$ *e* $y = (a - b)$, e portanto a *e* b são não nulos com $mdc\,(a, b) = 1$ e de paridades diferentes. Segue da equação $x^3 + y^3 + z^3 = 0$ que:

$$-z^3 = x^3 + y^3 = (a + b)^3 + (a - b)^3 = 2a\,(a^2 + 3b^2)$$

Como $(a^2 + 3b^2)$ é ímpar, pois a *e* b tem paridades diferentes e z é par, portanto 8 divide z^3 e assim 8 divide $2a$. Portanto a é par e b é impar.

Se a é par e b é impar então $mdc\,(2a, a^2 + 3b^2) = 1\ ou\ 3$. De fato, seja q um primo e q^k um fator comum dos termos acima, isto é, $2a = q^k c$ *e* $(a^2 + 3b^2) = q^k d$. Como $(a^2 + 3b^2)$ é ímpar, pois b é impar, logo $q \neq 2$ e q^k divide a e assim q^k divide $3b^2$. Como $mdc\,(a, b) = 1$ e q divide a então q não divide b e como divide $3b^2$ concluímos que $k = 1$ *e* $q = 3$. Agora consideremos os 2 casos:

Caso 1: $mdc\ (2a, a^2 + 3b^2) = 1$

Claramente 3 não divide a pois se 3 divide a então $mdc\ (2a, a^2 + 3b^2) \geq 3$. Da equação $-z^3 = 2a\ (a^2 + 3b^2)$ e da fatoração única de inteiros em primos, temos que $(2a)$ e $(a^2 + 3b^2)$ são cubos:

$$\begin{cases} 2a = r^3 \\ a^2 + 3b^2 = s^3 \end{cases}$$

onde s é ímpar e não é um múltiplo de 3. Neste ponto faremos uso de um fato que justificaremos mais tarde: Se s é ímpar e $s^3 = (a^2 + 3b^2)$ com $mdc\ (a, b) = 1$ então s também será da forma $s = (u^2 + 3v^2)$ com $u, v \in \mathbb{Z}$ e

$$\begin{cases} a = u\ (u^2 - 9v^2) \\ b = 3v\ (u^2 - v^2) \end{cases}$$

Deste modo, temos que v é ímpar, u é par (porque b é impar), u é não nulo, 3 não divide u (visto que 3 não divide a) e $mdc(u, v) = 1$. Portanto $2u, (u + 3v), (u - 3v)$ são relativamente primos aos pares e da equação

$$r^3 = 2a = 2\,.\,u(u^2 - 9v^2) = 2u\ (u - 3v)\ (u + 3v)$$

Segue que $2u, (u + 3v), (u - 3v)$ são cubos:

$$\begin{cases} 2u = -n^3 \\ u - 3v = p^3 \\ u + 3v = m^3 \end{cases}$$

e temos que na terna (p, m, n) todos são distintos de 0 (visto que 3 não divide u) e relativamente primos entre si dois a dois e satisfazem a equação $X^3 + Y^3 + Z^3 = 0$, pois

$$p^3 + m^3 + n^3 = (u - 3v) + (u + 3v) - 2u = 0$$

onde n é par e $|z| > |n|$. De fato:

$$\begin{aligned} |z|^3 &= |2a\,.\,(a^2 + 3b^2)| \\ &= \left|2.u\,.\,\underbrace{(u^2 - 9v^2)}_{p^3.m^3 \neq 0}.\ \underbrace{(a^2 + 3b^2)}_{\geq 3\ pois\ b\ impar}\right| \\ &\geq |-n^3|\,.\,|p^3m^3|\,.\,3 \\ &> |n^3| \end{aligned}$$

e isto contradiz a escolha inicial da terna (x, y, z) solução da equação $X^3 + Y^3 + Z^3 = 0$ para o qual $|z|$ é a menor escolha possível.

Caso 2: $mdc\ (2a, a^2 + 3b^2) = 3$

Escrevemos $a = 3c$. Como 8 divide $2a$ segue que 4 divide c, c é par, e 3 não divide b visto que $mdc\ (a, b) = 1$ são primos entre si. Assim

$$-z^3 = 2a\ (a^2 + 3b^2) = 2.(3c).[(3c)^2 + 3b^2] = 18c.(3c^2 + b^2)$$

Afirmamos que $mdc\ (18c, 3c^2 + b^2) = 1$. De fato, como c é par e b é ímpar temos que $(3c^2 + b^2)$ é ímpar, 3 não divide $(3c^2 + b^2)$ pois 3 não divide b e $mdc(b, c) = 1$. Pela fatoração única de inteiros, temos que $18c\ e\ (3c^2 + b^2)$ são cubos:

$$\begin{cases} 18c = r^3 \\ 3c^2 + b^2 = s^3 \end{cases}$$

onde s é impar e 3 divide r. Neste ponto faremos novamente uso de um fato que justificaremos mais tarde: Se s é impar e $s^3 = (b^2 + 3c^2)$ com $mdc\ (b, c) = 1$ então s também será da forma $s = (u^2 + 3v^2)$ com $u, v \in \mathbb{Z}$ e

$$\begin{cases} b = u\ (u^2 - 9v^2) \\ c = 3v\ (u^2 - v^2) \end{cases}$$

Deste modo, temos que u é impar, v é par (porque b é impar), $v \neq 0$, e $mdc\ (u, v) = 1$. Portanto $2v, (u + v), (u - v)$ são relativamente primos dois a dois e da equação

$$r^3 = 18c = 18.[\ 3v.(u^2 - v^2)\ ] = 54v.(u + v).(u - v)$$

deduzimos que

$$\left(\frac{r}{3}\right)^3 = 2v.(u + v).(u - v).$$

Portanto $2u, (u + 3v), (u - 3v)$ são cubos:

$$\begin{cases} 2v = -n^3 \\ u + v = p^3 \\ u - v = -m^3 \end{cases}$$

e temos que na terna (p, m, n) todos são distintos de 0, relativamente primos entre si dois a dois e satisfazem a equação $X^3 + Y^3 + Z^3 = 0$, pois

$$p^3 + m^3 + n^3 = (u + v) + (v - u) - 2v = 0$$

onde n é par e $|z| > |n|$.

De fato:

$$
\begin{aligned}
|z|^3 &= |18.c.(3c^2+b^2)| \\
&= \left|9\,.\,2\,.\underbrace{3v\,(u^2-\,v^2)}_{c}\,.(3c^2+b^2)\right| \\
&= 27\,|2v\,.(u^2-v^2)|\,.\,|3c^2+b^2| \\
&> 3^3\,.\,|n|^3\,.\,\underbrace{|u^2-v^2|}_{-p^3m^3\neq 0}\,.\,\underbrace{|3c^2+b^2|}_{\geq 1} \\
&> |n|^3
\end{aligned}
$$

e outra vez isto contradiz a escolha inicial da terna (x, y, z) solução da equação $X^3 + Y^3 + Z^3 = 0$ para o qual |z| é a menor escolha possível. ■

Com o Lema a seguir, estabelecemos a justificativa restante usado na prova do Teorema anterior.

Lema 2.8: *Se s é impar e* $s^3 = (a^2 + 3b^2)$ *com* $mdc\,(a, b) = 1$ *então s também será da forma* $s = (u^2 + 3v^2)$ *com* $u, v \in \mathbb{Z}$ *e*

$$
\begin{cases} a = u\,(u^2 - 9v^2) \\ b = 3v\,(u^2 - v^2) \end{cases}
$$

Prova: Para esta prova, são usados argumentos já conhecidos por Fermat, em conexão com o estudo de inteiros da forma $u^2 + 3v^2$. Seja S o conjunto de todos os inteiros da forma $(a^2 + 3b^2)$, com $a, b \in \mathbb{Z}$. S é claramente fechado para a multiplicação, pois

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

onde a igualdade esta assegurada com os sinais correspondentes. Para mostrar que s também pode ser escrito da forma $s = u^2 + 3v^2$ com $u, v \in \mathbb{Z}$, pode ser consultada a referência bibliográfica: [**2] –página 30 – Lema 4.7**:

$$
\begin{aligned}
(u^2 + 3v^2)^2 &= (u^2)^2 + 2.u^2.3v^2 + (3v^2)^2 \\
&= u^4 \underbrace{-6u^2v^2 + 12u^2v^2}_{+\,6.s^2.v^2} + 9v^4 \\
&= u^4 - 6u^2v^2 + 9v^4 + 12u^2v^2 \\
&= (u^2 - 3v^2)^2 + 3(2uv)^2
\end{aligned}
$$

Segue que

$$s^3 = (u^2 + 3v^2)^3$$

$$= (u^2 + 3v^2).(u^2 + 3v^2)^2$$

$$= (u^2 + 3v^2).[\ (u^2 - 3v^2)^2 + 3(2uv)^2\ ]$$

$$= [\ u(u^2 - 3v^2) - 3v(2uv)]^2 + 3\ [\ u(2uv) + v(u^2 - 3v^2)\ ]^2$$

$$= \left(u^3 \underbrace{-3uv^2 - 6uv^2}\right)^2 + 3\ \left(\underbrace{2vu^2 + vu^2} - 3v^3\right)^2$$

$$= \left[\underbrace{u\ (u^2 - 9v^2)}_{a}\right]^2 + 3\ \left[\underbrace{3v\ (u^2 - v^2)}_{b}\right]^2$$

$$= a^2 + 3\ b^2$$ por hipótese.

Comparando as expressões na igualdade, segue que:

$$\begin{cases} a = u\ (u^2 - 9v^2) \\ b = 3v\ (u^2 - v^2) \end{cases}$$ ■

Na tabela abaixo, citaremos alguns autores que apresentaram outras provas do Último Teorema de Fermat para o expoente $n = 3$.

Autor	**Ano**
Euler	1770.
Kausler	1795/6 (publicado 1802)
Legendre	1823, 1830
Calzolari	1855
Lamé	1865
Tait	1872
Günther	1878
Gambioli	1901
Krey	1909
Rychilik	1910
Stockhaus	1910
Carmichael	1915
Van der Corput	1915
Thue	1917
Duarte	1944

CAPÍTULO 3

"Não existe alegria ou recompensa maior que fazer uma diferença fundamental na vida de uma pessoa"

Irmã Mary Rose McGeady

Vimos no capitulo anterior, que Euler ao usar o método de descida infinita de Fermat conseguiu provar o Último teorema para o caso $n = 3$, e assim para todos os seus múltiplos , a saber, 6,9,12,... o que foi uma realização extraordinária. Esta demonstração é bastante significativa, pois 3 é um número primo, e os mesmos são considerados os alicerces da teoria dos números. Bastava agora provar o Último Teorema de Fermat para os números primos, o que reduziria um pouco o trabalho.

Desde a época de Euclides (540 a.C.) já se sabia que existiam infinitos números primos e a prova de Euclides para esta fato, constitui uma das demonstrações clássicas da Matemática. Nas atividades propostas apresentaremos duas novas provas elementares da existência de infinitos números primos, que são variantes da argumentação utilizada por Euclides.

