UNIVERSIDADE ESTADUAL DE MARINGÁ
CENTRO DE CIÊNCIAS EXATAS
DEPARTAMENTO DE MATEMÁTICA
MESTRADO PROFISSIONAL EM MATEMÁTICA EM REDE NACIONAL

Sobre Números Irracionais

MAISA CARLA GIMENEZ
Orientador: Marcos Roberto Teixeira Primo

Maringá - PR
2021

Sobre Números Irracionais

MAISA CARLA GIMENEZ

Dissertação apresentada ao Programa de Mestrado Profissional em Matemática em Rede Nacional do Departamento de Matemática, Centro de Ciências Exatas da Universidade Estadual de Maringá, como requisito parcial para obtenção do título de Mestre em Matemática.

Orientador: Prof. Dr. Marcos Roberto Teixeira Primo

Maringá - PR
2021

Dissertação apresentada ao Programa de Mestrado Profissional em Matemática em Rede Nacional do Departamento de Matemática, Centro de Ciências Exatas da Universidade Estadual de Maringá, como requisito parcial para obtenção do título de Mestre em Matemática.

BANCA EXAMINADORA

Prof. Dr. Marcos Roberto Teixeira Primo
Universidade Estadual de Maringá

Profa. Dra. Claudete Matilde Webler Martins
Universidade Estadual de Maringá

Profa. Dra. Mariza Stefanello Simsen
Universidade Federal de Itajubá

Maringá, 24 de Fevereiro de 2021.

Dados Internacionais de Catalogação na Publicação (CIP)
(Biblioteca Setorial BSE-DMA-UEM, Maringá, PR, Brasil)

Gimenez, Maisa Carla
G491s Sobre números irracionais / Maisa Carla Gimenez. -- Maringá, 2021.
81 f. : il., color.

Orientador: Prof. Dr. Marcos Roberto Teixeira Primo.
Dissertação (mestrado) - Universidade Estadual de Maringá, Centro de Ciências Exatas, Departamento de Matemática, 2021.

1. Números irracionais. 2. Teoria analítica dos números. I. Primo, Marcos Roberto Teixeira, orient. II. Universidade Estadual de Maringá. Centro de Ciências Exatas. Programa de Mestrado Profissional em Matemática em Rede Nacional - PROFMAT. III. Título.

CDD 22.ed. 512.73

Edilson Damasio CRB9-1.123

Agradecimentos

Agradeço ao meu professor e orientador Marcos e a professora Luciene, pelos momentos de conselho, atenção e direcionamento para concluir este trabalho, ao meu noivo e as minhas amigas Francielly, Mariana, e Thialine que me ajudaram principalmente dando ânimo nos momentos de dificuldade. Agradeço também a minha família pelo suporte que sempre deu para que eu conseguisse meus objetivos e também a todos os meus professores que ministraram aula neste programa e que de certa forma contribuíram nessa caminhada.

Sumário

Resumo

No presente trabalho temos como objetivo principal apresentar o conceito de números irracionais, mais especificamente os números irracionais da forma $\sqrt{n}$, com $n \in \mathbb{N}$. Mostraremos que um número do tipo $\sqrt{n}$, com $n \in \mathbb{N}$, é um irracional ou inteiro de forma algébrica, utilizando a teoria dos números. Além disso, para os números primos $2, 3$ e 5 mostraremos este resultado também de forma geométrica.

Abstract

In this work we have as main objective to present the concept of irrational numbers, more specifically the irrational numbers of the form $\sqrt{n}$, with $n \in \mathbb{N}$. We will show that a number of type $\sqrt{n}$, with $n \in \mathbb{N}$, is an irrational or integer in algebraic form, using a theory of numbers. In addition, for prime numbers $2, 3$ and 5 we will show this result in a geometric form as well.

Introdução

Os números irracionais, de acordo com os Parâmetros Curriculares Nacionais (PCN), devem ser abordados no 4º ciclo, equivalente hoje ao 8º ou 9º ano do Ensino Fundamental. No entanto, ensiná-lo de maneira simples, de modo que, para os alunos não seja um conteúdo complicado não é uma tarefa fácil, uma vez que para entender os números irracionais é preciso imaginar processos infinitos e proximidades que tendem a zero. Os PCN sugerem, ao abordar o conteúdo de números irracionais, não seguir por um caminho formal e ressalta a importância de discutir sobre a notação decimal infinita e não periódica, a aproximação por números racionais além de discutir a necessidade e as consequências do arredondamento de um número com infinitas casas decimais. Já a Base Nacional Comum Curricular (BNCC) converge com algumas recomendações dos PCN e em sua segunda versão orientava "é necessário ter cautela para a construção dos números irracionais e reais, pois os/as estudantes do 9º ano, de maneira geral, ainda não têm maturidade suficiente para essa aprendizagem de forma significativa"(BNCC, 2016, p. 425). De fato, os erros mais comuns por parte dos alunos vão desde a definição de números irracionais quando os definem como números que possuem reticências, até a representação equivocada ao escreverem $\pi = 3,14$, $e = 2,71$ ou $\sqrt{2} = 1,4$, por exemplo.

Com base nessas dificuldades em relação a tais números, a presente dissertação tem como principal objetivo a verificação da irracionalidade dos números da forma raiz quadrada de n, com n um número natural, a partir do uso de calculadora com alunos dos anos finais do ensino fundamental, além de apresentar demonstrações geométricas da irracionalidade de alguns casos particulares desses números, que são menos abstratas e de mais fácil compreensão, e ainda, da irracionalidade da constante matemática e, um pouco mais detalhada, seguindo os passos de demonstração conforme Djairo G. de Figueiredo em *Números Irracionais e Transcendentes*, ([6]).

Para atingirmos tais obejtivos, nosso projeto será estruturado da seguinte forma: O primeiro capítulo se debruça sobre o estudo da lógica proposicional, a fim de lançar as bases da demonstração

do teorema que trabalharemos ao longo de nosso estudo. Nossa ideia inicial se pauta, justamente, no uso da calculadora como forma dos alunos do ensino fundamental aplicarem o teorema de uma forma mais concreta e, possivelmente, passível de ser entendida. Ora, é perceptível a dificuldade que os alunos, de todos os anos, encontram de frente à matemática, pois estamos falando de uma área com conceitos exatos, fórmulas a serem aplicadas e nem sempre é fácil, aos discentes, a compreensão desses termos. Por isso escolhemos a calculadora como um instrumento facilitador da aprendizagem. Desse modo, nosso objetivo se pauta na demonstração do teorema pela calculadora, porém, antes desse passo, faz-se necessário a explicação e o lançar mão das bases que o constrói. Por esse motivo, tal primeiro capítulo se pauta nas linguagens lógica e matemática com a perspectiva de tornar essa linguagem, de alguma maneira, mais compreensível, fato necessário quando se trata de uma busca como a nossa: a de cativar alunos do ensino fundamental através de mecanismos de demonstrações mais fáceis.

O segundo capítulo mostra o desenvolvimento e as bases do teorema que pode ser apresentado aos alunos do Ensino Básico, isto é, nele se encontram as propriedades que serão usadas na demonstração algébrica do teorema. Esse passo dado na segunda parte de nosso estudo dialoga com o que é proposto no início da dissertação, pois se no primeiro passo mostramos a contrapositiva como uma das formas de demonstração de uma implicação do tipo "se p, então q", nosso segundo objetivo é adentrar mais nas definições fundamentais para a compreensão do teorema, sua demonstração e de suas aplicações. Os conceitos que serão estudados neste capítulo são frequentemente utilizados no Ensino Básico, porém a abordagem será feita com o devido rigor matemático.

No tocante ao terceiro capítulo falamos sobre os números irracionais, afinal, é importante ao teorema aqui trabalhado explicarmos o conceito desses números, além de demonstrar a irracionalidade de alguns deles, em especial do número e que é bastante utilizado em cálculos sobre juros, funções logarítmicas e exponenciais. Estará aqui não somente o conceito de número irracional, mas também a demonstração algébrica desse teorema. É importante ressaltar que na ordem estrutural do projeto, se no primeiro capítulo falamos sobre lógica e contrapositiva como método de demonstração, levantando a hipótese do teorema ser apresentado de outras formas e no segundo capítulo apresentamos as propriedades a serem usadas nessa demonstração, então em nossa sequência argumentativa o terceiro capítulo mostra de fato o teorema e sua construção, que será demonstrado nas formas citadas acima. Ainda neste capítulo abordaremos de forma sucinta a classificação dos números reais em algébricos e transcendentes a fim de observarmos que a transcendência de um número garante sua irracionalidade,

porém, saber se um dado número é transcendente, é, em geral, uma questão muito difícil e em relação a transcendência de e, sabe-se esta foi um desafio aos matemáticos até o século XIX. Desta forma, por conter cálculos que demandam conhecimentos um pouco além da matemática do Ensino Fundamental e Médio, optamos por ocultá-la e concluir sua irracionalidade demonstrando-a passo a passo.

No quarto e último capítulo damos continuidade ao estudo dos irracionais da forma raiz quadrada de um número natural $n \in \mathbb{N}$, fornecendo demonstrações geométricas de irracionalidade, agora, a dos números $\sqrt{2}, \sqrt{3}$ e $\sqrt{5}$ seguindo a mesma ideia da demonstração do teorema principal do terceiro capítulo, porém de modo a torná-la mais visual e consequentemente mais "palpável", sendo portanto mais fáceis de serem compreendidas por alunos do ensino fundamental e médio.

Capítulo 1

Lógica Proposicional

O presente capítulo tem como objetivo apresentar a lógica informal para o leitor, tendo em vista que suas bases serão usadas para exemplificar o teorema presente no final de nossa dissertação. Pois, visamos demonstrar que se n não é um quadrado perfeito então sua raiz quadrada é um número irracional. Para tal feito usaremos a contra-positiva, presente na lógica, como método de demonstração. A fim de nos auxiliar nos termos lógicos, usaremos como referência as páginas iniciais do livro *Um Convite à Matemática*, de Daniel Cordeiro de Morais Filho e do *Fundamentos de Matemática: uma introdução à lógica matemática, teoria dos conjuntos, relações e funções*, de João Roberto Gerônimo e Valdeni Soliani Franco, veja [7] e [9].

1.1 Sentenças, Sentenças Abertas e Quantificadores

É possível sentir, na área da matemática, a dificuldade de expressar seus resultados de forma clara e concisa. Sua linguagem não permite ambiguidades, assim como também não se faz uso de certas formas de comunicação da língua corrente, a exemplo: ironia ou metáforas. Embora nossa linguagem falada e escrita se comporte de uma forma específica, ao tentar explicar a matemática a partir desses princípios, por vezes esbarramos na dificuldade de conseguir transportar uma expressão numérica para termos comuns e do dia-a-dia dos indivíduos.

> No dia a dia, quando alguém diz a frase: "Estou chegando num minuto!!!" significa que ela vai chegar em pouco tempo. Já na Matemática, um minuto representa um minuto mesmo, 60 segundos. Matematicamente, essa pessoa não pode levar nenhum segundo a mais nem a menos para chegar. Felizmente, podemos ficar tranquilos, ninguém no dia a dia é obrigado a interpretar matematicamente a frase anterior.
> De um simples exemplo, já é possível perceber que na Matemática as mensagens devem ser expressas com a linguagem e os cuidados específicos, muitas vezes, diferentes daqueles que estamos acostumados a usar e a interpretar na linguagem coloquial.[1]

Vejamos como isso é feito.

Definição 1.1. *Chamamos* ***frase*** *a um conjunto de palavras ou de símbolos matemáticos, incluindo os sinais de acentuação e pontuação, que se relacionam para comunicar uma ideia.*

Definição 1.2. *Uma* ***sentença matemática*** *ou* ***proposição*** *é uma frase, expressa em linguagem matemática, podendo conter apenas símbolos matemáticos, que cumpre as condições:*

(1) Apresenta-se estruturada como uma oração, com sujeito e predicado, incluindo o verbo.

(2) É afirmativa declarativa (não é interrogativa, nem exclamativa).

(3) Satisfaz os seguintes princípios:

(3.1) Princípio da Identidade: uma sentença é igual a si mesma.

(3.2) Princípio do Terceiro Excluído: uma sentença é falsa ou verdadeira, excluindo-se uma terceira alternativa.

(3.3) Princípio da Não-Contradição: uma sentença não pode ser falsa e verdadeira ao mesmo tempo, não podendo contradizer-se.

Exemplo 1.3. *Considere as frases:*

P_1 : *A soma das medidas dos ângulos internos de um triângulo no plano é cento e oitenta graus.*

P_2 : *O número* 87 *não é maior do que ou igual a* 85^2.

P_3 : $\sqrt{2} \notin \mathbb{N}$.

P_4 : *Todo número par é divisível por 3.*

[1] FILHO, Daniel de Cordeiro de Morais. *Um Convite à Matemática.* Rio de Janeiro, 2013, p.28.

P_5 : *O Brasil é o maior país da América Latina.*

Observe que todas as frases acima são sentenças, pois elas satisfazem as condições (1), (2) e (3) da Definição 1.2. Apenas P_5 não é uma **sentença matemática**, pois nela não aparecem objetos matemáticos.

Segundo a Definição 1.2 toda sentença é ou verdadeira ou falsa, porque não há uma terceira opção, e porque ela não pode ser falsa e verdadeira ao mesmo tempo. Por isso, a lógica aqui utilizada chama-se **Lógica Bivalente**.

O valor lógico de uma sentença é dito **verdadeiro** quando a sentença for verdadeira, e **falso**, caso contrário. Assim, segue do item (3) da Definição 1.2 que toda sentença está associada a um único valor lógico: falso ou verdadeiro. Observe que o valor lógico das sentenças P_1, P_2, P_3 e P_5 é verdadeiro e da sentença P_4 é falso.

Um dos objetivos da Matemática é descobrir e provar se certas sentenças são falsas ou verdadeiras. Já a Lógica Formal visa estudar as relações entre sentenças, sem se preocupar com o conteúdo ou em determinar os valores lógicos das sentenças.

Vejamos, agora, exemplos que parecem ser sentenças matemáticas:

(a) $\frac{1}{9} + 9$

(b) $10^9 > 9^{10}$?

(c) $2x + 6 = 3$

O item (a) não está estruturado como uma sentença, pois não cumpre a condição de possuir verbo e predicado, além de não haver afirmação alguma nela. Para torná-la uma sentença matemática, temos que completá-la, por exemplo, como

$$\frac{1}{9} + 9 = \frac{82}{9}.$$

Agora, a frase é uma sentença matemática, pois é uma afirmação que possui um sujeito (um nono mais nove), verbo e predicado (é igual a oitenta e dois nonos) e não contraria nenhum dos três princípios fundamentais.

Já no item (b) não existe uma afirmação e sim uma interrogação. Para torná-la uma sentença matemática devemos, apenas, retirar o ponto de interrogação, visto que dessa forma ela satisfaz os três princípios.

No item (c) temos uma afirmação que possui um sujeito (dois x mais seis), um verbo e predicado (é igual a três) mas não cumpre o princípio do terceiro excluído, ou seja, a frase é verdadeira para $x = -\frac{3}{2}$ e falso para qualquer outro x diferente desse valor. Logo, não é possível determinar se ela é verdadeira ou falsa pois nada foi dito sobre a variável x.

Frases como a do item (c) subordinadas a uma variável livre e que por isso não possui valor lógico definido, são chamadas de **sentenças abertas**.

1.2 Os Quantificadores Universal e Existencial

Uma das maneiras de transformar uma sentença aberta em uma sentença é, para cada variável livre de sentença aberta, encontrar um conjunto adequado e indicar uma quantidade de elementos desse conjunto que satisfazem as condições envolvidas na variável livre. Das opções para quantificar, destacam-se duas: as que utilizam as palavras *existe* ou *para todo*.

Exemplo 1.4. *Uma maneira de transformar a sentença aberta anterior,* $2x + 6 = 3$*, em uma sentença seria escrever:*

$$\textit{Existe } x \in \mathbb{Z}, \textit{ tal que } 2x + 6 = 3.$$

Dessa maneira temos uma sentença cujo valor lógico é verdadeiro. Poderíamos também ter escrito:

$$\textit{Para todo } x \in \mathbb{Z}, \textit{ temos } 2x + 6 = 3.$$

Onde temos agora uma sentença e seu valor lógico é falso.

O termo *para todo* é chamado de **quantificador universal**, o termo *existe* é chamado de **quantificador existencial**, e são denotados usando-se os símbolos $\forall$ e $\exists$, respectivamente.

Os quantificadores têm grande importância na linguagem matemática, o quantificador universal é usado para expressar condições satisfeitas por todos os elementos de um conjunto, já o quantificador existencial é usado para expressar condições satisfeitas por, pelo menos, um elemento de um conjunto.

Outras expressões podem ser usadas para substituir os quantificadores. Por exemplo, podemos usar *dado, para cada, para qualquer, (para) qualquer que seja* ao invés de usar *para todo*. Também, podemos substituir *existe* por *existe algum, exite pelo menos um.*

1.3 Conectivos e Proposições Compostas

Comecemos a seção recordando duas operações muito importantes envolvendo conjuntos: união e interseção. Esses conceitos, mesmo sendo conhecidos desde os primeiros anos do colégio, ainda causam muitas dúvidas e ainda é muito comum ver-se confundir uniões com interseções.

Considerando A e B conjuntos quaisquer, podemos construir outros dois conjuntos extremamente úteis:

(1) O primeiro é formado pelos elementos de A juntamente com os elementos de B, chamado A **união** B e é representado por $A \cup B$. Escrevemos $x \in A \cup B$ se $x \in A$ ou se $x \in B$.

(2) O segundo é formado pelos elementos de A que também são elementos de B, chamado A **interseção** B e é denotado por $A \cap B$. Escrevemos $x \in A \cap B$ se $x \in A$ e $x \in B$.

Portanto, a união está relacionada com a conjunção gramatical *ou* e a interseção com a conjunção *e*.

A união $A \cup B$ dos conjuntos A e B é dita **disjunta** quando $A \cap B = \emptyset$. No uso matemático, ao se referir a qualquer união, sempre deve-se levar em consideração a interseção, pois para dois conjuntos quaisquer A e B temos $(A \cap B) \subset (A \cup B)$, e nem sempre uma união é disjunta. Diferentemente, em nosso cotidiano, na linguagem coloquial é como se o uso do *ou* representasse sempre uma união disjunta. Observe, por exemplo, que na frase: *Pedro é filho de Maria ou de Joana*, fazemos o uso do *ou* no sentido excludente.

Podemos construir proposições matemáticas a partir de outras, utilizando certas palavras, chamadas **conectivos lógicos**. São estes:

$$\text{"}não\text{"},\ \text{"}se\ldots,\ então\text{"},\ \text{"}se,\ e\ somente\ se\text{"},\ \text{"}ou\text{"}\ e\ \text{"}e\text{"}. \tag{1.1}$$

Observe que foram utilizados alguns desses conectivos no Exemplo 1.3 para construir a proposição P_2. Proposições desse tipo, formadas por outras proposições com o auxílio de conectivos, são chamadas **proposições compostas**. Chamam-se **proposições simples** aquelas que não contêm mais de uma proposição em sua formação. Denotaremos as proposições simples por letras latinas minúsculas, e as mais frequentes serão as letras p, q e r. Caso existam muitas proposições, utilizaremos

índices numéricos nas letras, por exemplo: p_0, p_1, p_2, etc. As proposições compostas serão denotadas por letras maiúsculas.

Como ocorre com os conjuntos, usando as proposições p e q podemos formar duas proposições bastante especiais:

p e q, chamada **conjunção** das sentenças p e q

e

p ou q, chamada **disjunção** das sentenças p e q.

Vamos estudar o valor lógico das proposições compostas formadas com cada um dos cinco conectivos dados em (1.1).

Vamos começar com o conceito de **Conjunção**.

Definição 1.5. *Sejam p e q proposições, a **conjunção** das proposições p e q, denotada por $p \wedge q$, é uma nova proposição que assume o valor lógico verdadeiro somente quando p e q forem verdadeiras simultaneamente.*

Exemplo 1.6. *Sejam p: "O céu é azul" e q: "O rio é de água doce", então a proposição $p \wedge q$ corresponde à proposição "O céu é azul e o rio é de água doce".*

Exemplo 1.7. *Sejam p: "João é magro" e q: "José é alto", então a proposição $p \wedge q$ corresponde à proposição "João é magro e José é alto".*

Em uma proposição composta com duas componentes como $p \wedge q$, existem $2 \times 2 = 4$ possibilidades, chamadas **possibilidades lógicas** a serem consideradas, a saber:

1. p é verdadeira e q é verdadeira;
2. p é verdadeira e q é falsa;
3. p é falsa e q é verdadeira;
4. p é falsa e q é falsa.

As quatro possibilidades são colocadas em quatro linhas de uma tabela. Para o valor lógico verdadeiro, escreveremos a letra V e, para o valor lógico falso, escreveremos a letra F. Utilizamos uma primeira coluna para p, uma segunda coluna para q e uma terceira coluna para a conexão. No caso da conjunção $p \wedge q$, essa tabela é dada por:

p	q	$p \wedge q$
V	V	V
V	F	F
F	V	F
F	F	F

Tabela 1.1: Conjunção $p \wedge q$.

A Tabela 1.1 nos indica que a proposição composta $p \wedge q$ só será verdadeira quando p é verdadeira e q é verdadeira.

Exemplo 1.8. *Consideremos as seguintes proposições:*

a) O céu é verde e $2 + 2 = 5$*;*

b) O céu é azul e $2 + 2 = 5$*;*

c) O céu é verde e $2 + 2 = 4$*;*

d) O céu é azul e $2 + 2 = 4$*.*

De acordo com a Tabela 1.1, só o item d) é verdadeiro, pois só nesse caso ambas as componentes são verdadeiras.

Vejamos agora outro conceito importante, a **Disjunção**.

Definição 1.9. *Sejam p e q proposições, a* ***disjunção*** *das proposições p e q, denotada por $p \vee q$, é uma nova proposição que assume o valor lógico verdadeiro quando p ou q forem verdadeiras (não necessariamente simultâneas).*

Exemplo 1.10. *Na sentença "Maria foi à praia ou ao mercado", basta que Maria tenha ido, pelo menos, a um dos lugares para que ela se torne verdadeira.*

A tabela da disjunção de p e q é:

p	q	$p \vee q$
V	V	V
V	F	V
F	V	V
F	F	F

Tabela 1.2: Disjunção $p \vee q$.

