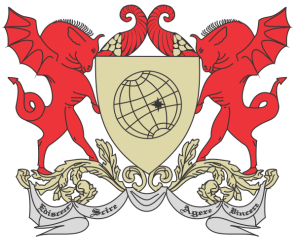
Universidade Federal de Viçosa
Trabalho de Conclusão de Curso



Suéllen Aparecida de Oliveira

Um estudo sobre o Último Teorema de Fermat

Florestal
Minas Gerais – Brasil
2020

Suéllen Aparecida de Oliveira

UM ESTUDO SOBRE O ÚLTIMO TEOREMA DE FERMAT

Trabalho de Conclusão de Curso apresentado à Universidade Federal de Viçosa, como parte das exigências do Curso de Licenciatura em Matemática, para obter o diploma de Licenciado em Matemática.

Florestal
Minas Gerais – Brasil
2020

Ficha Catalográfica

Copie o arquivo

`ficha_catalografica.pdf`

fornecido pela UFV para a pasta do trabalho e a ficha catalográfica será automaticamente incluída aqui.

Suéllen Aparecida de Oliveira

UM ESTUDO SOBRE O ÚLTIMO TEOREMA DE FERMAT

Trabalho de Conclusão de Curso apresentado à Universidade Federal de Viçosa, como parte das exigências do Curso de Licenciatura em Matemática, para obter o diploma de Licenciado em Matemática.

Aprovada: 21 de dezembro de 2020.

Alexandre Alvarenga Rocha

Vinícius Lara Lima

Danielle Franco Nicolau
(Orientadora)

Agradecimentos

Primeiramente agradeço a Deus, por ter me permitido chegar até aqui e por ter estado ao meu lado em cada instante desse percurso. Por ter me amparado nos momentos de choro e desespero - que se tornaram tão comuns durante esses anos - acalmando meu coração e nunca me deixando sentir sozinha. Obrigada por ter me fortalecido em cada momento que pensei em desistir, ajudando-me a driblar as dificuldades, encontrando uma solução para todas elas.

A meus pais Antônio e Edilene, pelo amor, incentivo e apoio; em especial à minha mãe que se abdicou de muitas coisas para me manter na universidade durante esses anos. Essa vitória é nossa, e agora chegou a hora de eu retribuir tudo o que a senhora fez por mim.

A meu irmão Gabriel, pela compreensão e apoio.

A minha avó Maria Florinda, por sempre me colocar em suas orações e compreender minha ausência.

A minha orientadora Danielle, por aceitar conduzir o meu trabalho, pela atenção e comprometimento.

Aos amigos que fiz durante a graduação, por fazerem o ambiente acadêmico mais agradável e acolhedor.

A todos que direta ou indiretamente fizeram parte da minha formação e contribuíram para meu crescimento acadêmico e pessoal. Sou o resultado da confiança e do apoio de cada um de vocês. É com imensa gratidão e amor a profissão, que chego ao final dessa jornada. Sem vocês, ela seria bem mais difícil e dolorosa. Obrigada!

Resumo

OLIVEIRA, Suéllen Aparecida de, Lic., Universidade Federal de Viçosa, dezembro de 2020. **Um estudo sobre o Último Teorema de Fermat** . Orientadora: Danielle Franco Nicolau.

Este trabalho tem o intuito de exibir a história do Último Teorema de Fermat e os eventos ocorridos ao longo do tempo à procura por sua resolução. Faz um resumo histórico sobre a busca da sua solução e apresenta demonstrações para os casos $n = 4$ e $n = 3$, sendo duas demonstrações para este último.

O último teorema de Fermat foi um enigma que atentou as mentes mais brilhantes da matemática. Um teorema de simples entendimento, tão modesto, que qualquer indivíduo alcançaria o entendimento, entretanto, de resolução estimada como impossível para muitos.

Ele é um dos eventos mais instigantes da história da matemática e que serviu para motivar vários matemáticos de todas as ocasiões a arriscar solucioná-lo. Inclusive, até pouco tempo pensava-se que o Último Teorema de Fermat era falso, porém, ao término do século XX o matemático britânico Andrew Wiles demonstrou-o.

Palavras chaves: Fermat. Teorema. Euler. Andrew Wiles.

Abstract

OLIVEIRA, Suéllen Aparecida de, Universidade Federal de Viçosa, December, 2020. **A study on Fermat's Last Theorem** . Adviser: Danielle Franco Nicolau.

This work has the purpose of displaying the history of Fermat's Last Theorem and the events that occurred over time looking for its resolution. Make a historical summary of the search for your solution and presents demonstrations for the cases $n = 4$ and $n = 3$, being two demonstrations for the lattercase.

The Fermat's last theorem was an enigma that confused the brightest minds of mathematics. A theorem of simple understanding, so modest, that any individual would reach the understanding, however, resolution considered impossible for many.

That is one of the most exciting events in the history of mathematics and which served to motivate many mathematicians to solve it. Until recently, it was thought that the Last Theorem Fermat was false, however, at the end of the 20th century, British mathematician Andrew Wiles presented its proof.

keyword: Fermat. Teorema. Euler. Andrew Wiles.

Sumário

1

Introdução

Pierre Fermat, filho de um rico mercador, trabalhou como funcionário público de Toulouse (França), no século XVIII. Sua dedicação aos estudos era apenas em horas livres, motivo pelo qual não se preocupou em realizar demonstrações formais acerca de seus achados, e por isso, ficou conhecido como príncipe dos amadores. Ele tinha o costume de deixar anotações escritas nas margens dos livros, espaço onde registrou além de outras anotações importantes seu último teorema conhecido como o Último teorema de Fermat que diz que não existe soluções inteiras para a equação $x^n + y^n = z^n$ para n maior que 2, com x,y,$z \neq 0$. Fermat não deixou demonstração para tal teorema, com justificativa de que a margem daquele livro era muito estreita para contê-la. Este teorema permaneceu por mais de 300 anos sem solução, mesmo após ser analisado pelos maiores estudiosos da matemática dos últimos tempos. Só na década de 1990, Andrew Wiles, após longos anos de estudo e se baseando em teorias recentes, conseguiu chegar à demonstração.

Em 1670, após alguns anos à morte de Fermat, seu filho foi quem descobriu o teorema, nas margens do livro "Arithmetica de Diofanto", famoso algebrista da Grécia do século II A.C., este livro contava com cerca de 48 anotações sem provas realizadas por Fermat. Estas anotações, exceto seu último teorema, foram provadas posteriormente. Nos achados de Fermat, foi encontrada um prova para o caso $n = 4$ usando um método que ficou conhecido com descenso infinito de Fermat, porém, a prova para todo n, ainda ficara em aberto.

Este trabalho objetiva apresentar parte da história e dos grandes avanços obtidos nos ensaios da demonstração do mencionado Último Teorema de Fermat, bem como as personalidades que fizeram parte de sua demonstração. No discorrer dos capítulos que compõem este trabalho, observam-se as demonstrações do Último de Teorema de Fermat para os casos $n = 3$ e $n = 4$.

Inicialmente será descrita a história principal da vida e obra de Pierre de Fermat, que enunciou esse enigma conhecido como um dos mais complexos da matemática. Neste capítulo, será feito um passeio sobre a parte histórica do teorema, descrevendo seu contexto e registros.

Dando sequência ao trabalho, no terceiro capítulo, abordaremos ferramentas algébricas que serão utilizadas nas demonstrações. Assim sendo, este capítulo

apresenta os Preliminares Algébricos, que tem como objetivo estabelecer as definições, proposições, teoremas e os resultados principais que serão empregados nesse trabalho nas demonstrações para os casos $n = 3$ e $n = 4$. Iniciará, dando algumas definições, e teoremas aritméticos. Posteriormente, estudaremos duas estruturas algébricas essenciais: Anéis e o Anel $\mathbb{Z}[\omega]$; abordando os conceitos básicos de anéis, subanéis, domínios de integridade, ideais, anel quociente, domínios de ideias principais (DIP), divisibilidade em domínios, irredutíveis e primos, domínios de fatoração única (DFU), Domínios Euclidianos (DE), homomorfismo de anéis e, por fim, o Anel $\mathbb{Z}[\omega]$.

Seguindo a explanação da temática, o quarto capítulo apresenta as demonstrações para os casos $n = 3$ e $n = 4$. Inicia-se com demonstração de Fermat para o caso $n = 4$. Posteriormente, relata um pouco sobre Leonhard Euler (1707 – 1783) que foi quem realizou o primeiro avanço acerca da prova do Último Teorema de Fermat. Ele acreditava que antes de criar uma demonstração para todas as possibilidades possíveis, teria que criar uma para $n = 3$, e este foi o degrau que ele tentou usar como ponto de partida para construir uma prova geral para todas as outras equações. No dia 4 de agosto de 1753, Euler divulgou em uma carta enviada ao matemático Prussiano Christian Goldbach, que tinha adaptado o método do descenso infinito de Fermat e conseguira provar com sucesso o caso $n = 3$. Depois de 100 anos esta era a primeira vez que alguém conseguiu fazer algum progresso na direção de solucionar o desafio de Fermat. Após relato sobre a história de Euler, será proferida sua demonstração para o caso $n = 3$. Neste capítulo, também apresentamos uma demonstração para $n = 3$ utilizando o anel $\mathbb{Z}[\omega]$ onde $\omega = e^{\frac{2\pi}{3}i} = \frac{-1+i\sqrt{3}}{2}$ é a raiz primitiva cúbica da unidade, isto é, $\omega^3 = 1$. Este anel é um anel quadrático, o que facilita bastante a demonstração. Ao final, é apresentado um exemplo de aplicação do teorema na prova de que $\sqrt[n]{2}$ é irracional.

Já o quinto capítulo, aborda a narrativa do matemático Andrew Wiles, que em 1995, finalmente conseguiu demonstrar o teorema; descrevendo um pouco de sua história com o teorema, sua solução, o erro encontrado e os prêmios que obteve devido à demonstração. Andrew Wiles teve seu primeiro contato com o teorema aos dez anos de idade e se encantou com o mesmo, porém, só aprofundou seus estudos após cerca de duas décadas e durante sete anos de estudos intensos, secretos e em total isolamento; empregou todas as descobertas antecedentes para ordenar uma demonstração lógica e no dia 23 de junho de 1993, quando participava de uma Conferência no Instituto Isaac Newton - Cambridge, Andrew Wiles anunciou sua demonstração. Porém, os avaliadores encontraram um erro na demonstração. Depois de cerca de dois anos de estudo e com a ajuda de Richard Taylor, foi apresentada a demonstração correta, tornando Wiles um dos matemáticos mais conceituados da história da matemática.

Para concluir, no sexto capítulo será descrito as considerações finais do trabalho, evidenciando que não há soluções inteiras para a equação $x^n + y^n = z^n$ para $n = 3$ e $n = 4$, com x,y,$z \neq 0$, que, de acordo com definições, proposições e teoremas concernentes aos números inteiros a ao anel $\mathbb{Z}[\omega]$, se ajustaram como alicerce para as demonstrações do Último Teorema de Fermat para os casos citados.

2

Pierre de Fermat - O príncipe dos amadores

Figura 2.1: Imagem de Pierre de Fermat

Pierre de Fermat (1601-1665), filho do rico mercador de peles, Dominique de Fermat, pôde receber uma educação excepcional, primeiramente no Mosteiro Franciscano de Grandselve e posteriormente na Universidade de Toulouse. Pierre de Fermat ingressou no serviço público em 1631.

No ano de 1652 Fermat foi promovido a Juiz Supremo na Corte Criminal Soberano do Parlamento de Toulouse. Neste mesmo ano Fermat ficou doente e houve até relatos afirmando que ele havia evoluído para óbito.

Ao se averiguar a obra matemática de Fermat, nota-se com facilidade a essência amadora dominante em seus trabalhos. Sem formação matemática, durante sua vida ativa, não fez nenhum registro de publicações e não fez nenhuma apresentação sistêmica de seus achados e de sua metodologia. A matemática se apresentou de forma padrão como a fundamental ocupação em sua vida.

Fermat tinha por profissão Jurisprudência e magistrado, dedicou ao estudo da Matemática somente em suas horas de folga como lazer e, ainda assim, se destacou como o maior matemático da ocasião, sendo visto como o príncipe dos amadores.

No século XVII a matemática se recuperava da Idade das Trevas, assim sendo, não é de se surpreender o costume amador dos trabalhos de Fermat. Contudo, sendo ele um amador, pode-se dizer que era o melhor deles, de acordo com exatidão e à seriedade de seus estudos.

Gundlach (2001), salienta que na época de Fermat (século XVII) a matemática era discutida por meio de cinco temas principais:

a) A geometria analítica de Fermat (1629) e Descartes (1637);

b) O cálculo infinitesimal de Newton e Leibniz;

c) A análise combinatória (1654). Particularmente com os trabalhos de Fermat e Pascal, que delineiam o cálculo de probabilidade;

d) A aritmética superior, de Fermat (1630-1665);

e) A dinâmica de Galileu (1612) e Newton (1666-1684) e a gravitação universal de Newton (1684-1687);

Fermat precede Descartes na geometria analítica. A metodologia utilizada por Fermat é mais simples do que as de Descartes. No ano de 1629 Fermat já apresenta, a equação geral da reta, da circunferência e de certas cônicas. Fermat divulgou em 1639 uma nova metodologia para determinar as tangentes, estudo que induziria aos máximos e mínimos. Especialmente, Fermat estabelece em (1657, 1661) o princípio do tempo mínimo, da óptica, que se tornou o primitivo dos maiores princípios variacionais da física.

Fermat também se destaca no campo do cálculo de probabilidades. Antoine Gombaud, o escritor francês incomodado com algumas dificuldades proporcionadas em alguns modelos de jogos de azar, envia os mesmos para Pascal, que juntamente com Fermat, buscam resolver as questões propostas, momento em que Fermat corrigiu determinadas falhas cometidas por Pascal.

Contudo, observa-se que Fermat tinha preferência pela teoria dos números, na qual se dedicava com devoção. Sempre impulsionou consideravelmente à aritmética superior moderna; exercendo, de tal modo, ampla influência sobre o desenvolvimento da álgebra. Graças a Fermat o teorema inédito, evidente pela concepção, que transpôs sem embargo à história da matemática foi classificado como o "último teorema de Fermat".

2.1 O último Teorema de Fermat

Considerando-se a equação $x^n + y^n = z^n$, Fermat estabeleceu que não existem valores inteiros para x, y e z que a satisfaçam, quando n é um número inteiro e maior do que 2.

A propósito de sua demonstração, Fermat escreveu à margem de um exemplar da edição preparada por Méziriac (1581-1638) das obras do matemático grego, Diofanto (século. III dc).

Muitas foram as dúvidas sobre a veracidade. Por um longo período de tempo, mais de três séculos, os ilustres expoentes da Matemática, entre eles Euler e Gauss, dedicaram-se ao tema.

Com o avanço da tecnologia e após a chegada dos computadores, testaram inúmeros algarismos com distintos valores para x, y, z e n e a igualdade $x^n + y^n = z^n$ não se verificou.

Nesse trabalho de conclusão de curso, serão apresentadas demonstrações para os casos $n = 3$ e $n = 4$

Esse teorema foi demonstrado em 1995 por Andrew Wiles.

2.1.1 Parte histórica do teorema

Fermat (1601- 1665) em seus últimos estudos escreveu um enunciado, conhecido e popularizado como o Último Teorema de Fermat. Ele próprio não o demostrou e sua solução permaneceu em aberto por mais de 350 anos .

Este teorema pode ser considerado uma generalização do Teorema de Pitágoras, que diz que o quadrado da hipotenusa é igual à soma do quadrado dos catetos. Tomando x e y como catetos e z como hipotenusa, a expressão que origina essa relação é: $x^2 + y^2 = z^2$.

Encontrar números inteiros que satisfaçam a equação do Teorema de Pitágoras $x^2 + y^2 = z^2$ é relativamente simples, mas, ao mudar a potência de dois para três (do quadrado para o cubo), essa tarefa parece impossível. Na equação de Pitágoras, o desafio era rearrumar os ladrilhos de dois quadrados para formar um terceiro quadrado maior.

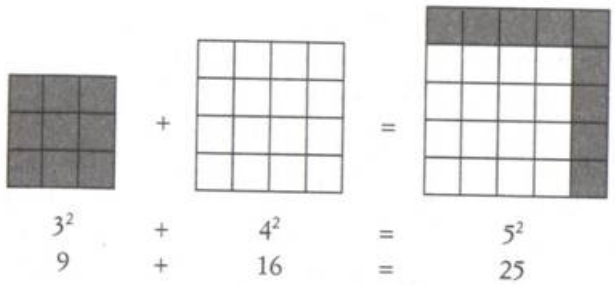


Figura 2.2: Exemplo: O quadrado de $9 = 3^2$ ladrilhos pode ser somado ao quadrado de $16 = 4^2$ ladrilhos, formando um terceiro quadrado com $25 = 5^2$ ladrilhos.

Na versão "ao cubo" o desafio é rearrumar dois cubos para formar um terceiro cubo maior. Aparentemente, para quaisquer cubos escolhidos como ponto de partida, quando eles são combinados, o resultado ou é um cubo completo, com alguns cubos menores sobrando, ou um cubo incompleto. O mais próximo que alguém já chegou de um arranjo perfeito foi aquele em que sobra ou falta um tijolo.

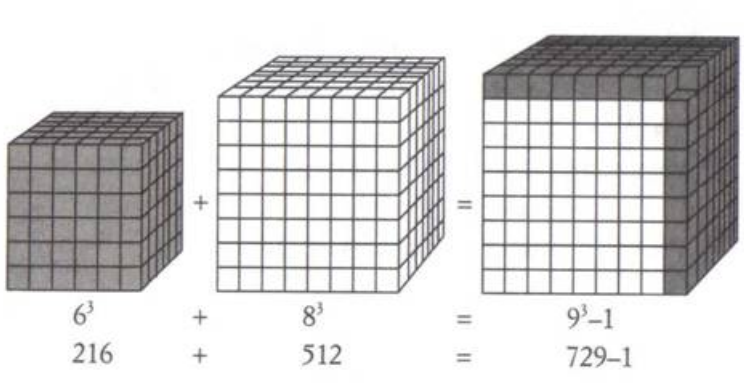


Figura 2.3: Exemplo: O primeiro cubo possui 216 (6^3) cubinhos e o segundo possui 512 (8^3) cubinhos. Rearrumando-os em um terceiro cubo, o total de cubinhos é 728, faltando assim, apenas um para completar (9^3).

Além disso, ao trocar o expoente 2 da equação de Pitágoras por qualquer número inteiro maior, a busca por soluções deixa de ser um problema relativamente simples e se torna um desafio impossível.
Fermat tinha hábitos de fazer anotações informais sobre seus estudos experimentais e, nas margens de seu exemplar do livro Aritmética de Diofanto, o mesmo fez a espantosa afirmação de que não existiriam soluções para essa equação:

"É impossível para um cubo ser escrito como a soma de dois cubos, ou uma quarta potência ser escrita como uma soma de dois números elevados a quatro, ou, em geral, para qualquer número que seja elevado a uma potência maior do que dois ser escrito como a soma de duas potências semelhantes. Eu tenho uma demonstração realmente maravilhosa para esta proposição, mas esta margem é muito estreita para contê-la."

De tal modo, o Último teorema de Fermat afirma que:

Não existe soluções inteiras para a equação

$$\mathbf{x^n + y^n = z^n}$$

para n maior que 2, com $\mathbf{x,y,z \neq 0}$.

A anotação de Fermat foi satisfatória para diferentes gerações de matemáticos envolvidos na tentativa de resolver o problema ou de demonstrar que ele é falso. Várias tentativas para solução do problema foram apresentadas, porém sem o sucesso aguardado. Contudo, sobrevieram importantes implicações para a matemática e para as ciências em geral.

Inicialmente todos questionavam sobre como Fermat chegou à demonstração do teorema, uma vez que ele não deixou quase nada registrado em seus estudos. Hoje se sabe que, para tal demonstração, é necessário o uso de uma ferramenta matemática que não estava disponível no século XVIII. Assim sendo, a desconfiança

se verdadeiramente Fermat teria descoberto uma demonstração para o teorema, se torna plausível e foi essa dúvida que incentivou gerações de matemáticos a se comprometerem na solução, produzindo material acadêmico que aprimorou o campo da matemática.

Vários matemáticos obtiveram provas do teorema para fatos particulares: Peter Barlow (1811) para n=4, Peter Dirichlet (1825) para n=4 e n=14, Andrie-Marie Legendre para n=5, Gabriel Lamé (1839) para n=7, em meio a outros. Além disso, no século XX, alguns matemáticos como Sophie Germain, Ernst Kummer e Carl Friedrich Gauss, fizeram abordagens procurando demonstrar o teorema em faixas exclusivas de números. No meio dos mais reconhecidos, temos Leonhard Euler (1707-1783), um dos grandes matemáticos do século XVIII, que foi o primeiro a obter avanço acerca do teorema, demonstrando o caso para n=3, até chegar em Andrew Wiles (1953), o matemático que em 1995 provou o último teorema de Fermat.(SINGH,2012).

Embora versado como principal e ser considerado o responsável pela sua demonstração, Andrew Wiles permanece bem longe de ser o exclusivo enredado no procedimento. A prova do teorema é consequência de anos de incremento da matemática e tarefas de múltiplos estudiosos. O documentário "O último teorema de Fermat" (Fermat's Last Theorem, 1996) exibe partes do envolvimento e dos achados feitos por diferentes matemáticos que contribuíram direta ou indiretamente.

O problema era tão interessante que foram ofertados prêmios para o vencedor do desafio, que chegou ao maior valor em 1908, 100.000 marcos (aproximadamente R$ 340.000,00), oferecida como premiação pelo professor Paul Wolfskhel ao indivíduo que obtivesse uma demonstração válida para o teorema. Tal premiação foi um grande incentivo para que os matemáticos da ocasião se dedicassem firmemente ao problema.

O matemático inglês Andrew Wiles impetrou o feito empregando como fundamento uma teoria criada pelos matemáticos Yutaka Taniyama e Goro Shimura (versada como conjectura Taniyama-Shimura) acerca de equações elípticas. As provas foram apresentadas numa conferência internacional em Hong Kong, cujo título foi: Formas modulares, curvas elípticas e representações galoisianas. Compete elucidar que Wiles empregou considerações matemáticas avançadíssimas, com as quais Fermat nem poderia ter imaginado. (SINGH, 2002).

3

Preliminares Algébricos

Este trabalho tem como objetivo demonstrar o Último Teorema de Fermat para os casos em que $n = 3$ e $n = 4$. Para isso, precisamos de ferramentas algébricas das quais apresentaremos neste capítulo. As definições, teoremas e exemplos nele contido, foram transcritas de [9], [10] e [11].

3.1 Aritmética

Uma das propriedades importantes dos números inteiros ($\mathbb{Z}$) é a divisibilidade. Mesmo não existindo inverso multiplicativo para todo inteiro, conseguimos obter características interessantes.

Definição 3.1: Dados a,$b \in \mathbb{Z}$, dizemos que a divide b e escrevemos $a|b$, quando existir $c \in \mathbb{Z}$ tal que $b = a \cdot c$.

Se a não divide b, notacionamos por $a \nmid b$. Por exemplo, $2 \nmid 3$.

Se $a|b$, pela definição acima temos que $b = a \cdot c$ e podemos dizer que:

- a é divisor de b;
- b é múltiplo de a.

Exemplo 3.1.1: Seja $a = 7$ e $b = 28$, como $28 = 7 \cdot 4$ temos que 7 é divisor de 28 e 28 é múltiplo de 7.

Proposição 3.1: Dados a,b,$c \in \mathbb{Z}$, tais que $a|b$ e $a|c$, então $a|(mb+nc)$, para quaisquer $m, n \in \mathbb{Z}$.

