Universidade Estadual Paulista "Júlio de Mesquita Filho"
Instituto de Geociências e Ciências Exatas
Campus de Rio Claro

"A Irracionalidade e Transcendência do Número π"

João Milton de Oliveira

Dissertação apresentada ao Programa de Pós-Graduação – Mestrado Profissional em Matemática em Rede Nacional como requisito parcial para a obtenção do grau de Mestre

Orientadora
Profa. Dra. Elíris Cristina Rizziolli

2013

512 Oliveira, João Milton de
O48i "A Irracionalidade e Transcendência do Número π"/ João Milton de Oliveira- Rio Claro: [s.n.], 2013.
43 f.: il., forms., tabs.

Dissertação (mestrado) - Universidade Estadual Paulista, Instituto de Geociências e Ciências Exatas.
Orientadora: Elíris Cristina Rizziolli

1. Álgebra. 2. Teoria dos Números. 3. Números Algébricos. I. Título

Ficha Catalográfica elaborada pela STATI - Biblioteca da UNESP
Campus de Rio Claro/SP

TERMO DE APROVAÇÃO

João Milton de Oliveira

"A Irracionalidade e Transcendência do Número π"

Dissertação APROVADA como requisito parcial para a obtenção do grau de Mestre no Curso de Pós-Graduação Mestrado Profissional em Matemática em Rede Nacional do Instituto de Geociências e Ciências Exatas da Universidade Estadual Paulista "Júlio de Mesquita Filho", pela seguinte banca examinadora:

Profa. Dra. Elíris Cristina Rizziolli
Orientadora

Prof. Dr. Aldicio José Miranda
Instituto de Ciências Exatas - UNIFAL - MG - ALFENAS/MG

Profa. Dra. Marta Cilene Gadotti
Departamento de Matemática - IGCE - UNESP/Rio Claro

Rio Claro, 28 de Janeiro de 2013

À minha esposa e meu filho...

Agradecimentos

Primeiramente a Deus que permitiu que tudo isso acontecesse, ao longo de minha vida.

Agradeço a minha esposa Márcia e ao meu filho João Pedro pelo apoio e compreensão da minha ausência, nos momentos dedicados aos estudos.

Obrigado a todos os meus familiares, que nos momentos de minha ausência dedicados ao estudo, sempre fizeram entender que o futuro é feito a partir da dedicação no presente.

Agradeço à Profa. Dra. Elíris Cristina Rizziolli, pela orientação e tempo dedicado a esse projeto.

Agradeço aos professores do Departamento de Matemática da Unesp de Rio Claro, em especial à Profa. Dra. Suzinei Aparecida Siqueira Marconato por sempre ter uma palavra de apoio. Agradeço também à CAPES, pelo apoio financeiro, importante para o desenvolvimento desse projeto.

Por fim quero agradecer aos meus amigos. Aos que estiveram presentes tanto nos momentos difíceis como nos momentos felizes, em especial aos amigos Gilberto, Maciel e Amauri, cujo apoio foi fundamental.

A todos citados acima, muito obrigado!

As leis da natureza nada mais são que pensamentos matemáticos de Deus.

Kepler.

Resumo

O objetivo desta dissertação é fazer uma exposição elementar sobre a irracionalidade de certos números reais, a construção de um número transcendente, além disso, demonstrar a irracionalidade e transcendência do número π. Entre outras ferramentas, utilizamos o Cálculo Diferencial e Integral de uma variável.

Palavras-chave: Álgebra, Teoria dos Números, Números Algébricos.

Abstract

The purpose of this dissertation is to present an elementary statement about irrationality of certain real numbers, the construction of a transcendental number, furthermore demonstrate the irrationality and transcendence of the π number. Among other tools, we have made use the Differential and Integral Calculus of one variable.

Keywords: Algebra, Number Theory, Algebraic Numbers.

Sumário

Introdução

Como se sabe π, é o número mais famoso da história universal, o qual recebeu um nome próprio, um nome grego, pois embora seja um número, não pode ser escrito com um número finito de algarismos. O π representa a razão entre o perímetro de qualquer círculo e seu diâmetro.