Assim, $p \vee q$ é falsa somente quando ambas, p e q, são falsas.

Exemplo 1.11. *Consideremos as seguintes proposições:*

a) O céu é verde ou $2 + 2 = 5$*;*

b) O céu é azul ou $2 + 2 = 5$*;*

c) O céu é verde ou $2 + 2 = 4$*;*

d) O céu é azul ou $2 + 2 = 4$*.*

De acordo com a Tabela 1.2, só o item a) é falso, pois só nesse caso ambas as componentes são falsas.

Se p é uma proposição qualquer, a **Negação** desta proposição é definida da seguinte forma:

Definição 1.12. *Dada uma proposição p, a* ***negação*** *de p, denotada por* $\sim p$*, é uma proposição com valor lógico contrário ao valor lógico de p, isto é, se p tem valor lógico verdadeiro então* $\sim p$ *tem valor lógico falso e, se p tem valor lógico falso, então* $\sim p$ *tem valor lógico verdadeiro.*

Vejamos alguns exemplos.

Exemplo 1.13. *Considere as três proposições seguintes:*

a) O céu é azul.

b) É falso que o céu é azul.

c) O céu não é azul.

Nesse caso, os itens b) e c) são negações do item a), que é verdadeiro. Logo, os itens b) e c) são falsos.

Exemplo 1.14. *A negação da proposição* p : "$2+2=5$" *é* "$2+2\neq 5$" *ou "É falso que* $2+2=5$*". Temos que* p *é falsa e* $\sim p$ *é verdadeira.*

A tabela para a negação de p é:

p	$\sim p$
V	F
F	V

Tabela 1.3: Negação $\sim p$.

Muitas proposições, especialmente em Matemática, são da forma "se p, então q". Tais proposições são originadas de uma proposição composta que definiremos agora.

Definição 1.15. *Sejam* p *e* q *proposições, a* ***condicional*** *de* p *e* q*, denotada por* $p \rightarrow q$ *onde se lê: "p condiciona q", é a proposição que assume o valor falso somente quando* p *for verdadeira e* q *for falsa.*

A proposição p é chamada antecedente e a proposição q consequente da condicional. Vamos a alguns exemplos.

Exemplo 1.16. *Consideremos a seguinte sentença: "Seu eu receber um aumento de salário então vou comprar um carro novo". Como podemos estabelecer o valor lógico de uma operação condicional, conhecidos os valores verdade do antecedente e do consequente? Vejamos cada caso:*

1. *Suponhamos que ambas as coisas aconteçam, isto é, que eu recebi um aumento de salário e comprei um carro novo. Como prometido, significa que eu disse a verdade e portanto a sentença é verdadeira.*

2. *Suponhamos por outro lado, que eu recebi um aumento de salário, mas não comprei um carro novo, significa que eu menti, pois não cumpri o prometido, logo, a sentença é falsa.*

3. *Analisemos, com muito cuidado, o caso em que eu não recebi o aumento de salário. Observe que se eu comprar ou não um carro novo, ninguém pode me acusar de mentiroso, uma vez que eu não falei o que ocorreria se eu não recebesse um aumento de salário. Assim, nestes dois casos, a sentença é verdadeira.*

Assim, a tabela para a condicional de p e q, é a seguinte:

p	q	$p \to q$
V	V	V
V	F	F
F	V	V
F	F	V

Tabela 1.4: Condicional $p \to q$.

Quando temos uma proposição do tipo condicional $p \to q$, diremos que a proposição $q \to p$ é a **recíproca** de $p \to q$. É importante observarmos que elas somente possuirão o mesmo valor lógico quando p e q são simultaneamente falsos. Logo, elas não possuem a mesma tabela. De fato, a tabela da recíproca da condicional de p e q é a seguinte:

p	q	$q \to p$
V	V	V
V	F	V
F	V	F
F	F	V

Tabela 1.5: Recíproca de $q \to p$.

Sabemos que uma sentença condicional "se p, então q" pode ser considerada como uma sentença implicativa $p \to q$, que também pode ser lida como p implica q, e vice versa. Outras duas maneiras de apresentar uma sentença implicativa $p \to q$ muito comuns na Matemática ao se enunciar resultados como teoremas, lemas, etc, são:

p é (uma) condição suficiente para q

ou

q é (uma) condição necessária para p.

Exemplo 1.17. *Suponhamos que p seja a asserção "Pedro é brasileiro", e q a asserção "Pedro é terráqueo". Como Pedro é brasileiro, e todo brasileiro é um terráqueo, concluímos que Pedro é terráqueo, logo $p \to q$. Podemos expressar este fato de várias maneiras:*

1ª Versão: *Pedro é brasileiro, implica Pedro é terráqueo.*

2ª Versão: *Pedro ser brasileiro é uma condição suficiente para Pedro ser terráqueo.*

3ª Versão: *Pedro ser terráqueo é uma condição necessária para Pedro ser brasileiro.*

Observe os significados das palavras *suficiente* e *necessária* nesse exemplo. Atentamos aqui que ser *suficiente* significa que basta Pedro ser brasileiro para ser terráqueo. Por outro lado, como não há brasileiros que não sejam terráqueos, é *necessário* Pedro ser terráqueo para ser brasileiro.

Vejamos outro exemplo.

Exemplo 1.18. *Seja $n \in \mathbb{Z}$ um número inteiro. Se n for um múltiplo de 5, então n termina em 0 ou em 5.*

Nessa sentença, vamos considerar:

$$p\text{: Um número inteiro } n \text{ é múltiplo de } 5$$

$$e$$

$$q\text{: } n \text{ termina em } 0 \text{ ou em } 5.$$

Sabemos valer a implicação $p \to q$. Pelo que acabamos de expor, duas outras maneiras de enunciar esse resultado são:

Um número inteiro ser múltiplo de 5 é uma condição suficiente para que ele termine em 0 ou em 5.

Ou então,

Um número inteiro terminar em 0 ou em 5 é uma condição necessária para que ele seja múltiplo de 5.

Também é muito comum na Matemática aparecerem expressões do tipo "p se, e somente se, q". Essas expressões são originadas da utilização da proposição que definimos a seguir:

Definição 1.19. *Sejam p e q proposições, a* ***bicondicional*** *de p e q, denotada por $p \leftrightarrow q$ onde se lê: "p bicondiciona q", é a proposição que assume o valor lógico verdadeiro somente quando p e q forem verdadeiras ou p e q forem falsas.*

Assim, se uma proposição verdadeira bicondiciona a uma proposição falsa, então essa composição será falsa e, se uma proposição falsa bicondiciona a uma proposição verdadeira, a composição também será falsa. A bicondicional é uma proposição que pode ser definida como

$$(p \to q) \wedge (q \to p),$$

ou seja, a composição de duas condicionais pela conjunção.

Pela definição dada acima, para sabermos quando a bicondicional é verdadeira ou falsa, devemos conhecer quando a conjunção e a condicional sãs verdadeiras ou falsas. Analisando isso, temos a seguinte tabela para a bicondicional de p e q.

p	q	$p \leftrightarrow q$
V	V	V
V	F	F
F	V	F
F	F	V

Tabela 1.6: Bicondicional $p \leftrightarrow q$.

Vejamos alguns exemplos

Exemplo 1.20. *Na sentença "João será aprovado se, e somente se, ele estudar", o conectivo "se, e somente se" indica que se João estudar será aprovado, e que essa é a única possibilidade de João ser aprovado.*

Exemplo 1.21. *Consideremos as seguintes proposições bicondicionais:*

a) O céu é verde bicondiciona que, $2 + 2 = 5$*;*

b) O céu é azul bicondiciona que, $2 + 2 = 5$*;*

c) O céu é verde bicondiciona que, $2 + 2 = 4$*;*

d) O céu é azul bicondiciona que, $2 + 2 = 4$*.*

Assim, as proposições a) e d) são verdadeiras enquanto que as proposições b) e c) são falsas.

1.4 Tabelas-Verdade

A tabela verdade é um método usado pela lógica matemática, cujo o objetivo é definir o valor lógico de uma proposição, ou seja: verificar se uma determinada sentença é verdadeira ou falsa. É importante ressaltarmos que quando falamos em proposições, ao menos no tocante à lógica, nos referimos aos pensamentos completos e indicação de afirmação de situações.

> Ao formar proposições compostas através de proposições $p, q, \ldots$, com os conectivos $\wedge, \vee, \rightarrow, \leftrightarrow$ e a negação $\sim$, obtemos o que denominamos **forma sentencial**, ou seja, uma expressão da forma $P(p, q, \ldots)$. As proposições $p, q, \ldots$ são denominadas **variáveis sentenciais**. Assim, se temos uma forma sentencial $P(p, q, \ldots)$, a forma sentencial $P(r, q, \ldots)$ é obtida trocando em $P(p, q, \ldots)$ a proposição p pela proposição r, em todas as suas ocorrências. Devemos notar que o valor lógico de uma forma sentencial $P(p, q, \ldots)$ depende somente dos valores lógicos das proposições $p, q, \ldots$, e não das proposições propriamente ditas. A tabela que construímos com os conectivos $\wedge, \vee, \rightarrow, \leftrightarrow$ e $\sim$ é chamada **"tabela-verdade"**. Essa tabela pode ser construída para qualquer forma sentencial $P(p, q, \ldots)$, relacionando o valor lógico de P com os valores lógicos de $p, q, \ldots$ $(\ldots)$.[2]

Nela, os cabeçalhos são selecionados de modo que a proposição composta (que fica na última coluna) é gradualmente construída a partir de suas componentes. As duas primeiras colunas simplesmente registram todos os casos para os valores verdade de p e q.

Podemos observar então, que o número de linhas da tabela corresponde a uma possível combinação dos valores lógicos de suas componentes. Portanto, a tabela-verdade de uma sentença proposicional tem 2^n linhas, além do cabeçalho. Vejamos um exemplo de construção dessas tabelas.

Exemplo 1.22. *Vamos construir a tabela-verdade para a proposição composta* $\sim [(\sim p) \wedge (\sim q)]$.

p	q	$\sim [(\sim p) \wedge (\sim q)]$
V	V	
V	F	
F	V	
F	F	

Tabela 1.7: Tabela verdade de $\sim [(\sim p) \wedge (\sim q)]$.

Para isso, construímos uma tabela guia, onde colocamos nas colunas, as subproposições seguidas das proposições compostas até chegar na desejada.

p	q	$\sim p$	$\sim q$	$(\sim p) \wedge (\sim q)$	$\sim [(\sim p) \wedge (\sim q)]$
V	V	F	F	F	V
V	F	F	V	F	V
F	V	V	F	F	V
F	F	V	V	V	F

Tabela 1.8: Guia para construção da tabela-verdade de $\sim [(\sim p) \wedge (\sim q)]$.

[2] FRANCO, Valdeni Soliani.; GERÔNIMO, João Roberto. *Fundamentos da Matemática: uma introdução à lógica matemática, teoria dos conjuntos, relações e funções.* Maringá, 2008, p. 24-25.

Essa tabela serve apenas para facilitar a construção da tabela-verdade, que deve conter apenas as subproposições e a proposição composta desejada. Nesse caso, temos que

p	q	$\sim [(\sim p) \wedge (\sim q)]$
V	V	V
V	F	V
F	V	V
F	F	F

Tabela 1.9: Tabela verdade de $\sim [(\sim p) \wedge (\sim q)]$.

1.5 Tautologia e Contradição

Utilizando a tabela verdade, podemos obter algumas regras de identidade que são importantes na demonstração de um fato matemático. Iniciamos com os conceitos de tautologia e contradição.

Definição 1.23. *Uma forma sentencial $P(p, q, \ldots)$ é uma **tautologia** se ela assume o valor lógico verdadeiro, quaisquer que sejam os valores lógicos das variáveis sentenciais. Uma forma sentencial $P(p, q, \ldots)$ é tomada como um **absurdo**, uma **contradição** ou **contraválida** se ela assume o valor lógico falso, quaisquer que sejam os valores lógicos das variáveis sentenciais.*

Observação 1.24. *Como uma tautologia é sempre verdadeira, a negação de uma tautologia é sempre falsa e, portanto, é uma contradição.*

Vejamos alguns exemplos destes conceitos.

Exemplo 1.25. *Vamos examinar as tabelas-verdade de $p \vee \sim p$ e de $p \wedge \sim p$.*

p	$\sim p$	$p \vee \sim p$
V	F	V
F	V	V

Tabela 1.10: Tabela-verdade de $p \vee \sim p$.

p	$\sim p$	$p \wedge \sim p$
V	F	F
F	V	F

Tabela 1.11: Tabela-verdade de $p \wedge \sim p$.

Podemos observar que $p \vee \sim p$ é verdadeira em todos os casos, isto é, em todas as possibilidades lógicas da proposição p. Portanto $p \vee \sim p$ é uma tautologia. Já $p \wedge \sim p$ é falsa em todas as possibilidades lógicas de p. Portanto, $p \wedge \sim p$ é uma contradição.

1.6 Inferência e Equivalência Lógica

Iniciaremos essa seção com o estudo sobre inferência e equivalência de sentenças lógicas, que são obtidas através de tabelas verdades e importantes na demonstração matemática, pois em muitos casos é mais conveniente substituir uma sentença por outra que seja equivalente, simplificando assim o cálculo com sentenças e também facilitando algumas demonstrações

Definição 1.26. *Dadas duas proposições p e q, definimos a* ***implicação lógica*** *ou* ***inferência*** $p \Rightarrow q$, *quando a proposição $p \to q$ for uma tautologia. Diremos que p é* ***equivalente*** *à proposição q, se as suas tabelas-verdades forem idênticas. Representamos esse fato por $p \Leftrightarrow q$ que é lido como (a sentença) p é equivalente à (sentença) q.*

Para entendermos melhor a definição acima, vejamos alguns exemplos.

Exemplo 1.27. *Consideremos novamente a sentença: "Se eu receber um aumento de salário então vou comprar um carro novo". Nela temos:*

p: Se eu receber um aumento de salário

e

q: vou comprar um carro novo.

Logo, temos uma proposição condicional do tipo $p \to q$, cuja tabela-verdade é:

p	q	$p \to q$
V	V	**V**
V	F	**F**
F	V	**V**
F	F	**V**

Tabela 1.12: Condicional $p \to q$.

Observe agora a proposição condicional $\sim q \to \sim p$, ou seja, a proposição "Se eu não comprar um carro novo, então não vou receber um aumento de salário". A tabela-verdade dessa proposição é:

$\sim q$	$\sim p$	$\sim q \to \sim p$
F	F	**V**
V	F	**F**
F	V	**V**
V	V	**V**

Tabela 1.13: Contrapositiva $\sim q \to \sim p$.

Analisando as tabelas-verdades dessas duas proposições condicionais observamos que $p \to q$ *e* $\sim q \to \sim p$ *têm os mesmos valores lógicos. Assim, essas proposições são equivalentes e escrevemos* $(p \to q) \Leftrightarrow (\sim q \to \sim p)$.

Observação 1.28. *A sentença* $\sim q \to \sim p$ *é chamada* ***contrapositiva da sentença*** $p \to q$. *Semelhantemente, definimos Se* $\sim q$, *então* $\sim p$ *como a* ***contrapositiva da sentença condicional*** *Se p, então q. O método de demonstração usando a contrapositiva baseia-se em demonstrar* $\sim q \Rightarrow \sim p$ *para assegurar a validade da sentença* $p \Rightarrow q$. *O mesmo vale para sentenças condicionais.*

Vimos anteriormente que a bicondicional $p \leftrightarrow q$ pode ser definida como a composição de duas condicionais pela conjunção. Isto porque, $(p \to q) \wedge (q \to p)$ e $p \leftrightarrow q$ são equivalentes.

De fato, suas tabelas-verdade são:

p	q	$p \to q$	$q \to p$	$(p \to q) \wedge (q \to p)$	$p \leftrightarrow q$
V	V	V	V	**V**	**V**
V	F	F	V	**F**	**F**
F	V	V	F	**F**	**F**
F	F	V	V	**V**	**V**

Tabela 1.14: Guia para a construção das tabelas-verdade de $(p \to q) \wedge (q \to p)$ e $p \leftrightarrow q$.

Observação 1.29. *Na Matemática há três maneiras de provar uma sentença condicional "Se p, então q", onde p representa a hipótese e q a tese:*

1. *Demonstração direta: considera-se p e, por meio de um processo lógico-dedutivo, se deduz q.*
2. *Demonstração indireta por contradição ou por (redução a um) absurdo: considera-se p e* $\sim q$ *e, por meio de um processo lógico dedutivo, se deduz alguma contradição (absurdo).*
3. *Demonstração da Contrapositiva de* $p \Rightarrow q$ *(uma outra maneira indireta de se provar uma implicação): considera-se* $\sim q$ *e, por meio de um processo lógico-dedutivo, se deduz* $\sim p$.

1.7 Negação de Proposições Compostas

Vejamos, primeiramente, como se dá a negação de sentenças envolvendo os quantificadores.

Um erro muito comum, especialmente na Matemática é achar que a negação de "todos são" é "todos não são". Para ver que isso é um erro, basta pensar no conjunto $\{1, 2, 3, 4\}$ e notar que as sentenças "todos os elementos são pares" e "todos os elementos não são pares" são ambas falsas.

A negação de uma sentença quantificada universalmente é uma sentença quantificada existencialmente. Ou seja, o quantificador universal transforma-se em existencial e nega-se o complemento. Por exemplo, a negação de "todos gostam de futebol" é "pelo menos um não gosta de futebol" e a negação de "para todo $x \in \mathbb{Z}$, temos $2x + 6 = 3$" é "existe $x \in \mathbb{Z}$, tal que $2x + 6 \neq 3$".

Também é muito comum achar que a negação de "pelo menos um é" é "pelo menos um não é" quando na verdade, o correto é "nenhum é" o que é o mesmo que, "todos não são".

Para ver que isso é um erro, basta novamente pensar no conjunto $\{1, 2, 3, 4\}$ e notar que as sentenças "pelo menos um é par" e "pelo menos um não é par" são ambas verdadeiras.

Assim, a negação de uma sentença quantificada existencialmente é uma sentença quantificada universalmente. Ou seja, o quantificador existencial transforma-se em universal e nega-se o complemento. Por exemplo, a negação de "pelo menos um gosta de futebol" é "todos não gostam de futebol" e a negação da sentença "existe $x \in \mathbb{Z}$, tal que $2x + 6 = 3$" é "para todo $x \in \mathbb{Z}$, temos $2x + 6 \neq 3$".

Agora vejamos como se dá a negação de sentenças envolvendo os conectivos, começando pela negação da conjunção e da disjunção.

Sejam p e q proposições, a negação da proposição $p \wedge q$ é a proposição $\sim (p \wedge q)$ que é equivalente a $(\sim p) \vee (\sim q)$, ou seja, a negação da conjunção (de duas sentenças) é a disjunção das negações (destas sentenças). Para comprovar, basta verificar a igualdade de suas tabelas-verdade:

p	q	$\sim p$	$\sim q$	$p \wedge q$	$\sim (p \wedge q)$	$(\sim p) \vee (\sim q)$
V	V	F	F	V	**F**	**F**
V	F	F	V	F	**V**	**V**
F	V	V	F	F	**V**	**V**
F	F	V	V	F	**V**	**V**

Tabela 1.15: Negação da conjunção $p \wedge q$.

Exemplo 1.30. *Sejam as proposições p: o céu é azul e q: o rio é de água doce. Então temos que*

$p \wedge q$: o céu é azul e o rio é de água doce.

E a negação desta sentença é portanto,

$$\sim (p \wedge q)\text{: } o\ céu\ não\ é\ azul\ ou\ o\ rio\ não\ é\ de\ água\ doce.$$

Por outro lado, a negação da proposição $p \vee q$ é a proposição $\sim (p \vee q)$ que é equivalente a $(\sim p) \wedge (\sim q)$, ou seja, a negação da disjunção (de duas sentenças) é a conjunção das negações (destas sentenças). Vejamos a tabela-verdade:

p	q	$\sim p$	$\sim q$	$p \vee q$	$\sim (p \vee q)$	$(\sim p) \wedge (\sim q)$
V	V	F	F	V	**F**	**F**
V	F	F	V	V	**F**	**F**
F	V	V	F	V	**F**	**F**
F	F	V	V	F	**V**	**V**

Tabela 1.16: Negação da disjunção $p \vee q$.

Exemplo 1.31. *Sejam as proposições p: o céu é azul e q: o rio é de água doce. Então temos que*

$$p \vee q\text{: } o\ céu\ é\ azul\ ou\ o\ rio\ é\ de\ água\ doce.$$

E a negação desta sentença é portanto,

$$\sim (p \vee q)\text{: } o\ céu\ não\ é\ azul\ e\ o\ rio\ não\ é\ de\ água\ doce.$$

Para entendermos a **negação de uma sentença condicional**, recordemos pela Observação 1.29 que uma sentença condicional $p \to q$ é válida, quando todo elemento que satisfizer a hipótese p cumprir necessariamente a tese q. Dessa forma, a negação de uma sentença condicional $p \to q$ envolve a negação do quantificador universal, e é o mesmo que negar a frase *todo elemento que satisfaz a hipótese p cumpre a tese q*. Logo a negação da sentença condicional "se p, então q" é: *existe um elemento que satisfaz a hipótese p e não cumpre a tese q*. Portanto, $\sim (p \to q)$ é equivalente a $p \wedge \sim q$. E, de fato temos abaixo a tabela-verdade para conferir a equivalência:

p	q	$\sim q$	$p \to q$	$\sim (p \to q)$	$p \wedge \sim q$
V	V	F	V	**F**	**F**
V	F	V	F	**V**	**V**
F	V	F	V	**F**	**F**
F	F	V	V	**F**	**F**

Tabela 1.17: Negação da condicional $p \to q$.

Vejamos um exemplo.