Demonstração. Sejam a,b,$c \in \mathbb{Z}$ tais que $a|b$ e $a|c$, então existem x_1,$x_2 \in \mathbb{Z}$ tais que $b = ax_1$ e $c = ax_2$. Multiplicando ambas as equações por m e n respectivamente, temos:

$$mb = max_1 \tag{3.1}$$

$$nc = nax_2 \tag{3.2}$$

Somando (3.1) e (3.2) lado a lado, obtemos:
$mb + nc = max_1 + nax_2 = a(mx_1 + nx_2)$. Logo, $a|(mb + nc)$. □

Exemplo 3.1.2: Dado os inteiros $2, 8$ e 26; como $2|8$ e $2|26$, pela proposição anterior temos que $2|(3 \cdot 8 + 5 \cdot 26)$ que implica em $2|154$.

Mesmo um número inteiro a não dividindo o número inteiro $b \neq 0$, podemos sempre efetuar a divisão de a por b, usando o chamado Lema da divisão de Euclides, enunciado abaixo.

Teorema 3.1 (Lema da divisão de Euclides): Sejam a e b inteiros com $b > 0$. Então existem inteiros q e r tais que $a = bq + r$ onde $b > r \geq 0$, onde q e r são únicos.

Demonstração. Existência: Considere o conjunto $S = \{a - bk | k \in \mathbb{Z} \ e \ a - bk \geq 0\}$.
Se $0 \in S$, existe $q \in \mathbb{Z}$ tal que $a - bq = 0$. Fazendo $r = 0$ o algoritmo está provado.
Se $0 \notin S$ vamos aplicar o Princípio da Boa Ordenação[1] (PBO). Para isso temos que provar que $S \neq \emptyset$.
Se $a > 0$, $a - b0 = a > 0$, então $S \neq \emptyset$.
Se $a < 0$, $a - b2a = a(1 - 2b) > 0$ e então $S \neq \emptyset$.
Pelo PBO, S possui um menor elemento que chamaremos de r. Assim, existem q,$r \in \mathbb{Z}$ tais que $a - bq = r$, r é o menor elemento de S e $r > 0$. Só falta provar que $r < b$.
Se $r = b$

$$\begin{gathered} a - bq = r = b \\ a - bq = b \\ a - b(q + 1) = 0 \end{gathered}$$

Isto indica que $0 \in S$, o que não acontece neste caso.
Se $r > b$

$$\begin{gathered} a - bq = r > b \\ a - bq - b > 0 \\ a - b(q + 1) > 0 \end{gathered}$$

Isto indica que $a - b(q + 1)$ pertence a S o que é um absurdo pois é menor que $r = a - bq$ e r é o menor elemento de S.
Unicidade: Suponha que existam q, q',r,r' tais que

$$a = bq + r = bq' + r'$$

com $0 \leq r, r' < b$. Como

$$r' - r = b(q' - q)$$

[1] O Princípio da Boa Ordenação nos garante que todo subconjunto não vazio de inteiros positivos, possui um menor elemento. Sua prova pode ser verificada em [10].

temos que $b|(r'-r)$. Mas como $r'-r<b$ concluímos que $r'-r=0$, $r'=r$ e $q=q'$. □

Notação: q será chamado *quociente* e r será chamado de *resto* da divisão de a por b.

Exemplo 3.1.3: Se $a=34$ e $b=7$ o algoritmo diz que $34=7\cdot 4+6$; para $a=-49$ e $b=6$, o algoritmo de Euclides diz que $-49=6\cdot(-9)+5$.

Definição 3.2: Dados a,b,c,$d\in\mathbb{Z}$ com $d\geq 0$, dizemos que d é um *máximo divisor comum (mdc)* de a e b se possuir as seguintes propriedades:

- $d|a$ e $d|b$
- Se $c|a$ e $c|b$, então $c|d$

Notação: $mdc(a,b)=d$ ou $(a,b)=d$

Exemplo 3.1.4: Dados $a=36$, $b=16$, $c=2$ e $d=4$, temos que $mdc(36,16)=4$. De fato, pois $4|36$ e $4|16$; e, pela definição acima temos que se $2|36$, $2|16$ então $2|4$.

Definição 3.3: Dados $a,b\in\mathbb{Z}$ dizemos que a e b são *primos entre si*, *coprimos*, ou *relativamente primos*, se $mdc(a,b)=1$.

Exemplo 3.1.5: 20 e 21 são coprimos, pois, $mdc(20,21)=1$.

Lema 3.1: Sejam $a,b,n\in\mathbb{Z}$. Se existe $mdc(a,b-na)$, então $mdc(a,b)$ existe e $mdc(a,b)=mdc(a,b-na)$.

Demonstração. Seja $d=mdc(a,b-na)$. Como $d|a$ e $d|(b-na)$, segue que $d|(b-na+na)\Rightarrow d|b$. Logo, d é um divisor comum de a e b. Suponha que $c|a$ e $c|b$ então como c é um divisor comum de a e $b-na$, temos que $c|(b-na+na)=b$ e, consequentemente, $c|d$. Logo, $d=mdc(a,b)$. □

Exemplo 3.1.6: Vamos calcular o (637,3887).

Note que $3887=6\cdot 637+65$. Assim, pelo Lema anterior temos $(637,3887)=(637,65)$. Mas $637=65\cdot 9+52$, e pelo mesmo lema $(637,65)=(65,52)$. Novamente, por $65=52\cdot 1+13$ temos $(65,52)=(52,13)=13$. Logo, pelo Lema (3.1) $(637,3887)=(637,65)=(65,52)=(52,13)=13$.

Teorema 3.2 (Bachet-Bézout): Sejam $a,b\in\mathbb{Z}$ não ambos nulos. Então existem $x,y\in\mathbb{Z}$ tais que $ax+by=mdc(a,b)$.

Demonstração. Sejam $a,b\in\mathbb{Z}$, com $b\neq 0$. Consideremos o conjunto $I(a,b)=\{ax+by|x,y\in\mathbb{Z}\}$.Seja $d=ax_0+by_0$ o menor inteiro positivo em $I(a,b)$. Assim, existe pelo menos um inteiro positivo em $I(a,b)$; de fato, $|b|\in I(a,b)$.

Afirmação: d divide todos os elementos de $I(a,b)$.

De fato, dado $m=ax+by\in I(a,b)$ e $q,r\in\mathbb{Z}$ tais que $m=qd+r$ com $0\leq r<d$.

Temos que $r = m - qd = a \cdot (x - qx_0) + b \cdot (y - qy_0) = r \in I(a,b)$, e, como d é o menor inteiro positivo em $I(a,b)$, então $r = 0$.
Daí, como $a, b \in I(a,b)$ (basta escolher $(x,y) = (1,0)$ e $(x,y) = (0,1)$, respectivamente), temos que d divide a e b. Portanto, $d \leq mdc(a,b)$. Por outro lado, $mdc(a,b)$ divide a e b, de modo que $mdc(a,b)$ divide d e, juntamente com a desigualdade $d \leq mdc(a,b)$, concluímos que $mdc(a,b) = d$. □

Exemplo 3.1.7: Sejam $a = 20$ e $b = 35$, temos que $(20,35) = 5$. O teorema anterior nos garante que existem $x,y \in \mathbb{Z}$ tais que $ax + by = mdc(a,b)$. De fato, se $x = 2$ e $y = -1$ temos que $20 \cdot 2 + 35 \cdot -1 = 5 = mdc(20,35)$.

Proposição 3.2 (Lema de Gauss): Sejam a, b e c números inteiros. Se $a|bc$ e $mdc(a,b) = 1$, então $a|c$.

Demonstração. Se $a|bc$, então, existe $e \in \mathbb{Z}$, tal que $bc = ae$. Como $mdc(a,b) = 1$, pela Identidade de Bezout (3.2) existem x e y inteiros, tais que

$$ax + by = 1.$$

Multiplicando ambos os lados da equação acima por c, temos:

$$c = c(ax + by)) \Rightarrow c = cax + cby$$

Substituindo bc por ae nesta última igualdade temos que $c = cax + aey$, ou seja, $c = a(cx + ey)$, com $cx + ey \in \mathbb{Z}$. Portanto, $a|c$. □

Exemplo 3.1.8: Sejam $a = 4$, $b = 3$ e $c = 4$, temos que $4|12 = 2 \cdot 6$, mas $4 \nmid 2$ e $4 \nmid 6$. Além disso, $(4,2) = (4,6) = 2$ já que $4|12$ e $12 = 3 \cdot 4$. Como $(4,3) = 1$, pelo lema acima, $4|4$.

Proposição 3.3 (Lema de Euclides): Dados $a,b,p \in \mathbb{Z}$, com p primo. Se $p|ab$ então $p|a$ ou $p|b$.

Demonstração. Suponhamos que $p \nmid a$. Então $mdc(p,a) = 1$. Como $p|ab$ e $mdc(a,p) = 1$, pelo Lema de Gauss (3.2), temos que $p|b$. A demonstração é análoga para quando $p \nmid b$. Logo, $p|a$ ou $p|b$. □

Corolário 3.1: Se p é primo e $p|a_1a_2 \cdots a_n$ então $p|a_i$, para algum $1 \leq i \leq n$.

Demonstração. Suponha que $p \mid a_1 \cdot a_2 \cdots a_{n-1} \cdot a_n$ com p primo e $a_i \in \mathbb{Z}$ para $i \in \{1, \cdots n\}$.

Vamos provar por indução.

Se $p \mid a_1a_2$, temos pelo teorema anterior que $p \mid a_1$ ou $p \mid a_2$.

Suponha agora que sempre que p divide um produto de $n-1$ inteiros, p divide um dos números. Em símbolos: $p \mid a_1 \cdots a_{n-1}$ com $a_i \in \mathbb{Z}$, então $p \mid a_j$ para algum j.

Considere agora que $p \mid a_1 \cdots a_{n-1} \cdot a_n$ om $a_i \in \mathbb{Z}$ e chame $b = a_1 \cdots a_{n-1}$. Assim $p \mid b \cdot a_n$. Como $b \in \mathbb{Z}$, teremos $p \mid a_n$ ou $p \mid b$.

Se $p \mid a_n$, já chegamos onde queríamos demonstrar.

Se $p \mid b$, por indução teremos que $p \mid a_i$ para algum $i \in \{1, \cdots, n-1\}$. □

Teorema 3.3 (Teorema Fundamental da Aritmética): Seja $a > 1$ um inteiro positivo. Então a é primo, ou existem números primos positivos $p_1 \leq p_2 \leq \cdots \leq p_t$ tais que $a = p_1 p_2 \ldots p_t$ e essa decomposição é única.

Demonstração. Existência: Para $a = 2$ existe uma decomposição trivial em números primos, já que 2 é, ele próprio, um número primo. Suponhamos agora que existe uma decomposição para todo inteiro b tal que $2 \leq b < a$. Mostraremos que também vale para a.

Se a é primo, admite a decomposição trivial. Caso contrário, a admite um divisor positivo b tal que $1 < b < a$. Isto é, $a = bc$ e temos também $c < a$. Pela hipótese de indução, b e c podem ser escritos como produtos de primos, na forma

$$b = p_1 p_2 \ldots p_s \qquad \text{e} \qquad c = q_1 q_2 \ldots q_k$$

Substituindo, temos

$$a = p_1 p_2 \ldots p_s q_1 q_2 \ldots q_k$$

e o resultado também vale para a.

Unicidade: Dado um inteiro a ele poderia admitir, em princípio, mais de uma decomposição em produto de fatores primos. Suponhamos que a admita duas decomposições da forma

$$a = p_1 = q_1 q_2 \ldots q_s$$

onde p_1 é primo, e $q_1 \leq q_2 \leq \cdots \leq q_s$ são primos. Como q_1 divide $q_1 q_2 \ldots q_s$ então, também divide p_1 que é primo. Então, devemos ter $p_1 = q_1$. Portanto obtemos

$$1 = q_2 \ldots q_s$$

Se $s > 1$ teríamos que o primo q_2 seria invertível, uma contradição. Assim, $s = 1$ e, como já provamos que $p_1 = q_1$ o primeiro passo de indução está verificado.

Suponhamos agora o resultado verdadeiro para todo inteiro que admita uma decomposição de comprimento k e seja a um inteiro com uma decomposição de comprimento $k + 1$. Se a admitir outra decomposição, temos

$$a = p_1 p_2 \ldots p_{k+1} = q_1 q_2 \ldots q_s$$

em que $q_1 \leq q_2 \leq \cdots \leq q_s$ são primos. Como na primeira parte, q_1 divide $p_1 p_2 \ldots p_{k+1}$, temos pelo corolário 3.1 que q_1 divide p_i para algum i. Como p_i é primo, devemos ter novamente que $q_1 = p_i$. Em particular, $q_1 \leq p_1$. De forma análoga, pode-se obter que $p_1 = q_j$ para algum j. Logo, $p_1 \leq q_1$. De ambas as desigualdades, vem que $p_1 = q_1$. Finalmente, cancelando em $a = p_1 p_2 \ldots p_{k+1} = q_1 q_2 \ldots q_s$

temos que

$$p_2 \dots p_{k+1} = q_2 \dots q_s$$

Agora, o primeiro membro da igualdade tem uma decomposição de comprimento k logo, da hipótese de indução, admite uma única decomposição. Assim, temos $k = s - 1$ de onde $s = k + 1$ e $p_i = q_i$, para $i = 2, \dots, k + 1$. Como já provamos que $p_1 = q_1$, ambas as expressões de a coincidem. □

Assim para todo $a > 1$ existem $q_1 < q_2 < \cdots < q_r$ primos e $\alpha_1 \cdot \alpha_2, \cdots, \alpha_r \in \mathbb{N} - \{0\}$ tais que $a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$, que chamamos de *fatoração canônica* de a em primos.

Exemplo 3.1.9: Seja $a = 68$. Como 68 não é primo, pelo Teorema Fundamental da Aritmética ele pode ser decomposto em primos, de uma única maneira. De fato, $68 = 2^2 \cdot 17$.

Uma definição importante em $\mathbb{Z}$ é a relação de congruência, que veremos a seguir.

Definição 3.4: Seja $n \in \mathbb{Z}^+$. Dizemos que dois números a e b (a,$b \in \mathbb{Z}$) são congruentes módulo m, se os restos de sua divisão euclidiana por m são iguais.

Notação: $a \equiv b (\text{mod } m)$

Exemplo 3.1.10: Temos $7 \equiv 4 (\text{mod } 3)$, pois o resto da divisão de 7 por 3 e de 4 por 3 são ambos 1.

Note que $a \equiv b (\text{mod } m)$ se e só se $m|(a - b)$. De fato, se $a \equiv b (\text{mod } m)$ temos que

$$a = q_1 m + r$$

$$b = q_2 m + r$$

com $0 \leq r < m$. E, efetuando $a - b$, temos $a - b = (q_1 - q_2)m$. Logo, $m|q_1 - q_2$.

Agora, se $m|(a - b)$ temos $a - b = mk$, para algum $k \in \mathbb{Z}$. Efetuando a divisão

$$a = q_1 m + r_1 \text{ e } b = q_2 m + r_2 \text{ com } 0 \leq r_1, r_2 < m$$

que implica em $a - b = (q_1 - q_2)m + r_1 - r_2$. Como $m|(a - b)$, $r_1 - r_2 = 0$. Portanto, $r_1 = r_2$.

Exemplo 3.1.11: $11 \equiv 23 (\text{mod } 4)$, pois $23 - 11 = 12$ e $4|12$.

3.1.1 Trio Pitagórico

Os trios de números (a,b,c) com a,b,$c \in \mathbb{Z}$ que satisfazem a equação $a^2 + b^2 = c^2$ são denominados *trios* ou *ternos Pitagóricos*. Nesta seção iremos encontrar todos os trios Pitagóricos.

Se existir um p primo tal que $p|a$ e $p|b$ então $p|a^2$ e $p|b^2$. Daí, $p|(a^2 + b^2) = c^2$ e consequentemente, $p|c$, pois p é primo. Logo, $\left(\frac{a}{p}, \frac{b}{p}, \frac{c}{p}\right)$ também é um trio pitagórico, o que não acontece se a, b e c são primos entre si. Um trio pitagórico em que os termos são dois a dois primos entre si é chamado *trio pitagórico primitivo*.

Assim, quando o trio pitagórico é primitivo, a e b não podem ser pares ao mesmo tempo. Suponhamos, sem perda de generalidade, que a é ímpar. Sabemos que todo número n pode ser escrito como $2k$ ou $2k+1$, com $k \in \mathbb{Z}$. Deste modo, $n^2 = (2k)^2 = 4k^2 \equiv 0 \pmod 4$ ou $n^2 = (2k+1)^2 = 4k^2 + 4k + 1 \equiv 1 \pmod 4$. Daí, segue que todos os quadrados perfeitos são congruentes a 0 ou a 1 módulo 4. Portanto, b não pode ser ímpar, pois se for, $c^2 = a^2 + b^2 \equiv 1 + 1 \equiv 2 \pmod 4$. Absurdo! Portanto, b é par. Logo, a é ímpar, b é par e, consequentemente, c é ímpar.

Por outro lado, $b^2 = c^2 - a^2 = (c+a)(c-a)$. Como $mdc(a,c) = 1$ então pelo lema 3.1 temos que $mdc(c,c+a) = mdc(c, -c+c+a) = mdc(c,a) = 1$ e $mdc(c+a,c-a) = mdc(c-a,c+a-(c-a)) = mdc(c-a,2a) = 2$, já que a é ímpar e $c-a$ é par. Assim, $mdc\left(\frac{c+a}{2}, \frac{c-a}{2}\right) = \frac{2}{2} = 1$ ou seja, são coprimos e seu produto é um quadrado perfeito, pois

$$\left(\frac{b}{2}\right)^2 = \frac{c^2 - a^2}{4} = \left(\frac{c+a}{2}\right)\left(\frac{c-a}{2}\right).$$

Pelo Teorema Fundamental da Aritmética (3.3), cada um desses fatores devem ser o quadrado de um número natural, pois se $\left(\frac{b}{2}\right)^2 = \frac{c^2-a^2}{4} = \left(\frac{c+a}{2}\right)\left(\frac{c-a}{2}\right)$ então $\left(\frac{c+a}{2}\right)\left(\frac{c-a}{2}\right)$ é um quadrado perfeito. Com efeito, $\frac{b}{2} = p_1 \cdot p_2 \cdot p_3 \cdots p_n$ onde p_i são primos, com $i = 1,2,3,\cdots,n$ então $\left(\frac{b}{2}\right)^2 = p_1^2 \cdot p_2^2 \cdot p_3^2 \cdots p_n^2$. Daí $\left(\frac{c+a}{2}\right)\left(\frac{c-a}{2}\right) = p_1^2 \cdot p_2^2 \cdot p_3^2 \cdots p_n^2$. Logo $\frac{c+a}{2}$ e $\frac{c-a}{2}$ são quadrados perfeitos.

Dessa forma, existem m e n tais que $\frac{c+a}{2} = m^2$ e $\frac{c-a}{2} = n^2$. Assim, $\frac{b^2}{4} = m^2 \cdot n^2 \Rightarrow b^2 = 4m^2n^2 \Rightarrow b = 2mn$, com $mdc(m,n) = 1$.

Escrevendo a,b e c em termos de m e n, temos:

$$\left(\frac{c+a}{2}\right) + \left(\frac{c-a}{2}\right) = \frac{2 \cdot c}{2} = m^2 + n^2 \Rightarrow c = m^2 + n^2$$

Daí,

$$\frac{c+a}{2} = \frac{m^2 + n^2 + a}{2} = m^2 \Rightarrow m^2 + n^2 + a = 2m^2 \Rightarrow a = m^2 - n^2$$

Portanto, $a = m^2 - n^2$, $b = 2mn$ e $c = m^2 + n^2$.

Exemplo 3.1.12: Os números $a = 3$, $b = 4$ e $c = 5$ formam um trio pitagórico primitivo. De fato, considerando $m = 2$ e $n = 1$ temos que $3 = m^2 - n^2$, $4 = 2mn$ e $5 = m^2 + n^2$, o que satisfaz a demonstração anterior.

3.2 Anéis

Em matemática, mais especificamente na álgebra abstrata, um anel é uma estrutura algébrica que consiste em um conjunto não vazio, associado a duas operações binárias, normalmente chamadas de adição e multiplicação; em que cada operação combina dois elementos para formar um terceiro.

Para se qualificar como um anel, o conjunto e suas duas operações devem satisfazer determinadas condições. Vejamos abaixo:

3.2.1 Definições e propriedades

Definição 3.5: Um conjunto $A \neq \emptyset$ munido de duas operações $+$ e $\cdot$, tal que

$$\begin{aligned} + : A \times A &\longrightarrow A \\ (a_1,a_2) &\mapsto a_1 + a_2 \end{aligned}$$

e

$$\begin{aligned} \cdot : A \times A &\longrightarrow A \\ (a_1,a_2) &\mapsto a_1 \cdot a_2 \end{aligned}$$

é um *anel* se satisfaz as seguintes condições:

1. *Comutatividade da soma:* $\forall\ x,y \in A$, temos

$$x + y = y + x$$

2. *Associatividade da soma:* $\forall\ x,y,z \in A$, temos

$$(x + y) + z = x + (y + z)$$

3. *Elemento neutro da adição:* $\forall\ x \in A$, $\exists\ e \in A$ tal que

$$x + e = x$$

   Notação: $e = 0$

4. *Elemento simétrico:* $\forall\ x \in A$, $\exists\ y \in A$ tal que

$$x + y = e \Rightarrow x + y = 0$$

   Notação: $y = -x$

5. *Associatividade da multiplicação:* $\forall\ x,y,z \in A$ temos

$$(x \cdot y) \cdot z = x \cdot (y \cdot z)$$

6. *Distributividade da multiplicação em relação à soma:* $\forall\ x,y,z \in A$ temos

$$x \cdot (y + z) = x \cdot y + x \cdot z$$

$$(y + z) \cdot x = y \cdot x + z \cdot x$$

Notação: $(A, +, \cdot)$

Exemplo 3.2.1: O conjunto dos inteiros $\mathbb{Z}$ com adição e a multiplicação usuais é um anel.

Podemos observar que a multiplicação não necessita ser comutativa.

Definição 3.6: Quando em um anel A, a multiplicação é comutativa, dizemos que A é um *anel comutativo*.

Um anel não necessita ter elemento neutro da multiplicação (isto é, um elemento y tal que $xy = yx = x \ \forall \ x \in A$). Este elemento, quando existir, será denotado por 1 e chamado de *identidade do anel* A.

Definição 3.7: Quando um anel A possui o elemento neutro da multiplicação dizemos que A é um *anel com unidade.*

Exemplo 3.2.2: O anel $\mathbb{Z}$ é um anel comutativo com unidade. Note que o elemento neutro da multiplicação é 1.

Os elementos não nulos de um anel não necessariamente precisam possuir um inverso multiplicativo, (isto é, y é inverso multiplicativo de x se só se $xy = yx = 1$). Por exemplo, $2 \in \mathbb{Z}$ não possui inverso, pois não existe inteiro y tal que $2y = 1$.

Definição 3.8: Os elementos de um anel A que possuem inverso multiplicativo são chamados *invertíveis de* A ou *unidades de* A.

Usaremos a notação $U(A) = \{x \in A \mid x \text{ é uma unidade de A}\}$ para o conjunto das unidades de um anel A.

Exemplo 3.2.3: Vamos encontrar as unidades de $\mathbb{Z}_6$.
Note que se $x \in \mathbb{Z}$ é unidade, existe $x^{-1} \in \mathbb{Z}$ tal que $x \cdot x^{-1} = 1$.
Assim $x^{-1} = \frac{1}{x}$ e, portanto, $x = \pm 1$.
Logo $U(\mathbb{Z}) = \{-1, +1\}$.

