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 $n = 5$

Samuel de Oliveira Cardoso

RIO DE JANEIRO
2020

Samuel de Oliveira Cardoso

O Último Teorema de Fermat para $n = 5$

Dissertação apresentada ao Programa de Pós-graduação em Matemática PROFMAT da UNIRIO, como pré-requisito para a obtenção do grau de MESTRE em Matemática.

Orientador: Silas Fantin

Doutor em Matemática – USP

Rio de Janeiro

2020

Catalogação informatizada pelo autor

C266 Cardoso, Samuel de Oliveira

O Último Teorema de Fermat para $n = 5$ / Samuel de Oliveira Cardoso. -- Rio de Janeiro, 2020. 121 f.

Orientador: Silas Fantin.

Dissertação (Mestrado) - Universidade Federal do Estado do Rio de Janeiro, Programa de Pós-Graduação em Matemática, 2020.

1. Último Teorema de Fermat. 2. Divisibilidade.
3. Congruências. 4. Estruturas Algébricas.
I. Fantin, Silas, orient. II. Título.

Samuel de Oliveira Cardoso

O Último Teorema de Fermat para $n = 5$

Dissertação apresentada ao Programa de Pós-graduação em Matemática PROFMAT da UNIRIO, como requisito para a obtenção do grau de MESTRE em Matemática.

Aprovada em 12 de Fevereiro de 2020.

BANCA EXAMINADORA

Prof. Dr. Silas Fantin – Orientador
UNIRIO

Profª Drª Cristiane de Mello
UNIRIO

Profª Drª Andrea Gomes Guimarães
UFF

Rio de Janeiro

2020

Dedico este trabalho às minhas queridas esposa Aline e mãe Moema e, in memoriam, aos meus amados avô e pai: João Norberto e Rivaldo Cardoso, importantes alicerces na minha trajetória.

AGRADECIMENTOS

À minha família e a Deus por estarem sempre ao meu lado e por serem fontes constantes de inspiração e de sabedoria.

Da minha família, destaco as minhas queridas esposa Aline e mãe Moema e ainda os amados da família Dantas Cardoso, que estão em um outro plano, mas que, de algum modo, sempre estarão comigo: os meus avós João e Flora, o meu pai Rivaldo e os meus tios Floriano, Diva e Levy.

Agradeço também (*in memoriam*) aos meus sogros, Eldes e Neli, pelo carinho que dedicaram à minha esposa; e aos meus avós maternos, Laudelino e Else, pelas doces lembranças de minha mãe. Ao tio Paulo, pois não poderia esquecer das nossas longas conversas sobre matemática, história e filosofia.

Aos Professores do PROFMAT (UNIRIO) pelas aulas ministradas e pelas orientações e contribuições acadêmicas e profissionais.

Aos meus colegas e amigos do PROFMAT (UNIRIO) – Turma 2017 pela união de todos, pelo constante aprendizado em nossos debates e também pela oportunidade de conhecer excelentes profissionais do ensino de matemática no Rio de Janeiro.

Ao meu orientador, professor Silas Fantin, pela confiança, em mim depositada, para escrever sobre este interessante e cativante tema, pelo seu modo paciente, meticuloso e colaborativo de orientar, pela sua amizade e pelos incentivos finais à conclusão deste trabalho.

Às professoras Andrea e Cristiane, integrantes da Banca Examinadora, por suas importantes contribuições ao texto final desta Dissertação.

RESUMO

Este trabalho acadêmico estrutura-se para tornar acessível o conhecimento de ideias gerais sobre o **Último Teorema de Fermat (UTF)**, apresentando-se alguns dos seus elementos algébricos e históricos. Desenvolve-se, de forma central, uma demonstração para o caso $n = 5$ da equação do UTF. No trabalho, detalham-se ainda: curiosidades, exemplos e atividades resolvidas.

Palavras-chaves: Fermat. Teorema. Álgebra. Aritmética. Divisibilidade. Congruências.

ABSTRACT

This academic work is structured to make accessible the knowledge of general ideas about **Fermat's Last Theorem (FLT)**, showing some of its algebraic and historical elements. Centrally, a demonstration for case $n = 5$ of the FLT equation is presented. In the work, are also detailed: curiosities, examples and activities solved.

Keywords: Fermat. Theorem. Algebra. Arithmetic. Divisibility. Congruences.

SUMÁRIO

INTRODUÇÃO

A conjectura de Fermat foi motivada pela observação da infinidade de soluções que apresenta uma *equação pitagórica*, ou seja, uma equação da forma $\mathbf{X^2 + Y^2 = Z^2}$.

Na equação anterior, tem-se que (X, Y, Z) denota uma *terna pitagórica*. Estas ternas tem, claramente, respaldo na Geometria Plana com a utilização de uma simples relação entre áreas de quadrados, que pode ainda ser verificada com o *Teorema de Pitágoras*.

Após esta motivação inicial, em uma etapa de aprofundamento, estudou-se a existência ou não das soluções inteiras não nulas para as "**Equações Fermatianas**", ou seja, para as equações da forma:

$$\mathbf{X^n + Y^n = Z^n \ \ com \ \ n > 2}$$

Conjecturou-se, assim, que, em tais equações, não existiam soluções inteiras não nulas. Após a conjectura, a demonstração final, contudo, só seria obtida cerca de três séculos e meio mais tarde.

Estudando-se, particularmente, o caso $n = 3$, pode-se, por exemplo, intuir alguma relação entre as variáveis com a Geometria Espacial. Neste sentido, poderíamos colocar a seguinte questão: "A soma dos volumes de dois cubos seria igual ao volume de um outro cubo qualquer?" Certamente não, pois, se isso acontecesse, teríamos um contraexemplo do **Último Teorema de Fermat (UTF)**, invalidando a conjectura proposta.

Como ponto de partida, os matemáticos concentraram esforços nas provas dos casos particulares para, assim, obter-se uma *prova geral*, isto é, uma prova com validade para $n > 2$.

Demonstraram-se, inicialmente, as seguintes equações, *casos particulares do* UTF*:*

- ✓ *Fermatiana Cúbica* $(n = 3)$: $X^3 + Y^3 = Z^3$;
- ✓ *Fermatiana Biquadrática* $(n = 4)$: $X^4 + Y^4 = Z^4$; e
- ✓ *Fermatiana Quíntupla* $(n = 5)$: $X^5 + Y^5 = Z^5$.

Destaca-se que, em 2014, Salvador da Silva Bruno abordou o tema da Equação Fermatiana Cúbica na sua dissertação, apresentada com o seguinte título: "**O Último Teorema de Fermat para $n = 3$**". O texto desta dissertação encontra-se disponível na Base de Dados de Dissertações do PROFMAT.

Com o desenvolvimento das provas de novos casos particulares e com a elaboração de teoremas auxiliares ao UTF, a Teoria Algébrica foi, ao longo do tempo, aumentando o seu corpo teórico. Ressalta-se ainda o importante papel do estudo de casos particulares de expoentes primos em virtude da generalização dos seus resultados.

Um destacado papel desempenhou Sophie Germain, matemática francesa, que assumiu identidade de homem para estudar matemática, apresentando importantes resultados sobre o UTF. Publicou um teorema, cujos resultados subsidiaram as provas obtidas por Legendre e Dirichlet para a *Equação Fermatiana Quíntupla*.

Ao fim, após desenvolvidas teorias sobre curvas elípticas e formas modulares e com o esforço de muitos outros matemáticos, Andrew Wiles elabora, em 1995, a versão final da tão esperada *prova geral do UTF*.

Pode-se dizer que essa demonstração, na verdade, condensou um conjunto de ideias, "fracassos", teorias e teoremas; isso desde os primeiros a se dedicarem à prova, como Euler, Germain e Kummer.

Objetiva-se, com esta dissertação, contribuir com a divulgação deste assunto de Teoria dos Números através da apresentação de uma demonstração do **UTF para o caso particular $n = 5$**.

Para tanto, assume-se que o referencial teórico é suficiente para a leitura de todas as etapas da demonstração apresentada. Complementarmente, à teoria e à demonstração, desenvolve-se ainda um capítulo com curiosidades e exercícios.

Destaca-se que a maior parte das demonstrações e das atividades propostas requer conhecimentos básicos de aritmética. Contudo, uma parte delas necessita de alguns conhecimentos um pouco mais elaborados de álgebra, abordados na parte teórica.

A relevância do trabalho se dá na medida em que se verificam poucas publicações em português sobre o UTF, especialmente para o caso $n = 5$, além, é claro, da importância do Teorema no contexto histórico-matemático.

Outro ponto de destaque é que há educadores matemáticos que defendem "apresentação de certos teoremas e de algumas de suas demonstrações ou esboços, a fim de que matemática não se transforme em uma *ciência dogmática*." (Ávila, 2010)

No que se refere à metodologia, realizou-se um levantamento bibliográfico. Faremos, a seguir, uma descrição sucinta sobre o conteúdo abordado nos capítulos.

No **Capítulo 1**, que trata dos Pré-requisitos, faz-se uma síntese teórica sobre *Aritmética e Teoria Algébrica* com princípios, definições, provas e exemplos para dar suporte ao entendimento das demonstrações apresentadas e à realização das atividades propostas. No capítulo, levantam-se ainda *aspectos histórico-matemáticos*, que abrangem a conjectura inicial, a elaboração das primeiras provas e a demonstração final.

O **Capítulo 2** centra-se na demonstração da **Equação Fermatiana Quíntupla**. Inicialmente, aborda importantes aspectos do *Teorema de Sophie Germain* (TSG) aplicados ao estudo da Equação Fermatiana Quíntupla. Logo depois, apresentam-se, detalhadamente, *as etapas da demonstração*, a fim de que, idealmente, o leitor possa refazê-las sozinho.

O **Capítulo 3** – Curiosidades, exemplos e atividades – esta parte desempenha um *papel complementar ao resto do texto*, servindo para ampliar alguns exemplos da teoria e também para reforçar certos pontos abordados na demonstração principal.

CAPÍTULO 1 – PRÉ-REQUISITOS

O conceito de divisibilidade representa a base do desenvolvimento teórico de aritmética e álgebra, conteúdos importantes nas demonstrações presentes no UTF. A noção de divisibilidade, estudada de forma intuitiva no ensino básico, terá uma apresentação formal neste trabalho.

Conforme Tao (2013), as aplicações matemáticas que derivam do conceito de divisibilidade nos inteiros são inúmeras e são alicerces para muitos campos da matemática. O referido autor, ganhador da *Medalha Fields* de 2006, afirma:

> *O conceito de divisibilidade leva naturalmente ao de número primo, o que conduz ao estudo detalhado de fatoração. O conceito das operações entre inteiros adapta-se à aritmética modular, a qual se aplicando aos subconjuntos dos inteiros, é generalizada pela álgebra dos grupos, anéis e corpos finitos, e, assim, leva à teoria algébrica dos números onde o conceito de número é alargado aos irracionais quadráticos, aos elementos dos corpos ciclotômicos e aos números complexos.*

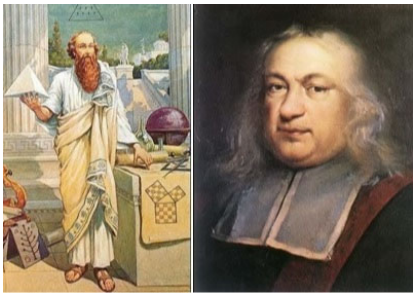
Nos pré-requisitos, realiza-se um resumo teórico com princípios, definições, provas e exemplos, abordando tópicos de divisibilidade nos inteiros, aritmética modular e teoria algébrica para apoio à leitura e ao entendimento das etapas da demonstração do capítulo seguinte e para realização das atividades propostas.

Espera-se que, como uma aplicação didática, os passos da demonstração sejam lidos linha a linha e refeitos com consulta ao compêndio teórico, caso necessária. Também se espera que este compêndio desempenhe papel similar no que se refere ao capítulo de Curiosidades, exemplos e atividades.

Neste capítulo, inicialmente, são abordados alguns aspectos histórico-matemáticos, abrangendo a conjectura inicial, a elaboração das primeiras provas e a demonstração final para a contextualização e o entendimento do desenvolvimento histórico do teorema proposto na dissertação. Deste modo, serão introduzidas certas questões histórico-matemáticas com relevância na demonstração e, em sequência, será desenvolvida uma explanação teórica.

1.1 Aspectos Históricos

Conjectura de Fermat



Fermat fez uma importante anotação no Livro Aritmética do matemático grego Diofanto de Alexandria como comentário sobre a proposição da infinitude de soluções de uma equação pitagórica.

Assim, para agregar mais conhecimento àquela informação, conjecturou, portanto, a solução de um problema que só seria, de fato, demonstrado três séculos e meio mais tarde, desafiando, nesse período, várias centenas de matemáticos e de não-matemáticos na busca de um desfecho para a conjectura enunciada e que ficou muito tempo em aberto. Extrapolou, estudando expoentes maiores que 2.

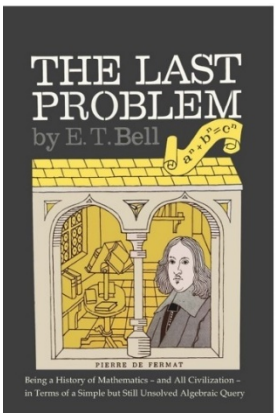
A nota de Fermat dizia o seguinte em Latim, com tradução para o português:

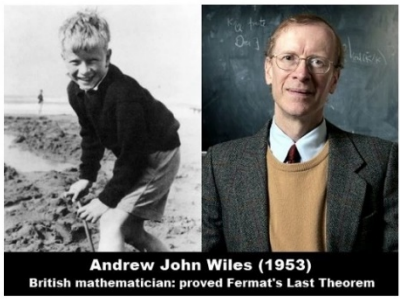
> *É impossível decompor um cubo em dois cubos, um biquadrado em dois biquadrados e, de um modo geral, qualquer potência acima de dois na soma de duas potências de igual expoente. Para isso, eu descobri uma demonstração verdadeiramente maravilhosa, mas a margem é pequena demais para contê-la.*

Desta forma, Fermat declarava que não podiam existir três números inteiros, todos não nulos, satisfazendo a "*Equação Fermatiana*" ($\mathbf{X^n + Y^n = Z^n}$), isto é, tal equação não podia apresentar soluções inteiras não triviais.

Brilhantes matemáticos não conseguiram reconstituir a prova geral, mencionada por Fermat, tais como Euler e Gauss. Foi apenas, em 1993, que Wiles, utilizando técnicas e conteúdos matemáticos ainda não disponíveis no século XVII, desenvolveu a citada demonstração.

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





Wiles, quando criança, leu a Conjectura de Fermat no livro "*The Last Problem*" do autor Eric Bell.

ALGUMAS RELAÇÕES SOBRE O UTF:

Expressões Fermatianas

$$\overbrace{\begin{bmatrix} x \neq 0 \\ \text{e} \\ y \neq 0 \\ \text{e} \\ z \neq 0 \end{bmatrix}}^{\text{INTEIROS}} \Longrightarrow \begin{bmatrix} x^2 + y^2 = z^2 \text{ (Equação Pitagórica)} \\ \\ \text{Relações Fermatianas:} \\ \left.\begin{matrix} x^3 + y^3 \neq z^3 \\ x^4 + y^4 \neq z^4 \\ x^5 + y^5 \neq z^5 \end{matrix}\right\} \text{Casos } n = 3, 4 \text{ e } 5 \\ \\ \vdots \\ \\ \overbrace{x^n + y^n \neq z^n}^{n > 2 \text{ (Caso Geral)}} \end{bmatrix}$$

Teorema de Fermat – Primeiras provas

A figura, a seguir, ilustra os principais personagens desta primeira etapa.

Em relação aos personagens citados, pode-se destacar:

- Fermat enunciou a conjectura em 1637 e, por volta de 1640, esboçou a prova para o caso do expoente $n = 4$, apresentando uma importante técnica de demonstração por contradição, conhecida, na literatura, como **Método da Descida Infinita de Fermat**, que consiste em uma "descida infinita" de soluções naturais. Pode ser aplicada também nos casos $n = 3$ e 5.
- Samuel de Fermat, publicou, por volta de 1670, uma edição do livro Aritmética de Diofanto com as anotações do seu pai.
- Apenas em 1770, foi publicado o trabalho de Leonhard Euler do caso $n = 3$ (*Equação Fermatiana Cúbica*), no qual se aplicou o conceito do número imaginário $i = \sqrt{-1}$ na fatoração. Para o aprofundamento da prova, estudaram-se os Anéis Eisenstein. Destaca-se ainda que Euler

verificou “algumas pistas” nas anotações de Fermat sobre a ideia da “descida infinita”, método que não era de fácil extrapolação.

- Em 1823, Sophie Germain propôs um teorema auxiliar ao Último Teorema de Fermat, dividido em dois casos. Relaciona a divisibilidade das ternas de inteiros a certos expoentes primos (primos de Germain). Os trabalhos de Germain foram importantes nas demonstrações dos casos $n = 5$ e 7, entre outros casos.
- Por volta de 1825, Dirichlet e Legendre provaram, de forma independente, o caso particular $n = 5$, estudando-se a fatoração única nos Anéis de Dedekind.
- Dirichlet demonstrou, em 1832, o caso do expoente $n = 14$.
- Já, em 1839, Lamé apresentou uma elaborada demonstração para o caso $n = 7$, aprimorando, inclusive, certos aspectos da prova original de Germain. Utilizou uma expressão algébrica com fatores lineares e quadráticos equivalente à $(X + Y + Z)^7 - (X^7 + Y^7 + Z^7)$.
- Em 1847, Kummer enunciou um outro importante teorema auxiliar, também dividido em dois casos, que relaciona o Último Teorema de Fermat a uma importante classe de primos, denominados regulares, úteis em várias outras demonstrações. Assim, tendo-se um “expoente primo e regular em uma equação fermatiana, garante-se a não existência de solução de inteiros não nulos”.
- Kummer trouxe ainda um importante “método para os divisores complexos”.
- Segue um diagrama útil que resume a estratégia dessas provas iniciais:

Fonte: Elaboração Própria.

Em qualquer **Equação Fermatiana** tem-se:

$$\boldsymbol{mdc(x,y) = 1 \Leftrightarrow mdc(x,z) = 1 \Leftrightarrow mdc(y,z) = 1}$$

$$\text{Existe } \underbrace{(x_0, y_0, z_0)}_{\substack{Sol.\ inteira \\ não\ nula}} \Longrightarrow \text{ Existe } \underbrace{(x_1, y_1, z_1)}_{\substack{Sol.\ inteira \\ não\ nula\ com \\ mdc\ (x_1,y_1)=1}}$$

Ainda sobre estas equações, observa-se:

$$\mathbf{X^n + Y^n = (X + Y)(X + \zeta Y) \dots (X + \zeta^{n-1} Y) = Z^n}$$

Onde: $\underbrace{\zeta = cos\left(\frac{2\pi}{n}\right) + i\, sen\left(\frac{2\pi}{n}\right) = e^{\left(\frac{2\pi i}{n}\right)}}_{para\ n\ primo\ ímpar}$

$$\boldsymbol{\zeta^n = 1} \text{ com } \boldsymbol{\zeta \neq 1}$$

Observação: as potências de ζ são chamadas de "**inteiros ciclotômicos**" ("*os que cortam o círculo*").

A figura, a seguir, resume importantes considerações gerais acerca dos *Ternos Fermatianos*:

$X^n + Y^n = Z^n$ (UTF – Caso Geral)

- $(X.Y.Z) \neq 0$: é importante observar se este produto de inteiros é ou não múltiplo do expoente n, especialmente nos casos em que n é primo. Os primos de Germain e os primos regulares são essenciais em várias demonstrações de casos particulares de expoentes.
- $mdc(x,y) = 1 \Leftrightarrow mdc(x^n, y^n) = 1$
- $\left.\begin{matrix}(\text{par})^n + (\text{par})^n \\ (\text{ímpar})^n + (\text{ímpar})^n\end{matrix}\right\} = \text{par}$ e $\left.\begin{matrix}(\text{par})^n + (\text{ímpar})^n \\ (\text{ímpar})^n + (\text{par})^n\end{matrix}\right\} = \text{ímpar}$

Fonte: Elaboração Própria.

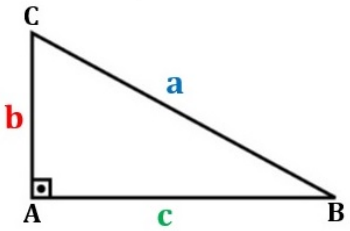
No caso da "*Equação Fermatiana Biquadrática*", analisam-se os ternos pitagóricos reduzidos (x^2, y^2, z^2), tomados a partir dos números inteiros m e n (não ambos ímpares), com $m > n > 0$ e $mdc\,(m,n) = 1$:

$$(x^2, y^2, z^2) = (m^2 - n^2,\ 2mn,\ m^2 + n^2)$$

A apresentação anterior dos ternos é útil para se estudar certas *relações de paridade*.

Na Escola Básica, pode-se abordar a ideia dos **ternos pitagóricos** da seguinte forma:

TERNOS PITAGÓRICOS
(com os inteiros m, n > 0)



$\mathbf{a = (m^2 + n^2)}$
$\mathbf{b = 2mn}$
$\mathbf{c = (m^2 - n^2)}$

$$\Rightarrow \underbrace{\left(\mathbf{m^2 + n^2}\right)^2 = (\mathbf{2mn})^2 + \left(\mathbf{m^2 - n^2}\right)^2}_{\text{Por Pitágoras}}$$

Em relação à "*descida infinita*" (aplicada ao caso $n = 4$), merece destaque que a sua ideia central é, sem perda de generalidade, esboçar uma terna que seja solução com inteiros positivos (a_1, b_1, c_1) para a equação $\mathrm{X}^4 + \mathrm{Y}^4 = \mathrm{Z}^4$ e, em sequência, esboçar uma outra solução, também de inteiros positivos (a_2, b_2, c_2), de modo que se tenha, assim, um c_2 com $0 < c_2 < c_1$.

Em seguida, exibe-se outra terna (a_3, b_3, c_3), tendo-se $0 < c_3 < c_2 < c_1$.

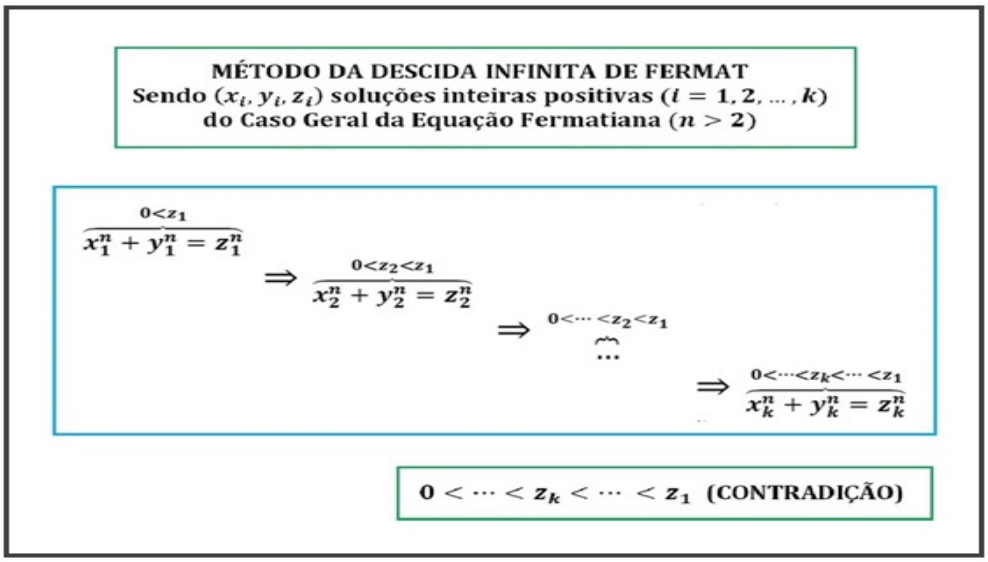
Recursivamente, tal procedimento pode ser repetido "*infinitas vezes*", de maneira a sempre se obter um inteiro positivo menor que o anterior:

$$0 < \cdots < c_k < \cdots < c_3 < c_2 < c_1$$

Chega-se, assim, a uma contradição, pois estão sendo exibidos números inteiros positivos sempre menores que os anteriores, mas, entre um número inteiro positivo e o número zero, existe apenas uma **quantidade finita** de possibilidades.

Note que se isso não representasse uma contradição, também não haveria um *menor elemento* para o conjunto dos inteiros positivos.

O **Método da Descida Infinita de Fermat** esquematiza-se a seguir:



Fonte: Elaboração Própria.

No que se refere à **Estrutura Algébrica** específica das *Equações Biquadráticas*, estuda-se a fatoração única no Anel dos Inteiros de Gauss com representação a seguir:

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

$$= (x + y).(x + iy).(x - y).(x - iy)$$

De fato, pela **Reciprocidade Biquadrada de Gauss**, os Inteiros Gaussianos são da seguinte forma:

$$\mathbb{Z}[i] = \{a + bi;\ a \text{ e } b \in \mathbb{Z}\}\ (\pm 1 \text{ e } \pm i \text{ são suas unidades}),$$

sendo $\mathbb{Z}[i]$: *Domínio de Fatoração Única* (será estudado na teoria)

Euler, ao estudar a "*Equação Fermatiana Cúbica*" introduz um sistema de números da forma $a + b\sqrt{-3}$ em $\mathbb{Z}[\sqrt{-3}]$, que nem sempre apresenta fatoração única neste domínio. Este era um problema que precisava ser resolvido.

Na prova do caso $n = 3$, há um importante conceito acerca da *divisibilidade* dos "**números inteiros da forma $a^2 + 3b^2$**", que pode ser apresentado da seguinte forma:

$$\underbrace{p}_{\substack{primo \\ ímpar}} \mid \underbrace{(a^2 + 3b^2)}_{\substack{a \text{ e } b \text{ inteiros} \neq 0 \\ mdc\,(a,b)=1}} \Longrightarrow \left[\begin{array}{c} Existem\ inteiros\ a_0 \text{ e } b_0, tais\ que: \\ p = {a_0}^2 + 3{b_0}^2 \end{array}\right]$$

Exemplos: $\begin{cases} 7 \mid 28 = (5)^2 + 3.(1)^2 \Longrightarrow 7 = (2)^2 + 3.(1)^2 \\ 13 \mid 39 = (6)^2 + 3.(1)^2 \Longrightarrow 13 = (1)^2 + 3.(2)^2 \end{cases}$

Neste caso, explora-se a **Reciprocidade Cúbica de Gauss**, obtendo-se os Inteiros de Eisenstein, assim, representados:

$$\mathbb{Z}[w] = \{a + bw;\ a \text{ e } b \in \mathbb{Z}\}$$

Sendo:

$$w = e^{\left(\frac{2\pi i}{3}\right)} = \frac{-1 + \sqrt{-3}}{2}$$

Tem-se também:

$$\underbrace{\mathbb{Z}[\boldsymbol{w}] = \left\{\frac{(\boldsymbol{\alpha_1} + \boldsymbol{\alpha_2}\sqrt{-3})}{2} \textbf{ com } \boldsymbol{\alpha_1} \equiv \boldsymbol{\alpha_2}\ (\boldsymbol{mod}\ \mathbf{2})\right\}}_{\text{DOMÍNIO DE FATORAÇÃO ÚNICA}}$$

Pode-se escrever a *Equação Fermatiana Cúbica* em $\mathbb{Z}[w]$:

$$\mathrm{X}^3 + \mathrm{Y}^3 = (\mathrm{X} + \mathrm{Y})(\mathrm{X} + \mathrm{wY})(\mathrm{X} + \mathrm{w}^2\mathrm{Y})$$

Na demonstração de $n = 3$, Euler verifica que há "**cubos de números da forma $a^2 + 3b^2$**".

Assim, perda de generalidade, existe um número z, tal que:

$$z^3 = a^2 + 3b^2 = \left(a + b\sqrt{-3}\right)\left(a - b\sqrt{-3}\right)$$

Como $\left(a + b\sqrt{-3}\right)$ e $\left(a - b\sqrt{-3}\right)$ são *primos entre si*, uma ideia bem interessante para esta demonstração é ver que estes fatores também representam cubos.

Analogamente, na demonstração do caso $n = 5$, como há "**quintas potências de números da forma $a^2 - 5b^2$**", os fatores $(a + b\sqrt{5})$ e $(a - b\sqrt{5})$ também são primos entre si.

Para as *Equações Fermatianas Quíntuplas*, é importante observar ainda a **Estrutura Algébrica dos Inteiros de Dedekind**:

$$\mathbb{Z}[\theta] = \{a + b\theta;\ a \text{ e } b \in \mathbb{Z}\}$$

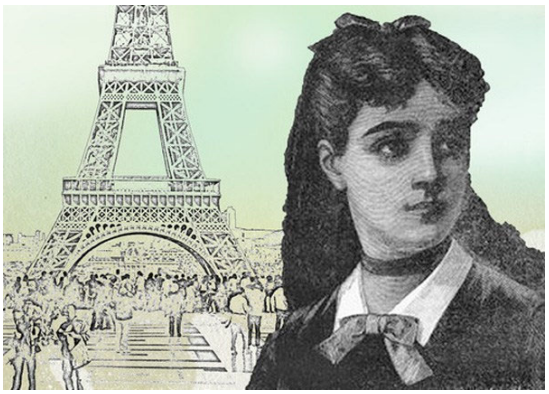
Sendo:

$$\theta = e^{\left(\frac{2\pi i}{5}\right)} = \frac{1 + \sqrt{5}}{2}$$

Tem-se também:

$$\underbrace{\mathbb{Z}[\boldsymbol{\theta}] = \left\{\frac{(\boldsymbol{w_1} + \boldsymbol{w_2}\sqrt{\mathbf{5}})}{\mathbf{2}} \textbf{ com } \boldsymbol{w_1} \equiv \boldsymbol{w_2}\ (\boldsymbol{mod}\ \mathbf{2})\right\}}_{\text{DOMÍNIO DE FATORAÇÃO ÚNICA}}$$

A francesa **Sophie Germain**, ilustrada na figura a seguir, assumiu a identidade de homem para desenvolver os seus estudos matemáticos. Ela trouxe uma grande contribuição para algumas provas do Último Teorema de Fermat.



Esta matemática trouxe o conceito dos *números de Germain*, que representam uma classe de primos, tais que se "**p é primo de Germain, então $2p + 1$ é primo**".

Exemplos de primos de Germain**:** 2, 3, 5, 11, 23, 29, 41, 53, 83 e 89. Uma questão ainda em aberto é se estes números são infinitos ou não.

O **Teorema de Sophie Germain (TSG)**, aplicável aos primos de Germain, pode ser enunciado da seguinte forma:

> *Se, em uma terna de inteiros* (x, y, z)*, nenhum ou apenas um destes números for divisível por* $p > 2$ *(primo de Germain), então não existem soluções inteiras não nulas para a equação:* $X^p + Y^p = Z^p$.

