Universidade Federal da Paraíba
Centro de Ciências Exatas e da Natureza
Departamento de Matemática
Mestrado Profissional em Matemática
em Rede Nacional PROFMAT

Demonstrações Elementares para a Equação de Fermat $x^n + y^n = z^n$, para $n \in \{2, 3, 4, 5\}$

por

Josinaldo José da Silva

sob orientação do

Prof. Dr. Alexandre de Bustamante Simas

Dissertação apresentada ao Corpo Docente do Mestrado Profissional em Matemática em Rede Nacional PROFMAT-CCEN-UFPB, como requisito parcial para a obtenção do título de Mestre em Matemática.

Agosto/2019
João Pessoa - PB

Demonstrações Elementares para a Equação de Fermat $x^n + y^n = z^n$, para $n \in \{2, 3, 4, 5\}$

por

Josinaldo José da Silva

Dissertação apresentada ao Corpo Docente do Mestrado Profissional em Matemática em Rede Nacional PROFMAT-CCEN-UFPB, como requisito parcial para a obtenção do título de Mestre em Matemática.

Área de Concentração: Matemática.

Aprovada por:

Prof. Dr. Alexandre de Bustamante Simas -UFPB (Orientador)

Prof. Dr. Carlos Bocker Neto - UFPB

Prof. Dr.Henrique de Barros Correia Vitório - UFPE

Agosto/2019

Agradecimentos

Agradeço primeiramente a Deus, por me proporcionar essa oportunidade e por sempre me manter centrado em meus objetivos.
Agradeço ao meu professor orientador Alexandre de Bustamantes. Pela oportunidade de aprender seus ensinamentos, e estender meu conhecimento além de fronteiras que nunca imaginei. Pela orientação no presente trabalho,agradeço pela dedicação, profissionalismo, paciência, conhecimento compartilhado, enfim, por toda ajuda prestada.
A todos os professores que tive em toda minha vida acadêmica, em especial aos da UFPB por todos os ensinamentos, profissionais e pessoais.
Agradeço também a minha esposa Rubiana Menezes. Pilar de minha conquista, sem ela isso não seria possível. Compreensiva, amiga, minha principal motivadora.
Aos meus pais e meus avós, por serem meus referenciais de força e determinação.
Meus irmãos, por depositarem toda fé e crença em minha capacidade.
A todos os meus amigos que souberam compreender minha ausência, aos conselhos fornecidos, além da amizade incondicional.

Dedicatória

As minhas duas filhas Maria Júlia e Maria Manuella

Resumo

Este trabalho apresenta algumas demonstrações elementares para alguns casos particulares do Último Teorema de Fermat. Por muitas vezes buscamos encontrar soluções inteiras para uma equação polinomial, ou seja, solucionar uma equaçáo diofantina. Esta ideia foi a base do que é considerado o problema mais famoso e duradouro da história da matemática, o Último teorema de Fermat. A busca por provas ou contraprovas desse resultado foi determinante no desenvolvimento da teoria algébrica dos números, permitindo estabelecer-se diversas ferramentas poderosas e sofisticadas, muito contributivas para a matemática moderna. Um fato é que o último Teorema de Fermat foi um dos grandes mistérios da história da Matemática e que desafiou as mentes mais brilhantes e determinadas do mundo da matemática. Um teorema de fácil entendimento, mas de resolução considerada por muitos como impossível. Este trabalho tem como foco apresentar algumas demonstrações elementares para o Último Teorema de Fermat $x^n + y^n = z^n$ para os casos $n \in \{2, 3, 4, 5\}$, mostrando que tal equação de fato não possui soluções inteiras não-triviais para $n > 2$. Para o caso $n = 5$ é feita uma demonstração parcial, onde mostra-se que se $5 \nmid x, 5 \nmid y, 5 \nmid z$, com x, y, z inteiros, então $x^5 + y^5 \neq z^5$.

Palavras-chave: Fermat, Equações, Demonstrações.

Abstract

This paper presents some elementary demonstrations for some particular cases of Fermat's Last Theorem. We often seek to find whole solutions for a polynomial equation, that is, to solve a diophantine equation. This idea was the basis of what is considered to be the most famous and enduring problem in the history of mathematics, Fermat's Last Theorem. The search for evidence or evidence of this result was crucial in the development of the algebraic theory of numbers, allowing to establish several tools. powerful and sophisticated, very contributory to modern mathematics. One fact is that Fermat's last Theorem was one of the great mysteries of the history of mathematics and it challenges the most brilliant and determined minds in the world of mathematics. An easy-to-understand theorem that many consider impossible. This paper focuses on presenting some elementary demonstrations for Fermat's Last Theorem $x^n + y^n = z^n$ for cases $n \in 2, 3, 4, 5$, showing that such an equation does not have non-trivial integer solutions for $n > 2$. For the case $n = 5$ a partial demonstration is made, showing that if $5 \nmid x, 5 \nmid y, 5 \nmid z$, with x, y, z integers, then $x^5 + y^5 = z^5$.

Keywords: Fermat, Equations, Demonstrations.

Sumário

Introdução

Como sabemos o último teorema de Fermat é representado pela equação diofantina $x^n + y^n = z^n$. Fermat afirmava que era impossível separar um cubo em dois cubos, ou uma quarta potência em duas quartas potências, de forma geral, qualquer potência maior do que as já citadas, em duas potências semelhantes. Fermat é mais bem lembrado quando associado a seu trabalho em teoria dos números, em particular pelo Último Teorema de Fermat. Este teorema diz que: não tem solução inteira não nula para x, y e z quando $n > 2$. Esse problema é de origem grega e partiu do tão conhecido teorema de Pitágoras. Fermat observou que de fato a equação de Pitágoras $x^2 + y^2 = z^2$ é válida para todos os triângulos retângulos, porém, se ao invés de um quadrado, tivéssemos um cubo ou uma potência maior, se tornaria impossível encontrar soluções inteiras não nulas.
Ao afirmar que a equação $x^n + y^n = z^n$ não possuia solução para $n > 2$, fez com que Fermat criasse assim, o mais famoso e difícil problema matemático que o mundo já tinha visto. O mais interessante é que tal problema durou mais de três séculos e meio desafiando as mentes mais brilhantes da Matemática.
Fermat afirmou que tinha uma demonstração maravilhosa para o problema por ele proposto, entretanto, disse, que a margem onde escrevia era muito estreita para contê-la. Isso foi mais do que suficiente para fazer com que várias gerações de matemáticos ficassem na vontade de desenvolver uma solução para o problema ou de provar que ele era falso, mas até então, isto não aconteceu e, muitas tentativas de solucionar o problema foram exploradas sem o êxito esperado.

O que mais indagava os estudiosos matemáticos, era sobre, como Fermat chegou a prova do problema, do que ele se utilizou, visto que ele não tinha deixado nada registrado sobre essa demonstração.
Depois de provas e mais provas sem o êxito esperado pelos estudiosos matemáticos, Andrews Wiles, um desses matemáticos, conseguiu apresentar a prova para esse problema. Tal prova foi publicada no ano de 1995, fazendo com que chegasse ao fim, o mistério que durou mais de três séculos e meios. Nesse trabalho, vamos apre-

sentar algumas demonstrações elementares para a equação de Fermat, mostrando que, de fato, não existem soluções inteiras não-trivial para $x^n + y^n = z^n$. Com isso estruturamos o trabalho da seguinte forma: No primeiro capítulo é apresentada a demonstração da equação $x^2 + y^2 = z^2$, onde são caracterizadas todas as soluções para essa equação. No segundo capítulo é apresentada a demonstração da equação $x^3 + y^3 = z^3$. Onde mostramos que tal equação não possui solução inteira não-trivial como Fermat afirmava, pois, não se pode separar um cubo em dois cubos. Para tal demonstração, usamos a minimalidade de $\mid xyz \mid$. No terceiro capítulo é apresentada a demonstração da equação $x^4 + y^4 = z^4$. Nesse capítulo mostramos que tal equação não possui solução inteira não-trivial. Para a prova, partirmos de que não se pode ter a soma de duas quartas potências , resultando em um potência de grau 2. No quarto e último capítulo é apresentada a demonstração da equação $x^5 + y^5 = z^5$, onde mostramos que tal equação não possui solução inteira não-trivial. Para chegarmos em tal resultado, partimos do fato que, se 5 não divide nenhum dos x, y, z então $x^5 + y^5 + z^5 \neq 0$.

Capítulo 1

Demonstração para equação $x^2 + y^2 = z^2$

Nesse capítulo iremos apresentar uma prova elementar para a equação de Pitàgoras, isto é, uma demonstração para equação de Fermat $x^n + y^n = z^n$ para $n = 2$, onde será caractezizada todas as soluções para tal equação.

1.1 Caso $n = 2, x^2 + y^2 = z^2$

A equação

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

É a equação de Pitágoras e possui soluções inteiras. Vamos agora caracterizar todas essas soluções.

Teorema 1.1. *Seja $(x, y, z) \in \mathbb{N}^3$, uma terna pitagórica, isto é, uma terna tal que $mdc(x, y, z) = 1$ e $x^2 + y^2 = z^2$ então :*

(a) um dos números x, y é par e o outro é ímpar, e o número z é ímpar.
(b) Suponha que x é ímpar, então existem $a, b \in \mathbb{N}$, coprimos, tais que $a > b$,$a \not\equiv b$ mod 2, e

$$x = a^2 - b^2, y = 2ab, z = a^2 + b^2$$

Demonstração: Vamos começar mostrando que x, y e z são dois a dois coprimos. De fato suponha que p é primo e

$$p \mid mdc(x, y)$$

então, $p \mid x^2 + y^2 \Rightarrow p \mid z^2 \Rightarrow p \mid z$.

Absurdo! Pois x , y, z são coprimos. Portanto x e y são coprimos. O mesmo argumento serve para mostrar que x e z são coprimos e y e z também são coprimos.