Teorema 3.4 (Propriedades:): Sejam a,b e c elementos de um Anel A. Então:

1. Se $a + b = a + c$ então $b = c$
2. O elemento neutro aditivo é único.
3. O inverso aditivo é único.
4. $a \cdot 0 = 0 \cdot a = 0$
5. $a(-b) = (-a)b = -(ab)$
6. $(-a)(-b) = ab$
7. $a(b - c) = ab - ac$ e $(b - c)a = ba - ca$

   Se A tem unidade 1 então

8. $(-1)a = a$
9. (-1)(-1)=1
10. O elemento neutro da multiplicação é único.
11. O inverso multiplicativo é único.

Demonstração.

1. Basta somarmos aos dois lados da igualdade, o simétrico de a.

$$a + b = a + c \Rightarrow -a + a + b = -a + a + c \Rightarrow b = c$$

2. Suponha que e_1 e e_2 são elementos neutros da soma.
   Como e_1 é elemento neutro,

$$e_1 + e_2 = e_2.$$

   Mas e_2 também é elemento neutro, então

$$e_1 + e_2 = e_1.$$

   Temos, portanto

$$e_1 + e_2 = e_2$$

   e

$$e_1 + e_2 = e_1.$$

   Logo $e_1 = e_2$ e o elemento neutro da soma é único.
3. Suponhamos que $a \in A$ possua dois inversos aditivos a_1 e a_2. Então

$$a + a_1 = a + a_2 = 0 \Rightarrow -a + a + a_1 = -a + a + a_2 \Rightarrow a_1 = a_2.$$

   Portanto, o inverso aditivo da soma é único.
4. Pela distributividade temos $a \cdot 0 = a(0 + 0) = a \cdot 0 + a \cdot 0$. Pelo cancelamento em 1, temos que $a \cdot 0 = 0$.
   Analogamente, $0 \cdot a$.
5. Queremos provar que $a(-b)$ é o simétrico de ab. Para isso, basta somar $a(-b) + ab$ e verificar se o resultado é zero. Como $a(-b) + ab = a(-b + b) = a \cdot 0 = 0$, segue o resultado.
   A demonstração é análoga para provar que $(-a)b$ é o simétrico de ab.
6. Pelo item anterior $(-a)(-b) = -[a(-b)] = -[-ab]$. É fácil ver que $-(-a) = a$ para todo a em A, e assim $(-a)(-b) = a \cdot b$.

7. Pelas propriedades anteriores temos

$$a(b-c) = a(b+(-c)) = ab + a(-c) = ab + (-ac) = ab - ac$$

8. Pela propriedade 5 temos que $(-1)a = -(1a) = -a$
9. A demonstração é direta pela propriedade 6.
10. Suponhamos que existam duas unidades em A: 1 e b. Pela definição de unidade teremos $1 = 1 \cdot b = b$
11. Suponhamos que b e c sejam inversos multiplicativos de a. Assim, $ba = ab = ac = ca = 1$ e $b = b1 = bac = 1c = c$. Logo, $b = c$ e portanto, o inverso multiplicativo é único.

□

Exemplo 3.2.4: O anel $2\mathbb{Z} = \{2k \mid k \in \mathbb{Z}\}$ com a soma e o produto, é um anel comutativo sem unidade.

3.2.2 Subanéis

Nesta subseção vamos estudar os subconjuntos de um anel.

Definição 3.9: Um subconjunto S de um anel A é um *subanel* de A se S for um anel com as operações de A.

Exemplo 3.2.5: $(\mathbb{Z}, +, \cdot)$ é um subanel de $(\mathbb{Q}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$ é um subanel de $(\mathbb{R}, +, \cdot)$ e $(\mathbb{R}, +, \cdot)$ é um subanel de $(\mathbb{C}, +, \cdot)$.

Para facilitar a verificação se um subconjunto S de um anel A é um subanel, há um teste que diz que podemos apenas verificar se para todo a,$b \in S$, $a - b \in S$ e $ab \in S$, que é provado no teorema abaixo.

Teorema 3.5 (Teste de subanel): Seja $S \neq \emptyset$ um subconjunto de A. S é um subanel de A se for fechado para a soma e a multiplicação, ou seja, se $\forall$ a,$b \in S$, $a - b \in S$ e $ab \in S$.

Demonstração. As propriedades comutativa, associativa e distributiva são válidas para A, como $S \subset A$ então também são válidas para S.
Por hipótese, se a e $b \in S$ então $ab \in S$. Como $S \neq \emptyset$, tome $x \in S$. Por hipótese $x - x = 0 \in S$. Também por hipótese, $0 - a = -a \in S$ $\forall a \in S$. □

Exemplo 3.2.6 (Inteiros de Gauss): Os inteiros de Gauss é o anel $\mathbb{Z}[i]$ definido por $\mathbb{Z}[i] = \{a + bi \mid a,b \in \mathbb{Z}\}$. Vamos mostrar que $\mathbb{Z}[i]$ é um subanel de $\mathbb{C}$.
De fato, $\mathbb{Z}[i] \neq \emptyset$ e $\mathbb{Z}[i] \subset \mathbb{C}$, além disso

$$(a+bi)(c+di) = (ac-bd) + (ad+bc)i \in \mathbb{Z}[i]$$
$$(a+bi) - (c+di) = (a-c) + (b-d)i \in \mathbb{Z}[i].$$

Pelo teorema 3.5, $\mathbb{Z}[i]$ é um subanel de $\mathbb{C}$.

3.2.3 Domínio de Integridade

Nesta seção trabalharemos com um anel especial, dito Domínio de Integridade.

Definição 3.10 (Divisor de zero): Um elemento não nulo a em um anel comutativo A é chamado um *divisor de zero* se existe um elemento b não nulo em A tal que $ab = 0$.

Exemplo 3.2.7: Vamos definir o anel $\mathbb{Z}_n$. Note que a relação de congruência em $\mathbb{Z}$ definida em (3.4) é uma relação de equivalência. A classe módulo m de $a \in \mathbb{Z}$ é, por definição

$$\begin{aligned} \overline{a} &= \{b \in \mathbb{Z} | a \equiv b \mod m\}, \quad \text{ou ainda,} \\ \overline{a} &= \{b \in \mathbb{Z} | b = a + km\} \end{aligned}$$

Pela divisão Euclidiana, podemos ver que, em módulo m temos m classes distintas, a saber $\overline{0}, \overline{1}, \overline{2}, \cdots, \overline{m-1}$.

O conjunto quociente[2] dessa relação é notacionado por $\mathbb{Z}_m$.

$$\begin{aligned} \mathbb{Z}_m &= \{\overline{a} \mid a \in \mathbb{Z}\} \\ \mathbb{Z}_m &= \left\{\overline{0}, \overline{1}, \cdots, \overline{m-1}\right\} \end{aligned}$$

Em $\mathbb{Z}_m$ definimos duas operações :

Soma: $\overline{a} \oplus \overline{b} = \overline{a+b}$
Multiplicação: $\overline{a} \odot \overline{b} = \overline{a \cdot b}$

Pode-se verificar $(\mathbb{Z}_m, \oplus, \odot)$ é um anel comutativo com unidade. (veja [10]).

Por exemplo, $\mathbb{Z}_6 = \left\{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}\right\}$ e note que $\overline{2} \cdot \overline{3} = \overline{2 \cdot 3} = \overline{6} = \overline{0}$. Logo, em $\mathbb{Z}_6$, $\overline{2 \cdot 3} = \overline{0}$ e $\overline{2}, \overline{3} \neq \overline{0}$. Assim, $\overline{2}$ e $\overline{3}$ são divisores de zero em $\mathbb{Z}_6$.

Definição 3.11 (Domínio de integridade): Um anel comutativo com unidade é chamado de *domínio de integridade* ou simplesmente *domínio* se ele não tem nenhum divisor de zero.

Assim, num domínio de integridade $ab = 0 \Leftrightarrow a = 0$ ou $b = 0$

Exemplo 3.2.8: $\mathbb{Z}[x]$ é um domínio de integridade.
De fato, sejam

$$f(x) = a_0 + a_1 x + \cdots + a_n x^n$$

e

$$g(x) = b_0 + b_1 x + \cdots + b_m x^m$$

em $\mathbb{Z}[x]$ tal que $f(x)g(x) = 0$.
Suponha que $f(x)$ e $g(x)$ não são nulos. Tome $a_{i_0} \in \mathbb{Z}$ de modo que i_0 seja o menor coeficiente de $f(x)$ tal que a_{i_0}. Analogamente, tome b_{j_0} em $g(x)$ tal que j_0 é o menor

[2] Conjunto quociente de uma relação de equivalência é o conjunto das classes de equivalência.

índice tal que $b_{j_0} \neq 0$. Se $f(x)g(x) = c_0 + c_1x + c_2x^2 + \cdots + c_{n+m}x^{n+m}$ teremos pela nossa escolha de i_0 e j_0 que $c_{i_0+j_0} = a_{i_0}b_{j_0} \neq 0$. Absurdo!

Logo $f(x)$ ou $g(x)$ é nulo.

3.2.4 Ideais

Já sabemos o que é um subanel, mas entre eles há alguns que possuem uma característica bem interessante, os chamados ideais.

Definição 3.12 (Ideal): Um subanel I de um anel A é um *ideal* de A se para todo $a \in A$ e todo $x \in I$, $xa \in I$ e $ax \in I$.

Assim, um subanel de um anel A é um ideal se ele "absorve"os elementos de A, isto é, $aI \subseteq I$ e $Ia \subseteq I$ para todo a em A .

Teorema 3.6 (Teste para saber se é ideal): Um subconjunto não vazio de um anel I é um ideal de A se :

1. $a - b \in I$, $\forall$ a,$b \in I$
2. xa e ax estão em I quando $a \in A$ e $x \in I$

Definição 3.13: Seja A um anel comutativo com unidade e $x \in A$. O conjunto $\langle x \rangle = \{ax \mid a \in A\}$ é um ideal de A e chamado *ideal gerado por x.*

De fato $\langle x \rangle$ é um ideal, note que para todo $b \in A$ temos $by \in \langle x \rangle$ para todo $y \in \langle x \rangle$, já que $y = ax$ para algum a em A, e $by = b(ax) = (ba)x$.

Além disso, para todo y,$z \in \langle x \rangle$ temos $y = ax, z = bx$ para a e b em A. E $y - z = ax - bx = (a - b)x \in \langle x \rangle$. Logo, pelo teste acima, $\langle x \rangle$ é um ideal de A.

Todo ideal deste tipo é dito Ideal Principal.

Exemplo 3.2.9: O ideal de $\mathbb{Z}$, $4\mathbb{Z}$ é principal pois, $4\mathbb{Z} = \langle 4 \rangle = \{4t \mid t \in \mathbb{Z}\}$.

Ideais Principais são ideais muito importantes na teoria de anéis, aparecendo em diversos contextos. No decorrer do trabalho, vamos estudar um domínio dito Domínio de Ideias Principais.

3.2.5 Anel Quociente

Nesta seção vamos estudar um anel, dito anel quociente. Ele é estabelecido a partir de uma relação de equivalência. Assim, para sua construção, considere um anel A e I um ideal de A. Defininimos em A a relação:

$$x \sim y \Leftrightarrow x - y \in I$$

É fácil ver que $\sim$ é uma relação de equivalência:

1. $x \sim x$ pois $x - x = 0 \in I$
2. Se $x \sim y$ então $y \sim x$ pois se $x - y \in I$ implica em $y - x = -(x - y) \in I$ por que I é um ideal.

3. Se $x \sim y$ e $y \sim z$ então $x \sim z$, pois se $x - y \in I$ e $y - z \in I$, somando temos que $x - z \in I$ pela definição de Ideal.

Assim, como toda relação de equivalência determina uma partição temos que A vai ser a união disjunta das classes de equivalência:

$$A = \bigcup_{x \in A} [x]$$

onde

$$[x] = \{y \in A \mid y \sim x\} = \{y \in A \mid y - x \in I\} = \{y \in A \mid y \in x + I\}$$

Usaremos a notação

$$x + I = [x]$$

e

$$A/I = \{x + I \mid x \in A\}.$$

Queremos transformar A/I em um anel. Para isso, vamos definir em A/I duas operações e depois provar que elas estão bem definidas, pois como estamos trabalhando com classes, e portanto, conjuntos, elas não poderão depender do representante da classe.
As operações vão ser:

$$(x_1 + I) + (x_2 + I) = (x_1 + x_2) + I$$

e

$$(x_1 + I) \cdot (x_2 + I) = (x_1 \cdot x_2) + I$$

Suponha que $x_1 + I = y_1 + I$ e $x_2 + I = y_2 + I$. Então $x_1 - y_1 \in I$ e $x_2 - y_2 \in I$. Como I é um ideal $(x_1 - y_1) + (x_2 - y_2) \in I$, ou seja, $(x_1 + x_2) - (y_1 + y_2) \in I$. Pela definição da relação de equivalência, isto indica que $(x_1 + x_2) + I = (y_1 + y_2) + I$ e fica provado que a soma está bem definida.

Para provar que o produto está bem definido, observe que

$$x_1x_2 - y_1y_2 = (x_1 - y_1)x_2 + y_1(x_2 - y_2)$$

Como I é um ideal, $(x_1 - y_1)x_2 \in I$ e $y_1(x_2 - y_2) \in I$, $x_1x_2 - y_1y_2 \in I \Rightarrow x_1x_2 + I = y_1y_2 + I$. Logo o produto fica bem definido.

Teorema 3.7: Seja I um ideal do anel A, então $(A/I, +, \cdot)$ é um anel.

Demonstração.

Vamos mostrar que a operação soma no conjunto quociente A/I satisfaz as condições de anel.

1. Comutatividade:

$$(x_1 + I) + (x_2 + I) = (x_1 + x_2) + I$$

$$(x_2 + I) + (x_1 + I) = (x_1 + x_2) + I$$

2. Associatividade:

$$\begin{aligned}[(x_1 + I) + (x_2 + I)] + (x_3 + I) &= (x_1 + x_2)I + (x_3 + I) \\ &= (x_1 + x_2 + x_3) + I\end{aligned}$$

$$\begin{aligned}(x_1 + I) + [(x_2 + I) + (x_3 + I)] &= (x_1 + I) + (x_2 + x_3) + I \\ &= (x_1 + x_2 + x_3) + I\end{aligned}$$

3. Elemento Neutro: Note que a classe $0 + I$ é o elemento neutro da soma, pois

$$(x + I) + (0 + I) = (x + 0) + I = (x + I).$$

4. Simétricos: Note que o simétrico de $x + I$ é a classe $(-x) + I$, onde $-x$ é o simétrico de x em A.

$$(x + I) + (-x + I) = (x - x) + I = 0 + I.$$

Agora verificaremos as propriedades de anel para a multiplicação.

5. Associatividade:

$$\begin{aligned}[(x_1 + I) \cdot (x_2 + I)] \cdot (x_3 + I) &= [(x_1 \cdot x_2) + I] \cdot (x_3 + I) \\ &= (x_1 \cdot x_2 \cdot x_3) + I\end{aligned}$$

$$\begin{aligned}(x_1 + I) \cdot [(x_2 + I) \cdot (x_3 + I)] &= (x_1 + I) \cdot [(x_2 \cdot x_3) + I] \\ &= (x_1 \cdot x_2 \cdot x_3) + I\end{aligned}$$

6. Distributividade:

$$\begin{aligned}(x_1 + I) \cdot [(x_2 + I) + (x_3 + I)] &= [(x_1 + I) \cdot (x_2 + I)] + [(x_1 + I) \cdot (x_3 + I)] \\ &= [(x_1 \cdot x_2) + I] + [(x_1 \cdot x_3) + I] \\ &= [(x_1 \cdot x_2) + (x_1 \cdot x_3)] + I\end{aligned}$$

$$\begin{aligned}[(x_2 + I) + (x_3 + I)] \cdot (x_1 + I) &= [(x_2 + I) \cdot (x_1 + I)] + [(x_3 + I) \cdot (x_1 + I)] \\ &= [(x_2 \cdot x_1) + I] + [(x_3 \cdot x_1) + I] \\ &= [(x_1 \cdot x_2) + (x_1 \cdot x_3)] + I\end{aligned}$$

□

Chamaremos A/I de *anel quociente*.

Exemplo 3.2.10: $\mathbb{Z}/4\mathbb{Z} = \{0+4\mathbb{Z}, 1+4\mathbb{Z}, 2+4\mathbb{Z}\}$ é um anel quociente.

De fato, todo n em $\mathbb{Z}$ é da forma $n = 4q+r$ onde $q \in \mathbb{Z}$ e $0 \leq r \leq 3$ pelo algoritmo de Euclides. Pela definição de classe de equivalência temos que $n + 4\mathbb{Z} = r + 4\mathbb{Z}$ com $r = 0,1,2,3$.

Dentre os domínios, destacamos os que possuem a propriedade abaixo:

Definição 3.14: Um *domínio de ideais principais (DIP)* é um domínio R no qual todo ideal tem a forma $\langle a \rangle = \{ra \mid r \in R\}$.

Exemplo 3.2.11: O anel dos inteiros $\mathbb{Z}$ é um DIP. Todos os ideais de $\mathbb{Z}$ são do tipo $\langle n \rangle = n\mathbb{Z}$.

Para verificar essa afirmação o leitor pode ver [10].

3.3 Homomorfismo de anéis

É comum na Matemática, trabalharmos com determinados conjuntos e compararmos os mesmos via funções. Na teoria de anéis não é diferente. Aqui, essas funções são chamadas de homomorfismos.

Definição 3.15 (Homomorfismo e isomorfismo de anéis): Um mapa $\phi : G \to H$ é um *homomorfismo* de um anel G em um anel H se

$$\phi(a+b) = \phi(a) + \phi(b)$$

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

$\forall\ a,b \in G$.
Um homomorfismo bijetor é chamado *isomorfismo de anéis*. Nesse caso dizemos que G e H são isomorfos e denotamos por $G \cong H$.

Quando temos um isomorfismo $\phi : G \to H$ isso significa que G e H são algebricamente idênticos.

Definição 3.16 (Núcleo de um Homomorfismo): Seja $\phi : G \to H$ um homomorfismo de anéis. Definimos o núcleo de ϕ como sendo o conjunto $ker\phi = \{a \in A \mid \phi(a) = 0\}$.

Teorema 3.8 (Propriedades dos homomorfismos de anéis): Seja ϕ um homomorfismo de um anel G em um anel H. Então:

1. $\phi(0) = 0$
2. $\phi(-g) = -\phi(g)$, $\forall\ g \in G$
3. Para todo $g \in G$ e todo $n \in \mathbb{Z}^+$, $\phi(ng) = n\phi(g)$ e $\phi(g^n) = \phi(g)^n$.

4. Se A é um subanel de G, então $\phi(A)$ é um subanel de H.
5. Se I é um ideal de G e ϕ é sobrejetivo, então $\phi(I)$ é um ideal de H.
6. Se J é um ideal de H, então $\phi^{-1}(J)$ é um ideal de G.
7. Se G é comutativo, então $\phi(G)$ é comutativo.
8. Se G tem unidade 1 e ϕ é sobrejetivo, então $\phi(1)$ é a unidade de H se H for não nulo.
9. ϕ é um isomorfismo se só se ϕ é sobrejetivo e $ker\phi = \{g \in G \mid \phi(g) = 0\} = \{0\}$.
10. Se ϕ é um isomorfismo de G sobre H, então ϕ^{-1} é um isomorfismo de H sobre G.

Demonstração. 1. Aplicando ϕ à expressão $0+0=0$ temos que $\phi(0+0) = \phi(0)$ e assim $\phi(0) + \phi(0) = \phi(0)$, isto é, $2\phi(0) - \phi(0) = 0 \Leftrightarrow \phi(0) = 0$.

2. Aplicando ϕ à expressão $g + (-g) = 0$ temos que $\phi(g) + \phi(-g) = \phi(0) = 0$. Somando $-\phi(g)$ em ambos os lados temos $\phi(-g) = -\phi(g)$ como queríamos provar.
3. $\phi(ng) = \phi(g + g + g + \cdots + g) = n\phi(g)$ e $\phi(g^n) = \phi(g \cdot g \cdot g \cdots g) = \phi(g)^n$ pela definição de homomorfismo.
4. Sejam x,$y \in \phi(A)$. Então $x = \phi(a_1)$ e $y = \phi(a_2)$ com a_1,$a_2 \in A$. Pelo teste 3.5, basta provar que $x - y \in \phi(A)$ e $xy \in \phi(A)$. Mas $x - y = \phi(a_1) - \phi(a_2) = \phi(a_1 - a_2) \in \phi(A)$ pois A é um subanel. Pelo mesmo motivo, $xy = \phi(a_1)\phi(a_2) = \phi(a_1a_2) \in \phi(A)$.
5. Como I é um subanel, pelo item anterior $\phi(I)$ já é um subanel de H. Falta provar que $H \cdot \phi(I) \subset \phi(I)$. Como ϕ é sobrejetora, todo h em H é da forma $h = \phi(g)$ para algum g em G. Assim, $h\phi(a) = \phi(g) \cdot \phi(a) = \phi(ga) \in \phi(I)$ $\forall\ a \in I$.
6. Aplicando o teste para saber se é um ideal (teorema 3.6), sejam x,$y \in \phi^{-1}(J)$. Existem então j_1 e j_2 em J tais que $\phi(x) = j_1$ e $\phi(y) = j_2$. Como $\phi(x - y) = \phi(x) - \phi(y) = j_1 - j_2 \in J$ temos que $x - y \in \phi^{-1}(J)$. Também, para todo $g \in G$ e $x \in \phi^{-1}(J)$ temos $\phi(gx) = \phi(g)\phi(x) \in J$ o que mostra que $gx \in \phi^{-1}(J)$.
7. Basta observar que $\phi(g_1)\phi(g_2) = \phi(g_1g_2) = \phi(g_2g_1) = \phi(g_2)\phi(g_1)$ $\forall\ g_1$,$g_2 \in G$.
8. Para todo $h \in H$, $h = \phi(g)$ para algum $g \in G$ pois ϕ é sobrejetiva. Assim, $h\phi(1) = \phi(g)\phi(1) = \phi(g1) = \phi(g) = h$. Analogamente, $\phi(1)h = h$.
9. Se ϕ é isomorfismo, então ϕ é bijetiva, isto é, se $\phi(g_1) = \phi(g_2)$ então $g_1 = g_2$. Se $g \in ker\phi$ então $\phi(g) = \phi(0) = 0$ e portanto $g = 0$. Assim, $ker\phi = \{0\}$. Reciprocamente, suponha que ϕ é sobrejetiva e $\ker\phi = \{0\}$. Vamos provar que ϕ é injetiva. Para isso, suponha que $\phi(g_1) = \phi(g_2)$. Então $\phi(g_1 - g_2) = 0 \Rightarrow g_1 - g_2 = 0$, pois $ker\phi = \{0\}$. Assim,como ϕ é sobrejetiva e injetiva e portanto, bijetiva. Logo, podemos concluir que ϕ é um isomorfismo.

10. Devemos provar que $\phi^{-1}(h_1 + h_2) = \phi^{-1}(h_1) + \phi^{-1}(h_2)$ e $\phi^{-1}(h_1 \cdot h_2) = \phi^{-1}(h_1) \cdot \phi^{-1}(h_2)$.
    Suponha que $\phi^{-1}(h_1) = g_1$ e $\phi^{-1}(h_2) = g_2$. Logo $\phi(g_1) = h_1$, $\phi(g_2) = h_2$ e $\phi(g_1 + g_2) = \phi(g_2) + \phi(g_2) = h_1 + h_2$. Isto mostra que $\phi^{-1}(h_1 + h_2) = g_1 + g_2 = \phi^{-1}(h_1) + \phi^{-1}(h_2)$.
    Analogamente, $\phi^{-1}(h_1 \cdot h_2) = \phi^{-1}(h_1) \cdot \phi^{-1}(h_2)$.