Pode-se ainda dizer o seguinte:

Se $p > 2$, sendo p e $2p + 1$ primos, então não existem inteiros x, y e z, diferentes de zero e não múltiplos de p, tais que:

$$\mathbf{X^p + Y^p = Z^p}$$

Exemplo: Supondo $mdc\ (x, y, z) = 1$ e sendo 5 e 11, ambos primos de Germain, tem-se que:

$$\begin{cases} 5 \nmid (x.y.z) \Longrightarrow \underbrace{x^5 + y^5 = z^5}_{\substack{\text{não tem soluções inteiras} \\ \text{não nulas}}} \\ 11 \nmid (x.y.z) \Longrightarrow \underbrace{x^{11} + y^{11} = z^{11}}_{\substack{\text{não tem soluções inteiras} \\ \text{não nulas}}} \end{cases}$$

De fato, sabe-se que:

$p \nmid (x.y.z) \Longrightarrow p \nmid x$ e $p \nmid y$ e $p \nmid z$

O *Teorema de Germain* apresentou grande relevância na prova da "*Equação Fermatiana Quíntupla*" $(\mathbf{X^5 + Y^5 = Z^5})$.

Germain observou que, para a equação anterior poder apresentar uma solução inteira não nula, pelo menos *uma das variáveis* **X, Y e Z** deveria ser divisível por 5.

Lamé chegou a anunciar que tinha obtido a prova geral do Último Teorema de Fermat. Todavia, Kummer pontuou que uma prova genérica do teorema dependeria, fundamentalmente, de se garantir a decomposição única em fatores primos para certos inteiros pertencentes a anéis, tais como os *Inteiros de Eisenstein* e os de *Dedekind*, de forma a se "*estender o significado dos números inteiros*".

Para se resolver o imbróglio da *Decomposição Única no Teorema de Fermat*, Kummer, Lamé e Dedekind trabalharam arduamente nesta questão, estabelecendo-se,

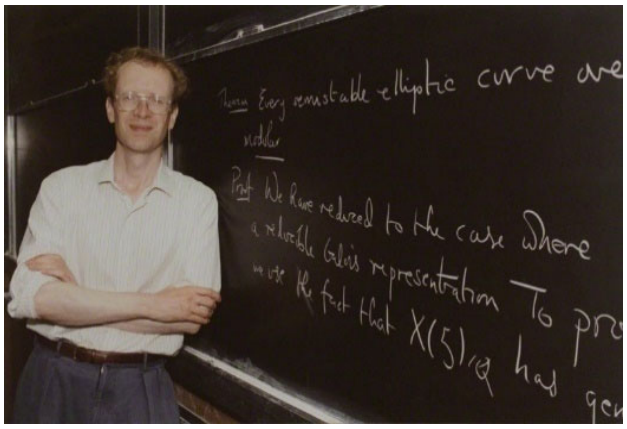
assim, um notável desenvolvimento da *Teoria dos Anéis* naquela época.

Kummer apresentou uma importante modalidade de números, denominados *Números Algébricos sobre Corpos*, isto é, números complexos que são raízes de equações polinomiais com coeficientes nestes corpos.

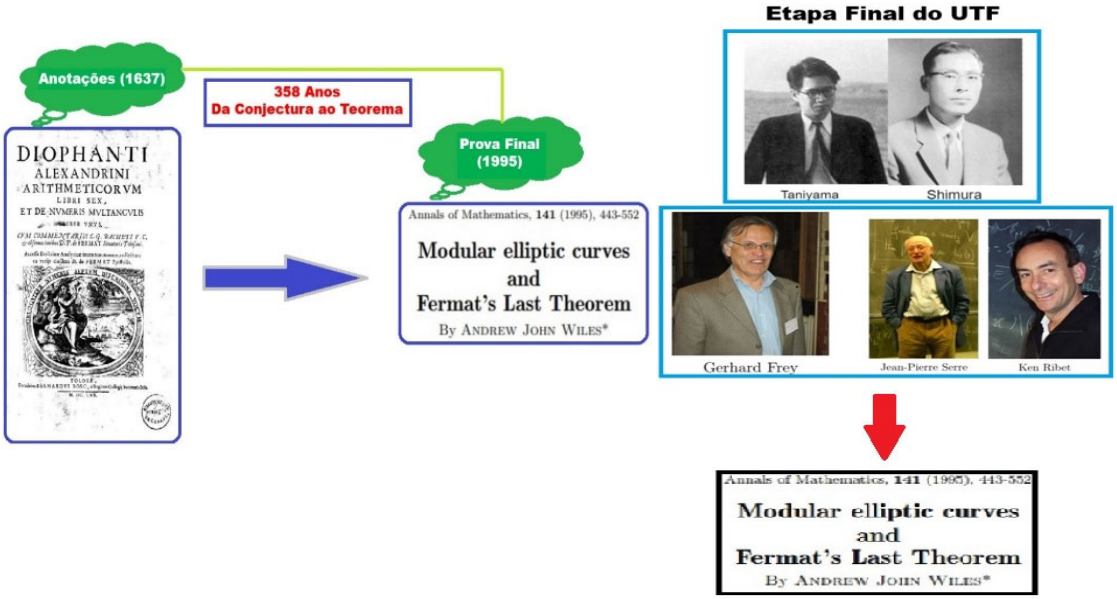
Embora o estudo dos Números Algébricos tenha representado um razoável avanço, a sua *fatoração nem sempre é única*. Apenas com os "**Números Ideais**" teríamos definidos os **Domínios de Fatoração Única**, estruturas algébricas fundamentais no UTF.

De acordo com Kleiner (2007), Kummer não elaborou um conceito matematicamente preciso acerca dos "Números Ideais", tendo enunciado uma importante ideia inicial sobre o tema, abordando a Fatoração Única em "*Primos Ideais Complexos"*. Deste modo, a formulação precisa e ainda hoje utilizada sobre os "Números Ideais" coube a Dedekind.

Teorema de Fermat-Wiles



Percurso da Prova **Contribuições para Wiles**



Andrew Wiles passou anos trabalhando sozinho e em segredo para realizar a prova do Último Teorema de Fermat. Em uma conferência em Cambridge, na Inglaterra, em junho de 1993, anunciou um resultado como prova do Último Teorema.

O manuscrito da demonstração circulou entre um seleto grupo de matemáticos, especialistas em Teoria nos Números e, durante o processo de arbitragem, uma lacuna foi encontrada. De fato, após uma verificação detalhada nos manuscritos de Wiles, descobre-se um erro sutil.

Wiles volta ao trabalho para tentar corrigir o erro apontado e, em dezembro do mesmo ano, pronuncia-se sobre o teorema através de uma mensagem eletrônica, que

circula em toda comunidade matemática.

Ele explica que, no processo de revisão da prova, surgiram vários problemas, muitos dos quais foram resolvidos, mas um, em particular, não foi.

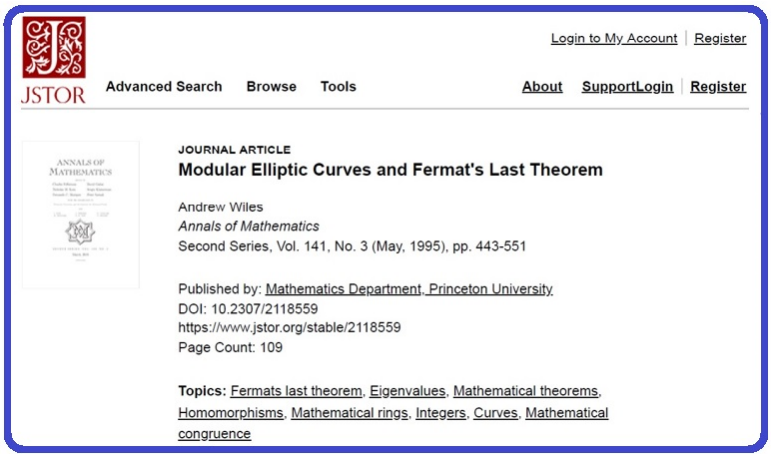
A questão a ser resolvida estava no passo da conjectura de Taniyama-Shimura, conforme detalhado, em inglês, no e-mail a seguir:

> Subject: Fermat Status
> Date: 4 Dec. 93 01:36:50 GMT
>
> In view of the speculation on the status of my work on the Taniyama-Shimura conjecture and Fermat's Last Theorem I will give a brief account of the situation. During the review process a number of problems emerged, most of which have been resolved, but one in particular I have not yet settled. The key reduction of (most cases of) the Taniyama-Shimura conjecture to the calculation of the Selmer group is correct. However the final calculation of a precise upper bound for the Selmer group in the semistable case (of the symmetric square representation associated to a modular form) is not yet complete as it stands. I believe that I will be able to finish this in the near future using the ideas explained in my Cambridge lectures.
>
> The fact that a lot of work remains to be done on the manuscript makes it still unsuitable for release as a preprint. In my course in Princeton beginning in February I will give a full account of this work.
>
> Andrew Wiles.

No início de 1994, decidiu continuar trabalhando no teorema, pedindo ajuda a Richard Taylor, doutor em Teoria dos Números e seu orientado em Princeton.

Durante o ano de 1994, trabalharam intensamente no *Grande Teorema*[1], que foi publicado em 1995 sob o título: *"Modular Elliptic Curves and Fermat's Last theorem"* (Curvas elípticas modulares e o Último Teorema de Fermat), in *Annals of Mathematics*, Nº 141(1995), p. 443-551.

[1] Wiles recebeu, dentre outros, os prêmios matemáticos: Fermat em 1995 e Abel em 2016, ambos por suas contribuições ao Último Teorema. Taylor foi ainda agraciado, em 2001, com o prêmio Fermat por suas importantes contribuições às representações de Galois e automorfismos.

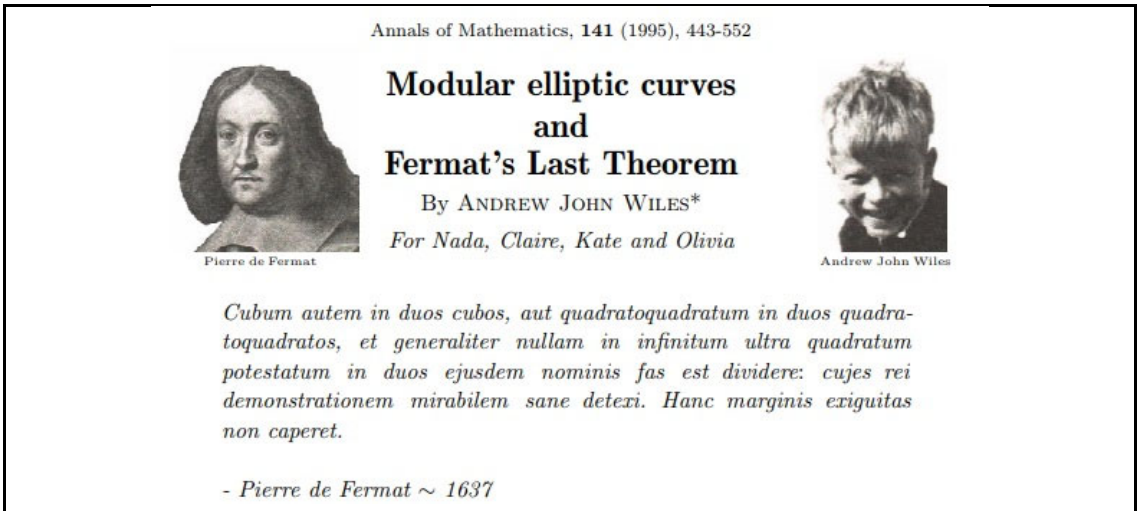


Trata-se de um artigo de 110 páginas, baseado em trabalhos de vários outros matemáticos, podendo ser lido no seguinte endereço, mantido pelo professor Nicolau Saldanha da PUC Rio: <http://www.mat.puc-rio.br/~nicolau/olimp/Wiles.pdf>.

A solução final do problema do Último Teorema de Fermat é, consideravelmente, técnica, havendo vários teoremas, lemas e proposições envolvidos.

Assim, buscamos realizar, nesta parte do trabalho, uma descrição bastante simplificada da ideia da prova de Wiles e de alguns conceitos aplicados a ela.

Segue o resumo, traduzido de Wiles, sobre a sua demonstração final:



Resumo (tradução nossa). Quando Andrew John Wiles tinha 10 anos de idade, leu "O Último Problema", obra do escritor e matemático Eric Temple Bell. Assim, ficou tão impressionado que decidiu ser a primeira pessoa a provar o Último Teorema de Fermat. Este teorema afirma que a terna (a, b, c), solução de $a^n + b^n = c^n$ com $n > 2$, não pode representar soluções inteiras não nulas da equação. Este artigo objetiva provar que todas as curvas elípticas semiestáveis sobre o conjunto de números racionais são modulares. O Último Teorema de Fermat segue como um corolário dos trabalhos de Frey, Serre e Ribet.

Conforme visto no resumo do artigo de Wiles, o enunciado do teorema é bem simples, entretanto, a prova a ele relacionada possui muitos passos e diferentes conceitos, além de um elevado grau de dificuldade. Assim, era improvável poder ser demonstrado apenas com o arcabouço conceitual da época de Fermat.

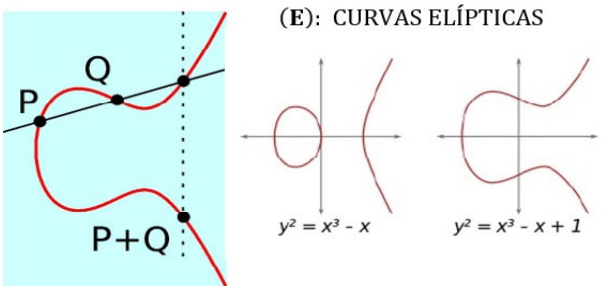
A primeira versão da prova dependia da construção de um **Sistema de Euler**[2], que era muito complexa e relacionada ao teorema de **Taniyama-Shimura**. Neste sentido, a colaboração de Taylor foi fundamental, resultando em uma demonstração final com importantes pontos acertados em relação à apresentada em 1993.

Destaca-se que o Teorema de *Taniyama-Shimura*, cuja conjectura deve-se, principalmente, ao matemático japonês Taniyama, estabelece um importante princípio para as curvas elípticas[3] e as formas modulares: "toda curva elíptica pode ser parametrizada por funções modulares". Uma das consequências da validade do teorema foi a proposição de Fermat-Wiles.

Destaca-se que "**Equações Elípticas**" são, por exemplo, as do tipo:

$$\mathbf{Y^2 = X^3 + aX^2 + bX + c}, \text{ sendo } \boldsymbol{a, b, c} \in \mathbb{Z}$$

Na figura, a seguir, são *formas elípticas*:



Um maior detalhamento sobre o tema de equações e formas elípticas pode ser consultado na dissertação do PROFMAT intitulada: "Criptografia via curvas elípticas" (Júnior, 2013).

Ainda se tem que as "**Formas Modulares**" são *funções complexas* e que possuem a propriedade de serem, desordenadamente, *simétricas*.

---

[2] Sistema de Euler é um conceito presente na Teoria dos Módulos de *Galois*, onde se tratam especialmente as curvas elípticas modulares.

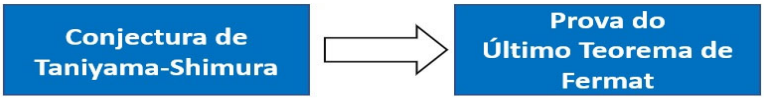
[3] Curvas Elípticas são objetos de um ramo da matemática, denominado Geometria Algébrica (combinação de conteúdos de Geometria e de Álgebra Abstrata).

Em 1984, **Gerhard Frey** conjecturou que um contraexemplo de $a^n + b^n = c^n$ para o UTF geraria uma *Curva Elíptica Semiestável* (*Curva Frey*):

$$\boldsymbol{y^2 = x.(x + a^n).(x - b^n)}$$

Esta curva possui *propriedades atípicas* que implicariam em uma forma de *contradição* da Conjectura Taniyama-Shimura (ainda não provada na época).

Kenneth Ribet, ganhador do Prêmio Fermat de 1989, demonstrou ainda a *Conjectura do Epsilon* (do matemático *Jean-Pierre Serre*), que afirma que uma Curva Frey não é configurável através de *funções modulares*. Portanto, se a conjectura de Taniyama-Shimura é verdadeira, então o Último Teorema também é. Assim:

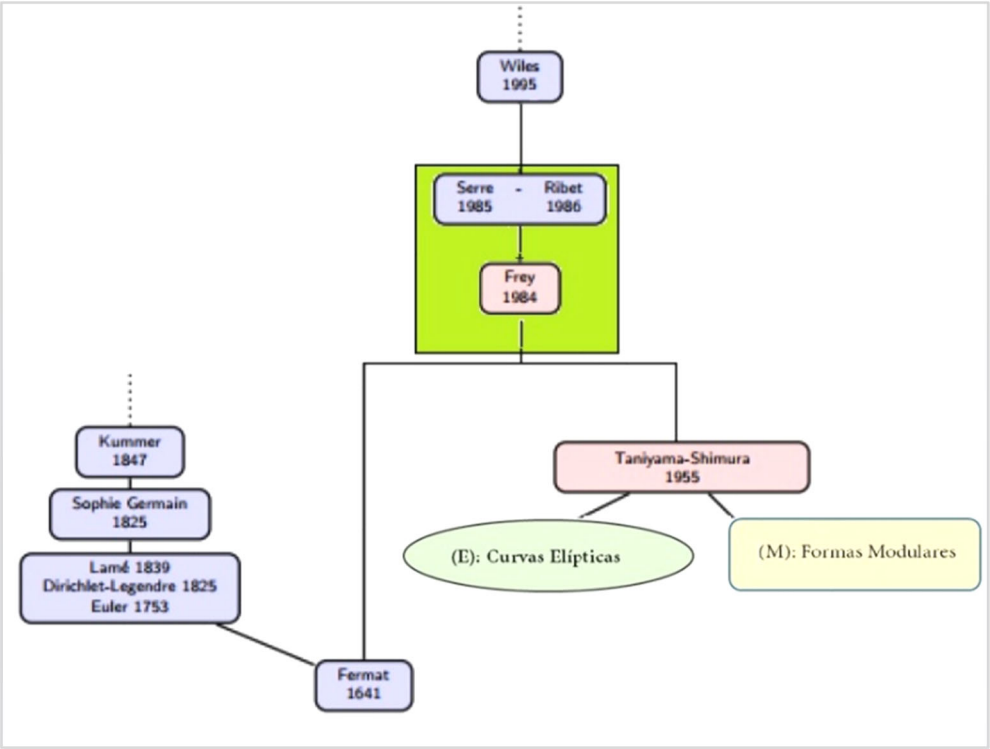


As *contribuições* de **Frey, Serre e Ribet** foram determinantes para a prova de **Fermat-Wiles**, o que justifica a citação dos nomes destes matemáticos no artigo final.

Em 2016, *Andrew Wiles* recebe o Prêmio Abel, atribuído anualmente pelo Rei da Noruega, com a seguinte justificativa e motivação: "pela sua impressionante demonstração do Último Teorema de Fermat com recurso à conjetura da modularidade para curvas elípticas semiestáveis, dando início a uma nova era na *Teoria dos Números*".

Conforme Singh (2004): "*Uma demonstração como a de Fermat é um grande triunfo intelectual e não se deve perder de vista o fato de que ela revolucionou a Teoria dos Números em um só golpe*".

O seguinte diagrama esquematiza e sintetiza algumas das principais etapas do processo de elaboração da demonstração geral ao longo do tempo:



Fonte: Elaboração Própria

1.2 Aritmética

O **conceito de divisibilidade**, possui um papel central na aritmética dos inteiros.

Sejam a e $b \in \mathbb{Z}$. Diz-se que "a é divisor de b" quando existe um inteiro q, tal que:

$$\boldsymbol{b = q.a}$$

Denota-se assim: $a \mid b$.

A sua negação é denotada por: $a \nmid b$.

Para todo $a \neq 0$, dizer que $a \mid b$ é equivalente à afirmação de que:

$$\boldsymbol{\frac{b}{a}}$$

é uma fração que representa um número inteiro.

Exemplos 1.1 – Temos que:

a) $d \mid 4 \Leftrightarrow d \in \{\pm 1, \pm 2, \pm 4\}$, pois existem inteiros q que satisfazem $4 = q.d$ (fatorações possíveis do número 4).
b) Considere os números inteiros: $7, 17$ e 21. Tem-se que $7 \mid 21$, pois existe um inteiro 3, tal que $21 = 3.7$. Mas, $7 \nmid 17$, pois, supondo ser q um inteiro qualquer, verifica-se que $17 \neq q.7$. De fato, as relações a seguir terão a sua sequência explicada na *Divisão Euclidiana*:

$$14 = 2.7 < 17 = 2.7 + 3 < 3.7 = 21 \text{ e } q' = \frac{17}{7} = \frac{(2.7+3)}{7} = \left(2 + \frac{3}{7}\right) \notin \mathbb{Z}$$

Observação: As seguintes expressões são todas equivalentes: "a é um fator ou divisor de b"; "a divide b"; "b é múltiplo de a"; e "b é divisível por a".

No âmbito da Teoria Axiomática dos Conjuntos, há um importante conceito, denominado de **Princípio da Boa Ordenação (PBO)**. Este princípio informa que todo subconjunto não vazio de inteiros, formado por números naturais, possui um menor elemento.

Merece destaque que, nesta parte teórica, incluímos o *zero* no conjunto dos números naturais ($\mathbb{N}$). Todavia, há autores que não consideram o *zero* como elemento dos naturais.

A figura anterior representa a estátua de Arquimedes de Siracusa, matemático e físico da Grécia Antiga, que propôs a chamada **Propriedade Arquimediana**, enunciada e provada a seguir.

Propriedade 1.2 (**Arquimediana**)*:* Sejam a e $b \in \mathbb{Z}$ com $a \neq 0$, então existe um inteiro n tal que $n.a > b$.

Prova: $a \neq 0 \Longrightarrow |a| \neq 0 \Longrightarrow |a| \geq 1 \Longrightarrow (|b|+1).|a| \geq |b|+1 > |b| \geq b$.
Logo, supondo existir um inteiro $n = |b|+1$, tem-se:

$$(|b|+1).|a| > b \Leftrightarrow \begin{cases} a > 0, \text{existe } n_1 = |b|+1 \in \mathbb{Z}, \text{tal que } n_1.a > b \\ a < 0, \text{existe } n_2 = -(|b|+1) \in \mathbb{Z}, \text{tal que } n_2.a > b \end{cases}$$

$$\text{Portanto, existe um inteiro } n = \begin{cases} n_1, \text{ se } a > 0 \\ n_2, \text{ se } a < 0 \end{cases} \Longrightarrow n.a > b. \blacksquare$$

Será apresentada uma modalidade de divisão entre quaisquer números naturais com divisor não nulo, fundamentada no **Algoritmo de Euclides** do matemático grego Euclides, ilustrado a seguir.

Assim, daremos o enunciado formal da **Divisão Euclidiana em** $\mathbb{N}$.

Propriedade 1.3 (**Divisão Euclidiana em** $\mathbb{N}$): Dados dois números inteiros positivos a e b, com $b \neq 0$ e $0 < a < b$, então existem e são únicos inteiros q e r (*quociente* e *resto*, respectivamente), com $0 \leq r < a$, tais que $b = q.a + r$, sendo a o *divisor* e b o *dividendo*.

Prova: Sendo $0 \neq b > a > 0$

Tome o conjunto $S = \{b,\ b-1.a,\ b-2.a, \ldots,\ b-n.a\} \subseteq \mathbb{N}$

Note que, pela *Propriedade Arquimediana*, existe um inteiro n, tal que:

$$n.(-a) > -b \Leftrightarrow b - n.a > 0$$

Pelo PBO, S tem um menor elemento r, isto é, existe $q \in \mathbb{N}$ tal que:

$$r = b - q.a \implies b = q.a + r$$

Afirmação: $r < a$.

A afirmação é verdadeira, pois caso contrário teríamos:

$$r > a \implies \exists\, c \in \mathbb{N};\ r = a + c$$
$$\implies c = r - a = (b - q.a) - a = b - (q+1).a \in S$$
$$\implies c < r \text{ com } c \in S$$

Isto é um absurdo, pois r é o menor elemento de S.

Definindo $r = b - q.a$

Como $r \in S$, afirma-se o seguinte:

$$q.a \leq b < (q+1).a \Longrightarrow \begin{cases} r = (b - q.a) < a \\ \\ r \geq 0 \end{cases}$$

Portanto, existem os inteiros q e r com $0 \leq r < a$, tais que $b = q.a + r$

Note que $r = 0$ representa a **divisão exata**.

A *prova da unicidade* consiste em supor, inicialmente, que:

$$b = q_1.a + r_1 = q_2.a + r_2$$

Para mostrar a igualdade dos quocientes e restos da igualdade anterior.

Sendo:

$$q_1, r_1, q_2, r_2 \in \mathbb{Z}$$
$$0 \leq r_1 \leq a$$
$$0 \leq r_2 \leq a$$

Deste modo, tem-se:

$$q_1.a + r_1 = q_2.a + r_2 \Longrightarrow 0 = (q_1 - q_2)a + (r_1 - r_2)$$
$$\Longrightarrow (r_2 - r_1) = (q_1 - q_2)a$$
$$\Longrightarrow a \mid (r_2 - r_1)$$
$$\left.\begin{matrix} 0 \leq r_2 < a \\ -a < (-r_1) \leq 0 \end{matrix}\right\} \Longrightarrow -a < (r_2 - r_1) < a \Longrightarrow |r_2 - r_1| < a$$

Como a divide $|r_2 - r_1|$, então $(r_2 - r_1) = 0$.

Assim:

$$r_1 = r_2 \Longrightarrow q_1 = q_2$$

Portanto, conclui-se a *existência e a unicidade* desta proposição. ■

Exemplo 1.4: Seja $b = 48$ e $a = 6$. Temos que $48 = 8.6$. Verificando também $b = 50$ e $a = 6$, tem-se que $r \neq 0$, já que 50 não é um múltiplo de 6 como, por exemplo, 48. Assim, devem-se observar os múltiplos de 6, entre os quais, 50 está compreendido, que são 48 e 54. Note que:

$$48 = 8.6 < 50 < (8+1).6 = 54$$

Logo:

$$\underbrace{r = 50 - 8.6 = 2}_{\substack{resto\ sempre\ será \\ positivo}}$$

O resultado anterior pode ainda ser estendido para $\mathbb{Z}$.

Desta forma, daremos o enunciado formal da **Divisão Euclidiana em** $\mathbb{Z}$.

Propriedade 1.5 (**Divisão Euclidiana em** $\mathbb{Z}$): Dados dois números inteiros a e b com $b \neq 0$, então existem e são únicos os inteiros q e r (*quociente* e *resto*, respectivamente) com $0 \leq r < a$ (a inteiro *estritamente positivo*), tais que $b = q.a + r$, sendo a o *divisor* e b o *dividendo*.

Prova: Considerando números inteiros b e q e a inteiro positivo e observando ainda os argumentos da *Propriedade Arquimediana,* sempre se verificam apenas uma das seguintes possibilidades, sendo a primeira b é múltiplo de a e a segunda b está entre múltiplos de a:

1ª Possibilidade: $b = q.a \Longrightarrow b - q.a = 0$

2ª Possibilidade: $q.a < b < (q+1).a \Longrightarrow 0 < b - q.a < a$

Fazendo também: $b - q.a = r \Longrightarrow b = q.a + r$, com $0 < r < a$

Juntado as duas possibilidades, pode-se afirmar que, dados dois inteiros a e b quaisquer, com $a > 0$, então existem dois inteiros q e r, tais que $b = q.a + r$, em que $0 \leq r < a$. Note que, sendo b múltiplo de a:

$$r = b - q.a = 0$$

Observe também o seguinte artifício que pode ser utilizado na questão dos sinais e que ficará mais claro com o exemplo numérico:

$$b = q_1.(-a) + r \text{ com } 0 \leq r < a$$

$$b = \underbrace{(-q_1).a + r}_{(-q_1) = q \in \mathbb{Z}}$$

Já a prova da unicidade é análoga à da *Divisão Euclidiana em* $\mathbb{N}$.

Temos, assim, a *existência e a unicidade* desta proposição. ■

Exemplo 1.6: Seja $b = -48$ e $a = 6$. Temos que $-48 = (-8).(+6)$. Observando ainda $b = -50$ e $a = 6$, verifica-se que $r \neq 0$, pois -50 não é um múltiplo de 6 como, por exemplo, -48. Assim, devem-se observar os múltiplos de 6, entre os quais, -50 está compreendido, que são -54 e -48. Note que:

$$-54 = (-9).(+6) < -50 < (-9+1).(+6) = -48$$

Portanto, tem-se que:

$$\underbrace{r = -50 - (-9).(+6) = 4}_{\substack{resto\ sempre\ será \\ positivo}}$$

Conceito geral 1.7 (**Anel**): Anéis são estruturas algébricas que possuem duas operações binárias com propriedades similares às dos inteiros. A matemática Emmy Noether escreveu um livro em 1921, cujo título é "*Ideal Theory in Rings*", o qual estabeleceu importantes fundamentos axiomáticos, especialmente aos anéis comutativos.

Definição 1.8 (**Anel**): Sendo A um conjunto não vazio, tem-se a seguinte *definição de anel* – Seja A munido de duas operações: "$+$" e "$*$", condição também denotada por $(\mathrm{A}, +, *)$. Afirma-se que A é um anel se, para quaisquer elementos $a, b, c \in A$, as propriedades são todas satisfeitas:

i. *Comutatividade* para a operação $(+)$:

$$a + b = b + a$$

ii. Existência de *elemento neutro* para a operação $(+)$, denominado *zero do anel* $(0_{\mathrm{A}} \in \mathrm{A})$:

$$a + 0_{\mathrm{A}} = 0_{\mathrm{A}} + a = a$$

iii. Existência e unicidade do *elemento simétrico,* também chamado de *inverso aditivo*:

$$a + b = b + a = 0_{\mathrm{A}} \Longrightarrow b = -a \quad \text{e} \quad a = -(-a) = -b$$

iv. *Associatividade* para as operações $(+)$ e $(*)$:

$$(a + b) + c = a + (b + c) \quad \text{e} \quad (a * b) * c = a * (b * c)$$

v. *Distributividade* à esquerda e à direita:

$$a * (b + c) = a * b + a * c$$
$$(b + c) * a = b * a + c * a$$

Observações: Se além destas propriedades, o anel possuir a propriedade de comutatividade para $(*)$: $a * b = b * a$, denomina-se **anel comutativo**. Existindo também uma unidade (1_A) no anel A, com $0_A \neq 1_A$, tem-se: $a * 1_A = 1_A * a = a$, caso de **anel com unidade**. Se tivermos $a * b = 0_A \Longrightarrow a = 0_A$ ou $b = 0_A$, verifica-se ainda o caso de **anel sem divisores de zero.**

Reunindo os três casos, temos um **DOMÍNIO DE INTEGRIDADE**. Neste trabalho, para fins de simplificação, quando nos referirmos ao termo anel estamos, de forma geral, nos referindo a anel comutativo com unidade.