Exemplo 1.32. *Sejam as proposições p: o céu é azul e q: o rio é de água doce. Então temos que*

$$p \to q\text{: se o céu é azul então o rio é de água doce.}$$

E a negação desta sentença é portanto,

$$\sim (p \to q)\text{: o céu é azul e o rio não é de água doce.}$$

Para finalizar este capítulo, vamos estudar a **negação de uma sentença bicondicional**. Para isto sejam p e q proposições. Vimos que a bicondicional $p \leftrightarrow q$ é equivalente a proposição $(p \to q) \wedge (q \to p)$. Portanto, negar a bicondicional $p \leftrightarrow q$ é o mesmo que negar a conjunção das condicionais $(p \to q) \wedge (q \to p)$ e como já vimos acima a negação da conjunção e da condicional, temos:

$$\begin{aligned} \sim (p \leftrightarrow q) &\Leftrightarrow \sim [(p \to q) \wedge (q \to p)] \\ &\Leftrightarrow \sim (p \to q) \vee [\sim (q \to p)] \\ &\Leftrightarrow [p \wedge (\sim q)] \vee [q \wedge (\sim p)] \end{aligned} .$$

E, portanto, $\sim (p \leftrightarrow q) \Leftrightarrow [p \wedge (\sim q)] \vee [q \wedge (\sim p)]$, o que podemos conferir abaixo.

p	q	$\sim p$	$\sim q$	$p \leftrightarrow q$	$\sim (p \leftrightarrow q)$	$[p \wedge (\sim q)]$	$[q \wedge (\sim p)]$	$[p \wedge (\sim q)] \vee [q \wedge (\sim p)]$
V	V	F	F	V	**F**	F	F	**F**
V	F	F	V	F	**V**	V	F	**V**
F	V	V	F	F	**V**	F	V	**V**
F	F	V	V	V	**F**	F	F	**F**

Tabela 1.18: Negação da bicondicional $p \leftrightarrow q$.

Exemplo 1.33. *Sejam as proposições p: o céu é azul e q: o rio é de água doce. Então temos:*

$$p \leftrightarrow q\text{: o céu é azul se, e somente se, o rio é de água doce.}$$

E a negação desta sentença é portanto,

$$\sim (p \leftrightarrow q)\text{: o céu é azul e o rio não é de água doce ou o rio é de água doce e o céu não é azul.}$$

Capítulo 2

Números Inteiros

Neste capítulo nossa abordagem será essencialmente axiomática conforme feita em [10], ou seja, a partir de uma lista razoavelmente pequena de propriedades básicas dos números inteiros e das duas operações, vamos mostrar como podem ser obtidas as demais propriedades.

Observação 2.1. *Na seção 2.1, quando queremos trabalhar propriedades de soma e multiplicação em* $\mathbb{N}$*, consideraremos* $0 \in \mathbb{N}$*. A partir da seção 2.2, consideraremos* $0 \notin \mathbb{N}$*.*

2.1 Os Números Naturais

Para estudarmos o conjunto dos Números Inteiros vamos rever alguns fatos básicos sobre **Números Naturais**.

Seja $\mathbb{K}$ um conjunto de elementos. Uma operação $*$ é uma função

$$* : \mathbb{K} \times \mathbb{K} \to \mathbb{K}$$
$$(a, b) \mapsto a * b.$$

Para esta operação ser considerada "boa" ela dever satisfazer as seguintes propriedades:

1. $a * b \in \mathbb{K}$, para quaisquer $a, b \in \mathbb{K}$. (fechamento)

2. $a * b = b * a$, para quaisquer $a, b \in \mathbb{K}$. (comutatividade)

3. $(a * b) * c = a * (b * c)$, para quaisquer $a, b, c \in \mathbb{K}$. (associatividade)

4. existe $0 \in \mathbb{K}$ tal que $a * 0 = a$, para qualquer $a \in \mathbb{K}$. (existência do elemento neutro)

5. para todo $a \in \mathbb{K}$, existe $-a \in \mathbb{K}$ tal que $a * (-a) = 0$. (existência do elemento oposto)

Com relação a conjunto de números comecemos considerando o conjunto dos números naturais

$$\mathbb{N} := \{0, 1, 2, 3, \ldots\},$$

cujos elementos nos dão a noção de quantidade de objetos. Neste conjunto assumimos conhecidas as operações de soma e produtos usuais em $\mathbb{R}$:

$$\begin{aligned} + : \mathbb{N} \times \mathbb{N} &\to \mathbb{N} \\ (a, b) &\mapsto a + b \end{aligned}$$

e

$$\begin{aligned} \cdot : \mathbb{N} \times \mathbb{N} &\to \mathbb{N} \\ (a, b) &\mapsto a \cdot b. \end{aligned}$$

As duas operações acima satisfazem as propriedades do fechamento, da comutatividade e da associatividade. Com relação a existência do elemento neutro temos que

(i) existe $0 \in \mathbb{N}$ tal que $a + 0 = a$, para todo $a \in \mathbb{N}$.

(ii) existe $1 \in \mathbb{N}$ tal que $a \cdot 1 = a$, para todo $a \in \mathbb{N}$.

Porém, com relação à existência do elemento oposto vemos que

(i) para todo $a \neq 0$, não existe $-a \in \mathbb{N}$ tal que $a + (-a) = 0$.

(ii) para todo $a \neq 1$, não existe $\dfrac{1}{a} \in \mathbb{N}$ tal que $a \cdot \dfrac{1}{a} = 1$.

Definição 2.2. *Dados dois números naturais $m, n \in \mathbb{N}$, diremos que m é menor do que n se existir $p \in \mathbb{N}$, $p \neq 0$, tal que $n = m + p$, ou seja,*

$$m < n \iff \exists\ p \in \mathbb{N},\ p \neq 0;\ n = m + p.$$

Ainda, diremos que m é menor ou igual a n se existir $p \in \mathbb{N}$ tal que $n = m + p$, ou seja,

$$m \leq n \iff \exists\ p \in \mathbb{N};\ n = m + p.$$

Assim, pela definição acima,

- $2 < 5$, pois existe $0 \neq p = 3 \in \mathbb{N}$ tal que $5 = 2 + 3$.
- $2 \leq 5$, pois existe $p = 3 \in \mathbb{N}$ tal que $5 = 2 + 3$.
- $2 \leq 2$, pois existe $p = 0 \in \mathbb{N}$ tal que $2 = 2 + 0$.
- $2 \not< 2$, pois não existe $p \in \mathbb{N}$, com $p \neq 0$, tal que $2 = 2 + p$.

Definição 2.3. *Dados dois números naturais $m, n \in \mathbb{N}$, diremos que m é maior do que n se existir $p \in \mathbb{N}$, $p \neq 0$, tal que $m = n + p$, ou seja,*

$$m > n \iff \exists\ p \in \mathbb{N},\ p \neq 0;\ m = n + p.$$

Ainda, diremos que m é maior ou igual a n se existir $p \in \mathbb{N}$ tal que $m = n + p$, ou seja,

$$m \geq n \iff \exists\ p \in \mathbb{N};\ m = n + p.$$

Assim, pela definição acima,

- $5 > 2$, pois existe $0 \neq p = 3 \in \mathbb{N}$ tal que $5 = 2 + 3$.
- $5 \geq 2$, pois existe $p = 3 \in \mathbb{N}$ tal que $5 = 2 + 3$.
- $2 \geq 2$, pois existe $p = 0 \in \mathbb{N}$ tal que $2 = 2 + 0$.
- $2 \not> 2$, pois não existe $p \in \mathbb{N}$, com $p \neq 0$, tal que $2 = 2 + p$.

Proposição 2.4. *Sejam $m, n, p \in \mathbb{N}$ três números naturais. Então*

1. *se $m < n$ e $n < p$, então $m < p$.*
2. *$m < n$ se, e somente se, $m + p < n + p$.*

Demonstração: Para o item 1. temos

- como $m < n$, então existe $0 \neq p_1 \in \mathbb{N}$ tal que $n = m + p_1$.
- como $n < p$, então existe $0 \neq p_2 \in \mathbb{N}$ tal que $p = n + p_2$.

Assim,

$$p = n + p_2 = (m + p_1) + p_2 = m + (p_1 + p_2),$$

ou seja, tomando $p_3 = p_1 + p_2$ obtemos que

$$p = m + p_3,$$

mostrando que

$$m < p$$

e completando a demonstração de 1.

A demonstração do item 2. é feita de forma análoga. ■

Princípio da Tricotomia *Se $m, n \in \mathbb{N}$ são números naturais quaisquer, então uma e somente uma das três condições abaixo acontece:*

- $m < n$;
- $m = n$;
- $m > n$.

Proposição 2.5. *Sejam $m, n, p \in \mathbb{N}$ três números naturais. Então*

(a) $m \leq m$.

(b) *se* $m \leq n$ *e* $n \leq m$, *então* $n = m$.

(c) *se* $m \leq n$ *e* $n \leq p$, *então* $m \leq p$.

(d) $m \leq n$ *se, e somente se,* $m + p \leq n + p$.

Demonstração: Para mostramos o item (b), como $m \leq n$ e $n \leq m$, temos que existem $p_1, p_2 \in \mathbb{N}$ tais que

$$n = m + p_1 \quad \text{e} \quad m = n + p_2.$$

Logo,

$$m = n + p_2 = (m + p_1) + p_2 = m + (p_1 + p_2).$$

Pela propriedade da unicidade do elemento neutro da soma, obtemos que

$$0 = p_1 + p_2.$$

Assim, p_2 é o elemento oposto de p_1, ou seja, $p_2 = -p_1$. Mas, pelo item (i) acima (da existência do elemento oposto), p_1 só admite oposto se não for diferente de zero e, portanto, obtemos que $p_1 = p_2 = 0$, ou seja, $m = n$.

Os itens (a), (c) e (d) provam-se da mesma forma. ■

2.2 A Adição e a Multiplicação de Números Inteiros

Consideremos agora o conjunto dos números inteiros

$$\mathbb{Z} := \{\ldots, -4,\ -3,\ -2,\ -1,\ 0,\ +1,\ +2,\ +3,\ +4,\ \ldots\}.$$

As operações de adição e de multiplicação no conjunto dos números inteiros, $\mathbb{Z}$, possuem as seguintes propriedades:

1) A adição e a multiplicação são *bem definidas*, isto é, para todos $a, b, a', b' \in \mathbb{Z}$, temos que se $a = a'$ e $b = b'$, então $a + b = a' + b'$ e $a \cdot b = a' \cdot b'$.

2) A adição e a multiplicação satisfazem a propriedade *comutativa*, isto é, para todos $a, b \in \mathbb{Z}$, temos que

$$a + b = b + a \quad \text{e} \quad a \cdot b = b \cdot a.$$

3) A adição e a multiplicação são *associativas*, isto é, para todos $a, b, c \in \mathbb{Z}$, temos

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

4) A adição e a multiplicação satisfazem a propriedade de *existência do elemento neutro*, isto é, para todo $a \in \mathbb{Z}$, $a+0=a$ e $a\cdot 1 = 0$.

5) A adição possui *elementos simétricos*, isto é, para todo $a \in \mathbb{Z}$, existe $b = -a$ tal que $a+b=0$.

6) A multiplicação é *distributiva* com relação à adição, isto é, para todos $a, b, c \in \mathbb{Z}$, tem-se $a\cdot(b+c) = a\cdot b + a\cdot c$.

A Propriedade 1 é que permite somar um dado número a ambos os lados de uma igualdade, ou multiplicar ambos os lados por um mesmo número. Note que o conjunto dos números inteiros é particionado em três subconjuntos:

$$\mathbb{Z} = \mathbb{N} \cup (-\mathbb{N}),$$

onde $\mathbb{N} = \{0, 1, 2, 3, 4, \ldots\}$ e $-\mathbb{N} = \{-n \ ; \ n \in \mathbb{N}\}$, ou seja, $-\mathbb{N}$ é o conjunto dos simétricos dos elementos de $\mathbb{N}$ no conjunto dos números inteiros.

Como consequência das propriedades acima obtemos os próximos resultados.

Proposição 2.6. *Para todo $a \in \mathbb{Z}$ tem-se que $a\cdot 0 = 0$.*

Demonstração: Das Propriedades 4 e 6 temos que

$$\begin{aligned} a\cdot 0 &= a(0+0) \\ &= a\cdot 0 + a\cdot 0. \end{aligned}$$

Utilizando as Propriedades 4 e 3 e a igualdade acima, temos

$$\begin{aligned} a \cdot 0 &= 0 + a \cdot 0 \\ &= (-(a \cdot 0) + (a \cdot 0)) + a \cdot 0 \\ &= -(a \cdot 0) + (a \cdot 0) + a \cdot 0 \\ &= -(a \cdot 0) + a \cdot 0 + a \cdot 0 \\ &= -(a \cdot 0) + a(0 + 0) \\ &= -(a \cdot 0) + a \cdot 0 \\ &= (-(a \cdot 0) + a \cdot 0) \\ &= 0, \end{aligned}$$

demonstrando a proposição. ■

Proposição 2.7. *Para $a, b \in \mathbb{Z}$, tem-se que $(-a) \cdot b = -(a \cdot b)$.*

Demonstração: Como $a \cdot b + (-a) \cdot b = (a + (-a)) \cdot b = 0 \cdot b = 0$ temos pela unicidade do elemento oposto de um número que $(-a) \cdot b = -(a \cdot b)$, completando a demonstração. ■

Proposição 2.8. *A adição é compatível e cancelativa com respeito à igualdade, isto é, para todos $a, b, c \in \mathbb{Z}$, temos que*

$$a = b \Longleftrightarrow a + c = b + c.$$

Demonstração: A implicação $a = b \Rightarrow a + c = b + c$ é consequência do fato de a adição ser bem definida (Propriedade 1). Suponhamos agora que $a + c = b + c$. Somando $(-c)$ em ambos os lados desta igualdade temos

$$[a + c] + (-c) = [b + c] + (-c)$$

e pela propriedade associativa, temos

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

onde pela propriedade de existência do elemento oposto temos

$$a + (0) = b + (0)$$

o que implica pela propriedade de existência do elemento neutro

$$a = b,$$

completando a demonstração. ■

2.3 Ordenação dos Inteiros

Existem outros conjuntos diferentes dos inteiros, munidos de operações de adição e multiplicação que possuem as Propriedades de 1 a 6 da seção anterior. Tais conjuntos, como por exemplo o conjunto dos números racionais, reais e os complexos, juntamente com suas operações são chamados de *aneis*. Portanto, dada a existência com operações de adição e multiplicação sujeitos às leis básicas da aritmética, vemos que os axiomas acima não caracterizam os inteiros. No decorrer dessa seção veremos mais alguns axiomas necessários para diferenciar o conjunto dos inteiros desses outros conjuntos.

Admitiremos que em $\mathbb{Z}$ também valem as seguintes propriedades do conjunto $\mathbb{N}$:

7) *Fechamento de* $\mathbb{Z}$: O conjunto $\mathbb{Z}$ é fechado para a adição e para a multiplicação, ou seja, para todos $a, b \in \mathbb{Z}$, tem-se que $a + b \in \mathbb{Z}$ e $a \cdot b \in \mathbb{Z}$.

8) *Tricotomia*: Dados $a, b \in \mathbb{Z}$, uma e apenas uma, das seguintes possibilidades é verificada:

(i) $a = b$;

(ii) $b - a \in \mathbb{N}^* = \mathbb{N}\backslash\{0\}$;

(iii) $-(b - a) = a - b \in \mathbb{N}^* = \mathbb{N}\backslash\{0\}$.

Sejam $a, b \in \mathbb{Z}$. Diremos que a é *menor do que* b, simbolizado por $a < b$, toda vez que o item (ii) da propriedade acima for verificado. Com essa definição, temos que o item (iii) da propriedade

acima equivale a afirmar que $b < a$. Assim, a Tricotomia nos diz que, dados $a, b \in \mathbb{Z}$, uma, e somente uma, das seguintes condições é verificada:

(i) $a = b$;

(ii) $a < b$;

(iii) $b < a$.

Utilizaremos a notação $b > a$, que se lê b é *maior do que* a, para representar $a < b$. Como $a - 0 = a$, decorre das definições que $a > 0$ se, e somente se, $a \in \mathbb{N}$. Portanto,

$$\{x \in \mathbb{Z} \ ; \ x > 0\} = \mathbb{N}$$

e

$$\{x \in \mathbb{Z} \ ; \ x < 0\} = -\mathbb{N}.$$

Daí decorre que $a > 0$ se, e somente se, $-a < 0$.

Proposição 2.9. *A relação "menor do que" é transitiva, isto é, para todos* $a, b, c \in \mathbb{Z}$, *temos que*

$$a < b \quad e \quad b < c \Longrightarrow a < c.$$

Demonstração: Sejam a, b e $c \in \mathbb{Z}$. Supondo $a < b$ e $b < c$, temos que $b - a \in \mathbb{N}$ e $c - b \in \mathbb{N}$. Como $\mathbb{N}$ é fechado com relação a adição, temos que

$$c - a = c + 0 - a = c + (-b + b) - a = (c - b) + (b - a) \in \mathbb{N}.$$

Logo, $a < c$, finalizando a demonstração. ■

Proposição 2.10. *A adição é compatível e cancelativa com respeito à relação "menor do que", isto é, para todos* $a, b, c \in \mathbb{Z}$, *temos que*

$$a < b \Longleftrightarrow a + c < b + c.$$

Demonstração: Sejam a, b e $c \in \mathbb{Z}$ e suponhamos $a < b$. Logo, $b - a \in \mathbb{N}$. Portanto,

$$\begin{aligned}(b+c)-(a+c) &= b+c+(-1\cdot(a+c))\\ &= b+c+((-1\cdot a)+(-1\cdot c))\\ &= b+c+(-a+(-c))\\ &= b+c-a-c\\ &= b+c-c-a\\ &= b+0-a\\ &= b-a \in \mathbb{N},\end{aligned}$$

o que implica que $a + c < b + c$.

Reciprocamente, supondo que $a + c < b + c$. Pela primeira parte da demonstração, podemos somar $(-c)$ em ambos os lados da desigualdade e assim temos $a < b$. ■

Proposição 2.11. *A multiplicação por elementos de $\mathbb{N}$ é compatível e cancelativa com respeito à relação "menor do que", isto é, para todos $a, b \in \mathbb{Z}$ e para todo $c \neq 0 \in \mathbb{N}$, temos que*

$$a < b \Longleftrightarrow a \cdot c < b \cdot c.$$

Demonstração: Sejam $a, b \in \mathbb{Z}$, $c \in \mathbb{N}$ e suponhamos que $a < b$. Logo, $b - a \in \mathbb{N}$. Pelo fato de $\mathbb{N}$ ser fechado para a multiplicação, temos

$$b \cdot c - a \cdot c = (b - a) \cdot c \in \mathbb{N}.$$

Logo, $a \cdot c < b \cdot c$.

Reciprocamente, suponhamos que $a \cdot c < b \cdot c$, com $c \in \mathbb{N}$. Temos três possibilidades a analisar.

(i) Caso $a = b$. Este caso não ocorre, pois isso acarretaria $a \cdot c = b \cdot c$ uma vez que a multiplicação está bem definida.

(ii) Caso $b < a$. O que também não ocorre, pois pela primeira parte da demonstração teríamos $b \cdot c < a \cdot c$ mas por hipótese $a \cdot c < b \cdot c$.

(iii) Caso $b > a$. Segue da Tricotomia que este é o único caso possível, completando a demonstração.

■

Observação 2.12. *Note que se $d, e \in \mathbb{Z}$ temos $d < e$ se, e somente se, $-d > -e$.*

De fato: Se $d < e$, somando $-(d + e)$ em ambos os lados, temos $-e < -d$, ou então, $-d > -e$.

Reciprocamente, se $-d > -e$, somando $(d + e)$ em ambos os lados da desigualdade, temos $e > d$, ou ainda $d < e$. □

Esta observação permanece válida ao trocarmos $<$ por $\leq$.

Proposição 2.13. *A multiplicação é compatível e cancelativa com respeito à igualdade, isto é, para todos $a, b \in \mathbb{Z}$ e todo $c \in \mathbb{Z}\backslash\{0\}$, temos que*

$$a = b \iff a \cdot c = b \cdot c.$$

Demonstração: A implicação $a = b \Rightarrow a \cdot c = b \cdot c$ decorre do fato da multiplicação ser bem definida e vale também quando $c = 0$.

Reciprocamente, suponhamos que $a \cdot c = b \cdot c$. Temos duas possibilidades para analisar.

(i) Caso $c > 0$. Pela tricotomia temos que $a < b$ ou $b < a$ ou $a = b$. Se $a < b$, pela Proposição 2.11, temos que $a \cdot c < b \cdot c$, o que é um absurdo. Se $b < a$, pelo mesmo argumento temos $b \cdot c < a \cdot c$, que também é um absurdo. Portanto, a única alternativa válida é $a = b$.

(ii) Caso $-c > 0$. Se $a < b$, pela Proposição 2.11, temos que $a \cdot (-c) < b \cdot (-c)$ e então pela Proposição 2.7, temos $-a \cdot c < -b \cdot c$ e pela Observação 2.12 isto implica em $a \cdot c > b \cdot c$, o que é um absurdo. Se $b < a$, temos $b \cdot (-c) < a \cdot (-c) \Rightarrow -b \cdot c < -a \cdot c$ e do mesmo modo isto implica em $b \cdot c > a \cdot c$ que também é um absurdo. Logo, $a = b$.

Assim, completamos a demonstração. ■

Definimos agora a importante noção de valor absoluto.

Definição 2.14. *Seja $a \in \mathbb{Z}$, definimos*

$$|a| = \begin{cases} a, \ se & a \geq 0 \\ -a, \ se & a < 0 \end{cases} .$$

Note que para todo $a \in \mathbb{Z}$, tem-se que $|a| \geq 0$ e $|a| = 0$ se, e somente se, $a = 0$.

O número inteiro não negativo $|a|$ é chamado de *módulo* ou *valor absoluto* de a.

Proposição 2.15. *Para $a, b \in \mathbb{Z}$ e $r \in \mathbb{N}$, temos*

i) $|a \cdot b| = |a| \cdot |b|$;

ii) $-|a| \leq a \leq |a|$;

iii) $|a| \leq r$ *se, e somente se,* $-r \leq a \leq r$;

iv) a desigualdade triangular

$$|a + b| \leq |a| + |b|.$$

Demonstração: Para o item *i)* temos seis casos a analisar de acordo com sinais de a e de b:

Caso 1: $a = 0$ e $b \in \mathbb{Z}$ qualquer. Como $a = 0$, então $a \cdot b = 0$ e $|a| = 0$. Assim, $|a \cdot b| = |0| = 0$ e $|a| \cdot |b| = 0$. Logo, $|a \cdot b| = |a| \cdot |b|$.