□

Exemplo 3.3.1: $\frac{\mathbb{Z}}{4\mathbb{Z}} \cong \mathbb{Z}_4$, basta notarmos que

$$\phi : \frac{\mathbb{Z}}{4\mathbb{Z}} \to \mathbb{Z}_4$$

$$a + 4\mathbb{Z} \longmapsto \overline{a}$$

é um isomorfismo de anéis.

Um dos mais importantes teoremas da teoria de anéis básica, é o Teorema Fundamental do Homomorfismo, ou, para alguns autores, dito como Primeiro Teorema do Isomorfismo. Com ele conseguimos provar diversos isomorfismos entre anéis.

Teorema 3.9 (Teorema fundamental do homomorfismo(TFH)): Seja ϕ um homomorfismo de um anel G no anel H. Então $\phi(G)$ é isomorfo ao anel quociente $\frac{G}{ker\phi}$. Em símbolos, $\phi(G) \cong \frac{G}{ker\phi}$.

Demonstração. Seja

$$\psi : \frac{G}{ker\phi} \to \phi(G)$$
$$g + ker\phi \longmapsto \phi(g)$$

Devemos mostrar que ψ é um isomorfismo.
Primeiramente, vamos provar que ψ está bem definida, isto é, que independe da escolha do representante da classe.
Suponha que $g_1 + ker\phi = g_2 + ker\phi$. Então $g_1 - g_2 \in ker\phi$, isto é, $\phi(g_1) = \phi(g_2)$ e $\psi(g_1 + ker\phi) = \psi(g_2 + ker\phi)$ e ψ está bem definida.

ψ é um homomorfismo pois

$$\begin{aligned}\psi(g_1 + ker\phi + g_2 + ker\phi) &= \psi(g_1 + g_2 + ker\phi)\\ &= \phi(g_1 + g_2)\\ &= \phi(g_1) + \phi(g_2)\\ &= \psi(g_1 + ker\phi) + \psi(g_2 + ker\phi)\end{aligned}$$

e

$$\begin{aligned}\psi\left[(g_1 + ker\phi)\cdot(g_2 + ker\phi)\right] &= \psi(g_1 \cdot g_2 + ker\phi)\\ &= \phi(g_1 \cdot g_2)\\ &= \phi(g_1)\cdot\phi(g_2)\\ &= \psi(g_1 + ker\phi)\cdot\psi(g_2 + ker\phi)\end{aligned}$$

ψ é injetiva, pois, $ker\psi = \left\{g + ker\phi \in \frac{G}{ker\phi} \mid \phi(g) = 0\right\} = \{0 + ker\phi\}$

É fácil ver que ψ é sobrejetora.

Logo, ψ é um isomorfismo, como queríamos provar.

□

Exemplo 3.3.2: $\frac{\mathbb{R}[x]}{<x^2+1>}$ é isomorfo a $\mathbb{C}$.

De fato, utilizando o TFH basta criar um homomorfismo ϕ sobre $\mathbb{R}[x]$ e $\mathbb{C}$ tal que $ker\phi$ seja igual a $< x^2 + 1 >$.

Defina

$$\begin{aligned}\phi : \mathbb{R}[x] &\to \mathbb{C}\\ f(x) &\longmapsto f(i)\end{aligned}$$

É fácil ver que ϕ é um homomorfismo sobrejetor e que $< x^2 + 1 > \subset ker\phi$.

Seja agora $f(x) \in ker\phi$. Dividindo $f(x)$ por x^2+1 temos que existem $q(x) \in \mathbb{R}[x]$ e a,$b \in \mathbb{R}$ tais que $f(x) = (x^2+1)q(x) + ax + b$. Queremos provar que a e b são nulos. Como $f(x) \in ker\phi$, aplicando ϕ na expressão acima temos que $ai + b = 0$. Logo $a = b = 0$ e $f(x) \in < x^2 + 1 >$. Assim, $ker\phi =< x^2 + 1 >$ e pelo TFH, $\mathbb{C} \cong \frac{\mathbb{R}[x]}{<x^2+1>}$.

Exemplo 3.3.3: Voltando ao exemplo 3.3.1, vamos calcular o núcleo de ϕ:

- $ker\phi = \left\{x \in \mathbb{Z} | \phi(x) = \overline{0}\right\}$

  $ker\phi = \left\{x \in \mathbb{Z} | \overline{x} = \overline{0}\right\}$

  $ker\phi = \{x \in \mathbb{Z} | x = 4k\}$

  $ker\phi = 4\mathbb{Z}$

- ϕ é sobrejetiva

  Se $\overline{y} \in \mathbb{Z}_4$, $\phi(y) = \overline{y}$, com $y \in \mathbb{Z}$.

  Pelo teorema anterior, $\frac{\mathbb{Z}}{4\mathbb{Z}} \cong \mathbb{Z}_4$.

3.4 Divisibilidade em Domínios

Em $\mathbb{Z}$ temos um teorema muito importante, dito "Teorema Fundamental da Aritmética", que diz que todo número inteiro maior que 1 pode ser decomposto num produto de números primos. Nesta seção iremos examinar a fatoração num contexto geral.

3.4.1 Irredutíveis e primos

Em todo domínio D podemos definir múltiplos e divisores de D. Se $a = bc$ podemos dizer que:

- b é dito divisor de a
- a é dito múltiplo de b.

Além das definições acima, temos

- Dois elementos a e b são ditos *associados* se $a = ub$, onde u é uma unidade de D.
- Um elemento não nulo a de D é chamado *irredutível* se a não for uma unidade e sempre quando $a = bc$ com b e c em D então b ou c é uma unidade.
- Um elemento a não nulo de um domínio D é chamado *primo* se a não for uma unidade, e se $a|bc$ então $a|b$ ou $a|c$.

Grosseiramente falando, irredutível é um elemento que pode ser fatorado apenas com a fatoração trivial.

Observe que um elemento a é primo se, e somente se $< a >$ é um ideal primo[3].

A distinção entre primos e irredutíveis é melhor ilustrada nos domínios da forma

$$\mathbb{Z}\left[\sqrt{d}\right] = \left\{a + b\sqrt{d} \mid a,b \in \mathbb{Z}\right\} \text{ onde } d \text{ é livre de quadrados.}$$

Estes anéis são de fundamental importância na teoria dos números.

Antes, vamos mostrar que $\mathbb{Z}\left[\sqrt{d}\right]$ é um domínio. De fato, $\mathbb{Z}\left[\sqrt{d}\right]$ é comutativo com unidade ($1 \in \mathbb{Z}$). Além disso, se $(a + b\sqrt{d}) \cdot (c + e\sqrt{d}) = 0$, temos

$$(ac + ebd) + (ae + bc)\sqrt{d} = 0 \Rightarrow ac + ebd = 0 \quad \text{e} \quad ae + bc = 0$$

Supondo $(c + e\sqrt{d}) \neq 0$, temos $c \neq 0$ ou $e \neq 0$. Assim, $ae + bc = 0 \Rightarrow a = -\frac{bc}{e}$, se $e \neq 0$ e, de $ac + ebd = 0$ temos

$$\left(\frac{-bc}{e}\right) c + ebd = 0$$

$-bc^2 + e^2bd = 0 \Rightarrow b(-c^2 + e^2d) = 0 \Rightarrow b = 0$ *oû* $-c^2 + e^2d = 0 \Rightarrow c^2 = e^2d \Rightarrow c = e\sqrt{d}$,

mas $\sqrt{d} \notin \mathbb{Z}$, logo essa solução não é possível. Portanto, $b = 0$ e, $a = \frac{bc}{e} \Rightarrow a = 0$.

Assim, $a + b\sqrt{d} = 0$. Mas se $e = 0$, temos $ae + bc = 0$ e $bc = 0$, o que nos dá $b = 0$ (pois c deve ser não nulo).

De $ac + ebd = 0$, teremos

$$ac = 0 \Rightarrow a = 0$$

. De toda forma, $a + b\sqrt{d} = 0$ e $\mathbb{Z}\left[\sqrt{d}\right]$ é domínio.

[3]Um ideal $P \neq A$ do anel A chama-se primo se, para quaisquer $a,b \in P$, $ab \in P$ implica $a \in P$ ou $b \in P$.

Para analisar esses anéis, nós necessitamos de um método conveniente para encontrar suas unidades, irredutíveis e primos. Para fazer isso, definiremos função norma:

Definição 3.17 (Função norma):

$$N : \mathbb{Z}\left[\sqrt{d}\right] \to \mathbb{Z}^+$$
$$a + b\sqrt{d} \longmapsto \left|a^2 - db^2\right|$$

É fácil verificar as propriedades da função norma:

1. $N(x) = 0$ se e somente se $x = 0$
2. $N(xy) = N(x)N(y)$ para toodo x,$y \in \mathbb{Z}\left[\sqrt{d}\right]$
3. x é unidade se e somente se $N(x) = 1$
4. Se $N(x)$ é primo, então x é irredutível.

Exemplo 3.4.1: Vamos mostrar que em $\mathbb{Z}\left[\sqrt{-3}\right]$ um irredutível não é primo.

Temos aqui que $N(a + b\sqrt{-3}) = a^2 + 3b^2$. Considere $1 + \sqrt{-3}$. Suponha que podemos fatorar $1+\sqrt{-3}$ como um produto $x \cdot y$ onde x e y não são unidades. Então $N(xy) = N(x)N(y) = N(1 + \sqrt{-3}) = 4$, e segue que $N(x) = 2$. Mas não existem inteiros a e b satisfazendo $a^2+3b^2 = 2$. Assim x ou y é unidade e $1+\sqrt{-3}$ é irredutível. Para provar que $1+\sqrt{-3}$ não é primo, observamos que $(1+\sqrt{-3})(1-\sqrt{-3}) = 4 = 2\cdot 2$, o que mostra que $(1 + \sqrt{-3}) \mid 2 \cdot 2$. Por outro lado, para existirem inteiros a e b tal que $2 = (a + b\sqrt{-3})(1 + \sqrt{-3}) = (a - 3b) + (a + b)\sqrt{-3}$ nós devemos ter $a - 3b = 2$ e $a + b = 0$ o que é impossível.

Do exemplo anterior, surge a pergunta: Quais domínios possuem primos que não são irredutíveis?
A resposta é: Não existem!

Teorema 3.10: Num domínio, todo primo é irredutível.

Demonstração. Suponha que a é um primo em um domínio D. Então $a \neq 0$ e a não é uma unidade e se $a = b \cdot c$ nós devemos provar que b ou c é uma unidade. Pela definição de primo, nós temos que $a|b$ ou $a|c$.
Suponha que $at = b$ e substituindo, temos $b \cdot 1 = b = at = (bc)t = (bc)t$ e pelo cancelamento, $ct = 1$, o que mostra que c é uma unidade.

□

E ao contrário?

Em $\mathbb{Z}$ todo irredutível é também primo. O teorema abaixo nos diz quando isso ocorre. Ou seja, se D é um DIP, temos a equivalência.

Teorema 3.11: Num DIP, um elemento é irredutível se e somente se ele é primo.

Demonstração. Usando o teorema anterior, só falta provar que num DIP, todo irrred. é primo. Seja a um elemento irredutível num DIP e suponha que $a|bc$. Devemos mostrar que $a|b$ ou $a|c$. Considere o ideal $I = \{ax + by \mid x,y \in D\}$ e como D é um DIP, existe $d \in D$ tal que $I =< d >$. Como $a \in I$, podemos escrever $a = dr$ para algum r em D, e como a é ired., d ou r é uma unidade. Se d for uma unidade $I =< d >= D$ e nós podemos escrever $1 = ax + by$. Então $c = acx + bcy$ e como a divide ambos os termos, temos que $a|c$. Por outro lado, se r é uma unidade, então $< a >=< d >= I$, e como $b \in I$, existe um $t \in D$ tal que $at = b$. Assim $a|b$. □

Uma consequência fácil do algorítmo da Divisão em $\mathbb{Z}$ e $F[x]$ onde F é um corpo, é que eles são DIP. Nosso próximo exemplo mostra entretanto, que um dos nossos anéis mais familiares não é um DIP.

Exemplo 3.4.2: Mostraremos que $\mathbb{Z}[x]$ não é um DIP.

Considere em $\mathbb{Z}[x]$ o ideal $I = \{ax + 2b \mid a,b \in \mathbb{Z}\} =< x,2 >$. Nós afirmamos que I não é da forma $< h(x) >$. Com efeito, se fosse, deveriam existir $f,g \in \mathbb{Z}[x]$ tal que $2 = hf$ e $x = hg$, pois x e 2 estão em I.

Pela regra do grau, temos $0 = gr2 = grh + grf$ e concluímos que h é constante, observamos que $2 = h(1)f(1)$. Assim, $h(1) = \pm 1$ ou ± 2, mas como $1 \notin I$ nós devemos ter $h(x) = \pm 2$. Mas então $x = \pm 2g(x)$, o que não faz sentido.

3.4.2 Domínios de Fatoração Única (DFU)

Vamos estudar sobre a existência de fatoração única em domínios. Sabemos que em $\mathbb{Z}$ todo número maior que 1 pode ser escrito como produto de primos; podemos estender esse resultado para $\mathbb{Z}[x]$.

Teorema 3.12: Todo polinômio em $\mathbb{Z}[x]$ de grau positivo, não nulo e não unidade pode ser escrito na forma

$$b_1 b_2 \cdots b_s p_1(x) p_2(x) \cdots p_m(x)$$

onde os $b's$ são primos (isto é, polinômios irred. de grau 0), e os $p(x)'s$ são pol. irred. de grau positivo.
Também, se

$$b_1 b_2 \cdots b_s p_1(x) \cdots p_m(x) = c_1 c_2 \cdots c_t q_1(x) \cdots q_n(x)$$

são duas tais fatorações, então $s = t$ e $m = n$ e, após renumeração dos $c's$ e $q's$ nós temos $b_i = \pm c_i$, para $i = 1, \cdots s$, e $p_i(x) = \pm q_i(x)$, para $i = 1, \cdots, m$.

Demonstração. Existência: Seja f não nulo e não unidade em $\mathbb{Z}[x]$. Se $grf = 0, f \in \mathbb{Z}$ e o resultado segue do TFA (3.3). Se $grf > 0$, seja b, o conteúdo de f e $b_1 b_2 \cdots b_s$ sua fatoração em $\mathbb{Z}$. Então $f = b_1 \cdots b_s f_1(x)$, onde $f_1 \in \mathbb{Z}[x]$ é primitivo e tem grau positivo. Assim, para provar a parte da existência, é suficiente mostrar que todo polinômio primitivo de grau maior que 1 pode ser escrito como um produto de polinômios irredutíveis de grau positivo.

Usaremos indução no grau de f.

Se $grf = 1$ então já é irredutível e então OK.

Agora suponha que todo polinômio de grau menor que grf e primitivo pode ser escrito como um produto de polinômio irredutível de grau positivo. Se f é irredutível, nada a demonstrar.

Se f não for irredutível $f = gh$ onde g e h são primitivos e $grf, grh < grf$. Pela hipótese de indução, ambos g e h são produtos de irredutíveis de grau positivo, o que mostra que fe também será.

Unicidade: Suponha que

$f = b_1 b_2 \cdots b_s p_1(x) p_2(x) \cdots p_m(x) = c_1 c_2 \cdots c_t q_1(x) \cdots q_n(x)$

onde os $b's$ e $c's$ são polinômios irredutíveis de grau zero e os $p(x)'s$ e $q(x)'s$ são polinômios irredutíveis de grau positivo.

Sejam $b - b_1 \cdots b_s$ $c = c_1 \cdots c_t$ .Como os polinômios $p's$ e $q's$ são primitivos segue do Lema de Gauss(3.2) que $p_1 p_2 \cdots p_m$ e $q_1 q_2 \cdots q_n$ são primitivos. Portanto, tomando o conteúdo de f temos $b = c$.

Pelo TFA (3.3) e após renumeração $b_i = c_i$ onde $i = 1,2,\cdots,s$. Assim, cancelando o conteúdo temos $p_1(x)p_m(x) = q_1(x) \cdots q_n(x)$. Segue pelo corolário 6.2.10 (ver em (10)) e considerando os $p's$ e $q's$ como elementos de $\mathbb{Z}[x]$, que $p_1 \mid qq_j$ para algum $j \in \{1,2 \cdots ,n\}$. Renumerando, podemos supor $j = 1$. Assim $q_1 = p_1 \cdot \frac{r}{s}$ com $r,s \in \mathbb{Z}$. Como p_1 e q_1 são primitivos segue que $r = s$ e $p_1 \pm q_1$.

Após o cancelamento, $p_2(x) \cdots p_m(x) = \pm q_2(x) \cdots q_n(x)$ e repetindo o argumento com $p_2(x)$ teremos $p_2 = \pm q_2$.

Sim $m < n$, após tais passos teremos que $\pm 1 = q_{m+1} \cdots q_n$. Isso diz que os polinômios $q_i's$ com $i = m + 1, \cdots, n$ são unidades, o que é um absurdo pois eles são irredutíveis. Analogamente se $m > n$ chegaremos num tal absurdo.Assim, $m = n$ e $p_i = q_i$ após renumeração. □

A questão de fatoração única em domínios surgiu na tentativa de resolver o Último Teorema de Fermat.

Estudaremos agora domínios que possuem fatoração única em irredutíveis.

Definição 3.18: Um domínio D é domínio de fatoração única (DFU) se:

1. Todo elemento de D não nulo e não unidade, pode ser escrito como produto de irredutíveis em D.

2. A fatoração em irredutíveis é única a menos de associados e da ordem em que aparecem.

Naturalmente o Teorema Fundamental da Aritmética (3.3) nos diz que $\mathbb{Z}$ é DFU. O teorema 3.12 diz que $\mathbb{Z}[x]$ é DFU. Provaremos que muitos dos domínios que conhecemos são DFU. Provaremos antes a condição de **cadeia ascendente**.

Teorema 3.13: Num DIP toda cadeia ascendente de ideais $I_1 \subset I_2 \subset \cdots$ é estacionária (isto é, existe um k tal que $I_k = I_{k+1} = \cdots$).

Demonstração. Seja $I_1 \subset I_2 \subset \cdots$ uma cadeia ascendente de ideais num domínio D e seja $I = \bigcup I_i$. É fácil mostrar que I é um ideal em D. Como D é um DIP, $I =< a >$ para algum $a \in D$. Como $a \in I$, $a \in I_k$ para algum inteiro k e asssim $I =< a > \subset I_k$. Mas pela definição de I, temos que $I_i \subset I \subset I_k$ para todo I_i da cadeia e assim I_k deve ser o último ideal da cadeia. □

Teorema 3.14: Todo DIP é um DFU.

Demonstração. Existência: Seja d um DIP. Primeiro mostraremos que todo $a \in D, a \neq 0$ e a não unidade é um produto de irredutíveis (observe que o produto pode constar de apenas um fator). Para ver isso, seja $a_0 \neq 0$ não unidade e não irredutível. Então existem a_1 e b_1 não unidades em D tais que $a_0 = b_1 a_1$.

Se ambos a_1 e b_1 podem ser escritos como produto de irredutíveis então a_0 também pode. Suponha que a_0 não pode ser escrito como produto de irredutíveis. Assim,b_1 ou b_2 não pode ser escrito como produto de irredutíveis, digamos a_1. Então $a_1 = a_2 b_2$ onde nem a_2 nem b_2 é unidade. Continuando neste processo, obtemos uma sequência infinita b_1,$b_2, \cdots$ de elementos que não são unidades de D, e uma sequência $a_0, a_1, \cdots$ de elementos não nulos de D, com $a_n = b_{n+1} a_{n+1}$ para cada n. Como b_{n+1} não é unidade nós temos

$$< a_n > \subset < a_{n+1} > \text{ para cada } n$$

Assim $< a_0 > \subset < a_1> \subset \cdots$ é uma cadeia infinita crescente de ideais. Isto contraria o teorema anterior. Desse modo que concluímos que a_0 é um produto de irredutíveis (observe que a cadeia não pára pois senão $< a_n >=< a_{n+1} >, a_{n+1} = da_n, a_n = b_{n+1} a_{n+1}$. Juntando essas equações temos que b_{n+1} é uma unidade, o que é um absurdo.)

Unicidade: Temos que mostrar que a fatoração é única a menos de associados e a ordem em que os fatores aparecem. Para fazer isto, suponha que um elemento $a \in D$ pode ser escrito como:

$$a = p_1 p_2 \cdot p_r = q_1 q_2 \cdots q_s$$

onde os p e q são irredutíveis e a repetição é permitida. Faremos indução em r.

Se $r = 1$, então a é irredutível e claramente $s = 1$ e $p_1 = q_1$

Nós assumimos que todo elemento o qual pode ser expresso como um produto de $r - 1$ elementos irredutíveis é escrito de modo único (a menos de associados e ordem). Vamos agora provar que é isso também vale para um produto de r irredutível. Como $p_1 | (q_1 q_2 \cdots q_s)$ ele divide algum q_i. Então $q_1 = u p_1$ onde u é 1 unidade de D. Assim,

$$ua = u p_1 p_2 \cdots p_r = q_1 (u q_2) \cdots q_s,$$

e por cancelamento,

$$p_2 p_3 \cdots p_r = (u q_2) \cdots q_s.$$

Pela hipótese de indução, estas duas fatorações são idênticas a menos de associados e a ordem em que aparecem. Assim, o mesmo é verdade para as duas fatorações de a. □

Observação:
Na parte da existência é que usamos que D é um DIP quando afirmamos que a cadeia tem que parar. Um domínio com esta propriedade é chamado de *domínio Noetheriano* em homenagem a Emmy Noether, que introduziu as condições de cadeia.

Corolário 3.2: Se F é um corpo, então $F[x]$ é um DFU.

Demonstração. Pelo teorema sabemos que $F[x]$ é um domínio. Seja agora I um ideal de $F[x]$. Se $I = 0$, nada a demonstrar. Suponha então que $I \neq 0$ e seja g o polinômio de menor grau que pertence a I.
Vamos provar que $I =< g >$. Como $g \in I, gF[x] \subset I$ e então $< g > \subset I$. Tome $h \in I$. Pelo algoritmo da divisão temos que existem q e r em $F[x]$ tais que $h = qg + r$ com $r = 0$ ou grr $<$ grg. Temos que $r = h - qg \in I$ e então pela escolha de g,r só pode ser 0. Logo $g|h$ o que prova que $I \subset < g >$ e portanto $I =< g >$. Logo F é um DIP, e como por (3.14) todo DIP é um DFU, concluímos que F é DFU. □

3.4.3 Domínios Euclidianos (DE)

Nesta seção trabalharemos com um domínio muito importante para o estudo de divisibilidade em domínios, os Domínios Euclidianos (DE). Além disso, veremos que todo DE é um Domínio Principal, mas não o contrário, e que, em Domínios Euclidianos, podemos estabelecer um algorítimo de divisão.

Definição 3.19: Um domínio D é chamado *Domínio Euclidiano(DE)* se existe uma função d de elementos não nulos de D em $\mathbb{Z}^+$ tal que:

1. $d(a) \leq d(ab)$ para todo a,$b \in D - \{0\}$
2. Se a,$b \in D, b \neq 0$, então existem q,$r \in D$ de modo que $a = bq + r$ onde $r = 0$ ou $d(r) < d(b)$.

Exemplo 3.4.3: Inteiros com a função $d(x) = |x|$, e o algoritmo da divisão de Euclides.

Teorema 3.15 (DE $\Rightarrow$ DIP): Todo Domínio Euclidiano é um Domínio de Ideais Principais.