Neste capítulo descreveremos algumas das tentativas de grandes matemáticos para solucionar o Último Teorema de Fermat durante mais de dois séculos. Apesar dos fracassos eles foram importantes na construção de um arcabouço matemático para desembocar nas últimas tentativas de se conseguir demonstrar o Teorema e que teve seu momento crucial com Andrew Wiles. Além disso, aborda como a invenção dos computadores, as curvas elípticas e as formas modulares contribuíram para a demonstração do Último Teorema de Fermat.

3.1. Um avanço lento

Através dos séculos as mulheres foram desencorajadas a estudar Matemática, mas apesar da discriminação houve algumas mulheres matemáticas que lutaram contra os preconceitos gravando seus nomes na história da ciência. Pitágoras é conhecido como o filósofo feminista, porque ativamente encorajava mulheres estudantes.

Para realizar suas pesquisas, Sophie Germain foi obrigada a assumir uma identidade falsa, estudar sobre condições terríveis e trabalhar em isolamento intelectual.

Sua família pertencia à alta burguesia francesa, e após um período de resistência familiar, seu pai financiou suas pesquisas.

Sophie Germain (1776 – 1831) participava das agitações da revolução francesa, e descobria o seu fascínio pela matemática na época da bastilha, ao ler sobre Arquimedes (287 a.C a 212 a.C), que segundo a lenda, durante a invasão de Siracusa, Arquimedes estava tão entretido estudando uma figura geométrica desenhada na areia da praia, deixando de responder a uma pergunta de um soldado foi morto por uma lança. Germain concluiu se alguém poderia ser tão envolvido por um problema de geometria, a ponto de ser morto, então a Matemática deveria ser um assunto interessante de ser estudado.

Após tornar-se autodidata em grego e latim, estudou os trabalhos de Newton e de Euler. Em 1794 em Paris, a Ècole Polythecnique, não aceitava mulheres, e após conseguir as notas de um curso que Lagrange (1736–1813) que acabara de ministrar, Sophie assumiu a identidade de um ex-aluno da academia, Monsiuer Leblanc, e enviou a Lagrange seus progressos. Após Lagrange descobrir a autoria do artigo tornou-se seu mentor.

Ao trabalhar no Último Teorema de Fermat e precisando debater suas ideias com algum teórico de teoria dos números, recorreu ao matemático alemão Frederich Gauss (1777-1885), considerado o maior teórico de teoria dos números, através de seu pseudônimo, Monseiur Leblanc.

Euler publicou em 1770 sua demonstração para o caso de $n = 3$ e desde então os matemáticos vinham tentando demonstrar sem sucesso os casos individuais. Germain adotara uma nova estratégia, e descreveu para Gauss a chamada abordagem geral para o problema. Em outras palavras, seu objetivo imediato não era provar um caso particular e sim dizer algo sobre muitos casos de uma só vez. Ela delineou um cálculo tomando como base um tipo especial de número primo p de modo que $(2p + 1)$ também fosse primo, este tipo de número primo foram denominados primos de Germain. Como 5 é primo e 11 $(2.5 + 1)$ é primo temos que 5 é um primo de Germain mas 13 é primo e como 27 $(2.13 + 1)$ não é primo, logo 13 não é um primo de Germain.

Em 1825 o método de Germain teve seu primeiro sucesso completo graças a Dirichlet (1805–1859) e a Legendre (1752–1833). Independentemente os dois foram capazes de provar que a equação fermatiana para $n = 5$ não tinha solução. Ambos basearam suas provas no trabalho de Sophie Germain.

Em 1839, quatorze anos depois, Gabriel Lamé (1795–1870) fez alguns acréscimos engenhosos ao método de Germain e provou o caso $n = 7$. Observe que $p = 7$ não é primo de Germain pois 15 $(2.7 + 1)$ não é primo. Os trabalhos de Germain permitiram aos teóricos dos números uma maneira de eliminar um conjunto de números primos e agora cabia aos esforços combinados de seus colegas a demonstração do Último Teorema de Fermat, um caso de cada vez.

DIRICHLET

LEGENDRE

LAMÉ

3.2. Os envelopes lacrados

Depois da descoberta de Sophie Germain, a academia francesa de Ciências ofereceu uma série de prêmios, incluindo uma medalha de ouro e três mil francos ao matemático que pudesse finalmente terminar com o mistério do Último Teorema de Fermat. Os salões de Paris ficaram cheio de boatos sobre quem estava adotando qual estratégia e quão perto estariam de anunciar um resultado. Então no dia 1º de março de 1847, a Academia teve a reunião mais dramática de sua história.

A ata descreve como Gabriel Lamé, que tinha demonstrado o caso de $n = 7$ alguns anos antes, subiu ao pódio diante dos mais importantes matemáticos de sua época e anunciou que estava muito perto de demonstrar o Último Teorema de Fermat. Ele admitiu que sua prova ainda estava incompleta, mas delineou o método e previu que dentro dos próximas semanas publicaria a demonstração completa no Jornal da Academia.

Toda a audiência ficou perplexa, mas assim que Lamé desceu do pódio, Augustin Louis Cauchy (1789–1857), outro dos melhores matemáticos de Paris, pediu a palavra. Cauchy anunciou para a Academia que estivera trabalhando numa abordagem semelhante à de Lamé, e que também estava a ponto de publicar uma demonstração completa.

Ambos Cauchy e Lamé, percebiam que a questão de tempo se tornara crucial. Aquele que publicasse primeiro a demonstração completa receberia o prêmio mais valioso e de maior prestigio na Matemática. Embora nenhum dos dois tivesse a prova completa, os dois rivais estavam ansiosos por reivindicar o direito da descoberta. Assim, apenas três semanas depois do anuncio, eles depositaram envelopes lacrados no cofre da academia. Esta era uma pratica comum na época, que permitiu aos matemáticos fazerem um registro sem revelar os detalhes exatos de seu trabalho. Se mais tarde surgisse uma disputa quanto à originalidade das ideias, os envelopes lacrados forneceriam a evidencia necessária para estabelecer a prioridade.

A expectativa aumentou em abril, quando Cauchy e Lamé publicaram detalhes vagos mais fascinantes de suas demonstrações no Jornal da Academia. Embora toda a comunidade Matemática estivesse desesperada para ver a demonstração completa, muitos torciam para que fosse Lamé e não Cauchy o vencedor da corrida. Todos conheciam Cauchy como um hipócrita, fanático religioso e era pessoa extremamente impopular com

seus colegas. Ele só era tolerado na Academia por seu talento. Então, no dia 24 de maio, foi feito um anuncio que acabou com todas as especulações. Mas não foi nem Cauchy nem Lamé quem se dirigiu a Academia e sim Joseph Liouville, que chocou o público ao ler o conteúdo de uma carta do matemático alemão Ernst Kummer.

Ernst Kummer (1810–1893) era um dos melhores teóricos dos números de todo o mundo e ao se dedicar a pesquisa de Matemática pura, estava ciente da disputa que ocorria na Academia Francesa. Ele tinha lido os anais e analisado os poucos detalhes que Cauchy e Lamé tinham se atrevido a revelar. Para Kummer ficou óbvio que os dois franceses estavam-se encaminhando para o mesmo beco sem saída.

Assim como temos o conjunto dos números inteiros $\mathbb{Z}$, podemos considerar o conjunto dos números $\mathbb{Z}[\sqrt{p}\,i] = \{a + b\sqrt{p}\,i; a, b \in \mathbb{Z}\} = \mathbb{Z} + \mathbb{Z}\sqrt{p}\,i \subset \mathbb{C}$ para um número primo $p \in \mathbb{Z}$, munido das operações usuais de soma e produto:

- $(+)\quad (a + b\sqrt{p}\,i) + (c + d\sqrt{p}\,i) \overset{\text{def}}{=} (a + c) + (b + d)\sqrt{p}\,i$
- $(.)\quad (a + b\sqrt{p}\,i)\,.\,(c + d\sqrt{p}\,i) \overset{\text{def}}{=} (ac - bdp) + (ad + bc)\sqrt{p}\,i$

Um conjunto A munido das operações de soma e produto, satisfazendo as seguintes propriedades básicas: associativa, comutativa, existência de elemento neutro para as operações de soma e produto, existência de simétrico da soma, e distributividade são denominados a*nel*. Se o anel A possuir a propriedade adicional: "se o produto de dois elementos for zero então um dos elementos é zero, isto é, se $\alpha\,.\,\beta = 0$ então $\alpha = 0\ ou\ \beta = 0$", ele será denominado domínio. Temos que $\mathbb{Z}$ e $\mathbb{Z}[\sqrt{p}\,i]$ são domínios. Se A é um anel diremos que:

- $a \in A$ é unidade se existe $b \in A$ tal que $a.b = 1$.
- $q \in A$ é irredutível se $q = b.c$ então b é unidade ou c é unidade.
- $p \in A$ é primo se p divide $a.b$ então p divide a ou p divide b.

Em um domínio A, se p é primo então p é irredutível. De fato, supondo que $p = a.b$ então p divide $a.b$ e como p é primo temos que p divide a $(a = k_1\,p)$ ou p divide b $(b = k_2 p)$. Mas

- $a = k_1 p \overset{*b}{\Rightarrow} p = a.b = k_1 pb \Rightarrow p\,(1 - k_1 b) = 0 \overset{dom.}{\Rightarrow} 1 = k_1 b \Rightarrow b$ é unidade.
- $b = k_2 p \overset{*a}{\Rightarrow} p = b.a = k_2 pa \Rightarrow p\,(1 - k_2 a) = 0 \overset{dom.}{\Rightarrow} 1 = k_2 a \Rightarrow a$ é unidade.

Considere a função $N: \mathbb{Z}[\sqrt{p}\, i] \to \mathbb{N}$ dada por $N(\beta) = \beta.\bar{\beta}$. Deste modo, temos que se $\beta = a + b\sqrt{p}\, i$ então $N(\beta) = N(a + b\sqrt{p}\, i) = (a + b\sqrt{p}\, i)(a - b\sqrt{p}\, i) = a^2 + pb^2$. Analogamente $N: \mathbb{Z} \to \mathbb{N}$ dada por $N(\beta) = \beta.\bar{\beta}$ e neste caso $N(a) = a^2$. Claramente temos que $N(x.y) = xy\,.\overline{xy} = x\bar{x}.y\bar{y} = N(x).N(y)$. Esta função é a restrição da função norma $N: \mathbb{C} = \mathbb{R} + \mathbb{R}i \to \mathbb{R}$ dada por $N(\beta) = \beta.\bar{\beta}$ para todo $\beta = a + bi \in \mathbb{C}$, isto é, $N(a + bi) = (a + bi)(a - bi) = a^2 - (bi)^2 = a^2 + b^2$.