O número π tem uma história fascinante, que começou milênios atrás. No velho testamento (Primeiro Livro dos Reis $7:23$) lê-se: *"E ele (Salomão) fez também um lago de dez cúbitos, de margem a margem, circular, cinco cúbitos de fundo, e trinta cúbitos em redor."* Este mesmo verso aparece também em (II Crónicas $4:2$). Esta passagem ocorre numa lista de especificações para a construção do grande templo de Salomão. A circunferência era, seis vezes o raio, ou três vezes o diâmetro. Isto significa que os antigos Hebreus se contentavam em atribuir a π o valor 3.

Este valor foi muito possivelmente encontrado por medição. O valor 3 foi usado durante muito tempo por motivos religiosos e culturais em certas civilizações, como a dos Egípcios e a dos Babilônios, quando já se conheciam, nessas mesmas civilizações determinações melhores. Os melhores valores Egípcios e Babilônios que se conhecem são respectivamente $4(\frac{8}{9})^2 = 3,16$ e $3+\frac{1}{8} = 3,125$.

No caso egípcio ignoramos como chegaram ao valor $4(\frac{8}{9})^2$, que se encontra no Papiro de Ahmes ou Rhind, gravado no segundo século a.C.. Curiosamente é este valor que se obtém experimentalmente, medindo a circunferência de latas, pratos e cestas e dividindo-a pelos diâmetros respectivos.

No caso Babilônio o valor $3+\frac{1}{8}$ deduz-se de uma das Placas de Susa, único exemplo conhecido nessas épocas do que parece ser familiaridade com um processo geral que, em princípio, permite determinações tão exatas quanto se queira. Não sabemos de que modo os Babilônios chegaram a esta boa aproximação.

Arquimedes de Siracusa (287-212 a.C.), pôs mãos à obra com experimentos novos, muito mais profundos. Sabia que π não era racionalmente determinável, ou, ao menos, o suspeitava. Assim sendo, propôs-se descobrir um processo para a determinação de π, o Método de Arquimedes, com a precisão que se desejasse. Ele usou, processos geométricos, que dão limites inferiores e superiores para π. Arquimedes utilizou alguns polígonos regulares, com um número crescente de lados, até chegar ao polígono de 96 lados, através do qual obteve a seguinte aproximação de π,

$$3,1410 < \pi < 3,1428.$$

A época do Renascimento Europeu trouxe, na altura devida, um novo mundo matemático. Entre os primeiros efeitos deste renascer está a necessidade de encontrar uma fórmula para o π. Descobriu-se então a definição não geométrica de π e do papel "não geométrico"deste valor. Assim se chegou à descoberta das representações de π por séries infinitas. Um dos primeiros foi Wallis (1616-1703) com a fórmula,

$$\pi = 2 \cdot \left(\frac{2}{1} \cdot \frac{2}{3} \cdot \frac{4}{3} \cdot \frac{4}{5} \cdot \frac{6}{5} \cdot \frac{6}{7} \cdot ... \right).$$

Uma outra fórmula que é por vezes atribuída a Leibniz (1646-1716), mas que parece ter sido primeiro descoberta por James Gregory (1638-1675) é

$$\pi = 4 \cdot \left(\frac{1}{1} - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} + \frac{1}{9} - ... \right).$$

A série de Gregory converge lentamente, de tal forma que se pretendermos obter quatro casas decimais corretas temos que ter cerca de 10000 termos da série. Esta fórmula é mais apropriada para o cálculo computacional do que para o cálculo humano. Contudo Gregory também demonstrou um resultado mais geral,

$$arctg(x) = x - \frac{x^3}{3} + \frac{x^5}{5} - \frac{x^7}{7} + ..., \qquad -1 \leq x \leq 1,$$

então usando o seguinte fato

$$arctg\left(\frac{1}{\sqrt{3}}\right) = \frac{\pi}{6}$$

conclui-se que,

$$\frac{\pi}{6} = \left(\frac{1}{\sqrt{3}}\right) \cdot \left(1 - \frac{1}{(3 \cdot 3)} + \frac{1}{(5 \cdot 3 \cdot 3)} - \frac{1}{(7 \cdot 3 \cdot 3 \cdot 3)} + ...\right)$$

a qual converge mais rapidamente, pois para se obter quatro casas decimais corretas necessitamos apenas de nove termos da série.