Daí, concluímos que como x e y são coprimos, não podem ser ambos pares. Vamos mostrar agora que também não podem ser ambos ímpares. De fato, se x e y fossem ambos ímpares, então:

$$x \equiv 1 \ mod \ 4 \text{ ou } x \equiv 3 \ mod \ 4,$$

daí,

$$x^2 \equiv 1 \ mod \ 4$$

Da mesma forma

$$y^2 \equiv 1 \ mod \ 4.$$

Sendo assim,

$$x^2 + y^2 \equiv 2 \ mod \ 4.$$

Por outro lado, temos que, se z é par, então

$$z^2 \equiv 0 \ mod \ 4$$

Se z é ímpar, repetimos o argumento anterior para mostrar que

$$z^2 \equiv 1 \ mod \ 4.$$

Como

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

obtemos um absurdo! Logo, x e y não podem ser ambos ímpares.

Assim temos que x é par e y é ímpar ou x é ímpar e y par. Em ambos os casos temos que z é ímpar. Isto prova (a).

Vamos provar (b). Suponha sem perda de generalidade, que x é ímpar (renomeando as variáveis se necessário). Assim,

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

Daí,

$$y^2 = z^2 - x^2 = (z - x)(z + x) \tag{1.1}$$

Seja $d = mdc(z + x, z - x)$. Daí,

$$d \mid (z + x) - (z - x) \Rightarrow d \mid 2x,$$

e

$$d \mid (z + x) + (z - x) \Rightarrow d \mid 2z.$$

Como z e x são coprimos, segue então que $d \mid 2$. Além disso, como x e z são ímpares, então

$$2 \mid x + z \text{ e } 2 \mid z - x.$$

Portanto, segue que $d = 2$.

Desta forma,

$$z + x = 2u \text{ e } z - x = 2v,$$

com u e v coprimos.

Por (a) , como x é ímpar e y é par, temos que $\exists w \in \mathbb{N}$, tal que $y = 2w$. Daí por (1.1)

$$4w^2 = 4uv \Rightarrow w^2 = uv \tag{1.2}$$

Seja p primo e $q \in \mathbb{N}$ tal que $p^q \mid u$ e $p^{q+1} \nmid u$.

Seja ainda

$$\overline{q} = \begin{cases} q + 1, & \text{se } q \text{ é ímpar} \\ q, & \text{se } q \text{ é par} \end{cases}$$

Então,

$$p^q \mid u \Rightarrow p^q \mid w^2 \Rightarrow p^{\overline{q}} \mid w^2 \Rightarrow p^{\overline{q}} \mid uv$$

e como u e v são coprimos, segue que

$$p^{\overline{q}} \mid u$$

Logo, $\overline{q} = q \Rightarrow q$ é par. Sendo assim, u é um quadrado perfeito.

Portanto, existe $a \in \mathbb{N}$, tal que $u = a^2$. Da mesma forma, mostra-se que v é

quadrado perfeito. Assim, $\exists b \in \mathbb{N}$ tal que $v = b^2$.

Sendo assim, por (1.2) segue que

$$w^2 = a^2 b^2 \Rightarrow w = ab$$

pois $w, a, b \in \mathbb{N}$, e daí

$$y = 2w = 2ab \Rightarrow y = 2ab.$$

Além disso,

$$z + x = 2u = 2a^2 \Rightarrow a^2 = \frac{z+x}{2}$$
$$z - x = 2v = 2b^2 \Rightarrow b^2 = \frac{z-x}{2}$$

Daí,

$$z = \frac{z+x}{2} + \frac{z-x}{2} = a^2 + b^2$$

e

$$x = \frac{z+x}{2} - \frac{z-x}{2} = a^2 - b^2.$$

O que conclui a prova.

■

Capítulo 2

Demonstração para equação $x^3 + y^3 = z^3$

Nesse capítulo iremos apresentar uma prova elementar para a equação $x^3+y^3 = z^3$, isto é, uma demonstração para equação de Fermat $x^n+y^n = z^n$ para $n = 3$, onde será apresentado que não existem soluções inteiras não-triviais para esta equação.

2.1 Caso $n = 3,\ \ x^3 + y^3 = z^3$

Vamos fornecer um prova elementar para o teorema de Fermat com $n = 3$. A estratégia se baseia no artigo do Liu (2000).

Teorema 2.1. *A equação*

$$x^3 + y^3 = z^3 \tag{2.1}$$

não possui soluções inteiras não-triviais.

Demonstração: Realizaremos uma demonstração por absurdo. Assim suponha que a equação 2.1 admite solução não-trivial.
Assim,

$$W = \left\{ |\ xyz\ | \in \mathbb{N},\ \ (x, y, z) \in \mathbb{Z},\ \ x \neq 0,\ \ y \neq 0,\ \ z \neq 0 \text{ e } x^3 + y^3 = z^3 \right\}$$

é não vazio. Isto é, $W \neq \emptyset, W \subset \mathbb{N}$.

Portanto, pelo princípio da boa ordenação, W possui um menor elemento. Ou seja, (x, y, z) uma solução de (2.1) tal que $|xyz|$ é o menor elemento de W.

Afirmação 1 : x, y e z são dois-a-dois distintos.

De fato, se $x = y$ temos

$$2x^3 = z^3$$

Seja $q \in \mathbb{N}$, $2^q \mid z^3$, mas $2^{q+1} \nmid z^3$. Como z é cubo perfeito, segue que $q = 3k$ com $k \in \mathbb{N}$. Assim $2^{3k} \mid z^3$, mas $2^{3k+1} \nmid z^3$. Seja agora $\tilde{q} \in \mathbb{N}$ tal que $2^{\tilde{q}} \mid x^3$, mas $2^{\tilde{q}+1} \nmid x^3$. Como x^3 é cubo perfeito, então $\tilde{q} = 3\tilde{k}$ com $\tilde{k} \in \mathbb{N}$. Daí faça

$$x^3 = 2^{3\tilde{k}}\tilde{x}^3, \text{com } mdc(2, \tilde{x}) = 1,$$
$$z^3 = 2^{3k}\tilde{z}^3, \text{com } mdc(2, \tilde{z}) = 1$$

Daí,

$$2^{3\tilde{k}+1}\tilde{x}^3 = 2^{3k}\tilde{z}^3 \Rightarrow 2^{3\tilde{k}+1} = 2^{3k} \Rightarrow 3\tilde{k} + 1 = 3k$$

Absurdo! Logo, $x \neq y$.

Se $x = z \Rightarrow y^3 = 0 \Rightarrow y = 0$. Absurdo! Pois, a solução é não-trivial.

Se $y = z \Rightarrow x^3 = 0 \Rightarrow x = 0$. Absurdo!

Isto prova a afirmação (1)

■

Afirmação 2 : $mdc(x, y) = mdc(x, z) = mdc(y, z) = 1$. Além disso, exatamente um dos x, y, z é par.

Vamos começar mostrando que $mdc(x, y) = 1$. De fato, seja $d = mdc(x, y)$, então $\exists \tilde{x}$, $\tilde{y} \in \mathbb{Z}$, $x = d\tilde{x}$ e $y = d\tilde{y}$. Assim, temos que

$$d^3\tilde{x}^3 + d^3\tilde{y}^3 = z^3 \Rightarrow d^3(\tilde{x}^3 + \tilde{y}^3) = z^3 \Rightarrow d^3 \mid z^3$$

Assim, $\exists \tilde{z}^3 \in \mathbb{Z}$, $z^3 = d^3\tilde{z}^3$
Portanto,

$$\tilde{x}^3 + \tilde{y}^3 = \tilde{z}^3$$

Se $d > 1$, então $\mid \tilde{x}\tilde{y}\tilde{z} \mid < \mid xyz \mid$, contrariando a minimalidade de $\mid xyz \mid$. Logo, $d = 1$.

Seja agora $d = mdc(x, z)$. Então, $\exists \tilde{x}$, $\tilde{z} \in \mathbb{Z}$, $x = d\tilde{x}$ e $z = d\tilde{z}$. Daí

$$\begin{aligned} d^3\tilde{x}^3 + d^3(-\tilde{z})^3 = (-y)^3 &\Rightarrow d^3 \mid y^3 \\ &\Rightarrow \exists \tilde{y} \in \mathbb{Z}, \text{ tal que } y^3 = d^3(-\tilde{y})^3 \\ &\Rightarrow \tilde{x}^3 + (-\tilde{z})^3 = (-\tilde{y})^3 \\ &\Rightarrow \tilde{x}^3 + \tilde{y}^3 = \tilde{z}^3. \end{aligned}$$

Da mesma forma, se $d > 1$, então $\mid \tilde{x}\tilde{y}\tilde{z} \mid < \mid xyz \mid$, o que contraria a minimalidade de $\mid xyz \mid$. Logo, $d = 1$. Da mesma forma mostra-se que $mdc(y, z) = 1$

Agora vamos mostrar que teremos exatamente um número par entre os números x, y e z. De fato, se dois deles forem pares, segue que 2 é um divisor comum, o que contraria o fato de serem dois-a-dois coprimos (primeira parte da afirmação 2).

Como não podemos ter dois números pares entre x, y e z, segue que dois deles são ímpares. Como dois deles são ímpares, o terceiro é par.

De fato, se x e y são ímpares, olhando a congruência módulo 2

$$\begin{aligned} x^3 + y^3 = z^3 &\Rightarrow x^3 + y^3 \equiv z^3 \ \ mod\ 2 \\ &\Rightarrow 1 + 1 \equiv z^3, \ \ mod\ 2 \\ &\Rightarrow z^3 \equiv 0 \ \ mod\ 2 \\ &\Rightarrow z \equiv 0 \ \ mod\ 2. \end{aligned}$$

Da mesma forma, provam-se os outros casos. Isto conclui a afirmação (2).