Dado um anel A, denotaremos por $A^* = \{a \in A;\ a \text{ é } unidade\}$. Afirmamos que $A^* = \{y \in A;\ N(y) = 1\}$. De fato:

- $x \in A^* \Rightarrow \exists y \in A; x.y = 1 \Rightarrow N(x.y) = N(1) \Rightarrow N(x).N(y) = 1 \overset{em\ \mathbb{N}}{\Rightarrow} N(x) = 1.$
- $x \in \{y \in A; N(y) = 1\} \Rightarrow N(x) = 1 \Rightarrow x.\bar{x} = 1 \Rightarrow x \in A^*.$

Em um domínio A, um elemento q ser irredutível não implica que q é primo. Afirmamos que $q = 3$ é irredutível em $\mathbb{Z}[\sqrt{5}\, i]$ mas $q = 3$ não é primo em $\mathbb{Z}[\sqrt{5}\, i]$. De fato, supondo que $3 = x.y$ com $x, y \in \mathbb{Z}[\sqrt{5}\, i]$ e x não é unidade, temos $N(x) > 1$. Logo

$$9 = N(3) = N(x.y) = N(x).N(y) \overset{N(x)>1}{\Rightarrow} N(x) = 3 \ \ ou \ \ N(x) = 9$$

Mas $N(x) = 3$ não acontece pois senão $N(x) = a^2 + 5b^2 = 3$ com $a, b \in \mathbb{Z}$ o que é impossível. Logo $N(x) = 9$ e $N(y) = 1$ o que garante que y é unidade e portanto $q = 3$ é irredutível em $\mathbb{Z}[\sqrt{5}\, i]$. Por outro lado, $9 = 3.3 = (2 + \sqrt{5}i)(2 - \sqrt{5}i)$. Temos que 3 divide $(2 + \sqrt{5}i)(2 - \sqrt{5}i) = 2^2 - (\sqrt{5}i)^2 = 9$ mas $q = 3$ não divide $(2 + \sqrt{5}i)$ e $q = 3$ não divide $(2 - \sqrt{5}i)$ e portanto $q = 3$ não é primo em $\mathbb{Z}[\sqrt{5}\, i]$.

Um domínio A é dito um Domínio de Fatoração Única (D.F.U) se todo elemento $a \in A$, não é nulo e não é unidade, pode ser representado por um produto de elementos irredutíveis de A, e esta representação é única a menos da ordem dos elementos. Temos que $\mathbb{Z}[\sqrt{5}\, i]$ não é um D.F.U.

Em um domínio de fatoração única A, temos que q é irredutível se e somente se q é primo. De fato, suponha que q é irredutível com q dividindo $a.b$ e q não divide a, vamos mostrar que q divide b. Com efeito

$$q\ divide\ a.b\ \Rightarrow a.b = q.c \overset{q\ irred}{\Rightarrow} q\ esta\ na\ fatoração\ do\ b\ \Rightarrow q\ divide\ b$$

Isto mostra que q é irredutível então q é primo em um D.F.U e a recíproca do resultado já fizemos para domínio.

De acordo com Kummer, o problema fundamental era que as demonstrações de Cauchy e Lamé dependiam do uso de uma propriedade dos números conhecida como fatoração única para inteiros, conhecido como o Teorema Fundamental da Aritmética que fora descoberta no século IV a.C., por Euclides.

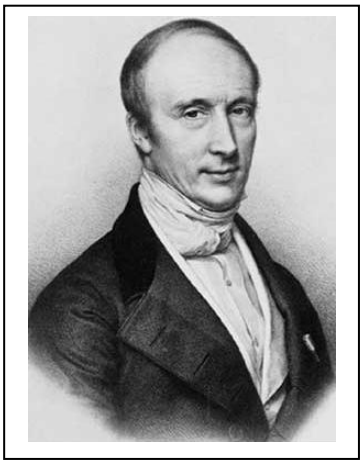
A primeira vista pode parecer não existir motivo para Cauchy e Lamé não usarem a fatoração única, como centenas de matemáticos já tinham feito antes deles. Infelizmente ambas as demonstrações envolviam números imaginários. E embora a fatoração única seja verdadeira para os números inteiros, ela pode se tornar falsa quando introduzimos números imaginários, lembrava Kummer. E em sua opinião esta era uma falha fatal.

Por exemplo $12 = 2^2.3 = (1+\sqrt{11}i).(1-\sqrt{11}i) = (2+\sqrt{8}i).(2-\sqrt{8}i)$. Não existe mais fatoração única e sim uma escolha de fatorações. Essa perda de fatoração única colocou as provas de Cauchy e Lamé em perigo grave, mas não as destruiu completamente. Como a demonstração do Último Teorema de Fermat só precisava ser verificada para os números primos, o problema da fatoração única poderia ser evitado para todos os números primos menores ou iguais $n = 31$. Contudo o número primo $n = 37$ não pode ser vencido de modo tão fácil. E entre os números primos menores do que 100, dois outros, $n = 59$ e $n = 67$, são também casos problemáticos e são chamados de ***primos irregulares.***

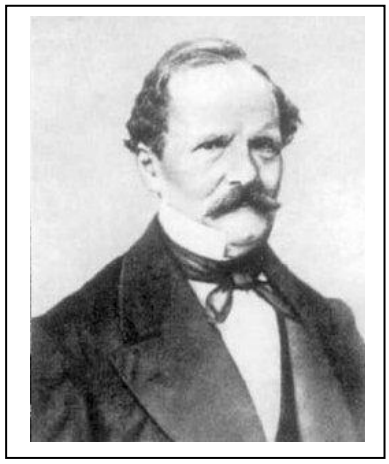
Kummer chamou a atenção para o fato de que nenhuma Matemática conhecida poderia abordar todos esses primos irregulares de uma só vez. Contudo ele acreditava que, através de técnicas cuidadosamente elaboradas para cada primo irregular, cada caso poderia ser resolvido individualmente. Mas o desenvolvimento destas técnicas seria um exercício lento e penoso. Pior ainda, o número de primos irregulares é infinito.

A carta de Kummer teve um efeito devastador sobre Lamé. Enquanto Lamé se sentia humilhado, Cauchy se recusava aceitar a derrota e achava que comparada à demonstração de Lamé, a sua abordagem dependia menos de fatoração única. Por varias semanas continuou a publicar artigos sobre o assunto, até que pelo fim do verão, ele também se calou.

Kummer tinha mostrado que a demonstração completa do Último Teorema de Fermat encontrava-se além da abordagem com a Matemática da época. Era uma peça brilhante de lógica matemática, mais um golpe devastador em toda uma geração de matemáticos que tivera esperanças de resolver o mais difícil dos problemas.



CAUCHY



KUMMER

Uma frase do famoso matemático francês, Henri Poicaré (1854–1912), considerado o último universalista matemático, se aplica perfeitamente ao Último Teorema de Fermat: "É das hipóteses mais simples que mais devemos desconfiar, porque são aquelas que tem mais possibilidades de passar despercebidas".

3.3. Curiosidades e novas abordagens

No final do século XIX o problema ainda ocupava um lugar especial no coração dos teóricos dos números, e Paul Wolfskehl, um empresário alemão deu uma nova vida ao problema. Ele não era nenhum matemático talentoso e a história começa com a obsessão de Wolfskehl por uma linda mulher, cuja identidade nunca foi determinada, que o rejeitava. Em virtude disso, como estava apaixonado e não era impetuoso, planejou o seu suicídio exatamente a meia noite de um determinado dia após cumprir todos os seus negócios pendentes. Paul foi tão eficiente, que terminou seus compromissos bem antes da meia noite, e para passar o tempo ate a hora fatal, foi para a biblioteca e ficou diante do trabalho clássico de Kummer sobre o fracasso da Cauchy e Lamé. Era um dos grandes

cálculos de sua época e uma leitura adequada para os últimos momentos de um matemático suicida.

Lendo o livro, Paul se encanta e fica cada vez mais envolvido a tal ponto de julgar um erro no texto de Kummer. Mais tarde concluiu que Kummer estava certo, aquela abordagem que ele usara era inconclusiva, o teorema seguia sem ser resolvido. Muitas horas haviam se passado, e a hora marcada para o suicídio havia se passado, onde seu desespero e magoa tinha evaporado e a matemática lhe dera uma nova vontade de viver.

Quando Paul Wolfskehl (1856–1906) morreu, seu testamento foi divulgado e sua família ficou chocada ao descobrir que Paul destinara uma grande porção de sua fortuna como premio, no valor de ***100 mil marcos***, a ser entregue a primeira pessoa que pudesse provar o ultimo teorema de Fermat, e era o seu modo de pagar um divida com o enigma que salvara sua vida.

O dinheiro foi colocado sob a guarda do *Konigliche Gesellshaft der Wissenchaften de Gottingen*, que anunciou oficialmente o inicio da competição pelo Prêmio Wolfskehl em 27 de junho de 1908, e a noticia da competição espalhou-se rapidamente pela Europa, onde foram estipuladas algumas regras, entre elas, se o prêmio não for entregue até 13 de setembro de 2007, não serão aceitos mais trabalhos.

A maioria dos matemáticos profissionais viam o Último Teorema de Fermat como uma causa perdida e achavam que não podiam desperdiçar suas carreiras numa busca pela prova do teorema, entretanto, o prêmio teve o mérito de apresentar o problema a toda uma nova audiência e várias mentes ávidas estavam prontas a se entregarem ao derradeiro enigma, abordando-o com completa inocência.

O Dr. F. Schlichting foi responsável pela avaliação dos candidatos ao Prêmio Wolfskehl na década de 1970. Esta carta foi escrita para ***Paulo Ribenboim*** e foi publicada em seu livro *13 palestras sobre o Último Teorema de Fermat* dando uma perspectiva única do trabalho do Comitê Wolfskehl:

“Prezado Senhor

O número total de soluções apresentadas até agora ainda não foi contado. No primeiro ano (1907-1908), 621 soluções foram registradas nos arquivos da Akademie e hoje temos 3 metros de correspondência armazenadas sobre o problema de Fermat. Nas

ultimas décadas, temos lidado com isso da seguinte maneira, o secretário da Akademie divide os manuscritos que chegam em 2 (duas) categorias:

1. Absurdo completo, que é enviado de volta imediatamente.
2. Material que parece Matemática.

A segunda parte é enviada ao departamento de Matemática e lá é feito o trabalho de leitura, descoberto os erros e a resposta é delegado a um dos assistentes científicos (nas universidades alemãs estes são indivíduos graduados trabalhando para obter o seu Ph.D) – ***no momento eu sou a vitima***. Existem 3 ou 4 cartas para responder todo mês e isto inclui um bocado de material engraçado e curioso, por exemplo, um sujeito mandou a primeira parte da demonstração e promete a segunda se pagarmos 1000 (mil) marcos adiantados. Outro me prometeu 1 % do lucro que vai ter com a publicação e as entrevistas para o rádio e a TV depois que ficar famoso, desde que eu o apoie agora. Caso contrário ele ameaça enviar seu trabalho para um departamento de matemática da Rússia de modo a privar-nos da glória de tê-lo descoberto. De vez em quando alguém aparece em *Gottingen* e insiste numa discussão pessoal.

Quase todas as soluções são escritas num nível muito elementar (usando noções de Matemática do ginásio e talvez alguns trabalhos não digeridos da teoria dos números), mas isto pode ser bem complicado de entender. Socialmente os candidatos são pessoas com uma educação técnica, mas uma carreira fracassada, e tentam obter sucesso com a demonstração do teorema de Fermat. Eu entreguei alguns manuscritos para médicos que diagnosticaram esquizofrenia aguda.