Exemplos 1.9 – Observe os seguintes casos:

a) O conjunto $\mathbb{Z}$ (números inteiros), munido das operações de soma e produto, que satisfaz as propriedades acima é chamado de anel dos inteiros.
b) O anel dos inteiros pares, $A = 2.\mathbb{Z}$, não possui unidade (1_A).
c) $A = \mathbb{Z}_6$ não é um domínio de integridade, pois, neste anel, existem elementos não nulos cujo produto resulta 0_A. Por exemplo, neste anel, $\overline{2}$ e $\overline{3}$ são divisores de zero.
d) Observe que o anel $M_{n\,x\,n}(\mathbb{R})$, matrizes n x n com entradas nos números reais, é um anel não-comutativo para $n \geq 2$.
e) Os Inteiros de Gauss, subconjunto dos números complexos $\mathbb{C}$, definido da seguinte forma $\mathbb{Z}[i] = \{ a + b\,i\,;\ a\,, b\ \in\ \mathbb{Z}\}$ é outro exemplo de anel, pois é munido das operações de $(+)$ e $(*)$:

$$(+)\ z_1\ +\ z_2\ =\ (a_1\ +\ b_1 i\ ) +\ (a_2\ +\ b_2 i\ ) =\ (a_1 +\ a_2) + (b_1\ +\ b_2)i$$

$$(*)\ z_1 * z_2 = (a_1 + b_1 i)\ *\ (a_2 + b_2 i) = (a_1 a_2 - b_1 b_2) + (a_1 b_2 + a_2 b_1)i$$

Propriedades 1.10 (**Divisibilidade em um Anel**): Sendo $a\ e\ b \in$ A, sendo A um anel, pode-se realizar as seguintes afirmações:

i. $a \mid a$ para todo $a\ \in$ A, $a \neq 0$
ii. Se $a \mid b$ e $b \mid a$, então $a = b$
iii. Se $a \mid b$ e $b \mid c$, então $a \mid c$
iv. Se $a \mid b$ e $b \mid c$, então $a \mid (b * x + c * y)$ para todo $x, y \in$ A

Diremos que d é um *divisor comum* de a e b, se: $d \mid a$ e $d \mid b$.

Convém mencionar que a "*operação de dividir*" é igual à usual, pois, no algoritmo da divisão, utilizam-se as operações de $(+)$ e $(*)$ presentes nos anéis.

Examinando os conjuntos dos divisores de dois números inteiros quaisquer, que podem ser tanto positivos como negativos, falar em **Máximo Divisor Comum (MDC)** é analisar se é possível determinar um divisor que seja comum aos inteiros dados e que apresente ainda um "valor máximo" no conjunto dos divisores comuns.

Para fins didáticos, serão apresentadas duas proposições de MDC para melhor fixação deste tópico.

Proposições 1.11 (MDC):

a) A primeira é: "dados dois números inteiros a e b (não simultaneamente nulos), o maior divisor comum ou o máximo divisor comum de a e b é denotado por $mdc\ (a,b)$, maior inteiro que divide a e b ao mesmo tempo. Esta proposição estende-se ainda aos elementos de um anel."

b) A segunda contém uma caracterização que possibilita uma abordagem de mais fácil manipulação para certas demonstrações. Enuncia-se assim: "sendo a e b inteiros, tem-se um inteiro positivo $d = mdc\ (a,b)$, se são válidas as seguintes condições":

$$i)\ \ d \mid a \ \text{ e } \ d \mid b; \text{ e}$$
$$ii)\ \ c \mid a \ \text{ e } \ c \mid b \implies c \mid d$$

A partir destas proposições, temos algumas afirmações com MDC:

$$mdc\ (0,a) = |a|,\ mdc\ (1,a) = 1 \ \text{ e } \ mdc\ (a,a) = |a|$$
$$mdc(a,b) = mdc(-a,b) = mdc(-a,-b) = mdc(a,-b)$$
$$mdc(c.a;\ c.b) = c.[mdc(a,b)]$$

Exemplo 1.12 – Mostrar que:

$a, b \in \mathbb{Z}$ e $mdc\ (a,b) = 1 \implies mdc\ (a+b, a-b) = 1$ ou 2

Seja $d = mdc\ (a+b, a-b)$. Então existem $k_1, k_2 \in \mathbb{Z}$, tais que:

$$\begin{cases} (1)\ a + b = k_1.d \\ (2)\ a - b = k_2.d \end{cases}$$

Tem-se ainda:

$$(*)\begin{cases}(1)+(2)\Longrightarrow\ 2a=\ (k_1+\ k_2).d\\ (1)-(2)\Longrightarrow\ 2b=\ (k_1-\ k_2).d\end{cases}$$

Sabe-se ainda que:

$$mdc\ (2a,2\ b)=2.\underbrace{mdc\ (a,b)}_{=1}=2(**)$$

De $(*)$ e $(**)$, segue que d divide simultaneamente:

$$(k_1+\ k_2).d\ \text{ e }\ (k_1-\ k_2).d$$

E ainda utilizando a *Proposição* 11.1 b), obtém-se*:*

$$d\mid 2\Longrightarrow\begin{cases}d=1\\ \text{ou}\\ d=2\end{cases}\blacksquare$$

Há também um outro importante tópico, que é o do **Mínimo Múltiplo Comum (MMC)** entre dois inteiros não nulos, que, em termos gerais, consiste na determinação do "menor valor positivo", escolhido no conjunto dos múltiplos comuns dos inteiros dados.

Proposição 1.13 (MMC): Sejam a e b inteiros não nulos, tem-se um inteiro positivo $m=mmc\ (a,b)$, se são válidas as seguintes condições:

$$i)\ a\mid m\ \ e\ \ b\mid m;\text{ e}$$
$$ii)\ a\mid c\ \ e\ \ b\mid c\Longrightarrow\ m\mid c$$

Propriedade 1.14 (**Relação entre MDC e MMC**): Se a e b são inteiros positivos, então $mmc\ (a,b).mdc\ (a,b)=a.b$.

Será realizada uma primeira aplicação de MDC e MMC no ensino básico. Na educação básica, costuma-se abordar, intuitivamente, o conceito de máximo divisor comum entre dois números inteiros, conforme exemplificado a seguir.

Exemplo 1.15 – Calcular o máximo divisor comum e o mínimo múltiplo comum entre 62 e 30. No ensino básico, em geral, realizam-se os seguintes passos para o exemplo proposto:

i. Achar os divisores de 62, assim denotados $D(62) = \{1, 2, 31, 62\}$

ii. Depois achar os de 30: $D(30) = \{1, 2, 3, 5, 6, 10, 15, 30\}$

iii. Com este procedimento, verifica-se que: $D(62) \cap D(30) = \{1, 2\}$ representa o conjunto dos divisores comuns de 62 e 30

iv. Conclui-se, assim, que o $mdc\ (62{,}30) = \max\ \{1{,}2\} = 2$

v. $mmc\ (62{,}30) = \frac{(62).(30)}{2} = 930$

Antes da segunda aplicação, será apresentado o **Lema de Euclides**, importante conceito para o entendimento do mecanismo utilizado no **Algoritmo de Euclides**.

Lema 1.16 (**Lema de Euclides**): Se $a, b, n \in \mathbb{Z}$, então $mdc\ (a, b) = mdc\ (a, b - na)$.

Prova: Seja $c = mdc\ (a, b)$ e $d = mdc\ (a, b - na)$.

Tem-se que:

$$\left.\begin{array}{l} d = mdc\ (a, b - na) \Longrightarrow d \mid a \text{ e } d \mid (b - na) \\ d \mid (b - na) \Longrightarrow d \mid b;\ b = (b - na) + na \end{array}\right\} \Longrightarrow$$

$$\Longrightarrow d \mid a \text{ e } d \mid b$$

$$\Longrightarrow d \mid c$$

Também se afirma que:

$$c = mdc\ (a, b) \Longrightarrow c \mid a \text{ e } c \mid b$$

$$\Longrightarrow c \mid a \text{ e } c \mid (b - na)$$

$$\Longrightarrow c \mid d$$

Sendo c e d ambos inteiros positivos, então: $c = d$. ■

A segunda aplicação consiste na utilização do **Algoritmo de Euclides** para o cálculo do MDC. No ensino básico, explora-se também o Algoritmo de Euclides como um método de cálculo do máximo divisor comum.

Primeiramente, vamos mostrar a base teórica deste método de MDC e depois vamos aplicá-lo com um exemplo.

Se a e $b \in \mathbb{Z}$, então existem $q_1, r_1 \in \mathbb{Z}$ tal que $b = aq_1 + r_1$. Do Lema de Euclides, verifica-se:

$$mdc\,(a,b) = mdc\,(a,(b - aq_1)) = mdc\,(a,r_1)$$

De forma análoga, para a e r_1 existem $q_2, r_2 \in \mathbb{Z}$ tal que $a = r_1q_2 + r_2$ e verifica-se ainda:

$$mdc\,(r_1,a) = mdc\,(r_1,(a - r_1q_2)) = mdc\,(r_1,r_2)$$

Logo: $mdc\,(a,b) = mdc\,(a,r_1) = mdc\,(r_1,r_2)$

Note que se trata de um método recursivo, pois, a partir da primeira divisão, vão se efetuando novas divisões entre o "antigo divisor" e o "resto anterior" até que se obtenha o último e menor resto não nulo, que será o resultado do $mdc\,(a,b) = r_n$. O $mdc\,(a,b)$ será sempre o último resto não nulo. Este procedimento é chamado de *Algoritmo de Euclides* ou "*Método das Divisões Sucessivas*".

O Algoritmo de Euclides esquematiza-se no seguinte dispositivo prático:

	q_1	q_2	$\cdots$	q_n	q_{n+1}
a	b	r_1	$\cdots$	r_{n-1}	r_n
r_1	r_2	r_3	$\cdots$	$r_{n+1} = 0$	

Exemplo 1.17 – Seja a $= 82$ e b $= 30$. Calculando os restos de cada um dos valores do mdc e aplicando-se o Lema de Euclides, tem-se:

$$mdc\,(82,30) = mdc\left(30, \overbrace{(82 - 2.30)}^{r_1 = 22}\right) = mdc\,(30,22)$$

$$mdc\,(30,22) = mdc\left(22, \overbrace{(30 - 1.22)}^{r_2 = 8}\right) = mdc\,(22,8)$$

$$mdc\,(22,8) = mdc\left(8, \overbrace{(22 - 2.8)}^{r_3 = 6}\right) = mdc\,(8,6)$$

$$mdc\,(8,6) = mdc\left(6, \overbrace{(8 - 1.6)}^{r_4 = 2}\right) = \overbrace{mdc\,(6,2) = 2}^{r_5 = 0}$$

A aplicação direta do Algoritmo de Euclides no exemplo é:

	$q_1 = 2$	$q_2 = 1$	$q_3 = 2$	$q_4 = 1$	$q_5 = 3$
$a = 82$	$b = 30$	$r_1 = 22$	$r_2 = 8$	$r_3 = 6$	$r_4 = 2$
$r_1 = 22$	$r_2 = 8$	$r_3 = 6$	$r_4 = 2$	$r_5 = 0$	

Teorema 1.18 (**Teorema de Bézout**): Se $d = mdc\ (a, b)$ então existem $k_1, k_2 \in \mathbb{Z}$ tal que $d = k_1.a + k_2.b$.

Prova: Seja $B = \{m.a + n.b;\ m, n \in \mathbb{Z}\}$.

Pelo PBO (aplicado ao subconjunto de B formado por naturais), existe um $c \in$ B, menor inteiro positivo, de modo que $c = k_1.a + k_2.b$ com $k_1, k_2 \in \mathbb{Z}$.

Suponha, por absurdo, que c não divida a.

Então, existem $q, r \in \mathbb{Z}$, tal que $a = q.c + r$ com $0 < r < c$.

Logo: $r = a - q.c = a - q.(k_1.a + k_2.b) = (1 - q.k_1).a + (-q.k_2).b$

Então, $r \in B$ (absurdo), pois $0 < r < c$ e c é menor inteiro positivo de B.

Como $d = mdc(a, b)$, temos que *d* é divisor comum de *a* e *b*.

Assim: $a = w_1.d$ e $b = w_2.d \Rightarrow c = k_1.a + k_2.b = k_1.(w_1.d) + k_2.(w_2.d) \Rightarrow d \mid c$.

Como d e c são positivos, temos $d \leq c$. Mas como $d < c$ não é possível pois d é o maior divisor comum de a e b, então:

$$\begin{cases} d = c \\ d = k_1.a + k_2.b \end{cases} \blacksquare$$

Corolário 1.19: Se c divide a e b e $d = mdc(a, b)$, então c divide d.

Prova: Seja $d = mdc(a, b)$. Pelo Teorema de Bézout, tem-se que $d = k_1.a + k_2.b$ com $k_1, k_2 \in \mathbb{Z}$.

Como $c \mid a$ e $c \mid b$, temos que $d = k_1.(w_1.c) + k_2.(w_2.c)$ com $w_1, w_2 \in \mathbb{Z}$.

Logo: $c \mid d$.■

Definição 1.20 (*primos*): Diremos que os números inteiros p, maiores que 1 e com ± 1 e $\pm p$ como os seus únicos possíveis divisores, são denominados *números primos*. Se um número não é primo, ele é dito composto.

Definição 1.21 (*primos entre si*): Dois números inteiros a e b são primos entre si se o $mdc\ (a, b) = 1$.

Exemplo 1.22: São inteiros primos entre si os números 2 e 3; 3 e 5; 7 e -11, pois, em relação ao MDC, afirma-se que $1 = mdc\ (2,3) = mdc\ (3,5) = mdc\ (7,-11)$.

Proposição 1.23: *O conjunto dos números primos é infinito*.

Prova: Euclides supôs que a sucessão $p_1 = 2,\ p_2 = 3, \ldots, p_r$ dos r números primos é finita. Assim, considera-se $P\ =\ p_1\ .p_2\ \ldots p_r + 1$ e seja p um número primo que divide P. Esse número não pode ser igual a qualquer um dos números $p_1, p_2, \ldots, p_r$ porque, deste modo, 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 consequência, $p_1, p_2, \ldots, p_r$ não podem formar o conjunto de todos os números primos. ■

Teorema 1.24 (**Teorema Fundamental da Aritmética – TFA**): Todo inteiro $a > 1$ ou é primo ou se escreve, de maneira única e a menos da ordem dos fatores, como um produto de números primos".

Prova (**por indução**): Se $n = 2$, o resultado é obviamente verificado. Suponhamos o resultado valido para todo número inteiro menor do que n e vamos provar que vale para n.

Se o número n é primo, nada temos a demonstrar.

Suponhamos, então, que n seja composto. Logo, existem números inteiros positivos n_1 e n_2 tais que:

$$n = n_1.n_2 \text{ com } 1 < n_1 < n \text{ e } 1 < n_2 < n.$$

Pela hipótese de indução, temos que existem números primos:

$$p_1, \ldots, p_r \text{ e } q_1, \ldots, q_s, \text{ tais que: } n_1 = p_1 \ldots p_r \text{ e } n_2 = q_1 \ldots q_s.$$

Portanto, $n = n_1.n_2 = p_1 \ldots p_r.q_1 \ldots q_s$.

Vamos agora provar a unicidade da escrita.

Suponha que tenhamos $n = p_1 \ldots p_r = q_1 \ldots q_s$, onde os p_1 e os q_j são números primos.

Como $p_1 \mid q_1 \ldots q_s$, temos que $p_1 = q_j$ para algum j, que, após reordenamento de $q_1, \ldots, q_s$, podemos supor que seja q_1.

Portanto: $p_2 \ldots p_r = q_2 \ldots q_s$.

Como $p_2 \ldots p_r < n$, a hipótese de indução acarreta que $r = s$ e os p_i e q_j são iguais aos pares. ■

Será apresentada uma definição para **Relação de Equivalência**. Uma relação de equivalência representa uma "espécie de generalização" da relação de igualdade, pois elementos de um dado conjunto, mesmo distintos, podem vir a cumprir um papel equivalente.

Definição 1.25 (**Relação de Equivalência**) – Para que uma relação entre elementos em um conjunto A seja definida como *Relação de Equivalência* (~), as seguintes condições devem ser sempre satisfeitas:

i. (*Reflexividade*) $x \sim x;\ \forall x \in A$.
ii. (*Simetria*) $x \sim y \Longrightarrow y \sim x;\ \forall x, y \in A$.
iii. (*Transitividade*) $x \sim y$ e $y \sim z \Longrightarrow x \sim z;\ \forall x, y, z \in A$.

Observação: Define-se por $\overline{x}$ a **classe de equivalência** do elemento x de A em relação a (~) da seguinte forma:

$$\overline{x} = \{a \in \mathrm{A};\ a \sim x\}$$

Definição 1.26 (**Congruências nos inteiros**) – Sendo n um número natural maior que um, verificam-se a seguintes possíveis relações de congruência entre os inteiros a e b:

i. a é dito *congruente* (módulo n) a b, denotando-se:
$$a \equiv b\ (mod\ n) \ \Leftrightarrow\ n \mid (a - b)$$
ii. a é dito *incongruente* (módulo n) a b, denotando-se:
$$a \not\equiv b\ (mod\ n) \ \Leftrightarrow n \nmid (a - b)$$

Observações: O símbolo: $\equiv$ representa uma relação de congruência. Na aritmética modular módulo n, tem-se que o n foi identificado com a classe residual zero, ou seja, $n \equiv 0\ (mod\ n)$ ou ainda $\bar{n} = \bar{0}$. O conjunto quociente de $\mathbb{Z}$ é denotado por:

$$\mathbb{Z} / \sim = \mathbb{Z}_n = \{\overline{a};\ a \in \mathbb{Z}\}$$
$$\overline{a} = \{a + k.n; k \in \mathbb{Z}\}$$
$$\mathbb{Z}_n = \{\bar{0}, \bar{1}, \bar{2}, \ldots \overline{n-1}\}$$

E ainda:

$$\overline{a} = \overline{b} \in \mathbb{Z}_n \Leftrightarrow (a-b) \equiv 0\ (mod\ n) \Leftrightarrow \underbrace{a = b + kn}_{k \in \mathbb{Z}}$$

Exemplo 1.27: $7 \equiv 4\ (mod\ 3)$, pois $3 \mid (7-4)$. Este resultado é assegurado porque 7 e 4 têm o mesmo resto na divisão por 3: $7 = 2.3 + 1$ e $4 = 1.3 + 1$. Portanto, nesta relação de congruência (e também de equivalência), 7 e 4 estão na mesma classe de equivalência: $\overline{7} = \overline{4}$.

Proposição 1.28 – Propriedades das congruências ($a, b, n, k \in \mathbb{Z}$ e $n, k > 1$):

i. $a \equiv b\ (mod\ n)$ e $c \equiv d\ (mod\ n) \Leftrightarrow (a \pm c) \equiv (b \pm d)\ (mod\ n)$

ii. $a \equiv b\ (mod\ n)$ e $c \equiv d\ (mod\ n) \Leftrightarrow (a.c) \equiv (b.d)(mod\ n)$

iii. $a \equiv b\ (mod\ n) \Leftrightarrow a^k \equiv b^k\ (mod\ n)$

iv. $ac \equiv bc\ (mod\ n)$ e $mdc\ (c, n) = d \Leftrightarrow a \equiv b\ \left(mod\ \left(\frac{n}{d}\right)\right)$

Observação: Garante-se a aplicação destas propriedades, pois o anel $(\mathbb{Z}_n, +, *)$ é definido da seguinte forma: $\mathbb{Z}_n = \{\overline{a};\ a \in \mathbb{Z}\}$ com $\overline{a} = \{a + k.n; k \in \mathbb{Z}\}$.

Exemplo 1.29: Encontre o resto da divisão de 237^{28} por 13.

$$237 \equiv 3\ (mod\ 13) \Leftrightarrow 237^4 \equiv 3^4 = 81 \equiv 3\ (mod\ 13)$$

$$237^{12} = (237^4)^3 \equiv (3^4)^3 \equiv 3^3 = 27 \equiv 1\ (mod\ 13)$$

$$237^{28} = (237^{12})^2.237^4 \equiv 1^2.3 = 3\ (mod\ 13)$$

De fato, $(237^{28} - 3)$ é um número divisível por 13, ou seja, existe um inteiro k, tal que:

$$(237^{28} - 3) = 13k \Longrightarrow 237^{28} = 13k + 3$$

Logo, a divisão de 237^{28} por 13 apresenta resto 3

Pode-se verificar que, a partir das propriedades das congruências, várias manipulações aritméticas podem ser feitas para obtenção de restos de certas potências.

Definição 1.30 (**Sistema Completo de Resíduos Módulo n** – SCRM (n)): Para um conjunto de inteiros $\{r_1, r_2, \ldots r_n\}$, tem-se um SCRM (n), se:

a) $r_i \not\equiv r_j \ (mod\ n)$ para $i \neq j$; e
b) considerando $k \in \mathbb{Z}$, existe um r_i tal que $r_i \equiv k(mod\ n)$, denominado resíduo de k módulo n.

Exemplo 1.31: Para $n = 6$, tem-se que os seguintes conjuntos formam *Sistemas Completos de Resíduos Módulo 6*:

$$\{0, 1, 2, 3, 4, 5\}; \{19, 18, 17, 16, 15, 14\}; \text{e } \{-22, -32, -60, 9, -53, 47\}$$

Definição 1.32 (**Função ϕ de Euler**): A função ϕ de um inteiro n $(n \geq 1)$ é denotada por $\phi(n)$ e representa o número de inteiros positivos, menores ou iguais a n e primos com n, onde se tem: $\phi(n) = \#\{m \in \mathbb{N}; 1 \leq m \leq n \ e \ \text{mdc}(m, n) = 1\}$.

Exemplos 1.33 – Temos que: $\phi(6) = \#\{1, 5\} = 2$; $\phi(7) = \#\{1, 2, 3, 4, 5, 6\} = 6$; e $\phi(8) = \#\{1, 3, 5, 7\} = 4$.

Definição 1.34 (**Sistema Reduzido de Resíduos Módulo n –** SRRM (n)): Pode-se dizer que o SRRM (n) é um conjunto constituído por alguns elementos de SCRM (n). Assim, o SRRM (n) trata-se de um conjunto com $\phi(n)$ inteiros, assim representados: $\{r_1, r_2, \ldots r_{\phi(n)}\}$, de modo que temos:

a) $r_i \in$ SCRM (n); e
b) $mdc\ (r_i, n) = 1$ para cada $i = 1, 2, \ldots, \phi(n)$.

Exemplo 1.35: $\{0, 1, 2, 3, 4, 5, 6, 7\}$ representa um dos possíveis *Sistemas Completos de Resíduos Módulo 8*. Considerando apenas os elementos do conjunto anterior, que são relativamente primos com 8, temos: $\{1, 3, 5, 7\}$, subconjunto que representa um dos possíveis *Sistemas Reduzidos de Resíduos Módulo 8*. Escolhendo um número, como 9, onde: $mdc\ (8, 9) = mdc\ (2^3, 3^2) = 1$, pode-se construir um novo conjunto da seguinte forma: $\{1x9, 3x9, 5x9, 7x9\} = \{9, 27, 45, 63\}$, que representa um outro *Sistema Reduzido de Resíduos Módulo* 8.

Lema 1.36 (**Lema para o Pequeno Teorema de Fermat**): Se p é primo, então p divide $\mathrm{C}_{p,i}$, para $0 < i < p$.

Prova: Temos que

$$\mathrm{C}_{p,i} = \frac{p!}{i!\,(p-i)!} = \frac{p.(p-1)\ldots(p-i+1)}{i!} \in \mathbb{N}$$

Como $0 < i < p$, temos que todos os fatores irredutíveis de $i!$ são estritamente menores do que p. Assim:

$i! \mid p.(p-1).(p-2)\ldots(p-i+1)$ e sendo p um primo, então

$i! \mid (p-1).(p-2)\ldots(p-i+1)$

$\therefore (p-1)\ldots(p-i+1) = m_i.i!$ com $m_i \in \mathbb{N}$.

Logo, $\mathrm{C}_{p,i} = p.m_i \Longrightarrow p \mid \mathrm{C}_{p,i}$. ■

Teorema 1.37 (**Pequeno Teorema de Fermat – PTF**): Se p é primo e a é um inteiro positivo, então:

$$a^p \equiv a\ (mod\ p)$$

Prova: Utilizemos indução sobre a.

1º) $a = 1 \Rightarrow (1^p - 1) = 0.p$

2º) Suponha verdadeiro: $a = k \Rightarrow (k^p - k) = c.p \quad com\ c \in \mathbb{Z}$

3º) Vamos mostrar que vale para $a = k + 1$, isto é,

$$(k+1)^p - (k+1) = d.p \ \ com\ d \in \mathbb{Z}$$

Com efeito, segue da fórmula binomial e do Lema anterior, que:

$$(k+1)^p = k^p + \underbrace{C_p^1.k^{p-1}.1 + \cdots + C_p^p.k.1^{p-1}}_{m.p\ ,\ m\in\mathbb{N}} + 1^p$$

Subtraindo $(k+1)$ em ambos os termos da igualdade, tem-se:

$$(k+1)^p - (k+1) = k^p + mp + 1 - (k+1)$$

Pela hipótese de indução (2º) temos:

$$(k+1)^p - (k+1) = \underbrace{k^p - k}_{c.p} + mp = (c+m)p$$

Portanto, $p \mid (k+1)^p - (k+1)$. ■

Note ainda que: $\overbrace{(x \pm y)^p \equiv x^p \pm y^p}^{(x\pm y)^p = x^p + (\pm y)^p + k.p} \equiv x \pm y \ (mod\ p)$ com p primo, pois:

$$\begin{cases} (x \pm y)^p \equiv x^p \pm y^p \ (mod\ p) \\ x^p \equiv x \ (mod\ p) \\ y^p \equiv y \ (mod\ p) \end{cases}$$

Corolário 1.38 (**Corolário do PTF**): Se p é primo, a é um inteiro positivo e $p \nmid a$, então:

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

Prova: Sendo k_1 e k_2 inteiros, segue, do PTF, que:

$$(a^p - a) = a.(a^{p-1} - 1) = k_1 p \quad \overbrace{\Rightarrow}^{mdc\ (a,p) = 1} \quad (a^{p-1} - 1) = k_2 p. \blacksquare$$

Assim, resumindo o *Teorema e o seu Corolário*, são válidas as afirmações:

i. Se $a,\ p \in \mathbb{Z}$ com p primo, então $a^p \equiv a\ (mod\ p)$.

ii. Se p é primo e $mdc\ (a,p) = 1$, então $a^{p-1} \equiv 1\ (mod\ p)$.

Exemplo 1.39: Calcule o resto da divisão de 3^{1003} por 101. Sabe-se que 101 é um número primo e que $101 \nmid 3$, o que implica que $mdc\ (3, 101) = 1$. Assim, pode-se aplicar o Corolário do PTF ($a^{p-1} \equiv 1\ (mod\ p)$), onde se tem:

$$3^{(101-1)} \equiv 1\ mod\ 101 \therefore 3^{100} \equiv 1\ mod\ 101$$

Pode-se afirmar também:

$$\begin{cases} 3^{1000} = (3^{100})^{10} \equiv 1^{10} \equiv 1\ (mod\ 101) \\ 3^3 = 27\ (mod\ 101) \\ 3^{1003} = (1).(27) = 27\ (mod\ 101) \end{cases}$$

Portanto, o resto da divisão de 3^{1003} por 101 é 27.

Teorema 1.40 (**Teorema de Euler**): Se a e n são inteiros positivos com $n > 1$, tais que, se $mdc\ (a,n) = 1$, então:

$$a^{\phi(n)} \equiv 1\ (mod\ n)$$

Ideia da prova com um exemplo numérico:

Pensando nos argumentos da demonstração do Corolário do PTF, verificar se existe um inteiro positivo k, tal que $5^k \equiv 1\ (mod\ 8)$. Sabe-se que $mdc\ (5,8) = 1$ e que

$\{5, 15, 25, 35\}$ é um *sistema reduzido de resíduos módulo 8* com todos os seus elementos sendo congruentes a exatamente um elemento do conjunto $\{1, 3, 5, 7\}$. Pode-se verificar:

$$\left.\begin{array}{l} 1.5 \equiv 5\ (mod\ 8) \\ 3.5 \equiv 7\ (mod\ 8) \\ 5.5 \equiv 1\ (mod\ 8) \\ 7.5 \equiv 3\ (mod\ 8) \end{array}\right\} \Longrightarrow \underbrace{(1.3.5.7).5^4 \equiv 1.3.5.7\ (mod\ 8)}_{mdc((1.3.5.7),8)=1} \Longrightarrow 5^4 \equiv 1\ (mod\ 8)$$

Logo, $k = \phi(8) = 4$ e $5^{\phi(8)} \equiv 1\ (mod\ 8)$ ■

Prova: Considere o sistema reduzido de resíduos módulo n por:

$$\{r_1, r_2, \dots, r_{\phi(n)}\} \subseteq \{0,1,2, \dots, n-1\}$$

Segue que $\{a.r_1, \dots, a.r_{\phi(n)}\}$ é um sistema reduzido de resíduos e, assim, cada elemento deste conjunto é congruente a um único elemento de: $\{r_1, \dots, r_{\phi(n)}\}$.

Desse modo:

$$a.r_1 \dots a.r_{\phi(n)} \equiv r_1 \dots r_{\phi(n)}\ (mod\ n) \Longrightarrow a^{\phi(n)}.\prod_{i=1}^{\phi(n)} r_i \equiv \prod_{i=1}^{\phi(n)} r_i\ (mod\ n)$$

Sendo $mdc\left(\prod_{i=1}^{\phi(n)} r_i, n\right) = 1$, tem-se que: $a^{\phi(n)} \equiv 1\ (mod\ n)$. ■

Observação: O Corolário do PTF é um caso particular do Teorema de Euler, pois se p for primo, temos que $\phi(p) = p - 1$ e, portanto: $a^{p-1} \equiv 1\ (mod\ p)$.

Lema 1.41: Seja p um inteiro primo. Sabe-se que os únicos elementos do conjunto $\{1, 2, \dots, p-1\}$ que satisfazem a equação quadrática $x^2 \equiv 1\ (mod\ p)$ são os elementos 1 e $p-1$.