■

Como temos que

$$\begin{aligned} x^3 + y^3 = z^3 &\Rightarrow x^3 + (-z)^3 = (-y)^3 \\ &\Rightarrow x^3 + \tilde{y}^3 = \tilde{z}^3, \end{aligned}$$

onde $\tilde{y} = -z$ e $\tilde{z} = -x$ e também

$$(-z)^3 + y^3 = (-x)^3 \Rightarrow \tilde{\tilde{x}} + y^3 = \tilde{\tilde{z}}^3$$

onde $\tilde{\tilde{x}} = -z$ e $\tilde{\tilde{z}} = -y$. Podemos supor, sem perda de generalidade, utilizando a afirmação 2, que

$$z \text{ é par} \tag{2.2}$$

Assim, segue da afirmação 2 que

$$x \text{ e } y \text{ são ímpares} \tag{2.3}$$

Portanto,

$$x + y \text{ e } x - y$$

são pares. Daí, existem $u, w \in \mathbb{Z}$ tais que

$$x + y = 2u \text{ e } x - y = 2w$$

Daí,

$$x = u + w \text{ e } y = u - w$$

Assim,

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

Assim,

$$z^3 = 2u(u^2 + 3w^2).$$

Afirmação 3: $mdc(u, w) = 1$ e exatamente um deles é ímpar.

De fato, se $d = mdc(u, w)$, temos que $d \mid x$ e $d \mid y \Rightarrow d \mid mdc(x, y) \Rightarrow d = 1$.

Como x é ímpar, por (2.3), e além disso, como $x = u + w$, então, se u e w forem pares, teríamos x par, absurdo. Por outro lado, se u e w fossem ímpares teríamos x par, absurdo.

Portanto, ou u é par e w é ímpar, ou u é ímpar e w é par. Isso prova a afirmação 3.

■

Vamos agora realizar a análise em dois casos:

Caso 1: u não é divisível por 3.
Como estamos supondo que $3 \nmid u$ e como $mdc(u, w) = 1$, segue que $mdc(u, 3w) = 1$. Além disso, como temos que u é par e w é ímpar ou u é ímpar e w é par, segue que em ambos os casos

$$\begin{aligned} u^2 + 3w^2 &\equiv 1 \ mod \ 2 \\ &\Rightarrow 2 \nmid u^2 + 3w^2 \end{aligned}$$

Assim, fazendo

$$d = mdc(2u, u^2 + 3w^2)$$

temos que

$$d = mdc(2u, u^2 + 3w^2) = mdc(u, u^2 + 3w^2)$$

Assim,

$$d \mid u \text{ e } d \mid u^2 + 3w^2 - u^2 \Rightarrow d \mid 3w^2$$

Como estamos supondo (caso 1) que $3 \nmid u$, segue que

$$d \mid w^2.$$

Se $d > 1$, tome p fator primo de d, então

$$p \mid u \text{ e } p \mid w^2 \Rightarrow p \mid w \Rightarrow p \mid mdc(u, w).$$

Porém, $mdc(u, w) = 1$. Absurdo! Portanto $d = 1$, ou seja

$$mdc(2u, u^2 + 3w^2) = 1.$$

Como temos que

$$z^3 = 2u(u^2 + 3w^2),$$

temos que existem $r, s \in \mathbb{Z}$ tais que

$$2u = r^3 \text{ e } u^2 + 3w^2 = s^3. \tag{2.4}$$

Caso 2: Suponha agora que u é divisível por 3.

Assim, existe $v \in \mathbb{Z}$ tal que $u = 3v$. Assim,

$$\begin{aligned} z^3 &= 2u(u^2 + 3w^2) \\ &= 6v(9v^2 + 3w^2) \\ &= 18v(3v^2 + w^2) \\ z^3 &= 18v(3v^2 + w^2). \end{aligned}$$

Observe que como $mdc(u, w) = 1$, temos que

$$mdc(3v, w) = 1$$

pois, $u = 3v$.

Note que $mdc(3v, w) = 1 \Rightarrow 3 \nmid w$. Além disso, u é par e w é ímpar, ou u é ímpar e w é par, temos que v é par e w é ímpar ou v é ímpar e w é par. Em qualquer um dos casos, tem-se que

$$3v^2 + w^2 \equiv 1 \ mod \ 2 \Rightarrow mdc(18v, 3v^2 + w^2) = mdc(9v, 3v^2 + w^2)$$

Se $3 \mid mdc(9v, 3v^2 + w^2)$, então

$$3 \mid 3v^2 + w^2 \Rightarrow 3 \mid w^2 \Rightarrow 3 \mid w.$$

Absurdo! Pois, $3 \nmid w$. Logo, $3 \nmid mdc(9v, 3v^2 + w^2)$. Por outro lado,

$$mdc(v, 3v^2 + w^2) = mdc(v, w^2)$$

mas, como $mdc(3v, w) = 1$, segue que $mdc(v, w^2) = 1$.

Assim,

$$\begin{aligned} mdc(18v, 3v^2 + w^2) &= mdc(9v, 3v^2 + w^2) \\ &= mdc(v, 3v^2 + w^2) \\ &= mdc(v, w^2) \\ &= 1 \\ &\Rightarrow mdc(18v, 3v^2 + w^2) = 1. \end{aligned}$$

Como temos que

$$z^3 = 18v(3v^2 + w^2),$$

segue que existem $r, s \in \mathbb{Z}$, tais que

$$18v = r^3 \ \text{ e } \ 3v^2 + w^2 = s^3. \tag{2.5}$$

Note que a equação Diofantina

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

onde $mdc(a, 3b) = 1$ e $a + b \equiv 1 \ mod \ 2$, apareceu tanto no caso 1 quanto no caso 2.

Vamos então, resolver essa equação Diofantina. Vamos começar com o caso em que s é primo.

Afirmação 4: Se s é primo, $a, b \in \mathbb{Z}$, $mdc(a, 3b) = 1$, $a + b \equiv 1 \ mod \ 2$ e

$$a^2 + 3b^2 = s^3$$

então $s > 3$, e , além disso, $s \nmid a$ e $s \nmid b$.

De fato, olhando módulo 2:

$$\begin{aligned} s^3 &\equiv a^2 + 3b^2 \ mod \ 2 \\ &\equiv a^2 + b^2 \ mod \ 2 \\ &\equiv a + b \ mod \ 2 \\ &\equiv 1 \ mod \ 2 \\ &\Rightarrow 2 \nmid s \Rightarrow s > 2. \end{aligned}$$

Olhando módulo 3:

$$\begin{aligned} s^3 &\equiv a^2 + 3b^2 \ mod 3 \\ &\equiv a^2 \ mod \ 3 \\ &\not\equiv 0 \ mod \ 3 \end{aligned}$$

pois, o $mdc(a, 3b) = 1 \Rightarrow 3 \nmid a$. Logo, como $s^3 \not\equiv 0 \ mod \ 3$, segue que $s \neq 3 \Rightarrow s > 3$. Isto prova a primeira parte da Afirmação 4.

Para a segunda parte suponha que $s \mid a$. Fazendo a congruência módulo s:

$$\begin{aligned} s^3 &\equiv a^2 + 3b^2 \ mod \ s \\ &\Rightarrow 0 \equiv 0 + 3b^2 \ mod \ s \\ &\Rightarrow 3b^2 \equiv 0 \ mod \ s \end{aligned}$$

Como $3 \nmid s$, segue que:

$$b^2 \equiv 0 \ mod \ s.$$

Como s é primo, segue que

$$b \equiv 0 \ mod \ s.$$

Daí, $s \mid mdc(a, b) \Rightarrow s \mid mdc(a, 3b) = 1$. Absurdo. Portanto $s \nmid a$.

Analogamente, temos que $s \nmid b$. Isto, conclui a afirmação 4.

■

Como $s \nmid b$, segue do Pequeno Teorema de Fermat que

$$b^{s-1} \equiv 1 \ mod \ s$$

Daí, b^{s-2} é a inversa de b módulo s, onde $s - 2 > 0$, pois pela afirmação 4, $s > 3$

Assim, seja

$$g = ab^{s-2}$$

Como

$$a^2 + 3b^2 \equiv 0 \ mod \ s,$$

temos que

$$\begin{aligned} a^2b^{2(s-2)} + 3b^{2+2s-4} &\equiv 0 \ mod \ s \\ &\Rightarrow (ab^{s-2})^2 + 3(b^{s-1})^2 \equiv 0 \ mod \ s \\ &\Rightarrow g^2 + 3 \equiv 0 \ mod \ s. \end{aligned}$$

Assim

$$g^2 + 3 \equiv 0 \ mod \ s$$

Agora, faça $q = \lfloor \sqrt{s} \rfloor$. Como s é primo, então

$$q < \sqrt{s} < q + 1 \tag{2.6}$$

Afirmação 5: Existem $i', j', i", j"$ inteiros, tais que $i', j', i", j" \in \{0, 1, ..., q\}$, com $i' \neq i"$ ou $j' \neq j"$ tais que

$$g \cdot (i' - i") \equiv j' - j" \ mod \ s.$$

Comece notando que como

$$g^2 \equiv -3 \ mod \ s$$

segue que $s \nmid g$, já que $3 \nmid s$. Por 2.6, temos que

$$q + 1 > \sqrt{s} \Rightarrow (q + 1)^2 > s.$$

Considere a expressão

$$gi - j \ \text{ com } \ i, j \in \{0, 1, ..., q\}$$

Temos $(q+1)^2 > s$ expressões diferentes e apenas s restos possíveis, na divisão por s. Assim, existem dois pares diferentes (i', j') e $(i", j")$ tais que

$$(i', j') \neq (i", j"),$$

isto é,

$$\begin{aligned} & i' \neq i" \text{ ou } j' \neq j" \text{ e} \\ & gi' - j' \equiv gi" - j" \ mod \ s \\ & \Rightarrow g(i' - i") - (j' - j") \equiv 0 \ mod \ s. \end{aligned}$$

Assim,

$$g(i' - i") \equiv j' - j" \mod s.$$

Isto prova a afirmação 5.