Uma das condições do testamento de Wolfskehl era de que a *Akademie* deveria publicar o anuncio do premio todos os anos nos principais periódicos sobre matemática. Mas depois dos primeiros anos, os periódicos passaram a se recusar a publicar o anuncio, porque eles fica entulhados de cartas e manuscritos malucos.

Espero que esta informação seja do seu interesse.

Sinceramente,

F. Schlichting.”

Os matemáticos que ainda lutavam com o Último Teorema de Fermat começaram a atacar o problema com os computadores, confiando numa versão computadorizada da abordagem de Kummer no século XIX.

Kummer tinha descoberto uma falha no trabalho de Cauchy e Lamé e mostrara que o maior problema para demonstrar o Último Teorema de Fermat era lidar com os casos onde n é igual a um número primo irregular – para valores de n até 100 os únicos primos irregulares são os números 37, 59 e 67. Ao mesmo tempo Kummer mostrou que, em teoria, todos os primos irregulares podem ser abordados de modo individual, o único problema seria a enorme quantidade de calculo necessária. E para demonstrar o ponto de vista de Kummer, seu colega Dimitri Mirimanoff exibiram semanas de cálculos necessárias para provar o teorema para os números primos irregulares menores do que 100. Contudo, ele e outros matemáticos não estavam preparados para lidar com o grupo seguinte de primos irregulares que ficam entre 100 e 1.000.

Algumas décadas depois os problemas de cálculos imensos começaram a desaparecer. Com a chegada dos computadores, os casos mais difíceis do Último Teorema de Fermat podiam ser enfrentados com rapidez. Depois da segunda guerra mundial, equipes de matemáticos e cientistas dos computadores demonstraram o teorema para valores de n até 500, depois para valores até 1.000 e logo chegaram até 10.000.

Na década de 1980, Samuel S. Wagstaff da Universidade de Illinois elevou o limite para 25.000 e mais recentemente os matemáticos já podiam afirmar que o Último Teorema de Fermat é verdadeiro para todos os valores de n até $4.000.000$ (quatro milhões).

Embora os leigos pudessem achar que a tecnologia moderna estava levando a melhor sobre o Último Teorema de Fermat, os matemáticos sabiam que este sucesso era apenas aparente. Mesmo que os supercomputadores passassem décadas demonstrando um valor de n e depois do outro eles nunca poderiam demonstrar todos os valores de n até o infinito e portanto, nunca poderiam demonstrar todo o teorema. Mesmo que o teorema fosse verdadeiro ate um bilhão não há motivo para garantir que fosse verdade para um bilhão e um. E se fosse demonstrado para um trilhão, ele poderia ser falso para um trilhão e um e assim por diante.

Extrapolar uma teoria para cobrir uma infinidade de números baseando-se na evidencia de alguns números pode conduzir a erros. Há uma sequencia em particular de números primos que nos mostra como a extrapolação é uma muleta perigosa de se apoiar.

No século XVII os matemáticos mostraram, através de exames detalhados, que os seguintes números são todos primos:

31, 331, 3.331, 33.331, 333.331, 3.333.331, 33.333.331

Os próximos números da série se tornam cada vez maiores e o trabalho de verificar se eles também são primos teria exigido um esforço descomunal. Naquela época os matemáticos ficaram tentados a extrapolar a partir deste padrão e presumir que todos os números da série são primos. Contudo o número seguinte revelou não ser primo:

$$333.333.331 = 17\ x\ 19.607.843$$

Outro bom exemplo que demonstra por que os matemáticos se recusam a ser convencidos por alguns exemplos ou pela evidencia dos computadores é o caso da conjectura de Euler (1707 – 1783) que afirmava que não existe solução não trivial nos inteiros para a equações que são soma de $(n-1)$ potências de grau n resultando uma potência de grau n, para $n \geq 3$, isto é:

$$X_1^n + X_2^n + \cdots + X_{n-1}^n = Z^n$$

Em particular:

- $n = 3 \quad \therefore \quad X^3 + Y^3 = Z^3$ (equação fermatiana cúbica)
- $n = 4 \quad \therefore \quad X^4 + Y^4 + Z^4 = W^4$
- $n = 5 \quad \therefore \quad X^5 + Y^5 + Z^5 + W^5 = T^5$

Em 1966, Lander e Parkin encontraram uma solução para $n = 5$:

$$(27)^5 + (84)^5 + (110)^5 + (133)^5 = (144)^5$$

Em 1986, Elkies, encontrou uma solução para $n = 4$:

$$(2.682.440)^4 + (15.365.639)^4 + (18.796.760)^4 = (20.615.673)^4$$

Em 1988, Roger Frye, encontrou o menor contraexemplo para $n = 4$ usando técnicas computacionais sugeridas por Elkies:

$$(95.800)^4 + (217.529)^4 + (414.560)^4 = (422.481)^4$$

3.4. Andrew Wiles

Em 1975, Andrew Wiles começou sua carreira como estudante de pós-graduação na universidade de Cambridge, que fora fundada em 1209 no Reino Unido. Durante os três anos seguintes ele trabalhou em sua tese de Ph.D. Cada estudante é orientado e estimulado por um supervisor, que no caso de Wiles foi o australiano John Coates, que ainda se recorda de como aceitou Wiles como aluno: "Eu lembro que um colega me disse que tinha um estudante muito bom que acabara de terminar a parte III dos exames para distinção em Matemática, e ele me pediu que aceitasse Wiles como meu aluno, o que me trouxe grande satisfação."

Wiles conheceu o problema de sua vida, ainda criança, quando certo dia, voltava para casa e decidiu passar na biblioteca da Rua Milton, uma pequena biblioteca, mas que tinha uma boa coleção de livros sobre enigmas, e foi atraído por um livro que tinha apenas um problema, mas sem solução.

O livro era "O Último Problema", de Eric Temple Bell, onde apresentava a história de um problema matemático de origem grega, mas só atingiria sua maturidade no século *XVII*, quando Fermat o colocara como desafio, e que durante trezentos anos nenhum matemático tinha conseguido a solução. Além do problema, o livro continha a tentativa de vários matemáticos em solucioná-lo.A partir daí, Wiles trilhou sua infância e sua vida acadêmica na tentativa de descoberta de uma solução para esse desafio.

Wiles se lembra de como teve que abandonar temporariamente o seu sonho: "Quando fui para Cambridge eu realmente tive que deixar Fermat de lado. Não é que o tivesse esquecido, ele estava sempre lá – mas percebi que as únicas técnicas para se lidar com o problema tinham 130 anos de idade. E não me parecia que estas técnicas estavam chegando à raiz. O risco de se trabalhar com Fermat era que se poderia passar anos sem chegar à parte alguma. É ótimo trabalhar em qualquer problema desde que ele gere uma Matemática interessante ao longo do caminho – mesmo que não consiga resolve-lo ao final da vida. A definição de um bom problema de Matemática reside na Matemática que ele produz, não no problema em si."

Seria responsabilidade de John Coates encontrar uma nova obsessão para Andrew, alguma coisa que ocupasse suas pesquisas por pelo menos três anos. "Eu creio que tudo

que um supervisor de pesquisa pode fazer por um estudante é tentar empurrá-lo numa direção de pesquisa frutífera. É claro que é impossível ter certeza do que será uma direção frutífera em termos de pesquisa, mas talvez algo que um experiente matemático pode fazer é usar seu senso prático, sua intuição do que seja uma boa área e então dependerá só do estudante decidir até onde ele pode ir naquela direção."

Finalmente 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. O nome "*curvas elípticas*" é de certa forma enganador porque elas não são elipses e nem ao menos são curvas no sentido normal da palavra. Elas receberam este nome porque no passado eram usadas para medir o perímetro de elipses e os comprimentos das órbitas dos planetas, aonde iremos nos referir a elas como equações elípticas no lugar de curvas elípticas:

$$y^2 = x^3 + ax^2 + bx + c \qquad onde \qquad a, b, c \in \mathbb{Z}$$

O desafio com as equações elípticas assim como no caso do Último Teorema de Fermat é determinar se elas possuem soluções para números inteiros, e se assim for, quantas. Por exemplo, a equação elíptica

$$y^2 = x^3 - 2 \qquad onde \qquad a = 0,\ b = 0,\ c = -2$$

tem apenas um conjunto finito de soluções para números inteiros, a saber $5^2 = 3^3 - 2$. Simplesmente, mudando-se os valores de a, b, c em uma equação elíptica geral, os matemáticos podem gerar uma variedade de equações, cada uma com suas características próprias, mas todas elas possíveis de serem solucionadas.

As equações elípticas foram originalmente estudadas pelos antigos matemáticos gregos, incluindo Diofante, que dedicou uma grande parte de sua Aritmética ao estudo de suas propriedades. Provavelmente inspirado por Diofante, Fermat também aceitou o desafio de estudar as equações elípticas. Como elas tinham sido estudadas por seu herói, Wiles ficou feliz em explorá-las ainda mais. Mesmo depois de 2000 anos as equações elípticas ainda apresentavam problemas formidáveis para estudantes como Wiles. Ele disse: "Ainda estamos longe de entendê-las completamente. Eu poderia apresentar muitas perguntas aparentemente simples sobre equações elípticas que ainda não foram respondidas. Mesmo perguntas que o próprio Fermat considerou ainda não foram

respondidas. De certo modo, toda a Matemática que eu fiz tem suas origens em Fermat, se não no Último Teorema de Fermat."

Nas equações que Wiles estudou como estudante de graduação, a determinação do numero exato de soluções era tão difícil que o único modo de fazer algum progresso era simplificar o problema, como por exemplo, usando o que os matemáticos chamam de aritmética modular. Trabalhando junto com John Coates, Wiles rapidamente estabeleceu sua reputação como um brilhante teórico dos números, uma pessoa dotada de uma compreensão profunda das equações elípticas. À medida que chegava a cada novo resultado e publicava mais um trabalho, Wiles não percebia que estava reunindo a experiência que o levaria, muitos anos depois, a beira de demonstrar o Último Teorema de Fermat.

Embora ninguém tivesse ciente disso na ocasião, a Matemática japonesa do pós-guerra já tinha iniciado uma corrente de acontecimentos que ligaria as equações elípticas ao Último Teorema de Fermat. Ao encorajar Wiles a estudar as equações elípticas, Coates lhe dera as ferramentas que o capacitariam para trabalhar em seu sonho.

Em 1954,Yutaka Taniyama (1927- 1958) e Goro Shimura (1930 -) que estavam no começo de suas carreiras matemáticas, encontraram se casualmente em virtude do empréstimo do *volume* 24 *do Mathematische Annalen,* emprestado a Taniyama pela biblioteca da Universidade de Tókio que também interessava a Shimura, iniciando uma parceria que mudaria o curso da história da Matemática. Embora Shimura tivesse um lado excêntrico – ainda hoje ele mantém o gosto por piada zen – ele era muito mais conservador e convencional do que seu parceiro intelectual. Shimura se levantara ao raiar do dia e imediatamente começava a trabalhar enquanto seu colega frequentemente continuava dormindo, tendo trabalhado a noite toda. Enquanto Shimura era obstinado, Taniyama era despreocupado a ponto de ser preguiçoso. Surpreendentemente esta era uma característica que Shimura admirava: "Ele tinha uma capacidade de cometer muitos erros, a maioria deles na direção certa. Eu o invejava por isso e tentei imitá-lo em vão, mas descobri que era muito difícil cometer bons erros".