Prova: Com efeito, se $a \in \{1, 2, \dots, p-1\}$ é tal que:

$$a^2 \equiv 1\ mod\ p \Rightarrow p \mid (a^2 - 1) = (a-1)(a+1)$$

Como p é primo, segue que:

$$p \mid (a-1)\ \ ou\ \ p \mid (a+1)$$

Equivalente a $a \equiv 1\ mod\ p$ ou $a \equiv -1 \equiv (p-1)\ (mod\ p)$

Como $a \in \{1, 2, \dots, p-1\}$, segue que $a = 1$ ou $a = (p-1)$. ■

Teorema 1.42 (**Teorema de Wilson**): Se p é primo, então:

$$(p-1)! \equiv -1(mod\ p)$$

Prova: Conforme Santos (2015), serão utilizados os seguintes resultados, demonstrados no livro **"***Introdução à Teoria dos Números*":

i. A congruência $a.x \equiv 1\ (mod\ p)$ admite única solução para $a \in \{1, \ldots, p-1\}$.

ii. Somente $a = 1$ e $a = (p-1)$ satisfazem a equação $x^2 \equiv 1\ (mod\ p)$.

Assim, segue das duas afirmações anteriores que, para quaisquer números $a, b \in \{2, \ldots, p-2\}$ com $a \neq b$, existe a seguinte relação:

$$a.b \equiv 1\ (mod\ p)$$

Fazendo o produto dos elementos, aos pares, com a propriedade anterior, temos:

$$2 \ldots . (p-2) \equiv 1\ (mod\ p)$$

$$(p-1) \equiv -1\ (mod\ p) \Longrightarrow\ 2 \ldots . (p-2)(p-1) \equiv -1\ (mod\ p)$$

$$\Longrightarrow (p-1)!\ \equiv -1\ (mod\ p). \blacksquare$$

Exemplo 1.43: A exemplificação numérica a seguir contém a ideia da demonstração do Teorema de Wilson. Considere um primo $p = 11$. Conforme o Lema anteriormente enunciado, os únicos elementos do conjunto: $\{1, 2, 3, \ldots, 9, 10\}$ que satisfazem a equação: $x^2 \equiv 1\ mod\ 11$ são 1 e $10 \equiv -1\ mod\ 11$. De fato: $(1)^2 \equiv (-1)^2 \equiv 1\ mod\ 11$. Pode-se verificar:

$$\left.\begin{array}{l} 2.6 \equiv 12 \equiv 1\ mod\ 11 \\ 3.4 \equiv 12 \equiv 1\ mod\ 11 \\ 5.9 \equiv 45 \equiv 1\ mod\ 11 \\ 7.8 \equiv 56 \equiv 1\ mod\ 11 \end{array}\right\} \Longrightarrow 9! \equiv (1)^4 \equiv 1\ mod\ 11$$

A congruência $ax \equiv 1\ mod\ 11$ é verificada na relação:

$$2.6 \equiv 3.4 \equiv 5.9 \equiv 7.8 \equiv 1\ mod\ 11$$

Finalmente, como se tem que $9! \equiv 1\ mod\ 11$ e $10 \equiv -1\ mod\ 11$, conclui-se o seguinte:

$$10! \equiv -1\ mod\ 11$$

Proposição 1.44 (**Binômio de Newton**): Sejam a e b inteiros e $n \in \mathbb{N}$, então $(a+b)^n = \sum_{k=0}^{n} \mathrm{C}_{n,k}.\, a^{n-k}.\, b^k$. Esta proposição pode ser provada por indução.

A partir dela, desenvolve-se o **Triângulo Aritmético de Tartaglia e Pascal**, que se refere a uma série de números binomiais, coeficientes dos Binômios de Newton. Para construí-lo, associam-se os coeficientes $\mathrm{C}_{1,0}$ e $\mathrm{C}_{1,1}$ do binômio $(a+b)^1$ à primeira linha e, assim, sucessivamente, até os coeficientes do binômio $(a+b)^n$, escritos na *n*-ésima. Verifica-se, portanto, um padrão, no qual os números, a partir da segunda linha e de cima para baixo, podem ser calculados pela soma dos dois acima dele, excetuando-se os números da forma $\mathrm{C}_{k,0}$ e $\mathrm{C}_{k,k}$. Segue a construção deste **Triângulo Aritmético** até o expoente 5:

$$(a+b)^1 = a+b$$
$$(a+b)^2 = a^2+2ab+b^2$$
$$(a+b)^3 = a^3+3a^2b+3ab^2+b^3$$
$$(a+b)^4 = a^4+4a^3b+6a^2b^2+4ab^3+b^4$$
$$(a+b)^5 = a^5+5a^4b+10a^3b^2+10a^2b^3+5ab^4+b^5$$

1.3 Estruturas Algébricas

Definição 1.45 (**Domínio ou Domínio de Integridade**): Diremos que um anel $(\mathrm{A}, +, *)$ comutativo e com unidade trata-se de um Domínio ou Domínio de Integridade quando apresentar a seguinte propriedade para os seus elementos, de forma que, para $a, b \in \mathrm{A}$, tem-se:

$$a * b = 0_{\mathrm{A}} \Longrightarrow a = 0_{\mathrm{A}} \text{ ou } b = 0_{\mathrm{A}} \text{ (“}\textit{anel sem divisores de zero}\text{”)}$$

Exemplos 1.46: O anel dos inteiros $(\mathbb{Z}, +, *)$ é um domínio, bem como os números racionais $(\mathbb{Q}, +, *)$, os números reais $(\mathbb{R}, +, *)$ e os complexos $(\mathbb{C}, +, *)$. Todos estes são munidos com suas duas operações: $(+)$ e $(*)$. Note que $(\mathbb{Z}_5, +, *)$ é um domínio e que $(\mathbb{Z}_6, +, *)$ não é. Apenas este último apresenta divisores de zero.

Definição 1.47 (**Corpo**): Diremos que um domínio $(\mathrm{A}, +, *)$ é um corpo quando possuir a seguinte propriedade adicional para todos os elementos $a \in \mathrm{A}$ com $a \neq 0$:

$$\text{Existe } b \in A, \text{ tal que } a * b = 1_{\mathrm{A}}$$

Exemplos 1.48: $(\mathbb{Q}, +, *)$, $(\mathbb{R}, +, *)$ e $(\mathbb{C}, +, *)$ são corpos.

Observações:

i. Todo corpo é um *domínio de integridade*.

ii. $\mathbb{Q} = \left\{ \frac{p}{q} \in \mathbb{Z} \text{ e } q \neq 0 \right\}$

iii. $\mathbb{Z}_p$ é corpo $\Leftrightarrow$ p é primo

Definições 1.49 (**unidade e elemento inverso**): Seja A um anel. Diremos que $a \in \mathrm{A}$ é uma unidade ou é inversível se existe $b \in \mathrm{A}$, tal que $a * b = 1_{\mathrm{A}}$ e, neste caso, diremos que b é o *elemento inverso* ou *inverso multiplicativo* de a.

Definição 1.50 (**elemento irredutível**): Sendo A um domínio com $a,\ b$ e $p \in \mathrm{A}$, um elemento p será irredutível em A, observando-se:

$$p = (a * b) \Longrightarrow a \text{ é } \textit{unidade} \text{ em A ou } b \text{ é } \textit{unidade} \text{ em A.}$$

Definição 1.51 (**elemento primo**): Sendo A um domínio com a, b e $p \in$ A, um elemento p será primo em A, verificando-se:

$$p \mid (a * b) \Longrightarrow p \mid a \text{ ou } p \mid b$$

Proposição 1.52 – Relaciona primos e irredutíveis. Sendo $(\mathrm{A}, +, *)$ um domínio:

"Se p *é primo em* A, *então* p *é irredutível em* A"

Prova: Vamos mostrar que

$$p = (a * b) \Longrightarrow a \text{ é } unidade \text{ em A ou } b \text{ é } unidade \text{ em A.}$$

$$p = (a * b) \Longrightarrow \underbrace{p \mid (a * b) \Longrightarrow p \mid a \text{ ou } p \mid b}_{Da\ hipótese:\ p\ é\ primo\ em\ A}$$

Divide-se a prova nos casos a seguir:

Caso 1: $p \mid a$ para algum $k_1 \in \mathbb{Z}$

$$p \mid a \Longrightarrow a = (k_1 * p)$$

$$p = \underbrace{(a * b) = (k_1 * p) * b}_{a = (k_1 * p)}$$

$$\Longrightarrow p - (k_1 * b) * p = 0 \Longrightarrow p * (1 - k_1 * b) = 0$$

Como A é domínio e $p \neq 0$, segue que:

$$(1 - k_1 * b) = 0 \implies k_1 * b = 1_{\mathrm{A}} \implies b \text{ é } unidade.$$

Caso 2: $p \mid b$ para algum $k_2 \in \mathbb{Z}$

$$p \mid b \Longrightarrow b = (k_2 * p)$$

$$p = \underbrace{(a * b) = a * (k_2 * p)}_{b = (k_2 * p)}$$

$$\Longrightarrow p - (a * k_2) * p = 0 \Longrightarrow p * (1 - a * k_2) = 0$$

Analogamente:

$$(1 - a * k_2) = 0 \implies a * k_2 = 1_{\mathrm{A}} \implies a \text{ é } unidade. \blacksquare$$

Temos ainda que a recíproca do resultado anterior é falsa, isto é, em um domínio A:

"*Um elemento* p *irredutível em A não implica que* p *seja primo em A*"

De fato, basta considerar o seguinte domínio como exemplo:

$$A = \mathbb{Z}\left[i\sqrt{5}\right] = \{\, a + bi\sqrt{5} \;; a, b \in \mathbb{Z} \,\}$$

Neste domínio, o elemento 6 pode ser escrito de duas formas distintas em um produto de elementos irredutíveis:

$$6 = 2.3 = \left(1 + i\sqrt{5}\ \right)\left(1 - i\sqrt{5}\right)$$

Sabe-se que 2 é um elemento irredutível em $A = \mathbb{Z}\left[i\sqrt{5}\ \right]$ e ainda que:

i. Divide $\left(1 + i\sqrt{5}\ \right).\left(1 - i\sqrt{5}\right) = 6$

ii. Não divide $\left(1 + i\sqrt{5}\ \right)$

Caso 2 dividisse $\left(1 + i\sqrt{5}\right)$, então existiria um elemento $\left(a + bi\sqrt{5}\right)$ tal que:

$$\left(1 + i\sqrt{5}\right) = 2.\left(a + bi\sqrt{5}\right)$$

Deste modo, teríamos: $\left(1 + i\sqrt{5}\right) = 2a + 2bi\sqrt{5}$.

Portanto:

$$\begin{cases} 2a = 1 \Longrightarrow a = \frac{1}{2} \notin \mathbb{Z} \\ \\ 2b = 1 \Rightarrow b = \frac{1}{2} \notin \mathbb{Z} \end{cases}$$

Analogamente, 2 não divide $\left(1 - i\sqrt{5}\right)$.

Assim, pela definição de primo, conclui-se que 2 não é um elemento primo em $A = \mathbb{Z}\left[i\sqrt{5}\ \right]$.

Definição 1.53 (**Domínio de Fatoração Única – DFU**): Um domínio A é chamado de DFU, se todo elemento não nulo e não inversível de A pode ser escrito de maneira única, a menos da ordem, como um produto de elementos irredutíveis. Engloba, assim, um conceito também construído para aplicação nas provas de casos particulares do Último Teorema de Fermat.

Exemplos 1.54: Considerando a definição anterior, tem-se que $A = \mathbb{Z}\left[\ i\sqrt{5}\right]$ não é um DFU, pois, por exemplo, o elemento 6 tem duas fatorações distintas em elementos irredutíveis em A. Contudo, verificando-se os elementos de $A = \mathbb{Z}$, conclui-se que se trata de um DFU.

Proposição 1.55 – Seja A um DFU, então vale a seguinte relação:

" p *é irredutível em A, se e somente se,* p *é primo em A*"

Prova: (⇐) Já provado anteriormente

(⇒) Seja p irredutível em A.

Supondo que p divide $a * b$ e que p não divide a, vamos mostrar que p divide b. Assim, como p divide $a * b$, segue que $a * b = p * k$ e como p é irredutível e p não divide a, segue que p aparece na fatoração de b. Portanto, p divide b e, consequentemente, p é primo em A. Na suposição de que p não divide b, a prova seria análoga. ■

Definição 1.56 (Anéis de Inteiros Quadráticos $\mathbb{Z}[\sqrt{\mathbf{n}}]$): Seja $n \neq 0$ e $n \neq 1$ um inteiro livre de quadrados, define-se $\mathbb{Z}[\sqrt{n}]$ como o seguinte subanel de $\mathbb{C}$: $\mathbb{Z}[\sqrt{n}] = \{a + b\sqrt{n} \mid a, b \in \mathbb{Z}\}$.

Exemplos 1.57 – Temos que:

i. $\mathbb{Z}[i]$, caso em que $n = -1$, o Anel de Inteiros de Gauss.

ii. $\mathbb{Z}[\sqrt{5}] = \{a + b\sqrt{5} \mid a, b \in \mathbb{Z}\}$.

Observações:

$\mathbb{Q}[\sqrt{n}] = \{a + b\sqrt{n} \mid a, b \in \mathbb{Q}\}$ representa os *Anéis dos Corpos Quadráticos*.

O *estudo aritmético* de $\mathbb{Z}[\sqrt{\mathrm{n}}]$ necessita do *conceito da norma* de um elemento deste anel.

Definição 1.58 (**Norma de um elemento do anel $\mathbb{Z}[\sqrt{\mathbf{n}}]$**): Se $\delta = a + b\sqrt{n} \in \mathbb{Z}[\sqrt{n}]$, então a norma de δ, denotada por $N(\delta)$, fica assim determinada:

Função Norma – $N: \mathbb{Z}[\sqrt{n}] \longrightarrow \mathbb{Z}$, definida para todo $\delta = a + b\sqrt{n}$, onde se tem $N(\delta) = \delta.\bar{\delta} = \overbrace{(a + b\sqrt{n})}^{=\delta}.\overbrace{(a - b\sqrt{n})}^{=\bar{\delta}} = (a^2 - b^2 n)$, sendo $\bar{\delta}$ o conjugado de δ.

Proposição 1.59 – *Propriedades da Norma*:

i. $N(\delta) = 0 \Leftrightarrow \delta = 0$

ii. $N(\delta.\beta) = N(\delta).N(\beta)$

iii. $N(1) = 1$

iv. $N(\delta) = \pm 1 \Leftrightarrow \delta$ é inversível

v. $N(\delta) = p$ (primo) $\Longrightarrow \delta$ é um irredutível em $\mathbb{Z}\left[\sqrt{n}\,\right]$

Provas: Em relação aos itens i), ii) e iii), a prova é imediata pela definição de Norma.

Em relação ao item iv): tome $N(\delta) = a^2 - b^2 n = \pm 1$.

Desse modo, $\left(a + b\sqrt{n}\right).\left(a - b\sqrt{n}\right) = \pm 1 \in \mathbb{Z}$.

Como $\bar{\delta} = \delta^{-1} = \left(a - b\sqrt{n}\right) \in \mathbb{Z}\left[\sqrt{n}\,\right]$, tem-se que $\forall \delta = \left(a + b\sqrt{n}\right) \in \mathbb{Z}\left[\sqrt{n}\,\right]$ possui elemento inversível neste anel.

De forma recíproca: δ é inversível$\Longrightarrow \exists \beta \in \mathbb{Z}\left[\sqrt{n}\,\right]$, tal que: $\delta.\beta = 1 \Longrightarrow N(\delta.\beta) = N(\delta).N(\beta) = N(1) = 1$.

Logo: $N(\delta) \mid 1$ em $\mathbb{Z} \Longrightarrow N(\delta) = \pm 1$.

Em relação ao item v): sendo $N(\delta) = p \Longrightarrow N(\delta) \neq \pm 1$ e $N(\delta) \neq 0 \Longrightarrow \nexists\, \delta^{-1} \in \mathbb{Z}\left[\sqrt{n}\,\right]$ e $\delta \neq 0$. Supor: $\delta = \beta.\gamma$ em $\mathbb{Z}\left[\sqrt{n}\,\right]$. Daí, $N(\delta) = p = N(\beta.\gamma) = N(\beta).N(\gamma)$. Como tem-se, em $\mathbb{Z}$, $p = N(\beta).N(\gamma)$, logo: $N(\beta) = \pm 1$ ou $N(\gamma) = \pm 1$. Assim, β é inversível ou γ é inversível. Portanto, δ é irredutível. ■

CAPÍTULO 2 – EQUAÇÃO FERMATIANA QUÍNTUPLA

Neste capítulo, será demonstrado que a equação:

$$\mathbf{X^5 + Y^5 = Z^5 \ \ (1)}$$

Não admite soluções **inteiras não triviais**, isto é, inteiras todas não nulas.

É importante observar que as demonstrações do **Último Teorema de Fermat (UTF)** para os casos particulares $n = 3$ e $n = 4$ apresentaram soluções razoavelmente diferentes. Assim, nas primeiras provas, já haviam indícios da dificuldade de se estabelecer uma solução geral para o UTF.

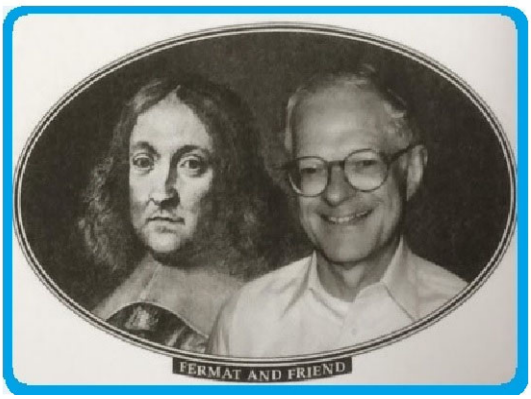
Antes de começarmos a elaborar a demonstração, objeto da Dissertação, será, oportunamente, apresentado o **Teorema de Sophie Germain (TSG)**, que possui importantes ideias para o caso $n = 5$. Germain trouxe argumentos relacionados à divisibilidade por 5, possibilitando que a prova do UTF para $n = 5$ pudesse ser estudada e demonstrada em duas partes:

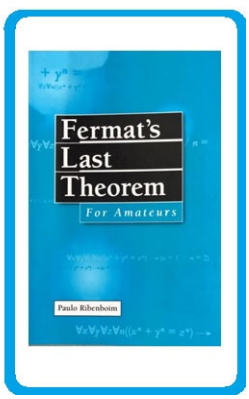
- (PRIMEIRA PARTE): Nenhum dos inteiros x, y e z é divisível por 5, ou seja, **5 não divide** $(x.y.z)$; e
- (SEGUNDA PARTE): Apenas um dos inteiros x, y e z é **divisível por 5**, sendo tal inteiro divisível por 5, analisado, separadamente, em dois casos:

  $(1º\ caso)$: **inteiro par** divisível por 5.

  $(2º\ caso)$: **inteiro ímpar** divisível por 5.

A demonstração do caso particular em que $n = 5$ foi estudada, em grande parte, na seguinte referência do autor Paulo Ribenboim:





Conforme Ribenboim (1999), as principais demonstrações apresentadas para a **Equação Fermatiana Quíntupla**, cuja prova completa se subdivide em dois casos, foram as seguintes:

Autor	Caso ($n = 5$)	Ano
Gauss	Ambos	1863 (com publicação póstuma)
Schopis	1° Caso	1825
Lebesgue	Ambos	1843
Lamé	Ambos	1847
Gambioli	Ambos	1901 e 1903
Werebrusow	Ambos	1905
Mirimanoff	1° Caso	1909
Rychlik	Ambos	1910
Hayashi	Ambos	1911
van der Corput	Ambos	1915
Terjanian	Ambos	1987

No que se refere à **Teoria Algébrica**, merecem destaque, em $n = 5$, as definições e os exemplos de:

- *Corpos, Domínios de Integridade e Domínios de Fatoração Única* (DFU).
- *Unidades, elementos inversos, irredutíveis e primos*.

2.1 Breve apresentação do Teorema de Sophie Germain

A francesa Sophie Germain, utilizando um pseudônimo masculino, desenvolveu trabalhos matemáticos, interagindo com alguns de seus colegas da época, como Gauss, que a apoiava e a admirava pela sua originalidade matemática.

Germain buscava resolver o UTF sob uma nova estratégia, que era a de uma abordagem geral, consideravelmente complexa, visto que muitos casos particulares apresentavam estruturas algébricas e estratégias de solução diferentes entre si. Por exemplo, nos casos $n = 3$ e $n = 5$, em relação à questão da fatoração única, tem-se

que, no primeiro caso, estuda-se o Anel de Inteiros de Eisenstein e, no segundo, o Anel de Inteiros de Dedekind.

Assim, sem perda de generalidade, temos números das seguintes formas:

$$\begin{cases} z^3 = a^2 + 3b^2 = \left(a + b\sqrt{-3}\right).\left(a - b\sqrt{-3}\right) \\ z^5 = c^2 - 5d^2 = \left(c + d\sqrt{5}\right).\left(c - d\sqrt{5}\right) \end{cases}$$

É importante notar, nos exemplos a seguir, que as *expressões fermatianas* podem sem decompostas em fatores lineares associados às seguintes *estruturas algébricas*:

$$z^3 = \underbrace{(x+y).(x+wy).\left(x+w^2y\right)}_{fatores\ únicos\ pertencentes\ a\ \mathbb{Z}[\sqrt{w}]}$$

$$z^5 = \underbrace{(x+y).(x+\theta y)\ldots\left(x+\theta^4 y\right)}_{fatores\ únicos\ pertencentes\ a\ \mathbb{Z}[\sqrt{\theta}]}$$

De fato, conforme os expoentes vão aumentando, a complexidade algébrica vai, invariavelmente, crescendo. Mesmo diante deste grande desafio, Germain concentrou esforços na busca de uma solução definitiva para o problema do UTF.

Embora não tenha elaborado a sonhada prova final do UTF, Germain apresentou um teorema com o seu nome, que foi um passo relevante no desenvolvimento de ideias sobre o UTF. Ela o demonstrou através de uma prova para dois casos, que, neste capítulo, serão apenas enunciados para $n = 5$.

Kummer, inspirando-se na ideia de Germain de estudar o UTF em dois casos, elaborou um outro importante teorema, abrangendo o conceito de *números regulares*, que, em linhas gerais, representam certos primos com propriedades de *corpos ciclotômicos* (estruturas algébricas que, dentre outros papéis, possibilitam analisar a fatoração nas Equações Fermatianas).

O **TEOREMA DE SOPHIE GERMAIN (TSG)** para $n = 5$ tem o enunciado:

O **TSG** para as potências quíntuplas $(n = 5)$, subdivide-se nos CASOS I e II a seguir:

CASO I – Se nenhum dos inteiros $x,\ y$ e z é divisível por 5, então não existem soluções inteiras não nulas (x, y, z) para $\mathrm{X}^5 + \mathrm{Y}^5 + \mathrm{Z}^5 = 0\ (2)$.

CASO II – Se apenas um dos inteiros $x,\ y$ e z é divisível por 5, então não existem soluções inteiras não nulas (x, y, z) para $\mathrm{X}^5 + \mathrm{Y}^5 + \mathrm{Z}^5 = 0\ (2)$.

De forma equivalente, escreve-se ainda o **CASO I**:

Se a equação (2) apresenta soluções inteiras não nulas (x, y, z), então:

x ou y ou z deve ser **divisível por 5**.

Neste trabalho não será elaborada demonstração para o TSG. Contudo, caso algum leitor deseje aprofundar os seus conhecimentos sobre este teorema, recomenda-se a leitura do artigo: "*Sophie Germain and Special Cases of Fermat's Last Theorem*", que consta nas Referências Bibliográficas.

Ressalta-se, a seguir, duas implicações (em negrito) com ideias utilizadas na demonstração do TSG para $n = 5$ (CASO I), desenvolvida por EDWARDS (1977).

Assim, assumindo x, y e z inteiros não nulos, tem-se:

$$\begin{cases} \boldsymbol{x\ \text{ou}\ y\ \text{ou}\ z \equiv 0\ (mod\ 11)} \Longrightarrow x^5 + y^5 + z^5 \equiv 0\ (mod\ 11) \\ \boldsymbol{x\ \text{e}\ y\ \text{e}\ z \not\equiv 0\ (mod\ 11)} \Longrightarrow x^5 + y^5 + z^5 \not\equiv 0\ (mod\ 11) \end{cases}$$

Para entender corretamente os argumentos das afirmações anteriores, deve-se observar o comportamento das potências quíntuplas de inteiros não nulos em relação à divisibilidade por 11, pois esta prova tem, como estratégia, analisar as classes de equivalência dessas potências quíntuplas, que, no caso, são: $\overline{0}$ e $\pm\overline{1}$.

Deste modo, sem perda de generalidade, dividindo-se x^5 por 11, podemos apresentar os seguintes pontos de destaque:

- $$\begin{cases} x^5 \equiv 0\ (mod\ 11) \Leftrightarrow x \equiv 0\ (mod\ 11) \\ \text{ou} \\ \underbrace{x^{10} = (x^5)^2 \equiv 1\ (mod\ 11)}_{\text{PTF } e\ sendo\ x \not\equiv 0\ (mod\ 11)} \end{cases} \Longrightarrow x^5 \equiv \pm 1\ (mod\ 11) \Leftrightarrow x \equiv \pm 1\ (mod\ 11)$$

- A redução a apenas três possíveis (0 e ± 1) deve-se à estratégia da prova do TSG para $n = 5$ (CASO I), que é a de se realizar uma demonstração por absurdo, apresentando-se resíduos diferentes de $-1,\ 0$ e $+1$.

- Considerando, sem perda de generalidade, $x \equiv 0\ (mod\ 11)$, temos:

  $$\left.\begin{cases} x \equiv y \equiv z \equiv 0\ (mod\ 11) \\ \text{ou} \\ x \equiv 0 \ \text{ e } \ y \equiv -z \equiv \pm 1\ (mod\ 11) \end{cases}\right\} \Longrightarrow x^5 + y^5 + z^5 \equiv 0\ (mod\ 11)$$

  Em outras palavras, isso quer dizer o seguinte:

  $$\text{HIPÓTESE: } \left[\begin{array}{c} \text{As três variáveis são divisíveis por 11.} \\ \text{ou} \\ \text{Apenas uma das variáveis é divisível por 11.} \end{array}\right]$$

  $$\text{TESE: } x^5 + y^5 + z^5 \equiv 0 \text{ é divisível por 11}$$

- Observe que $(\pm 1)^5 + (\pm 1)^5 + (\pm 1)^5 \not\equiv 0\ (mod\ 11)$. De fato, se nenhuma variável for divisível por 11, tem-se:

  $$\left.\begin{cases} x \not\equiv 0\ \ (mod\ 11) \\ y \not\equiv 0\ \ (mod\ 11) \\ z \not\equiv 0\ \ (mod\ 11) \end{cases}\right\} \Longrightarrow x^5 + y^5 + z^5 \not\equiv 0\ \ (mod\ 11)$$

  Isto é: “Se nenhuma das variáveis é divisível por 11, então $x^5 + y^5 + z^5$ não é divisível por 11”.

No Apêndice desta dissertação, será apresentada uma ideia das provas dos Lemas da *Equação Fermatiana Quíntupla*, denominados Lemas 1 e 2, cujos resultados serão aplicados diretamente (sem as suas provas neste momento) na demonstração do Teorema da *Equação Fermatiana Quíntupla* (Teorema 2.2), que ainda será apresentado.

Os enunciados dos Lemas encontram-se nas tabelas a seguir com o Anel A denotando os Inteiros de Dedekind, Anel de Inteiros no Corpo $\mathbb{Q}(\sqrt{5})$.

Lema 1 – Para o Teorema da Equação Fermatiana Quíntupla

Sejam a e b inteiros não negativos com:

$$mdc\ (a,b) = 1; a \not\equiv b\ (mod\ 2); 5 \nmid a;\ \text{e}\ 5 \mid b$$

Se $(\boldsymbol{a^2 - 5b^2})$ é a quinta potência de um elemento do Anel A, então existem c e d, inteiros não nulos, tais que:

$$\begin{cases} a = c.(c^4 + 50c^2d^2 + 125d^4) \\ b = 5d.(c^4 + 10c^2d^2 + 5d^4) \end{cases}$$

onde: $mdc\ (c,d) = 1;\ c \not\equiv d\ (mod\ 2);\ \text{e}\ 5 \nmid c.$

Lema 2 – Para o Teorema da Equação Fermatiana Quíntupla

Sejam a e b inteiros não negativos e ímpares com:

$$mdc\ (a,b) = 1;\ a \not\equiv b\ (mod\ 2); 5 \nmid a;\ \text{e}\ 5 \mid b$$

Se $\frac{(\boldsymbol{a^2 - 5b^2})}{\boldsymbol{4}}$ é a quinta potência de um elemento do Anel A, então:

existem c e d, inteiros não nulos, tais que:

$$\begin{cases} a = \dfrac{c.(c^4 + 50c^2d^2 + 125d^4)}{16} \\ b = \dfrac{5d.(c^4 + 10c^2d^2 + 5d^4)}{16} \end{cases}$$

onde: $mdc\ (c,d) = 1;\ c\ \text{e}\ d\ \text{ímpares};\ \text{e}\ 5 \nmid c.$

2.2 Teorema da Equação Fermatiana Quíntupla

TEOREMA 2.2: A Equação Fermatiana Quíntupla $\mathbf{X^5 + Y^5 + Z^5 = 0}$ $\mathbf{(2)}$ não apresenta solução com números inteiros não nulos.

Prova: Suponha por absurdo que a equação $\mathrm{X}^5 + \mathrm{Y}^5 + \mathrm{Z}^5 = 0$ possui solução (x, y, z) de inteiros não nulos, onde podemos assumir $mdc\ (x, y, z) = 1$. E, portanto, x, y e z são relativamente primos aos pares.

Dividiremos esta prova em duas partes.

Primeira parte – 5 não divide $(x.y.z)$

Deste modo, x, y e z são congruentes a ± 1 ou a $\pm 2\ (mod\ 5)$.

Segue do PTF que

$$\begin{cases} x^5 \equiv x\ (mod\ 5) \\ y^5 \equiv y\ (mod\ 5) \\ z^5 \equiv z\ (mod\ 5) \end{cases} \Longrightarrow x + y + z \equiv \overbrace{x^5 + y^5 + z^5}^{\equiv 0\ (por\ hipótese)} \equiv 0\ (mod\ 5)$$

Se x, y e z são, aos pares, incongruentes módulo 5, então:

$$x + y + z \not\equiv 0\ (mod\ 5)$$

Obtemos uma contradição que implica na nossa suposição inicial ser falsa.