Em 1706, John Machin introduziu uma variação da série de Gregory com um aumento significativo da convergência. Ele conseguiu calcular o π com 100 casas decimais. A fórmula de Machin é uma das que ainda hoje é usada, pelos programas de computadores, para calcular os dígitos do π. A fórmula encontrada por Machin é dada por,

$$\frac{\pi}{4} = 4 \cdot arctg\left(\frac{1}{5}\right) - arctg\left(\frac{1}{239}\right).$$

Um inglês chamado Shanks, usou a fórmula de Machin para calcular π até às 707 casas decimais, das quais só 527 estavam corretas, publicando o resultado do seu trabalho em 1873.

Em 1949 um computador foi usado para calcular π até às 2000 casas decimais. Em 1961 conseguiu-se através de computação a aproximação de π através de 100 265 casas decimais, mais tarde em 1967 aproximou-se até às 500 000 casas decimais.

Recentemente, David Bailey, Peter Borwein e Simon Plouffe contabilizaram dez bilhões de casas decimais para π , usando uma fórmula que dá cada casa decimal do π individualmente, para cada n escolhido.

É ainda importante destacar, que o primeiro a usar o símbolo π, com o significado que este tem hoje em dia, foi o matemático inglês William Jones em 1706. O matemático suíço Leonhard Euler em 1737 adotou o símbolo que rapidamente se tornou uma notação padrão.

Após esta Introdução a estrutura do trabalho foi organizada como segue:

No capítulo 2 iniciamos a teoria de inteiros algébricos, números algébricos e números transcendentais, bem como um exemplo de construção de um número transcendental.

No capítulo 3 demonstramos a irracionalidade do número π.

No capítulo 4, a demonstração de que o número π é transcendente, é baseada na demonstração feita por R. Moritz, em Annals of Mathematics, vol. 2 (1901). Contudo faremos uma substituição na demonstração de Moritz: no momento em que aplica o teorema do valor médio para polinômios complexos substituiremos esse passo por uma "desigualdade do valor médio".

Finalmente, no capítulo 5, apresentamos uma sugestão de aula contendo os tópicos abordados nos capítulos anteriores.

1 Sobre Teoria dos Números

Neste capítulo apresentamos tópicos sobre teoria dos números, os quais são necessários aos demais.

Definição 1.1. *Dados $a, b \in \mathbb{Z}$, dizemos que* ***a divide b****, e escrevemos $a|b$, se existir $q \in \mathbb{Z}$ tal que $b = qa$.*

Exemplo 1.1. $a = 2$, $b = 4$; $4 = q2 \Longrightarrow q = 2$.

Definição 1.2. ***(a)*** *Um número $p \in \mathbb{N}$, $p > 1$, é* ***primo*** *se os únicos números inteiros que o dividem são ele próprio e o 1. Ou seja, p é primo se para todo $b \in \mathbb{N}$ tal que $b|p$, então $b = p$ ou $b = 1$.*

(b) *Um número $p \in \mathbb{Z}$, $p \neq 0$ e $p \neq \pm 1$, é* ***primo*** *se os únicos números inteiros que o dividem são $\pm p$ e ± 1.*

Exemplo 1.2. $p = 7, \quad b|7 \Longleftrightarrow b = 7$ *ou* $b = 1$.

Definição 1.3. *Seja $a \in \mathbb{Z}$. Um número inteiro b é chamado* ***múltiplo*** *de a se $b = aq$, para algum $q \in \mathbb{Z}$.*

Exemplo 1.3. $a = 6$, $q = 3$; $\quad b = 6.3 \Longrightarrow b = 18$. Logo, b é múltiplo de 6 e também de 3.

Definição 1.4. *Dados $a, b \in \mathbb{Z}$, um número natural d é chamado o* ***máximo divisor comum*** *de a e b, denotado por $d = m.d.c(a, b)$, se satisfaz as afirmações abaixo:*

(i) $d|a$ e $d|b$,

(ii) se $r \in \mathbb{Z}$, é tal que $r|a$ e $r|b$, então $r|d$.

Exemplo 1.4. $a = 16$, $b = 32$ $m.d.c.(16, 32) = 16 = d$. Pois $16|16$ *e* $16|32$ e além disso se $r|16$ *e* $r|32$ então $r|16$ (por exemplo se $r = 4$, temos que $4|16$, $4|32$ e ainda que $4|16$.