Caso 2: $b = 0$ e $a \in \mathbb{Z}$ qualquer. Como $b = 0$, então $a \cdot b = 0$ e $|b| = 0$. Assim, $|a \cdot b| = |0| = 0$ e $|a| \cdot |b| = 0$. Logo, $|a \cdot b| = |a| \cdot |b|$.

Caso 3: $a > 0$ e $b > 0$. Como a e b são positivos, temos $a \cdot b > 0$, $|a| = a$ e $|b| = b$ então $|a \cdot b| = a \cdot b = |a| \cdot |b|$.

Caso 4: $a > 0$ e $b < 0$. Como a é positivo e b negativo, temos $a \cdot b < 0$, $|a| = a$ e $|b| = -b$. Então, $|a \cdot b| = -(a \cdot b) = a \cdot (-b) = |a| \cdot |b|$.

Caso 5: $a < 0$ e $b > 0$. Como a é negativo e b positivo, temos $a \cdot b < 0$, $|a| = -a$ e $|b| = b$. Então, $|a \cdot b| = -(a \cdot b) = (-a) \cdot b = |a| \cdot |b|$.

Caso 6: $a < 0$ e $b < 0$. Como a e b são negativos temos $a \cdot b > 0$, $|a| = -a$ e $|b| = -b$. Então $|a \cdot b| = a \cdot b = (-a) \cdot (-b) = |a| \cdot |b|$.

Em qualquer caso temos sempre que $|a \cdot b| = |a| \cdot |b|$, completando o item i).

Para o item ii) temos que analisar quando $a > 0$ e $a < 0$:

Caso 1: Se $a > 0$ temos $|a| = a$, $-|a| = -a$ e $-a \leq a$. Como $a = |a|$, então $a \leq |a|$ e como $-a \leq -|a|$, usando a desigualdade acima, obtemos

$$-|a| \leq a \leq |a|.$$

Caso 2: Se $a < 0$ temos $|a| = -a$, $-|a| = a$ e $a \leq -a$. Daí, como $-|a| = a$, então $-|a| \leq a$ e usando a última desigualdade acima, temos

$$-|a| \leq a \leq |a|,$$

finalizando o item ii).

Para o item iii), se $|a| \leq r$, então pela Observação 2.12 temos $-|a| \geq -r$. Pelo item ii) temos $-|a| \leq a \leq |a|$. Daí

$$-r \leq -|a| \leq a \leq |a| \leq r.$$

Logo, $-r \leq a \leq r$, terminando o item iii).

Para o item iv), se a e $b \in \mathbb{Z}$, temos pelo item ii) que $-|a| \leq a \leq |a|$ e que $-|b| \leq b \leq |b|$. Somando estas duas desigualdades membro a membro obtemos que

$$\begin{array}{rcccl} -|a| - |b| & \leq & a + b & \leq & |a| + |b| \\ -(|a| + |b|) & \leq & a + b & \leq & |a| + |b|, \end{array}$$

onde pelo item iii) concluímos que $|a + b| \leq |a| + |b|$ e completamos a demonstração. ■

2.4 Princípio da Boa Ordenação

As propriedades dos números inteiros e de suas operações que descrevemos até o momento não bastam para caracterizá-los. Por exemplo, os números racionais possuem todas as propriedades descritas anteriormente, trocando-se apenas na Propriedade 8 (Tricotomia) $\mathbb{N}$ por $\mathbb{Q}_+$. No entanto, há uma propriedade adicional que só os inteiros possuem, que é o *Princípio da Boa Ordenação* e o descreveremos logo adiante.

Diremos que um subconjunto S de $\mathbb{Z}$ é limitado inferiormente, se existir $c \in \mathbb{Z}$ tal que $c \leq x$ para todo $x \in S$. Diremos que $a \in S$ é um menor elemento de S se $a \leq x$ para todo $x \in S$. Convencionamos que o conjunto vazio, apesar de não possuir nenhum elemento, é limitado inferiormente, tendo qualquer número como cota inferior.

Observe que um menor elemento de S, se existir, é único pois se a e a' são menores elementos de S, temos $a \leq a'$ e $a' \leq a$, logo $a = a'$. Por exemplo, $\mathbb{Z}$ e $-\mathbb{N}$ não são limitados inferiormente, nem possuem menor elemento. Por outro lado, $\mathbb{N}$ é limitado inferiormente e possui $1 \in \mathbb{N}$ como menor elemento.

A_0. **Princípio da Boa Ordenação - PBO:**

> Se S é um subconjunto não vazio de $\mathbb{Z}$ e limitado inferiormente, então S possui um menor elemento. Em particular, como qualquer subconjunto de $\mathbb{N}$ é limitado inferiormente (por $1 \in \mathbb{N}$), temos que todo subconjunto não vazio de $\mathbb{N}$ possui um menor elemento.

Vejamos agora, exemplos de propriedade de $\mathbb{Z}$ que podem ser demonstradas com o PBO ou A_0.

Proposição 2.16. *Não existe nenhum número inteiro n tal que $0 < n < 1$.*

Demonstração: Suponhamos, por absurdo, que exista $n \in \mathbb{Z}$ tal que $0 < n < 1$. Assim, o conjunto $S = \{x \in \mathbb{Z}\,;\, 0 < x < 1\}$ é não vazio e limitado inferiormente. Portanto, S possui um menor elemento $a \in S$, com $0 < a < 1$. Multiplicando esta última desigualdade por a, obtemos $0 < a^2 < a < 1$. Logo, $a^2 \in S$ e $a^2 < a$. Absurdo, pois a é o menor elemento. Portanto, $S = \emptyset$, finalizando a demonstração. ■

Corolário 2.17. *Dado um número $n \in \mathbb{Z}$ qualquer, não existe nenhum número $m \in \mathbb{Z}$ tal que $n < m < n + 1$.*

Demonstração: Suponhamos, por absurdo, que exista um inteiro tal que $n < m < n+1$. Subtraindo n em ambos os membros desta desigualdade, obtemos $n - n < m - n < n + 1 - n \Rightarrow 0 < m - n < 1$. Como $m, n \in \mathbb{Z}$ então $m - n \in \mathbb{Z}$, mas pela Proposição 2.16 temos que não existe um inteiro entre 0 e 1. Logo, temos uma contradição e, portanto, não existe um inteiro m tal que $n < m < n + 1$. ■

Corolário 2.18. *Se $a, b \in \mathbb{Z}$, com $b \neq 0$, então $|a \cdot b| \geq |a|$.*

Demonstração: Como temos por hipótese que $b \neq 0$ e que por definição o módulo de um número é sempre não negativo, temos então pela Proposição 2.16 que $|b| \geq 1$. Multiplicando ambos os lados dessa desigualdade por $|a|$ e usando a Proposição 2.15 item i) temos

$$|a \cdot b| = |a| \cdot |b| \geq |a|,$$

completando a demonstração. ■

Corolário 2.19 (Propriedade Arquimediana)**.** *Sejam $a, b \in \mathbb{Z}$, com $b \neq 0$. Então existe $n \in \mathbb{Z}$ tal que $n \cdot b > a$.*

Demonstração: Como $b \neq 0$, então $|b| \neq 0$ e da Proposição 2.16 temos $|b| \geq 1$. Logo, multiplicando ambos os membros dessa igualdade por $|a| + 1$, temos que

$$\begin{aligned}(|a|+1) \cdot |b| > |a| + 1 &\Rightarrow (|a|+1) \cdot |b| > |a| + 1 > |a| \geq a \\ &\Rightarrow (|a|+1) \cdot |b| > a \\ &\Rightarrow (|a|+1) \cdot b > a, \text{ se } b > 0 \text{ ou } -(|a|+1) \cdot b > a, \text{ se } b < 0.\end{aligned}$$

Tomando $n = |a| + 1$, se $b > 0$ e $n = -(|a| + 1)$ se $b < 0$ temos $n \cdot b > a$, obtendo assim o resultado desejado. ■

Uma das mais importantes consequências do Princípio da Boa Ordem é o Princípio de Indução Matemática também conhecido como Princípio de Indução Finita - PIF, que na axiomática de Peano consta como Axioma 4.

A_1. **Primeira Forma do Princípio de Indução Finita:**

Seja B um subconjunto de números inteiros e positivos. Suponha que B possui as duas seguintes propriedades

(i) $1 \in B$;

(ii) $k + 1 \in B$ sempre que $k \in B$.

Então, B contém todos os números inteiros positivos.

A_2. **Segunda Forma do Princípio de Indução Finita:**

Seja B um subconjunto de números inteiros e positivos. Suponha que B possui as duas seguintes propriedades

(i) $1 \in B$;

(ii) $k+1 \in B$ sempre que $1, 2, \ldots, k \in B$.

Então, B contém todos os números inteiros positivos.

Esses conceitos definidos acima são equivalentes, como mostra o próximo teorema.

Teorema 2.20. *O Princípio da Boa Ordem - A_0, a Primeira Forma do Princípio de Indução Finita - A_1 e a Segunda Forma do Princípio de Indução Finita - A_2 são equivalentes.*

Demonstração: Mostremos inicialmente que $A_0 \Rightarrow A_1$. Para este caso faremos a demonstração por contradição. Suponhamos que o conjunto B possui as propriedades (i) e (ii) mas não contém todos os inteiros positivos. Seja então A o conjunto dos números inteiros positivos não pertencentes a B. Pelo Princípio da Boa Ordem A possui um menor elemento, que denotaremos por $a_0 \in A$. Pelo item (i) $1 \in B$, então $a_0 > 1$. Então $a_0 - 1 \in B$ e, como B satisfaz (ii), o sucessor de $a_0 - 1$ que é a_0, também deve pertencer a B. Absurdo. Logo, $A = \emptyset$ e, portanto, B contém todos os inteiros positivos.

Mostremos agora que $A_1 \Rightarrow A_2$. Seja C um conjunto qualquer de números inteiros positivos satisfazendo as propriedades (i) e (ii) de A_2. Devemos mostrar que C contém todos os números inteiros positivos usando A_1. Seja B_n a sentença "todos os inteiros de 1 a n, estão em C". B_1 é verdadeira por hipótese. Assumimos agora que B_k é verdadeira para um número inteiro positivo qualquer $k \in \mathbb{Z}$. Então os inteiros de 1 a k estão em C. Como pelo Corolário 2.17 não existe um inteiro entre dois inteiros consecutivos, concluímos por hipótese que $k+1$ está em C e B_{k+1} é verdadeira. Logo, por A_1, B_n é verdadeira para todo inteiro positivo n e, portanto, C contém todos os números inteiros positivos.

Mostremos agora que $A_2 \Rightarrow A_0$. Seja C um conjunto não vazio de números inteiros positivos. Temos que mostrar que C possui um menor elemento. Suponhamos, por absurdo, que C não possui um elemento menor elemento e seja B_n a sentença "n não é um elemento de C". Logo, B_1 é verdadeira

pois 1 é o menor número inteiro positivo. Assumimos agora, B_k verdadeira para todo $n = 1, 2, \ldots, k$. Disto concluímos que B_{k+1} é verdadeira pois caso contrário, $k + 1$ seria o menor elemento de C, uma vez que não existe um número inteiro entre dois inteiros consecutivos. Portanto, por A_2, B_n é verdadeira para todo número inteiro positivo $n \in \mathbb{Z}$. Mas isto implica que C é vazio, contrariando a hipótese. Portanto, C possui um elemento mínimo, completando a demonstração do teorema. ■

Vejamos agora alguns exemplos desses conceitos.

Exemplo 2.21. *Vamos mostrar que*

$$1 + x^2 + ... + x^{n-1} = \frac{x^n - 1}{x - 1},$$

para todo $x \in \mathbb{R}, x \neq 1$.

De fato: Primeiro devemos mostrar que a expressão é verdadeira para $n = 1$. De fato,

$$x^0 = 1 = \frac{x^1 - 1}{x^1 - 1},$$

mostrando que a afirmação é verdadeira para $n = 1$.

Assumimos a validade da expressão para $n-1$ e mostraremos que ela se verifica para n. Temos

$$\begin{aligned} 1 + x + x^2 + \cdots + x^n &= 1 + x + x^2 + \cdots + x^{n-1} + x^n \\ &= \frac{x^n - 1}{x - 1} + x^n \\ &= \frac{x^n(x - 1) + x^n - 1}{x - 1} \\ &= \frac{x^{n+1} - x^n + x^n - 1}{x - 1} \\ &= \frac{x^{n+1} - 1}{x - 1}. \end{aligned}$$

Logo, a validade da expressão para $n - 1$ implica na validade da expressão para n e portanto, pelo PIF, concluímos a validade desta fórmula para todo inteiro positivo, completando o exemplo. □

Fixaremos que a partir desta seção usaremos a notação xy ou $x.y$ quando necessário, ao invés de $x \cdot y$, para representar a multiplicação usual de números reais x e y quaisquer.

2.5 Divisibilidade

Dados dois números inteiros quaisquer, é possível somá-los, subtraí-los e multiplicá-los. Entretanto, nem sempre é possível dividir um pelo outro, por exemplo: em $\mathbb{Z}$ não é possível dividir 3 por 2, mas é possível dividir 4 por 2. Como a divisão de um número inteiro por outro nem sempre é possível, expressa-se essa possibilidade através da relação de divisibilidade. Quando não existir uma relação de divisibilidade entre dois números inteiros, veremos que, ainda assim, será possível efetuar uma "divisão com resto pequeno", chamada de *divisão euclidiana*. O fato de sempre ser possível efetuar tal divisão é responsável por inúmeras propriedades dos inteiros que exploraremos nesta seção.

Definição 2.22. *Sejam $a, b \in \mathbb{Z}$ números inteiros. Dizemos que a divide b e denotamos $a|b$, se existir um inteiro $c \in \mathbb{Z}$ tal que $b = ac$. Se a não divide b escrevemos $a \nmid b$.*

Vejamos algumas propriedades da divisibilidade de números inteiros.

Proposição 2.23. *Sejam $a, b, c \in \mathbb{Z}$ números inteiros tais que $a|b$ e $b|c$. Então $a|c$.*

Demonstração: Como $a|b$ então existe um $q_1 \in \mathbb{Z}$ tal que $b = aq_1$. Como $b|c$ existe um $q_2 \in \mathbb{Z}$ tal que $c = bq_2$.

Assim, substituindo $b = aq_1$ em $c = bq_2$, temos que

$$c = bq_2 = (aq_1)q_2 = a(q_1q_2).$$

Como q_1 e $q_2 \in \mathbb{Z}$ então $q_1q_2 \in \mathbb{Z}$. Logo, $a|c$, completando a demonstração. ■

Proposição 2.24. *Se $a, b, c, m, n \in \mathbb{Z}$ são inteiros tais que $c|a$ e $c|b$. Então $c|(ma + nb)$.*

Demonstração: Como $c|a$ e $c|b$ então existem inteiros $q_1, q_2 \in \mathbb{Z}$ tais que $a = cq_1$ e $b = cq_2$. Multiplicando $a = cq_1$ por m e $b = cq_2$ por n, temos $ma = mcq_1$ e $nb = ncq_2$. Somando estas duas equações membro a membro obtemos que

$$ma + nb = mcq_1 + ncq_2 = c(mq_1 + nq_2)$$

e como m, q_1, n e $q_2 \in \mathbb{Z}$ temos $mq_1, nq_2 \in \mathbb{Z}$ e $mq_1 + nq_2 \in \mathbb{Z}$. Portanto, $c|(ma + nb)$. ■

Suponhamos que $a|b$ e que $a \neq 0$. Seja $c \in \mathbb{Z}$ tal que $b = ca$. **O número c, univocamente determinado é chamado de quociente de b por a e denotado por $c = \frac{b}{a}$.** Para mostrarmos a unicidade suponhamos que existam $c_1, c_2 \in \mathbb{Z}$ tais que $b = c_1a$ e $b = c_2a$. Então $c_1a = c_2a$ e a Proposição 2.11 implica que $c_1 = c_2$.

Teorema 2.25. *Dados $a, b, c, d, n \in \mathbb{Z}$ números inteiros. A divisibilidade tem as seguintes propriedades:*

(i) $n|n$.

(ii) $d|n \Rightarrow ad|an$.

(iii) *Se* $ad|an$ *e* $a \neq 0$, *então* $d|n$.

(iv) $1|n$.

(v) $n|0$.

(vi) *Se* $d|n$ *e* $n \neq 0$, *então* $|d| \leq |n|$.

(vii) *Se* $d|n$ *e* $n|d$, *então* $|d| = |n|$.

(viii) *Se* $d|n$ *e* $d \neq 0$, *então* $(\frac{n}{d})|n$.

(ix) $0|a \iff a = 0$.

(x) a *divide* b *se, e somente se,* $|a|$ *divide* $|b|$.

(xi) *Se* $a|(b \pm c,)$ *então* $a|b \iff a|c$.

Demonstração: Para o item (i), como $n = 1 \cdot n$, segue da definição que $n|n$, inclusive para $n = 0$.

Para o item (ii), temos que se $d|n$, então $n = dc$ para algum $c \in \mathbb{Z}$. Multiplicando esta última igualdade por $a \in \mathbb{Z}$, temos $an = adc$, ou seja, $an = (ad)c$ e como $c \in \mathbb{Z}$ temos que $ad|an$.

Para o item (iii), se $ad|an$, então $an = tad$ para algum inteiro $t \in \mathbb{Z}$. Como $a \neq 0$, dividindo ambos os lados da igualdade por a, obtém-se $n = td$ concluindo que $d|n$.

Para o item (iv), como $n = n \cdot 1$, segue da definição que $1|n$.

Para o item (v), como $0 = 0 \cdot n$, segue da definição que $n|0$.

Para o item (vi), se $d|n$, então $n = dc$ para algum $c \in \mathbb{Z}$. Tomando o módulo em ambos os lados desta igualdade, temos,

$$|n| = |dc| = |d||c|.$$

Como $n \neq 0$ temos $c \neq 0$, logo $|c| \geq 1$. Daí, multiplicando essa última desigualdade por $|d|$, temos

$$|d||c| \geq |d|1 = |d|.$$

Logo,

$$|n| = |d||c| \geq |d|.$$

Para o item (vii), se $d|n$ temos pelo item anterior que $|d| \leq |n|$. Do mesmo modo, se $n|d$ temos $|n| \leq |d|$. Logo, $|d| = |n|$.

Para o item $(viii)$, se $d|n$, então $n = kd$ para algum $k \in \mathbb{Z}$, portanto, $\frac{n}{d} \in \mathbb{Z}$ é um número inteiro. Como $\frac{n}{d} \cdot d = n$ segue da definição que $(\frac{n}{d})|n$.

Para o item (ix), suponhamos que $0|a$. Logo, existe $c \in \mathbb{Z}$ tal que $a = c \cdot 0$. Pela Proposição 2.6, conclui-se que $a = 0$. Reciprocamente, se $a = 0$ segue do item (v) que $0|0$, uma vez que qualquer inteiro divide o zero.

Para o item (x), se a divide b, então existe $c \in \mathbb{Z}$ tal que $b = ac$. Tomando o módulo em ambos os lados desta igualdade temos $|b| = |ac|$ e a Proposição 2.15 implica que $|b| = |a||c|$ e assim $|a|$ divide $|b|$. Reciprocamente, se $|a|$ divide $|b|$ então existe $c > 0$ (uma vez que $|a|, |b| \geq 0$) tal que $|b| = |a|c$. Como $c > 0$ temos $c = |c|$ e assim,

$$\begin{aligned} |b| = |a||c| &\Rightarrow |b| = |ac| \\ &\Rightarrow b = \pm ac \\ &\Rightarrow b = a(\pm c). \end{aligned}$$

Então,

$$b = a(-c) \text{ ou } b = a(+c).$$

Em ambos os casos concluímos que $a|b$.

Para o item (xi), suponhamos que $a|(b+c)$. Logo, existe $f \in \mathbb{Z}$ tal que $b + c = fa$. Agora se $a|b$, temos que existe $g \in \mathbb{Z}$ tal que $b = ga$. Juntando as duas igualdades temos

$$\begin{aligned} ga + c = fa &\Rightarrow c = fa - ga \\ &\Rightarrow c = (f - g)a. \end{aligned}$$

Logo, $a|c$. Por outro lado, se $a|(b-c)$ e $a|b$, temos que $a|(-c)$, o que implica que $a|c$.

Reciprocamente, se $a|(b+c)$ existe $f_1 \in \mathbb{Z}$ tal que $b + c = f_1 a$. Se $a|c$ existe $g_1 \in \mathbb{Z}$ $c = g_1 a$. Assim,

$$\begin{aligned} b + g_1 a = f_1 a &\Rightarrow b = f_1 a - g_1 a \\ &\Rightarrow b = (f_1 - g_1)a \end{aligned}$$

e portanto, $a|b$. Do mesmo, se $a|(b-c)$ e $a|c$, temos que $a|b$, finalizando o item e completando a prova do teorema. ■

Vamos apresentar agora o Algoritmo da Divisão de Euclides.

Teorema 2.26 (Divisão Euclidiana)**.** *Se $a, b \in \mathbb{Z}$, com $b \neq 0$, então existem únicos números inteiros $q, r \in \mathbb{Z}$, com $0 \leq r < |b|$ tais que*

$$a = bq + r.$$

Demonstração: Considere o conjunto

$$S = \{x = a - by; y \in \mathbb{Z}\} \cap \{\mathbb{N} \cup \{0\}\}.$$

Vamos separar a demonstração em duas partes.

Para provarmos a existência, a propriedade Arquimediana implica que existe $n \in \mathbb{Z}$ tal que $n.(-b) > -a$, logo $a - nb > 0$, o que mostra que S é não vazio. O conjunto S é limitado inferiormente por 0, logo pelo Princípio da Boa Ordenação, temos que S possui um menor elemento $r \in S$. Logo, existe $q \in \mathbb{Z}$ tal que $r = a - bq$. Sabemos que $r \geq 0$. Vamos mostrar que $r < |b|$. Suponhamos, por absurdo, que $r \geq |b|$, então existe $s \in \mathbb{N} \cup \{0\}$ tal que $r = |b| + s$, logo $0 \leq s < r$. Mas isso contradiz o fato de r ser o menor elemento de S, pois $s = r - |b| = a - bq - |b| = a - (q \pm 1)b \in S$, com $s < r$. Portanto, $r < |b|$.