■

Observe que como $i', j', i", j" \in \{0, 1, ..., q\}$ temos que

$$i' - i" \in \{-q, ..., q\} \text{ e } j' - j" \in \{-q, ..., q\} \tag{2.7}$$

Defina

$$i = \mid i' - i" \mid \text{ e } j = \mid j' - j" \mid .$$

Assim, segue da afirmação 5 que

$$gi \equiv j \ mod \ s \text{ ou } gi \equiv -j \ mod \ s.$$

Assim,

$$gi + j \equiv 0 \ mod \ s \text{ ou } gi - j \equiv 0 \ mod \ s.$$

Daí, em qualquer um dos casos acima temos que

$$(gi + j)(gi - j) \equiv 0 \ mod \ s \Rightarrow g^2 i^2 - j^2 \equiv 0 \ mod \ s \tag{2.8}$$

Por (2.6) e (2.7) temos que

$$i < \sqrt{s} \text{ e } j < \sqrt{s}.$$

Além disso, se

$$j = 0 \Rightarrow g^2 i^2 \equiv 0 \ mod \ s$$

e como $s \nmid g$, segue que

$$i^2 \equiv 0 \ mod \ s.$$

Como $0 \leq i < \sqrt{s}$, segue que

$$i = 0.$$

Absurdo!, pois teríamos

$$i = j = 0 \Rightarrow i' = i\text{"} \ \text{ e } \ j' = j\text{"},$$

contrariando a Afirmação 5 .

Logo, $j \neq 0$. Analogamente temos que $i \neq 0$. Portanto

$$0 < i < \sqrt{s} \ \text{ e } \ 0 < j < \sqrt{s} \tag{2.9}$$

Assim, como

$$g^2 + 3 \equiv 0 \ mod \ s$$

e por (2.8)

$$g^2 i^2 \equiv j^2 \ mod \ s.$$

temos que

$$\begin{aligned} g^2 i^2 &\equiv -3i^2 \ mod \ s \\ \Rightarrow j^2 &\equiv -3i^2 \ mod \ s \\ \Rightarrow j^2 + 3i^2 &\equiv 0 \ mod \ s \end{aligned}$$

Daí, $\exists h \in \mathbb{Z}$ tal que $3i^2 + j^2 = hs$.

Como $3i^2 + j^2 > 0 \Rightarrow h > 0$.

Por (2.9), $i^2 < s$ e $j^2 < s$, daí

$$3i^2 + j^2 < 4s.$$

Assim, $h \leq 3$ e $h > 0$. Logo, $h = 1, h = 2$ ou $h = 3$.

Vamos mostrar agora que $h \neq 2$.

De fato, se $h = 2$, temos que

$$\begin{aligned} & 3i^2 + j^2 = 2s \\ & \Rightarrow 3i^2 + j^2 \equiv 0 \ mod \ 2 \\ & \Rightarrow i^2 + j^2 \equiv 0 \ mod \ 2 \\ & \Rightarrow i + j \equiv 0 \ mod \ 2. \end{aligned}$$

Assim i e j são pares ou i e j são ímpares.

Se i e j forem pares, temos que

$$\begin{aligned} & 3i^2 + j^2 \equiv 0 \ mod \ 4 \\ & \Rightarrow 2s \equiv 0 \ mod \ 4 \\ & \Rightarrow s \equiv 0 \ mod \ 2. \end{aligned}$$

Absurdo!

Se i e j forem ímpares, segue que

$$i^2 \equiv 1 \ mod \ 4 \ \text{ e } \ j^2 \equiv 1 \ mod \ 4.$$

Para a demonstração de que

$$i \ \text{ímpar} \Rightarrow i^2 \equiv 1 \ mod \ 4$$

(ver caso $n = 2$) feito no capítulo 1.

Portanto,

$$\begin{aligned} & 3i^2 + j^2 \equiv 3 + 1 \ mod \ 4 \\ & \Rightarrow 2s \equiv 0 \ mod \ 4 \\ & \Rightarrow s \equiv 0 \ mod \ 2. \end{aligned}$$

Desta forma, chegamos a outro absurdo! Portanto, $h \neq 2$.

Logo, temos $h = 1$ ou $h = 3$

Se $h = 1$ temos que $3i^2 + j^2 = s$

Se $h = 3$, então

$$3i^2 + j^2 = 3s \Rightarrow j^2 = 3(s - i^2) \Rightarrow 3 \mid j^2 \Rightarrow 3 \mid j.$$

Daí, $j = 3k$, onde $k \in \mathbb{Z}$. Assim,

$$3i^2 + 9k^2 = 3s \Rightarrow i^2 + 3k^2 = s$$

Assim , para qualquer caso acima, $h = 1$ ou $h = 3$, temos que

$$s = m^2 + 3n^2 \tag{2.10}$$

onde $m, n \in \mathbb{Z}$.

Suponha então que temos (2.10), vamos mostrar que $mdc(m, 3n) = 1$.

Se $3 \mid m$, então temos que

$$\begin{aligned} s &\equiv m^2 + 3n^2 \ \ mod\ 3 \\ &\equiv 0 \ \ mod\ 3 \end{aligned}$$

Absurdo. Logo $3 \nmid m$ e $mdc(m, 3n) = mdc(m, n)$.

Se $d \mid m$ e $d \mid n$, segue que $d \mid s$. Porém s é primo, logo $d = 1$ ou $d = s$. Como $m < s$ e $d \mid m \Rightarrow d < s \Rightarrow d = 1$. Assim, $mdc(m, n) = 1$ e $mdc(m, 3n) = 1$.

Além disso,

$$\begin{aligned} &s \equiv m^2 + 3n^2 \ \ mod\ 2 \\ &\Rightarrow 1 \equiv m^2 + n^2 \ \ mod\ 2 \\ &\Rightarrow 1 \equiv m + n \ \ mod\ 2. \end{aligned}$$

Assim, $mdc(m, 3n) = 1$ e $m + n \equiv 1 \ \ mod\ 2$

Por (2.10) temos que

$$s = m^2 + 3n^2$$

e temos que

$$s^3 = a^2 + 3b^2$$

Assim,

$$a^2 + 3b^2 = (m^2 + 3n^2)^3 = m^6 + 9m^4n^2 + 27m^2n^4 + 27n^6.$$

Tome agora

$$\tilde{a} = m^3 - Amn^2 \ \text{ e } \ \tilde{b} = Bm^2n - 3n^3$$

Assim,

$$\tilde{a}^2 + 3\tilde{b}^2 = m^6 + (3B^2 - 2A)m^4n^2 + (A^2 - 18B)m^2n^4 + 27n^6$$

Daí,

$$\begin{cases} 3B^2 - 2A = 9, \\ A^2 - 18B = 27 \end{cases} \tag{2.11}$$

Assim temos que

$$\begin{aligned} A &= \frac{3B^2 - 9}{2} \\ &\Rightarrow \left(\frac{3B^2 - 9}{2}\right)^2 - 18B = 27 \\ &\Rightarrow B^4 - 6B^2 - 8B - 3 = 0 \end{aligned}$$

Vemos que $B = -1$ (após testar os valores clássicos $B = \pm 1$ e $B = 0$) é raiz do polinômio acima. Realizando a divisão polinomial obtemos

$$\frac{B^4 - 6B^2 - 8B - 3}{B + 1} = B^3 - B^2 - 5B - 3.$$

Vemos que, novamente -1 é raiz de $B^3 - B^2 - 5B - 3$. Assim,

$$\frac{B^3 - B^2 - 5B - 3}{B + 1} = B^2 - 2B - 3$$

Temos facilmente que $B^2 - 2B - 3 = (B - 3)(B - 1)$, assim

$$B^4 - 6B^2 - 8B - 3 = (B - 3)(B + 1)^3$$

Portanto, $B = 3$ ou $B = -1$, e respectivamente, temos $A = 9$ ou $A = -3$. Assim, as soluções do sistema (2.11) são : $A = 9$ e $B = 3$ ou $A = -3$ e $B = -1$

Como temos, portanto, duas soluções possíveis, a saber,

$$\begin{cases} \tilde{\tilde{a}} = m^3 + 3mn^2, \\ \tilde{\tilde{b}} = -m^2n - 3n^3 \end{cases}$$

e

$$\begin{cases} \tilde{a} = m^3 - 9mn^2, \\ \tilde{b} = 3m^2n - 3n^3 \end{cases}$$

Em resumo, mostramos que se s é primo e $a^2 + 3b^2 = s^3$, com $mdc(a, 3b) = 1$ e $a + b \equiv 1 \ mod \ 2$, então:

i) $s > 3,\ a \nmid s,\ b \nmid s$

ii) Existem $\tilde{a}$ e $\tilde{b} \in \mathbb{Z}$ tais que $\tilde{a}^2 + 3\tilde{b}^2 = s^3$ e $\tilde{a} = m^3 - 9mn^2$ e $\tilde{b} = 3m^2n - 3n^3,\ m, n \in \mathbb{Z}$, onde $mdc(m, 3n) = 1$ e $m + n \equiv 1 \ mod\ 2$.

Vamos mostrar agora que a afirmação anterior continua valendo mesmo no caso em que s não é primo. Assim vamos mostrar que:

Proposição 2.2. : Se $a^2 + 3b^2 = s^3$, com $mdc(a, 3b) = 1$ e $a + b \equiv 1 \ mod\ 2$, então, existe uma solução $s = m^2 + 3n^2,\ \tilde{a} = m^3 + 9mn^2$ e $\tilde{b} = 3m^2n - 3n^3$, com $m, n \in \mathbb{Z}$, $mdc(m, 3n) = 1$ e $m + n \equiv 1 \ mod\ 2$, onde s é natural não necessariamente primo, e $\tilde{a}^2 + 3\tilde{b}^2 = s^3$.