Taniyama e Shimura estudavam formas modulares, que estão entre os objetos mais maravilhosos da Matemática. No século XX, o teórico dos números Martin Escher dedicou boa parte dos seus estudos a compreender as formas modulares.

As formas modulares são desconectadas na Matemática. Na verdade, elas parecem completamente desligadas do assunto que Wiles iria estudar em Cambridge, as equações elípticas. A forma modular é bastante complicada, sendo estudada principalmente devido a sua simetria, e foi descoberta no século XIX. A equação elíptica vem da Grécia antiga e não tem relação nenhuma com a simetria. Taniyama e Shimura iriam chocar a comunidade Matemática ao sugerirem que as equações elípticas e as formas modulares eram na verdade uma coisa só. Segundo eles seria possível unificar os mundos modulares e elípticos.

Em 1955, em um simpósio internacional de matemática em Tókio nasceu à conjectura de Taniyama – Shimura que dizia que: "**Toda curva elíptica racional é modular**". Esta conjectura é uma das mais significativas da Matemática, tornou-se conhecida através do trabalho do matemático francês André Weil (1906-1998), um dos grandes nomes da teoria dos números do século XX. Ele encontrou evidências ainda mais fortes da conjectura e inspirou na década de 1960 o famoso e importante "Programa de Langlands", do professor Robert Langlands de Princeton, um grande projeto de pesquisa matemática que investiga as profundas e sutis relações entre as várias áreas da Matemática.

Após a morte de Taniyama em 1958 aos 31 anos por suicídio, Shimura concentrou todos os seus esforços para compreender a relação exata entre as equações elípticas e formas modulares. Os outros matemáticos ainda duvidavam e Shimura se lembra de uma conversa que teve com um iminente colega. O professor perguntou: "Ouvi dizer que você propõe que algumas equações elípticas podem ser ligadas a formas modulares". Respondeu Shimura: "Não, você não entendeu. Não são apenas algumas equações elípticas, são todas as equações elípticas."

Em 1984, Gerhard Frey fez a extraordinária afirmação 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 a equação elíptica:

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

Ao transformar a equação de Fermat em uma curva elíptica, Frey tinha ligado o Último Teorema de Fermat à conjectura de Taniyama-Shimura. De acordo com Frey, demonstrar a conjectura de Tanayama-Shimura era o único obstáculo a vencer para obter a prova do Último Teorema de Fermat.

Esta idéia apresentava um erro elementar em sua lógica, que fora percebido por quase todos os presentes no simpósio, entre eles Ken Ribert, exceto pelo próprio Frey. Houve uma corrida matemática para que fosse corrigida. No verão de 1986, Ken Ribert em conversa com Barry Mazur, informou que conseguiu demonstrar um caso muito especial da conjectura de Frey, mas não sabia o que fazer para generalizar e conseguir a prova toda. Mazur disse: "Mas você não percebe? Tudo que precisa fazer é somar alguns gama-zero de estrutura (M) e prosseguir com seu argumento que vai funcionar. Vai lhe dar tudo o que precisa". Era o momento mais importante da carreira de Ribert e ele relembra os mínimos detalhes. Ribert disse: "você esta absolutamente certo – é claro! – como não percebi isto? eu estava totalmente perplexo porque nunca me ocorrera somar os gama-zero da estrutura (M), embora pareça simples."

Deve ser notado que embora somar gama zero da estrutura (M) possa parecer simples para Ken Ribert, trata-se de um passo difícil de lógica que somente um punhado de matemáticos no mundo inteiro teria bolado durante um encontro casual. Por três séculos e meio o Último Teorema de Fermat fora uma problema isolado, um enigma curioso e impossível na fronteira da Matemática. Agora Ken Ribert, inspirado por Gerhard Frey, o trouxera ao centro das atenções. Andrew Wiles era provavelmente uma das poucas pessoas no mundo que tinha a audácia de sonhar que poderia realmente ir em frente e provar a conjectura de Taniyama-Shimura.

Em 1986, Wiles soube através de um amigo que Ken Ribet tinha demonstrado a ligação entre Taniyama-Shimura e o Último Teorema de Fermat: "Casualmente, no meio da conversa, ele me disse que Ken Ribet tinha demonstrado a ligação entre Taniyama-Shimura e o Último Teorema de Fermat. Eu fiquei eletrizado. Eu sabia naquele momento que o rumo de minha vida estava mudando, porque isto significava que para demonstrar o Último Teorema de Fermat eu só precisaria provar a conjectura de Taniyama-Shimura."

Wiles sabia que para ter alguma esperança de encontrar uma prova ele teria que primeiro mergulhar completamente no problema. *Leu os trabalhos mais recentes e então se exercitou nas últimas técnicas, repetidas vezes, até que elas se tornaram naturais para*

ele, de modo a reunir as armas necessárias para a batalha à frente. Wiles dedicou-se por 18 meses para se familiarizar com cada elemento da Matemática que fora usado ou que derivara das curvas elípticas e das formas modulares. Este era um investimento comparativamente pequeno, tendo em mente que qualquer tentativa séria de obter uma demonstração iria exigir 10 anos de esforço solitário.

Assim, Wiles 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, Wiles tomou a decisão de trabalhar em completo isolamento e segredo. A única pessoa que conhecia seu segredo era sua esposa.

Para evitar distrações na faculdade, trabalha em casa onde se refugiava em seu escritório no sótão. Lá ele procurava expandir o poder das técnicas estabelecidas esperando desenvolver uma estratégia para seu ataque sobre a conjectura de Taniyama-Shimura. Até os colegas mais chegados não conheciam sua pesquisa. John Coates se lembra das conversas com Wiles durante as quais ele não deu nenhuma indicação do que estava acontecendo. "Até me lembro de ter falado com ele, em algumas ocasiões, que achava muito boa esta ligação com o Último Teorema de Fermat, mas que não havia esperanças de se provar Taniyama-Shimura. Acho que ele apenas sorriu."

Para provar que cada equação elíptica esta relacionada com uma forma modular era necessário um argumento lógico, passo a passo, que efetivamente apresentasse uma razão e explicasse por que cada equação elíptica teria que ser modular. Para encontrar a demonstração Wiles só usava lápis, papel e sua mente, e nunca usava o computador, pois embora um computador possa verificar os casos individuais em alguns segundos, ele jamais poderá verificar todos os casos. Nos anos seguintes, Wiles faria uma série de descobertas extraordinárias, mas não publicou nem discutiu nenhuma delas até que sua demonstração estivesse completa.

A primeira ideia de Wiles foi atacar o problema de usando o poder da teoria dos grupos. Enquanto os grupos originais de Galois eram construídos a partir das soluções da equações de quinto grau. Wiles construiu seus grupos usando um punhado de soluções para cada equação elíptica. Depois de meses de estudos Wiles usou esses grupos elípticos para tentar igualar cada equação elíptica com sua forma modular. Embora fosse o primeiro

passo para demonstrar a conjectura de Taniyama-Shimura, a estratégia de Wiles, usando Galois, era uma conquista brilhante, digna de ser publicada.

Em 1983, o geômetra algébrico Gerd Faltings, foi capaz de eliminar a possibilidade de um número infinito de soluções para o Último Teorema de Fermat.

Em 1988, Wiles ficou chocado ao ler as manchetes na primeira página dos jornais anunciando que o Último Teorema de Fermat fora resolvido. O Washington Post e o New York times afirmaram que Yoichi Miyaoka, com 38 anos, tinha descoberto uma solução para o problema mais difícil do mundo. Abordando o problema com técnicas de geometria diferencial através de paralelos com teoria dos números, Miyaoka afirmara que o número de soluções para a equação de Fermat não era apenas finito, mas igual à zero. O matemático britânico Don Zagier, que estivera na plateia, resumiu o otimismo da comunidade. "A demonstração de Miyaoka é muito interessante e algumas pessoas acham que existe uma boa chance que funcione. Isto ainda não é definitivo, mas até agora parece ótimo."

Após Miyaoka divulgar as 5 páginas de álgebra que detalhavam sua demonstração, e o exame escrupuloso começou. Quatro semanas depois, Gerd Faltings, cujo trabalho abrira caminho para Miyaoka, anunciou ter localizado a razão exata para a aparente quebra de paralelismo – um erro na lógica de Miyaoka. Um grupo especializado em teoria dos números tentaram ajudar Miyaoka a consertar o erro, mas seus esforços terminaram em fracasso. Dois meses depois do anuncio inicial o consenso geral era de que a demonstração original fracassara, *e Wiles respirou aliviado*.

Depois de três anos de esforços contínuos, Wiles fizera uma série de avanços. Ele aplicara os grupos de Galois nas equações elípticas e as dividiria num número infinito de peças. Então demonstrara que cada primeira peça, de cada equação elíptica, tinha que ser modular, mas não conseguiu encontrar um meio de provar que se um elemento da equação elíptica era modular, então o elemento seguinte também seria, para gerar o efeito dominó. Wiles começou a reestudar a teoria Iwasawa que era um método para analisar equações elípticas que ele aprendera como estudante em Cambridge, sob a tutela de John Coates. Embora o método fosse a principio inadequado, Wiles esperava poder modificá-lo para que ficasse suficientemente poderoso para gerar o efeito dominó, mas em 1991 sentiu que perdera a batalha de adaptar a teoria de Iwasawa.

A segunda ideia de Wiles, foi dedicada a desenvolver o método de Kolyvagin-Flach de análise de equações elípticas após um encontro com John Coates, onde passou vários meses se familiarizando com esta técnica recém-descoberta, para em seguida adaptá-la e implementá-la. Depois de seis anos de esforço intenso, Wiles acreditava que o fim estava próximo, provando que famílias novas e maiores de curvas deviam ser modulares

Wiles começou a questionar se estava usando o método Kolyvagin-Flach de modo completamente rigoroso. "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 do 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."

Nick Katz lembra em detalhe o momento em que Wiles revelou seu segredo: "Um dia Wiles me procurou na hora do chá e pediu que eu fosse ao seu escritório – havia alguma coisa que ele queria me contar. Eu não tinha ideia de que poderia ser. Entrei no escritório e ele fechou a porta. Então me disse que achava que poderia provar a conjectura de Taniyama-Shimura. Eu estava surpreso, perplexo – era fantástico."

Katz sugeriu que para algo tão grandioso nós precisamos montar uma estrutura formal de aulas semanais, de outro modo à coisa ia degenerar. E assim criamos um curso com várias aulas. Eles combinaram que a melhor estratégia seria anunciar uma série de palestras abertas aos estudantes graduados do departamento.Wiles daria o curso e Katz estaria na plateia. O curso cobriria a parte da demonstração que precisava ser verificada, mas os estudantes graduados não saberiam disso. O interesse em disfarçar a verificação da prova deste modo é que forçaria Wiles a explicar tudo passo a passo e no entanto, não levaria suspeitas dentro do departamento. No que diz respeito aos outros era apenas outro curso de graduação.