Observação 1.1. O $m.d.c(a, 0)$ não existe caso a seja **nulo**. Além disso, assumimos que $m.d.c(a, 0) = a$, se $a \neq 0$.

Teorema 1.1. ***(Algoritmo da Divisão)***. *Se $a, b \in \mathbb{Z}$, com $b \neq 0$, então existem (e são únicos) $q, r \in \mathbb{Z}$ com $0 \leq r < |b|$, tais que,*

$$a = qb + r. \tag{1}$$

Demonstração. (i) **Existência.**

$\mathbf{b > 0}$. Consideremos o conjunto dos números múltiplos de b ordenados de acordo com a ordem natural da reta, isto é, o conjunto ..., $-3b$, $-2b$, $-b$, 0, b, $2b$, $3b$, ..., com,

$$...-3b \leq -2b \leq -b \leq 0 \leq b \leq 2b \leq 3b...$$

Note que disso decorre uma decomposição da reta em intervalos disjuntos da forma

$$[qb, (q+1)b] = \{x \in \mathbb{R} : qb \leq x < (q+1)b, \text{ com } q \in \mathbb{Z}\}.$$

Por exemplo $[-3b, -2b] = [-3b, (-3+1)b]$, $[b, 2b] = [1b, (1+1)b]$,
$[2b, 3b] = \{x \in \mathbb{R} : 2b \leq x < 3b\}$.

Assim, dado $a \in \mathbb{Z}$, este pertence a apenas um desses intervalos e portanto necessariamente é da forma $a = qb+r$, com $q \in \mathbb{Z}$ e $r \geq 0$. É claro que $r < (q+1)b - qb = b$.

$\mathbf{b < 0}$. Aplicamos o teorema no caso demonstrado em (i) para determinar $q', r \in \mathbb{Z}$, com $0 \leq r < |b|$ para escrever:

$$a = q'|b| + r. \tag{2}$$

Fazendo $q = -q'$, como $|b| = -b$, (pois $b < 0$), obtemos de (2) $a = qb + r$, onde $q, r \in \mathbb{Z}$ e $0 \leq r < |b|$.

(ii) **Unicidade**.

Resta demonstrar que q e r, os quais satisfazem (1) são únicos. De fato, suponha que $a = qb + r$ e $a = q_1 b + r_1$, com $0 \leq r < |b|$ e $0 \leq r_1 < |b|$. Assim,

$$qb + r = q_1 b + r_1 \Rightarrow$$

$$r - r_1 = (q_1 - q)b \tag{3}$$

Afirmamos que $r = r_1$.

Com efeito, se $r \neq r_1$, então: $0 < |r_1 - r|$. Além disso, $|r_1 - r| < b$. De fato, vamos admitir, sem perda de generalidade que $r < r_1$, consequentemente $r_1 - r > 0$ e $|r_1 - r| = r_1 - r$.

Assim, se $r_1 - r = |b|$, então $r_1 = |b| + r$ e portanto $r_1 > |b|$, que é absurdo.

Também, se $r_1 - r > |b|$, então $r_1 > |b| + r > |b|$, gerando novamente o absurdo $r_1 > b$.

Logo pela Lei da Tricotomia,

$$|r_1 - r| = r_1 - r < |b|.$$

Segue que

$$0 < |r_1 - r| < |b|. \tag{4}$$

Agora de (3) obtemos,

$$|r_1 - r| = |q_1 - q||b|. \tag{5}$$

Substituindo (5) em (4), obtemos,

$$0 < |q_1 - q||b| < |b|.$$

Logo, $0 < |q_1 - q| < 1$, o que é um absurdo, pois $|q_1 - q|$ é um número inteiro (pois q *e* $q_1 \in \mathbb{Z}$ e em $\mathbb{Z}$ vale a Lei do Fechamento da Adição).

Portanto $r = r_1$.

Note que essa igualdade combinada com (3) implica $q_1 = q$, já que $0 = (q_1 - q)b$ e $b \neq 0$ por hipótese. □

Exemplo 1.5. $a = 11, b = 5; \quad q = 2 \;\; r = 1 \Longrightarrow 11 = 2.5 + 1.$

Teorema 1.2. *Dados $a, b \in \mathbb{Z}$, pelo menos um deles não nulo, existem $x_0, y_0 \in \mathbb{Z}$ tais que $ax_0 + by_0 = d$, onde $d = m.d.c(a, b)$.*

Demonstração. Limitando-se ao caso em que $a > 0$ e $b > 0$.