Para demonstrarmos a unicidade, suponhamos que $a = bq + r = bq' + r'$, onde $q, q', r, r' \in \mathbb{Z}, \underbrace{0 \leq r < |b|}_{i}$ e $\underbrace{0 \leq r' < |b|}_{ii}$. Assim, multiplicando i por (-1), obtemos $\underbrace{-|b| < -r \leq 0}_{iii}$ e somando ii e iii, temos

$$-|b| < r' - r < |b|.$$

Então,

$$|r' - r| < |b|.$$

Por outro lado, como

$$a = bq + r = bq' + r' \Rightarrow bq - bq' = r' - r \Rightarrow b(q - q') = r' - r,$$

temos que

$$|b||q - q'| = |r' - r| < |b| \Rightarrow |b||q - q'| < |b| \Rightarrow |q - q'| < 1.$$

Mas isso só é possível se $q = q'$ e consequentemente se $r = r'$, provando a unicidade desejada e completando a demonstração do teorema. ■

Nas condições do teorema acima, os números q e r são chamados, respectivamente, de *quociente*

e de *resto* da divisão de a e b. Da Divisão Euclidiana, temos que o resto da divisão de a por b é zero se, e somente se, b divide a. Vamos agora apresentar alguns exemplos.

Exemplo 2.27. *O quociente e o resto da divisão de* 19 *por* 5 *são* $q = 3$ *e* $r = 4$. *O quociente e o resto da divisão de* -19 *por* 5 *são* $q = -4$ *e* $r = 1$.

Exemplo 2.28. *Dado um número inteiro* $n \in \mathbb{Z}$ *qualquer, temos duas possibilidades:*

i) o resto da divisão de n *por* 2 *é* 0, *isto é, existe* $q \in \mathbb{N}$ *tal que* $n = 2q$; *ou*

ii) o resto da divisão de n *por* 2 *é* 1, *ou seja, existe* $q \in \mathbb{N}$ *tal que* $n = 2q + 1$.

Portanto, os números inteiros dividem-se em duas classes, a dos números das forma $2q$ para algum $q \in \mathbb{Z}$, chamados de *números pares*, e a dos números da forma $2q + 1$ para algum $q \in \mathbb{Z}$, chamados de *números ímpares*. Os naturais são classificados em pares e ímpares, pelo menos, desde Pitágoras, 500 a.C.

2.6 O Máximo Divisor Comum

Nesta seção abordaremos o conceito de máximo divisor comum, presente na definição de primos entre si, que por sua vez tem grande importância nas demonstrações dos resultados contidos na próxima seção.

O máximo divisor comum de dois inteiros $a, b \in \mathbb{Z}$ nem todos nulos, denotado por $mdc(a, b)$, é o maior inteiro que divide a e b ao mesmo tempo.

Teorema 2.29. *Dados* $a, b \in \mathbb{Z}$ *dois números inteiros nem todos nulos, existem* $x_0, y_0 \in \mathbb{Z}$ *tais que*

$$ax_0 + by_0 = mdc(a, b) > 0.$$

Demonstração: Considere a combinação linear $ax + by$ com $x, y \in \mathbb{Z}$. Este conjunto de inteiros denotado por

$$\mathcal{C}_{a,b} = \{ax + by \ ; \ x, y \in \mathbb{Z}\}$$

inclui valores positivos e negativos. Além disso, este conjunto é não vazio, pois $a^2+b^2 = a.a+b.b \in \mathcal{C}_{a,b}$ e ainda, escolhendo $x = y = 0$ vemos que $0 \in \mathcal{C}_{a,b}$. Pelo Princípio da Boa Ordenação, podemos escolher x_0, y_0 tais que $\lambda = ax_0 + by_0$ seja o menor número inteiro positivo contido no conjunto $\mathcal{C}_{a,b}$.

Agora, mostraremos que $\lambda|a$ e $\lambda|b$. Provaremos que $\lambda|a$ apenas pois o caso $\lambda|b$ segue analogamente. Suponhamos, por absurdo, que $\lambda \nmid a$, então existem inteiros $q, r \in \mathbb{Z}$ tais que $a = \lambda q + r$ com $0 < r < \lambda$. Portanto,

$$r = a - \lambda q = a - q(ax_0 + by_0) = a(1 - qx_0) + b(-qy_0).$$

Assim, $r \in \mathcal{C}_{a,b}$, o que contradiz a hipótese de λ ser o menor elemento positivo em $\mathcal{C}_{a,b}$. Resta agora provar que $\lambda = mdc(a, b)$. Seja $d = mdc(a, b)$, então temos que $d|a$ e $d|b$. Assim, $a = da_1$, $b = db_1$ e

$$\lambda = ax_0 + by_0 = da_1x_0 + db_1y_0 = d(a_1x_0 + b_1y_0).$$

Logo, $d|\lambda$. Como $d|\lambda$ e $\lambda \in \mathbb{Z}$ é um número inteiro positivo temos pelo Teorema 2.25 item (vi) que $d \leq \lambda$. Agora, $d < \lambda$ é impossível pois $d = mdc(a, b)$ e, portanto, $d = \lambda = ax_0 + by_0 = mdc(a, b)$, completando a demonstração. ■

Uma observação pertinente é a seguinte:

Observação 2.30. *Na demonstração deste teorema mostramos não apenas que o máximo divisor comum de a e b pode ser expresso como uma combinação linear destes números, mas que este número é o menor valor positivo dentre todas estas combinações lineares. O próximo teorema nos dá uma outra caracterização para o máximo divisor comum de dois números inteiros.*

Teorema 2.31. *Sejam $a, b \in \mathbb{Z}$ não todos nulos. O máximo divisor comum $d = mdc(a, b)$ de a e b é o divisor positivo de a e b o qual é divisível por todo divisor comum de a e b.*

Demonstração: Seja $d = mdc(a.b)$ o máximo divisor comum de a b. Se d_1 é divisor comum de a e b temos pela Proposição 2.24 que d_1 divide qualquer combinação de a e b. Do teorema anterior, como d é uma combinação de a e b concluímos que $d_1|d$. ■

Observação 2.32. *Note que este teorema implica que se $d = mdc(a, b)$ e $d' = mdc(a, b)$ para $a, b \in \mathbb{Z}$, então $d|d'$ e $d'|d$ e juntamente com as condições $d > 0$ e $d' > 0$ temos pelo Teorema 2.25 item $(viii)$ que $d = d'$, ou seja, o mdc de dois números, quando existe é único. Sendo assim, diremos que um número inteiro positivo $d = mdc(a, b)$ é o máximo divisor comum de a e b, se possuir as seguintes propriedades:*

(i) d é um divisor comum de a e b, e

(ii) se c é um divisor comum de a e b, então $c|d$.

Como o máximo divisor comum de a e b não depende da ordem em que a e b são tomados, temos que

$$mdc(a,b) = mdc(b,a).$$

Em algum casos particulares, é simples verificar a existência do máximo divisor comum. Por exemplo, se a é um número inteiro tem-se que $mdc(0,a) = |a|$, $mdc(1,a) = 1$ e que $mdc(a,a) = |a|$. Mais ainda, para todo $b \in \mathbb{Z}$, temos que

$$a|b \iff mdc(a,b) = |a|.$$

Para demonstramos este fato, temos que se $a|b$, então $|a|$ é um divisor comum de a e b, se c é um divisor comum de a e b, então c divide $|a|$, o que mostra que $|a| = mdc(a,b)$. Reciprocamente, se $mdc(a,b) = |a|$, segue-se que $|a|$ divide b, logo $a|b$.

Além disso, temos que

$$a = b = 0 \iff mdc(a,b) = 0.$$

De fato, como todo número inteiro divide 0, o máximo divisor comum de a e b, onde $a = b = 0$, é 0, pois esse é um divisor comum de a e b e é o único número divisível por todos os divisores de 0. Reciprocamente, se o $mdc(a,b) = 0$, então 0 divide a e divide b, mas o único número divisível por 0 é o próprio 0, logo $a = b = 0$.

Observamos que dados $a, b \in \mathbb{Z}$, se existir o $mdc(a,b)$, então

$$mdc(a,b) = mdc(-a,b) = mdc(a,-b) = mdc(-a,-b).$$

Para mostrarmos a primeira igualdade, seja $d = mdc(a,b)$. Pelo item (i) da Observação 2.32 isso implica que $d|a$ e $d|b$. Para mostrarmos que $d = mdc(-a,b)$ temos que mostrar $d|-a$, $d|b$ e se c é um outro divisor comum de $-a$ e b então $c|d$.

Já temos que $d|b$ e como $d|a$ então $a = dq$, para algum inteiro $q \in \mathbb{Z}$. Multiplicando essa última igualdade por (-1) temos $-a = -dq \Rightarrow -a = d(-q)$ e assim $d|-a$. Agora, seja c um divisor comum de $-a$ e b. Como $c|-a$ temos que $c|a$, logo $c|a$ e $c|b$. Ou seja, c é um divisor comum de a e b,

mas pelo item (ii) da Observação 2.32 isso implica que $c|mdc(a,b) = d$. Portanto, $d = mdc(-a,b)$.

As outras igualdades são demonstradas de forma análoga.

Assim, para efeito do cálculo do máximo divisor comum de dois números, podemos sempre supô-los não negativos. Para provar a existência do máximo divisor comum de dois inteiros não negativos, Euclides utilizou, essencialmente, o resultado que demonstraremos mais abaixo (Lema 2.38).

Proposição 2.33. *Para todo inteiro positivo* $0 < t \in \mathbb{Z}, mdc(ta,tb) = t\ mdc(a,b)$

Demonstração: Seja $\tilde{d} = mdc(ta,tb)$. Pelo Teorema 2.29 temos que $mdc(ta,tb)$ é o menor valor positivo dentre todas as combinações de $mta + ntb$ com $m,n \in \mathbb{Z}$, isto é, existem $\tilde{m},\tilde{n}$ tais que

$$0 < \tilde{d} = mdc(ta,tb) = \tilde{m}ta + \tilde{n}tb = t(\tilde{m}a + \tilde{n}b).$$

Se mostrarmos que $\tilde{m}a + \tilde{n}b = d = mdc(a,b)$, teremos que $mdc(ta,tb) = \tilde{d} = t(\tilde{m}a + \tilde{n}b) = td = t\ mdc(a,b)$. De fato, se $d = mdc(a,b)$, temos pelo Teorema 2.29 que d é o menor valor positivo dentre todas as combinações de $ma + nb$ com $m,n \in \mathbb{Z}$ quaisquer, ou seja, existem $m_1,n_1 \in \mathbb{Z}$ tais que

$$0 < d = mdc(a,b) = m_1a + n_1b.$$

Como $\tilde{m}a + \tilde{n}b$ também é uma combinação linear de a e b então

$$0 < d = mdc(a,b) = m_1a + n_1b \leq \tilde{m}a + \tilde{n}b.$$

E assim,

$$0 < m_1a + n_1b \leq \tilde{m}a + \tilde{n}b.$$

Multiplicando esta desigualdade por $t > 0$, obtemos

$$t0 < t(m_1a + n_1b) \leq t(\tilde{m}a + \tilde{n}b) \Rightarrow 0 < m_1ta + n_1tb \leq \tilde{m}ta + \tilde{n}tb = \tilde{d}.$$

Logo, $m_1ta + n_1tb$ é uma outra combinação linear positiva de ta e tb e que não pode ser menor do que $\tilde{d}$. Então, só nos resta

$$m_1ta + n_1tb = \tilde{m}ta + \tilde{n}tb \Rightarrow t(m_1a + n_1b) = t(\tilde{m}a + \tilde{n}b) \Rightarrow m_1a + n_1b = \tilde{m}a + \tilde{n}b.$$

Ou seja,

$$d = m_1a + n_1b = \tilde{m}a + \tilde{n}b,$$

completando a prova da proposição. ■

Como decorrência imediata do resultado acima temos o

Corolário 2.34. *Dados $a, b \in \mathbb{Z}$ não ambos nulos, tem-se que*

$$mdc\left(\frac{a}{mdc(a,b)}, \frac{b}{mdc(a,b)}\right) = 1.$$

Demonstração: Suponhamos que

$$mdc\left(\frac{a}{mdc(a,b)}, \frac{b}{mdc(a,b)}\right) = d \neq 0.$$

Multiplicando por $mdc(a,b)$ em ambos os lados desta igualdade, temos que

$$mdc(a,b)\ mdc\left(\frac{a}{mdc(a,b)}, \frac{b}{mdc(a,b)}\right) = mdc(a,b)d.$$

Pela Proposição 2.33,

$$\left(mdc(a,b)\frac{a}{mdc(a,b)}, mdc(a,b)\frac{b}{mdc(a,b)}\right) = mdc(a,b)d,$$

ou seja,

$$mdc(a,b) = mdc(a,b)d,$$

de onde concluímos que $d = 1$, finalizando a demonstração do corolário. ■

Definição 2.35. *Dois números inteiros $a, b \in \mathbb{Z}$ serão ditos primos entre si, ou relativamente primos, ou coprimos, se $mdc(a,b) = 1$, ou seja, o único divisor comum positivo de ambos é 1.*

Proposição 2.36. *Dois números inteiros $a, b \in \mathbb{Z}$ são primos entre si se, e somente se, existem números inteiros $m, n \in \mathbb{Z}$ tais que $ma + nb = 1$.*

Demonstração: Suponhamos que a e b sejam primos entre si. Logo, $mdc(a, b) = 1$. Pelo Teorema 2.29, temos que existem números inteiros $m, n \in \mathbb{Z}$ tais que $ma + nb = mdc(a, b) = 1$, de onde segue a primeira parte da demonstração. Reciprocamente, suponhamos que existam números inteiros $m, n \in \mathbb{Z}$ tais que $ma + nb = 1$. Se $d = mdc(a, b)$, temos pela Proposição 2.24 que $d|m_0a + n_0b$ com m_0 e n_0 inteiros quaisquer. Em particular, $d|ma + nb$, o que mostra que $d|1$, e portanto, $d = 1$, completando a demonstração. ■

Teorema 2.37. *Sejam $a, b, c \in \mathbb{Z}$ 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 $bc = ae$. Se $mdc(a, b) = 1$, então pela Proposição 2.36, temos que existem $m, n \in \mathbb{Z}$ tais que

$$ma + nb = 1.$$

Multiplicando por c ambos os lados da igualdade acima, temos que

$$c = mac + nbc.$$

Como $bc = ae$, temos que

$$c = mac + nae = a(mc + ne)$$

e, portanto, $a|c$, finalizando a demonstração. ■

Lema 2.38. *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 $d = mdc(a, b - na)$. Então $d|a$ e $d|b - na$. Como $d|a$, temos que $d|na$ e pela Proposição 2.13 $d|(b - na) + na$, ou seja, $d|b$. Logo, d é um divisor comum de a e b. Suponhamos agora que c seja um divisor comum de a e b. Logo, c é um divisor comum de a e $b - na$ e, portanto,

c divide qualquer combinação de a e $b - na$ inclusive a menor combinação positiva e, portanto, $c|d$. Isso prova que $d = mdc(a, b)$. ■

Observação 2.39. *Note que se a, b são inteiros e $b \neq 0$ temos pelo Teorema 2.26 (Divisão Euclidiana) que $a = bq + r \Rightarrow a - bq = r$ e pelo Lema 2.38 $mdc(a, b) = mdc(b, a) = mdc(b, a - bq) = mdc(b, r)$ onde r é o resto da divisão de a por b.*

Vamos apresentar agora o algoritmo de Euclides para o cálculo do máximo divisor comum. Este algorítimo é uma prova construtiva da existência do máximo divisor comum dada por Euclides (*Os elementos*, Livro VII).

Dados $a, b \in \mathbb{N}$, podemos supor $b \leq a$. Se $b = 1$ ou $b = a$, ou ainda $b|a$, já vimos que $mdc(a, b) = a$. Suponhamos, então, que $1 < b < a$ e que $b \nmid a$. Logo, pela Divisão Euclidiana, podemos escrever

$$a = bq_1 + r_1, \text{ com } 0 < r_1 < b.$$

Temos duas possibilidades:

1) $r_1|b$. Nesse caso, $r_1 = (b, r_1)$ e, pelo Lema 2.38, temos que

$$r_1 = mdc(b, r_1) = mdc(b, a - q_1 b) = mdc(b, a) = mdc(a, b),$$

e o algoritmo termina.

2) $r_1 \nmid b$. Nesse caso, podemos efetuar a divisão de b por r_1, obtendo

$$b = r_1 q_2 + r_2, \text{ com } 0 < r_2 < r_1.$$

Novamente temos duas possibilidades:

2.1) $r_2|r_1$. Nesse caso, $r_2 = (r_1, r_2)$ e novamente pelo Lema 2.38,

$$r_2 = mdc(r_1, r_2) = mdc(r_1, b - q_2 r_1) = mdc(r_1, b) = mdc(a - q_1 b, b) = mdc(a, b),$$

e paramos, pois termina o algoritmo.

2.2) $r_2 \nmid r_1$. Nesse caso, podemos efetuar a divisão de r_1 por r_2, obtendo

$$r_1 = r_2 q_3 + r_3, \text{ com } 0 < r_3 < r_2.$$

Continuamos esse procedimento até que pare e isto sempre ocorre, pois, caso contrário, teríamos uma sequência de números naturais $b > r_1 > r_2 > \ldots$ que não possui menor elemento, o que não é possível pelo Princípio da Boa Ordenação. Logo, para algum n, temos que $r_n | r_{n-1}$, o que implica que $mdc(a, b) = r_n$.

Vejamos um exemplo.

Exemplo 2.40. *Calculemos o máximo divisor comum de* 372 *e* 162*:*

De fato: o Algoritmo de Euclides nos fornece que

$$\begin{aligned} 6 &= 18 - 1 \cdot 12 \\ 12 &= 48 - 2 \cdot 18 \\ 18 &= 162 - 3 \cdot 48 \\ 48 &= 372 - 2 \cdot 162. \end{aligned}$$

Donde segue que

$$\begin{aligned} 6 &= 18 - 1 \cdot 12 \\ &= 18 - 1 \cdot (48 - 2 \cdot 18) \\ &= 3 \cdot 18 - 48 \\ &= 3 \cdot (162 - 3 \cdot 48) - 48 \\ &= 3 \cdot 162 - 10 \cdot 48 \\ &= 3 \cdot 162 - 10 \cdot (372 - 2 \cdot 162) \\ &= 23 \cdot 162 - 10 \cdot 372. \end{aligned}$$

Temos, então que

$$mdc(372, 162) = 6 = 23 \cdot 162 + (-10) \cdot 372,$$

finalizando o exemplo. □

Note que conseguimos, através do uso do Algoritmo de Euclides de trás para frente, escrever $6 = mdc(372, 162)$ como múltiplo de 162 mais um múltiplo de 372.

Em geral, seguindo o procedimento detalhado no exemplo, vê-se que o Algoritmo de Euclides também nos fornece um meio de escrever o máximo divisor comum de dois números como soma de múltiplos dos números em questão.

2.7 Números Primos e o Teorema Fundamental da Aritmética

Iniciaremos nesta seção o estudo dos números primos, um dos conceitos mais importantes de toda Matemática. Esses números desempenham papel fundamental e do ponto de vista da estrutura multiplicativa dos inteiros, são os mais simples mas ao mesmo tempo são suficientes para gerar todos os inteiros, como veremos adiante no Teorema Fundamental da Aritmética. A eles estão associados muitos problemas famosos cujas soluções têm resistido aos esforços de várias gerações de matemáticos.

Definição 2.41. *Um número natural $n \in \mathbb{N}$, com $n > 1$, que só possui como divisores positivos 1 e ele próprio é chamado de número primo.*

Dados dois números primos p e q e um número inteiro a qualquer, decorrem da definição acima os seguintes fatos:

I) Se $p|q$, então $p = q$.

De fato: Como $p|q$ e sendo q primo, temos que $p = 1$ ou $p = q$. Como p também é primo, tem-se $p > 1$, o que acarreta $p = q$. □

II) Se $p \nmid a$, então $mdc(p, a) = 1$.

De fato: Se $mdc(p, a) = d$, temos que $d|p$ e $d|a$. Como p é primo temos que $d = 1$ ou $d = p$. Mas $d \neq p$ pois por hipótese, $p \nmid a$ e consequentemente, $d = 1$. □

Um número natural $n > 1$ e que não é primo será dito *composto*. Portanto, se um número natural $n > 1$ é composto, existirá um divisor natural n_1 de n tal que $1 < n_1 < n$. Logo, existirá um número natural n_2 tal que

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

Proposição 2.42 (Lema de Euclides)**.** *Sejam $a, b, p \in \mathbb{Z}$, com $p \in \mathbb{N}$ um número primo. Se $p|ab$, então $p|a$ ou $p|b$.*

Demonstração: Suponhamos que $p \nmid a$, temos que mostrar que $p|b$. Se p é primo e $p \nmid a$ temos que $mdc(p, a) = 1$ e a conclusão segue do Teorema 2.37. ■

Corolário 2.43. *Se $p, p_1, \ldots, p_n$ são números primos e, se $p|p_1 \cdot \ldots \cdot p_n$, então $p = p_i$ para algum $i = 1, \ldots, n$.*

Demonstração: A demonstração será feita usando indução sobre n. Seja $\mathrm{P}(n)$ a sentença

$$\text{"se } p|p_1 \cdot \ldots \cdot p_n \text{ então } p = p_i \text{ para } i = 1, \ldots, n,\ p, p_i \text{ números primos"}.$$

Para $n = 1$ temos que p e p_1 são primos e se $p|p_1$ já provamos que de fato $p = p_1$. Suponhamos que a sentença seja verdadeira para n, e mostremos que a validez de $\mathrm{P}(n)$ implica na validez de $\mathrm{P}(n+1)$, onde $\mathrm{P}(n+1)$ é a sentença

$$\text{"Se } p|p_1 \cdot \ldots \cdot p_n \cdot p_{n+1}, \text{ então } p = p_i \text{ para } i = 1, \ldots, n+1,\ p, p_i \text{ números primos"}.$$

Note que, se $p|p_1 \cdot \ldots \cdot p_n \cdot p_{n+1}$ então podemos escrever $p|(p_1 \cdot \ldots \cdot p_n) \cdot p_{n+1}$ e pela Proposição 2.42 $p|p_1 \cdot \ldots \cdot p_n$ ou $p|p_{n+1}$. Se $p|p_1 \cdot \ldots \cdot p_n$ por hipótese de indução temos que então que $p = p_i$ para $i = 1, \ldots, n$. Se $p|p_{n+1}$ temos que $p = p_{n+1}$. E portanto, pela Primeira Forma do Princípio de Indução Finita temos que $\mathrm{P}(n)$ é verdadeira. ■

Teorema 2.44 (Teorema Fundamental da Aritmética)**.** *Todo número natural, $n \in \mathbb{N}$, maior do que 1 ou é primo ou se escreve de modo único (a menos da ordem dos fatores) como um produto de números primos.*

Demonstração: Demonstraremos usando a segunda forma do Princípio de Indução, (A_2).