E assim Wiles anunciou seu curso chamado "Cálculos em Curvas Elípticas", relembrando Katz com um sorriso matreiro, "o que é um título completamente inócuo, poderia significar qualquer coisa. Ele não mencionou Fermat nem Taniyama-Shimura apenas mergulhou direto nos cálculos. Não havia meio de alguém adivinhar o que estava acontecendo. Era feito de um modo que a menos que você soubesse para o que era tudo

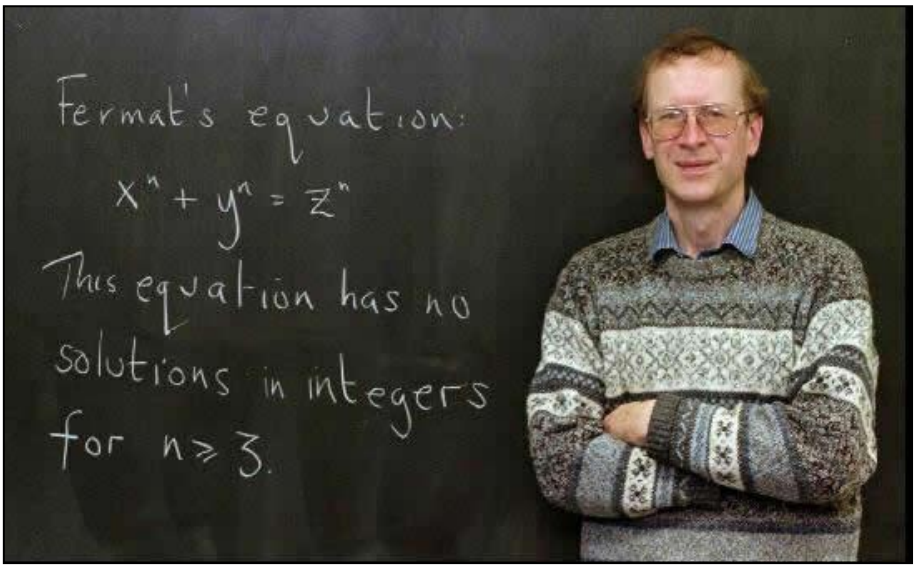
aquilo, os cálculos pareceriam incrivelmente tediosos e complexos. E quando você não sabe para que serve uma determinada Matemática é impossível seguir o raciocínio. Já é difícil de acompanhar mesmo quando você conhece o objetivo. De qualquer modo, um por um os estudantes graduados foram abandonando as aulas e depois de algumas semanas eu era a única pessoa que restara na sala."

Ninguém desconfiava de que Wiles estava à beira de conquistar o prêmio mais importante da Matemática. O plano fora um sucesso. Ele tivera sucesso em aplicar o método Kolyvagin-Flach a família após família de equações elípticas e apenas uma família ainda se recusava a se submeter à técnica. Wiles descreve como ele tentou completar o último elemento da demonstração: "Uma manhã, no final de maio de 1993, pensando na família de equações que restara, olhava casualmente para um trabalho de Barry Mazur, ele mencionava um trabalho do século XIX, e subitamente eu percebi que poderia usar aquilo para fazer o método de Kolyvagin-Flach funcionar na última família de elípticas. O trabalho se estendeu pela tarde e esqueci-me de almoçar. Por volta de três ou quatro horas da tarde eu estava realmente convencido de que isto resolveria o último obstáculo. Era hora do chá e eu desci para a parte inferior da casa e minha esposa ficou surpresa de me ver chegar tão tarde, então eu contei a ela: resolvi o Último Teorema de Fermat.".

Em junho de 1993, 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, Wiles começou sua terceira e última palestra. Todas as pessoas que contribuíram para as ideias 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".



Andrew Wiles

Wiles submeteu seu trabalho à revista ***Inventiones Mathematicae***. E seu editor Barry Mazur, começou o processo de selecionar os juízes para julgarem o trabalho, e não selecionou apenas 2 ou 3 examinadores, como é normal, mais nomeou 6 examinadores. Entre eles Nick Katz, Ken Ribet, Richard Taylor entre outros. O capitulo 3 era de responsabilidade de Nick Katz, onde a demonstração era um argumento gigantesco, construído de um modo intrincado a partir de centenas de cálculos matemáticos grudados por milhares de elos lógicos. Em 23 de agosto, Katz detectou um erro em uma parte crucial do argumento envolvendo o método Kolyvagin-Flach, mas algo tão sutil que Katz não percebera até este momento. O erro era tão abstrato que não pode ser descrito em termos simples. Em setembro a esposa de Wiles disse que o único presente que ela queria no seu aniversário, em 6 de outubro, era a demonstração completa.

Wiles se isolou completamente não se manifestando sobre o assunto e nem os examinadores se manifestavam havendo grande pressão sobre uma posição e a liberação dos manuscritos. Seu amigo Peter Sarnak perguntava: "Sabe que há uma tempestade lá fora?" Finalmente Wiles chegou à conclusão de que não poderia manter o silêncio para sempre e enviou o seguinte e-mail para o quadro de informações do departamento de Matemática:

Assunto: Situação da prova do Último Teorema de Fermat

Data: 04 de dezembro de 1993

Em vista das especulações sobre o estado do meu trabalho com a conjectura de Taniyama-Shimura e o Último Teorema de Fermat eu vou fazer um breve resumo da situação. Durante o processo de avaliação surgiram alguns problemas. A maioria foi resolvida logo, mas um problema em particular ainda não foi solucionado.

A redução chave da (em sua maioria dos casos) conjectura de Taniyama-Shimura para o cálculo do grupo Selmer esta correto. Contudo, o cálculo final de uma fronteira superior precisa para o grupo Selmer no caso semi-estável (da representação do quadrado simétrico associado com a forma modular) ainda não esta completa. Eu acredito que serei capaz de terminar isto no futuro próximo, usando as ideias explicadas em minhas palestras de Cambridge.

O fato de que ainda resta um bocado de trabalho a ser feito no manuscrito o torna inadequado para impressão. Em meu curso em Princeton, que vai começar em fevereiro, eu farei um relato completo deste trabalho.

Andrew Wiles.

Poucos acreditavam no otimismo de Wiles e alguns jornais lembravam-se da fracassada demonstração de Miyaoka em 1988. Menos de seis meses depois da palestra no Instituto Newton a demonstração de Wiles estava em frangalhos. Wiles lembra agora que seu sonho de infância se tornara um pesadelo. Enquanto isso, no departamento de Matemática, os mexericos continuavam. O professor John Conway, matemático de Princeton, relembra o clima na sala de chá do departamento e alguém dizia: “Eu vi o Andrew hoje de manhã,”. “Ele sorriu?” Bom, sorriu, mas não parecia feliz. “Só podíamos avaliar seus sentimentos pela própria expressão em seu rosto.”

Wiles admitiu para Peter Sarnak que a situação estava ficando desesperadora e que ele estava a ponto de aceitar a derrota. Peter então sugeriu que Wiles conseguisse um

auxiliar de confiança e tentasse uma vez mais consertar a demonstração. Wiles precisava de alguém que fosse especialista em manipular o método Kolyvagin-Flach e que mantivesse em segredo os detalhes do problema. Depois de pensar longamente no assunto, ele decidiu convidar Richard Taylor, um professor de Cambridge, para vir a Princeton trabalhar com ele.

Taylor era um dos avaliadores da demonstração e um ex-aluno de Wiles, sendo portanto de confiança. Por volta de janeiro, Wiles com a ajuda de Taylor tinha mais uma vez explorado incansavelmente o método Kolyvagin-Flach tentando um meio de sanar o problema. Na primavera de 1994, Wiles disse a Taylor que não via motivos para continuar com suas tentativas de consertar a demonstração. Taylor já planejara passar o mês de setembro em Princeton antes de retornar a Cambridge e assim, apesar do desânimo de Wiles, ele sugeriu que continuassem por mais um mês. Se não houvesse sinal de uma solução no final de setembro eles desistiriam, reconhecendo publicamente o fracasso. A prova defeituosa seria publicada para permitir que outros tivessem a oportunidade de examiná-la.

Wiles decidiu passar o mês de setembro examinando uma última vez a estrutura do método Kolyvagin-Flach, para tentar determinar exatamente por que ele não estava funcionando. Ele se lembra vividamente, daqueles últimos dias fatídicos, na manha de 19 de setembro: “Eu percebia que embora o método de Kolyvagin-Flach não estava funcionando completamente, ele era tudo de que precisava para fazer a minha teoria original Iwasawa funcionar”. A teoria de Iwasawa sozinha fora inadequada. O método Kolyvagin-Flach sozinho também fora inadequado. Mas juntos eles se completavam perfeitamente. Foi um momento de inspiração que Wiles nunca iria esquecer.

Assim, na primeira noite eu voltei para casa e dormi. Verifique tudo de novo na manhã do dia seguinte e por volta das 11 horas fiquei satisfeito, desci e contei para minha mulher. “consegui, acho que encontrei!” e ela disse: “descobri o quê?” e eu disse: “Eu consertei minha demonstração.”

No mês seguinte Wiles pode cumprir a promessa que não conseguira no ano anterior. “Estava chegando novamente o aniversário de minha esposa em 06 de outubro e da última vez eu não pudera lhe dar o presente que ela queria. Desta vez, na noite do seu aniversario, eu pude lhe dar o manuscrito completo. Eu acho que ela gostou mais deste presente do que qualquer outro que eu lhe dera anteriormente.”

Assunto: Atualização do Último Teorema de Fermat

Dia 25 de outubro de 1994.

Nesta manhã, dois manuscritos foram divulgados:

Curvas Elípticas Modulares e o Último Teorema de Fermat

Por Andrew Wiles

Propriedades teóricas de um anel em certas álgebras de Hecke

Por Richard Taylor e Andrew Wiles

Desta vez não havia duvidas quanto à demonstração. Os dois trabalhos de 130 páginas ao todo, eram os manuscritos matemáticos mais minuciosamente examinados em toda a história e foram publicados no ***Annals of Mathematics (maio de 1995).***

John Coates disse: "Uma demonstração de Fermat é um grande triunfo intelectual e não se deve perder de vista o fato de que ela revolucionou a teoria de números num golpe só. Para mim, o charme e a beleza do trabalho de Andrew é que ele foi um tremendo passo na teoria dos números" Ele criou técnicas matemáticas completamente novas e as combinou com técnicas tradicionais de um modo que nunca fora feito antes. E ao fazer isso, criou novas linhas de ataque para todo um conjunto de outros problemas. Embora Taniyama tivesse cometido suicídio trinta anos antes, seu colega Shimura esta lá para ver a conjectura ser provada. Quando lhe perguntaram sobre sua reação sobre a demonstração, Shimura sorriu suavemente e de um modo contido e digno disse: "Eu tinha falado para vocês."

Através da conjectura de Taniyama-Shimura, Wiles unificara os mundos elípticos e modulares e ao fazê-lo dera a matemática um atalho para muitas outras provas – problemas de um domínio podem ser resolvidos por analogia com problemas de um domínio paralelo.