Nos resultados seguintes, considere a seguinte afirmação para x, y e $p \in \mathbb{N}$ com p primo:

$$x \equiv y\ \ (mod\ p)\ \ \Longrightarrow\ \ x^p \equiv y^p\ (mod\ p^2)$$

Assim, com $p = 5$, temos que:

$$x^5 \equiv y^5\ (mod\ 5^2)$$

Sem perda de generalidade, considere x e y da solução da equação (2), de modo que:

$$x \equiv y\ (mod\ 5)\ \Longrightarrow\ \begin{cases} -z \equiv x + y \equiv 2x\ (mod\ 5)\ \Longrightarrow\ -z^5 \equiv 2^5 x^5\ (mod\ 5^2) \\ x^5 \equiv y^5\ (mod\ 5^2)\ \Longrightarrow\ -z^5 \equiv x^5 + y^5 \equiv 2x^5\ (mod\ 5^2) \end{cases}$$

$$\Longrightarrow -z^5 \equiv 2^5 x^5 \equiv 2x^5 (mod\ 5^2)$$

Por outro lado, isto gera uma contradição, pois:

$$2^5 \equiv 7 \not\equiv 2 \ (mod\ 5^2)$$

Obtemos uma contradição que implica na nossa suposição inicial ser falsa. ■

Ideia Geral da Demonstração para a segunda parte:

No que se refere à análise da paridade da equação $\mathrm{X}^5 + \mathrm{Y}^5 + \mathrm{Z}^5 = 0 \ (2)$, tem-se:

(**1º caso**): z é par $\Longrightarrow x$ e y são ímpares

Desta forma, existem p e $q \in \mathbb{Z}$, tais que:

$$\begin{cases} 2p = x + y \\ 2q = x - y \end{cases} \Longrightarrow \begin{cases} (+) \Longrightarrow x = p + q \\ (-) \Longrightarrow y = p - q \end{cases}$$

Implicando p e q terem paridades distintas.

Sabe-se ainda que:

$$mdc\ (x, y) = mdc\ (p + q;\ p - q) = 1 \implies mdc\ (p;\ q) = 1$$

(**2º caso**): z é ímpar $\Longrightarrow x$ e y têm paridades distintas $\Longrightarrow \begin{cases} x \text{ é par} \Longrightarrow y \text{ é ímpar} \\ x \text{ é ímpar} \Longrightarrow y \text{ é par} \end{cases}$

Com isso, existem u e $v \in \mathbb{Z}$, tais que:

$$\begin{cases} u = x + y \\ v = x - y \end{cases} \Longrightarrow \begin{cases} (+) \Longrightarrow x = \dfrac{u + v}{2} \\ (-) \Longrightarrow y = \dfrac{u - v}{2} \end{cases}$$

Implicando u e v serem ímpares.

Sabe-se também que:

$$mdc\ (x, y) = 1 \implies mdc\ (x + y;\ x - y) = mdc\ (u;\ v) = 1$$

De fato, na terna (x, y, z), solução da equação $\mathrm{X}^5 + \mathrm{Y}^5 + \mathrm{Z}^5 = 0$ (2), observa-se sempre a seguinte associação entre as variáveis:

uma variável par e duas ímpares

Segunda parte – sem perda de generalidade, 5 divide z.

Deste modo: $5 \mid z \Longrightarrow 5 \nmid (x.y)$, onde: $mdc\ (x, y) = 1$.

($\mathbf{1º}$ **caso**): z é par $\Longrightarrow x$ e y são ímpares

Assim:

$$\begin{cases} 2 \mid z \\ \\ 5 \mid z \end{cases} \Longrightarrow \underbrace{z = 2^m.5^n.z'}_{\substack{sendo\ os\ inteiros \\ m,n \geq 1}} \quad \text{com} \quad 2 \nmid z' \ \text{ e } \ 5 \nmid z'$$

Suponha por absurdo que a equação $\mathrm{X}^5 + \mathrm{Y}^5 + \mathrm{Z}^5 = 0$ apresenta solução não nula. Deste modo, pode-se exibir uma trinca de inteiros não nulos (x, y, z) tais que:

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

Esta equação pode ser reescrita da seguinte forma:

$$-2^{5m}.5^{5n}.(z')^5 = x^5 + y^5 \qquad (3)$$

Pode-se fazer p e q **inteiros não nulos** com $mdc\ (p, q) = 1$.

De fato:

$$\underbrace{x \text{ e } y \text{ ímpares}}_{por\ hipótese} \Longrightarrow \underbrace{\begin{cases} x = p + q \\ \\ y = p - q \end{cases}}_{\substack{p \text{ e } q \rightarrow inteiros\ com\ paridades \\ distintas}}$$

Reescrevendo-se a equação (3), obtém-se:

$$-z^5 = -2^{5m}.5^{5n}.(z')^5 = (p + q)^5 + (p - q)^5 = 2p.(p^4 + 10p^2q^2 + 5q^4) \qquad (4)$$

Como 5 é primo, temos que:

$$5 \mid p \quad \text{ou} \quad 5 \mid (p^4 + 10p^2q^2 + 5q^4)$$

Assumindo que 5 divide p, então:

$$p = 5r \text{ com } r \in \mathbb{Z}$$

E ainda, 5 não divide q, pois:

$$\underbrace{mdc\,(5r, q) = mdc\,(r, q) = 1}_{mdc\,(p;\,q)\,=\,1}$$

Como p e q apresentam paridades diferentes, então r e q também apresentam.

Substituindo $p = 5r$ com $r \in \mathbb{Z}$ na equação (4), obtemos:

$$-z^5 = -2^{5m} \,.\, 5^{5n} \,.\, (z')^5 = 2.5^2 r.\underbrace{(q^4 + 50q^2r^2 + 125r^4)}_{=\,t}$$

Consideremos ainda t expresso através das variáveis auxiliares u e v:

- $t = (\underbrace{q^2 + 25r^2}_{=\,u})^2 - 5\,.\,(\underbrace{10r^2}_{=\,v})^2$

$$\Longrightarrow \left\{ \begin{array}{c} u;\ v \neq 0, \text{pois } r;\ q \neq 0 \\ \underbrace{u \text{ é } primo\ ímpar}_{r\ e\ q\ tem\ paridades\ distintas} \\ 10 \mid v \\ \underbrace{mdc\,(u, v) = 1}_{10 \nmid u\ e\ mdc\,(r,q)=1} \end{array} \right\} \Longrightarrow t = u^2 - 5v^2$$

$$\Longrightarrow \left\{ \begin{array}{c} \underbrace{\text{t é ímpar}}_{u \text{ e } v \text{ tem paridades distintas}} \\ \underbrace{mdc\,(t, r) = 1}_{mdc\,(r;\,q)=1} \\ 5 \nmid t \end{array} \right\} \Longrightarrow 5 \mid r \text{ (desde que } 5n > 2)$$

$$\Longrightarrow mdc\,(2.5^2 r;\ t) = 1 \Longrightarrow \underbrace{2.5^2 r \text{ e } t}_{\substack{representam \\ quintas\ potências \\ de\ inteiros}}$$

Pode-se escrever o seguinte:

$$\left\{ \begin{array}{c} t = u^2 - 5v^2 \\ \text{com} \\ \underbrace{u \not\equiv v\ (mod\ 2)}_{mdc\,(u;\,v)\,=\,1} \end{array} \right\}$$

Observe, novamente, o seguinte ponto:

$$\begin{cases} \underbrace{5 \nmid u}_{u=q^2+5^2r^2} \\ \\ \underbrace{5 \mid v}_{v=(2.5).r^2} \end{cases}$$

Considerando o Lema 1, a ser demonstrado no Apêndice, pode-se reescrever u e v com c e d inteiros não nulos, tais que $mdc\ (c,d) = 1;\ c \not\equiv d\ (mod\ 2);$ e $5 \nmid c$:

$$\begin{cases} \underbrace{u = c.(c^4 + 2.5^2.c^2d^2 + 5^3d^4) \not\equiv 0\ (mod\ 5)}_{c \not\equiv 0\ (mod\ 5)} \\ \\ v = 5d.(c^4 + 2.5.c^2d^2 + 5d^4) \equiv 0\ (mod\ 5) \end{cases}$$

Sabe-se que:

$$\begin{cases} 5 \mid r \\ \\ v = 2.5.r^2 \end{cases} \Longrightarrow 5 \mid d$$

Multiplicando-se v por $2\ .\ 5^3$, tem-se:

$$2.5^3.v = (2\ .5^2\ r)^2 = \underbrace{2.5^4.d.(c^4 + 2.5.c^2d^2 + 5d^4)}_{\substack{Potência\ de\ 5\ se\ (2\ .5^2\ r\ ) \\ também\ for}}$$

Assim:

$$\left.\begin{cases} mdc\ (c;\ d) = 1 \\ \\ c \not\equiv d\ (mod\ 2) \\ \\ 5 \nmid c \end{cases}\right\} \Longrightarrow \quad mdc\ (2.5^4.d;\ \ c^4 + 2.5.c^2d^2 + 5d^4) = 1$$

$$\Longrightarrow\ (c^4 + 2.5.c^2d^2 + 5d^4)\ \text{é ímpar}$$

Sendo 2.5^2r uma quinta potência de inteiros, o produto dos inteiros, a seguir, também é uma potência de 5. Sendo o MDC desses inteiros igual a 1, então eles, isoladamente, representam potências quíntuplas:

$$\begin{cases} 2.5^4.d \\ \\ \underbrace{(c^4 + 2.5.c^2d^2 + 5d^4)}_{\text{é ímpar}} = \underbrace{(c^2 + 5d^2)^2 - 5.(2d^2)^2}_{\left.\begin{matrix}(c^2+5d^2) \\ (2d^2)\end{matrix}\right\} têm\ paridades \neq} \end{cases}$$

O MDC é 1 porque, além do exposto acima, temos o seguinte:

$$5 \nmid c \quad \text{e} \quad mdc\,(c,d) = 1$$

Afirma-se ainda para posterior reaplicação do Lema 1:

$$\underbrace{\left.\begin{matrix}(c^2+5d^2)\\(2d^2)\end{matrix}\right\}}_{\substack{Não\ são\ ambos\\ímpares}} \Longrightarrow \begin{cases} mdc\,(c^2+5d^2;\ 2d^2) = 1 \\ 5 \nmid (c^2+5d^2) \\ 5 \mid (2d^2) \end{cases}$$

Utilizando, recursivamente, o Lema 1, existem c' e d' inteiros não nulos, tais que $mdc\,(c',d') = 1;\ c' \not\equiv d'\ (mod\ 2);$ e $5 \nmid c'$:

$$\begin{cases} \underbrace{c^2+5d^2 = c'.\left(c'^4+2.5^2.c'^2d'^2+5^3d'^4\right) \not\equiv 0\ (mod\ 5)}_{c' \not\equiv 0\ (mod\ 5)} \\ 2d^2 = 5d'.\left(c'^4+2.5.c'^2d'^2+5d'^4\right) \equiv 0\ (mod\ 5) \end{cases}$$

Analogamente, tomando um $d' > 0$:

$$5 \mid d' \implies 5^2 \mid d$$

Multiplicando-se agora $2d^2$ por $2\,.\,5^8$, tem-se:

$$2d^2.(2\,.\,5^8) = (2\,.\,5^4d)^2 = \underbrace{2\,.\,5^9.\,d'.(c'^4+2.5.c'^2d'^2+5d'^4)}_{\substack{Potência\ de\ 5\ se\ (2\,.5^4.d\,)\\ também\ for}}$$

De forma análoga:

$mdc\,(2\,.\,5^9.\,d';\ c'^4+2.5.c'^2d'^2+5d'^4\,) = 1 \implies c'^4+2.5.c'^2d'^2+5d'^4$ (ímpar)

A seguir, tomando os inteiros como potências de 5:

$$\begin{cases} 2\,.\,5^9.\,d' \\ c'^4+2.5.c'^2d'^2+5d'^4 = (c'^2+5d'^2)^2 - 5.(2d'^2)^2 \end{cases}$$

Tem-se ainda que:

$$0 < d' < d$$

Com efeito:

$$5d'^4 \leq \underbrace{(c'^4 + 2.5.\, c'^2 d'^2)}_{\geq 0} + 5d'^4$$

E multiplicando-se a inequação anterior por $5d'$, obtém-se:

$$5^2 d'^5 \leq 5d'.(c'^4 + 2.5.\, c'^2 d'^2 + 5d'^4) = 2d^2$$

$$d'^5 \leq \frac{d'.(c'^4 + 2.5.\, c'^2 d'^2 + 5d'^4)}{5} = \frac{2d^2}{25}$$

$$d'.\underbrace{(c'^4 + 2.5.\, c'^2 d'^2 + 5d'^4)}_{\geq d'} = \frac{2d^2}{5}$$

Logo:

$$0 < d'^2 \leq \frac{2d^2}{5} \Longrightarrow 0 < d' \leq \sqrt{\frac{2d^2}{5}} = \sqrt{\frac{2}{5}}.d < d$$

Prosseguindo com este raciocínio, pode-se obter uma sequência infinita de inteiros entre zero e um inteiro d (**Princípio da Descida Infinita de Fermat**), o que implica ser falsa a suposição inicial.

Portanto, neste caso, os argumentos provam a inexistência de solução inteira não nula para a equação $\mathrm{X}^5 + \mathrm{Y}^5 + \mathrm{Z}^5 = 0$.■

(**2º caso**): z é ímpar $\Longrightarrow x$ e y têm paridades distintas

Assim:

$$\underbrace{z = 5^n.z'}_{\substack{sendo\ o\ inteiro \\ n\geq 1}} \text{, onde: } \begin{cases} 2 \nmid z' \\ 5 \nmid z' \end{cases}$$

Suponha também por absurdo que a equação $X^5 + Y^5 + Z^5 = 0$ apresenta solução não nula. Deste modo, pode-se exibir uma trinca de inteiros não nulos (x, y, z) tais que:

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

Esta equação pode ser reescrita também da seguinte forma:

$$\underbrace{-z^5 = -5^{5n}.(z')^5 = x^5 + y^5}_{com\ x \not\equiv y\ (mod\ 2)} \qquad (5)$$

Tem-se u e v inteiros ímpares não nulos com $mdc\,(u, v) = 1$:

$$\begin{cases} x = \dfrac{u+v}{2} \Longrightarrow 2x = (u+v) \\ y = \dfrac{u-v}{2} \Longrightarrow 2y = (u-v) \end{cases}$$

A partir da equação (5), pode-se afirmar:

$$(2x)^5 + (2y)^5 = 2^5.(x^5 + y^5) = \overbrace{-2^5.z^5 = -2^5.5^{5n}.(z')^5}^{(5)}$$

Utiliza-se ainda a seguinte identidade:

$$(2x)^5 + (2y)^5 = (u+v)^5 + (u-v)^5 = 2u.(u^4 + 10u^2v^2 + 5v^4) = -2^5.5^{5n}.(z')^5$$

Obtendo-se a seguinte a equação:

$$-2^5.z^5 = -2^5.5^{5n}.(z')^5 = 2u.(u^4 + 10u^2v^2 + 5v^4) \qquad (6)$$

Como 5 é primo, temos que 5 divide u, isto é, $u = 5r$ com $r \in \mathbb{Z}$.

Tem-se, portanto, que:

- $5 \nmid v$
- $\underbrace{mdc\,(5r, v) = mdc\,(r, v) = 1}_{mdc\,(u;\,v)=1}$
- u e v ímpares $\Longrightarrow r$ e v ímpares

Substituindo-se $u = 5r$ com $r \in \mathbb{Z}$ na equação (6):

$$-2^5.z^5 = -2^5.5^{5n}.(z')^5 = (2.5^2).r.(\underbrace{v^4 + 2.5^2.v^2r^2 + 5^3r^4}_{=t \in \mathbb{Z}})$$

Desta forma:

$$-2^5.5^{5n}.(z')^5 = 2.5^2.r.t \qquad (7)$$

Analogamente, podemos escrever $t = u'^2 - 5v'^2$ com:

$$\begin{cases} \underbrace{u' = v^2 + 5^2r^2}_{u' \neq 0} \\ \underbrace{v' = 2.5.r^2}_{v' \neq 0} \end{cases}$$

Pode-se ainda concluir:

$$mdc\,(r, v) = 1 \Longrightarrow mdc\,(r, t) = 1$$

Como:

$$\underbrace{\begin{cases} v \equiv 1 \ \text{ ou } \ 3 \ \ (mod\ 4) \\ r \equiv 1 \ \text{ ou } \ 3 \ \ (mod\ 4) \end{cases}}_{\text{pois } v \ e \ r \ \text{são ímpares}}$$

Observa-se que:

$$\begin{cases} u' \equiv v^2 + r^2 \equiv 2\ (mod\ 4) \\ v' \equiv 2r^2 \equiv 2\ (mod\ 4) \end{cases}$$

Garante-se ainda o seguinte:

$$\underbrace{5 \nmid v \implies 5 \nmid t}_{t = (v^4 + 2.5^2.v^2r^2 + 5^3r^4)}$$

Tem-se que 5 divide r, como argumentado a seguir:

$$\left.\begin{array}{c} u';\ v' \neq 0, \text{pois } v;\ r \neq 0 \\ u' \text{ e } v' \text{ são pares} \\ 5 \nmid t \\ mdc\,(t, r) = 1 \end{array}\right\} \Longrightarrow 5 \mid r \ \text{ (para 5n} > 2)$$

Reescrevendo as variáveis, com analogia a etapas já desenvolvidas neste texto, tem-se:

$$\begin{cases} u' = 2u'' \\ v' = 2v'' \\ t = 4.(u'')^2 - 20.(v'')^2 \\ t' = \dfrac{t}{4} = (u'')^2 - 5(v'')^2 \end{cases}$$

Note que:

$$\begin{cases} u' \equiv 2\ (mod\ 4) \Longrightarrow u' = 4k_1 + 2 = 2.(2k_1 + 1) = 2u'' \\ v' \equiv 2\ (mod\ 4) \Longrightarrow v' = 4k_2 + 2 = 2.(2k_1 + 1) = 2v'' \end{cases} \Longrightarrow \underbrace{u''\ \text{e}\ v''}_{(números\ ímpares)}$$

$$\Longrightarrow \begin{cases} u'' \equiv 1 \ \text{ ou } \ 3\ (mod\ 4) \\ v'' \equiv 1 \ \text{ ou } \ 3\ (mod\ 4) \\ mdc\ (r, v) = 1 \Longrightarrow mdc\ (u'', v'') = 1 \end{cases}$$

Assim, 5 não divide u'' e 5 divide v''. E como:

$$t' = (u'')^2 - 5(v'')^2 \Longrightarrow t' \equiv 0\ (mod\ 4)$$

Das equações (5) e (7), tem-se:

$$-5^{5n}.(z')^5 = 5^2 r.\left(\frac{t}{16}\right) = 5^2 r.\left(\frac{t'}{4}\right)$$

Verificando-se ainda a seguinte relação:

$$mdc\left(5^2 r;\ \frac{t'}{4}\right) = 1$$

Com argumentos análogos aos do 1º Caso, sabe-se que são potências de 5:

$$\begin{cases} 5^2 r \\ \dfrac{t'}{4} = \dfrac{(u'')^2 - 5(v'')^2}{4} \end{cases}$$

Considerando o Lema 2, a ser demonstrado no Apêndice, reescreve-se u'' e v'' com c e d inteiros não nulos, tais que $mdc\ (c,d) = 1$; c e d são ambos ímpares; e $5 \nmid c$:

$$\begin{cases} u'' = \dfrac{c.(c^4 + 2.5^2.c^2d^2 + 5^3d^4)}{2^4} \\ v'' = \dfrac{5d.(c^4 + 2.5.c^2d^2 + 5d^4)}{2^4} \end{cases}$$

Visto que:

$$5 \mid r \implies 5^2 \mid v'' \implies 5 \mid d$$

Pode-se assumir um $d > 0$ e ainda multiplicar-se v'' por 5^3:

$$5^3v'' = (5^2r)^2 = \frac{5^4d}{4}.\left[\left(\frac{c^2 + 5d^2}{2}\right)^2 - 5d^4\right]$$

de onde se afirma que:

$$\left(\frac{c^2 + 5d^2}{2}\right)^2 - 5d^4 \equiv 0\ (mod\ 4)$$

Sabe-se que:

$$mdc\left[\frac{5^4d}{4};\ \left(\frac{c^2 + 5d^2}{2}\right)^2 - 5d^4\right] = 1$$

Como são quintas potências os números:

$$(5^2r)^2 \text{ e } \frac{(u'')^2 - 5(v'')^2}{4}$$

Então também são potências de 5 os números a seguir:

$$\begin{cases} 5^4d \\ \dfrac{1}{4}.\left[\left(\dfrac{c^2 + 5d^2}{2}\right)^2 - 5.(d^2)^2\right] \end{cases}$$

Assumindo, novamente, o Lema 2, existem c' e d' inteiros não nulos, tais que $mdc\ (c', d') = 1$; c' e d' são ambos ímpares; e $5 \nmid c'$:

$$\begin{cases} \dfrac{c^2 + 5d^2}{2} = c'.\left(\dfrac{c'^4 + 2.5^2.c'^2d'^2 + 5^3d'^4}{2^4}\right) \\ \\ d^2 = 5d'.\left(\dfrac{c'^4 + 2.5.c'^2d'^2 + 5d'^4}{2^4}\right) \end{cases}$$

Considerando um $d' > 0$, sabe-se que 5 divide d'.

Agora, multiplicando-se d^2 por 5^8, tem-se:

$$5^8d^2 = (5^4d)^2 = \frac{5^9d'}{2^4}.(c'^4 + 10c'^2d'^2 + 5d'^4)$$

$$= \frac{5^9d'}{4}.\left[\left(\frac{c'^2 + 5d'^2}{2}\right)^2 - 5.\left(d'^2\right)^2\right]$$

Analogamente, são ainda potências de 5:

$$\begin{cases} 5^9d' \\ \\ \dfrac{1}{4}.\left[\left(\dfrac{c'^2 + 5d'^2}{2}\right)^2 - 5.\left(d'^2\right)^2\right] \end{cases}$$

Tem-se, portanto que:

$$0 < d' < d, \text{ pois } 25d'^5 \leq 16d^2$$

Logo, analogamente, pelo **Princípio da Descida Infinita de Fermat**, conclui-se ser falsa a suposição inicial.

Portanto, neste caso também, os argumentos provam a inexistência de solução inteira não nula para a equação $X^5 + Y^5 + Z^5 = 0$.■

CAPÍTULO 3 – CURIOSIDADES, EXEMPLOS E ATIVIDADES

3.1 Curiosidades e exemplos

I) Euler afirmava também que não existe solução não trivial nos inteiros para as equações que são soma de $(n-1)$ potências de grau n, resultando uma potência de grau n, para $n \geq 3$, isto é: $X_1^n + X_2^n + \cdots + X_{n-1}^n = Z^n$. Contudo, encontraram-se algumas soluções de casos particulares $n = 4$ e 5 como contraexemplos ao resultado geral de Euler:

$$(95.800)^4 + (217.529)^4 + (414.560)^4 = (422.481)^4$$
$$(2.682.440)^4 + (15.365.639)^4 + (18.796.760)^4 = (20.615.673)^4$$
$$(27)^5 + (84)^5 + (110)^5 + (133)^5 = (144)^5$$

II) Na equação fermatiana cúbica, o resultado mais próximo que alguém já chegou de uma terna, solução não trivial, foi $x = 6$, $y = 8$ e $z = 9$, valores que apresentam a seguinte relação: $6^3 + 8^3 = 216 + 512 = 728 == 9^3 - 1$. Já, nas potências sétimas, 348^7 representa um resultado apenas 0,028% maior do que a soma $232^7 + 345^7$.

III)

Em dois Programas da série norte-americana “The Simpsons”, o personagem Homer acha ter encontrado contraexemplos para o Último Teorema de Fermat com o expoente 12 em ambos os casos. Embora as seguintes igualdades sejam falsas, os valores apresentados nos lados esquerdo e direito destas “igualdades” são muito próximos:

$\mathbf{1782^{12} + 1841^{12} = 1922^{12}}$ (lado direito é 0,000000028% maior)

$\mathbf{3987^{12} + 4365^{12} = 4472^{12}}$ (lado esquerdo é 0,0000000019% maior)

IV) O número 30 pode ser escrito como a seguinte soma de três cubos:

$$2.220.422.932^3 + (-283.059.965)^3 + (-2.218.888.517)^3 = 30$$

V) Os maiores primos encontrados até as datas de 2018, de 2017 e de 2016 e as suas respectivas quantidades de dígitos são:

$$2^{82.589.933} - 1 \ \ (24.862.048 \text{ dígitos})$$
$$2^{77.232.917} - 1 \ (23.249.425 \text{ dígitos})$$
$$2^{74.207.281} - 1 \ (22.338.618 \text{ dígitos})$$

VI) O número composto $2^{193} - 1$ é, realmente, muito grande. Foi, com auxílio de computador, que se conseguiu determinar os fatores primos deste número, que também são grandes números:

$$p = 13.821.503$$
$$q = 61.654.440.233.248.340.616.559$$
$$r = 14.732.265.321.145.317.331.353.282.383$$

$$\therefore 2^{193} - 1 = p.q.r$$

VII) Há uma importante identidade na fatoração utilizada para provar certas afirmações sobre números primos e compostos, que é a identidade de Sophie Germain, enunciada a seguir. Dados $a, b \in \mathbb{R}$, vale a igualdade:

$$a^4 + 4b^4 = (a^2 + 2b^2 + 2ab).(a^2 + 2b^2 - 2ab). \text{ Isto pois:}$$
$$a^4 + 4b^4 = a^4 + 4a^2b^2 + 4b^4 - 4a^2b^2 = (a^2 + 2b^2)^2 - 4a^2b^2 =$$
$$(a^2 + 2b^2 + 2ab).(a^2 + 2b^2 - 2ab)$$

VIII) A relações de paridade dos números inteiros são, normalmente, utilizadas nas provas de Casos Particulares do Último Teorema de Fermat. Assim, se P e I denotam, respectivamente, em $\mathbb{Z}$, os subconjuntos referentes aos números pares e aos números ímpares, então, tem-se:

$$\mathrm{P} = \{2k; k \in \mathbb{Z}\} \text{ e } \mathrm{I} = \{2k + 1; \ k \in \mathbb{Z}\}$$
$$\mathrm{P} \cap \mathrm{I} = \emptyset \text{ e } \mathrm{P} \cup \mathrm{I} = \mathbb{Z}$$

$$\text{Sendo } x \text{ e } y \text{ inteiros arbitrários (pares ou ímpares)} \Longrightarrow \begin{cases} x, y \in \mathrm{P} \\ x, y \in \mathrm{I} \\ x \in \mathrm{P} \text{ e } y \in \mathrm{I} \\ x \in \mathrm{I} \text{ e } y \in \mathrm{P} \end{cases}$$

Verifica-se na soma algébrica $(\pm)$ e multiplicação $(\,.\,)$ entre x e y:

$$x, y \in P \Longrightarrow (x \pm y) \in P \; e \; (x.y) \in P$$
$$x, y \in I \Longrightarrow (x \pm y) \in P \; e \; (x.y) \in I$$
$$x \in P \text{ e } y \in I \Longrightarrow (x \pm y) \in I \text{ e } (x.y) \in P$$
$$x \in I \; e \; y \in P \Longrightarrow (x \pm y) \in I \; e \; (x.y) \in P$$

IX) As ternas de números inteiros positivos (x, y, z) com $mdc\,(x, y) = 1$, que satisfazem a equação $\mathrm{X}^2 + \mathrm{Y}^2 = \mathrm{Z}^2$ são denominadas ternas pitagóricas primitivas e o triângulo retângulo de catetos x e y e hipotenusa z é chamado de triângulo pitagórico primitivo. Assim, estas ternas podem ser escritas na seguinte forma, considerando ainda os inteiros positivos a, b com $a > b$: $x = a^2 - b^2,\ y = 2ab$ e $z = a^2 + b^2$. Esta relação é bastante útil na prova do Último Teorema de Fermat para o caso $n = 4$.

X) Um importante conceito é que apenas em domínios de fatoração única ou domínios fatoriais, diz-se que primos e irredutíveis representam os mesmos números. Isto, de fato, ocorre no conjunto dos inteiros e, assim, neste conjunto, tem-se o conceito de decomposição em "produto de primos" para o Teorema Fundamental da Aritmética (TFA). Contudo, há outros anéis, além dos inteiros, em que o conceito do TFA se relaciona à decomposição em um "produto de irredutíveis". Note, no exemplo a seguir, que não há uma fatoração única, mas, sim, uma escolha entre possíveis formas de fatoração:

$$12 = \ 2^2.3 = (1 + \sqrt{11}i).\left(1 - \sqrt{11}i\right) = \left(2 + \sqrt{8}i\right).\left(2 - \sqrt{8}i\right)$$

XI) O conceito dos Inteiros de Eisenstein foi muito importante na realização da prova do Último Teorema de Fermat para o caso $n = 3$, especialmente no que se refere ao estudo de suas formas fatoradas. Tem-se que os Inteiros de Eisenstein são certos domínios de integridade, que podem ser escritos da

forma a seguir, tendo w como unidade:

$$\mathbb{Z}[w] = \{x + y.w \mid x, y \in \mathbb{Z}\} \text{ com } w = \frac{-1+\sqrt{-3}}{2} = e^{\left(\frac{2\pi i}{3}\right)}$$

Pode-se tomar ainda os números α_1 e α_2, inteiros de mesma paridade, que possuem a seguinte relação:

$$\alpha_1 = 2x - y \text{ e } \alpha_2 = y$$

Assim, equivalentemente, tem-se que Inteiros de Eisenstein são números presentes no corpo $\mathbb{Q}[\sqrt{-3}]$ e que podem ser escritos da seguinte forma:

$$\frac{(\alpha_1 + \alpha_2\sqrt{-3})}{2} \text{ com } \alpha_1 \equiv \alpha_2 \ (mod\ 2)$$

Note que:

$$w^2 = \overline{w} = \frac{-1-\sqrt{-3}}{2} = e^{\left(-\frac{2\pi i}{3}\right)}$$

Observe, em relação à prova do Último Teorema de Fermat $(n = 3)$, a importância da seguinte relação na análise das formas fatoradas no anel dos Inteiros de Eisenstein:

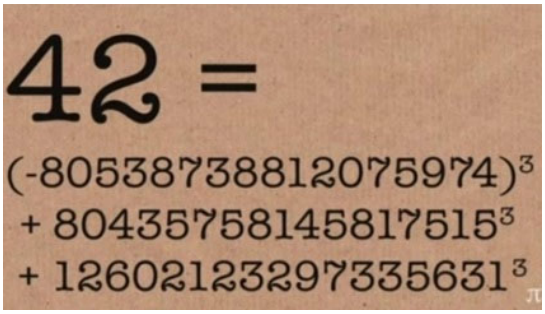
$$x^3 + y^3 = (x + y).(x^2 - xy + y^2) = (x + y).(x + wy).(x + w^2y)$$

Observando ainda o anel $\mathbb{Z}[\sqrt{-3}]$ e o número 4 (elemento do anel), afirma-se que o anel não é um domínio fatorial, pois $4 = 2.2 = \left(1 + \sqrt{-3}\right).\left(1 - \sqrt{-3}\right)$.