Demonstração: A prova será por indução no número de fatores primos de s. Comece observando que provamos (a partir da fórmula 3) a seguinte afirmação.
Afirmação 6: Se s é primo e $a^2 + 3b^2 \equiv 0 \mod s$, então existem $c, d \in \mathbb{Z}$, tais que $s^3 = c^2 + 3d^2$, com $s = m_1^2 + 3n_1^2,\ c = m_1^3 - 9m_1n_1^2,\ d = 3m_1^2n_1 - 3n_1^3$, onde $m_1, n_1 \in \mathbb{Z}$, $mdc(m_1, 3n_1) = 1,\ m_1 + n_1 \equiv 1 \ mod\ 2$.

Voltemos agora ao caso em que s é natural não-necessariamente primo. Faremos a indução no número de fatores primos de s. Chamemos o número de fatores primos de s de l.

Se $l = 0$, então $s = 1$, temos $m = \pm 1,\ n = 0$. Segue que $mdc(m, 3n) = 1$ e $m + n \equiv 1 \ mod\ 2$. Isto prova a base da indução.
Suponha agora que o resultado é verdade para valores de s com l fatores primos. Assim, seja $s \in \mathbb{N}$ com $l + 1$ fatores primos e seja $p \in \mathbb{N}$ um fator primo de s. Então $s = p \cdot t,\ t \in \mathbb{N},\ t$ possuindo l fatores primos. Note que t pode ser divisível por p.

Como $p \mid s$ e $a^2 + 3b^2 = s^3$,temos que

$$a^2 + 3b^2 \equiv 0 \ mod\ p$$

Pela Afirmação 6 segue que existem $c, d \in \mathbb{Z}$ tais que

$$p^3 = c^2 + 3d^2 \tag{2.12}$$

com $p = m_1^2 + 3n_1^2,\ c = m_1^3 - 9m_1n_1^2,\ d = 3m_1^2n_1 - 3n_1^3,\ m_1, n_1 \in \mathbb{Z},\ mdc(m_1, 3n_1) = 1,\ m_1 + n_1 \equiv 1 \ mod\ 2$.
Desta forma, por um lado, $p^3 \cdot s^3 = (t \cdot p)^3 \cdot p^3 = t^3p^6$. Por outro lado, $p^3 \cdot s^3 = (c^2 + 3d^2)(a^2 + 3b^2)$.

Assim,

$$\begin{aligned} t^3p^6 &= (c^2 + 3d^2)(a^2 + 3b^2) \\ &= (ac + 3bd)^2 + 3(ad - bc)^2 \\ &= (ac - 3bd)^2 + 3(ad + bc)^2. \end{aligned}$$

além disso,

$$\begin{aligned} (ad - bc)(ad + bc) &= a^2d^2 - b^2c^2 \\ &= a^2d^2 + 3b^2d^2 - 3b^2d^2 - b^2c^2 \\ &= d^2(a^2 + 3b^2) - b^2(c^2 + 3d^2) \\ &= d^2s^3 - b^2p^3 \\ &= d^2t^3p^3 - b^2p^3 \\ &= p^3(d^2t^3 - b^2) \end{aligned} \tag{2.13}$$

Juntando a Afirmação 6 com a Afirmação 4, podemos concluir que $p > 3$, em particular p é primo.
Se $p \mid ad + bc$ e $p \mid ad - bc$, então $p \mid (ad + bc) + (ad - bc) \Rightarrow p \mid 2ad$. Como p é ímpar, temos que $p \mid ad$. Analogamente $p \mid (ad + bc) - (ad - bc) \Rightarrow p \mid 2bc$, e como p é ímpar, então $p \mid bc$. Logo $p \mid ad$ e $p \mid bc$.
Porém, $p^3 = c^2+3d^2$. Daí, se $p \mid d$, então $p \mid p^3-3d^2 \Rightarrow p \mid c^2 \Rightarrow p \mid c \Rightarrow p \mid mdc(c, d)$. Como $mdc(c, d) = mdc(c, 3d) = 1$, temos que $p = 1$, absurdo!. Portanto $p \nmid d$. O mesmo argumento mostra que $p \nmid c$.
Como $p \mid ad$ e $p \mid bc$, temos que $p \nmid d \Rightarrow p \mid a$ e $p \nmid c \Rightarrow p \mid b$, porém, $mdc(a, b) = mdc(a, 3b) = 1$. Daí, $p = 1$, absurdo!
Assim não podemos ter $p \mid ad + bc$ e $p \mid ad - bc$

Como por ((2.13)) $p^3 \mid p^3(t^3d^2 - b^2) \Rightarrow p^3 \mid (ad + bc)(ad - bc)$, segue daqui que, ou $p^3 \mid ad + bc$ ou $p^3 \mid ad - bc$. Vamos supor que $p^3 \mid ad - bc$ e $p \nmid ad + bc$, (o outro caso se resolve analogamente). (Relembre que mostramos que se $p \mid ad - bc$, então $p \nmid ad + bc$ e vice-versa).

Como temos que

$$t^3p^6 = (ac + 3bd)^2 + 3(ad - bc)^2 \tag{2.14}$$

e $p^3 \mid ad - bc$, segue $p^6 \mid (ad - bc)^2$ e $p^6 \mid (ac + 3bd)^2 \Rightarrow p^3 \mid ac + 3bd$
Portanto,

$$\frac{ad - bc}{p^3} \in \mathbb{Z} \text{ e } \frac{ac + 3bd}{p^3} \in \mathbb{Z},$$

daí sejam

$$e = \frac{ad - bc}{p^3} \text{ e } f = \frac{ac + 3bd}{p^3} \tag{2.15}$$

com $e, f \in \mathbb{Z}$. Note que 2.14 pode ser reescrita como

$$t^3\left(\frac{ac + 3bd}{p^3}\right) + 3\left(\frac{ad - bc}{p^3}\right)^2 \Rightarrow t^3 = f^2 + 3e^2.$$

Temos ainda que $p^3 = c^2 + 3d^2$, daí 2.15 nos dá

$$\begin{cases} ad - bc & = ep^3 \Rightarrow a = \frac{ep^3 + bc}{d} \\ ac + 3bd & = fp^3 \Rightarrow fp^3 = \frac{ep^3c + bc^2 + 3bd^2}{d} \\ \Rightarrow fp^3d & = ep^3c + b(c^2 + 3d^2) \Rightarrow fdp^3 = ecp^3 + bp^3 \end{cases}$$

daí temos que

$$b = fd - ec \tag{2.16}$$

substituindo o valor de b chegamos em

$$a = cf + 3de \tag{2.17}$$

Logo,

$$t^3 = f^2 + 3e^2$$

com $a = cf + 3de$, $b = fd - ec$. Como sabemos que $mdc(a, 3b) = 1$, se $d = mdc(e, f)$ segue que $d \mid a$ e $d \mid b \Rightarrow d \mid mdc(a, b) \Rightarrow d = 1$. Daí, $mdc(e, f) = 1$. Além disso, se $3 \mid f$, então $3 \mid cf + 3de \Rightarrow 3 \mid a$. Porém, $mdc(a, 3b) = 1$, daí $3 \nmid a$. Portanto $3 \nmid f$ e segue que $mdc(f, 3e) = 1$. Por fim, como $a + b \equiv 1 \ mod \ b$, segue que

$$\begin{aligned} & s^3 \equiv a^2 + 3b^2 \ mod \ 2 \\ \Rightarrow\ & s^3 \equiv a^2 + b^2 \ mod \ 2 \\ \Rightarrow\ & s^3 \equiv a + b \ mod \ 2 \\ \Rightarrow\ & s^3 \equiv 1 \ mod \ 2 \\ \Rightarrow\ & s \equiv 1 \ mod \ 2. \end{aligned}$$

Como $s = p \cdot t$, segue que $t \equiv 1 \ mod \ 2$. Daí, $t^3 \equiv 1 \ mod \ 2 \Rightarrow f^2 + 3e^2 \equiv 1 \ mod \ 2 \Rightarrow f + e \equiv 1 \ mod \ 2$.

Em resumo temos que

$$t^3 = f^2 + 3e^2$$

onde $mdc(f, 3e) = 1$ e $f + e \equiv 1 \ mod \ 2$. Como t possui l fatores primos, segue da hipótese de indução que $\exists m_2, \ n_2 \in \mathbb{Z}$ tais que $mdc(m_2, 3n_2) = 1$, $m_2 + n_2 \equiv 1 \ mod \ 2$,

$$t = m_2^2 + 3n_2^2, \ \text{com} \ f = m_2^3 - 9m_2n_2^2 \ \text{e} \ e = 3m_2^2n_2 - 3n_2^3.$$

Relembre a definição de $m_1, \ n_1 \in \mathbb{Z}$ definidos abaixo da equação . Defina

$$m = m_1m_2 + 3n_1n_2 \ \text{e} \ n = m_2n_1 - n_2m_1$$

Afirmação 7: Temos que $mdc(m, 3n) = 1, \ m + n \equiv 1 \ mod \ 2, \ s = m^2 + 3n^2, \ a = m^2 - 9mn^2$ e $b = 3m^2n - 3n^3$.