Problemas clássicos de elípticas, não resolvidos desde a Grécia antiga, podem agora ser reexaminados com todas as técnicas modulares disponíveis.

Wiles dera o primeiro passo em direção ao grande esquema de unificação de Langlands. Agora existe um esforço renovado para demonstrar outras conjecturas de unificação entre campos da Matemática.

Em março de 1996, Wiles dividiu os 100 mil dólares do prêmio Wolf (não confundir com o Premio Wolfskeshl) com Langlands.

No dia 27 de junho de 1997, Andrew Wiles recebeu o prêmio Wolfskehl no valor 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 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".

CAPÍTULO 4

"De que me irei ocupar no céu, durante toda a eternidade, se não me derem uma infinidade de problemas de matemática para resolver?"

Augustin Louis Cuchy

Neste capítulo propomos algumas atividades que podem ser desenvolvidas em salas de aulas no Ensino Médio, visando o enriquecimento do conteúdo abordado nesta monografia.

Abordamos também algumas atividades lúdicas, que vão ao encontro da educação matemática, visando tornar as aulas mais participativas, dinâmicas e motivadas.

4.1. Atividades propostas

ATIVIDADE 4.1: (Bingo das Ternas Pitagóricas primitivas).

O objetivo desta atividade é brincar com as ternas pitagóricas primitivas.

MATERIAL UTILIZADO: cartelas para bingo.

DINÂMICA DA ATIVIDADE:

- Distribua uma cartela para cada aluno.
- O professor deve sortear os números.
- Os alunos devem marcar os números sorteados na cartela.
- Cada aluno deve verificar a quantidade de ternas pitagóricas que é possível formar através dos números sorteados (se tiver, é claro).
- O aluno que tiver mais ternas na cartela é o vencedor.

ATIVIDADE 4.2 (Completando ternas pitagóricas):

O objetivo desta atividade é continuar brincando com as ternas pitagóricas.

MATERIAL UTILIZADO: Utilizaremos dados de 20 faces (**icosaedro regular**).

DINÂMICA DA ATIVIDADE:

- Separar a turma em grupos de cinco alunos.
- Entregar para cada grupo formado **2 (dois)** dados.
- Eleger no grupo o aluno representante que fará o sorteio. Este aluno jogará os dados, todos deverão ficar atentos às faces sorteadas inclusive o representante.
- O aluno que perceber que os 2 números sorteados podem ser completados como um terceiro número para formar uma terna pitagórica, deverá gritar imediatamente **TERNA** e completá-la. Quem o fizer primeiro, formando a terna pitagórica é o ganhador da rodada.
- Por exemplo: se foram sorteados os números: 3 e 5. O aluno deverá gritar "**TERNA"** e dizer que 3 e 5 formam uma terna pitagórica com 4.
- Se completar errado o aluno perde 1 (um) ponto, se acertar ganha 2 (dois) pontos.
- O aluno que tiver a maior pontuação após um número pré-determinado de sorteios, será declarado o vencedor daquele grupo.
- O professor deve estabelecer quantas rodadas deve ter o jogo e os critérios de desempate, como por exemplo, em caso de empate, o mais velho seja declarado o vencedor.
- Reúna os vencedores de cada grupo para fazer uma grande final.

ATIVIDADE 4.3: (Contando quadrados unitários)

O objetivo desta atividade é determinar quantos quadradinhos de lado de medida 1 serão necessários para construir n quadrados de lados de medidas $1,2,\ldots,n$.. Em linguagem matemática, este problema se resume a determinar em função de n quanto vale a seguinte soma:

$$S_n = 1^2 + 2^2 + 3^2 + \cdots + n^2$$

ATIVIDADE 4.4 (Rearrumando quadrados) :

O objetivo desta atividade é encontrar as ternas pitagóricos, isto é, encontrar uma trinca de inteiros (x, y, z) satisfazendo a equação do teorema de Pitágoras $x^2 + y^2 = z^2$, com auxilio da geometria, usando o conceito de área.

MATERIAL UTILIZADO: Pequenos quadrados, todos do mesmo tamanho, feitos de cartolina. Papel, caneta e calculadora.

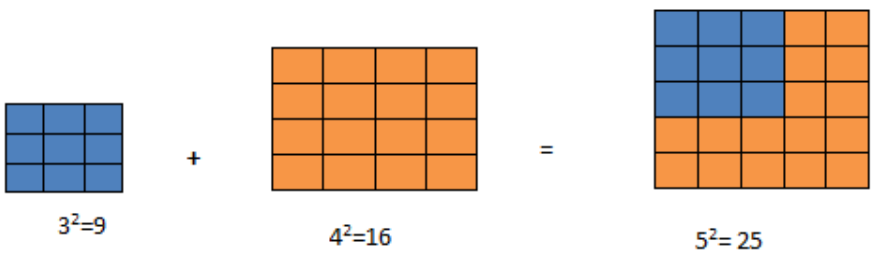
DINÂMICA DA ATIVIDADE:

- Separar a turma em grupos (de três a quatro alunos, como preferir).
- Entregar para os grupos quadrados de lados de medidas 1 feito de cartolina ou material similar.
- Proponha aos grupos que construa novos quadrados de lados de medidas 2, 3, 4, 5.

  Segue da solução da atividade 4.3 que teremos de disponibilizar a cada grupo

$$S_5 = \frac{1}{6}\,5.(5+1).(2.5+1) = \frac{1}{2.3}\,5\,.2\,.3\,.11 = 55$$

- Proponha que os alunos pintem de cores diferentes cada novo quadrado de lados 2,3,4,5.
- Pergunte aos alunos se é possível rearrumar a soma dos quadrinhos de dois quadrados para que possam formar um terceiro quadrado de lado maior.
- Uma possível solução seria a arrumação conforme figura abaixo:



- Se a igualdade for verificada você esta diante de um terno pitagórico.

- Anote os valores em uma tabela e confira os cálculos na calculadora.
- **Agora é com a turma toda junta**: Proponha aos grupos que construa novos quadrados de lados de medidas 2, ..., 13. Segue da solução da atividade 4.3 que teremos de disponibilizar a turma

$$S_{13} = \frac{1}{6}\,13.(13+1).(2.13+1) = \frac{1}{2.3}\,13\,.2\,.7\,.3^3 = 819$$

- Pergunte aos alunos se é possível rearrumar a soma dos quadrinhos de dois quadrados para que possam formar um terceiro quadrado de lado maior, diferente da formação da primeira atividade ? onde foi formando a terna pitagórica $(3,4,5)$.
- Avalie as respostas dos alunos.

ATIVIDADE 4.5: (Rearrumando Cubos).

O objetivo desta atividade é continuar brincando com as ternas pitagóricas.

MATERIAL UTILIZADO: montagem de cubos encaixantes ou um punhado de dados em forma de cubo que é de fácil aquisição.

DINÂMICA DA ATIVIDADE:

- Deixe a turma toda reunida.
- Monte um cubo de aresta 2 e apresente o cubo de aresta 1
- Pergunte qual é a quantidade de cubos de aresta 1 disponíveis?
  Resposta: $2^3 + 1^3 = 9$
- Pergunte se é possível juntar a soma de cubos unitários dos 2 cubos anteriores de modo a formar um terceiro cubo, eu caso contrario, qual a medida da aresta do cubo mais próximo, informando a quantidade de sobra ou falta :
  Resposta: não, o cubo mais próximo, tem aresta 2 e **sobra** 1 cubo.
- Pergunte qual a quantidade de cubos unitários em 2 cubos de arestas 3?
  Resposta: $3^3 + 3^3 = 54$.
- Pergunte qual a medida da aresta do cubo mais próximo, informando a quantidade de sobra ou falta.

  Resposta: 4 pois $4^3 = 64$ e **faltam** 10 cubinhos pois temos 54 cubos unitários
- Pergunte qual a quantidade de cubos unitários em 2 cubos de arestas 4?
  Resposta: $4^3 + 4^3 = 128$.

- Pergunte qual a medida da aresta do cubo mais próximo, informando a quantidade de sobra ou falta.

  Resposta: 5 pois $5^3 = 125$ e **sobram** 3 cubinhos pois temos 128 cubos unitários

- Caso seja possível encontrar uma terna de números (a, b, c) satisfazendo a equação $a^3 + b^3 = c^3$, esta terna é chamada de ***terna fermatiana cúbica*** e foi inspirada na situação anterior, que é a ***terna pitagória*** onde vale a equação $a^2 + b^2 = c^2$

- Comente um pouquinho sobre Fermat e sobre o Ultimo Teorema de Fermat.

ATIVIDADE 4.6 (Buscando uma terna Fermatiana cúbica com o EXCEL)

O objetivo desta atividade e fazer um experimento e tentar intuir se a equação fermatiana cúbica vai ser satisfeita para uma terna de inteiros não nulos.

MATERIAL UTILIZADO: computador com o programa EXCEL

DINÂMICA DA ATIVIDADE:

- Separar a turma em grupos (de três, quatro, como preferir).
- Leve-os para o laboratório de informática.
- Proponha aos alunos a utilização de uma planilha de Excel e solicite aos alunos encontrar uma terna fermatiana cúbica (x, y, z) com todos não nulos, satisfazendo a equação dada por $x^3 + y^3 = z^3$**.**
- Pergunte se algum grupo conseguiu êxito nesta atividade
- O professor pode perguntar se alguém acredita que é possível encontrar uma terna fermatiana cúbica.
- Em qualquer uma das 3 (três) possibilidades: SIM, NÃO, ou NÃO FAÇO A MENOR IDEIA, o que o levou a acreditar na possibilidade escolhida.
- Comente um pouquinho sobre Fermat e sobre o Último Teorema de Fermat

ATIVIDADE 4.7 (Enigma da idade de Diofante)

Não sabemos com precisão qual a época em que Diofante de Alexandria viveu, mas uma data em torno de 250 a.C é aceita como sendo a estimativa mais provável.

Diofante gostava de resolver questões que exigiam números inteiros, e hoje tais problemas são conhecidos como *equações diofantinas*. Sua carreira foi passada em Alexandria, onde ele reunia problemas bem conhecidos e inventava novos. Seu tratado intitulado Aritmética continha 13 (treze) volumes que formaram a ARITMÉTICA DE DIOFANTE e somente 6 (seis) volumes sobreviveram da biblioteca de Alexandria no ano de 642 d.C devido aos ataques dos cristãos.

De acordo como a memória de um resolvedor de problemas, o único detalhe sobre a vida de Diofante que restou foi um enigma, que dizem ter sido gravado na lápide de seu túmulo:

> *"Deus lhe concedeu a graça de ser um menino pela sexta parte de sua vida. Depois por um doze anos, ele cobriu seu rosto com a barba. A luz do casamento iluminou o após a sétima parte e cinco anos depois do casamento. Ele concedeu-lhe um filho. Ah! Criança tardia e má, depois de viver metade da vida de seu pai o destino frio o levou. Após consolar sua mágoa em sua ciência dos números, por quatro anos,. Diofante terminou sua vida."*

O desafio é calcular quanto tempo Diofante viveu.