Demonstração. Seja D um DE e I um ideal não nulo de D. Entre os elementos de I escolha a tal que $d(a)$ é mínimo. Então $I =< a >$. Com efeito, se $b \in I, \exists\, q$,$r \in D$ tais que $b = aq + r$ onde $r = 0$ ou $d(r) < d(a)$. Mas $r = b - aq \in I$ e portanto $d(r)$ não pode ser menor que $d(a)$. Assim $r = 0$ e $b \in < a >$. □

Uma imediata consequência dos teoremas anteriores é o seguinte:

Corolário 3.3 (DE ⇒ DFU): Todo Domínio Euclidiano é um DFU.

Demonstração. Pelo teorema (3.15) temos que todo DE é um DIP, e por (3.14) temos que todo DIP é um DFU. Logo, por transitividade, o teorema está demonstrado. □

Note que temos então DE ⇒ DIP ⇒ DFU.

3.5 O anel $\mathbb{Z}[\omega]$

Um grande exemplo de Domínio Euclidiano é o domínio $\mathbb{Z}[\omega]$ que apresentaremos nesta seção.

Primeiramente, vamos definir nosso elemento ω e, para isso, devemos relembrar alguns conceitos dos números complexos.

Seja $z \in \mathbb{C}$, então $z = a + bi$, com a,$b \in \mathbb{Z}$. Para extrairmos a raiz n-ésima de $z = a+bi \in \mathbb{C}$, precisamos da fórmula de Moivre que por sua vez, necessita da escrita de z em sua forma trigonométrica. Assim, para $z = a + bi$ e $||z|| = \sqrt{a^2 + b^2}$, temos que $z = ||z||(cos\theta + isen\theta)$.

Se $z = 1$, então $z = 1+0i$ e $||z|| = \sqrt{1^2 + 0^2} = 1$. Logo, $z = 1 = 1 \cdot (cos\theta + isen\theta)$, e como $z = 1$ implica em $\theta = 0$, temos que $z = 1 = (\cos 0 + isen0)$.

Como queremos calcular $\sqrt[3]{1}$ e sabemos que em $\mathbb{C}$ possui soluções; pela fórmula de Moivre para cálculo de raízes complexas

$$\sqrt[n]{z} = z_k = \sqrt[n]{||z||} \cdot \left[cos\left(\frac{\theta + 2k\pi}{n}\right) + isen\left(\frac{\theta + 2k\pi}{n}\right)\right]; k \in \{0,1,\cdots,n-1\}$$

como $z = 1$, para calcularmos $\sqrt[3]{z}$, basta utilizarmos a fórmula acima, e teremos para $z = 1, n = 3$ e $k = 0,1,2$ que

$$\sqrt[3]{1} = 1 \cdot cos\left(\frac{2k\pi}{3}\right) + isen\left(\frac{2k\pi}{3}\right)$$

- $k = 0 \Rightarrow cos0 + isen0 = 1$
- $k = 1 \Rightarrow cos\left(\frac{2\pi}{3}\right) + isen\left(\frac{2\pi}{3}\right) = -\frac{1}{2} + i\frac{\sqrt{3}}{2} = \omega$
- $k = 2 \Rightarrow cos\left(\frac{4\pi}{3}\right) + isen\left(\frac{4\pi}{3}\right) = -\frac{1}{2} - i\frac{\sqrt{3}}{2} = \omega^2$

Consideremos $\omega \in \mathbb{C}$ a raiz cúbica da unidade $\omega = -\frac{1}{2} + \frac{\sqrt{3}}{2}i$. Dessa maneira, ω é a raiz do polinômio

$$x^3 - 1 = 0$$

Fatorando-o temos $(x-1)(x^2 + x + 1) = 0$ que possui três raízes: 1, ω e ω^2.

Note que ω e ω^2 são raízes de $f(x) = x^2 + x + 1$. Assim,

$$\omega^2 + \omega + 1 = 0 \tag{3.3}$$

A partir de ω vamos definir um anel dito $\mathbb{Z}[\omega]$ (lido $\mathbb{Z}$ de ômega), mas para isso precisamos introduzir o conceito de adjunção de um elemento em um anel.

Definição 3.20 (Adjunção de um anel qualquer): Seja A um anel e α um elemento de um anel B que contém A. Considere o conjunto $A[\alpha] = \{f(\alpha) \mid f(x) \in A[x]\}$. Lembremos que $A[\alpha]$ é o anel de polinômios na variável x e coeficientes em A. De fato, $A[\alpha]$ é um anel, e se $a(\alpha)$,$b(\alpha) \in A[x]$, temos

$a(\alpha) = a_0 + a_1\alpha + \cdots + a_m\alpha^m$

$b(\alpha) = b_0 + b_1\alpha + \cdots + b_n\alpha^n$

Com isso,

- A soma em $A[\alpha]$ é definida como:

  $a(\alpha) + b(\alpha) = (a_0 + b_0) + (a_1 + b_1) + \cdots (a_m + b_m)\alpha^m + b_{m+1}\alpha^{m+1} + \cdots + b_n\alpha^n$

  aqui consideramos $n > m$.

- O produto em $A[\alpha]$ é definido como:

  $a(\alpha) \cdot b(\alpha) = a_0b_0 + (a_0b_1 + a_1b_0)\alpha + (a_0b_2 + a_1b_1 + a_2b_0)\alpha^2 + \cdots + a_mb_n\alpha^{m+n}$.

Para maiores informações sobre o anel de polinômio $A[\alpha]$, veja [8].

O anel $A[\alpha]$ é chamado anel A adjunção α.

Se $A = \mathbb{Z}$ e $\alpha = \omega$, então $\mathbb{Z}[\omega] = \{f(\omega)|f(x) \in \mathbb{Z}))\}$. Como visto acima, ω é raiz do polinômio $p(x) = x^2 + x + 1$, portanto para todo $f(x) \in \mathbb{Z}[x]$ podemos aplicar o algorítmo da divisão (veja [8] para mais detalhes) e teremos $f(x) = p(x)q(x) + r(x)$.

Temos duas possibilidades para $r(x)$: ou ele é identificamente nulo, ou seu grau é menor que o de f. Se f for múltiplo de $p(x)$, temos que $r(x) = 0$. Se não, como o grau de f é dois, o grau de r pode ser no máximo 1. Logo, $r = ax + b$.

Os elementos de $\mathbb{Z}[\omega]$ são os $f(\omega)$, então $f(\omega) = p(\omega)q(\omega) + r(\omega)$. Mas $p(\omega) = 0$, logo $f(\omega) = r(\omega) = a\omega + b$.

Por esse motivo, $\mathbb{Z}[\omega] = \{a + b\omega \mid a,b \in \mathbb{Z} \quad e \quad \omega^2 + \omega + 1 = 0\}$ (Existe toda uma teoria por trás dessa questão de adjunção, aqui, demos apenas uma ideia para mostrar como se chega ao anel em questão. O leitor mais curioso pode verificar em [8]).

Com isso, definimos o anel $\mathbb{Z}[\omega]$:

$$\mathbb{Z}[\omega] \stackrel{def}{=} \{a + b\omega \in \mathbb{C} \mid a,b \in \mathbb{Z}\}.$$

Como $\mathbb{Z}[\omega] \subset \mathbb{C}$ é um subanel de $\mathbb{C}$, temos que a soma e a multiplicação em $\mathbb{Z}[\omega]$ se faz como em $\mathbb{C}$:

Dados $\alpha = a + b\omega$ e $\beta = c + d\omega$ em $\mathbb{Z}[\omega]$, a soma desses elementos é da forma:

$$(a + b\omega) + (c + d\omega) = (a + c) + (b + d)\omega$$

e o produto é

$$\begin{aligned}(a+b\omega)(c+d\omega) &= ac+(ad+bc)\omega+bd\omega^2\\ &= ac+(ad+bc)\omega+bd(\omega^2+\omega+1)-bd\omega-bd\\ &= (ac-bd)+(ad+bc-bd)\omega\end{aligned}$$

onde, para eliminar o termo quadrático, somamos e subtraímos o termo $bd(\omega+1)$ e usamos que ω satisfaz a igualdade (3.3).

Esse anel é um domínio pois é um subanel do corpo $\mathbb{C}$.

Vamos estudar mais este domínio.

Definição 3.21: Em $\mathbb{Z}[\omega]$ definimos a função:

$$\begin{aligned}N : \mathbb{Z}[\omega]-\{0\} &\to \mathbb{Z}^+\\ a+b\omega &\mapsto a^2-ab+b^2\end{aligned}$$

a qual chamaremos de função **norma**.

Proposição 3.4: Em $\mathbb{Z}[\omega]$,

1. Se $a+b\omega \in \mathbb{Z}[\omega]$ é escrito na forma $u+iv \in \mathbb{C}$ então $N(a+b\omega)=u^2+v^2$. Com isso, concluímos que N está bem definida.

2. $\forall\ \alpha,\beta \in \mathbb{Z}[\omega]$ temos $N(\alpha\beta)=N(\alpha)N(\beta)$ Temos também que, se $\alpha|\beta$ então $N(\alpha)|N(\beta)$ em $\mathbb{Z}$.

3. O conjunto das unidades (elementos inversíveis) de $\mathbb{Z}[\omega]$ é

$$U(\mathbb{Z}[\omega]) = \{\alpha \in \mathbb{Z}[\omega] \mid N(\alpha)=1\} = \{1,-1,\omega,-\omega,1+\omega,-1-\omega\}.$$

4. O corpo quociente de $\mathbb{Z}[\omega]$ é $\mathbb{Q}[\omega]$.

Demonstração. 1. O elemento $a+b\omega$ de $\mathbb{Z}[\omega]$ pode ser escrito como

$$a+b\left(\frac{-1+i\sqrt{3}}{2}\right) = a-\frac{-b}{2}+\frac{\sqrt{3b}}{2}i$$

Como número complexo, a norma ao quadrado desse elemento é

$$\left|a-\frac{-b}{2}+\frac{\sqrt{3b}}{2}i\right|^2 = \left(a-\frac{b}{2}\right)^2+\left(\frac{\sqrt{3b}}{2}\right)^2 = a^2-ab+\frac{b^2}{4}+\frac{3b^2}{4} = a^2-ab+b^2 = N(a+b\omega)$$

Portanto vemos que a função N está bem definida em $\mathbb{Z}[\omega]$.

2. Dados $\alpha = a + b\omega$ e $\beta = c + d\omega$, temos que $\alpha\beta = (ac - bd) + (ad + bc - bd)\omega$ e portanto,

$$\begin{aligned} N(\alpha\beta) &= (ac - bd)^2 - (ac - bd)(ad + bc - bd) + (ad + bc - bd)^2 \\ &= a^2c^2 - a^2cd + a^2d^2 - abc^2 + abcd - abd^2 + b^2c^2 - b^2cd + b^2d^2 \\ &= (a^2 - ab + b^2)(c^2 - cd + d^2) \\ &= N(\alpha)N(\beta) \end{aligned}$$

   Se $\alpha|\beta$, $\exists\ \kappa \in \mathbb{Z}[\omega]$ tal que $\beta = \kappa\alpha$. Aplicando a função N temos $N(\beta) = N(\kappa)N(\alpha)$ de onde concluímos que $N(\alpha)|N(\beta)$ em $\mathbb{Z}$.

3. Suponha que v seja uma unidade de $\mathbb{Z}[\omega]$. Então existe v^{-1} tal que $uv^{-1} = 1$ Aplicando a função N temos $N(u)N(v^{-1}) = N(1) = 1$. Mas $\mathbb{Z}^+$, a única fatoração de 1 é $1 = 1 \cdot 1$.Portanto, $N(u) = N(v^{-1}) = 1$

   Vamos agora obter os elementos que possuem norma 1, isto é, os elementos $a + b\omega$ que satisfazem a equação $a^2 - ab + b^2 = 1$. Para isso, considere o polinômio $p(a) = a^2 - ab + b^2 - 1 \in \mathbb{Z}[a]$. Esse polinômio tem raízes se, e só se, o discriminante ν é não negativo, ou seja, se $b^2 - 4(b^2 - 1) \geq 0$.
   Resolvendo essa inequação em $\mathbb{R}$ obtemos $|b| \leq \frac{2}{\sqrt{3}}$ implicando que os possíveis valores inteiros de b são -1, 0 e 1. Vamos analisar cada caso.

   - $b = -1$: Então $p(a) = a^2 + a$ e suas raízes são $a = 0$ e $a = -1$
   - $b = 0$: Então $p(a) = a^2 - 1$ e suas raízes são $a = 1$ e $a = -1$
   - $b = 1$: Então $p(a) = a^2 - a$ e suas raízes são $a = 0$ e $a = 1$

   Portanto, o conjunto dos elementos de $\in \mathbb{Z}[\omega]$ com norma 1 é $\{1, -1, \omega, -\omega, 1 + \omega, -1 - \omega\}$. Podemos facilmente verificar que $1 \cdot 1 = (-1) \cdot (-1) = \omega \cdot (-1 - \omega) = (-\omega) \cdot (1 + \omega) = 1$. Logo, um elemento de $\in \mathbb{Z}[\omega]$ é unidade, se, e só se, sua norma é igual a 1.

4. Antes vamos definir o elemento "conjugado" em $\mathbb{Z}[\omega]$. Dado um elemento $\alpha = a + b\omega \in \mathbb{Z}[\omega]$, queremos encontrar $\overline{\alpha} \in \mathbb{Z}[\omega]$ tal que $\alpha \cdot \overline{\alpha} = N(\alpha)$. Para obter esse elemento basta resolver o seguinte sistema nas variáveis x e y:

$$(a + b\omega)(x + y\omega) = a^2 - ab + b^2.$$

   Assim, temos que para qualquer $\alpha \in \mathbb{Z}[\omega]$, $\overline{\alpha} = (a - b) - b\omega$. Podemos verificar que esses elementos, quando escritos na forma $u + iv$, são realmente conjugados em $\mathbb{C}$.

   Agora vamos à demonstração da propriedade 4:

   O corpo quociente de $\mathbb{Z}[\omega]$ denotado por $\mathbb{Z}(\omega)$, e o corpo $\mathbb{Q}[\omega]$ são descritos por:

$$\mathbb{Z}(\omega) = \left\{ \frac{a + b\omega}{c + d\omega} \mid a,b,c,d \in \mathbb{Z} \text{ e } c^2 + d^2 \neq 0 \right\}$$

   e

$$\mathbb{Q}[\omega] = \left\{ \frac{a}{c} + \frac{b}{d}\omega \mid a,b,c,d \in \mathbb{Z} \text{ e } c^2 + d^2 \neq 0 \right\}$$

Considere um elemento de $\mathbb{Z}(\omega)$, digamos $\frac{a+b\omega}{c+d\omega}$. Multiplicando numerador e denominador pelo conjugado do denominador temos

$$\begin{aligned}\frac{(a+b\omega)(c-d-d\omega)}{(c+d\omega)(c-d-d\omega)} &= \frac{(ac-ad-bd)+(bc-ad)\omega}{c^2-cd+d^2} \\ &= \frac{ac-ad-bd}{c^2-cd+d^2}+\frac{bc-ad}{c^2-cd+d^2}\omega \in \mathbb{Q}[\omega]\end{aligned}$$

Por outro lado, dado um elemento $\frac{a}{c}+\frac{b}{d}\omega$ de $\mathbb{Q}[\omega]$, podemos escrever

$$\frac{a}{c}+\frac{b}{d}\omega = \frac{ad}{cd}+\frac{cb}{cd}\omega = \frac{ad+cb\omega}{cd} \in \mathbb{Z}(\omega).$$

Desse modo concluímos que $\mathbb{Q}[\omega]$ é um corpo quociente de $\mathbb{Z}[\omega]$.

□

Proposição 3.5: O anel $\mathbb{Z}[\omega]$ com a função N é um domínio Euclidiano (DE).

Demonstração. Vamos verificar as duas propriedades de um (DE):

- $N(\alpha\beta) \geq N(\alpha)$:
  Pela proposição 3.4, item 2 temos $N(\alpha\beta) = N(\alpha)\cdot N(\beta)$. Como a imagem da função N é o conjunto dos inteiros positivos, concluímos que $N(\alpha\beta) \geq N(\alpha)$ e $N(\alpha\beta) \geq N(\beta)$.
- Algoritmo da divisão de Euclides:
  Se x,$y \in \mathbb{Z}[\omega]$ com $y \neq 0$, pelo item 4 da proposição 3.4, $xy^{-1} \in \mathbb{Q}[\omega]$. Assim, temos que $xy^{-1} = s+t\omega$, onde s,$t \in \mathbb{Q}[\omega]$.Vamos considerar inteiros m e n tais que $|m-s| \leq \frac{1}{2}$ e $|n-t| \leq \frac{1}{2}$, ou seja, m e n são os inteiros mais próximos dos racionais s e t. Então,

$$\begin{aligned}xy^{-1} = s+t\omega &= (m-n+s)+(n-n+t)\omega \\ &= (m+n\omega)+[(s-m)+(t-n)\omega].\end{aligned}$$

  Portanto,

$$x = (m+n\omega)y+[(s-m)+(t-n)\omega]y.$$

  Afirmamos que $q = (m+n\omega)$ e $r = [(s-m)+(t-n)\omega]$ satisfazem o algorítmo da divisão.

  De fato, $q \in \mathbb{Z}[\omega]$ e, como podemos escrever $r = x-qy$, o mesmo acontece para r.
  Além disso,

$$\begin{aligned}N(r) &= N([(s-m)+(t-n)\omega])N(y) \\ &= [(s-m)^2-(s-m)(t-n)+(t-n)^2]N(y) \leq \\ &\leq \frac{1}{4}N(y) < N(y).\end{aligned}$$

Feito isso, concluímos que $\mathbb{Z}[\omega]$ é de fato um domínio Euclidiano.

□

Corolário 3.4: O anel $\mathbb{Z}[\omega]$ é um DIP, e todo DIP é um DFU.

Demonstração. De fato, todo DE é um DIP e todo DIP é um DFU. □

O anel $\mathbb{Z}[\omega]$ aqui estudado será essencial para a demonstração do Último teorema de Fermat, caso n=3. O que veremos no próximo capítulo.

4

Demonstrações para os casos n = 3 e n = 4

Neste capítulo demonstraremos o Último Teorema de Fermat para os casos n=3 e n=4. Iniciaremos com o que julgamos mais simples.

4.1 Fermat e a demonstração para o caso $n = 4$

Muito do que Fermat observou e conjecturou, não foi demonstrado por ele, como o ocorrido com o Último Teorema de Fermat. Para o caso $n = 4$, o próprio deixou a prova utilizando o descenso infinito. Esse método e a prova, serão descritos a seguir com base no livro [11].

4.1.1 Descenso Infinito de Fermat

Dada uma equação

$$f(x_1,x_2,\cdots,x_n) = 0,$$

o método do descenso infinito (quando aplicável) permite mostrar que essa equação não possui soluções inteiras positivas ou, sob certas condições, até mesmo encontrar todas as soluções inteiras.

Se

$$A = \{(x_1,x_2,\cdots,x_n) \in \mathbb{Z}^n \mid f(x_1,x_2,\cdots,x_n) = 0\}$$

com $A \neq \emptyset$ é o conjunto solução de f, então A possui uma solução "mínima". O descenso consiste em, a partir dessa solução mínima, obter uma ainda menor; nos conduzindo a uma contradição e, provando assim, que A é vazio, ou seja, que f não possui solução.

4.1.2 O Último Teorema de Fermat para $n = 4$

Para a demonstração do caso $n = 4$, utilizaremos o teorema abaixo.

Teorema 4.1 (Fermat): A equação $x^4+y^4 = z^2$ não possui soluções inteiras positivas.

Demonstração. Suponhamos que $x^4 + y^4 = z^2$ possui uma solução inteira com $x,y,z > 0$. Pelo descenso infinito, existe uma solução (a,b,c) na qual c é mínimo.

Em particular, temos que a e b são primos entre si. De fato, pois, se $d = mdc(a,b) > 1$ então $d|a$ e $d|b$ e consequentemente $d^4|a^4 + b^4 = c^2 \Rightarrow d^2|c$. Assim, poderíamos substituir (a,b,c) por $\left(\frac{a}{d}, \frac{b}{d}, \frac{c}{d^2}\right)$ e obter uma solução com c menor que o mínimo, já que $\frac{a}{d}$, $\frac{b}{d}$ e $\frac{c}{d^2}$ são inteiros.

De $(a^2)^2 + (b^2)^2 = c^2$ temos que (a^2,b^2,c) é um trio pitagórico primitivo e assim, existem inteiros positivos m e n primos relativos tais que, de acordo com 3.1.1 a^2 e b^2 tem paridades distintas e c é ímpar. Logo

$$a^2 = m^2 - n^2,\ b^2 = 2mn \text{ e } c = m^2 + n^2$$

Como $a^2 = m^2 - n^2 \Rightarrow a^2 + n^2 = m^2$ temos que (a,n,m) é uma tripla pitagórica primitiva e portanto m é ímpar.

Como $c = m^2 + n^2$ e m e c são ímpares, temos que m^2 é ímpar e n^2 é par. Portanto, n é par. De fato, se n fosse ímpar teríamos $n = 2k + 1$, para algum $k \in \mathbb{Z}$ o que implicaria em $n^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$. Absurdo! Assim, de $b^2 = 2mn$ concluímos que b^2 é par, e consequentemente, b é par. Observando ainda que $b^2 = (2n)m$ é um quadrado perfeito e $mdc(2n,m) = 1$, concluímos por 3.3 que tanto $2n$ como m são quadrados perfeitos, donde podemos encontrar inteiros positivos s e t tais que

$$2n = 4s^2, \text{ e } m = t^2$$

Por outro lado, dado que $a^2 + n^2 = m^2$, então por 3.1.1 existirão inteiros positivos i e j primos entre si, tais que

$$a = i^2 - j^2,\ n = 2ij \text{ e } m = i^2 + j^2.$$

Portanto $s^2 = \frac{n}{2} = ij$, logo i e j serão quadrados perfeitos, digamos $i = u^2$ e $j = v^2$. Logo temos que $m = i^2 + j^2$, $i = u^2$, $j = v^2$ e $m = t^2$, assim

$$t^2 = m = i^2 + j^2 = (u^2)^2 + (v^2)^2 = u^4 + v^4,$$

isto é, (u,v,t) é outra solução de $x^4 + y^4 = z^2$. Porém,

$$t \leq t^2 = m \leq m^2 < m^2 + n^2 = c$$

e $t \neq 0$ já que $m \neq 0$. Absurdo! Já que c é mínimo.

Logo $x^4 + y^4 = z^2$ não possui solução. □

Observemos além disso que, uma vez que $x^4 + y^4 = z^2$ não possui soluções inteiras positivas, então a equação $x^4 + y^4 = (z^2)^2 = z^4$ e, mais geralmente $x^{4n} + y^{4n} = z^{4n}$ também não possuem soluções inteiras. Logo, para $n = 4$ e $n = 4k$ com $k \in \mathbb{N}$ o Último Teorema de Fermat está provado.

4.2 Euler e a demonstração para $n = 3$

Figura 4.1: Imagem de Leonhard Euler

4.2.1 Euler – biografia e contribuições para a matemática

Leonhard Euler foi um dos matemáticos que obteve renome depois de resolver um problema em aberto, posteriormente a deparar com a resposta para o afamado problema da Basiléia, proposto inicialmente pelo matemático italiano Pietro Mengoli (1625 - 1686) em 1644 (Szpiro, 2008). O problema proposto por Mengoli consistia em apresentar o resultado da soma dos inversos dos quadrados perfeitos, ou seja,

$$\sum_{n=1}^{\infty} \frac{1}{n^2} = \frac{1}{1^2} + \frac{1}{2^2} + \frac{1}{3^2} + \frac{1}{4^2} \cdots$$

Atualmente Euler é reconhecido como um dos nomes mais admiráveis da História da Matemática, não só por ter resolvido tal problema, mas sobretudo por ter colaborado com a matemática em diferentes áreas. Euler ficou famoso, com mais de 850 trabalhos, sendo muitos de extremo valor (SIMMONS, 2002).