Inicialmente , temos que :

$$p = m_1^2 + 3n_1^2 \ \text{e} \ t = m_2^2 + 3n_2^2$$

Daí,

$$\begin{aligned} s = t \cdot p &= (m_2^2 + 3n_2^2)(m_1^2 + 3n_1^2) \\ &= m_1^2m_2^2 + 3m_2^2n_1^2 + 3n_2^2m_1^2 + 9n_1^2n_2^2 \\ &= m_1^2m_2^2 + 6m_1m_2n_1n_2 + 9n_1^2n_2^2 + 3m_2^2n_1^2 - 6m_1m_2n_1n_2 + 3n_2^2m_1^2 \\ &= (m_1m_2 + 3n_1n_2)^2 + 3(m_2n_1 - n_2m_1)^2 \\ &= m^2 + 3n^2 \\ \Rightarrow s &= m^2 + 3n^2 \end{aligned}$$

Além disso, pelas fórmulas (2.16) e (2.17), temos

$$a = cf + 3de \ \text{e} \ b = fd - ec.$$

Daí, dela definição de m_1 e n_1

$$c = (m_1^3 - 9m_1n_1^2) \ \text{e} \ d = 3m_1^2n_1 - 3n_1^3$$

e pela definição de m_2 e n_2

$$f = m_2^3 - 9m_2n_2^2 \ \text{e} \ e = 3m_2^2n_2 - 3n_2^3$$

Portanto,

$$\begin{aligned} a &= (m_1^3 - 9m_1n_1^2)(m_2^3 - 9m_2n_2^2) + 3(3m_1^2n_1 - 3n_1^3) + 3(3m_2^2n_2 - 3n_2^3) \\ &= m_1^3m_2^3 - 9m_1^3n_1^2n_2^2 - 9m_1m_2^3n_1^2 + 81m_1m_2n_1^2n_2^2 + 27m_1^2m_2^2n_1n_2 - \\ &\quad 27m_1^2n_1n_2^3 - 27m_2^2n_2n_1^3 + 27n_1^3n_2^3 \\ &= m_1^3m_2^3 + 9m_1^2m_2^2n_1n_2 + 27m_1m_2n_1^2n_2^2 + 27n_1^3n_2^3 + 54m_1m_2n_1^2n_2^2 + \\ &\quad 18m_1^2m_2^2n_1n_2 - 9m_1^3m_2^2n_2^2 - 27m_1^2n_1n_2^3 - 9m_2^3m_1n_1^2 - 27m_2^2n_1^3n_2 \\ &= (m_1m_2 + 3n_1n_2)^3 - 9(m_1m_2 + 3n_1n_2)(m_2n_1 - m_1n_2)^2 \\ &= m^3 - 9mn^2 \\ \Rightarrow a &= m^3 - 9mn^2 \end{aligned}$$

Temos que $b = 3m^2n - 3n^3$. Sabemos que como $a + b \equiv 1 \ mod \ 2$, então

$$\begin{aligned} s^3 &\equiv a^2 + 3b^2 \ mod \ 2 \\ &\equiv a^2 + b^2 \ mod \ 2 \\ &\equiv a + b \ mod \ 2 \\ &\equiv 1 \ mod \ 2 \\ s^3 &\equiv 1 \ mod \ 2 \\ \Rightarrow s &\equiv 1 \ mod \ 2 \end{aligned}$$

Daí,

$$\begin{aligned} 1 &\equiv m^2 + 3n^2 \ mod \ 2 \\ \Rightarrow 1 &\equiv m^2 + 3n^2 \ mod \ 2 \\ \Rightarrow 1 &\equiv m^2 + n^2 \ mod \ 2 \\ \Rightarrow 1 &\equiv m + n \ mod \ 2. \end{aligned}$$

ou seja, $m + n \equiv 1 \ mod \ 2$. Por fim, como $mdc(a, b) = 1$, pois, $mdc(a, 3b) = 1$ e $a = m^3 - 9mn^2$, $b = 3m^2n - 3n^3$, temos que $d = mdc(m, n)$ é tal que $d \mid a$ e $d \mid b \Rightarrow d \mid mdc(a, b) \Rightarrow d = 1 \Rightarrow mdc(m, n) = 1$.
Além disso $3 \mid m$, então

$$\begin{aligned} a &\equiv m^3 - 9mn^2 \ mod \ 3 \\ \Rightarrow a &\equiv 0 \ mod \ 3 \\ \Rightarrow 3 &\mid a. \end{aligned}$$

Porém, mdc $(a, 3b) = 1 \Rightarrow 3 \nmid a$. Esta contradição mostra que $3 \nmid m$. Portanto $mdc(m, 3n) = 1$
Em resumo, temos que

$s = m^2 + 3n^2$, $m + n \equiv 1 \ mod \ 2$, $mdc(m, 3n) = 1$, $a = m^3 - 9mn^2$ e $b = 3m^2n - 3n^3$.

Isto prova o passo da indução e conclui a prova da proposição.

Vamos agora completar a demonstração do teorema de Fermat para $n = 3$. Vamos primeiro provar para o (caso 1). Relembre que no caso 1 temos: $x + y = 2u$, $x - y = 2w$, daí, $x = u + w$, $y = u - w$. Além disso, $z^3 = 2u(u^2 + 3w^2)$ e existem $r, s \in \mathbb{Z}$, $s > 0$, tal que $2u = r^3$ e $u^2 + 3w^2 = s^3$.

Segue da proposição que a equação $u^2 + 3w^2 = s^3$ tem uma solução tal que $u = m^3 - 9mn^2$, para, $m, n \in \mathbb{Z}$ com $mdc(m, 3n) = 1$, daí, $mdc(m, n) = 1$ e $m+n \equiv 1 \ mod \ 2$.

Portanto,

$$\begin{aligned} r^3 &= 2u \\ &= 2(m^3 - 9mn^2) \\ &= 2m(m^2 - 9n^2) \\ &= 2m(m-3n)(m+3n) \\ \Rightarrow r^3 &= 2m(m-3n)(m+3n). \end{aligned}$$

Como $m + n \equiv 1 \ mod \ 2 \Rightarrow m - 3n \equiv 1 \ mod \ 2$ e $m + 3n \equiv 1 \ mod \ 2 \Rightarrow 2 \nmid m - 3n$ e $2 \nmid m + 3n$

Além disso, como $mdc(m, n) = 1$, segue que $mdc(m, m - 3n) = 1$ e $mdc(m, m + 3n) = 1$. Logo, $mdc(2m, m - 3n) = 1$ e $mdc(2m, m + 3n) = 1$. Por fim, seja $d = mdc(m - 3n, m + 3n)$, então $d \mid 2m$. Como $m - 3n$ e $m + 3n$ são ímpares então $2 \nmid d \Rightarrow d \mid m$. Como $mdc(m, 3n) = 1 \Rightarrow 3 \nmid m \Rightarrow 3 \nmid d \Rightarrow mdc(3, d) = 1$. Como $d \mid m - 3n$ e $d \mid m + 3n$, temos que $d \mid 6n$. Como $mdc(2, d) = mdc(3, d) = 1$, segue que $d \mid n$. Daí, $d \mid mdc(m, n) \Rightarrow d \mid 1 \Rightarrow d = 1$. Assim, $mdc(2m, m + 3) = mdc(2m, m - 3n) = mdc(m - 3n, m + 3n) = 1$.

Como $r^3 = 2m(m - 3n)(m + 3n)$, segue que existem $\alpha, \beta, \delta \in \mathbb{Z}$ tais que $2m = \alpha^3$, $m - 3n = \beta^3$ e $m + 3n = \delta^3$.
Logo, $\alpha^3 = 2m = m - 3n + m + 3n = \beta^3 + \delta^3 \Rightarrow \alpha^3 = \beta^3 + \delta^3$. Além disso, segue que

$$\begin{aligned} \mid r \mid^3 &= \mid 2m \mid\mid m + 3n \mid\mid m - 3n \mid \\ &= \mid \alpha \mid^3 \mid \beta \mid^3 \mid \delta \mid^3 \\ \Rightarrow \mid \alpha\beta\delta \mid^3 &= \mid r \mid^3 \end{aligned}$$

temos também que $r^3 = 2u$ e $2u = x + y$, logo

$$\begin{aligned} \mid \alpha\beta\delta \mid^3 &= \mid r \mid^3 = \mid 2u \mid = \mid x + y \mid \\ \Rightarrow \mid \alpha\beta\delta \mid^3 &= \mid x + y \mid \leq \mid xyz \mid < \mid xyz \mid^3, \end{aligned}$$

Observe que como $z > 2$, a desigualdade $\mid x + y \mid \leq \mid xyz \mid$ segue do argumento abaixo:

$$\mid zxy \mid > \mid 2xy \mid = \mid xy \mid + \mid xy \mid \geq \mid x \mid + \mid y \mid \geq \mid x + y \mid$$

Assim,

$$\mid \alpha\beta\delta \mid < \mid xyz \mid,$$

o que contradiz a minimalidade de $| xyz |$. Absurdo! O Absurdo foi supor que existe a solução não-trivial da equação de Fermat com $n = 3$ e que u não é divisível por 3. Vamos mostrar que também não pode ocorrer o (caso 2).
Vamos relembrar agora o caso 2. Temos que $x + y = 2u$, $x - y = 2w$, $u = 3v$, daí $x + y = 6v$. Além disso temos que $z^3 = 18v(3v^2 + w^2)$ e existem $r, s \in \mathbb{Z}$ tais que $18v = r^3$ e $3v^2 + w^2 = s^3$.
Pela Proposição (2.2) segue que a equação $3v^2 + w^2 = s^3$ tem uma solução tal que $v = 3m^2n - 3n^3$, com $mdc(m, n) = 1$ e $m + n \equiv 1 \ mod 2$. Desta forma,

$$\begin{aligned} r^3 &= 18v = 18(3m^2n - 3n^3) \\ &= 18n(3m^2 - 3n^2)Q \\ &= 3^3.2n(m^2 - n^2) \\ &= 3^3.(2n)(m - n)(m + n) \end{aligned}$$