XII) No texto, faz-se menção a uma importante honraria matemática, denominada Medalha *Fields*, prêmio concedido apenas a matemáticos com menos de 40 anos. Andrew Wiles, infelizmente, completou essa idade na época da demonstração do "Último Teorema de Fermat", fato que o tornou inelegível a concorrer ao prêmio. Wiles, contudo, recebeu diversas honrarias por suas importantes contribuições às ciências exatas. Destaca-se que a citada medalha é concedida, a cada quatro anos, no Congresso da União Internacional de Matemática, tendo sido o brasileiro Artur Ávila um dos condecorados no ano de 2014. A insígnia da medalha traz, em um dos seus lados, a figura de

Arquimedes e uma citação a ele atribuída. Do outro lado, há também a seguinte frase escrita em latim: “Matemáticos do mundo inteiro reunidos deram este prêmio por seus escritos extraordinários”.

XIII) Recentemente, desvendou-se um mistério de 65 anos sobre a seguinte questão: “Existem três números ao cubo cuja soma seja 42?” Por exemplo, tem-se que $29 = 3^3 + 1^3 + 1^3$, mas há outros números insolúveis nesta forma de escrita algébrica. Em relação à questão inicial e após grande esforço matemático e computacional, obteve-se o seguinte resultado:



XIV) Na prova do Caso Particular em que $n = 7$, a seguinte identidade algébrica tem grande utilidade:

$$(\mathbf{X} + \mathbf{Y} + \mathbf{Z})^{\mathbf{7}} - (\mathbf{X^7} + \mathbf{Y^7} + \mathbf{Z^7}) =$$

$$= 7(\mathrm{X} + \mathrm{Y}).(\mathrm{X} + \mathrm{Z}).(\mathrm{Y} + \mathrm{Z}).[(\mathrm{X}^2 + \mathrm{Y}^2 + \mathrm{Z}^2 + \mathrm{XY} + \mathrm{XZ} + \mathrm{YZ})^2 + \mathrm{XYZ}.(\mathrm{X} + \mathrm{Y} + \mathrm{Z})$$

XV) Euler escreveu uma das mais belas fórmulas matemáticas que relaciona cinco importantes números, que são $0, 1, e, \pi, i$:

$$\boldsymbol{e^{i\pi} + 1 = 0 \Longrightarrow e^{i\pi} = \cos(\pi) + i.sen(\pi) = -1}$$

Assim, a partir desta identidade, tem-se que todo número complexo pode ser escrito da seguinte forma:

$$z = r.\big(\cos(\theta) + i.sen(\theta)\big) = r.e^{i\theta}$$

Euler fez esta descoberta verificando as seguintes identidades das séries de Taylor:

$$sen(\theta) = \frac{\theta}{1!} - \frac{\theta^3}{3!} + \frac{\theta^5}{5!} - \cdots,$$

$$cos(\theta) = 1 - \frac{\theta^2}{2!} + \frac{\theta^4}{4!} - \cdots,$$

$$e^{i\theta} = 1 + \frac{i\theta}{1!} + \frac{(i\theta)^2}{2!} + \frac{(i\theta)^3}{3!} + \frac{(i\theta)^4}{4!} + \cdots.$$

E ainda:

$$\left.\begin{aligned}\cos(\theta) + i.sen(\theta) = e^{i\theta}\\ \cos(\theta) - i.sen(\theta) = e^{-i\theta}\end{aligned}\right\} \Rightarrow \begin{cases} sen(\theta) = \dfrac{e^{i\theta} - e^{-i\theta}}{2i} \\ \cos(\theta) = \dfrac{e^{i\theta} + e^{-i\theta}}{2} \end{cases}$$

XVI) O produto de dois números, em que, cada um deles é igual à soma de dois quadrados, também é igual a uma soma de outros dois quadrados, observando a relação algébrica a seguir:

$$(a^2 + b^2).(c^2 + d^2) = (ac + bd)^2 + (ad - bc)^2 =$$
$$= (ac - bd)^2 + (ad + bc)^2$$

Pode-se fazer a seguinte exemplificação numérica para melhor ilustrar o que se afirmou acima:

$$\begin{cases} 61 = 25 + 36 = 5^2 + 6^2 \\ 65 = 49 + 16 = 7^2 + 4^2 \\ 61.65 = (6.4 + 5.7)^2 + (6.7 - 5.4)^2 = 59^2 + 22^2 = 3965 \\ 61.65 = (6.4 - 5.7)^2 + (6.7 + 5.4)^2 = 11^2 + 62^2 = 3965 \end{cases}$$

XVII) Em 1989, houve um episódio da Série de Televisão "*Jornada nas Estrelas*", ambientado no Século XXIV, em que o personagem fictício Jean-Luc Picard, Almirante da Frota Estelar, fala que, talvez, o **Último Teorema de Fermat** seja "*um tipo de enigma que jamais resolvamos*". Contudo, neste caso, a ficção extrapolou a realidade, já que supôs que este problema ficaria em aberto por, pelo menos, 700 anos ou, provavelmente, jamais seria resolvido. Sabe-se que Andrew Wiles concluiu a demonstração ainda no Século XX. Esse episódio retrata a complexidade da proposição intuída por Fermat e demonstrada por Wiles.

3.2 Atividades Matemáticas

I) Dizemos que um número natural é legal quando for soma de dois naturais consecutivos e também for soma de três naturais consecutivos. Mostre que 2001 é legal, mas 1999 e 2002 não são legais. Mostre ainda que 2001^{2001} é legal (Olimpíada Brasileira de Matemática).

II) Prove que se n é ímpar, então $n^2 - 1$ é múltiplo de 8.

III) Prove que, para qualquer número inteiro k, os números k e k^5 sempre terminam com o mesmo algarismo.

IV) Mostre que $a^7 \equiv a\ (mod\ 21)$ para todo inteiro a.

V) Ache o resto da divisão de $1^5 + 2^5 + \cdots + 183^5$ por 5 (Exame Nacional de Qualificação do PROFMAT).

VI) Mostre que o número $43^{101} + 23^{101}$ é divisível por 66, considerando verdadeira a seguinte afirmação com $a, b \in \mathbb{Z}$ e $n \in \mathbb{N}$: $(a - b) \mid (a^n - b^n)$

VII) Mostre que, para todo $n \in \mathbb{N}$, a fração $\frac{21n+4}{14n+3}$ é irredutível.

VIII) Determine todos os pares $x, y \in \mathbb{Z}$ da equação elíptica $Y^3 = X^2 + 2$.

IX) Mostre que $\log_{10} 3$ é um número irracional.

X) Mostre, como consequência direta do Último Teorema de Fermat, que $\sqrt[n]{2}$ representa um número irracional.

XI) Seja a função $f(x) = x^9 + \frac{1}{x^9}$ com domínio em $\left\{x \in \mathbb{R}_+^* \mid x^2 + \frac{1}{x^2} = 4\right\}$ e contradomínio em $\mathbb{R}$. $f(x)$ pode assumir qual dentre os seguintes números? (Magistério de Matemática – Prefeitura de Maricá)

$$153\sqrt{6}, \quad 156\sqrt{6}, \quad 204\sqrt{6}, \quad 208\sqrt{6} \quad \text{e} \quad 147\sqrt{6}$$

XII) Utilizando uma planilha Excel, solicitar que os alunos encontrem uma Terna Fermatiana Quíntupla (x, y, z) com todos não nulos satisfazendo a equação $\mathrm{X}^5 + \mathrm{Y}^5 = \mathrm{Z}^5$.

XIII) Mostre que $\mathbb{Z}[i\sqrt{7}]$ não é um Domínio de Fatoração Única (DFU).

XIV) Determinar três elementos inversíveis no anel $\mathbb{Z}[\sqrt{6}]$.

XV) Elencar os elementos inversos e as unidades do anel A, determinado a seguir:

$$\mathrm{A} = \left\{\frac{a + b\sqrt{5}}{2}, \text{tal que: } a, b \in \mathbb{Z} \; e \; a \equiv b \; (mod\; 2)\right\}$$

XVI) Utilizando o conceito de norma, mostre que se f e g são inteiros que, individualmente, representam uma soma de dois quadrados, então o produto $f.g$ também é uma soma de dois quadrados.

XVII) No Capítulo anterior, utilizou-se um resultado sem demonstrá-lo. O seu enunciado é:

Para x, y e $p \in \mathbb{N}$ com p primo, tem-se:

$$x \equiv y \; (mod\; p) \implies x^p \equiv y^p \; (mod\; p^2)$$

Apresentou-se ainda um caso particular $(p = 5)$:

$$x \equiv y \; (mod\; 5) \implies x^5 \equiv y^5 \; (mod\; 5^2)$$

Elabore uma demonstração para o caso geral.

XVIII) Prove que se a e b são números reais positivos, tais que $a^3 = a + 1$ e $b^6 = b + 3a$, então: $a > b$ (Olimpíada Brasileira de Matemática).

XIX) Mostre que:

$$a + b + c = 0 \Longrightarrow a^3 + b^3 + c^3 = 3abc$$

XX) Quantos restos diferentes são possíveis na divisão de n^2 por 11, sendo n um número natural? (Instituto Militar de Engenharia)

XXI) Sabendo-se que o resultado de: $12x11x10x \ldots x3x2x1 + 14$ é divisível por 13, qual é o resto da divisão do número $13x12x \ldots x3x2x1$ por 169? (Colégio Naval)

3.3 Soluções das Atividades Matemáticas

I) Sendo n um número natural, a soma de dois naturais consecutivos tem a seguinte representação: $2n + 1$, ou seja, é um ímpar e a de três naturais consecutivos: $3.(n + 1)$, ou seja, é um múltiplo de 3. Assim, pela definição do enunciado, um número legal é um número ímpar e múltiplo de 3.

Portanto, 2001 é legal, mas 1999 e 2002 não são. ■

Como 2001 é ímpar, tem-se que o número 2001^{2001}, na sua forma fatorada, não apresenta o 2 como fator, sendo, assim, um ímpar. Sabe-se também que: $2001^{2001} = (3)^{2001}.(667)^{2001}$ é um múltiplo de 3.

Portanto, 2001^{2001} é legal. ■

II) n é ímpar $\Longrightarrow n = 2k + 1; k \in \mathbb{Z}$

$$n^2 - 1 = (n + 1).(n - 1) = (2k + 2).(2k) = 4.k.(k + 1)$$

Sendo k um inteiro qualquer, tem-se que $k \equiv 0$ ou $1\ (mod\ 2)$. De onde se conclui:

- $k \equiv 0\ (mod\ 2) \Longrightarrow k.(k + 1) \equiv 0\ (mod\ 2)$
- $k \equiv 1\ (mod\ 2) \Longrightarrow k.(k + 1) \equiv 0\ (mod\ 2)$
- Assim, para qualquer inteiro k, tem-se que $2 \mid k.(k + 1)$

Portanto: $8 \mid 4.k.(k + 1) = n^2 - 1$ ■

III) Mostrar que um inteiro e a sua quinta potência apresentam sempre o mesmo algarismo das unidades é equivalente a mostrar que $k^5 \equiv k\ (mod\ 10)$. Tais números podem ser colocados da seguinte forma com $a_1, a_2 \in \{0,1, \dots, 9\}$: $k = (10b_1 + a_1)$ e $k^5 = (10b_2 + a_2)$. Assim, $a_2 \equiv a_1\ (mod\ 10)$.

Sendo k um inteiro qualquer, tem-se que $k \equiv 0$ ou $1\ (mod\ 2)$. De onde se conclui:

- $k \equiv 0\ (mod\ 2) \Longrightarrow k^5 \equiv 0\ (mod\ 2)$. Logo, $k^5 \equiv k\ (mod\ 2)$.
- $k \equiv 1\ (mod\ 2) \Longrightarrow k^5 \equiv 1\ (mod\ 2)$. Logo, $k^5 \equiv k\ (mod\ 2)$.
- Logo, $k^5 \equiv k\ (mod\ 2)$ para qualquer inteiro k.
- Pelo PTF, $k^5 \equiv k\ (mod\ 5)$.

- Como $mdc\ (2,5) = 1$, pode-se afirmar que:

$$k^5 \equiv k\ (mod\ 10)\ \blacksquare$$

IV) Sendo a um inteiro qualquer, tem-se que $a \equiv 0,\ 1$ ou $2\ (mod\ 3)$. De onde se conclui:

- $a \equiv 0\ (mod\ 3) \Longrightarrow a^7 \equiv 0\ (mod\ 3)$. Logo, $a^7 \equiv a\ (mod\ 3)$
- $a \equiv 1\ (mod\ 3) \Longrightarrow a^7 \equiv 1\ (mod\ 3)$. Logo, $a^7 \equiv a\ (mod\ 3)$
- $a \equiv 2\ (mod\ 3) \Longrightarrow a^7 \equiv 2^7 \equiv 2\ (mod\ 3)$. Logo, $a^7 \equiv a\ (mod\ 3)$
- Assim, $a^7 \equiv a\ (mod\ 3)$ para qualquer inteiro a
- Tem-se ainda, pelo PTF, que $a^7 \equiv a\ (mod\ 7)$

Portanto: $a^7 \equiv a\ (mod\ 21)$, pois $mdc\ (3,7) = 1\ \blacksquare$

V) Pode-se afirmar que $n^5 \equiv \text{n}\ (\text{mod}\ 5)$, conforme PTF.
Assim:

$$1^5 + 2^5 + \cdots + 183^5 \equiv 1 + 2 + \cdots + 183 = \frac{(184).(183)}{2}\ (\text{mod}\ 5)$$

$$\frac{(184).(183)}{2} = (92).(183) \equiv 2.3 \equiv 1(\text{mod}\ 5)$$

Portanto, a resposta é 1.

VI) Como $(a-b) \mid (a^n - b^n)$, sendo $a, b \in \mathbb{Z}$ e $n \in \mathbb{N}$, então tomando o exemplo $a = 43$ e $b = -23$ e ainda $n = 101$, tem-se, portanto que:

$$43 - (-23) \mid (43)^{101} - (-23)^{101} \therefore\ 66 \mid 43^{101} + 23^{101}$$

Portanto, o número $43^{101} + 23^{101}$ é divisível por 66. $\blacksquare$

VII) Deve-se mostrar que $mdc\ (21n+4, 14n+3) = 1$.

$$mdc\ (21n+4, 14n+3) = mdc\ (21n+4-14n-3, 14n+3) =$$

$$= mdc\ (7n+1, 14n+3) = mdc\ (7n+1, 14n+3-14n-2) =$$

$$= mdc\ (7n+1, 1) = 1\ \blacksquare$$

VIII) Considerando $(x, y) \in \mathbb{Z}^2$ um ponto da equação elíptica $Y^3 = X^2 + 2$, temos:

$$y^3 = x^2 + 2 = \left(x + \sqrt{2}.i\right).\left(x - \sqrt{2}.i\right)$$

Como $mdc\left(\left(x + \sqrt{2}.i\right), \left(x - \sqrt{2}.i\right)\right) = 1$, então são cubos os seguintes fatores:

$$\left(x + \sqrt{2}.i\right) \text{ e } \left(x - \sqrt{2}.i\right)$$

Daí, pode-se concluir a existência de inteiros p e q, tais que:

$$\left(x + \sqrt{2}.i\right) = \left(p + q\sqrt{2}.i\right)^3 = p^3 - 6pq^2 + (3p^2q - 2q^3).\sqrt{2}.i \Longrightarrow$$

$$1 = q.(3p^2 - 2q^2) \Longrightarrow \begin{cases} q = 1 \\ p = \pm 1 \end{cases}$$

$$x = p^3 - 6pq^2 \Longrightarrow x = \pm 5 \Longrightarrow x^2 = 25 \Longrightarrow y^3 = 27 \Longrightarrow y = 3.$$

Portanto: $(x, y) = (\pm 5, 3)$ ■

IX) Suponha que ser racional o seguinte número com p e q inteiros positivos e $mdc\ (p, q) = 1$ para se tomar uma fração irredutível:

$$\mathrm{Log}_{10}3 = \frac{\mathrm{p}}{\mathrm{q}} > 0 \Longrightarrow 10^{\left(\frac{p}{q}\right)} = 3$$

$$\therefore 10^p = 3^q \Longrightarrow 2^p.5^p = 3^q$$

Contudo, como $2, 3$ e 5 são primos e irredutíveis no anel dos inteiros, tem-se que a igualdade $2^p.5^p = 3^q$ trata-se de um absurdo pela questão da fatoração única.

Portanto: $\mathrm{Log}_{10}3$ é um número irracional. ■

X) Tomemos os inteiros não nulos a e b, tais que:

$$\sqrt[n]{2} = \frac{a}{b} \implies 2 = \left(\frac{a}{b}\right)^n = \frac{a^n}{b^n} \implies a^n = 2b^n \implies a^n = b^n + b^n$$

Tendo-se, assim, uma terna (b, b, a) como uma solução não trivial para o Último Teorema de Fermat, o que é um absurdo.

Portanto: $\sqrt[n]{2}$ é um número irracional ■

XI) Nesta função, tem-se:

$$\begin{cases} f(x) = x^9 + \dfrac{1}{x^9} \\ \text{Dom} = \left\{ x \in \mathbb{R}_+^* \mid x^2 + \dfrac{1}{x^2} = 4 \right\} \\ \text{Cd} = \mathbb{R} \\ \text{Im} = ? \end{cases}$$

$f(x)$ assume qual valor? $153\sqrt{6}$, $156\sqrt{6}$, $204\sqrt{6}$, $208\sqrt{6}$ e $147\sqrt{6}$.

Como:

$$\begin{cases} (x+y)^2 = x^2 + 2xy + y^2 \\ x^3 + y^3 = (x+y).(x^2 - xy + y^2) \end{cases}$$

Sabe-se que:

$$f(x) = (x^3)^3 + (x^{-3})^3 = (x^3 + x^{-3}).\left(x^6 - \underbrace{x^3.x^{-3}}_{=1} + x^{-6}\right)$$

$$= (x + x^{-1}).\left(x^2 - \underbrace{x.x^{-1}}_{=1} + x^{-2}\right)\left[(x^2 + x^{-2}).\left(x^4 - \underbrace{x^2.x^{-2}}_{=1} + x^{-4}\right) - 1\right]$$

$$f(x) = (x + x^{-1}).(x^2 + x^{-2} - 1).[(x^2 + x^{-2}).(x^4 + x^{-4} - 1) - 1]$$

Assim:

$$(x + x^{-1})^2 = \left(\underbrace{x^2 + x^{-2}}_{=4} + 2\right) = 6$$

$$\Longrightarrow \underbrace{(x + x^{-1}) = \sqrt{6}}_{x \in \mathbb{R}_+^*}$$

$$(x^2 + x^{-2})^2 = 16 = (x^4 + x^{-4} + 2)$$

$$\Longrightarrow (x^4 + x^{-4}) = 14$$

$$\therefore f(x) = \sqrt{6}.(4-1).[(4).(14-1) - 1] = 153\sqrt{6}\ \blacksquare$$

XII) Na atividade, objetiva-se fazer os alunos testarem possíveis soluções de Ternas Fermatianas Quíntuplas através do recurso didático do Excel. Obviamente, estas **não serão encontradas**.

XIII) Tomemos o domínio: $\mathbb{Z}\left[i\sqrt{7}\right] = \left\{ a + bi\sqrt{7};\ a, b \in \mathbb{Z} \right\}$

Tem-se que 2 é um elemento de $\mathbb{Z}\left[i\sqrt{7}\right]$, que divide o produto a seguir:

$$\left(1 + i\sqrt{7}\right).\left(1 - i\sqrt{7}\right) = 2^3 = 8$$

Contudo, 2 não divide $(1+i\sqrt{7})$, pois, caso dividisse, existiria um elemento $(a+bi\sqrt{7})$ tal que $(1+i\sqrt{7}) = 2.(a+bi\sqrt{7}) = 2a+2bi\sqrt{7}$

Pois, se a suposição fosse verdadeira, teríamos:

$$\begin{cases} 2a = 1 \Longrightarrow a = \dfrac{1}{2} \notin \mathbb{Z} \\ 2b = 1 \Rightarrow b = \dfrac{1}{2} \notin \mathbb{Z} \end{cases}$$

De fato, 2 não divide $(1+i\sqrt{7})$ e, por analogia, também não divide $(1-i\sqrt{7})$. Da mesma forma, 2 não é dividido por estes números.

Logo:

$2,\ (1+i\sqrt{7})$ e $(1-i\sqrt{7})$ são elementos irredutíveis em $\mathbb{Z}[i\sqrt{7}]$

Portanto: $\mathbb{Z}[i\sqrt{7}]$ não é um DFU.

Pois o elemento 8 apresenta *duas formas distintas de fatoração em irredutíveis.* ■

XIV) Seja $\theta = a+b\sqrt{6} \in \mathbb{Z}[\sqrt{6}]$, então, para se determinar os elementos inversíveis, coloca-se: $N(\theta) = a^2 - 6b^2 = \pm 1$.

$a = 0 \Longrightarrow -6b^2 = \pm 1 \Longrightarrow b = \pm\sqrt{\dfrac{1}{6}}\ \ ou\ \ b = \pm\sqrt{\dfrac{1}{6}}\,i \Longrightarrow b \notin \mathbb{Z}$

$a = 1 \Longrightarrow -6b^2 = 0$ ou $-6b^2 = -2 \Longrightarrow b = 0$ ou $b = \pm\sqrt{\dfrac{1}{3}} \Longrightarrow$

$\Longrightarrow b = 0$ ($\theta = a+b\sqrt{6} = 1+0.\sqrt{6} = 1 \longrightarrow$ unidade trivial)

$a = 2 \Longrightarrow -6b^2 = -3$ ou $-6b^2 = -5 \Longrightarrow b = \pm\sqrt{\dfrac{1}{2}}$ ou $b = \pm\sqrt{\dfrac{5}{6}} \Longrightarrow$

$\Longrightarrow b \notin \mathbb{Z}$

$a = 3 \Longrightarrow -6b^2 = -8$ ou $-6b^2 = -10 \Longrightarrow b = \pm\sqrt{\dfrac{4}{3}}$ ou $b = \pm\sqrt{\dfrac{5}{3}} \Longrightarrow$

$\Longrightarrow b \notin \mathbb{Z}$

$a = 4 \Longrightarrow -6b^2 = -15$ ou $-6b^2 = -17 \Longrightarrow b = \pm\sqrt{\dfrac{5}{2}}$ ou $b = \pm\sqrt{\dfrac{17}{6}}$

$\Longrightarrow b \notin \mathbb{Z}$

$a = 5 \Longrightarrow -6b^2 = -24$ ou $-6b^2 = -26 \Longrightarrow b = \pm 2$ ou $b = \pm\sqrt{\frac{13}{3}} \Longrightarrow$

$\Longrightarrow b = \pm 2$ ($\theta = a + b\sqrt{6} = 5 + 2\sqrt{6}$ ou $5 - 2\sqrt{6} \longrightarrow$ unidades não triviais)

Portanto, os *elementos inversíveis e unidades* em $\mathbb{Z}[\sqrt{6}]$ são:

$$1,\ 5 + 2\sqrt{6} \quad \text{e} \quad 5 - 2\sqrt{6}\ \blacksquare$$

XV) Sabe-se que o anel A possui unidade e elemento inverso, se e somente se, a sua norma, nos inteiros, é dada por: $N(A) = \pm 1$.

$$N(A) = \frac{(a + b\sqrt{5})}{2}.\frac{(a - b\sqrt{5})}{2} = \pm 1 \Longrightarrow a^2 - 5b^2 = \pm 4$$

$$a = \pm 1 \Longrightarrow a^2 = 1 \Longrightarrow \begin{cases} -5b^2 = 3 \\ -5b^2 = -5 \end{cases} \Longrightarrow b = \pm 1$$

$$a = \pm 1 \text{ e } b = \pm 1 \Longrightarrow \frac{(a + b\sqrt{5})}{2} = \frac{(\pm 1 \pm \sqrt{5})}{2}$$

$$a = \pm 2 \Longrightarrow a^2 = 4 \Longrightarrow \begin{cases} -5b^2 = 0 \\ -5b^2 = -8 \end{cases} \Longrightarrow b = 0$$

$$a = \pm 2\ e\ b = 0 \Longrightarrow \frac{(a + b\sqrt{5})}{2} = \pm 1$$

São unidades e elementos inversos de A:

- $\frac{(\pm 1 \pm \sqrt{5})}{2}$
- ± 1
- $a_1 \text{ e } b_1 \in \mathbb{Z}, \text{tais que} - 5b_1^2 = \pm 4 - a_1^2$

Pode-se destacar o seguinte ponto:

$$\underbrace{-5b_1^2 = \pm 4 - a_1^2 \Leftrightarrow \pm\left(\frac{a_1 + b_1\sqrt{5}}{2}\right)}_{a_1 \text{ e } b_1 \text{ geram } \frac{(a+b\sqrt{5})}{2} \text{ UNIDADES}}$$

Na determinação das unidades de A, verifica-se que estas estruturas apresentam a seguinte forma, sendo n inteiro ou zero:

$$\pm\left(\frac{1+\sqrt{5}}{2}\right)^{n}$$

XVI) Sejam a, b, c e d inteiros tais que $f = a^2 + b^2$ e $g = c^2 + d^2$. Então, $f.g =$

$= (a^2 + b^2).(c^2 + d^2) = \mathrm{N}(a + ib).\mathrm{N}(c + id) = \mathrm{N}\big((a + ib).(c + id)\big)$

$= \mathrm{N}\big((ac - bd) + i(ad + bc)\big) = (ac - bd)^2 + (ad + bc)^2 = f.g$ ■

XVII) Sejam os naturais, a seguir, tomados a partir da seguinte hipótese:

$$\underbrace{x \equiv y \ (mod\ p)}_{p\ natural\ primo}$$

Sem perda de generalidade, suponha ainda $y \geq x$.

Assim, utilizando o seguinte resultado:

$$x \equiv y\ (mod\ k) \implies x^i \equiv y^i\ (mod\ k) \text{ para } i, k \in \mathbb{N}$$

Afirma-se que:

$$x^p \equiv y^p\ (mod\ p) \Longrightarrow \begin{cases} y^p - x^p = k.p;\ k \in \mathbb{N} \\ y^p - x^p \equiv 0\ (mod\ p) \end{cases}$$

Tem-se ainda que: $(y - x)^p \equiv y^p - x^p \equiv 0\ (mod\ p)$

E também: $x \equiv y\ (mod\ p) \implies (y - x) \equiv 0\ (mod\ p)$

Ao fim, tem-se o seguinte:

$$(y - x)^p = (y - x).(y^{p-1} + xy^{p-2} + x^2y^{p-3} + \cdots + x^{p-3}y^2 + x^{p-2}y + x^{p-1})$$

$$\underbrace{(y^{p-1} + xy^{p-2} + x^2y^{p-3} + \cdots + x^{p-3}y^2 + x^{p-2}y + x^{p-1}) \equiv p.x^{p-1}(mod\ p)}_{Fazendo:\ x \equiv y\ (mod\ p)}$$

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

$$\Longrightarrow y^p - x^p = (k_1.p).(k_2.p) = k.p^2$$

$$\Longrightarrow x^p \equiv y^p\ (mod\ p^2)$$ ■

XVIII) Sendo a e b são números reais positivos:

$$a^3 = a + 1 \Longrightarrow (a^3)^2 = (a+1)^2$$

$$\Longrightarrow a^6 = a^2 + 2a + 1$$

$$\Longrightarrow (\boldsymbol{a^6 - a}) = \boldsymbol{a^2 + a + 1}$$

$$b^6 = b + 3a \Longrightarrow (\boldsymbol{b^6 - b}) = \boldsymbol{3a}$$

$$(a-1)^2 \geq 0 \Longrightarrow a^2 + 1 \geq 2a \Longrightarrow a^2 + a + 1 \geq 3a$$

$$\Longrightarrow (a^6 - a) \geq (b^6 - b) \Longrightarrow (a^6 - b^6) \geq (a - b)$$

$$\Longrightarrow (a-b).\left(\underbrace{a^5 + a^4.b + a^3.b^2 + a^2.b^3 + ab^4 + b^5}_{=K>1,\ \text{pois a,b}\geq 1}\right) \geq (a-b)$$

$$\Longrightarrow (a-b).K \geq (a-b) \text{ com } K > 1$$

$$\Longrightarrow (a-b).(K-1) \geq 0 \Longrightarrow (a-b) \geq 0 \Longrightarrow a \geq b, \text{ pois } K > 1.$$

Assim: $a = b$ ou $a > b$.

Assumindo $a = b$, tem-se:

$$a = b \Longrightarrow \begin{cases} (a^6 - a) = (b^6 - a) = a^2 + a + 1 \\ (b^6 - b) = (a^6 - a) = 3a \end{cases}$$

$$a = b \Longrightarrow a^2 + a + 1 = 3a \Longrightarrow a^2 - 2a + 1 = (a-1)^2 = 0 \Longrightarrow a = 1$$

Considerando: $a = b = 1$, verifica-se $(1^6 - 1) \neq 3.(1)$.

Portanto: $a > b$. ■

XIX) $a + b + c = 0 \Longrightarrow a + b = -c \Longrightarrow (a+b)^3 = (-c)^3 = -c^3$

$$\Longrightarrow a^3 + 3a^2b + 3ab^2 + b^3 = -c^3 \Longrightarrow a^3 + b^3 + c^3 = -(3a^2b + 3ab^2)$$

$$\Longrightarrow a^3 + b^3 + c^3 = -3ab\underbrace{(a+b)}_{=-c} = (-3ab).(-c)$$

$$\Longrightarrow a^3 + b^3 + c^3 = 3abc$$ ■

XX) Para a resolução deste exercício, tem-se que são **6 (seis) os restos possíveis**, conforme pode-se verificar na tabela a seguir:

$\boldsymbol{n \equiv k_1 (mod\ 11) \Longrightarrow n^2 \equiv (k_1)^2 (mod\ 11)}$	
$\boldsymbol{k_1}$	$\boldsymbol{(k_1)^2}$
$\bar{0}$	$\bar{0}$
$\pm\bar{1}$	$\bar{1}$
$\pm\bar{2}$	$\bar{4}$
$\pm\bar{3}$	$\bar{9}$
$\pm\bar{4}$	$\overline{16} = \bar{5}$
$\pm\bar{5}$	$\overline{25} = \bar{3}$

XXI) Seja $\mathrm{N} = 12\mathrm{x}11\mathrm{x}10\mathrm{x} \ldots \mathrm{x}3\mathrm{x}2\mathrm{x}1$

$\mathrm{N} + 14 \equiv 0\ (mod\ 13) \Longrightarrow \mathrm{N} \equiv -14 \equiv -14 + 26 \equiv 12\ (mod\ 13)$

Assim, N é um número da forma $\mathrm{N} = 13\mathrm{k} + 12$

$13\mathrm{x}12\mathrm{x} \ldots \mathrm{x}3\mathrm{x}2\mathrm{x}1 = 13\mathrm{N} = 13.(13\mathrm{k} + 12) = 13^2k + (13).(12)$

$13\mathrm{x}12\mathrm{x} \ldots \mathrm{x}3\mathrm{x}2\mathrm{x}1 = 169k + 156 \equiv \mathbf{156}\ (mod\ 169)$.