4.2.2 A vida de Euler

A história da vida de Euler relata que o grande matemático Leonhard Paul Euler nasceu em 1707 em uma importante cidade da Suíça, denominada Basiléia. Euler era filho de uma linhagem muito bem estruturada, o garoto teve acesso as melhores escolas e onde trabalhavam os mais renomados professores.

A grande preocupação com a boa formação do garoto se dava especialmente ao caso de que Paul Euler, pai de Leonhard, atuava como pastor da Igreja Calvinista e presumia que o garoto seguiria na profissão (BOYER, 2003).

Apesar de Leonhard não ingressar na carreira de pastor como almejava seu pai, adotou seus princípios contemplativos por toda a existência (SIMMONS, 2002).

A preferência de Leonhard não foi uma afronta para seu pai, pois o mesmo havia estudado Matemática com Jakob Bernoulli (1654 - 1705), professor e amigo. A proximidade das famílias de Euler e Bernoulli eventualmente levou ao entusiasmo e comprometimento do jovem na matemática (BOYER, 2003).

Euler, ainda adolescente, com apenas 14 anos de idade entrou na Universidade da Basiléia local onde primeiramente estudou "Medicina, Teologia e Ciências Humanas".

Após dois anos, nesta mesma universidade, dedicou-se a matemática (SIMMONS, 2002). Posteriormente, ao se formar, exerceu a profissão ainda na Basiléia, nas disciplinas de "Filosofia, Teologia e Matemática".

No ano de 1727, por influência dos irmãos Daniel e Nicolas Bernoulli, filhos de Jakob Bernoulli, Euler foi convocado a associar a Academia de Ciências São Petersburgo na Rússia, lugar onde foi designado professor de Física em 1730 e de Matemática em 1733 (SIMMONS, 2002). Euler perdeu completamente a visão do olho direito aos 28 anos de idade, o que não restringiu seu ritmo de trabalho.

A causa de tal evento foi o hábito de intensa rotina de trabalho, forçando as vistas por longos períodos da noite (BOYER, 2003).

O matemático continuou na Rússia até 1741, data em que foi chamado para ser professor de Matemática na Academia de Ciências de Berlim, local onde conquistou a admiração de vários membros da corte do imperador da Prússia, atualmente Alemanha e Polônia.

Contudo, Euler era tímido, e devido a perda de um olho, sujeitou-se a zombaria; mesmo assim, em 1766 aceita uma solicitação para regressar a Academia de Ciências de São Petersburgo local onde atuou até os últimos dias de sua vida (CAJORI, 2007).

Além disso, em 1766 entendeu que, pelo motivo da catarata, ocorria a perda da visão do segundo olho e, para permanecer atuando habilitou um de seus filhos para registrar a parte escrita enquanto ele ditava. A despeito de tais condições, sua memória esplêndida consentiu que prosseguisse trabalhando sem parar (EVES, 2004).

Euler morre em 1783 no momento em que tomava chá em companhia de um de seus netos, depois de ter passado o dia pesquisando e analisando a órbita do recém descoberto planeta Urano (SIMMONS, 2002).

Sua vida acadêmica agitada não o impediu de compor com Katharina Gsell uma notável família formada por uma prole que ao todo eram 13 filhos que, segundo alguns autores, sem muitas dificuldades conseguia escrever seus artigos no mesmo tempo em que cuidava das crianças. "Um amigo que presenciava sua vida doméstica disse: Uma criança no colo, um gato sobre o ombro, assim escrevia ele suas obras imortais" (GARBI, 1997).

4.2.3 A obra de Euler

Citar a obra de Euler é o mesmo que citar uma obra superior a 850 títulos literários entre livros e artigos. Na História da Matemática não se encontra outro estudioso que produziu igual quantidade; exclusivamente no tempo que esteve em Berlim produziu um número de 275 trabalhos (SIMMONS, 2002).

Eram várias as obras, dentre elas podem ser citados os assuntos de "Cálculo, Álgebra, Teoria dos números, Geometria, além de Física e Astronomia". Algumas de suas obras apresentavam fins didáticos objetivando a tornar a Matemática desenvolvida naquele período acessível para estudantes de Engenharia, Arquitetura e distintas áreas técnicas (BOYER, 2003).

4.2.4 Um pouco das tentativas de demonstração para o caso $n = 3$

No período de Fermat, os matemáticos eram conhecidos como calculistas amadores, pois a matemática não era sua profissão, a tinham como hobbie. Entretanto, no século XVIII os mesmos já eram considerados solucionadores profissionais de problemas. A cultura numérica havia mudado e, dramaticamente, se tornando em parte uma consequência dos cálculos científicos de Isaac Newton.

Newton acreditava que os matemáticos estavam perdendo tempo desafiando uns aos outros com enigmas sem sentido. Ele queria aplicar a matemática ao mundo físico, calculando tudo, das órbitas dos planetas as trajetórias das balas de canhões. Quando Newton morreu em 1727, a Europa tinha passado por uma revolução científica e no mesmo ano, Euler publicou seu primeiro trabalho.

Leonhard Euler (1707 – 1783) foi quem realizou o primeiro avanço acerca da prova do último teorema de Fermat.

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

Euler adaptou a prova de Fermat do caso, utilizando um conceito pouco conhecido para a época, que hoje conhecemos por números imaginários, que fora descoberta pelos matemáticos europeus do século XVI. É estranho pensar em novos números sendo descobertos, mas isso é porque estamos tão acostumados com os números que usamos no dia a dia que esquecemos que houve uma época em que estes números não eram conhecidos. No passado, outros matemáticos tentaram adaptar o método de descenso infinito de Fermat para resolver outros casos, mas cada uma dessas tentativas de estender a prova levava a brechas na lógica. Euler mostrou que, incorporando-se o número imaginário em sua prova, ele poderia tapar os buracos na demonstração e forçar o método do descenso infinito a funcionar para o caso n=3.

4.2.5 A demonstração de Euler para n=3

Antes de provarmos o Último Teorema de Fermat para $n = 3$, demonstraremos o lema abaixo.

Lema 4.1: Todas as soluções de $f^3 = g^2 + 3h^2$ em inteiros positivos tais que

mdc(h,g) = 1 e f é ímpar, são dadas por

$$f = m^2 + 3n^2, g = m^3 - 9mn^2, h = 3m^2n - 3n^3$$

com $m + n$ ímpar e mdc(m,$3n$) = 1.

Demonstração. ($\Longleftarrow$) Substituindo f,h e g na equação $f^3 = g^2 + 3h^2$, temos que

$$(m^2 + 3n^2)^3 = (m^3 - 9mn^2)^2 + 3(3m^2m - 3n^3)^2 \Rightarrow$$

$$(m^6+9m^4n^2+9m^2n^4+27n^6) = (m^6-38m^4n^2+81n^2n^4)+(27m^4n^2-54m^2n^4+27n^6).$$

Assim podemos afirmar que tais números são soluções da equação.

Como $m + n$ é ímpar então m é par e n ímpar ou m é ímpar e n é par. Dessa forma $f = m^2 + 3n^2$ é ímpar.

Além disso,

$$\text{mdc}(h,g) = \text{mdc}(m^3 - 9mn^2, 3m^2n - 3n^3) = \text{mdc}(m(m^2 - 9n^2),3n(m^2 - n^2)).$$

Devemos encontrar o mdc($m(m^2 - 9n^2)$,$3n(m^2 - n^2)$) para isso iremos usar o lema 3.1 e o TFH (teorema 3.9) . Como mdc(m,$3n$) = 1 então

$$\begin{aligned}\text{mdc}(m(m^2 - 9n^2),3n) &= \text{mdc}(m^2 - 9n^2,3n)\\ &= \text{mdc}(m^2 - 9n^2 + 3n \cdot 3n, 3n)\\ &= \text{mdc}(m^2,3n)\\ &= \text{mdc}(m \cdot m, 3n)\\ &= \text{mdc}(m,3n) = 1.\end{aligned}$$

Como mdc($m(m^2 - 9n^2)$,$3n$) = 1 então

$$\text{mdc}(m(m^2 - 9n^2),3n(m^2 - n^2)) = \text{mdc}(m(m^2 - 9n^2),m^2 - n^2)$$

Sabemos que

$$\text{mdc}(m,m^2 - n^2) = \text{mdc}(m,m^2 - n^2 - m \cdot m) = \text{mdc}(m, - n^2) = \text{mdc}(m,n^2) = 1,$$

pois mdc(m,$3m$) = 1. De fato, m e $3n$ não possuem fatores primos comuns. Daí m e n também não. Consequentemente, n^2 e m são coprimos. Como mdc(m,$m^2 - n^2$) = 1 então mdc($m(m^2 - 9n^2)$,$m^2 - n^2$) = mdc($m^2 - 9n^2$,$m^2 - n^2$).

Portanto

$$\begin{aligned}
\text{mdc}(m(m^2-9n^2),3n(m^2-n^2)) &= \text{mdc}(m(m^2-9n^2),m^2-n^2)\\
&= \text{mdc}(m^2-9n^2,m^2-n^2)\\
&= \text{mdc}(m^2-9n^2-m^2+n^2,m^2-n^2)\\
&= \text{mdc}(-8n^2,m^2-n^2)\\
&= \text{mdc}(8n^2,m^2-n^2)\\
&= \text{mdc}(8n^2+8m^2-8n^2,m^2-n^2)\\
&= \text{mdc}(8m^2,m^2-n^2) = 1
\end{aligned}$$

De fato, m^2-n^2 e m não possuem fatores primos comuns. Daí, m^2-n^2 e m^2 também não. Consequentemente, m^2-n^2 e $8m^2$ não possuem fatores comuns. Logo $\text{mdc}(h,g) = 1$.
($\Longrightarrow$)
Suponha que (g,h,f) é solução da equação. Seja p primo tal que $p|f$.
Como $\text{mdc}(g,h) = 1$ e f é ímpar então $p > 3$. De fato, se $p = 2$ então p não divide f, já que f é ímpar. Note que se $p|h$ e $p|f$ então $p|g$. Absurdo, pois $\text{mdc}(h,g) = 1$. Analogamente, se $p|g$ e $p|f$ então $p|h$, que também é absurdo pelo mesmo motivo. Logo p não divide h, p não não divide g e $p > 3$.

Como $p|f$ então $p|f^2$. Consequentemente, $p|(g^2+3h^2) \Leftrightarrow g^2 \equiv -3h^2 (\text{mod } p)$. Como p não divide h então $\text{mdc}(p,h) = 1$. Logo h é invertível módulo p. Dessa forma, temos que $\left(\frac{-3}{p}\right) = 1$ e daí pelas lei da reciprocidade quadrática (página 85 do livro 11), temos que $\left(\frac{p}{3}\right) = 1$. Pelo exemplo 4.8 (página 132 do livro 11), sabemos que existem inteiros m_1 e n_1 tais que $p = m_1^2 + 3n_1^2$ e que, pela volta deste lema, $p^3 = d^2 + 3c^2$ onde $d = m_1^3 - 9m_1n_1^2$ e $c = 3m_1^2n_1 - 3n_1^3$. Temos que $\text{mdc}(p,c) = 1$, como na demonstração anterior em que $\text{mdc}(g,h) = 1$. Logo, $\text{mdc}(p,m_1) = \text{mdc}(p,n_1) = 1$ e $p > 3$.

Iremos provar por indução sobre número de divisores primos de f. Se $f = 1$, o resultado é imediato, pois a única solução é $g = 1$, $h = 0$ e $f = 1$. Suponha que o resultado valha para todo f que tenha k fatores primos (não necessariamente distintos). Se f tem $k+1$ fatores primos, digamos $f = p \cdot t$ como p primo ($p > 3$) observemos que:

$$\begin{aligned}
t^3p^6 &= t^3p^3p^3\\
&= f^3p^3\\
&= (g^2+3h^2)(d^2+3c^2)\\
&= g^2d^2 + 3h^2d^2 + 3g^2c^2 + 9h^2c^2\\
&= (g^2d^2 \pm 6ghdc + 9h^2c^2) + 3(g^2c^2 \pm 2gchd + h^2d^2)\\
&= (gd \pm 3hc)^2 + 3(gc \pm hd)^2
\end{aligned}$$

Além disso,

$$\begin{aligned}(gc+hd)(gc-hd) &= (gc)^2-(hd)^2\\ &= c^2(g^2+3h^2)-h^2(d^2+3c^2)\\ &= c^2f^3-h^2p^3\\ &= c^2p^3t^3-h^2p^3\\ &= p^3(c^2t^3-h^2)\end{aligned}$$

Dessa forma $p^3|(gc+hd)(gc-hd)$. Se p^3 divide dois fatores então p também os divide. Assim, $p|(gc+hd)$ e $p|(gc-hd) \Rightarrow p|(gc+hd+gc-hd) \Rightarrow p|2gc \Rightarrow p|gc$ Consequentemente, $p|hd$. Como mdc(p,c) = mdc(p,d) = 1 então $p|h$ e $p|g$. Absurdo, pois mdc(h,g) = 1. Logo p^3 divide exatamente um dos fatores. A demonstração é análoga para $(gd+3hc)(gd-3hc)$.

Tomando adequadamente os sinais, existem u,$v \in \mathbb{Z}$ tais que

$$p^3u = gd \pm 3hc \Rightarrow u = \frac{gd \pm 3hc}{p^3}$$

$$p^3v = gc \pm hd \Rightarrow v = \frac{gc \pm hd}{p^3}$$

sendo que $t^3 = u^2+3v^2$. De fato,

$$\frac{(gd \pm 3hc)^2}{p^6} + 3 \cdot \frac{(gc \pm hd)^2}{p^6} = \frac{(gd \pm 3hc)^2+3(gc \pm hd)^2}{p^6} = \frac{t^3p^6}{p^6} = t^3$$

Como t tem k fatores primos, segue por hipótese de indução que existem m_2 e n_2 inteiros tais que $t = m_2^2+3n_2^2$, $u = m_2^3-9m_2n_2^2$ e $v = 3m_2^2n_2-3n_2^3$.

Agora, dado que $g = ud+3vc$ e $h = -(uc-vd)$, substituindo u,v,d,c em termos de m_i e n_i (i = 1,2) em z,y,x e fazendo $m = m_1m_2+3n_1n_2$ e $n = m_1n_2-m_2n_1$, obtemos:

$$\begin{aligned}g &= ud+3vc\\ &= (m_2^3-9m_2n_2^2)(m_1^3-9m_1n_1^2)+3(3m_2^2n_2-3n_2^3)(3m_1^2n_1-3n_1^3)\\ &= m_1^3m_2^3-9m_1n_1^2m_2^3-9m_1^3m_2n_2^2+81m_1n_1^2m_2n_2^2+27m_1^2n_1m_2^2n_2\\ &\quad -27n_1^3m_2^2n_2-27m_1^2n_1n_2^3+27n_1^3n_2^3\\ &= m_1^3m_2^3+9m_1^2m_2^2n_1n_2+27m_1m_2n_1^2n_2^2+27n_1^3n_2^3-9m_1^3m_2n_2^2+18m_1^2n_2n_1m_2^2\\ &\quad -9m_1n_1^2m_2^3-27n_1m_1^2n_2^3+54m_1n_1^2m_2n_2^2-27n_1^3m_2^2n_2\\ &= (m_1m_2+3n_1n_2)^3-9(m_1m_2+3n_1n_2)(m_1^2n_2^2-27m_1n_1m_2n_2+n_1^2m_2^2)\\ &= m^3-9mn^2\end{aligned}$$

e

$$
\begin{aligned}
h &= -(uc - vd) \\
&= -(m_2^3 - 9m_2n_2^2)(3m_1^2 - 3n_1^3) + (3m_1^2n_2 - 3n_2^3)(m_1^3 - 9m_1n_1^2) \\
&= 3m_1^2n_1m_2^3 + 3n_1^3m_2^3 - 27m_1^2n_1m_2n_2^2 - 27m_2n_2^2n_1^3 + 3m_1^3m_2^2n_2 - 27m_1n_1^2m_2^2n_2 \\
&\quad - 3m_1^3n_2^3 + 27m_1^2n_1^2n_2^3 \\
&= 3m_1^3m_2^2n_2 + 18m_1^2m_2n_1n_2^2 + 27m_1n_1^2n_2^3 - 3m_1^2n_1m_2^3 - 18m_1n_1^2m_2^2n_2 - 27n_1^3m_2n_2^2 \\
&\quad - 3m_1^3n_2 + 9m_1^2n_2^2n_1m_2 - 9m_1n_2n_1^2m_2^2 + 3n_1^3m_2^3 \\
&= 3(m_1^2m_2^2 + 6m_1m_2n_1n_2 + 9n_1^2n_2^2)(m_1n_2 - n_1m_2) \\
&\quad - 3(m_1^3n_2^3 - 3m_1^2n_2^2n_1m_2 + 3m_1n_2n_1^2m_2^2 - n_1^3m_2^3) \\
&= 3m^2n - 3n^3
\end{aligned}
$$

e

$$
\begin{aligned}
g^2 + 3h^2 &= (m^3 - 9mn^2)^2 + 3(3m^2n - 3n^3)^2 \\
&= m^6 - 18m^4n^2 + 81m^4n^2 + 81m^2n^4 + 27m^4n^2 - 54m^2n^4 = 27n^6 \\
&= m^6 + 9m^4n^2 + 27m^2n^4 + 27n^6 \\
&= (m^2 + 3n^2)^3 \\
&= f^3 \qquad (4.1)
\end{aligned}
$$

Logo, a única solução de f^3 é $h = 3m^2n - 3n^3$, $g = m^3 - 9mn^2$ e $f = m^2 + 3n^2$. □

Com esse lema e o Descenso Infinito de Fermat, podemos demonstrar que:

Teorema 4.2: A equação diofantina $x^3 + y^3 = z^3$ não possui soluções inteiras com $x,y,z \neq 0$.

Demonstração. Suponhamos que a equação $x^3 + y^3 = z^3$ possui solução com $x,y,z > 0$ e escolhemos essa solução de tal forma que x,y,z seja mínimo. Como qualquer fator comum de dois desses números é também do terceiro então podemos afirmar que são primos relativos dois a dois pois se não teria outra solução $\left(\frac{x}{k}, \frac{y}{k}, \frac{z}{k}\right)$ menor que (x,y,z). Em particular, um de tais números será par.
Se $x = y$ então $x^3 + y^3 = 2x^3 = z^3$ impossível, pois o expoente da maior potência de dois do lado direito seria múltiplo de três, enquanto do lado esquerdo não. Assim, sem perda de generalidade podemos considerar $x > y$ (para $x < y$ será análogo).

Suponha que x e y são ímpares e z é par. Podemos escrever $x = p + q$ e $y = p - q$ com $p > 0$ e $q > 0$ coprimos e de paridades diferentes. Assim,

$$
\begin{aligned}
z^3 = x^3 + y^3 &= (x + y)(x^2 - xy + y^2) \\
&= 2p\left[(p + q)^2 - (p + q)(p - q) + (p - q)^2\right] \\
&= 2p\left[p^2 + 3q^2\right]
\end{aligned}
$$

Dessa forma $2p\,[p^2 + 3q^2]$ é um cubo perfeito.

De igual forma, no caso em que z é ímpar e x ou y é par. Podemos supor que y é ímpar com $z > y$, substituindo $z = q + p$ e $y = q - p$ temos:

$$\begin{aligned} x^3 &= z^3 - y^3 \\ &= 2p\left[(p+q)^2 + (p+q)(q-p) + (q-p)^2\right] \\ &= 2p\left[p^2 + 3q^2\right] \end{aligned}$$

Como $p^2 + 3q^2$ é ímpar e $2p(p^2 + 3q^2)$ é um cubo perfeito, temos que p será par. Calculando o máximo divisor comum de de p e $p^2 + 3q^2$, temos

$$\text{mdc}(p,p^2 + 3q^2) = \text{mdc}(p,3q^2) = \text{mdc}(p,3)$$

já que $\text{mdc}(p,q) = 1$, pois p e q são coprimos. Logo, há dois casos:

$$\text{mdc}(p,3) = 1 \text{ e } \text{mdc}(p,3) = 3.$$

No primeiro, existem naturais a e b tais que $a^3 = 2p$ e $b^3 = p^2 + 3q^2$. Neste caso, pelo lema anterior, existem m e n de paridades diferentes e coprimos tais que $b = m^2 + 3n^2$, $p = m^3 - 9mn^2$ e $q = 3m^2n - 3n^3$.

Logo $a^3 = 2p = 2(m^3 - 9mn^2) = 2m(m^2 - 9n^2) = 2m(m-3n)(m+3n)$. Observe que $2m$, $m - 3n$ e $m + 3n$ são coprimos. Assim, existem e, f e g tais que $2m = e^3$, $m - 3n = f^3$ e $m + 3n = g^3$. Em particular, temos: $(m - 3n) + (m + 3n) = 2m$. Portanto $f^3 + g^3 = e^3$ e teremos uma solução menor, o que contradiz a escolha de x,y,z.

No caso em que $\text{mdc}(p,3) = 3$ temos que $3|p$. Assim, existe r inteiro tal que $p = 3r$, com $\text{mdc}(r,p) = 1$. Dessa forma, $z^3 = 2p(p^2 + 3q^2) = 18r(3r^2 + q^2)$. Logo, existem inteiros i e j tais que $18r = i^3$ e $3r^2 + q^2 = j^3$. Daí, novamente existem inteiros u e v tais que $j = u^2 + 3v^2$, $q = u^3 - 9uv^2$ e $r = 3u^2v - 3v^3$. Segue que $i^3 = 18r = 27(2v)(u - v)(u + v)$.

De igual forma, teremos que os números $2v$, $u + v$, e $u - v$ são coprimos. Assim, existem inteiros positivos k,l,s tais que $2v = k^3$, $u - v = l^3$ e $u + v = s^3$. Segue que $k^3 + l^3 = s^3$. Portanto (k,l,s) também é solução da equação e como já vimos contradiz a minimalidade da solução (x,y,z).

Logo a equação diofantina $x^3 + y^3 = z^3$ não possui soluções inteiras positivas. □

A demonstração acima, foi escrita por Euler, note que a mesma é puramente aritmética.

Dias, em 2018 relatou que :

> *A demonstração para $n = 3$ trouxe grandes recompensas. Isso se deve ao fato que a demonstração para $n = 3$ também serve para $n =$ 6,9,12,15,$\cdots$. Pois, se a equação $b^6 + c^6 = a^6$ tem solução, ao reescrevermos como $(b^2)^3 + (c^2)^3 = (a^2)^3$ e considerando $b^2 = B$, $c^2 = C$ e $a^2 = A$,*

> *temos que a equação $B^3 + C^3 = A^3$ tem solução, com isso gerando uma contradição. Assim, qualquer demonstração que funcione com a potência de 3 vai funcionar para um número elevado a 6 ou qualquer outro múltiplo de 3. Isso também é válido para o caso $n = 4$ que Fermat tinha demonstrado. A prova para $n = 4$ também serve para $n = 8, 12, 16, 20, \cdots$ e qualquer outro múltiplo de 4. Com essas duas classes de números provadas, o desafio era provar o teorema para o caso de n ser um número primo diferente de 2 e de 3. Com isso todos os outros casos seriam múltiplos dos casos primos e seriam provados implicitamente. Apesar dessa ideia tornar mais simples a demonstração, tinha um pequeno e crucial problema: a infinidade de números primos. Isso de uma forma geral pôs fim as esperanças de uma prova precoce para o Último Teorema de Fermat, (DIAS,2018.p49).*

Posteriormente à segunda guerra mundial, matemáticos começaram a utilizar os computadores como agregados aos cálculos. Segundo Singh (2012), os computadores foram de grande ajuda para os grupos de matemáticos fazerem a demonstração do Último teorema de Fermat para valores de n até 500, e em seguida para valores de 1.000 até 10.000. No decorrer da década de 1980 ele já havia aprovação para valores de n até 25.000.