Se $n = 2$, o resultado é verificado pois 2 é primo.

Suponhamos que o resultado é válido para todo número natural menor do que n e vamos provar que vale para n. Se o número n é primo, nada temos a demonstrar. Suponhamos então, que n seja composto. Logo, existem números naturais n_1 e n_2 tais que $n = n_1 n_2$, com $1 < n_1 < n$ e $1 < n_2 < n$. Pela hipótese de indução, temos que existem números primos $p_1, \ldots, p_r$ e $q_1, \ldots, q_s$ tais que $n_1 = p_1 \cdots p_r$ e $n_2 = q_1 \cdots q_s$. Portanto, $n = p_1 \cdots p_r q_1 \cdots q_s$.

Agora provaremos a unicidade da escrita, também utilizando a Segunda Forma do Princípio de Indução. Suponha que tenhamos $n = p_1 \cdots p_k = q_1, \ldots, q_l$, onde os p_i e os q_j são números primos. Como por definição de divisibilidade $p_1 | n = q_1 \cdots q_l$ pelo Corolário 2.43 acima, temos que $p_1 = q_j$ para algum j, que, após o reordenamento de $q_1, \ldots, q_l$, podemos supor que seja q_1. Portanto, $p_1 \cdots p_k = q_1 \cdots q_l$ e pela Proposição 2.13 podemos cancelar p_1 e assim

$$p_2, \ldots, p_k = q_2, \ldots, q_l.$$

Como $p_2 \cdots p_k < n$, e este número $p_2 \cdots p_k$ se escreve de modo único como um produto de primos a menos da ordem dos fatores, a hipótese de indução acarreta que $k = l$ e os p_i e q_j são iguais aos pares. ■

Teorema 2.45. *Existem infinitos números primos.*

Demonstração: Vamos supor que exista apenas um número finito de números primos $p_1, \ldots, p_r$. Consideremos o número natural

$$n = p_1 \cdot p_2 \cdot \ldots \cdot p_r + 1.$$

De fato, n não é primo pois $n \neq p_i$ e assim, pelo Teorema 2.44, n se escreve de modo único como produto de números primos. Assim, n possui um fator primo p (logo, este primo divide n) que, portanto, deve ser um dos $p_1, \ldots, p_r$ e, consequentemente, divide o produto $p_1 \cdot p_2 \cdot \ldots \cdot p_r$. Logo, pelo Teorema 2.25 temos que se $p | n = p_1 \cdot p_2 \cdot \ldots \cdot p_r + 1$ e $p | p_1 \cdot p_2 \cdot \ldots \cdot p_r$ então $p | 1$, o que é um absurdo. Portanto, existem infinitos números primos. ■

Lema 2.46. *Se $n \in \mathbb{N}$ não é primo, então possui, necessariamente, um fator primo menor ou igual a $\sqrt{n}$.*

Demonstração: Se n não é primo, então n é composto e assim, $n = n_1 n_2$ onde $1 < n_1 < n$, $1 < n_2 < n$. Sem perda de generalidade vamos supor $n_1 \leq n_2$. Logo $n_1 \leq \sqrt{n}$ pois, se $n_1 > \sqrt{n}$ temos $n > n_2 \geq n_1 > \sqrt{n}$ e por transitividade $n_2 > \sqrt{n}$. Então temos $n_1 n_2 > \sqrt{n}\sqrt{n} = n$ o que é um absurdo. Portanto, $n_1 \leq \sqrt{n}$. Como pelo Teorema 2.44, n_1 possui algum fator primo p, então $p \leq \sqrt{n}$ e como p sendo um fator primo de n_1 é também um fator primo de n, concluindo a demonstração. ■

Este resultado tem uma importante aplicação prática. Ele nos diz que, para testarmos se um número é primo, é suficiente testarmos divisibilidade apenas pelos primos menores ou iguais a $\sqrt{n}$. Portanto, se desejarmos obter a lista de todos os primos menores que 60, por exemplo, devemos excluir dentre os números de 2 a 60 aqueles que são múltiplos de $2, 3, 5$ e 7 pois estes são os primos menores ou iguais a $\sqrt{60}$.

	2	3	~~4~~	5	~~6~~	7	~~8~~	~~9~~	~~10~~
11	~~12~~	13	~~14~~	~~15~~	~~16~~	17	~~18~~	19	~~20~~
~~21~~	~~22~~	23	~~24~~	~~25~~	~~26~~	~~27~~	~~28~~	29	~~30~~
31	~~32~~	~~33~~	~~34~~	~~35~~	~~36~~	37	~~38~~	~~39~~	~~40~~
41	~~42~~	43	~~44~~	~~45~~	~~46~~	47	~~48~~	~~49~~	~~50~~
~~51~~	~~52~~	53	~~54~~	~~55~~	~~56~~	~~57~~	~~58~~	59	~~60~~.

Logo, os primos entre 2 e 60 são todos aqueles que não foram eliminados pelo processo descrito, isto é,

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59.$$

Este processo é chamado de crivo de Eratóstenes.

Capítulo 3

Números Irracionais

Em geral, não é uma tarefa simples determinar se certos números são ou não irracionais, apesar de ser fácil dar exemplos de números irracionais. Basta exibir um número, cuja forma decimal seja infinita e não periódica (ver [12], p. 13). Por exemplo, os números $1,234567891011\ldots$ e $2,01001000100001000001\ldots$ são irracionais. Esses números não foram construídos aleatoriamente, eles possuem uma lei de formação em sua construção não permitindo qualquer periodicidade em sua parte decimal. Já o número $e = 2,7182818284\ldots$ é um irracional que não possui uma lei de formação. Ele é um dos números irracionais mais populares e já era conhecido desde o século XVII a.C. Neste capítulo apresentaremos alguns importantes resultados acerca desses números bem como a demonstração da irracionalidade de e, dos irracionais da forma $\sqrt{n}$ com n $\in \mathbb{N}$. Começaremos fazendo uma breve apresentação dos números racionais, que é o complementar do nosso conjunto em questão.

3.1 Os Números Racionais

Consideremos agora o conjunto dos números racionais

$$\mathbb{Q} := \{\frac{a}{b};\ a, b \in \mathbb{Z} \ \text{ e } \ b \neq 0\}.$$

Fazendo as identificações:

$$a = \frac{a}{+1},$$

para todo $a \in \mathbb{Z}$, temos que

$$\mathbb{Z} \subset \mathbb{Q}.$$

Lembremos que (por identificação)

$$\mathbb{N} \subset \mathbb{Z}.$$

Assim, por identificação,

$$\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q}.$$

Definição 3.1. *Se* $\frac{a}{b}, \frac{c}{d} \in \mathbb{Q}$ *são dois números racionais, diremos que* $\frac{a}{b} = \frac{c}{d}$ *se, e somente se,*

$$ad = bc.$$

Dessa forma temos que

- $\frac{2}{3} = \frac{4}{6}$, pois $2.6 = 12 = 3.4$.
- $\frac{-2}{3} = \frac{4}{-6}$, pois $-2.-6 = 12 = 3.4$.
- $\frac{2}{-3} = \frac{4}{-6}$, pois $2.-6 = 12 = -3.4$.

Definição 3.2. *Se* $\frac{a}{b}, \frac{c}{d} \in \mathbb{Q}$ *são dois números racionais, então*

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}$$

e

$$\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}.$$

Temos que

- $\frac{2}{3} + \frac{-3}{5} = \frac{5.2 + (-3).3}{3.5} = \frac{10 + (-9)}{15} = \frac{1}{15}$.
- $\frac{-2}{-3} + \frac{7}{-5} = \frac{(-5).(-2) + 7.(-3)}{(-3).(-5)} = \frac{10 + (-21)}{15} = \frac{-11}{15} = -\frac{11}{15}$.
- $\frac{2}{3} \cdot \frac{-3}{5} = \frac{2.(-3)}{3.5} = \frac{-6}{15} = -\frac{6}{15} = -\frac{2}{5}$.

- $\frac{-2}{-3} \cdot \frac{7}{-5} = \frac{(-2).7}{(-3).(-5)} = \frac{-14}{15} = -\frac{14}{15}$.

Como descobrir quando um número racional é menor do que outro? Por exemplo, qual é o menor entre $\frac{3}{5}$ e $\frac{4}{6}$? Uma maneira é a seguinte: como

$$\frac{18}{30} = \frac{3}{5} \text{ e } \frac{20}{30} = \frac{4}{6}$$

e

$$\frac{18}{30} < \frac{20}{30},$$

então

$$\frac{3}{5} < \frac{4}{6}.$$

Definição 3.3. *Se* $\frac{a}{b}, \frac{c}{d} \in \mathbb{Q}$ *são dois números racionais com* $d, b \in \mathbb{N}$*, então*

$$\frac{a}{b} < \frac{c}{d} \iff ad < bc$$

e

$$\frac{a}{b} \leq \frac{c}{d} \iff ad \leq bc.$$

Assim,

- $\frac{-5}{4} < \frac{-4}{5}$, pois $-5.5 = -25 < -16 = -4.4$.
- $\frac{3}{-2} = \frac{-3}{2} < \frac{-2}{3}$, pois $-3.3 = -9 < -4 = 2.(-2)$.

Com essa relação de ordem, podemos associar a cada número racional um ponto da reta numérica, isto é podemos então representar graficamente o conjunto do números racionais como na figura abaixo.

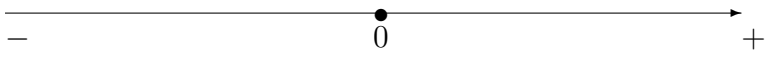

Figura 3.1: A Reta Numérica

Entretanto, existem pontos da reta numérica que não estão associados a nenhum número racional.

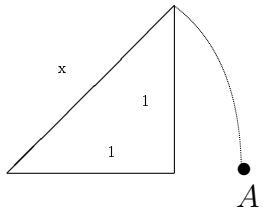

Figura 3.2: Ponto da reta que não está associado a nenhum número racional

Vamos mostrar que não existe nenhum número racional $x \in \mathbb{Q}$ associado ao ponto A. Esta demonstração será feita com todos os detalhes no decorrer deste capítulo.

De fato: Suponhamos, por absurdo, que exista um número racional $\frac{p}{q}$, que não possua fatores em comum, isto é, que p e q não possuam divisores em comum, tal que

$$\sqrt{2} = \frac{p}{q}.$$

Então,

$$\left(\frac{p}{q}\right)^2 = \sqrt{2}^2,$$

ou seja,

$$\frac{p^2}{q^2} = 2 \;\Rightarrow\; p^2 = 2q^2,$$

mostrando que p^2 é um número par (número divisível por 2). Concluímos daí que p também é um número par, pois se p fosse um número ímpar, então p^2 também seria um número ímpar. Assim,

$$p = 2r,\ r \in \mathbb{Z}.$$

Logo,

$$2q^2 = p^2 = (2r)^2 = 2^2r^2,$$

ou seja,

$$q^2 = 2r^2,$$

mostrando que q^2 também é um número par e, portanto q também é um número par, isto é,

$$q = 2s, \quad s \in \mathbb{Z}.$$

Portanto,

$$2|q \quad \text{e} \quad 2|p,$$

o que contraria nossa afirmação de que p e q não possuem divisores em comum. □

Dessa forma, vemos que existem pontos da reta que não estão associados a nenhum número racional, ou ainda, existem "números" que não podem ser escritos na forma de uma fração, os quais são chamados de **números irracionais**. A seguir estudaremos classificações dentro do conjunto dos números reais.

3.2 Inteiros Algébricos

Começaremos esta seção estudando os números reais que são raízes de um tipo específico de polinômio mônico e veremos que esse número real só poderá ser um número inteiro ou irracional. Ao generalizar este polinômio concluiremos que os números reais podem ser classificados de duas formas. Utilizamos como base as definições e resultados contidos em [6] e [12].

Definição 3.4. *Qualquer solução de uma equação polinomial da forma*

$$x^n + a_{n-1}x^{n-1} + \ldots + a_1x + a_0 = 0, \tag{3.1}$$

onde os coeficientes $a_0, \ldots, a_{n-1}$ são números inteiros, é chamada um inteiro algébrico.

Assim, qualquer número inteiro $b \in \mathbb{Z}$ é inteiro algébrico pois a equação

$$x - b = 0$$

tem b como solução. $\sqrt{2+\sqrt{3}}$ também é um inteiro algébrico, pois é solução da equação

$$x^4 - 4x^2 + 1 = 0.$$

Outros exemplos de inteiros algébricos são $\sqrt{2}$ e $-\sqrt{2}$, pois são soluções da equação

$$x^2 - 2 = 0.$$

Além do mais, todo número da forma $\pm\sqrt{n}$, com $n \in \mathbb{N}$, é um inteiro algébrico pois, de fato,

$$x = \pm\sqrt{n} \Rightarrow x^2 = (\pm\sqrt{n})^2 \Rightarrow x^2 = n \Rightarrow x^2 - n = 0$$

que é uma equação do tipo (3.1) onde $n = 1$ e $a_0 = n$.

Existem inteiros algébricos que não são números reais, ou seja, são números complexos, por exemplo, $i = \sqrt{-1}$ e $-i$ são inteiros algébricos, pois são raízes da equação

$$x^2 + 1 = 0.$$

De fato, para cada $a \in \mathbb{Z}^*$, o número complexo $\pm i\sqrt{a}$ é um inteiro algébrico uma vez que é solução da equação $x^2 + a = 0$.

Observação 3.5. *Dos exemplos acima, podemos observar que todos os números inteiros são Inteiros Algébricos. Também, existem Inteiros Algébricos Irracionais e Complexos. O teorema a seguir caracteriza os Inteiros Algébricos Reais.*

Teorema 3.6. *Um inteiro algébrico (real) é inteiro ou irracional.*

Demonstração: Seja $\alpha \in \mathbb{R}$ um inteiro algébrico. Suponhamos por contradição que α seja um racional irredutível $\alpha = \frac{p}{q}$ (p e q primos entre si). Como α é um inteiro algébrico, então $\alpha = \frac{p}{q}$ é solução de uma equação do tipo

$$x^n + a_{n-1}x^{n-1} + \ldots + a_1x + a_0 = 0.$$

Substituindo x por $\alpha = \frac{p}{q}$ na equação, temos que:

$$\left(\frac{p}{q}\right)^n + a_{n-1}\left(\frac{p}{q}\right)^{n-1} + \ldots + a_1\left(\frac{p}{q}\right) + a_0 = 0 \Rightarrow \frac{p^n}{q^n} + a_{n-1}\frac{p^{n-1}}{q^{n-1}} + \ldots + a_1\frac{p}{q} + a_0 = 0$$
$$\Rightarrow \frac{p^n}{q^n} = -a_{n-1}\frac{p^{n-1}}{q^{n-1}} - \ldots - a_1\frac{p}{q} - a_0$$
$$\Rightarrow p^n = q^n\left(-a_{n-1}\frac{p^{n-1}}{q^{n-1}} - \ldots - a_1\frac{p}{q} - a_0\right)$$
$$\Rightarrow p^n = -a_{n-1}p^{n-1}q - \ldots - a_1pq^{n-1} - a_0q^n)$$
$$\Rightarrow p^n = q(-a_{n-1}p^{n-1} - \ldots - a_1pq^{n-2} - a_0q^{n-1}).$$

Assim, vemos que p^n é múltiplo de q e portanto, q divide p^n. Como $mdc(p,q) = 1$, temos que $mdc(q^1, p^n) = 1$, pois caso contrário, existiria um primo r que dividiria ambos e assim,

$$r|p^n \Rightarrow r|\underbrace{p.p.p\ldots p}_{\text{n } vezes} \Rightarrow r|p \Rightarrow r|p \text{ e } q.$$

Mas isso é um absurdo, pois $mdc(p,q) = 1$. Agora, como temos que q divide p^n e $mdc(q,p^n) = 1$ então $q = 1$ e assim $\alpha = \frac{p}{q} = \frac{p}{1} = p$, que é um número inteiro. ■

Uma alternativa de classificarmos os números reais é em algébricos e transcendentes, onde dizemos que um número real x é algébrico quando satisfaz uma equação polinomial com coeficientes inteiros, ou seja, existem $a_0, \ldots, a_n \in \mathbb{Z}$ para os quais

$$a_nx^n + a_{n-1}x^{n-1} + \cdots + a_2x^2 + a_1x + a_0 = 0.$$

Note que esta definição é uma generalização da definição de inteiro algébrico onde o polinômio em questão era mônico.

Não é difícil percebermos que todo número racional é algébrico, pois se $x = \frac{p}{q} \in \mathbb{Q}$, então $qx - p = 0$, ou seja, $\frac{p}{q}$ é raiz do polinômio com coeficientes inteiros $P(x) = qx - p$. Assim, se um número não satisfizer a equação acima, necessariamente deve ser irracional. A recíproca dessa afirmação não é verdadeira pois, por exemplo, a raiz n-ésima de todo número primo é irracional sendo que tal número, no entanto, é algébrico.

Quando um número não satisfaz uma equação polinomial com coeficientes inteiros dizemos

que ele é um número transcendental indicando com isso apenas que esses números transcendem, ou seja, vão além no conjunto dos números algébricos.

A seguir, demonstraremos a irracionalidade de uma das mais importantes constantes matemáticas, além de um pequeno apanhado histórico sobre ela.

3.3 A Irracionalidade do Número e

Acredita-se que a noção de logaritmo já era conhecida pelos mesopotâmicos. No museu do Louvre, encontra-se um tablete de argila da mesopotâmia datado de 1700 a.C. contendo o seguinte problema, descrito em linguagem atual: quanto tempo levará para uma soma de dinheiro dobrar se for investida a uma taxa de 20 por cento de juros compostos anualmente? Esse problema pode ser traduzida na seguinte equação:

$$(1,2)^x = 2.$$

O valor encontrado para este problema foi $3,7870$, que para época era uma boa aproximação do valor correto, que é aproximadamente $3,8018$. Entre os tabletes de argilas que sobreviveram, um deles lista o resultado da potência de alguns números, o que indica que os mesopotâmicos tinham o auxílio de tábuas para resolução de determinados problemas.

Os logaritmos ressurgiram na Europa no século XVII da necessidade de simplificação de alguns cálculos matemáticos, como multiplicação e divisão. Até poucos anos antes do ressurgimento dos logaritmos, a simplificação das operações eram realizadas através de relações trigonométricas que poderiam ser usadas para transformar multiplicação e divisão em soma e subtração. Essas relações trigonométricas ficaram conhecidas como regras prostafaréticas, que vem do grego *prosthaphaeresis* que significa "adição e subtração"[1].

Um dos precursores no estudo dos logaritmos foi John Napier $(1550 - 1617)$ no qual tratou desse assunto pensando em potências sucessivas de um dado número. Ele publicou seu trabalho em 1614, levando vinte anos de sua vida para completá-lo, com o título *Mirifici logarithmornm canonis descriptio* (Uma descrição da maravilhosa regra dos logaritmos). Com o passar dos anos, a ideia de logaritmos foi sofrendo alguns ajustes até se tornar o que conhecemos hoje.

[1] Cf. ALFRADIQUE, 2017, p. 18-19.

Com o estudo mais profundo dos logaritmos, o número $2,71828\ldots$ aparece de forma natural em diversos trabalhos da época. No século XVIII, Leonhard Euler simboliza essa constante pela letra e, que se mantém até os dias atuais. Também é devido a Euler a primeira demonstração da irracionalidade de e, em 1737, utilizando frações contínuas.

Para demonstrarmos a irracionalidade do número e é necessário mostrarmos primeiro os dois resultados seguintes.

Teorema 3.7 (Limite Fundamental)**.** *Considere a função* $f :]0, \infty[\to \mathbb{R}$ *definida por* $f(n) = \left(1 + \frac{1}{n}\right)^n$. *Então* $\lim_{n\to\infty} \left(1 + \frac{1}{n}\right)^n = e$.

Demonstração: Usando a definição de derivada temos que

$$\frac{d}{dx}\ln(x) = \lim_{h\to 0} \frac{\ln(x+h) - \ln(x)}{h} = \lim_{h\to 0} \frac{1}{h}\ln(\frac{x+h}{x}) = \lim_{h\to 0} \ln((1+\frac{h}{x})^{\frac{1}{h}}).$$

Por outro lado, sabemos que

$$\frac{d}{dx}\ln(x) = \frac{1}{x}.$$

Logo,

$$\lim_{h\to 0} \ln((1+\frac{h}{x})^{\frac{1}{h}} = \frac{1}{x}.$$

Fazendo $x = 1$, obtemos que

$$\lim_{h\to 0} \ln(1+h)^{\frac{1}{h}} = 1.$$

A continuidade da função logarítmica natural implica que

$$\ln(\lim_{h\to 0}(1+h)^{\frac{1}{h}}) = 1 = \ln(e),$$

e a injetividade implica que

$$\lim_{h\to 0}(1+h)^{\frac{1}{h}} = e.$$

Fazendo a mudança de variável $h = \frac{1}{n}$ temos que se $h \to 0$, como $n = \frac{1}{h}$, então $n \to \infty$ e assim $\lim_{h\to 0}(1+h)^{\frac{1}{h}} = \lim_{n\to\infty} \left(1 + \frac{1}{n}\right)^n = e$, provando o teorema. ■

Lema 3.8. *e é o limite da sequência* $(S_n)_{n\in\mathbb{N}}$ *cujo termo geral é dado por* $S_n = 1 + \frac{1}{1!} + \frac{1}{2!} + \ldots + \frac{1}{n!}$

isto é, $e = \sum_{n=0}^{\infty} \frac{1}{n!}$.