Portanto, o resto que se pede é $\mathbf{156}$. ■

CONCLUSÃO

Neste trabalho, realizou-se uma fundamentação teórica em Aritmética e em Teoria Algébrica e uma breve apresentação histórica para subsidiarem o entendimento das etapas necessárias à demonstração do *Último Teorema de Fermat* – UTF $(n = 5)$ e, adicionalmente, para facilitarem a realização das atividades propostas, que reforçam e complementam aspectos teóricos, focalizados na demonstração principal.

Possivelmente, pela densidade das demonstrações deste texto, este proporcionará um aumento da *maturidade matemática* aos seus mais persistentes leitores. De fato, o entendimento das estruturas lógicas, bem como o encadeamento dos passos das demonstrações tendem a levar os seus leitores à necessidade de elaboração e de reelaboração de diferentes ideias algébricas.

O público que irá ler este trabalho deve ser constituído, principalmente, por professores de matemática, alunos de graduação em ciências exatas, autodidatas e alunos de ensino médio com boa curiosidade matemática.

No desenvolvimento deste trabalho, assumiu-se o pressuposto de que tanto o compêndio teórico como as atividades propostas são suficientes, pelo menos, para o entendimento da ideia geral do UTF $(n = 5)$.

A proposta didática desta Dissertação vai além da apresentada no Capítulo de curiosidades, exemplos e atividades, pois, idealmente, espera-se que os passos da demonstração sejam refeitos sem consulta ao seu texto base após a leitura do trabalho.

Um ponto de destaque é que a relevância da leitura do teorema não está no conhecimento da demonstração por si só, mas, sim, no desenvolvimento do "*pensamento matemático*", responsável pelo desenvolvimento contínuo de novas ideias matemáticas.

Almeja-se que este trabalho acadêmico sirva de importante fonte de consulta na *Base de Dados das Dissertações* do **PROFMAT** para os leitores desta temática.

REFERÊNCIAS BIBLIOGRÁFICAS

ACZEL, Amir D. **El Último Teorema de Fermat** – *El secreto de um antiguo problema matemático*. 1.ed. Four Walls Eight Windows, 2003.

AEBISCHER, A.M. Institut de Recherche sur l'Enseignement des Mathématiques de Franche-Comté: **Le fabuleux destin du théorème de Fermat**. Apresentação disponível em: <http://www-irem.univ-fcomte.fr/download/irem/document/ressources/fermat.pdf> Acesso em: 7 jun. 2019.

ALKALAY-HOULIHAN, C. McGill University **– Sophie Germain and Special Cases of Fermat's Last Theorem.** Disponível em: <http://www.math.mcgill.ca/darmon/courses/12-13/nt/projects/Colleen-Alkalay-Houlihan.pdf> Acesso em: 5 mai. 2019.

ANDRADE, José Fernandes. **Anéis Quadráticos Euclidianos**. Revista Matemática Universitária (RMU) nº48 e 49, 2012. Disponível em: <https://rmu.sbm.org.br/wp-content/uploads/sites/27/2018/03/n48_n49_Artigo05.pdf> Acesso em: 6 mai. 2019.

ÁVILA, Geraldo. **Várias Faces da Matemática** – *Tópicos para Licenciatura e Leitura Geral*. 2.ed. Editora Edgard Blücher, 2010.

BARBARA, Roy. **Fermat's Last Theorem in the Case n = 4**. The Mathematical Gazette Vol. 91, Nº. 521, 2007, pp. 260-262. Disponível em: <https://www.jstor.org/stable/40378352> Acesso em: 3 mai.2019.

_____. **Fermat's Last Theorem for the Exponent 3**. Publicado em 2016. Disponível em: <https://arxiv.org/pdf/1602.06726.pdf> Acesso em: 3 mai.2019.

BÁYER, P. **El Teorema de Fermat**. Publicacions de la Secció de Matemàtiques, Nº 2, 1976, pp. 94-110. Disponível em: < https://www.jstor.org/stable/43741372> Acesso em: 5 out. 2018.

BEUTER, Viviane Maria. **O Anel dos Inteiros Quadráticos**. Florianópolis, 2008. Monografia (Bacharelado em Matemática). Departamento de Matemática, Universidade Federal de Santa Catarina (UFSC). Disponível em: <https://repositorio.ufsc.br/bitstream/handle/123456789/119173/Viviane_Maria_Beuter.pdf?sequence=1&isAllowed=y> Acesso em: 3 abr. 2019.

BIOGRAFIA DE FERMAT (SOmatemática). Disponível em: <https://www.somatematica.com.br/biograf/fermat.php> Acesso em: 14 abr. 2019.

BIOGRAFIA DE SOPHIE GERMAIN (SOmatemática). Disponível em: <https://www.somatematica.com.br/biograf/sophie.php> Acesso em: 14 abr. 2019.

BOEING, Franciele. **Fatoração Única em Anéis Ciclotômicos e o Último Teorema de Fermat**. Joinville, 2013. Trabalho de Conclusão de Curso (Licenciatura em Matemática). Universidade do Estado de Santa Catarina (UDESC).

BOEING, Franciele; BEUTER, Viviane. **Fatoração Única em Anéis Ciclotômicos e o Último Teorema de Fermat**. 1.ed. Novas Edições Acadêmicas, 2015.

BOYER, Carl B. **História da Matemática**. 3.ed. Editora Edgard Blücher, 2012.

BLOG (FermatsLastTheorem.blogspot.com): **Fermat's Last Theorem**. Disponível em: <http://fermatslasttheorem.blogspot.com> Acesso em: 2 abr. 2019.

BYERLEY, Cameron. **Applications of Number Theory to Fermat's Last Theorem**. Disponível no site do Whitman College em: <https://www.whitman.edu/Documents/Academics/Mathematics/byerleco.pdf> Acesso em: 2 jun. 2019.

CANAL YOUTUBE: Cultura Fractal. **A matemática nos 30 anos de "Os Simpsons"**. Disponível em: <https://www.youtube.com/watch?v=F_4cO0Xz6qg> Acesso em: 2 set. 2019.

CARNEIRO, José Paulo Q. **O Princípio da Descida Infinita de FERMAT**. Revista do Professor de Matemática – RPM – nº 32, 1993. Disponível em: <http://www.rpm.org.br/cdrpm/32/8.htm> Acesso em: 6 abr. 2019.

CATALDO, João Carlos *et al*. **Tópicos de Aritmética – Volume 2**. 1.ed. MATVEST.

CLARK, Pete L. Homepage – Department of Mathematics, University of Georgia. **Number Theory: A Contemporary Introduction**. Disponível em: <http://math.uga.edu/~pete/4400FULL.pdf> Acesso em: 5 abr. 2019.

_____. Homepage – Department of Mathematics, University of Georgia. **The Fermat Equation**. Disponível em: <http://math.uga.edu/~pete/4400flt4.pdf> Acesso em: 5 abr. 2019.

COUTINHO, S. C. **Polinômios e Computação Algébrica Números**. 1.ed. IMPA-SBM, 2012.

COX, David A. **Introduction to Fermat's Last Theorem**. *The American Mathematical Monthly*, Vol. 101, Nº1, 1994, pp. 3-14. Disponível em: <https://www.jstor.org/stable/2325116> Acesso em: 19 ago. 2018.

_____. **Primes of the Form $x^2 + ny^2$** – *Fermat, Class Field Theory, and Complex Multiplication*. 2. ed. John Wiley & Sons Inc., 2013.

DANILOFF, Lene-Lise. **The Work of Sophie Germain and Niels Henrik Abel on Fermat's Last Theorem**. Master thesis, University of Oslo, 2017. Disponível em: <https://www.duo.uio.no/bitstream/handle/10852/57807/daniloff_master.pdf?sequence=1&isAllowed=y> Acesso em: 6 nov. 2019.

DASSEN, Erwin. **Teoria Algébrica de Números, Extensões Ciclotômicas e o Último Teorema de Fermat: a demonstração de Ernst Kummer**. Florianópolis, 2005. Dissertação de Mestrado. Universidade Federal de Santa Catarina (UFSC).

DICKSON, L.E. **Fermat's Last Theorem and the Origin and Nature of the Theory of Algebraic Numbers**. Annals of Mathematics, Second Series, Vol. 18, Nº 4, 1917, pp. 161-187. Disponível em: <https://www.jstor.org/stable/2007234> Acesso em: 5 out. 2018.

Dictionnaire des MATHÉMATIQUES à l'usage des professeurs de mathématiques et des élèves des lycées & collèges: **Grand théorème de Fermat , cas n = 3**. Disponível em: <http://serge.mehl.free.fr/anx/th_fermat_gd3.html> Acesso em: 4 abr. 2019.

Dictionnaire des MATHÉMATIQUES à l'usage des professeurs de mathématiques et des élèves des lycées & collèges: **Grand théorème de Fermat, cas n = 4**. Disponível em: <http://serge.mehl.free.fr/anx/th_ferm4.html> Acesso em: 4 abr. 2019.

Dictionnaire des MATHÉMATIQUES à l'usage des professeurs de mathématiques et des élèves des lycées & collèges: **Pierre Simon de FERMAT, français**. Disponível em: <http://serge.mehl.free.fr/chrono/Fermat.html#Gth> Acesso em: 4 abr. 2019.

DOLAN, Stan. **Pell's equation and Fermat**. The Mathematical Gazette, Vol. 96, Nº 535, 2012, pp. 66-70. Disponível em: <https://www.jstor.org/stable/23249517> Acesso em: 5 out. 2018.

DOMINGUES, Hygino; IEZZI, Gelson. **Álgebra Moderna**. 5.ed. SARAIVA, 2018.

DOMINGUES, Hygino. **Fundamentos da Aritmética**. 2.ed. Editora UFSC, 2009.

EDWARDS, Harold. **Fermat's Last Theorem** – *A Genetic Introduction to Algebraic Number Theory.* 1.ed. Springer-Verlag, 1977.

_____. **The Background of Kummer's proof of Fermat's Last Theorem for Regular Primes**. Arch. Rational Mech. 14, 219–236 (1975). Disponível em: <https://doi.org/10.1007/BF00327448> Acesso em: 6 jun. 2019.

ELLENBERB, Jordan. **O Poder do Pensamento Matemático** – *A Ciência de como não estar errado*. 1.ed. ZAHAR, 2015.

ENDLER, Otto. **Teoria dos Números Algébricos**. 2.ed. IMPA-SBM, 2014.

EVES, Howard. **Introdução à História da Matemática**. 5.ed. Editora Unicamp, 2011.

FERREIRA, Áurea. **O Último Teorema de Fermat**. Trabalho de Conclusão de Curso (Licenciatura em Matemática). Universidade Federal do Amapá. Disponível em: <https://www2.unifap.br/matematicaead/files/2016/03/TCC-AUREA-pronto-ok.pdf> Acesso em: 9 abr. 2019.

FUJIWARA, Guilherme. **Inteiros de Gauss e Inteiros de Eisenstein** – das páginas 23 a 31 da Revista Eureca nº 14 (2002). Disponível em: <https://www.obm.org.br/content/uploads/2017/01/eureka14.pdf> Acesso em: 8 abr. 2019.

GARBI, Gilberto Geraldo. **O Romance das equações Algébricas**. 4.ed. Livraria da Física, 2010.

GARCIA, Arnaldo; LEQUAIN, Yves. **Elementos de Álgebra**. 6.ed. IMPA-SBM, 2015.

GAZETA MATEMÁTICA (Sociedade Portuguesa de Matemática). **A Vida e o Trabalho de Sophie Germain**. Publicação de Janeiro de 2004, Nº 146. Disponível em: <http://gazeta.spm.pt/getArtigo?gid=89> Acesso em: 5 mai.2019.

GIL, Antônio Carlos. **Como Elaborar Projetos de Pesquisa**. 4.ed. Editora Atlas, 2002.

GIROUARD, Alexandre. Enseignement: **Relations d'Équivalence**. Disponível em: <https://archimede.mat.ulaval.ca/agirouard/enseignement/AlgGeo/Cours3.pdf> Acesso em: 3 mar. 2019.

GONÇALVES, Adilson. **Introdução à Álgebra**. 5.ed. IMPA-SBM, 2003.

GOUVÊA, F. Q. **Uma demonstração maravilhosa**. Revista Matemática Universitária, n.19, p. 16-43, Dezembro 1995. Disponível em: <https://rmu.sbm.org.br/wp-content/uploads/sites/27/2018/03/n19_Artigo03.pdf> Acesso em: 4 mai.2019.

GRAY, Jeremy. **A History of Abstract Algebra** – *From Algebraic Equations to Modern Algebra*. 1.ed. Springer, 2018.

HARDY, G. H.; WRIGHT, E. M. **An Introduction to The Theory of Numbers**. 6.ed. Oxford Mathematics, 2008.

HEFEZ, Abramo. **Aritmética (Coleção Profmat)**. 2.ed. SBM, 2016.

HEFEZ, Abramo; VILLELA, Maria L. Torres. **Polinômios e Equações Algébricas (Coleção Profmat)**. 1.ed. SBM, 2012.

HELLEGOUARCH, Yves. **Invitation aux Mathématiques de Fermat-Wiles**. 2.ed. Masson, 1997.

HERSTEIN, N. **Tópicos de Álgebra**. 1.ed. EDUSP, 1970.

HILL, Richard. **Introduction to Number Theory**. 1.ed. World Scientific, 2018.

JAGGIA, Akash. McGill University **– On Fermat's Method of Infinite Descent**, 2013. Disponível em: <http://www.math.mcgill.ca/darmon/courses/12-13/nt/projects/Akash-Jaggia.pdf> Acesso: 2 abr. 2019.

JARVIS, Frazer. **Algebraic Number Theory**. 1.ed. Springer, 2014.

KLEINER, Israel. **A History of Abstract Algebra**. 1.ed. Birkhäuser, 2007.

LANDAU, Edmund. **Teoria Elementar dos Números**. 1.ed. Ciência Moderna, 2002.

LANG. Serge. **Álgebra para Graduação**. 1.ed. Ciência Moderna, 2008.

LANGEVIN, Philippe. Université de Toulon. **Le Dérnier Théorème de Fermat**. Notas de aula disponíveis em: L<http://langevin.univ-tln.fr/notes/Fermat/fermat.pdf> Acesso em: 7 jun. 2019.

MADEIRA, Renato. *Superpoderes Matemáticos para Concursos Militares* – **Volume 5 (Colégio Naval: 25 anos de provas resolvidas)**. 2. ed. Dissonnarte, 2017.

MARQUES, Cristina Maria. Departamento de Matemática da UFMG. **APOSTILA de Introdução à Teoria de Anéis**, 1999 (revisada em 2005).

Matéria com o Andrew Wiles (**Prêmio Abel de 2016**). Disponível em: <http://g1.globo.com/ciencia-e-saude/noticia/2016/03/matematico-que-solucionou-problema-de-357-anos-recebe-premio-abel.html> Acesso em: 5 jun. 2019.

MENDES, Dheleon de Barcellos. **Uma Introdução aos Anéis Principais e Fatoriais**. Florianópolis, 2005. Monografia (Licenciatura em Matemática). Departamento de Matemática, Universidade Federal de Santa Catarina (UFSC). Disponível em: <https://repositorio.ufsc.br/xmlui/bitstream/handle/123456789/96429/Dheleon_de_Barcellos_Mendes.pdf?sequence=1&isAllowed=y> Acesso em: 3 abr. 2019.

MISAGHIAN, Manouchehr. **Factor Rings and their decompositions in the Eisenstein integers Ring** $\mathbb{Z}[w]$. Armenian Journal of Mathematics, 2013, Volume 5, Number 1, 58-68. Disponível em: <http://ajm.asj-oa.am/263/1/AJMv5i1a4.pdf> Acesso em: 10 abr. 2019.

Monografia da Disciplina de Mestrado Anéis e Corpos do Professor Fernando Torres (UNICAMP). Autores: MARTINS, Michel; MOREIRA, Paula. **Decomposições no Anel** $\mathbb{Z}[w]$ **dos Inteiros de Eisenstein**. 2014. Disponível em: <https://www.ime.unicamp.br/~ftorres/ENSINO/MONOGRAFIAS/MP_M1AC2014.pdf> Acesso em: 4. Jun. 2019.

Monografia da Disciplina de Mestrado Anéis e Corpos do Professor Fernando Torres (UNICAMP). Vários autores. **Sobre Domínios Euclidianos**. Disponível em: <https://www.ime.unicamp.br/~ftorres/ENSINO/MONOGRAFIAS/Felipe_M1_AC_2011.pdf> Acesso em: 4. Jun. 2019.

MÖRSCHBÄCHER, Carla. **Redução do Último Teorema de Fermat para Expoente Primo**. Florianópolis, 2007. Monografia (Licenciatura em Matemática). Departamento de Matemática, Universidade Federal de Santa Catarina (UFSC). Disponível em: <https://repositorio.ufsc.br/bitstream/handle/123456789/119186/Carla_Morschbacher.pdf?sequence=1&isAllowed=y> Acesso em: 3 abr. 2019.

MOREIRA, Carlos Gustavo; MARTÍNEZ, Fábio. **Primos Gêmeos, Primos de Sophie Germain e o Teorema de Brun**. Revista Matemática Universitária (RMU) nº48 e 49,

2012. Disponível em: <https://rmu.sbm.org.br/wp-content/uploads/sites/27/2018/03/n48_n49_Artigo06.pdf> Acesso em: 6 mai. 2019.

MOREIRA, Carlos Gustavo T. de A. *et al.* **Tópicos de Teoria dos Números (Coleção Profmat)**. 1.ed. SBM, 2012.

MUSIELAK, Dora. **Germain and Her Fearless Attempt to Prove Fermat's Last Theorem**. Publicado em 2019. Disponível em: <https://arxiv.org/pdf/1904.03553.pdf> Acesso em: 3 set. 2019.

NYAMBUYA, Golden. **On a Simpler, Much More General and Truly Marvellous Proof of Fermat's Last Theorem (II)**. Publicado em 2015. Disponível em: <https://vixra.org/pdf/1405.0023v4.pdf> Acesso em: 2 set. 2019.

NASCIMENTO, Sebastião V. **Desvendando os Segredos dos Problemas da Matemática e Descobrindo Caminhos para Resolvê-los**. 1.ed. Ciência Moderna, 2008.

NICOLAU, Saldanha (PUC Rio). **Página do artigo da Prova de Andrew Wiles**. Disponível em: <http://www.mat.puc-rio.br/~nicolau/olimp/Wiles.pdf>. Acesso em: 4 mai. 2019.

NIVEN, Ivan. **Números Racionais e Irracionais**. 1.ed. SBM, 2012.

Notas de Aula de Elementos da Teoria dos Números – Professores da UNESP. Disponível em: <http://wwwp.fc.unesp.br/~mauri/TN/TN.pdf> Acesso em: 2 abr.2019.

OHANA, R.Andrew. **On Fermat's Last Theorem for $n = 3$ and $n = 4$**. Disponível em: <https://wstein.org/edu/2010/414/projects/ohana.pdf> Acesso em: 4 jun. 2019.

OLIVEIRA, Krerley e FERNÁNDEZ, Adán. **Iniciação à Matemática: um curso com problemas e soluções** (*Coleção Olimpíadas de Matemática*). 2.ed. SBM, 2012.

PAIVA, Santiago. McGill University **– Elliptic Curve Cryptosystems**. Disponível em: <http://www.math.mcgill.ca/darmon/courses/12-13/nt/projects/Santiago-Paiva.pdf> Acesso em: 5 jun. 2019.

PICADO, Jorge. Homepage – Departamento de Matemática, Universidade de Coimbra. **Apontamentos de Aula sobre Anéis (revisitados)**. Disponível em: <http://www.mat.uc.pt/~picado/algcom/apontamentos/cap1.pdf> Acesso em: 4 abr. 2019.

PINTO, Ronald; COSTA, Liliana. **A Irracionalidade e Transcendência de certos Logaritmos**. Revista Eletrônica da SBM (Professor de Matemática ONLINE), Nº 1, Vol. 6, páginas 68-75, 2018. Disponível em: <http://pmo.sbm.org.br/wp-content/uploads/sites/16/dlm_uploads/2019/03/art6_vol6_2018_SBM_PMO-1.pdf> Acesso em: 4 set. 2019.

POGORELSKY, Bárbara. **Algumas Generalizações para o Último Teorema de Fermat**. Porto Alegre, 2005. Dissertação de Mestrado. Universidade Federal do Rio Grande do Sul (UFRGS).

PROFMAT – *Base de Dados das Dissertações.* BRITO, Francisco. **Resolução de Problemas via Inteiros Algébricos**. Universidade do Federal do Ceará (UFCE), 2017. Disponível em: <https://sca.profmat-sbm.org.br/sca_v2/get_tcc3.php?id=150160865> Acesso em: 6 ago. 2019.

PROFMAT – *Base de Dados das Dissertações.* BRUNO, Salvador da Silva. **O Último Teorema de Fermat para $n = 3$**. Universidade Federal do Estado do Rio de Janeiro (UNIRIO), 2014. Disponível em: <https://sca.profmat-sbm.org.br/sca_v2/get_tcc3.php?id=1396 > Acesso em: 10 jun. 2018.

PROFMAT – *Base de Dados das Dissertações.* CASTRO, Isabela Souza. **O Último Teorema de Fermat nos Ensinos Fundamental e Médio**. Universidade Federal de Viçosa (UFV), 2019. Disponível em: <https://sca.profmat-sbm.org.br/sca_v2/get_tcc3.php?id=170940301 > Acesso em: 11 jun. 2019.

PROFMAT – *Base de Dados das Dissertações.* DIAS, Olavo Gustave W. Gonçalves. **Do Teorema de Pitágoras ao Último Teorema de Fermat:** *um resgate histórico e uma proposta de aplicação no Ensino Básico***.** Universidade do Estado de Santa Catarina (UDESC), 2018. Disponível em: <https://sca.profmat-sbm.org.br/sca_v2/get_tcc3.php?id=161011351> Acesso em: 6 abr. 2019.

PROFMAT – *Base de Dados das Dissertações.* FORTES, Renato. **Soluções de certas congruências quadráticas.** Universidade do Federal do Mato Grosso (UFMT), 2017. Disponível em: < https://sca.profmat-sbm.org.br/sca_v2/get_tcc3.php?id=150310311> Acesso em: 7 ago. 2019.

PROFMAT – *Base de Dados das Dissertações.* GOMES, Ataniel. **Uma abordagem do ensino de congruência na educação básica**. Universidade Federal de Sergipe (UFS),

2015. Disponível em: <https://sca.profmat-sbm.org.br/sca_v2/get_tcc3.php?id=73678> Acesso em: 5 mai. 2019.

PROFMAT – *Base de Dados das Dissertações.* JÚNIOR, Sérgio dos Santos. **Criptografia via curvas elípticas.** Universidade Federal do Estado do Rio de Janeiro (UNIRIO), 2013. Disponível em: <https://sca.profmat-sbm.org.br/sca_v2/get_tcc3.php?id=29995> Acesso em: 5 mai. 2019.

PROFMAT – *Base de Dados das Dissertações.* LIMA, Luciana. **O Anel dos Inteiros de Gauss**. Universidade Federal do Estado do Rio de Janeiro (UNIRIO), 2016. Disponível em: <https://sca.profmat-sbm.org.br/sca_v2/get_tcc3.php?id=84484> Acesso em: 10 jun. 2018.

PROFMAT – *Base de Dados das Dissertações.* NASCIMENTO, Antônio. **Corpos Finitos e dois Problemas Olímpicos**. Universidade do Federal do Ceará (UFCE), 2019. Disponível em: <https://sca.profmat-sbm.org.br/sca_v2/get_tcc3.php?id=170162091> Acesso em: 6 ago. 2019.

PROFMAT – *Base de Dados das Dissertações.* SOUZA, João Paulo de Araújo. **Alguns Casos do Último Teorema de Fermat**. Universidade do Federal do Cariri (UFCA), 2019. Disponível em: <https://sca.profmat-sbm.org.br/sca_v2/get_tcc3.php?id=170170424> Acesso em: 6 jun. 2019.

Quang, Nguyen Van. **Euler's proof of Fermat's Last Theorem for n = 3 is incorrect**. Vietnam, 2016. Disponível em: <http://vixra.org/pdf/1605.0123v1.pdf> Acesso em: 4 abr. 2019.

_____. **Fermat's last theorem is wrong**. Vietnam, 2017. Disponível em: < http://vixra.org/pdf/1701.0397v1.pdf> Acesso em: 4 abr. 2019.

_____. **Is Dirichlet's proof of Fermat's Last Theorem for n = 5 flawed**. Vietnam, 2016. Disponível em: < https://rxiv.org/pdf/1607.0400v1.pdf> Acesso em: 4 abr. 2019.

RIBENBOIM, Paulo. **Fermat's Last Theorem For Amateurs**. 1.ed. Springer, 1999.

_____. **13 Lectures on Fermat's Last Theorem**. 1.ed. Springer-Verlag, 1979.

_____. **Números Primos** – *Velhos Mistérios e Novos Recordes*. 1.ed. IMPA-SBM, 2014.

ROMAGNY, Matthieu. CONFÉRENCE (Université Rennes, 2008) – **Le théorème de Fermat: huit ans de solitude**. Disponível em: <https://perso.univ-rennes1.fr/matthieu.romagny/exposes/conference_fermat.pdf> Acesso em: 20 abr. 2019.

SAIKIA, Manjil P. **A Study of Kummer's Proof of Fermat's Last Theorem for Regular Primes**. Publicado em 2013. Disponível em: <https://arxiv.org/pdf/1307.3459.pdf> Acesso em: 3 set. 2019.

SÁNCHEZ, Andrés Martín. **El Último Teorema de Fermat**. Anuario del Centro de la Universidad Nacional de Educación a Distancia en Calatayud, Nº 21, pp. 153-171, 2015. Disponível em: <http://www.calatayud.uned.es/web/actividades/revista-anales/21/03-07-AndresMartinSanchez.pdf> Acesso em: 4 abr. 2019.

SANTOS, J. P. O. **Introdução à Teoria dos Números**. 3.ed. IMPA-SBM, 2015.

SANTOS, A.L. S. (Gandhi). **Problemas Selecionados de Matemática**. 1.ed. Ciência Moderna, 2006.

SHINE, Carlos Yuzo. **21 Aulas de Matemática Olímpica**. 1.ed. IMPA-SBM, 2009.

SHOKRANIAN, Salahoddin. **Álgebra 1**. 1.ed. Ciência Moderna, 2010.

_____. **Uma Breve História da Teoria dos Números no Século Vinte**. 1.ed. Ciência Moderna, 2010.

SILVA, Daniel. **O Último Teorema de Fermat**. Rio de Janeiro, 2010. Trabalho de Conclusão de Curso. Instituto de Matemática e Estatística da Universidade do Estado do Rio de Janeiro (UERJ). Disponível em: <http://www.professores.uff.br/rsalomao/wp-content/uploads/sites/93/2017/08/danielcunha.pdf> Acesso em: 4 abr. 2019.

SILVA, Jhone C.; GOMES, Olímpio R. **Estruturas Algébricas para Licenciatura** – **Volume 2** – *Elementos de Aritmética Superior*. 1.ed. Editora Edgard Blücher, 2018.

SILVA, Franciele do Carmo. **O Último Teorema de Fermat: Casos Especiais**. Juiz de Fora, 2018. Trabalho de Conclusão de Curso (Bacharelado em Matemática). Departamento de Matemática, Universidade Federal de Juiz de Fora (UFJF). Disponível em:<http://www.ufjf.br/matematica/files/2014/02/TCC_Franciele_versaofinal.pdf> Acesso em: 4 abr. 2019.

SILVEIRA, Tamara. **Elementos da Teoria dos Números Algébricos**. Joinville, 2013. Trabalho de Graduação (Licenciatura em Matemática). Centro de Ciências Tecnológicas, Universidade do Estado de Santa Catarina (UDESC). Disponível em: <http://sistemabu.udesc.br/pergamumweb/vinculos/00001a/00001adb.pdf> Acesso em: 2 abr. 2019.

SINGH, Simon. **Fermat's Last Theorem** – *The Story of a Riddle that confounded the World's Greatest Minds for 358 years*. 1.ed. Fourth Estate Ltd, London, 1997.

_____. **Fermat's Enigma** – *The Epic Quest to Solve the World's Greatest Mathematical Problem*. 1.ed. Walker and Company, New York, 1997.

_____. **O Último Teorema de Fermat** – *A História do enigma que confundiu as maiores mentes do mundo durante 358 anos*. 10.ed. Record, 2004.

_____. **Os Segredos Matemáticos dos Simpsons**. 1.ed. Record, 2016.

SOUZA, Talita Bogler. **Os Três Séculos do Último Teorema de Fermat**. Artigo apresentado na XXIV Semana Acadêmica da Matemática da Universidade Estadual do Oeste do Paraná (UNIOESTE) em 2010. Disponível em: <http://projetos.unioeste.br/cursos/cascavel/matematica/xxivsam/artigos/38.pdf> Acesso em: 3 abr. 2019.

STEWART, Ian; TALL, David. **Algebraic Number Theory and Fermat's Last Theorem**. 4.ed. CRC Press, 2016.

STEWART, Ian. **Os Maiores Problemas Matemáticos de Todos os Tempos**. 1.ed. ZAHAR, 2014.

_____. **Os Mistérios Matemáticos do Professor Stewart**. 1.ed. ZAHAR, 2015.

TAO, Terence. **Como Resolver Problemas Matemáticos** – *Uma Perspectiva Pessoal*. 1.ed. SBM, 2013.

VIDIGAL, Ângela *et al*. **Fundamentos de Álgebra**. 1.ed. Editora UFMG, 2009.

VIEIRA, Vandenberg L. **Álgebra Abstrata para Licenciatura**. 1.ed. Livraria da Física e EDUEPB, 2013.

_____. **Um Curso Básico em Teoria dos Números**. 1.ed. Livraria da Física e EDUEPB, 2015.

WALTER, Charles. **CHAPITRE 5: Les Théorèmes de deux carrés**. Disponível em: <https://math.unice.fr/~walter/L1_Arith/cours5.pdf> Acesso em: 3 mar. 2019

WIKIPÉDIA-FRANÇA: **Anneau des entiers de $\mathbb{Q}(\sqrt{5})$**. Disponível em: <https://fr.wikipedia.org/wiki/ Anneau_des_entiers_de_Q(√5)> Acesso em: 5 abr. 2019.

WIKIPÉDIA-FRANÇA: **Démonstration du dernier théorème de Fermat pour les exposants 3, 4 et 5**. Disponível em: <https://fr.wikipedia.org/wiki/ Démonstration_du_dernier_théorème_de_Fermat_pour_les_exposants_3,_4_et_5> Acesso em: 5 abr. 2019.

WIKIPÉDIA-ESPANHA: **Entero cuadrático**. Disponível em: <https://es.wikipedia.org/wiki/Entero_cuadrático> Acesso em: 5 abr. 2019.