Ainda assim, mesmo que os computadores confirmassem valores imensos de n, consecutivamente permanecia o equívoco para um valor maior, pois o teorema se amplia para valores infinitos de n. Portanto, a tecnologia, ainda que competente e instantânea em cálculos, não seria competente para demonstrar o Último Teorema de Fermat (SINGH, 2012).

De acordo com Singh,(2012) os matemáticos teóricos tinham conhecimento disso. Eles permaneciam convictos de que a despeito das evidências originadas pelos computadores, exclusivamente uma prova absoluta seria apropriado para colocar fim a esse mistério. E isso iria suceder. Após 350 anos que Fermat espalhou seu desafio o magnífico matemático inglês Andrew Wiles por fim coloca um ponto final a esse enigma.

4.3 Demonstração para n = 3 utilizando o anel $\mathbb{Z}[\omega]$

Uma outra demonstração para o caso $n = 3$ do Último Teorema de Fermat é dada com argumentos algébricos.

Considere a equação

$$X^3 + Y^3 + Z^3 = 0 \tag{4.2}$$

Suponhamos que exista uma solução não trivial $(\alpha, \beta, \nu) \in \mathbb{Z}[\omega]^3$ para essa equação. Podemos considerar que α, β, ν são coprimos dois a dois. Com essa suposição e com os lemas a seguir, tentaremos chegar numa contradição, demonstrando assim o teorema 4.3.

Lema 4.2: Em $\mathbb{Z}[\omega]$ podemos escrever $X^3 + Y^3 = (X + 1Y)(X + \omega Y)(X + \omega^2 Y)$

Demonstração. Efetuando o produto:

$$\begin{aligned}(X+1Y)(X+\omega Y)(X+\omega^2 Y) &= (X^2+\omega XY+XY+\omega Y^2)(X+\omega^2 Y)\\ &= X^3+\omega^2X^2Y+\omega X^2Y+\cancelto{1}{\omega^3}XY^2+X^2Y+\omega^2XY^2+\\ &+\omega XY^2+\cancelto{1}{\omega^3}Y^3\\ &= X^3+X^2Y(\omega^2+\omega+1)+XY^2(1+\omega^2+\omega)+Y^3\\ &= X^3+Y^3\end{aligned}$$

□

Lema 4.3: O elemento $\gamma = 1-\omega$ é um *elemento irredutível* em $\mathbb{Z}[\omega]$ e a fatoração de 3 em elementos irredutíveis de $\mathbb{Z}[\omega]$ é $3 = -\omega^2(1-\omega)^2 = -\omega^2\gamma^2$.

Demonstração. Pelo item 3 da proposição 3.4, o elemento $\gamma = 1-\omega$ não é nulo nem invertível. Suponha agora que $\gamma = \alpha\cdot\beta$. Mostraremos que ou α ou β é invertível.
Aplicando a norma:

$$N(\alpha)N(\beta) = N(\gamma) = 3$$

Sabemos que, como 3 é primo no DIP $\mathbb{Z}$, a única fatoração de 3 em $\mathbb{Z}$ é $3 = 3\cdot 1$. Portanto, $N(\alpha) = 1$ ou $N(\beta) = 1$, ou seja, α ou β é invertível, novamente pelo item 3 da proposição 3.4.
Concluímos então que γ é irredutível e, como $\mathbb{Z}[\omega]$ é DIP (corolário 3.4), também é primo em $\mathbb{Z}[\omega]$.
Vamos agora verificar que $-\omega^2\gamma^2$ é a fatoração de 3 em elementos irredutíveis de $\mathbb{Z}[\omega]$:

$$\begin{aligned}-\omega^2\gamma^2 &= -\omega^2(1-\omega)^2\\ &= -\omega^2+2\omega^3-\omega^4\\ &= -\omega^2+2-\omega\\ &= -(\omega^2+\omega+1)+3\\ &= 3\end{aligned}$$

Como $\mathbb{Z}[\omega]$ é DFU, essa é a única fatoração de 3. □

Lema 4.4: Se um inteiro a é divisível por $\gamma = 1-\omega$ em $\mathbb{Z}[\omega]$, então $3|a$ em $\mathbb{Z}$.

Demonstração. Como a é divisível por γ, existe $\kappa\in\mathbb{Z}[\omega]$ tal que $a = \kappa\omega$. Aplicando a norma, temos $a^2 = N(\kappa)3$ implicando que 3 divide a^2 em $\mathbb{Z}$. Como 3 é primo em $\mathbb{Z}$, concluímos que $3|a$. O contrário também vale. De fato, se a é inteiro e $3|a$ em $\mathbb{Z}[\omega]$, então $\gamma|a$, uma vez que γ é fator de 3. □

Lema 4.5: $\dfrac{\mathbb{Z}[\omega]}{<\gamma>}\cong\mathbb{Z}_3$

Demonstração. Verificaremos esse isomorfismo usando o teorema fundamental do homomorfismo (TFH), isto é, precisamos definir um homomorfismo cuja imagem seja $\mathbb{Z}_3$ e cujo núcleo (ou kernel) seja o ideal $< \gamma >$.

Para isso, podemos observar qual é a forma dos elementos de $\dfrac{\mathbb{Z}[\omega]}{< \gamma >}$:

$$a + b\omega + < \gamma >= a + b - b\gamma + < \gamma >= a + b + < \gamma > .$$

Baseados nessa observação e, juntamente com a proposição 4.4, definimos a seguinte função:

$$\begin{aligned} \phi : \mathbb{Z}[\omega] &\to \mathbb{Z}_3 \\ a + b\omega &\mapsto \overline{a + b} \end{aligned}$$

onde $\overline{a + b}$ representa a classe de $a + b$ em $\mathbb{Z}_3$.

Vamos verificar que ϕ é um homomorfismo:

- Adição:

$$\begin{aligned} \phi((a + b\omega) + (c + d\omega)) &= \phi((a + c) + (b + d)\omega) \\ &= \overline{a + c + b + d} \\ &= \overline{a + b} + \overline{c + d} \\ &= \phi(a + b\omega) + \phi(c + d\omega) \end{aligned}$$

- Multiplicação:

$$\begin{aligned} \phi((a + b\omega) \cdot (c + d\omega)) &= \phi((ac - bd) + (ad + bc - bd)\omega) \\ &= \overline{ac - bd + ad + bc - bd} \\ &= \overline{(ac + ad + bc + bd)} \\ &= \overline{(a + b)} \cdot \overline{(c + d)} \\ &= \phi(a + b\omega) \cdot \phi(c + d\omega) \end{aligned}$$

Agora vamos verificar as condições necessárias para usar o TFH:

- O homomorfismo ϕ é sobrejetor. De fato, dado $\overline{n} \in \mathbb{Z}_3$, temos $\phi(n + 0\omega) = \overline{n}$.
- Considere $\alpha \in < \gamma >$. Então $\exists \kappa = c + d\omega \in \mathbb{Z}[\omega]$ tal que $\alpha = \kappa\omega$. Escrevendo de outra forma, temos $\alpha = (c + d\omega)(1 - \omega) = (c + d) + (2d - c)\omega$. Portanto $\phi(\alpha) = \overline{c + d + 2d - c} = \overline{0}$. Logo, $\alpha \in \text{Ker}\phi$.

  Por outro lado, seja $\alpha = a + b\omega \in \text{Ker}\phi$, isto é, $\phi(a + b\omega) = \overline{0}$. Assim, $\overline{a + b} = \overline{0}$, significando que, em $\mathbb{Z}$, podemos escrever $a + b = 3k$. Mas em $\mathbb{Z}[\omega]$, de acordo com a proposição 4.3, isso pode ser reescrito como $a + b = -\omega^2\gamma^2 k$. Pela observação feita no começo dessa demonstração, temos que $a = b\omega = -(b + \omega^2 k\gamma)\gamma$ e portanto, $\alpha \in < \gamma >$. Desse modo concluímos a igualdade entre esses dois conjuntos.

Portanto, pelo TFH

$$\frac{\mathbb{Z}[\omega]}{\mathrm{Ker}\phi} = \frac{\mathbb{Z}[\omega]}{<\gamma>} \cong \mathbb{Z}_3 = \mathrm{Im}\phi$$

Com esse isomorfismo demonstrado, podemos representar as classes de $\frac{\mathbb{Z}[\omega]}{<\gamma>}$ por $\overline{-1}$, $\overline{0}$ e $\overline{1}$.
Também vamos representar por $\alpha \mapsto \alpha \bmod \gamma$ o homomorfismo canônico entre $\mathbb{Z}[\omega]$ e $\frac{\mathbb{Z}[\omega]}{<\gamma>}$.

□

Lema 4.6: Seja $\alpha \in \mathbb{Z}[\omega]$. Se α não for divisível por γ, então $\alpha^3 \equiv \pm 1 \bmod \gamma^4$.

Demonstração. Suponha que $\alpha \equiv 1 \bmod \gamma$. Então $\exists\ \kappa \in \mathbb{Z}[\omega]$ tal que $\alpha = 1 + \kappa\gamma$. Elevando ao cubo ambos os membros da equação:

$$\alpha^3 = 1 + 3\kappa\gamma + 3\kappa^2\gamma^2 + \kappa^3\gamma^3 = 1 - \omega^2\gamma^3\kappa - \omega^2\gamma^4\kappa^2 + \kappa^3\gamma^3$$

Portanto

$$\alpha^3 - 1 = \gamma^3(\kappa^3 - \omega^2\kappa) = \gamma^3(\kappa(\kappa - \omega)(\kappa + \omega))$$

Queremos agora mostrar que o termo $(\kappa(\kappa - \omega)(\kappa + \omega))$ tem fator γ. Para isso, vamos analisar 3 casos:

- Se $\kappa \equiv 0 \bmod \gamma$ já temos o resultado que queremos.
- Se Se $\kappa \equiv 1 \bmod \gamma$: Então $\kappa - \omega \equiv 1 - \omega \equiv \gamma \equiv 0 \bmod \gamma$
- Se $\kappa \equiv -1 \bmod \gamma$: Então $\kappa + \omega \equiv -1 + \omega \equiv -\gamma \equiv 0 \bmod \gamma$

Assim, o termo $(\kappa(\kappa-\omega)(\kappa+\omega))$ é divisível por γ para todo κ. Logo, podemos escrever $\alpha^3 - 1 = \kappa\gamma^4$ e portanto, $\alpha^3 \equiv 1 \bmod \gamma^4$. Analogamente, supondo, $\alpha \equiv -1 \bmod \gamma$ chegamos a $\alpha^3 \equiv -1 \bmod \gamma^4$. □

Proposição 4.1: Se $(\alpha,\beta,\nu) \in \mathbb{Z}[\omega]$ for solução da equação $X^3 + Y^3 + Z^3 = 0$, então

1. O elemento $\gamma = 1 - \omega$ divide exatamente um dos elementos α , β ou ν.

2. Suponha que $\gamma|\nu$. Podemos afirmar que a equação

$$X^3 + Y^3 + U\gamma^{3n}Z^3 = 0 \tag{4.3}$$

admite solução $(x,y,u,z) \in \mathbb{Z}[\omega]^4$ para algum inteiro n positivo. Seja n_0 o menor inteiro n tal que a equação tenha solução.

3. $n_0 \geq 2$

4. Com relação ao item 2, podemos afirmar que $\gamma|(x+y)$, $\gamma|(x+\omega y)$ e $\gamma|(x+\omega^2 y)$

5. A equação
$$Y_1Y_2Y_3 = -U_1\gamma^{3n_0-3}Z_1^3 \tag{4.4}$$
tem solução $(y_1,y_2,y_3,u_1,z_1) \in \mathbb{Z}[\omega]^5$ com $\text{mdc}(y_1,y_2) = \text{mdc}(y_1,y_3) = \text{mdc}(y_3,y_2) = 1$.

6. Podemos escrever $y_1 = \epsilon_1\gamma^{3n_0-3}t_1^3$, $y_2 = \epsilon_2 t_2^3$ e $y_3 = \epsilon_3 t_3^3$, onde ϵ_i com $i \in 1,2,3$ são unidades de $\mathbb{Z}[\omega]$ e t_i com $i \in 1,2,3$ são elementos de $\mathbb{Z}[\omega]$, os quais são dois a dois relativamente primos e nenhum é divisível por γ.

7. Usando a escolha de n_0, obtemos um absurdo e concluímos que a equação $X^3 + Y^3 + Z^3 = 0$ não tem nenhuma solução não trivial em $\mathbb{Z}[\omega]$.

Demonstração. 1. Podemos supor α, β e ν coprimos dois a dois, então, de início já podemos descartar a possibilidade de haver um elemento que divida todos os três ao mesmo tempo ou quaisquer dois deles.
Assim, γ pode dividir apenas um deles, ou nenhum. Suponha que γ não divida nenhum deles. O lema 4.5 nos garante que $\dfrac{\mathbb{Z}[\omega]}{<\gamma>} \cong \mathbb{Z}_3$, logo, $\alpha \equiv \pm 1$ modγ, $\beta \equiv \pm 1$ modγ e $\nu \equiv \pm 1$ modγ.
Como $\alpha^3 + \beta^3 + \nu^3 = 0$ em $\mathbb{Z}[\omega]$, então
$$\alpha^3 + \beta^3 + \nu^3 \equiv 0 \text{ mod } \gamma^4 \tag{4.5}$$
Mas $\gamma \nmid \alpha$, $\gamma \nmid \beta$ e $\gamma \nmid \nu$, logo pelo lema 4.6 temos que $\alpha^3 \equiv \pm 1$ mod γ^4, $\beta^3 \equiv \pm 1$ modγ^4 e $\nu^3 \equiv \pm 1$ modγ^4.
De 4.5 e pelo lema 4.6 temos
$$0 \equiv \alpha^3 + \beta^3 + \nu^3 \equiv \pm 1 \pm 1 \pm 1 \equiv 0 \text{ mod } \gamma^4$$
Absurdo! Pois a soma $\pm 1 \pm 1 \pm 1$ só pode ser $\{\pm 1 \pm 3\}$. Como $1 \not\equiv 0$ mod γ e, pela proposição 4.3 temos que $3 = -\omega^2\gamma^2$ em $\mathbb{Z}[\omega]$, então $3 \not\equiv 0$ mod γ. Com isso, concluímos que $\pm 1 \pm 1 \pm 1 \not\equiv 0$ mod γ^4. Logo γ divide exatamente um elemento dentre α, β e ν.

2. Como γ divide um e somente um dos elementos α, β, ν, sem perda de generalidade, podemos supor que $\gamma \mid \nu$. Logo, $\nu = k \cdot \gamma^n$, $\text{mdc}(k,\gamma) = 1$ e $k \in \mathbb{Z}[\omega]$. Podemos fatorar k como $k = \epsilon \cdot t$, em que ϵ é a unidade, $t \in \mathbb{Z}[\omega]$ e mdc $(\gamma, t) = 1$. Assim,
$$\nu = \epsilon\gamma^n t$$
onde ϵ é invertível, t não é divisível por γ e n pelo menos igual a 1, já que $\gamma|\nu$.
Logo,
$$\alpha^3 + \beta^3 + \epsilon^3\gamma^{3n}t^3 = 0. \tag{4.6}$$
Portanto, $x = \alpha$, $y = \beta$, $u = \epsilon^3$, $z = t \in \mathbb{Z}[\omega]^4$ é solução da equação 4.3.

3. No item 1 vimos que $\alpha \equiv \pm 1 \bmod \gamma$ e $\beta \equiv \pm 1 \bmod \gamma$, então $\alpha^3 \equiv \pm 1 \bmod \ \gamma$, $\beta^3 \equiv \pm 1 \bmod \gamma$. Logo,

$$\alpha^3 + \beta^3 \equiv \pm 1 \pm 1 \bmod \gamma \tag{4.7}$$

Do item 2, temos $\alpha^3 + \beta^3 + \epsilon^3\gamma^{3n}t^3 = 0$ e, analisando-a módulo γ obtemos $\alpha^3 + \beta^3 + \epsilon^3\gamma^{3n}t^3 \equiv 0 \bmod \gamma$. Mas, $\gamma \equiv 0 \bmod \gamma$, então

$$\alpha^3 + \beta^3 \equiv 0 \bmod \gamma$$

e as classes de α e β tem sinais contrários.

Logo, sem perda de generalidade, se $\alpha \equiv 1 \bmod \gamma$, então $\beta \equiv -1 \bmod \gamma$

Desse modo, pela equação 4.6, temos a congruência

$$\alpha^3 + \beta^3 + \epsilon^3\gamma^{3n}t^3 \equiv 0 \bmod \gamma^4 \Rightarrow \epsilon^3\gamma^{3n}t^3 \equiv 0 \bmod \gamma^4$$

Mas como γ não divide ϵ nem t, pois pegamos a maior potência de γ na fatoração de ν, concluímos que γ^4 deve dividir γ^{3n}, o que só é possível se tivermos $n \geq 2$, como queríamos demonstrar.

4. Pela proposição 4.2, a equação 4.6 pode ser escrita como

$$(x + y)(x + \omega y)(x + \omega^2 y) = -u\gamma^{3n}z^3 = 0.$$

Como γ é primo em $\mathbb{Z}[\omega]$, e divide o lado direito da equação, ele deve dividir um dos fatores do lado esquerdo da equação. O que vamos mostrar agora é que se γ dividir um dos fatores, ele também dividirá os outros dois. Para isso, verificaremos as equivalências

$$\gamma|(x + y) \Leftrightarrow \gamma|(x + \omega y) \Leftrightarrow \gamma|(x + \omega^2 y)$$

- Suponha que $\gamma|(x + y)$, isto é, $(x + y) \equiv 0 \bmod \gamma$. Portanto,

$$\begin{aligned} x + \omega y &= x + wy + y - y \\ &= x + y + \omega y - y \\ &= x + y - y(1 - \omega) \\ &\equiv x + y \bmod \gamma \\ &\equiv 0 \bmod \gamma \\ &\Rightarrow x + \omega y \equiv 0 \bmod \gamma \end{aligned}$$

- Se $\gamma|(x + \omega y)$, então

$$\begin{aligned} x + \omega^2 y &= x + \omega(\omega y) \\ &= x + \omega(\omega y) + \omega y - \omega y \\ &= x + \omega y + \omega(\omega y) - \omega y \\ &= x + \omega y - \omega y(1 - \omega) \\ &\equiv 0 \mod \gamma \\ &\Rightarrow x + \omega^2 y \equiv 0 \mod \gamma \end{aligned}$$

- Finalmente, se $\gamma|(x + \omega^2 y)$:

$$\begin{aligned} x + y &= x + \omega^3 y \\ &= x + \omega(\omega^2 y) + \omega^2 y - \omega^2 y \\ &= x + \omega^2 y + \omega(\omega^2 y) - \omega^2 y \\ &= x + \omega^2 y - \omega^2 y(1 - \omega) \\ &\equiv 0 \mod \gamma \\ &\Rightarrow x + y \equiv 0 \mod \gamma \end{aligned}$$

Portanto, concluímos que γ divide os três fatores.

5. Pelo item anterior, como γ divide os três fatores, existem $y_1, y_2, y_3 \in \mathbb{Z}[\omega]$ tais que

$$(x + y) = y_1\gamma \ , \ (x + \omega y) = y_2\gamma \text{ e } (x + \omega^2 y) = y_3\gamma \tag{4.8}$$

Então a partir da solução da equação 4.3 e do lema 4.2, escrevemos:

$$\begin{aligned} \alpha^3 + \beta^3 &= -u^3\gamma^{3n}z^3 \\ (x + y)(x + \omega y)(x + \omega^2 y) &= -u^3\gamma^{3n}z^3 \\ y_1\gamma \cdot y_2\gamma \cdot y_3\gamma &= -u^3\gamma^{3n}z^3 \\ \gamma^3 \cdot y_1y_2y_3 &= -u^3\gamma^{3n}z^3 \\ y_1y_2y_3 &= \frac{-u^3\gamma^{3n}z^3}{\gamma^3} \\ y_1y_2y_3 &= -u^3\frac{\gamma^{3n}}{\gamma^3}z^3 \\ y_1y_2y_3 &= -u^3\gamma^{3n-3}z^3 \end{aligned}$$

Assim, $(y_1y_2y_3, u, z) \in \mathbb{Z}[\omega]^5$ é solução da equação 4.4.

Agora falta provar que y_1, y_2, y_3 são coprimos dois a dois. Para isso, suponha y_1 e y_2 não coprimos, então existe um elemento $a \in \mathbb{Z}[\omega]$ que divide ambos. Então pelas equações 4.8 temos

$$y_1 = \frac{x + y}{\gamma} \text{ e } a|y_1 \Rightarrow a \mid \frac{x + y}{\gamma}$$

e

$$y_2 = \frac{x+\omega y}{\gamma} \text{ e } a|y_2 \Rightarrow a \mid \frac{x+\omega y}{\gamma}$$

Se a divide os dois, ele também divide a diferença, logo

$$\begin{aligned} a \mid \left(\frac{x+y}{\gamma}\right) - \left(\frac{x+\omega y}{\gamma}\right) &\Rightarrow a \mid \left(\frac{x+y-x-\omega y}{\gamma}\right) \\ &\Rightarrow a \mid \frac{y-\omega y}{\gamma} \\ &\Rightarrow a \mid \frac{y(1-\omega)}{\gamma} \\ &\Rightarrow a \mid y \end{aligned}$$

Como $a \mid (x+y)$ e $a \mid y$ então $a|x$. Absurdo! Pois, pela demonstração do item 2, $x = \omega$, $y = \beta$ e mdc(x,y) = 1. Logo, y_1 e y_2 são coprimos.

Similarmente, supondo que $a|y_1$ e $a|y_3$, então $a \mid \frac{x+y}{\gamma}$ e $a \mid \frac{x+\omega^2 y}{\gamma}$. Segue daí que $a \mid \left(\frac{x+\omega^2 y-x-y}{\gamma}\right)$, ou seja, $a \mid (\omega+1)y$. Como $\omega+1$ é unidade, concluímos que $a|y$ e consequentemente $a|x$, contradizendo novamente a hipótese de que x e y são coprimos.

Finalmente, se $a|y_2$ e $a|y_3$, então $a \mid \frac{x+\omega y}{\gamma}$ e $a \mid \frac{x+\omega^2 y}{\gamma}$. Assim, $a| \left(\frac{x+\omega y-x-\omega^2 y}{\gamma}\right)$, isto é, $a \mid \omega y$. Mas ω é unidade, implicando que $a|y$ e segue também que $a|x$, de onde chegamos outra vez que numa contradição.

Logo y_1,y_2,y_3 são coprimos dois a dois.

6. Pelo item anterior, mdc(y_1,y_2)= mdc(y_1,y_3)= mdc(y_2,y_3)=1, portanto os $y_i's$ (i = 1,2,3) são coprimos dois a dois. Assim, por $\mathbb{Z}[\omega]$ ser um DFU, a fatoração é única e apenas um deles possui o fator γ^{3n_0-3}, pois se não, o mdc seria diferente de 1.

   Também pelo item anterior, temos que

$$y_1y_2y_3\gamma^3 = -u\gamma^{3n}z^3 \Rightarrow \gamma^{3n} \mid y_1y_2y_3\gamma^3 \Rightarrow \gamma^{3n-3} \mid y_1y_2y_3 \Rightarrow \gamma^{3n-3} \mid y_i$$

   para algum i.