Demonstração: Utilizando a expressão de expansão do Binômio de Newton, temos

$$\begin{aligned}\left(1+\frac{1}{n}\right)^n &= \sum_{k=0}^{n} \binom{n}{k} 1^{n-k} \cdot \left(\frac{1}{n}\right)^k \\ &= 1 + n \cdot \frac{1}{n} + \frac{n(n-1)}{2!} \cdot \frac{1}{n^2} + \ldots + \frac{n(n-1)\ldots(n-k+1)}{k!} \cdot \frac{1}{n^k} + \ldots + \frac{1}{n^n} \\ &= 1 + 1 + \frac{1}{2!} \cdot \left(1-\frac{1}{n}\right) + \ldots + \frac{1}{k!}\left(1-\frac{1}{n}\right) \cdot \left(1-\frac{2}{n}\right) \ldots \left(1-\frac{k-1}{n}\right) \\ &\quad + \frac{1}{n!} \cdot \left(1-\frac{1}{n}\right) \cdot \left(1-\frac{2}{n}\right) \ldots \left(1-\frac{n-1}{n}\right).\end{aligned}$$

Como cada fator entre parênteses no membro direito da igualdade é não negativo e menor do que 1, pode-se concluir que

$$\left(1+\frac{1}{n}\right)^n \leq 1 + 1 + \frac{1}{2!} + \ldots + \frac{1}{n!} = S_n, \text{ para todo } n \in \mathbb{N}.$$

Além disso, fixando $k \geq 1$ arbitrário, temos que, se $n > k$ então,

$$\left(1+\frac{1}{n}\right)^n > 1 + 1 + \frac{1}{2!} \cdot \left(1-\frac{1}{n}\right) + \ldots + \frac{1}{k!} \cdot \left(1-\frac{1}{n}\right) \cdot \left(1-\frac{2}{n}\right) \ldots \left(1-\frac{k-1}{n}\right).$$

Assim, fazendo $n \to \infty$, temos

$$e \geq 1 + 1 + \frac{1}{2!} + \ldots + \frac{1}{k!} = S_k, \quad \text{para todo } k \in \mathbb{N}.$$

Portanto,

$$\left(1+\frac{1}{n}\right)^n \leq S_n \leq e; \quad \text{para todo } n \in \mathbb{N}.$$

Logo,

$$e = \lim_{n\to\infty} \left(1+\frac{1}{n}\right)^n \leq \lim_{n\to\infty} S_n \leq \lim_{n\to\infty} e = e.$$

■

Teorema 3.9. *O número e é irracional.*

Demonstração: Suponhamos que e fosse um número racional, isto é, $e = \frac{p}{q}$ onde $p, q \in \mathbb{N}$, são primos entre si. Temos que

$$e = 1 + \frac{1}{1!} + \frac{1}{2!} + \ldots \Rightarrow \frac{p}{q} = 1 + \frac{1}{1!} + \frac{1}{2!} + \ldots + \frac{1}{q!} + \frac{1}{(q+1)!} + \ldots$$
$$\Rightarrow \frac{p}{q} - \left(1 + \frac{1}{1!} + \frac{1}{2!} + \ldots + \frac{1}{q!}\right) = \frac{1}{(q+1)!} + \frac{1}{(q+2)!} + \ldots.$$

Então,

$$\frac{p}{q} - \left(1 + \frac{1}{1!} + \frac{1}{2!} + \ldots + \frac{1}{q!}\right) = \sum_{j=q+1}^{\infty} \frac{1}{j!} \tag{3.2}$$

Agora, note que

$$\begin{aligned} \sum_{j=q+1}^{\infty} \frac{1}{j!} &= \frac{1}{q!}\left(\frac{1}{q+1} + \frac{1}{(q+1)(q+2)} + \ldots\right) \\ &< \frac{1}{q!}\left(\frac{1}{q+1} + \frac{1}{(q+1)^2} + \ldots\right) \end{aligned}$$

e como

$$\sum_{n=1}^{\infty} \frac{1}{(q+1)^n} = \frac{\frac{1}{q+1}}{1 - \frac{1}{q+1}} = \frac{1}{q},$$

obtemos que

$$\sum_{j=q+1}^{\infty} \frac{1}{j!} < \frac{1}{q!} \cdot \frac{1}{q}.$$

Voltando em (3.2), temos

$$0 < \frac{p}{q} - \left(1 + \frac{1}{1!} + \frac{1}{2!} + \ldots + \frac{1}{q!}\right) < \frac{1}{q!} \cdot \frac{1}{q}.$$

Então,

$$0 < q!. \left(\frac{p}{q} - 1 - \frac{1}{1!} - \frac{1}{2!} - \ldots - \frac{1}{q!}\right) < \frac{1}{q}.$$

Observamos que o termo do meio é um inteiro pois $q!$ cancela todos os denominadores das frações aí presentes. Mas isso é impossível pois sendo $q \in \mathbb{N}$, $\frac{1}{q} \leq 1$, esta última expressão nos diria que o termo do meio é um inteiro positivo estritamente menor que 1. O que é um absurdo. Portanto, e não é um número racional. Logo, e é irracional. ■

Observação 3.10. *Da conclusão da seção anterior, sabemos que para provar a irracionalidade de e bastaria provar sua transcendência, o que não seria viável em nosso trabalho por abordar cálculos mais complexos em sua demonstração. No entanto, esta pode ser consultada em [14].*

3.4 A Irracionalidade da Raiz Quadrada de um Número Primo $p \in \mathbb{N}$

"Provavelmente foram os matemáticos da Escola Pitagórica que descobriram que $\sqrt{2}$ não é um número racional"[2]. Há indícios de que esse foi o primeiro número irracional descoberto. Alguns comentadores se apoiam na ideia de que um pitagórico descobriu a irracionalidade de $\sqrt{2}$, tal descoberta o teria levado a morte, pois outros pitagóricos não gostariam desse fato divulgado, afinal, a demonstração dessa irracionalidade ia diretamente contra a crença pitagórica. Outras versões também existem, como uma em que Hipaso de Metaponto teria descoberto essa irracionalidade de $\sqrt{2}$ e ao invés de morto, teria sido somente expulso. De toda a forma, independente das teorias, sabemos que na Grécia essa descoberta gerou uma crise da Matemática e que a corrente pitagórica sempre acreditou que todos os números eram racionais.

> Na Grécia daquele tempo, os números eram considerados comprimentos de segmentos de reta, e acreditava-se que dois segmentos quaisquer eram sempre **comensuráveis**, isto é, existia sempre um terceiro segmento, do qual esses dois eram múltiplos inteiros. Esse conceito está relacionado com o de número racional, pois todo segmento de medida racional é comensurável com um segmento de medida unitária, e reciprocamente. Mas a Matemática parece ter pregado uma peça no seio da Escola Pitagórica: o número $\sqrt{2}$ aparece naturalmente ao usar o Teorema de Pitágoras, por ser a diagonal de um simples quadrado de lado medindo 1, mas $\sqrt{2}$ não é um número racional, ou com a linguagem dos antigos matemáticos gregos, a diagonal e o lado do quadrado não são segmentos comensuráveis.[3]

Enfim, qualquer que tenha sido o fato real, os pitagóricos não conseguiram manter essa amarga descoberta em segredo.

A demonstração desse fato é muito simples, contudo, antes de demonstrá-la é necessário provarmos a próxima proposição.

---

[2]FIGUEIREDO, Djairo G. De. *Números Irracionais e Transcendentes.* Rio de Janeiro, 1985, p. 2.
[3]FILHO, Daniel Cordeiro de Morais. *Um Convite à Matemática.* Rio de Janeiro, 2013, p. 250.

Proposição 3.11. *O número $a \in \mathbb{N}$ é par se, e somente se, a^n é par qualquer que seja $n \in \mathbb{N}$.*

Demonstração: Suponhamos que o número $a \in \mathbb{N}$ seja par. Então, $a = 2k$ para algum $k \in \mathbb{N}$. Assim,

$$a^n = \underbrace{a \cdot a \cdots a}_{\text{n vezes}} = \underbrace{2k \cdot 2k \cdots 2k}_{\text{n vezes}} = (2k)^n = 2^n k^n = 2(2^{n-1}k^n)$$

que é par.

Reciprocamente, queremos mostrar que se a^n é par então a é par com $a, n \in \mathbb{N}$. Suponhamos por absurdo que a^n seja par e que a não seja par, isto é, a seja ímpar. Se a é ímpar, então $a = p_1 \cdot p_2 \cdots p_k$ com p_i primos $\neq 2$. Daí, $a^n = (p_1 \cdot p_2 \cdots p_k)^n = p_1^n \cdot p_2^n \cdots p_k^n$ que pelo Teorema Fundamental da Aritmética é uma decomposição única de primos onde o fator 2 não aparece, logo não pode ser par. ■

Suponhamos, por contradição que $\sqrt{2}$ não é um número irracional. Então exitem inteiros positivos p e q, primos entre si, tais que $\sqrt{2} = \dfrac{p}{q}$. Daí obtemos

$$p^2 = 2q^2.$$

Isso quer dizer que p^2 é um número par. Logo, pelo resultado acima p deve ser também par. Logo, p é da forma $p = 2r$, de onde se segue

$$p^2 = 4r^2.$$

Dessas duas equações, obtemos $2q^2 = 4r^2$, isto é, $q^2 = 2r^2$. Logo, q^2 é par, e do mesmo modo obtemos que q também deve ser par, Mas, se p e q são pares, ambos são divisíveis por 2 e assim não podem ser primos entre si. Tal contradição provém da hipótese, feita inicialmente, de que $\sqrt{2}$ fosse racional.

Sabemos que 2 é um número primo e acabamos de provar que $\sqrt{2}$ é um número irracional. Isto decorre do primeiro item do seguinte resultado:

Proposição 3.12.

(i) Se p é um natural primo, $\sqrt{p}$ é um número irracional.

(ii) Se p e q são primos distintos, $\sqrt{pq}$ e $\sqrt{p} + \sqrt{q}$ também são irracionais.

Demonstração: Para mostrarmos o item (i) suponhamos, por absurdo, que $\sqrt{p}$ não é irracional, ou seja, $\sqrt{p}$ é racional, então podemos escrever $\sqrt{p} = \dfrac{r}{s}$ com $mdc(r, s) = 1$. Logo, $s^2 p = r^2$ e, portanto,

sendo p primo, ele seria fator de r^2 e também de r, isto é, $r = \lambda p$ para algum $\lambda \in \mathbb{N}$. Assim, $s^2 p = \lambda^2 p^2$ e então, p seria fator de s^2, logo também de s, o que é um absurdo pois $mdc(r, s) = 1$. Logo, $\sqrt{p}$ é irracional.

Do mesmo modo, para o item (ii) suponhamos que $\sqrt{pq}$ seja racional. Então existem $a, b \in \mathbb{Z}\backslash\{0\}$, primos entre si, tais que $\sqrt{pq} = \frac{a}{b}$, então $a^2 = b^2 pq$ e assim $p|a^2 = a \cdot a$ onde pela Proposição 2.42 $p|a$, logo existe $k \in \mathbb{Z}$ tal que $a = pk$. Elevando ao quadrado ambos os lados dessa igualdade concluímos que $p^2|a^2$. Do mesmo modo temos que $p|b \Rightarrow p^2|b^2$. Como $p^2|a$ e $q^2|a$, existe $r \in \mathbb{Z}\backslash\{0\}$ tal que $a^2 = p^2 q^2 r$. Substituindo nessa última igualdade a^2 por $b^2 pq$ obtemos $b^2 pq = p^2 q^2 r$. Cancelando p e q em ambos os lados da igualdade, obtemos $b^2 = pqr$ donde concluímos que $p|b^2$ e $q|b^2$, logo $p|b$ e $q|b$, mas isto é um absurdo uma vez que a e b são primos entre si.

Analogamente, suponhamos que $\sqrt{p} + \sqrt{q}$ seja racional. Então existem $a, b \in \mathbb{Z}\backslash\{0\}$, primos entre si, tais que $\sqrt{p} + \sqrt{q} = \frac{a}{b}$. Assim temos

$$(\sqrt{p} + \sqrt{q})^2 = \frac{a^2}{b^2} \Rightarrow p + 2\sqrt{pq} + q = \frac{a^2}{b^2} \Rightarrow \sqrt{pq} = \frac{1}{2} \cdot \left(\frac{a^2}{b^2} - p - q \right) \in \mathbb{Q}.$$

Mas isso é um absurdo pois já provamos que $\sqrt{pq}$ é irracional. ■

3.5 A Irracionalidade da Raiz Quadrada de um Número Natural $n \in \mathbb{N}$

Sabemos que $\sqrt{p}$ é um número irracional para p primo, como por exemplo, $\sqrt{2}, \sqrt{3}, \sqrt{5}$ e assim por diante. Além do mais, $\sqrt{n}$ também é irracional para outros valores $n \in \mathbb{N}$, como $\sqrt{6}, \sqrt{8}$ e $\sqrt{10}$. Observamos assim, que todos os valores $\sqrt{n}$ onde $n \notin \{1^2, 2^2, 3^2\} = \{m^2\}_{m \in \mathbb{N}}$, são irracionais. Ou seja, se n não é um quadrado perfeito então sua raiz quadrada é um número irracional. Usando a contra-positiva, isto é o mesmo que dizer que, se raiz quadrada de n não é um irracional então n é um quadrado perfeito. E assim, temos o seguinte resultado.

Teorema 3.13. *Seja $n \in \mathbb{N}$. Se $\sqrt{n} \in \mathbb{Q}$, então $\sqrt{n} \in \mathbb{Z}$.*

Demonstração: Se $\sqrt{n} \in \mathbb{Q}$, então $\sqrt{n} = \frac{a}{b}$, com $a, b \in \mathbb{Z}$ e primos entre si. Suponhamos que $\left(\frac{a}{b}\right)^2 = n \Rightarrow nb^2 = a^2$. Como os mesmos fatores primos aparecem na decomposição em ambos os lados de $nb^2 = a^2$ e a e b são primos entre si, concluímos que $b = 1$. Logo, $\sqrt{n} = \frac{a}{1} = a \in \mathbb{Z}$. ■

Graças a este teorema, qualquer raiz quadrada de um número natural que não for inteira é irracional. Assim, com o auxílio de uma calculadora, quando a raiz quadrada de um número natural não der exata, ou seja, não resultar em um número inteiro, concluímos que esta raiz quadrada é irracional.

Por exemplo, $\sqrt{2}, \sqrt{5}$ e $\sqrt{83}$ são irracionais pois possuem casas decimais.

Desta forma, com um estudo pouco aprofundado de lógica, ao abordarmos o conteúdo de números irracionais nos anos finais do Ensino Fundamental, podemos fazer a seguinte pergunta aos alunos: como verificar se a raiz quadrada de um número natural é ou não um número irracional? E então apresentarmos a eles este resultado explicando que com a contra-positiva fica simples a verificação por meio da calculadora ou então por meio da decomposição do número natural em potências pares de números primos.

Capítulo 4

A Irracionalidade de $\sqrt{p}$ para $p = 2,\ 3$ e 5, do Ponto de Vista Geométrico

Existem outras formas de se demonstrar a irracionalidade de raiz quadrada de 2. Uma delas, fazendo-se o uso da geometria, foi apresentada pelo matemático Stanley Tennenbaum (1927-2005) e popularizada pelo matemático britânico John H. Conway (1938-2020). A prova geométrica que ele apresentou nasceu da prova por contradição que já era bem conhecida, a qual apresentaremos abaixo. Esta e outras demostrações feitas neste capítulo podem ser consultadas com mais detalhes em [8].

4.1 Demonstrações Geométricas da Irracionalidade de $\sqrt{2}$

Nesta seção apresentaremos duas maneiras, usando argumentos geométricos, de demonstrar a irracionalidade de $\sqrt{2}$.

Teorema 4.1. *$\sqrt{2}$ é um número irracional.*

Demonstração: Suponhamos, por absurdo, que $\sqrt{2}$ não seja irracional, isto é, que seja racional. Então, exitem $a, b > 0$, inteiros e primos entre si, tais que $\frac{a}{b} = \sqrt{2}$. Assim, temos $\left(\frac{a}{b}\right)^2 = 2 \Rightarrow \frac{a^2}{b^2} = \sqrt{2} \Rightarrow a^2 = 2b^2$, o que pode ser interpretado geometricamente como uma igualdade entre as áreas de um quadrado de lado a e dois quadrados de lado b, respectivamente, conforme a Figura 4.1.

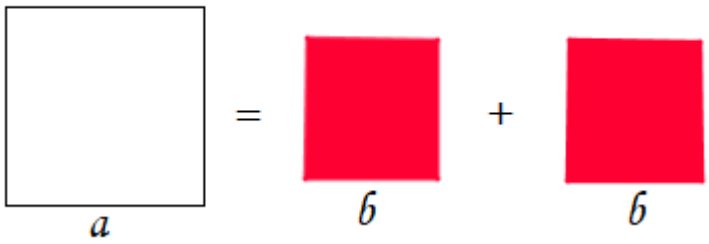

Figura 4.1: Prova geométrica da irracionalidade de $\sqrt{2}$ usando quadrados.

Movendo os quadrados de lado b a fim de cobrir a área do quadrado maior, de lado a, conforme a Figura 4.2.

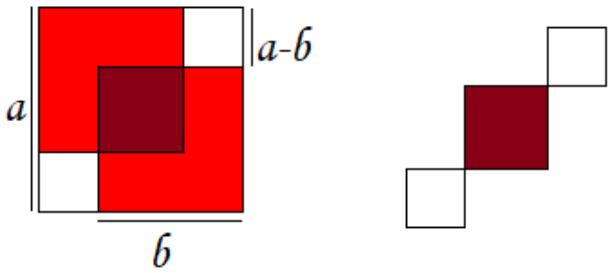

Figura 4.2: Prova geométrica da irracionalidade de $\sqrt{2}$ usando quadrados.

Observamos que, como as áreas dos quadrados eram iguais e a região do meio, que é um quadrado por ter dois ângulos internos comuns aos dos dois quadrados de lado b e os outros dois ângulos serem ângulos correspondentes além de todos os lados medirem $2b - a$, foi coberta duas vezes (e tal intersecção existe pois ao assumirmos $\frac{a}{b} = \sqrt{2} < 2$ temos $b > \frac{a}{2}$), e as regiões brancas, que são quadrados por terem um ângulo interno comum ao do quadrado de lado a e os outros restantes serem ângulos correspondentes além de todos os lados medirem $a - b$, não foram preenchidas, temos então que o quadrado vermelho tem área igual a soma das áreas dos quadrados brancos, conforme a Figura 4.3.

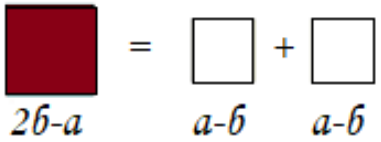

Figura 4.3: Prova geométrica da irracionalidade de $\sqrt{2}$ usando quadrados.

Logo, $(2b-a)^2 = 2(a-b)^2$, ou seja, $\dfrac{(2b-a)^2}{(a-b)^2} = 2$ de onde obtemos $\dfrac{(2b-a)}{(a-b)} = \sqrt{2}$, que nos dá uma nova maneira de escrever $\sqrt{2}$ como um número racional, uma vez que

$$1 < \sqrt{2} \Rightarrow 1 < \frac{a}{b} \Rightarrow b < a \Rightarrow 2b < 2a \Rightarrow 2b - a < 2a - a \Rightarrow 2b - a < a$$

e,

$$\sqrt{2} < 2 \Rightarrow \frac{a}{b} < 2 \Rightarrow a < 2b \Rightarrow a - b < 2b - b \Rightarrow a - b < b,$$

isto é, encontramos outra maneira de escrever $\sqrt{2}$ de modo que esta é uma solução menor que a anterior, o que é um absurdo. Portanto, $\sqrt{2}$ é irracional. ■

Também podemos mostrar que $\sqrt{2}$ é irracional utilizando triângulos equiláteros. Supomos as mesmas condições anteriores, isto é, $\sqrt{2}$ um número racional, igual a $\dfrac{a}{b}$ (com $a, b > 0$, inteiros e primos entre si). Daí, $2 = \left(\dfrac{a}{b}\right)^2 \Rightarrow \dfrac{a^2}{b^2} = 2 \Rightarrow a^2 = 2b^2$. Esta última igualdade garante que se $\sqrt{2}$ for racional, existem dois triângulos equiláteros com áreas A e B, de lados inteiros, medindo a e b, respectivamente, tais que a área do primeiro é duas vezes a área do segundo, ou seja,

$$A = 2B. \tag{4.1}$$

Na figura abaixo temos uma disposição deste fato.

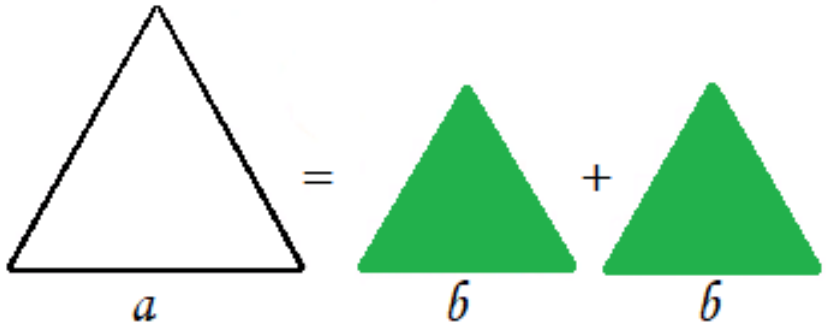

Figura 4.4: Prova geométrica da irracionalidade de $\sqrt{2}$ usando triângulos equiláteros.

Movendo os dois triângulos de lado b de modo a preencher a área do triângulo de lado a, conforme a Figura 4.5, temos que a interseção destes triângulos equiláteros também é um triângulo equilátero de lados $2b - a$ (e de fato essa intersecção existe pois como $\sqrt{2} < 2 \Rightarrow \frac{a}{b} < 2 \Rightarrow \frac{a}{2} < b$), já que possui os três ângulos internos de medidas iguais a 60°, conforme a Figura 4.5

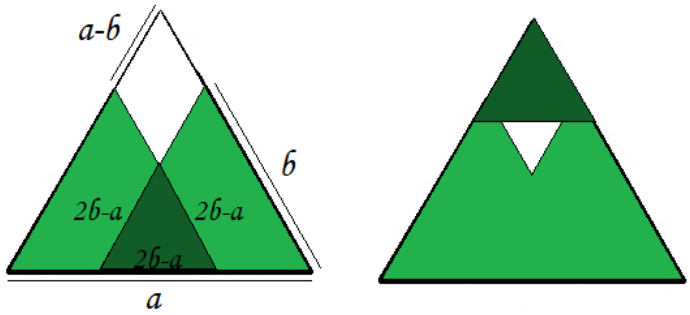

Figura 4.5: Prova geométrica da irracionalidade de $\sqrt{2}$ usando triângulos equiláteros.