WIKIPÉDIA-PORTUGAL: **Resolução do último teorema de Fermat**. Disponível em: <https://pt.wikipedia.org/wiki/Resolução_do_último_teorema_de_Fermat/> Acesso em: 5 abr. 2019.

WIKIWAND-PORTUGAL: **Último teorema de Fermat**. Disponível em: <https://www.wikiwand.com/pt/Último_teorema_de_Fermat> Acesso em: 6 mai. 2019.

APÊNDICE – Prova dos Lemas da Equação Fermatiana Quíntupla

Serão provados os Lemas 1 e 2, que se aplicam, exclusivamente, às potências quíntuplas.

Em ambos os Lemas, utiliza-se o conceito dos Inteiros do Anel de Dedekind, denotados por A. Os Inteiros de Dedekind (A) são um anel de inteiros no corpo $\mathbb{Q}(\sqrt{5})$.

$$\mathrm{A} = \mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right]$$

Os inteiros λ, elementos de A, podem ser escritos da seguinte forma:

$$\begin{cases} \lambda = \dfrac{w_1 + w_2\sqrt{5}}{2} \\ \text{com } \underbrace{w_1 \equiv w_2 \ (mod\ 2)}_{\substack{w_1\ e\ w_1\ têm\ a\ mesma \\ paridade}} \end{cases}$$

Temos também que os elementos inversíveis de A representam as suas unidades.

Assim:

$$\lambda = \frac{w_1 + w_2\sqrt{5}}{2}$$

É unidade de A, se e somente se, a sua norma, definida por $N: \mathrm{A} \longrightarrow \mathbb{Z}$, é representada por:

$$N(\lambda) = \frac{(w_1 + w_2\sqrt{5})}{2} . \frac{(w_1 - w_2\sqrt{5})}{2} = \frac{(w_1^2 - 5w_2^2)}{4} = \pm 1$$

Neste caso, afirma-se ainda: $w_1^2 - 5w_2^2 = \pm 4$.

Sabe-se que as unidades de A podem ser representadas por elementos que apresentam a seguinte forma, onde e representa um número inteiro:

$$\pm\left(\frac{1+\sqrt{5}}{2}\right)^{\mathrm{e}}$$

Destaca-se que os elementos de A podem ser escritos, de forma única, como um produto de potências de primos.

No caso, os primos são também irredutíveis, pois temos domínios fatoriais. Tal argumento pode ser verificado com o exemplo dos números 2 e $\sqrt{5}$ em que ambos são elementos primos e irredutíveis em A.

Nas demonstrações, a seguir, serão analisadas as potências quíntuplas de A.

Lema 1 – Para o Teorema da Equação Fermatiana Quíntupla

Sejam a e b inteiros não negativos com:

$$mdc\ (a,b) = 1; a \not\equiv b\ (mod\ 2); 5 \nmid a;\ \text{e}\ 5 \mid b$$

Se $(\boldsymbol{a^2 - 5b^2})$ é a quinta potência de um elemento do Anel A, então existem c e d, inteiros não nulos, tais que:

$$\begin{cases} a = c.(c^4 + 50c^2d^2 + 125d^4) \\ b = 5d.(c^4 + 10c^2d^2 + 5d^4) \end{cases}$$

onde: $mdc\ (c,d) = 1;\ c \not\equiv d\ (mod\ 2);\ \text{e}\ 5 \nmid c.$

Prova: Verifica-se, uma vez provada a existência dos inteiros não nulos c e d, que os números inteiros a e b podem ser escritos da seguinte forma:

$$\begin{cases} a = c.(c^4 + 50c^2d^2 + 125d^4) \\ b = 5d.(c^4 + 10c^2d^2 + 5d^4) \end{cases}$$

Tem-se que $mdc\ (c,d) = 1$, pois $\underbrace{mdc\ (a,b) = 1}_{da\ hipótese}$.

Logo, c e d não são ambos pares.

Assim, estudando ainda as paridades de a e b, a partir das paridades de c e d, tem-se que c e d não podem ser ambos ímpares, pois, caso contrário, a e b seriam ambos pares, contrariando, desta forma, a hipótese de que $a \not\equiv b\ (mod\ 2)$.

Portanto, c e d apresentam *diferentes paridades*.

Sabe-se ainda que b é múltiplo de 5. Tem-se ainda:

$$\underbrace{5 \mid b \Longrightarrow 5 \nmid a}_{mdc\ (a,b)=1} \Longrightarrow 5 \nmid c$$

Provemos, nos passos seguintes, a existência de c e d.

Afirmação 1 – Sendo a e b inteiros não negativos e tomando ainda os inteiros h e k, tais que $h \equiv k\ (mod\ 2)$, pode-se afirmar que se:

$$a + b\sqrt{5} = \left(\frac{h + k\sqrt{5}}{2}\right)^5 \in \text{Anel A}' \text{ de } \mathbb{Q}(\sqrt{5})$$

Então, h e k são pares.

Observe que:

$$\frac{h + k\sqrt{5}}{2} \in \text{Anel A}$$

Mas há ainda o Anel *A'*, gerado a partir das quintas potências dos elementos do Anel *A*.

Sabe-se que h e k possuem a mesma paridade.

Tem-se, para a prova da *Afirmação 1*, a seguinte equivalência:

$$2^5.\left(a + b\sqrt{5}\right) = 2^5.\left(\frac{h + k\sqrt{5}}{2}\right)^5$$

Desenvolvendo-a e ainda supondo, por contradição, que h e k sejam ímpares, tem-se:

$$2^5 a + 2^5 b\sqrt{5} = (h^5 + 50h^3k^2 + 125hk^4) + (5h^4k + 50h^2k^3 + 25k^5).\sqrt{5}$$

$$2^5 b = 5k.(h^4 + 10h^2k^2 + 5k^4)$$

Sendo k ímpar, tem-se que 2^5 divide $(h^4 + 10h^2k^2 + 5k^4)$, se e somente se:

$$(h^4 + 10h^2k^2 + 5k^4) = 2^5\lambda = 32\lambda;\ \ \lambda \in \mathbb{Z}$$

Em linguagem de congruências, pode-se escrever:

$$(h^4 + 10h^2k^2 + 5k^4) \equiv 0\ (mod\ 32)$$

Com a suposição de h e k sendo números ímpares e estudando ainda as suas congruências em um Sistema Completo de Resíduos (módulo 8), conclui-se que as possíveis representações destes ímpares são as seguintes:

$$h \equiv \pm 1;\ \pm 3\ \ (mod\ 8)$$
$$\text{e}$$
$$k \equiv \pm 1;\ \pm 3\ \ (mod\ 8)$$

Verifica-se ainda:

$$h^2 \equiv 1 \quad \text{ou} \quad 9\ (mod\ 16)$$

Porque se tem:

$$h^2 = (8k + a_1)^2 = 64k^2 + 16ka_1 + a_1^2 \ = 16.(4k^2 + ka_1) + a_1^2 \equiv a_1^2 \equiv$$

$$\equiv 1 \ \text{ou}\ 9\ (mod\ 16) \ \ \text{com} \ \ a_1 \in \{\pm 1, \pm 3\}$$

Observa-se também que:

$$h^4 \equiv 1 \ \ \text{ou} \ \ 17\ (mod\ 32)$$

Como $81 \equiv 17\ (mod\ 32)$ e, ainda utilizando o raciocínio análogo ao da prova de h^2, chega-se a esta conclusão para h^4.

Analogamente, $k^2 \equiv 1 \ \ \text{ou} \ \ 9\ (mod\ 16)$ e $k^4 \equiv 1 \ \ \text{ou} \ \ 17\ (mod\ 32)$.

Logo, sabe-se que tanto h^4 como k^4 são côngruos (módulo 32) a 1 ou a 17.

Como se verificam os seguintes resultados:

$$\begin{cases} h^2 \equiv 1 \ \text{ou}\ 9\ (mod\ 16) \\ 90 \equiv 26\ (mod\ 32) \\ 10 \equiv 10\ (mod\ 32) \end{cases}$$

Pode-se considerar, para $10h^2$ e para $10h^2k^2$, as seguintes equivalências (módulo 32):

$$\begin{cases} 10h^2 \equiv 10 \ \text{ou} \ 26 \ \ (mod\ 32) \\ 10h^2k^2 \equiv 10k^2 \ \ \text{ou} \ \ 26k^2\ (mod\ 32) \end{cases}$$

Portanto, considerando estas equivalências, tem-se:

$$(h^4 + 10h^2k^2 + 5k^4) \equiv 1 + 10k^2 + 5k^4 (mod\ 32)$$

ou

$$(h^4 + 10h^2k^2 + 5k^4) \equiv 17 + 26k^2 + 5k^4 (mod\ 32)$$

Assim, examinando todas as possibilidades, conclui-se, que, considerando módulo 32, $(h^4 + 10h^2k^2 + 5k^4)$ será sempre côngruo aos casos apresentados em (i) ou (ii):

$$\text{(i)}\ \ 1 + 10k^2 + 5k^4 \equiv \begin{cases} 1 + 10 + 5 \equiv 16\ (mod\ 32) \text{ para } k = \pm 1 \\ \text{ou} \\ 1 + 90 + 5.81 \equiv 16\ (mod\ 32) \text{ para } k = \pm 3 \end{cases}$$

$$\text{(ii)}\ \ 17 + 26k^2 + 5k^4 \equiv \begin{cases} 17 + 26 + 5 \equiv 16\ (mod\ 32) \text{ para } k = \pm 1 \\ \text{ou} \\ 17 + 26.9 + 5.81 \equiv 16\ (mod\ 32) \text{ para } k = \pm 3 \end{cases}$$

Logo, conclui-se que:

$$(h^4 + 10h^2k^2 + 5k^4) \equiv 2^4\ (mod\ 32)$$

E, portanto, chega-se a uma contradição, pois:

$$(h^4 + 10h^2k^2 + 5k^4) \equiv 16 \not\equiv 0\ (mod\ 32)$$

Utilizando-se da técnica da prova por contradição, desejava-se, provar, de início, que:

$$(h^4 + 10h^2k^2 + 5k^4) = 2^5\lambda;\ \ \lambda \in \mathbb{Z}, \text{com } h \text{ e } k \text{ ímpares}$$

Contudo, chegou-se, assim, a uma conclusão diferente:

$$(h^4 + 10h^2k^2 + 5k^4) \neq 2^5\lambda$$

Portanto:

h e k são pares. ■

Em sequência, deve-se ainda provar:

Afirmação 2 – Sendo o Anel A' um anel de inteiros de $\mathbb{Q}(\sqrt{5})$ e $a + b\sqrt{5}$, $a - b\sqrt{5} \in A'$, tem-se que:

$$mdc\left(a + b\sqrt{5};\ \ a - b\sqrt{5}\right) = 1$$

Suponha, por absurdo, a existência de um primo e irredutível d, elemento do Anel A', então:

$$\begin{cases} \left(a + b\sqrt{5}\right) = k_1.d \\ \left(a - b\sqrt{5}\right) = k_2.d \end{cases}, \text{com } k_1, k_2 \in A'$$

Somando $(k_1.d)$ a $(k_2.d)$, obtém-se:

$$\left(a + b\sqrt{5}\right) + \left(a - b\sqrt{5}\right) = 2a = (k_1 + k_2).d \Longrightarrow d \mid 2a$$

Subtraindo $(k_1.d)$ de $(k_2.d)$, obtém-se:

$$\left(a + b\sqrt{5}\right) - \left(a - b\sqrt{5}\right) = 2b.\sqrt{5} = (k_1 - k_2).d \Longrightarrow d \mid \left(2b.\sqrt{5}\right)$$

Assim:

$$\begin{cases} 2a = d.w_1 \\ \text{e} \\ 2b\sqrt{5} = d.w_2 \end{cases} \Longrightarrow d \mid 2a \text{ e } d \mid 2b.\sqrt{5} \Longrightarrow \begin{cases} d \mid 2a \\ \text{e} \\ d \mid 2b \text{ ou d } \mid \sqrt{5} \end{cases} \Leftrightarrow (i) \text{ ou } (ii)$$

(i) $\Longrightarrow d \mid 2a$ e $d \mid 2b$

Como $mdc\,(a\,,b) = 1$ e d é divisor comum de $2a$ e $2b$, pode-se garantir que:

$$mdc\,(2a\,,2b) = 2.\left[\underbrace{mdc\,(a\,,b)}_{=1}\right] = 2 = d$$

Suponha, por absurdo, que:

$$mdc\left(a + b\sqrt{5};\ a - b\sqrt{5}\right) = 2$$

Note que o Lema 1 estabelece a e b como inteiros não negativos com paridades distintas.

Sabe-se que:

$$d = 2 = mdc\left(a + b\sqrt{5};\ \ a - b\sqrt{5}\right) \Leftrightarrow a \equiv b\ (mod\ 2)$$

Isto contraria a hipótese do Lema.

Logo, $d = 2$ é um absurdo.

Assim, garante-se que $mdc\left(a + b\sqrt{5};\ a - b\sqrt{5}\right) \neq 2$.

Observe que 2 é primo e irredutível no Anel A'.

(ii) $\Longrightarrow\ d \mid 2a$ e $d \mid \sqrt{5}$

Tem-se que $\sqrt{5}$ é primo e irredutível no Anel A' (*domínio fatorial*).

Supondo que se tome, também em A', um elemento d que seja primo e irredutível, então existe um outro elemento θ, *inversível e unidade no anel*, de modo que se observa:

$$\sqrt{5} = d.\theta \ \Leftrightarrow\ d = \sqrt{5}.\beta \text{ com } \beta = \theta^{-1}$$

De fato, θ e β são elementos inversíveis e unidades em A'.

Suponha, por absurdo, que $d \mid \sqrt{5}$, então escreve-se:

$$\sqrt{5} = d.\theta \text{ e } d = \sqrt{5}.\beta, \text{ sendo } \theta \text{ e } \beta \text{ unidades em } A'$$

Mas tem-se ainda que:

$$d \mid 2a \Longrightarrow (\sqrt{5}.\beta) \mid 2a$$

Assim:

$$(\sqrt{5}.\beta) \mid 2a \Longrightarrow 2a = (\sqrt{5}.\beta).w$$

De forma que:

$$w \in A'$$

Como:

$$2a = \sqrt{5}.(\beta.w) \ \Longrightarrow\ 4a^2 = 5.(\beta.w)^2 \ \Longrightarrow\ 5 \mid a^2 \ \Longrightarrow\ 5 \mid a$$

Tem-se, portanto, uma contradição da hipótese do Lema.

Logo, nossa suposição é falsa e ainda:

$$d \nmid \sqrt{5}$$

Em virtude das suposições iniciais de (i) e (ii) serem falsas, conclui-se que $d = 1$ é unidade no Anel A' e único divisor de $a + b\sqrt{5}$ e $a - b\sqrt{5}$.

Portanto:

$$mdc\left(a + b\sqrt{5}, a - b\sqrt{5}\right) = 1. \blacksquare$$

Provados os argumentos das afirmações 1 e 2, retoma-se a *sequência da demonstração*.

Conforme o Lema 1*:*

$(a^2 - 5b^2)$ é um elemento do Anel A' e representa uma quinta potência de um Anel A com a e b inteiros não negativos e:

$$a \not\equiv b \ (mod\ 2)$$

Assim, pode-se reescrever $(a^2 - 5b^2)$ da seguinte forma:

$$(a^2 - 5b^2) = \left(a + b\sqrt{5}\right).\left(a - b\sqrt{5}\right)$$

São ainda elementos de A′, representando as quintas potências de A:

$$\underbrace{a + b\sqrt{5} \quad \text{e} \quad a - b\sqrt{5}}_{pois\ mdc\ \left(a+b\sqrt{5},\ \ a-b\sqrt{5}\right)=1}$$

Observe que existem m e n inteiros, tais que:

$$m \equiv n \ (mod\ 2) \implies \frac{m + n\sqrt{5}}{2} \in A$$

Pode-se escrever ainda em um domínio fatorial:

$$a + b\sqrt{5} = \left(\frac{m + n\sqrt{5}}{2}\right)^5$$

Como provado na *Afirmação 1*, m e n são pares.

Dessa forma:

$$m \equiv n \equiv 0 \ \ (mod\ 2)$$

Fazendo:

$$m = 2\lambda_1 \quad \text{e} \quad n = 2\lambda_2$$

E considerando:

$$\underbrace{mdc\ (a, b) = 1 \quad \text{e} \quad a \not\equiv b \ (mod\ 2)}_{da\ hipótese}$$

Realiza-se a expansão do seguinte *binômio*:

$$a + b\sqrt{5} = \left(\frac{m + n\sqrt{5}}{2}\right)^5$$

Para, assim, verificar que:

$$\lambda_1 \not\equiv \lambda_2 \ (mod\ 2)$$

Logo:

$$a + b\sqrt{5} = \left(\lambda_1 + \lambda_2\sqrt{5}\right)^5$$

De maneira que se tem:

$$\begin{cases} a \not\equiv b \ (mod\ 2) \\ \lambda_1 \not\equiv \lambda_2 (mod\ 2) \end{cases}$$

Portanto, são elementos irredutíveis no Anel A':

$$a + b\sqrt{5} \quad \text{e} \quad \lambda_1 + \lambda_2\sqrt{5}$$

Pode-se considerar a seguinte unidade:

$$1_{A'} = \lambda'_1 + \lambda'_2\sqrt{5}$$

De modo que seja ainda uma unidade no Anel A'.

Como se sabe que:

$$\lambda'_1 \not\equiv \lambda'_2 \ (mod\ 2)$$

Tem-se:

$$a + b\sqrt{5} = \left(\lambda_1 + \lambda_2\sqrt{5}\right)^5 . \left(\lambda'_1 + \lambda'_2\sqrt{5}\right)$$

Considerando:

$$t = 2.\lambda'_1 \ \text{ e } \ u = 2.\lambda'_2 \implies t \equiv u \equiv 0 \ (mod\ 2)$$

Reescreve-se:

$$a + b\sqrt{5} = \left(\frac{m + n\sqrt{5}}{2}\right)^5 . \overbrace{\left(\frac{t + u\sqrt{5}}{2}\right)}^{=1_{A'}}$$

Onde:

$$\begin{cases} m \equiv n \equiv 0\ (mod\ 2) \\ t \equiv u \equiv 0\ (mod\ 2) \end{cases}$$

Tem-se também que:

$$\frac{m + n\sqrt{5}}{2} \quad \text{e} \quad \frac{t + u\sqrt{5}}{2} \in \text{A}$$

Como se tem ainda:

$$t \equiv u \equiv 0\ (mod\ 2)$$

Pode-se afirmar que:

$$\frac{t + u\sqrt{5}}{2} \text{ é unidade de } A'$$

Para mostrar que este elemento é uma *unidade e é inversível neste anel*, deve-se estabelecer que:

A sua norma valha ± 1

A função norma é dada por:

$$\begin{cases} N: A' \longrightarrow \mathbb{Z} \\ z \longrightarrow N(z) = z.\bar{z} \end{cases}$$

$$\{z \in A' \mid z \text{ é inversível}\} \Leftrightarrow \{N(z) = \pm 1 \text{ em } \mathbb{Z}\}$$

Portanto:

$$N(z) = \frac{(t + u\sqrt{5})}{2}.\frac{(t - u\sqrt{5})}{2} = \frac{(\mathrm{t}^2 - 5u^2)}{4} = \pm 1 \implies \mathrm{t}^2 - 5u^2 = \pm 4$$

Seja também:

$$\left(\frac{m + n\sqrt{5}}{2}\right)^5 = \left(\frac{m' + n'\sqrt{5}}{2}\right)$$

Observada a seguinte relação:

$$\begin{cases} m \equiv n \equiv 0 \ (mod\ 2) \\ m' \equiv n' \equiv 0 \ (mod\ 2) \end{cases}$$

De forma que se conclui:

$$\left(m + n\sqrt{5}\right)^5 = 16m' + 16n'\sqrt{5} \Longrightarrow$$

$$(m^5 + 50m^3n^2 + 125mn^4) + (5m^4n + 50m^2n^3 + 25n^5)\sqrt{5} = 16m' + 16n'\sqrt{5} \Leftrightarrow$$

$$\Leftrightarrow \begin{cases} 16m' = m^5 + 50m^3n^2 + 125mn^4 \equiv m^5 \ (mod\ 5) \\ 16n' = 5m^4 + 50m^2n^3 + 25n^5 \equiv 0 \ (mod\ 5) \end{cases}$$

Portanto, tem-se:

$$\begin{cases} 16m' \equiv m^5 \ (mod\ 5) \\ 16n' \equiv 0 \ (mod\ 5) \end{cases}$$

De acordo com o PTF, verifica-se a relação:

$$m^5 \equiv m \ (mod\ 5)$$

Dessa forma:

$$16m' \equiv m^5 \equiv m \ (mod\ 5)$$

Logo:

$$16n' \equiv 0 \ (mod\ 5) \Longrightarrow 5 \mid 16n' \Longrightarrow 5 \mid n'$$

Seja:

$$a + b\sqrt{5} = \left(\frac{m' + n'\sqrt{5}}{2}\right).\left(\frac{t + u\sqrt{5}}{2}\right) \Longrightarrow$$

$$\Longrightarrow 4a + 4b\sqrt{5} = \left(m' + n'\sqrt{5}\right).\left(t + u\sqrt{5}\right) \Longrightarrow$$

$$\Longrightarrow 4a + 4b\sqrt{5} = (m't + 5n'u) + (m'u + n't).\sqrt{5} \Leftrightarrow \begin{cases} 4a = m't + 5n'u \\ 4b = m'u + n't \end{cases}$$

Supondo que:

$$5 \mid m' \Longrightarrow 5 \mid (4a = m't + 5n'u)$$

Assim, 5 deveria dividir a, o que, portanto, é uma *contradição*.

Logo:

$$5 \nmid m'$$

Afirma-se:

$$\begin{cases} \underbrace{16m' \equiv m \ (mod\ 5)}_{16 \equiv 1 \ (mod\ 5)} \Longrightarrow m' \equiv m \ (mod\ 5) \\ m' \equiv m \not\equiv 0 \ (mod\ 5) \\ 5 \nmid m \quad \text{e} \quad 5 \mid n' \end{cases}$$

Como:

$$\underbrace{5 \text{ divide } b}_{da\ hipótese}$$

Deve-se garantir que:

$$\underbrace{5 \mid (m'u) \implies 5 \mid u}_{pois\ 5 \nmid m'}$$

Fazendo $u = 0$ em:

$$t^2 - 5u^2 = \pm 4 \implies t = \pm 2 \ (\textit{soluções inteiras})$$

E observando ainda:

$$a + b\sqrt{5} = \left(\frac{m + n\sqrt{5}}{2}\right)^5 . \left(\frac{\pm 2 + 0.\sqrt{5}}{2}\right) = \pm \left(\frac{m + n\sqrt{5}}{2}\right)^5$$

Considerando $m,\ n,\ c$ e d, enunciados no Lema 1 e tomados da seguinte forma:

$$\begin{cases} c = \pm \dfrac{m}{2} \\ d = \pm \dfrac{n}{2} \end{cases}$$

Com a relação anterior e tomando $u = 0$, tem-se:

Uma prova da existência dos inteiros não nulos c e d.

Para que todas as possibilidades sejam cobertas e a prova, portanto, concluída, deve-se supor $u \neq 0$ e considerar a seguinte unidade de A':

$$\frac{t + u\sqrt{5}}{2} = \pm 1$$

Considere uma equação da forma:

$$\frac{(\mathrm{t}^2 - 5u^2)}{4} = \pm 1$$

Note que existe uma solução genérica do tipo:

$$\frac{t + u\sqrt{5}}{2} = \pm\left(\frac{1 + \sqrt{5}}{2}\right)^e$$

Já se analisou o caso em que $e = 0$:

$$e = 0 \implies t = \pm 1 \text{ e } u = 0$$

Assim, ficaremos agora restritos ao caso em que $e \neq 0$ para estudarmos as soluções genéricas, conforme apresentado acima.

Observe que, em relação aos números a seguir, um é o *inverso multiplicativo* do outro:

$$\frac{1 + \sqrt{5}}{2} \quad \text{e} \quad \frac{-1 + \sqrt{5}}{2}$$

Assume-se que $e > 1$:

$$\begin{cases} e = 1 \implies u = \pm 1 \text{ (impossível)} \\ 5 \mid u \end{cases}$$

Logo, escreve-se assim:

$$\pm 2^{e-1}.(t + u\sqrt{5}) = (1 \pm \sqrt{5})^e \implies$$

$$\pm 2^{e-1}t \pm 2^{e-1}u\sqrt{5} = \binom{e}{0} 1^e (\pm\sqrt{5})^0 + \binom{e}{1} 1^{e-1} (\pm\sqrt{5})^1 + \binom{e}{2} 1^{e-2} (\pm\sqrt{5})^2 + \cdots$$

Sabe-se que a parcela:

$$\pm 2^{e-1}.u\sqrt{5}$$

Corresponde às somas da expansão binomial de:

$$\left(1 \pm \sqrt{5}\right)^{e}$$

Em que se apresentam as potências ímpares para o termo $\pm\sqrt{5}$.

Desta forma:

$$\pm 2^{e-1}.u\sqrt{5} = e.\left(\pm\sqrt{5}\right) + \binom{e}{3}.\left(\pm\sqrt{5}\right)^{3} + \binom{e}{5}.\left(\pm\sqrt{5}\right)^{5} + \cdots$$

$$\pm 2^{e-1}.u\sqrt{5} = e.\left(\pm\sqrt{5}\right) + 5\binom{e}{3}.\left(\pm\sqrt{5}\right) + 5^{2}\binom{e}{5}.\left(\pm\sqrt{5}\right) + \cdots$$

$$\pm 2^{e-1}.u = e + 5\binom{e}{3} + 5^{2}\binom{e}{5} + \cdots$$

$$2^{e-1}.u \equiv \pm e \ (mod\ 5)$$

Tem-se que:

$$\begin{cases} 5 \mid u \Longrightarrow 5 \mid e \Longrightarrow 2^{e-1}.u \equiv \pm e \equiv 0 \ (mod\ 5) \\ e = 5f \ \text{ com } \ f \in \mathbb{Z} \end{cases}$$

Assim, reescreve-se a relação:

$$\frac{m + n\sqrt{5}}{2}.\left(\frac{1 \pm \sqrt{5}}{2}\right)^{f} = \frac{c' + d'\sqrt{5}}{2}$$

Sendo:

$$c' \equiv d' \ (mod\ 2)$$

Garante-se que:

$$a + b\sqrt{5} = \pm\left(\frac{c' + d'\sqrt{5}}{2}\right)^{5}$$

Retomando c e d do Lema 1, verifica-se:

$$c = \pm\frac{c'}{2} \quad \text{e} \quad d = \pm\frac{d'}{2}$$

Portanto, estabelecida esta relação:

Conclui-se a *prova de existência* dos inteiros não nulos c e d. ■

Lema 2 – Para o Teorema da Equação Fermatiana Quíntupla

Sejam a e b inteiros não negativos e ímpares com:

$$mdc\ (a,b) = 1;\ a \not\equiv b\ (mod\ 2); 5 \nmid a;\ \text{e}\ 5 \mid b$$

Se $\frac{(\boldsymbol{a^2-5b^2})}{\boldsymbol{4}}$ é a quinta potência de um elemento do Anel A, então:

existem c e d, inteiros não nulos, tais que:

$$\begin{cases} a = \dfrac{c.(c^4 + 50c^2d^2 + 125d^4)}{16} \\ \\ b = \dfrac{5d.(c^4 + 10c^2d^2 + 5d^4)}{16} \end{cases}$$

onde: $mdc\ (c,d) = 1;\ c$ e d ímpares; e $5 \nmid c$.

Prova: Analogamente ao Lema 1, tem-se:

$$mdc\ (a,b) = 1 \Longrightarrow mdc\ (c,d) = 1,$$

uma vez que se mostre a existência dos inteiros não nulos c e d, tais que:

$$\begin{cases} a = \dfrac{c.(c^4 + 50c^2d^2 + 125d^4)}{16} \\ \\ b = \dfrac{5d.(c^4 + 10c^2d^2 + 5d^4)}{16} \end{cases}$$

No estudo das paridades de a e b, a partir das de c e d, tem-se que:

- Se c e d forem ambos pares, a e b também serão, logo esta situação não é possível, pois, da hipótese, a e b são ímpares.
- Se c e d tiverem paridades diferentes:

$$c^4 + 50c^2d^2 + 125d^4 \quad \text{e} \quad c^4 + 10c^2d^2 + 5d^4$$

São ímpares e, assim, 16 não os divide, mas 16 deveria dividir c e d ao mesmo tempo, ocorrendo, com isso, uma contradição. Logo, c e d não podem ter paridades diferentes.

- Se c e d forem ímpares:

$$c^4 + 50c^2d^2 + 125d^4 \quad \text{e} \quad c^4 + 10c^2d^2 + 5d^4$$

São pares e 16 os dividirá, já que, por hipótese, a e b são ímpares.

Logo, este é o único caso possível.

Assim, c e d são ímpares, faltando apenas a prova a existência destes inteiros.

A demonstração da existência de c e d é análoga à proposta no Lema 1, observando ainda as especificidades do Lema 2, conforme detalhado a seguir:

Deve-se demonstrar que:

$$mdc\left(\frac{a + b\sqrt{5}}{2};\ \frac{a - b\sqrt{5}}{2}\right) = 1$$

Esta prova é análoga à anterior.

Portanto:

$$\frac{a + b\sqrt{5}}{2} = \left(\frac{m + n\sqrt{5}}{2}\right)^5 \cdot \left(\frac{t + u\sqrt{5}}{2}\right)$$

onde $m \equiv n\ (mod\ 2)$ e $t \equiv u\ (mod\ 2)$, sendo a unidade em A':

$$\left(\frac{t + u\sqrt{5}}{2}\right)$$

Tem-se também:

$$t^2 - 5u^2 = \pm 4$$

Conforme o Lema 1 e utilizando o raciocínio análogo, conclui-se que 5 divide u.

Neste sentido, fazendo $u = 0$ e assumindo:

$$c = \pm m \quad \text{e} \quad d = \pm n$$

Prova-se, assim:

A *existência dos inteiros não nulos* c e d, considerando este caso particular

Para concluir a prova, suponha ainda:

$$u \neq 0$$

Considerando a relação desenvolvida no Lema 1 para $e > 1$:

$$\pm 2^{e-1}.\left(t + u\sqrt{5}\right) = \left(1 \pm \sqrt{5}\right)^{e}$$

Conclui-se também que:

$$e = 5f \text{ com } f \in \mathbb{Z}$$

Portanto:

$$\left(\frac{m + n\sqrt{5}}{2}\right).\left(\frac{1 \pm \sqrt{5}}{2}\right)^{f} = \left(\frac{c + d\sqrt{5}}{2}\right)$$

Logo, conclui-se a prova ao se *mostrar a validade* da seguinte relação:

$$\left(\frac{a+b\sqrt{5}}{2}\right) = \left(\frac{c+d\sqrt{5}}{2}\right)^{5} \blacksquare$$