ATIVIDADE 4.8: (Qual foi o erro cometido) Descubra o que aconteceu na prova com a seguinte argumentação lógica a seguir:

$$a = b \;\Rightarrow\; a^2 = ab \;\Rightarrow a^2 + \underbrace{a^2 - 2ab} = ab + \underbrace{a^2 - 2ab} \;\Rightarrow 2\,(a^2 - ab) = (a^2 - ab)$$

Dividindo ambos os lados por $(a^2 - ab)$ podemos concluir que :

$$2 = 1$$

Qual foi o erro cometido para concluir que $2 = 1$?

ATIVIDADE 4.9: (Aplicação do Ultimo Teorema de Fermat)

Mostre como consequência direta do Último Teorema de Fermat que:

$$\sqrt[n]{2} \text{ é } irracional.$$

4.2. Solução das Atividades propostas

RESPOSTA DA ATIVDADE 4.1 (Bingo das ternas pitagóricas primitivas)

O objetivo desta atividade é que o aluno relembre das primeiras ternas pitagóricas apresentadas nesta monografia na Seção 2.1, página 32, ou utilize as ternas pitagóricas de primeiro e segundo tipo, para levar alguma vantagem neste Bingo Pitagórico primitivo, a saber:

$(3,4,5)$	$(12,5,13)$	$(8,15,17)$	$(24,7,25)$
$(20,21,29)$	$(12,35,37)$	$(40,9,41)$	$(28,45,53)$
$(60,11,61)$	$(56,33,65)$	$(16,63,65)$	$(48,55,73)$

RESPOSTA DA ATIVIDADE 4.2: (Completando ternos pitagóricos via icosaedro)

Em virtude dos dados serem um icosaedro regular, e portanto terem 20 lados, e caso os mesmos tenham em suas faces os números de 1 a 20, teremos 3 possibilidades de formarmos ternas pitagóricas, a saber:

$$(3,4,5), \quad (5,12,13), \quad (8,15,17)$$

Caso alteremos algumas faces dos dados, por exemplo, alteremos a face 1 para 24, a face 2 para 25, a face 6 para 21 e a face 9 para 29, teremos mais duas possibilidades de formarmos duas novas ternas pitagóricas, a saber:

$$(7,24,25), \quad (20,21,29)$$

Isto tornaria o jogo das ternas pitagóricas um pouco mais interessante.

RESPOSTA DA ATIVIDADE 4.3: (Contando quadrados unitários)

$$S_n = \frac{1}{6}\, n.(n+1).(2n+1)$$

Solução: Para obtermos um expressão para a soma de inteiros de 1 até n, basta agruparmos os extremos de fora para dentro, isto é, $1+n = (n+1)$, $2+(n-1) = (n+1)$ e assim por diante, e multiplicarmos pelo número de pares obtidos, isto é:

$$1 + 2 + \cdots + (n-1) + n \; = \frac{n}{2}(n+1)$$

Desenvolva o cubo da soma para $(1+n)$ para $n = 1, \ldots, n$ e some de ambos os lados eliminando os termos comum a cada lado.

$$(1+1)^3 \; = \; 1^3 + 3.1^2.1 + 3.1.1^2 + 1^3$$

$$(1+2)^3 \; = \; 1^3 + 3.1^2.2 + 3.1.2^2 + 2^3$$

$$\ldots \qquad\qquad \ldots$$

$$+ \quad (1+n)^3 \; = \; 1^3 + 3.1^2.n + 3.1.n^2 + n^3$$

Somando de ambos os lados, e eliminando os termos comum de cada lado, temos que

$$(1+n)^3 \; = \; n\,(1^3) + 3.1^2.(1 + 2 + \cdots + n) + 3\,.1\,.(1^2 + 2^2 + \cdots + n^2) \; + 1^3$$

$$(1+n)^3 \; = (n+1) + 3.\frac{n(n+1)}{2} + 3\,.1\,.(1^2 + 2^2 + \cdots + n^2)$$

Isolando a soma de quadrados,

$$3\,.(1^2 + 2^2 + \cdots + n^2) = (n+1)^3 - (n+1) - \frac{3n(n+1)}{2}$$

Logo

$$3\,.(1^2 + 2^2 + \cdots + n^2) \; = \frac{(n+1)}{2}\,[\; 2(n+1)^2 - 2 - \; 3n]$$

$$(1^2 + 2^2 + \cdots + n^2) \; = \frac{(n+1)}{2.3}\,[\; 2n^2 + \; n]$$

Segue que:

$$S_n = (1^2 + 2^2 + \cdots + n^2) = \frac{1}{6}\,n(2n+1).(n+1) \qquad \blacksquare$$

RESPOSTA DA ATIVIDADE 4.4 (Rearrumando quadrados):

A resposta à última pergunta é afirmativa, onde a próxima terna pitagórica é dada por $(5,12,13)$.

Desta forma, podemos imaginar a busca de soluções com números inteiros para a equação de Pitágoras como a busca de dois quadrados que possam ser somados para formar um terceiro quadrado.

Na monografia, apresentamos os 12 primeiras trios pitagóricos. Um trio pitagórico ainda maior é (99,4900,4901). Os trios pitagóricos se tornam raros à medida que os números aumentam, e encontrá-los se torna cada vez mais difícil.

RESPOSTA DA ATIVIDADE 4.5: (Rearrumando cubos)

Já esta contextualizada na própria atividade.

RESPOSTA DA ATIVIDADE 4.6 (Terna fermatiana cúbica via EXCEL**)**

Já esta contextualizada na própria atividade.

RESPOSTA DA ATIVIDADE 4.7 (Enigma da idade de Diofante)

De acordo como a memória de um resolvedor de problemas, o único detalhe sobre a vida de Diofante que restou foi um enigma, que dizem ter sido gravado na lápide de seu túmulo:

> *"Deus lhe concedeu a graça de ser um menino pela sexta parte de sua vida. Depois por doze anos, ele cobriu seu rosto com a barba. A luz do casamento iluminou o após a sétima parte e cinco anos depois do casamento ele concedeu-lhe um filho. Ah! Criança tardia e má, depois de viver metade da vida de seu pai o destino frio o levou. Após consolar sua mágoa em sua ciência dos números, por quatro anos,.Diofante terminou sua vida."*

O desafio é calcular quanto tempo Diofante viveu.

Solução: Seja V a duração da vida de Diofante. Vamos agora traduzir em linguagem matemática as informações do Enigma de Diofante que se encontrava na lápide do seu túmulo:

- $V/6$ de sua vida Diofante passou como menino
- $V/12$ de sua vida, Diofante passou como rapaz
- $V/7$ de sua vida, foi o período antes de se casar.
- Após 5 anos Diofante teve um filho.
- $V/2$ foi o tempo de vida de seu filho.
- Após 4 anos Diofante morreu.

A duração da vida de Diofante é a soma do que foi dito acima:

$$V = \frac{V}{6} + \frac{V}{12} + \frac{V}{7} + 5 + \frac{V}{2} + 4 \quad \Rightarrow V = \frac{75}{84}V + 9 \;\Rightarrow \left(1 - \frac{75}{84}\right)V = 9 \;\Rightarrow V = \frac{9.84}{9} = 84$$

Diofante viveu 84 anos. ■

RESPOSTA DA ATIVIDADE 4.8 (Qual foi o erro cometido)

Como por hipótese $a = b$ implica que $(a^2 - ab) = 0$ e portanto não podemos dividir a equação por $(a^2 - ab)$, o gerou o absurdo de concluir que $2 = 1$!!!! ■

RESPOSTA DA ATIVIDADE 4.9 ($\sqrt[n]{2}$ é $irracional$)

Suponhamos que existem inteiros não nulos a, b tais que

$$\sqrt[n]{2} = \frac{a}{b} \;\Rightarrow\; 2 = \frac{a^n}{b^n} \;\Rightarrow\; a^n = 2b^n \quad \Rightarrow \quad a^n = b^n + b^n$$

ou seja, (a, b, b) é uma solução não trivial do Último Teorema de Fermat. Absurdo !!!! ■

CONCLUSÃO

Vimos que uma ideia aparentemente simples denominado método da descida infinita utilizada por Fermat, possibilitou apresentarmos uma prova do Último Teorema de Fermat para o caso $n = 3$ e $n = 4$, que afirma que não existe solução nos inteiros não nulos para a equação $x^n + y^n = z^n \ para \ n \geq 3$. A prova apresentada é compreensível a alunos do ensino fundamental e médio.

A abordagem como os assuntos foram expostos foi feita em ordem cronológica e de forma a facilitar a compreensão do conteúdo de um aluno de ensino médio e foi evitado à utilização de conhecimentos específicos que vão alem de sua grade curricular, e devido a isso, houve uma grande preocupação com o uso da linguagem utilizada e destacamos a perseverança de um jovem matemático que jamais desistiu da prova do ultimo teorema de Fermat, o matemático Andrew Wiles.

Uma frase famosa de um matemático e filósofo Francês, Le Rond D'Alembert (1717-1783), mas conhecido no meio matemático apenas com D'alember, dizia que: "A álgebra é muito generosa, frequentemente ela da mais do se pode esperar dela."

Ao concluir esta dissertação esperamos que este texto possa contribuir como estímulo e fonte de referência aos possíveis leitores interessados neste tipo de assunto, na busca de ampliar seus conhecimentos, além da várias atividades propostas para serem desenvolvidas com alunos do ensino fundamental e médio.

REFERÊNCIAS BIBLIOGRÁFICAS

[1]-Singh, Simon – O Último Teorema de Fermat – Tradução de Jorge Luis Calife – 20ª edição – Rio de Janeiro – Editora Record – 2012.

[2]-Ribenboim, Paulo – Fermat's last theorem for amateurs – Springer Verlag New York – 2000.

[3]-Ribenboim, Paulo – Números Primos. Velhos Mistérios e Novos Recordes – 1ª Edição – Rio de Janeiro – Coleção Matemática Universitária – IMPA – 2012.

[4]- Dorrie, Henrich – 100 Great Problems of Elementary Mathematics – Their History and Solution – Editora Dover Publications Inc – 1965.

[5]- Moreira, Carlos G. T. A., Martinez, Fabio E. B. e Saldanha, Nicolau C. – Tópicos de Teoria dos Números – Rio de Janeiro – Coleção PROFMAT.02 – SBM – 2012.

[6]- Gouvêa, Fernando Q., – Em busca da "Demonstração Maravilhosa" – RPM, Nº 15 – 1989.

[7]- Gouvêa, Fernando Q., O Ultimo Teorema da Fermat – RPM – Nº 32 –1993.

[8]-Boyer, Carl B. *História da Matemática*, tradução: Elza F. Gomide. São Paulo, Ed. da Universidade de São Paulo, 1974.

[9]-Eves, Howard. Introdução à história da matemática, tradução: Hygino H. Domingues-Campinas, SP: Editora da Unicamp, 2004.

[10]-Fernandes, C.E.de M. Triplos Pitagóricos e não Pitagóricos-RJ: Editora interciência, 2002.

[11]-Filho, E. A. teoria Elementar dos Números,Editora Nobel,São Paulo,1985.

[12]-Garbi, Gilberto Geraldo. A Rainha das Ciências: um passeio histórico pelo maravilhoso mundo da matemática: Editora Livraria da Física, 2006