Como $mdc(m - n) = 1$ e $m + n \equiv 1 \ mod \ 2$, segue que $m - n \equiv 1 \ mod \ 2$ e $m + n \equiv 1 \ mod \ 2 \Rightarrow mdc(2, m - n) = mdc(2, m + n) = 1$. Além disso, $mdc(n, m + n) = mdc(n, m) = 1, mdc(n, m - n) = mdc(n, m) = 1$. Daí

$$mdc(2n, m - n) = mdc(2n, m + n) = 1.$$

Por fim, se $d = mdc(m - n, m + n)$, temos que $d \mid 2m$ e $d \mid 2n$, Como $2 \nmid m - n$ e $2 \nmid m + n$, segue que $d \mid m$ e $d \mid n \Rightarrow d \mid mdc(m, n) = 1 \Rightarrow d = 1$.
Assim,

$$mdc(2n, m + n) = mdc(2n, m - n) = mdc(m - n, m + n) = 1.$$

Como $r^3 = 3^3 \cdot (2n)(m - n)(m + n)$, segue que existem $\alpha, \beta, \delta \in \mathbb{Z}$ tais que

$$2n = \alpha^3, m - n = \beta^3 \ \text{ e } \ m + n = \delta^3.$$

Daí

$$\begin{aligned} \delta^3 = m + n = m - n + 2n = \beta^3 + \alpha^3 \\ \Rightarrow \delta^3 = \beta^3 + \alpha^3. \end{aligned}$$

Porém,

$$\begin{aligned} | \alpha\beta\delta |^3 =& | 2n || m + n || m - n | = \frac{| r^3 |}{3^3} \\ &= \frac{| 18v |}{3^3} = \frac{2}{3} | v | = \frac{2}{3} \cdot \frac{| u |}{| 3 |} = \frac{2}{9} | u | \\ &\Rightarrow | \alpha\beta\delta |^3 = \frac{| 2u |}{9} = \frac{| x + y |}{9} \neq 0. \end{aligned}$$

Além disso,

$$\begin{aligned} \mid \alpha\beta\delta \mid^3 &= \frac{1}{9} \mid x + y \mid \leq \frac{\mid x \mid + \mid y \mid}{9} \leq \frac{\mid xy \mid + \mid xy \mid}{9} \\ &= \frac{\mid 2xy \mid}{9} \leq \frac{\mid xyz \mid}{9} < \mid xyz \mid \leq \mid xyz \mid^3 \\ &\Rightarrow \mid \alpha\beta\delta \mid < \mid xyz \mid \end{aligned}$$

Isso contradiz a minimalidade de $\mid xyz \mid$. A contradição ocorreu em supor que a equação de Fermat com $n = 3$ admitia solução não-trivial e que u era divisível por 3. Isto mostra que a solução também não existe nesse caso.

Portanto, juntando os dois casos, temos que a equação de Fermat com $n = 3$ não admite solução não-trivial.
Isto concluí a demonstração.

■

Capítulo 3

Demonstração para equação $x^4 + y^4 = z^4$

Nesse capítulo iremos apresentar uma prova elementar para a equação $x^4 + y^4 = z^4$, isto é, uma demonstração para equação de Fermat $x^n + y^n = z^n$ para $n = 4$, onde será apresentado que não existem soluções inteiras não-triviais para esta equação.

3.1 Caso $n = 4$, $x^4 + y^4 = z^4$

Vamos demonstrar agora que a equação

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

não possui soluções inteiras.

A afirmação acima decorre facilmente do seguinte Teorema:

Teorema 3.1. *A equação*

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

não possui soluções inteiras.

Demonstração Suponha, por absurdo que existem soluções não-triviais. Defina :

$W = \{w \in \mathbb{N}, w > 0 \text{ e existem } x, y \in \mathbb{Z} \text{ tais que } x^4 + y^4 = w^2\}$

Por hipótese (de que existem soluções não-triviais) $W \neq \varnothing$ e pelo princípio da

boa ordenação dos naturais, W possui um menor elemento, digamos $\hat{w}$

Assim, tome $x, y \in \mathbb{Z}$ tais que

$$x^4 + y^4 = \hat{w}^2.$$

Temos que x é ímpar ou y é ímpar. De fato, se x e y são pares, existem $\tilde{x}$ e $\tilde{y} \in \mathbb{Z}$ tais que

$$x = 2\tilde{x} \text{ e } y = 2\tilde{y}$$

Daí,

$$x^4 + y^4 = \hat{w}^2 \Rightarrow 2^4\tilde{x}^4 + 2^4\tilde{y}^4 = \hat{w}^2$$

Assim,

$$2^4 \mid \hat{w}^2 \Rightarrow 2^2 \mid \hat{w}$$

Logo existe, $\tilde{w} \in \mathbb{N}$ tal que $\hat{w} = 2^2\tilde{w}$.

Assim, dividindo a equação $2^4\tilde{x}^4 + 2^4\tilde{y}^4 = \hat{w}^2$ por 2^4 , obtemos

$$\tilde{x}^4 + \tilde{y}^4 = \tilde{w}^2$$

Daí, $\tilde{w} \in W$ e $\tilde{w} < \hat{w}$. Absurdo! Pois, $\hat{w}$ é o menor elemento de W. Logo, x é ímpar ou y é ímpar.

Suponha, sem perda de generalidade (renomeando as variáveis se necessário) que x é ímpar.
Assim, temos que

$$x^4 + y^4 = \hat{w}^2$$

onde $(x, y, \hat{w})$ são coprimos. De fato, seja $d = mdc(x, y, \hat{w})$, então, $x = d\tilde{x}, y = d\tilde{y}, \hat{w} = d\tilde{w}$, onde $\tilde{x}, \tilde{y} \in \mathbb{Z}$ e $\tilde{w} \in \mathbb{N}$. Assim,

$$x^4 + y^4 = \hat{w}^2 \Rightarrow d^4\tilde{x}^4 + d^4\tilde{y}^4 = d^2\tilde{w}^2 \Rightarrow d^2(\tilde{x}^4 + \tilde{y}^4) = \tilde{w}^2 \Rightarrow d^2 \mid \tilde{w}^2.$$

Assim, $\exists\tilde{\tilde{w}} \in \mathbb{N}$ tal que $\tilde{w}^2 = d^2\tilde{\tilde{w}}^2$ e assim $\tilde{x}^4 + \tilde{y}^4 = \tilde{\tilde{w}}^2$, logo $\tilde{\tilde{w}} \in W$.

Se $d > 1$, temos que $\tilde{\tilde{w}} < \hat{w}$, o que contradiz o fato de $\hat{w}$ ser o menor elemento de W. Logo $d = 1$.
Portanto,

$$mdc(x, y, \hat{w}) = 1 \Rightarrow mdc(x^2, y^2, \hat{w}) = 1$$

e

$$x^4 + y^4 = \hat{w}^2 \Rightarrow (x^2)^2 + (y^2)^2 = \hat{w}^2$$

Desta forma, $(x^2, y^2, \hat{w})$ é uma terna pitagórica. Portanto, existe $a, b \in \mathbb{N}$, com a e b coprimos, onde a é par e b é ímpar, ou a é ímpar e b é par, tais que, pelo teorema do caso $n = 2$,

$$x^2 = a^2 - b^2, \;\; y^2 = 2ab \;\text{ e }\; a^2 + b^2 = \hat{w} \tag{3.1}$$

Observe que a é ímpar e b é par. De fato, se a fosse par e b ímpar, teríamos, já que x é ímpar , que

$$1 \equiv x^2 \;\; mod \;\; 4 \equiv a^2 - b^2 \;\; mod \;\; 4 \equiv -1 \;\; mod \;\; 4$$

veja a demonstração do caso $n = 2$, para a justificativa que x ímpar $\Rightarrow x^2 \equiv 1 \;\; mod \;\; 4$. Assim, segue que

$$1 \equiv -1 \;\; mod \;\; 4$$

Absurdo! Logo, a é ímpar e b é par.
Temos então, que

$$a^2 = x^2 + b^2$$

com a e x ímpares e b par.

Afirmamos que $mdc(x, b, a) = 1$. De fato, seja $d = mdc(x, b, a) \Rightarrow d \mid a$ e $d \mid b$. Como a e b são coprimos, segue que $d = 1$.
Desta forma, temos que (x, b, a) é uma terna pitagórica. Daí, existem c e $d \in \mathbb{N}$, coprimos, com c ímpar e d par , ou c par e d ímpar, tais que, pelo teorema do caso $n = 2$.

$$x = c^2 - d^2, \;\; b = 2cd \;\text{ e }\; a = c^2 + d^2$$

Afirmamos agora que a é quadrado perfeito. De fato, seja p fator primo de a. Como a é ímpar então $p > 2$.

Seja $q \in \mathbb{N}$, tal que $p^q \mid a$ e $p^{q+1} \nmid a$.
Além disso, seja

$$\overline{q} = \begin{cases} q + 1, & \text{se } \; q \text{ é ímpar} \\ q, & \text{se } \; q \text{ é par} \end{cases}$$

Logo, por (3.1), temos que

$$y^2 = 2ab,$$

e como $p^q \mid a$, temos que

$$p^q \mid 2ab \Rightarrow p^q \mid y^2 \Rightarrow p^{\overline{q}} \mid y^2 \Rightarrow p^{\overline{q}} \mid 2ab$$

Como $p > 2$, segue que,

$$p^{\overline{q}} \mid ab$$

Como o $mdc(a, b) = 1$, temos que

$$p^{\overline{q}} \mid a$$

Daí, $\overline{q} = q \Rightarrow q$ é par. Portanto, a é quadrado perfeito. Assim, existe $t \in \mathbb{N}$ tal que $a = t^2$.
Além disso, b é par $\Rightarrow b = 2k$, onde $k \in \mathbb{N}$.