Após movermos esse novo triângulo a fim de preencher a área que não foi coberta por estes dois, obtemos por interseção com o triângulo de lado b outros dois novos triângulos menores também equiláteros de lados $3b - 2a$ (essa intersecção existe do fato de termos válida a desigualdade $\frac{3}{2} > \sqrt{2} \Rightarrow \frac{3}{2} > \frac{a}{b} \Rightarrow 3b > 2a \Rightarrow 3b - a > a \Rightarrow (2b - a) + b > a$) uma vez que estes também têm todos os ângulos internos de medidas iguais a 60°. Por fim, a região não coberta, situada no meio do triângulo de lado a, também é um triângulo equilátero cujos lados medem $3a - 4b$, pois tem todos os ângulos iguais a 60° opostos pelo vértice aos ângulos dos triângulos menores obtidos no passo anterior. O que pode ser visto nas Figuras 4.6 e 4.7.

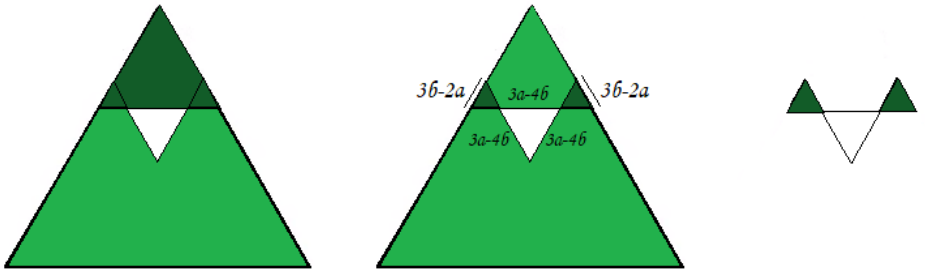

Figura 4.6: Prova geométrica da irracionalidade de $\sqrt{2}$ usando triângulos equiláteros.

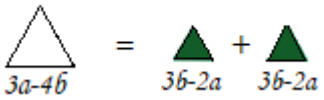

Figura 4.7: Prova geométrica da irracionalidade de $\sqrt{2}$ usando triângulos equiláteros.

Encontramos então uma outra solução menor que a inicial, pois temos $3a-4b < a$ e $3b-2a < b$. A primeira desigualdade decorre do fato que

$$\sqrt{2} < 2 \Rightarrow \frac{a}{b} < 2 \Rightarrow a < 2b \Rightarrow 2a < 4b \Rightarrow 2a + a < 4b + a \Rightarrow 3a - 4b < a.$$

A segunda decorre de

$$1 < \sqrt{2} \Rightarrow 1 < \frac{a}{b} \Rightarrow b < a \Rightarrow 2b < 2a \Rightarrow 2b + b < 2a + b \Rightarrow 3b - 2a < b.$$

Mas isso é um absurdo, pois supomos na hipótese a menor solução, uma vez que a e b são primos entre si. Portanto, o erro decorre de afirmarmos $\sqrt{2}$ um número racional.

É importante destacar que o fato de tais igualdades garantirem a visão geométrica das demonstrações, provém do próximo resultado.

Teorema 4.2. *A área de um polígono regular é proporcional ao quadrado da medida de seu lado.*

Demonstração: Consideremos um polígono regular de n lados de tamanho l. Sabemos que todo polígono regular pode ser dividido em n triângulos isósceles congruentes de base l e altura igual sua apótema. Assim, sua área A pode ser escrita como n vezes a área de um desses triângulos, ou seja,

$$A = n \cdot \left(\frac{l \cdot h}{2} \right). \tag{4.2}$$

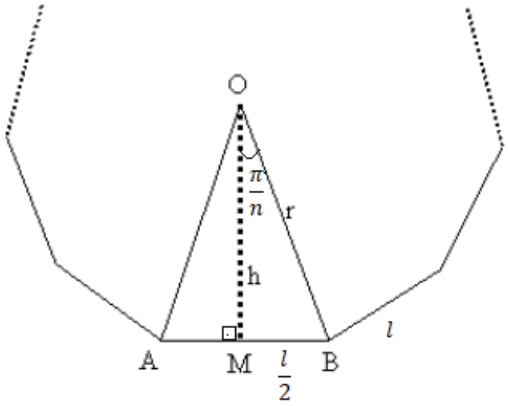

Figura 4.8: Exemplo de um polígono regular.

De fato, como o polígono é dividido em n triângulos isósceles congruentes, temos que cada um dos ângulos opostos à base medem $\frac{2\pi}{n}$. Além do mais, como estes triângulos são isósceles, a apótema coincide com sua altura que, por sua vez, coincide com mediana e mediatriz. Assim, a apótema divide o triângulo em outros dois triângulos retângulos congruentes de catetos de medida $\frac{l}{2}$ e h (apótema). Logo, nestes triângulos retângulos temos que o ângulo oposto a base de medida $\frac{l}{2}$ mede $\frac{\pi}{n}$ e calculando sua tangente obtemos

$$tg\left(\frac{\pi}{n}\right) = \frac{\frac{l}{2}}{h}.$$

Isolando h, obtemos

$$h = \frac{l}{2tg\left(\frac{\pi}{n}\right)}. \tag{4.3}$$

Por fim, substituindo (4.3) em (4.2), obtemos

$$A = \frac{nl^2}{4tg\left(\frac{\pi}{n}\right)}.$$

Fazendo $k = \dfrac{n}{4tg\left(\frac{\pi}{n}\right)}$, concluímos $A = kl^2$ e o resultado está provado. ■

Utilizando ainda este resultado e a demonstração por contradição é possível provar a irracionalidade de $\sqrt{3}$ e $\sqrt{5}$, o que faremos nas próximas seções.

4.2 Demonstração Geométrica da Irracionalidade de $\sqrt{3}$

Nesta seção demonstramos, usando argumentos geométricos, a irracionalidade de $\sqrt{3}$.

Teorema 4.3. *$\sqrt{3}$ é um número irracional.*

Demonstra ção: Suponhamos que é possível ter $\sqrt{3} = \dfrac{a}{b}$ (com $a, b > 0$, inteiros e primos entre si), ou seja, $3 = \left(\dfrac{a}{b}\right)^2 \Rightarrow 3 = \dfrac{a^2}{b^2} \Rightarrow a^2 = 3b^2$. Pelo Teorema 4.2, essa última igualdade garante que, se $\sqrt{3}$ for racional, existem dois triângulos equiláteros de áreas A e B, de lados inteiros medindo a e b, respectivamente, tais que a área do primeiro é três vezes a área do segundo:

$$A = 3B. \tag{4.4}$$

O que pode ser visto geometricamente na Figura 4.9.

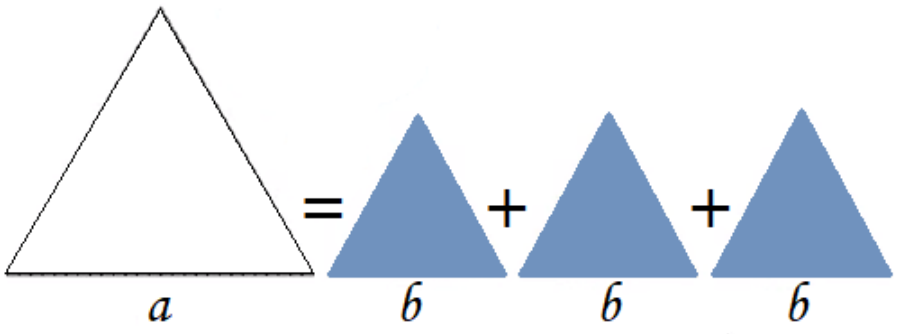

Figura 4.9: Prova geométrica da irracionalidade de $\sqrt{3}$ usando triângulos equiláteros.

Movendo os triângulos de lado b a fim de cobrir a área do triângulo de lado a, obtemos pela interseção dos triângulos de lado b outros três triângulos equiláteros de lados de medida $2b - a$, pois todos os ângulos têm medidas iguais a $60°$ (esta intersecção ocorre já que é válido a desigualdade $\sqrt{3} < 2$ então $\dfrac{a}{b} < 2 \Rightarrow \dfrac{a}{2} < b$) e um triângulo equilátero não coberto de lados $2a - 3b$. Então, como

a igualdade entre as áreas deve se manter e as áreas cobertas pelos triângulos de lados $2b-a$ foram preenchidas cada uma duas vezes e a área do triângulo de lados $2a-3b$ não foi preenchida, temos que a soma das áreas dos triângulos de lados $2b-a$ deve ser igual a área do triângulo de lados $2a-3b$. Isto significa que podemos repetir a construção já realizada para os triângulos de lados a e b, dessa vez usando os triângulos de lados $2a-3b$ e $2b-a$, conforme as Figuras 4.10 e 4.11.

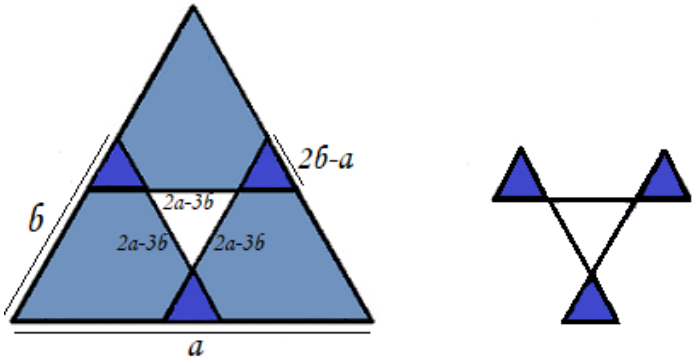

Figura 4.10: Prova geométrica da irracionalidade de $\sqrt{3}$ usando triângulos equiláteros.

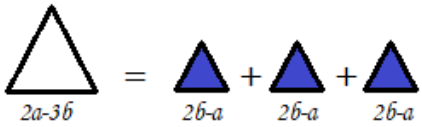

Figura 4.11: Prova geométrica da irracionalidade de $\sqrt{3}$ usando triângulos equiláteros.

Logo, usando novamente o Teorema 4.2, sabemos que a área do triângulo de lado $(-3b+2a)$ é $k(-3b+2a)^2$ e a área do triângulo de lado $2b-a$ é $k(2b-a)^2$, assim temos $k(-3b+2a)^2 = 3k(2b-a)^2 \Rightarrow \dfrac{(-3b+2a)^2}{(2b-a)^2} = 3 \Rightarrow \left(\dfrac{-3b+2a}{2b-a}\right)^2 = 3 \Rightarrow \dfrac{(-3b+2a)}{(2b-a)} = \sqrt{3}$. O que nos dá uma menor solução pois,

$$1 < \sqrt{3} \Rightarrow 1 < \frac{a}{b} \Rightarrow b-a < 0 \Rightarrow b-a+b < b \Rightarrow 2b-a < b$$

e,

$$\sqrt{3} < 3 \Rightarrow \frac{a}{b} < 3 \Rightarrow a < 3b \Rightarrow a-3b < 0 \Rightarrow a-3b+a < a \Rightarrow 2a-3b < a.$$

Mas isso é um absurdo pois supomos a e b irredutíveis. Portanto, $\sqrt{3}$ é irracional. ■

4.3 Demonstração Geométrica da Irracionalidade de $\sqrt{5}$

Nesta seção demonstramos, usando argumentos geométricos, a irracionalidade de $\sqrt{5}$.

Teorema 4.4. *$\sqrt{5}$ é irracional.*

Demonstração: Suponhamos, por absurdo, que $\sqrt{5}$ seja um número racional, ou seja, $\sqrt{5} = \frac{a}{b}$, com $a, b \in \mathbb{Z}$ e $a, b > 0$, isso implica $a^2 = 5b^2$. Pelo Teorema 4.2, temos que existe dois pentágonos regulares de áreas A e B, com lados inteiros medindo respectivamente a e b, tal que a área do primeiro é igual a cinco vezes a área do segundo pentágono:

$$A = 5B. \tag{4.5}$$

O que pode ser visto geometricamente na Figura 4.12.

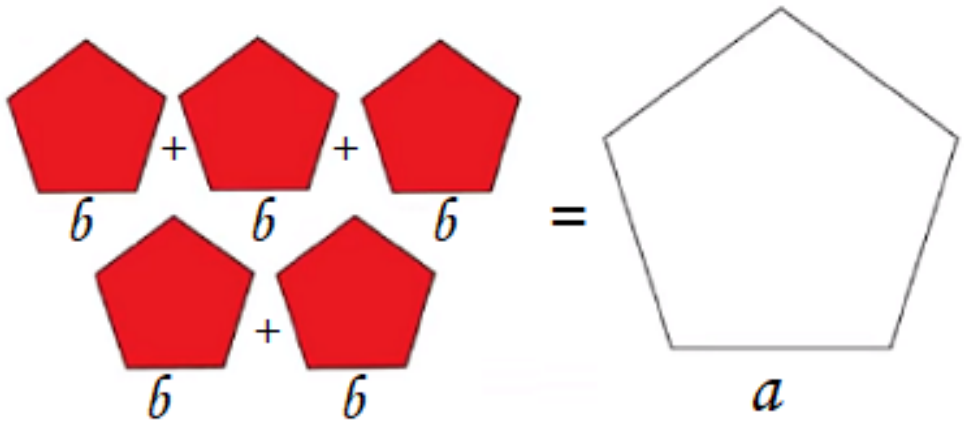

Figura 4.12: Prova geométrica da irracionalidade de $\sqrt{5}$ usando pentágonos regulares.

Movendo pentágonos de lado b de modo a preencher a área do pentágono de lado a, vemos que a área do pentágono de lado a pode ser expressa como: $A = 5B + C + 5D - 5P$ e usando (4.5) temos

$$C = 5(P - D).$$

Olhando com mais cuidado os polígonos P e D, percebemos que $P' = P - D$ é um pentágono. De fato, P' é um pentágono regular pois possui quatro de seus ângulos congruentes ao ângulo interno $\alpha = \frac{3\pi}{5}$ do pentágono regular B e tem lados de mesma medida $a - 2b$ devido ao lado do triângulo D após sobrepor ao P. Além disso, C também é um pentágono regular pois tem todos os seus ângulos internos opostos pelo vértice a ângulos internos do pentágono regular P' e todos os lados de C medem $b - 2(a - 2b) = 5b - 2a$. Uma disposição deste fato está nas Figuras 4.13 e 4.14 abaixo.

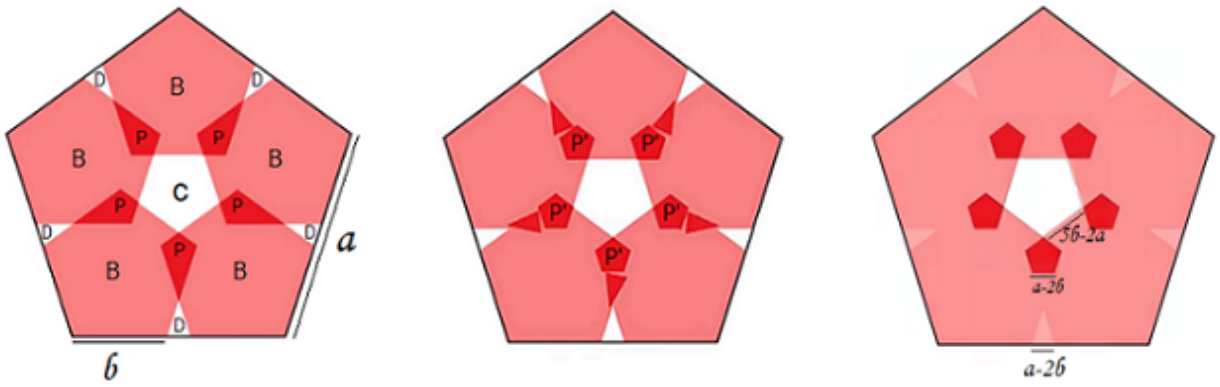

Figura 4.13: Prova geométrica da irracionalidade de $\sqrt{5}$ usando pentágonos regulares.

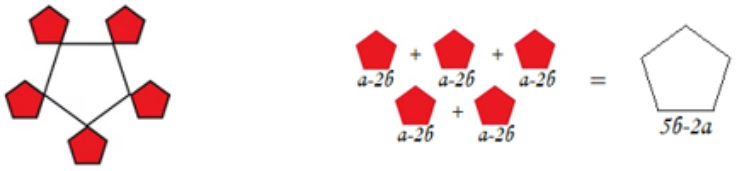

Figura 4.14: Prova geométrica da irracionalidade de $\sqrt{5}$ usando pentágonos regulares.

Recaímos dessa forma no raciocínio inicial da demonstração, onde temos que $C = 5P'$, e juntamente com o Teorema 4.2, temos $k(5b - 2a)^2 = 5k(a - 2b)^2 \Rightarrow \frac{(5b - 2a)}{a - 2b} = \sqrt{5}$ o que nos dá uma menor solução pois $\frac{5}{3} < 2 = \sqrt{4} < \sqrt{5} < \sqrt{9} = 3$. Então $\frac{5}{3} < \sqrt{5}$ e $\sqrt{5} < 3$. De $\frac{5}{3} < \sqrt{5}$ temos, $5 < 3\sqrt{5} \Rightarrow 5 < 3\frac{a}{b} \Rightarrow 5b < 3a \Rightarrow 5b - 3a < 0 \Rightarrow 5b - 3a + a < a \Rightarrow 5b - 2a < a$. De $\sqrt{5} < 3$ temos, $\frac{a}{b} < 3 \Rightarrow a < 3b \Rightarrow a - 3b < 0 \Rightarrow a - 3b + b < b \Rightarrow a - 2b < b$. Mas isso é uma contradição, uma vez que a e b eram mínimos. Portanto, $\sqrt{5}$ é irracional. ■

Podemos encontrar em [5] uma ilustração da irracionalidade de $\sqrt{5}$ e $\sqrt{6}$ utilizando triângulos equiláteros sem muitos detalhes, e em [8] temos a demonstração para $\sqrt{6}$ utilizando hexágonos regulares. Ainda em [8] a seguinte pergunta nos é apresentada: "para a demonstração da irracionalidade de $\sqrt{2}$ usa-se quadrados, para a de $\sqrt{3}$ usamos triângulos regulares, para a de $\sqrt{5}$ usamos pentágonos regulares, a irracionalidade de $\sqrt{6}$ também pode ser verificada usando hexágonos regulares. Logo, o método permite provar a irracionalidade de todos os números que não sejam quadrados perfeitos?" Nele, os autores esclarecem que não sabem responder a pergunta, uma vez que tentaram reproduzir essa técnica de demonstração para provar a irracionalidade de $\sqrt{7}$ sem sucesso, destacando ainda que o método se torna mais trabalhoso à medida que se necessita usar polígonos de mais lados. Da mesma forma em [11], os autores convidam os leitores a explorar outros números irracionais com essa técnica, isto é, se estamos querendo provar que "se n não é um quadrado perfeito então sua raiz quadrada não é um número racional", temos que provar geometricamente que dado n polígonos regulares idênticos de lados inteiros, o polígono regular semelhante cuja área é igual a soma das áreas desses n polígonos, não possuirá lados inteiros.

Referências Bibliográficas

[1] ALFRADIQUE, Zilvan de Oliveira. *Um olhar sobre as demonstrações da irracionalidade de dois e zeta de três*. 2017. 57 p. Dissertação (Mestrado Profissional em Matemática) - Pontifícia Universidade Católica do Rio de Janeiro, Rio de Janeiro.

[2] BRASIL. Secretaria de Educação Fundamental. *Parâmetros Curriculares Nacionais*: Matemática. Brasília, 1998.

[3] BRASIL. Ministério da Educação. *Base Nacional Comum Curricular*. Brasília, 2018.

[4] BRASIL. Ministério da Educação. *Base Nacional Comum Curricular*. Proposta Preliminar - Segunda Versão - Brasília, 2016.

[5] Canal Mathologer. 1 vídeo (18:08 min). *Visualising irrationality with triangular squares*. Disponível em: https://youtu.be/yk6wbvNPZW0. Acesso: 13 mar, 2020.

[6] FIGUEIREDO, Djairo G. de. *Números Irracionais e Transcendentes*. Brasília: Sociedade Brasileira de Matemática, 1985.

[7] FILHO, Daniel Cordeiro de Morais. *Um Convite à Matemática*. - 2ª ed. - Rio de Janeiro: SBM, 2013.

[8] FILHO, Daniel Cordeiro de Morais.; ANDRADE, Caio Antony Gomes de Matos.; SILVA, Ismael Sandro da. *Demonstrações Geométricas de Irracionalidade*. Rio de Janeiro: RPM, n° 94, 31-35.

[9] FRANCO, Valdeni Soliani.; GERÔNIMO, João Roberto. *Fundamentos da Matemática: uma introdução à lógica, teoria dos conjuntos, relações e funções*. - 2ª ed. - Maringá: EDUEM, 2008.

[10] HEFEZ, Abramo. *Aritmética*. - 2ª ed. - Rio de Janeiro: SMB, 2016.

[11] MILLER, Steven J.; MONTAGUE. David. *Irrationality from the Book*. Math. Mag. 85, 2012. p. 110 - 114.

[12] OLIVEIRA, Julimar Carlos de.; GOMES, Carlos Cruz. *Números Irracionais e Transcendentes*. 2009. 61 p. Monografia (Especialização em Matemática) - Universidade Federal de Santa Catarina e Universidade Virtual do Maranhão, Imperatriz.

[13] SANTOS, José Plínio de Oliveira. *Introdução à Teoria dos Números*. Rio de Janeiro: Instituto de Matemática Pura e Aplicada, CNPq, 1998.

[14] SILVA, Guimarães Vieira da. *Irracionalidade e Transcendência: Aspectos Elementares*. 2018. 48 p. Dissertação (Mestrado Profissional em Matemática) - Universidade Federal do Tocantins, Arraias.