   Sem perda de generalidade, podemos supor que $\gamma^{3n-3} \mid y_1$. Escolhendo n_0 como o menor inteiro que satisfaz essa condição e fatorando y_1,y_2 e y_3 temos

$$\begin{aligned} y_1 &= \epsilon_1\gamma^{3n_0-3}t_1^3 \\ y_2 &= \epsilon_2 t_2^3 \\ y_3 &= \epsilon_3 t_3^3 \end{aligned}$$

   onde ϵ_i com $i \in \{1,2,3\}$ são unidades de $\mathbb{Z}[\omega]$ e t_i com $i \in \{1,2,3\}$ são elementos de $\mathbb{Z}[\omega]$, os quais são coprimos dois a dois e nenhum é divisível por γ.

7. Observe que

$$\begin{aligned} y_1 + \omega y_2 + \omega^2 y_3 &= \frac{x+y}{\gamma} + \omega\frac{x+\omega y}{\gamma} + \omega^2\frac{x+\omega^2 y}{\gamma} \\ &= \frac{x(1+\omega+\omega^2) + y(1+\omega+\omega^2)}{\gamma} \\ &= 0 \end{aligned}$$

e assim, fazendo as substituições do item 6 temos

$$\omega^2\epsilon_3 t_3^3 + \omega\epsilon_2 t_2^3 + \epsilon_1\gamma^{3n_0-3}t_1^3 = 0$$

Como ω é unidade, podemos dividir por ω^2:

$$\frac{\omega^2\epsilon_3 t_3^3}{\omega^2} + \frac{\omega\epsilon_2 t_2^3}{\omega^2} + \frac{\epsilon_1\gamma^{3n_0-3}t_1^3}{\gamma^2} = \frac{0}{\omega^2}$$

Como ϵ_3 é unidade, também podemos dividir por ϵ_3. Daí, a equação ficará:

$$t_3^3 + \frac{\epsilon_2 t_2^3}{\omega\epsilon_3} + \frac{\epsilon_1\gamma^{3n_0-3}t_1^3}{\omega^2\epsilon_3} = 0$$

Note que $\frac{\epsilon_2}{\omega\epsilon_3} = \epsilon_2(\omega\epsilon_3)^{-1}$ e $\frac{\epsilon_1}{\omega^2\epsilon_3} = \epsilon_1(\omega^2\epsilon_3)^{-1}$ são unidades de $\mathbb{Z}[\omega]$ e, fazendo $\epsilon_2(\omega\epsilon_3)^{-1} = \epsilon_4$ e $\epsilon_1(\omega^2\epsilon_3)^{-1} = \epsilon_5$ temos:

$$t_3^3 + \epsilon_4 t_2^3 + \epsilon_5\gamma^{3n_0-3}t_1^3 = 0$$

Passando a equação acima mod γ^4 temos que $\epsilon_4 \in \{1, -1, \omega, -\omega, \omega^2, -\omega^2\}$, as únicas unidades existentes.

Fazendo uma substituição direta, temos que $\epsilon_4 \in \{1, -1\}$ e assim achamos uma solução da equação 4.3 e como $3n_0 - 3 < 3n_0$ temos um absurdo pela escolha do n_0.

□

Logo, provamos o seguinte teorema

Teorema 4.3: A equação diofantina:

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

não possui solução $(x,y,z) \in \mathbb{Z}^3$ tais que $x,y,z \neq 0$ e $x,y,z \in \mathbb{Z}$.

Essa demonstração é muito interessante, ao passo que não utilizamos ferramentas intrínsecas da teoria dos números, mas sim, de álgebra abstrata. Essa ligação entre as teorias, torna a Matemática uma ciência muito interessante, podendo o pesquisador, caminhar em várias áreas para a solução de um problema.

4.4 Uma aplicação do teorema

Saber aplicar conceitos matemáticos é muito importante. Isto facilita a compreensão dos alunos de escola básica, além de mostrar a importância do conteúdo. Podemos apresentar para um aluno do Ensino Médio o Último Teorema de Fermat, já que este aluno conhece o Teorema de Pitágoras e pode se perguntar se há possibilidade de alterar os expoentes de 2 para outro n inteiro. Não há necessidade de demonstrar, mas o conhecimento de sua existência já possibilita um olhar diferenciado para a aritmética.

Pensando numa aplicação do Último Teorema de Fermat para ser levada às escolas de ensino básico, podemos utilizar a demonstração que $\sqrt[3]{2}$ é irracional. Vejamos:

Exemplo 4.4.1: Supondo que $\sqrt[3]{2}$ seja racional, temos que $\sqrt[3]{2} = \frac{a}{b}$. Elevando a 3 os dois lados, temos: $(\sqrt[3]{2})^3 = (\frac{a}{b})^3 \Rightarrow 2 = \frac{a^3}{b^3} \Rightarrow a^3 = 2b^3 \Rightarrow a^3 = b^3 + b^3$ Absurdo! Pois, como demonstrado neste trabalho, a último igualdade não possui solução. Com isso, concluímos que $\sqrt[3]{2}$ é irracional.

Esse argumento pode ser generalizado.

Teorema 4.4: $\sqrt[n]{2}$ é irracional.

Demonstração. Suponhamos que $\sqrt[n]{2}$ seja racional. Logo $\sqrt[n]{2} = \frac{p}{q}$, com p,$q \in \mathbb{Z}$, $q \neq 0$ e $n > 2$.

Elevando ambos os lado à n-ésima potência e desenvolvendo a igualdade, obtemos:

$$\begin{aligned} \left(\sqrt[n]{2}\right)^n &= \left(\frac{p}{q}\right)^n \\ 2 &= \frac{p^n}{q^n} \\ p^n &= 2q^n \\ p^n &= q^n + q^n \end{aligned}$$

Mas a última igualdade contradiz o Último Teorema de Fermat. Logo, $\sqrt[n]{2}$ é irracional. □

D'Ambrósio em [4], aborda a prática matemática em sala de aula e cita o Último Teorema de Fermat como uma das possibilidades. Para ele, pesquisa é o elo entre a teoria e a prática e deve-se explorar essa matemática experimental no ensino básico. Ele cita que esse caráter experimental da matemática foi removido do ensino e que esse pode ser um dos fatores que contribuíram para o mau rendimento escolar. Ainda assim, cabe ao professor mudar essa realidade, buscando uma formação continuada e seu aprimoramento profissional, tornando a experimentação parte fundamental das aulas, principalmente as de matemática que atualmente são muito mecânicas.

Apresentar esse teorema para alunos do ensino básico é de suma importância, visto que, há ainda um tabu em relação à disciplina e, para a maior parte dos

indivíduos, o estudo da matemática é visto como ciência exata e perfeita. Além disso, nós como professores de matemática, temos o papel de apresentá-la de uma forma instigante, aguçando o interesse dos alunos pela disciplina e pela pesquisa.

5

Andrew Wiles e a solução do teorema

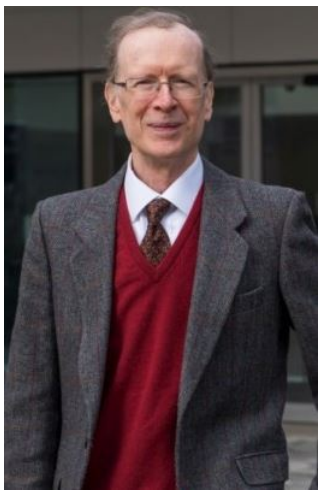


Figura 5.1: Imagem de Andrew Wiles

Nascido em 11 de Abril de 1953 em Cambridge, Inglaterra, Andrew Wiles tornou-se PhD em matemática pela Universidade de Cambridge (1975-1979) orientado pelo australiano John Coates. Andrew Wiles foi professor em Princeton, consagrou como matemático a partir dos anos 80, através da sua demonstração (1995) quando apresentou o mais célebre desafio matemático do tempo, o Teorema de Fermat:

> *"Considerando a equação $x^n + y^n = z^n$, Fermat afirmou que não existem valores inteiros para x,y e z que satisfaçam a equação quando n for um número inteiro maior do que 2. As possíveis provas de Fermat perderam-se e a demonstração deste teorema tornou-se um dos desafios mais famosos da história da matemática, enfrentado pela maioria dos matemáticos por mais de três séculos." (SALVADOR, 2014.86p)*

Após sete anos de trabalho, no dia 23 de junho de 1993, o matemático Andrew Wiles divulga, durante a conferência do *Sir Isaac Newton Institute for Mathematical Sciences* em Cambridge, que havia encontrado uma demonstração para o desafio.

Entretanto, logo em seguida, foi constatada uma pequena falha, que levou Wiles a se retirar por um período de mais de um ano e, por fim retornar com a demonstração reformulada.

Em 1995, posteriormente há vários meses de apreciação das 200 páginas, a sua demonstração é fatalmente aceita. Tratava-se de uma demonstração de forma técnica que somente alguns grupos de matemáticos no universo apresentariam qualidades para seguir o raciocínio. Wiles recebeu a consagração definitiva e 50.000 libras como recompensa da Fundação Wolfskehl pelo feito.

Em 1963, quando tinha dez anos de idade, Wiles retornava para casa e resolveu entrar na biblioteca da Rua Milton, uma pequena biblioteca, que tinha uma excelente coleção de livros sobre enigmas; e foi atraído por um livro que tinha apenas um problema, mas sem solução. O livro era "O Último Problema", de Eric Temple Bell, onde apresentava a história de um problema matemático de origem grega, que até então, nenhum matemático conseguira demonstrá-lo.

A partir daí, Wiles passou a infância e o período de vida acadêmica tentando descobrir a solução para tal desafio. Wiles teve que abdicar por um determinado tempo o seu sonho:

> *"Quando fui para Cambridge eu realmente tive que deixar Fermat de lado. Não é que o tivesse esquecido, ele estava sempre lá – mas percebi que as únicas técnicas para se lidar com o problema tinham* 130 *anos de idade. E não me parecia que estas técnicas estavam chegando à raiz. O risco de se trabalhar com Fermat era que se poderia passar anos sem chegar à parte alguma. É ótimo trabalhar em qualquer problema desde que ele gere uma Matemática interessante ao longo do caminho – mesmo que não consiga resolvê-lo ao final da vida. A definição de um bom problema de Matemática reside na Matemática que ele produz, não no problema em si." (SALVADOR, – 2014).*

John Coates estava com a responsabilidade de encontrar nova obsessão para Andrew, qualquer coisa que chamasse a atenção e ocupasse seu tempo com as pesquisas por mais uns três anos.

> *"Eu creio que tudo que um supervisor de pesquisa pode fazer por um estudante é tentar empurrá-lo numa direção de pesquisa frutífera. É claro que é impossível ter certeza do que será uma direção frutífera em termos de pesquisa, mas talvez algo que um experiente matemático pode fazer é usar seu senso prático, sua intuição do que seja uma boa área e então dependerá só do estudante decidir até onde ele pode ir naquela direção." (SALVADOR, – 2014).*

Finalmente, Coates decidiu que Wiles precisava estudar uma área da Matemática acerca das curvas elípticas. De modo que a determinação seria para evidenciar um ponto essencial na carreira de Wiles e ao mesmo tempo lhe proporcionaria as tecnologias indispensáveis para abordar o Último Teorema de Fermat. A denominação "curvas elípticas" é de certa forma enganadora porque não são elipses e não são

encurvadas no significado habitual da expressão. Elas ganharam esta nomenclatura visto que no transpor dos tempos eram utilizadas para medir o perímetro de elipses e a dimensão das órbitas planetárias, onde iremos mencionar como equações elípticas no lugar de curvas elípticas:

> *" O desafio com as equações elípticas assim como no caso do Último Teorema de Fermat é determinar se elas possuem soluções para números inteiros, e se assim for, quantas. Por exemplo, a equação elíptica tem apenas um conjunto finito de soluções para números inteiros, a saber. Simplesmente, mudando-se os valores de n em uma equação elíptica geral, os matemáticos podem gerar uma variedade de equações, cada uma com suas características próprias, mas todas elas possíveis de serem solucionadas. As equações elípticas foram originalmente estudadas pelos antigos matemáticos gregos, incluindo Diofante, que dedicou uma grande parte de sua Aritmética ao estudo de suas propriedades. Provavelmente inspirado por Diofante, Fermat também aceitou o desafio de estudar as equações elípticas. Como elas tinham sido estudadas por seu herói, Wiles ficou feliz em explorá-las ainda mais."(SALVADOR, – 2014).*

Após 2000 anos as equações elípticas ainda eram causa de grandes problemas para estudiosos. Wiles disse:

> *"Ainda estamos longe de entendê-las completamente. Eu poderia apresentar muitas perguntas aparentemente simples sobre equações elípticas que ainda não foram respondidas; inclusive, perguntas que o próprio Fermat considerou, ainda não possuem respostas. De certo modo, toda a Matemática que eu fiz tem suas origens em Fermat, se não, no Último Teorema de Fermat."*

Wiles estudou as equações durante a graduação, ele coloca que a resolução do número exato era tão difícil que o único modo de fazer algum progresso era simplificar o problema, como por exemplo, usando o que os matemáticos chamam de aritmética modular.

5.1 O erro encontrado

Há relatos que em 23 de agosto de 1993, foi detectado por Katz, um erro crucial envolvendo a metodologia de Kolyvagin-Flach, porém foi um tanto sutil que Katz não havia notado até o presente momento.

É evidente que mesmo com o erro, Andrew dera um grande passo. Antes dele, ninguém havia conseguido abordar a conjectura de Taniyama-Shimura e agora todos estavam empolgados pois ele mostrou muitas ideias novas; havia coisas novas, fundamentais, que ninguém tinha considerado antes. Mesmo que a demonstração não pudesse ser consertada, ela já era um grande avanço na matemática.

A esposa de Wiles, relatou que o único presente de aniversário que ela almejava, era que Wiles apresentasse a demonstração concluída. Devido a esse pedido, Wiles

foi para um isolamento e não fez nenhum manifesto a propósito do pedido da esposa, também nenhum dos examinadores se manifestaram, pois havia muita pressão a respeito da liberação dos manuscritos. Peter Sarnak, matemático e amigo confidente de Wiles, indagava: "Sabe que há uma tempestade lá fora?" Mas Wiles seguia desligado de tudo procurando se concentrar apenas na resolução do problema.

5.2 A demonstração correta

Após algum tempo sem sucesso trabalhando na demonstração do teorema, Wiles convidou Richard Taylor, um professor de Cambridge, para vir a Princeton trabalhar com ele na prova do teorema. Taylor era um dos avaliadores da demonstração e um ex-aluno de Wiles, sendo, portanto, de confiança. No ano anterior ele estivera na plateia do Instituto Isaac Newton vendo seu supervisor apresentar a demonstração do século. Agora era seu trabalho ajudar a resgatar a prova defeituosa.

Wiles e Taylor trabalharam um ano e dois meses, posteriormente à divulgação da demonstração. Wiles deu de presente de aniversário para sua esposa a prova do Último Teorema de Fermat, devido a mesma ser a única que tinha conhecimento do maior sonho de Wiles.

Andrew Wiles arrastou por oito anos de absoluto esforço e estudo para demonstrar o Último Teorema de Fermat, divulgado em 1995, atingindo assim, o término do mistério que persistira por três séculos e meios. Finalmente foi oficialmente provado o Último Teorema de Fermat. Nos termos de Wiles:

> *"Eu tive o raro privilégio de conquistar, em minha vida adulta, o que fora o sonho da minha infância. Sei que este é um privilégio raro, mas se você puder trabalhar, como adulto, com algo que significa tanto para você, isto será mais compensador do que qualquer coisa imaginável. Tendo resolvido este problema, existe certo sentimento de perda, mas ao mesmo tempo há uma tremenda sensação de liberdade. Eu fiquei tão obcecado por este problema durante oito anos, pensava nele o tempo todo quando acordava de manhã e quando ia dormir de noite. Isto é um tempo muito longo pensando só em uma coisa. Esta odisséia particular agora acabou. Minha mente pode repousar", (SALVADOR, – 2014).*

5.3 Prêmios que ganhou devido à demonstração

A demonstração do teorema rendeu ao matemático não apenas fama, mas também prêmios importantes na área, os quais incluem o Prêmio Real da Sociedade Real, o Prêmio de Matemática da Academia Nacional das Ciências dos EUA, o Prêmio Rolf Schock, o Prêmio Ostrowski, o Prêmio Wolf (50.000 libras), a Medalha Real da Sociedade Real, e o Prêmio Shaw. Além disso, com o prêmio Abel, concedido anualmente, Wiles recebeu 6 milhões de coroas norueguesas (700 mil dólares), valor também comparável ao do Nobel - tanto em remuneração financeira quanto em prestígio.

A União Internacional de Matemática presenteou-lhe com uma placa de prata, um acontecimento inédito. Ele foi agraciado com o primeiro Prêmio Clay de Investigação.

Em 2000, recebeu o título de cavaleiro.

Segundo um comunicado da Academia de Ciências da Noruega, que concede o Prêmio Abel:

> *"Andrew J. Wiles é um dos poucos matemáticos - se não o único - cuja prova de um teorema foi parar nas manchetes internacionais. Quando ele solucionou o último teorema de Fermat em 1995, esse era o mais famoso e mais antigo problema em aberto na história da matemática."*

5.3.1 Medalha Fiels

A medalha Fields, conferida pela União Internacional de Matemática (IMU), é contemplada como a grande honra recebida por um matemático. Assim sendo, é continuamente comparada ao prêmio Nobel. Entretanto a Fields tem uma particularidade: é uma premiação feita somente para os matemáticos com até 40 anos.

Infelizmente, Wiles estava com 41 anos, na data em que apresentou a prova final e, por estar acima da idade padronizada, o matemático não pôde receber o prêmio.

Em 2014 o Brasil apresentou em alto grau motivos para festejar: Artur Ávila, que pesquisa na área de Sistemas Dinâmicos, foi o primeiro brasileiro agraciado na história do prêmio (que começou em 1936). Isso não é pouco, é o maior prêmio já conquistado por um cientista brasileiro.

6

Considerações finais

Neste trabalho demonstramos que não existem soluções inteiras para a equação $x^n + y^n = z^n$ para $n = 3$ e $n = 4$, com x,y,$z \neq 0$. Durante anos, muitos matemáticos tentaram demonstrar o caso geral deste teorema ou provar sua inconsistência. Embora esses esforços tenham terminado em "fracasso", eles levaram à criação do maravilhoso arsenal de ferramentas e técnicas matemáticas que foram vitais para as últimas tentativas de se conseguir uma demonstração e, que hoje, são usadas nas mais diversas áreas da matemática.

Ao final, foi possível compreender a importância do Último Teorema de Fermat para a matemática e sua história. Em meio a procura de uma solução para o mesmo, foram criadas várias teorias que expandiram o meio matemático. Suas demonstrações para casos específicos usam conceitos diversos, e, como visto neste trabalho, pode-se demonstrar o mesmo caso usando diferentes ferramentas matemáticas. Para o caso em que $n = 3$ por exemplo, vimos aqui, uma demonstração usando ferramentas da teoria dos números e outra usando álgebra abstrata. Ainda assim, a demonstração geral, feita por Andrew Wiles, usa conceitos que a princípio não possuem nenhuma relação com o teorema citado. Isso reforça a ideia de que um matemático pesquisador pode caminhar em várias áreas para a solução de um problema.

Wiles, após longos anos de estudo, adentrou para a história da matemática e conseguiu provar o teorema mais excitante e desafiador da história da matemática, que sobreviveu a muitas épocas e encheu a mente de ilustres matemáticos ao decorrer desse período.

Considerando o estudo como um todo, o mesmo apresenta uma referência a mais ao aprofundar o estudo na teoria dos números e principalmente na teoria de anéis. Apesar das dificuldades encontradas em meio às demonstrações, posso afirmar que esse tema teve uma importância significativa em minha formação acadêmica.

Com o aprendizado aqui adquirido, foi possível perceber que há muito por trás daquilo que chega pronto aos estudantes e reforça a importância da pesquisa no meio acadêmico para entender os conceitos que existem por trás do problema. A dificuldade para chegar na solução de um problema, vai muito além das habilidades individuais, como é implantado em nossa mente em sala de aula. Há conceitos triviais que podem auxiliar bastante na compreensão e não terem sido passado para os alunos

ou como aqui visto, a teoria para sua resolução, pode nem ter sido criada.

É necessário aguçar a curiosidade dos alunos levando-os à compreensão do conteúdo e ao conhecimento eficiente e perdurável, despertando assim, e interesse dos mesmos, tirando aquele peso de que a matemática é difícil. A aplicação do Último Teorema de Fermat em sala de aula, como aqui assinalado, pode ser um bom caminho para isso.

Finalizo na esperança que este estudo contribua para motivar outros acadêmicos a desenvolverem pesquisas, reforçando relações em meio aos mais diferentes ramos da matemática.

Bibliografia

[1] BOSTON, Nigel. *THE PROOF OF FERMAT'S LAST THEOREM*. University of Wisconsin - Madison. Spring, 2003.

[2] BOYER, Carl B. *História da matemática*. Tradução de Elza F. Gomide. 2. ed. São Paulo: Edgard Blucher, 1996. BOYER, Carl B. História da matemática.

[3] CASTRO, Isabela Souza. *O último teorema de Fermat nos ensinos fundamental e médio*. Dissertação de Mestrado. Universidade Federal de Viçosa - *Campus* Florestal. Florestal, 2019.

[4] D'AMBRÓSIO, Ubiratam. *Educação matemática: Da teoria à prática*. 17ª ed. Campinas, SP: Papirus, 1996.

[5] DIAS, Olavo Gustavo Wagner Gonçalves. *Do Teorema de Pitágoras ao Ultimo Teorema de Fermat: Um resgate histórico e uma proposta de aplicação no Ensino Básico*. Joevile, 2018.

[6] Fermat's Last Theorem. Disponível em: http://en.wikipedia.org/wiki/Fermat's_Last_Theorem. Acesso em setembro de 2019.

[7] GARBI, Gilberto Geraldo. *A Rainha das Ciências: um passeio histórico pelo maravilhoso mundo da matemática*. Editora Livraria da Física, 2006.

[8] GONÇALVES, Adilson. Introdução à álgebra. Impa, 1979.

[9] HEFEZ, Abramo. *Aritmética*. 2ª ed. Rio de Janeiro: SBM, 2016.

[10] MARQUES, Cristina Maria. *Introdução à teoria dos números*. Departamento de Matemática-UFMG, 1999.

[11] MARTINEZ,Fabio Brochero et al. *Teoria dos números: um passeio com primos e outros números familiares pelo mundo inteiro*. 2ª ed. Rio de Janeiro: IMPA, 2011.

[12] MAZZA, Jose Luiz. *O Último Teorema de Fermat: a trajetória histórica do "enigma"*. Disponível em: https://www.ime.unicamp.br/~ftorres/ENSINO/MONOGRAFIAS/Mazza_M1_FM_2014.pdf. Acesso em agosto 2019.

[13] Roque, T. e Carvalho, J. B. P. de. *Tópicos de História da Matemática*. 1ª Ed. Coleção Profmat. SBM, 2012.

[14] SING, Simon. *O Último teorema de Fermat: A história que cofundiu as maiores mentes durante 358 anos.*; tradução de Jorge Luiz Calife. - 13ª ed. - Rio de Janeiro: Record, 2008.

[15] SINGH, Simon. *O Último Teorema de Fermat*, Notas de estudo de Engenharia de Produção. Disponível em: https://www.docsity.com/pt/o-ultimo-teorema-de-fermat-simon-singh/4905427/. Acesso em Agosto de 2019.

[16] Último Teorema de Fermat. Disponível em: https://www.infoescola.com/matematica/ultimo-teorema-de-fermat/. Acesso em setembro de 2019.