Seja p fator primo de k, com $p^q \mid k$, mas $p^{q+1} \nmid k$. Defina

$$\overline{q} = \begin{cases} q+1, & \text{se } q \text{ é ímpar} \\ q, & \text{se } q \text{ é par} \end{cases}$$

Se $p > 2$, temos que

$$p^q \mid k \Rightarrow p^q \mid 4ak \Rightarrow p^q \mid y^2 \Rightarrow p^{\overline{q}} \mid y^2 \Rightarrow p^{\overline{q}} \mid 4ak$$

Como a e k são coprimos, já que a e b são coprimos, segue que

$$p^{\overline{q}} \mid 4k$$

e como estamos supondo $p > 2$, temos que

$$p^{\overline{q}} \mid k \Rightarrow \overline{q} = q \Rightarrow q \text{ é par.}$$

Se $p = 2$, temos que $2^q \mid k \Rightarrow \exists k' \in \mathbb{N}$ tal que $k = 2^q k'$. Assim, $y^2 = 2^{q+2} ak'$. Daí

$$2^{2+q} \mid y^2 \Rightarrow 2^{2+\overline{q}} \mid y^2 \Rightarrow 2^{2+\overline{q}} \mid 2^{2+q} ak' \Rightarrow 2^{\overline{q}-q} \mid ak'.$$

Como a e k' são coprimos, já que a e b são coprimos , temos que

$$2^{\overline{q}-q} \mid k'.$$

Daí, $\bar{q} = q$, pois, $2 \nmid k'$. Logo q é par.

Portanto, k é quadrado perfeito, ou seja, $\exists g \in \mathbb{N}$, tal que $k = g^2 \Rightarrow b = 2g^2$.
Daí, como $b = 2cd$, temos que

$$g^2 = cd$$

Como c e d são coprimos, o mesmo argumento acima mostra que c e d são quadrados perfeitos, digamos

$$c = r^2 \text{ e } d = s^2$$

para r e $s \in \mathbb{N}$.

Logo, como

$$a = c^2 + d^2$$

segue que

$$t^2 = r^4 + s^4$$

Segue que $t \in W$. Porém,

$$t \leq t^4 = a^2 = \hat{w} - b^2 < \hat{w}$$

o que é absurdo, pois, w é o menor elemento de W.

■

Capítulo 4

Demonstração para equação $x^5 + y^5 = z^5$

Nesse capítulo iremos apresentar uma prova elementar para um caso particular da equação $x^5+y^5 = z^5$, isto é, uma demonstração para equação de Fermat $x^n+y^n = z^n$ para $n = 5$, onde será apresentado que se 5 não dividir nenhum dos x, y, z, então, não existem soluções inteiras não-triviais para esta equação.

4.1 Caso $n = 5,\ \ x^5 + y^5 = z^5$

Proposição 4.1. Se $p \in \mathbb{Z}$ é primo e ímpar e $a \in \mathbb{Z}$ é tal que $p \nmid a$, então

$$a^{\frac{p-1}{2}} \equiv \pm 1 \ \ mod \ \ p$$

Demonstração. Como $p \nmid a$ segue do pequeno teorema de Fermat que

$$a^{p-1} \equiv 1 \ \ mod \ \ p$$

Como p é primo ímpar, $p-1$ é par, daí $\frac{p-1}{2} \in \mathbb{Z}$. Logo,

$$\left(a^{\frac{p-1}{2}}\right)^2 \equiv 1 \ \ mod \ \ p \Rightarrow \left(a^{\frac{p-1}{2}} + 1\right)\left(a^{\frac{p-1}{2}} - 1\right) \equiv 0 \ \ mod \ \ p$$

Como p é primo, segue que

$$a^{\frac{p-1}{2}} \equiv 1 \ \ mod \ \ p \ \text{ ou } \ a^{\frac{p-1}{2}} \equiv -1 \ \ mod \ \ p$$

□

Faremos um caso particular simples para o caso $n = 5$. De fato, provaremos que se

$$x, y \text{ e } z \in \mathbb{Z} \text{ e } 5 \nmid x, 5 \nmid y, 5 \nmid z$$

então

$$z^5 \neq x^5 + y^5$$

A afirmação acima sai como consequência simples do seguinte Teorema.

Teorema 4.2. *Sejam x, y e $z \in \mathbb{Z}$ com $5 \nmid x, 5 \nmid y, 5 \nmid z$, então*

$$x^5 + y^5 + z^5 \neq 0$$

Demonstração: Sejam x, y e $z \in \mathbb{Z}$ com $5 \nmid x, 5 \nmid y, 5 \nmid z$

Suponha por absurdo que

$$x^5 + y^5 + z^5 = 0$$

Após fatorar, se necessário, podemos supor sem perda de generalidade que $mdc(x, y, z) = 1$

Temos que

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

Afirmamos que

$$mdc(x + y, x^4 - x^3y + x^2y^2 - xy^3 + y^4) = 1$$

Seja $d = mdc(x + y, x^4 - x^3y + x^2y^2 - xy^3 + y^4)$
Temos que como

$$d \mid x + y \text{ e } d \mid x^4 - x^3y + x^2y^2 - xy^3 + y^4$$

então,

$$d \mid x^4 - x^3y + x^2y^2 - xy^3 + y^4 - (x^3 - 2x^2y + 3xy^2 - 4y^3)(x + y) \Rightarrow d \mid 5y^4$$

Suponha por absurdo, que $d \neq 1$ e seja, p um fator primo de d, daí

$$p \mid 5y^4 \tag{4.1}$$

Se $p = 5$, então

$$5 \mid (x+y)(x^4 - x^3y + x^2y^2 - xy^3 + y^4) \Rightarrow 5 \mid x^5 + y^5 \Rightarrow 5 \mid -z^5 \Rightarrow 5 \mid z$$

Absurdo! Pois, $5 \nmid$ z.

Assim, $p \neq 5$. Como $p \mid 5y^4$, segue que

$$p \mid y^4 \Rightarrow p \mid y$$

Como $p \mid x + y$ e $p \mid y \Rightarrow p \mid x$. Além disso,

$$p \mid x^5 + y^5 = z^5 \Rightarrow p \mid z$$

Assim, $p \mid x$, $p \mid y$ e $p \mid z$. Absurdo! Pois $mdc(x, y, z) = 1$

Portanto,

$$mdc(x + y, x^4 - x^3y + x^2y^2 - xy^3 + y^4) = 1$$

Desta forma, como

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

e

$$mdc(x + y, x^4 - x^3y + x^2y^2 - xy^3 + y^4) = 1$$

segue que existem $A, T \in \mathbb{Z}$ tais que

$$x + y = A^5$$

e

$$x^4 - x^3y + x^2y^2 - xy^3 + y^4 = T^5$$

Trocando os papéis de x, y e z no argumento anterior, podemos concluir que existem B e $C \in \mathbb{Z}$ tais que

$$x + z = B^5$$

e

$$y + z = C^5$$

Suponha agora, por absurdo, que $11 \nmid x$, $11 \nmid y$ e $11 \nmid z$. Segue então da Proposição (4.1) que

$$x^5 \equiv \pm 1 \ mod \ 11, z^5 \equiv \pm 1 \ mod \ 11, z^5 \equiv \pm 1 \ mod \ 11 \Rightarrow x^5 + y^5 + z^5 \not\equiv 0 \ mod \ 11$$

Absurdo, pois, por hipótese $x^5+y^5+z^5 = 0$. Logo, algum dos x, y, z é múltiplo de 11.

Suponha, sem perda de generalidade(pois podemos renomear as variáveis se necessário) que $11 \mid z$.
Desta forma, como

$$-A^5 + B^5 + C^5 = -x - y + x + z + y + z = 2z$$

temos que

$$-A^5 + B^5 + C^5 \equiv 0 \ mod \ 11$$

Suponha, por absurdo, que $11 \nmid A$, $11 \nmid B$ $11 \nmid C$. Então, pela Proposição (4.1), temos que

$$A^5 \equiv \pm 1 \ mod \ 11, B^5 \equiv \pm 1 \ mod \ 11 \text{ e } C^5 \equiv \pm 1 \ mod \ 11$$

Logo,

$$-A^5 + B^5 + C^5 \not\equiv 0 \ mod \ 11$$

Absurdo! Portanto,

$$11 \mid A \text{ ou } 11 \mid B \text{ ou } 11 \mid C.$$

Se $11 \mid B$, como $x + z = B^5$ e $11 \mid z$, segue que $11 \mid x$. Como

$$x^5 + y^5 + z^5 = 0$$

segue que $11 \mid y \Rightarrow 11 \mid mdc(x, y, z)$. Absurdo! Logo $11 \nmid B$.

Analogamente , temos que $11 \nmid C$. Portanto $11 \mid A$.

Como $A^5 = x + y$, temos que

$$x \equiv -y \ mod \ 11 \tag{4.2}$$

daí, como

$$x^4 - x^3y + x^2y^2 - xy^3 + y^4 = T^5$$

segue que

$$x^4 - x^3y + x^2y^2 - xy^3 + y^4 = T^5 \equiv 5y^4 \ \ mod \ 11$$

Portanto,

$$T^5 \equiv 5y^4 \ \ mod \ 11$$

Por outro lado, como

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

segue que

$$y \equiv C^5 \ \ mod \ 11$$

Como $11 \nmid C$, segue da proposição (4.1) que

$$C^5 \equiv \pm 1 \ \ mod \ 11 \Rightarrow y \equiv \pm 1 \ \ mod \ 11$$

Portanto,

$$T^5 \equiv 5 \ \ mod \ 11 \Rightarrow 11 \nmid T.$$

Pela proposição 4.1 , como $11 \nmid T$, temos que

$$T^5 \equiv \pm 1 \ \ mod \ 11$$

Absurdo! Esta contradição conclui a demonstração.

■

Referências Bibliográficas

[1] SINGH, Simon, *Fermat's Enigma: The Epic Quest to Solve the World's Greatest Mathematical*. New York: Anchor Books, (1997).

[2] JOMOON, Jomin, *Book Book Book Mathematical*. New York: Anchor Books, 2008.

[3] RIBENBOIM, Paulo, *13 lectures on Fermat's last theorem*. New York: Springer-Verlag, 1979.

[4] LIU, Andy, *Another Do-It-Yourself Proof of the $n = 3$ case of Fermat's Last Theorem*. Alberta: Edmonton, 2000, p. 422-425.