Seja $L = \{ax + by \mid x, y \in \mathbb{Z}\}$. Evidentemente existem elementos estritamente positivos em L (faça-se, por exemplo, $x = y = 1$). Seja d o menor desses elementos, $d = min\{ax + by \in L, ax + by > 0\}$. Mostremos que d é o máximo divisor comum entre a e b.

(i) d é obviamente maior que zero;

(ii) Como $d \in L$, então existem $x_0, y_0 \in \mathbb{Z}$ de maneira que $d = ax_0 + by_0$. Aplicando o algorítmo da divisão aos elementos a e d:

$$a = dq + r, \text{ em que } 0 \leq r < d.$$

Das duas últimas igualdades obtemos

$$a = (ax_0 + by_0)q + r$$

ou, ainda

$$r = a(1 - qx_0) + b(-y_0)q$$

o que vem mostrar que $r \in L$.

Agora sendo r positivo, chegamos a uma contradição, pois $r < d$, contraria a minimalidade de d. A conclusão é que $r = 0$. Daí ficamos com $a = dq$ o que mostra que $d|a$. Analogamente se prova que $d|b$;

(iii) Se $d'|a$ e $d'|b$, como $d = ax_0 + by_0$, então é claro que $d'|d$, e portanto $d = m.d.c(a, b)$. □

Lema 1.1. *Sejam $a, x_0, b, y_0, d \in \mathbb{Z}$, se $d|a$ e $d|b$, então $d|(ax_0 + by_0)$.*

Demonstração. Como $d|a$ (pela definição 1.1) implica que existe $q \in \mathbb{Z}$, tal que $a = qd$. Também (pela definição 1.1) $d|b$ implica que existe $p \in \mathbb{Z}$, tal que $b = pd$.

Logo,

$$ax_0 + by_0 = qdx_0 + pdy_0 = d(qx_0 + py_0).$$

Observe que $K = (qx_0 + py_0) \in \mathbb{Z}$, (pois vale a lei do fechamento da adição e multiplicação em $\mathbb{Z}$ e $q, x_0, p, y_0 \in \mathbb{Z}$).

Portanto, $ax_0 + by_0 = dK, \quad K \in \mathbb{Z}$, ou seja,

$$d|(ax_0 + by_0).$$

□

Exemplo 1.6. $2|4$ e $2|6 \Rightarrow 2|(4x_0 + 6y_0)$, $\forall\ x_0,\ y_0\ \in\ \mathbb{Z}$.

Lema 1.2. *Seja $r \in \mathbb{N}$ um número primo, e $a, b \in \mathbb{Z}$. Se r divide o produto $\boldsymbol{ab}$ então r divide $\boldsymbol{a}$ ou $\boldsymbol{b}$.*

Demonstração. Se $r|a$, nada temos que provar.

Suponhamos que r não divide a, ou seja, r e a são primos entre si.

Logo, pelo Teorema 1.2, existem $x_0, y_0 \in \mathbb{Z}$ tais que $ax_0 + ry_0 = 1$.

Assim,

$$abx_0 + rby_0 = b. \tag{6}$$

Como $r|ab$ (por hipótese) e claramente $r|rb$, logo pelo Lema 1.1, segue que,

$$r|(abx_0 + rby_0).$$

Portanto de (6) segue que $r|b$. □

Exemplo 1.7. :

1) $r = 3$, $a = 9$, $b = 5$, temos que $3|9.5$ e também $3|9$.

2) $r = 3$, $a = 9$, $b = 6$, temos que $3|9.6$ e também $3|9$ e $3|6$.

Corolário 1.1. *Seja $r \in \mathbb{N}$ um número primo e $a \in \mathbb{Z}$. Se $r|p^n$, então $r|p$.*

Demonstração. Esse resultado segue usando o Princípio da Indução Finita.

Queremos mostrar a veracidade da sentença.

$$\mathcal{P}(n): \text{ “ Se } r|p^n, \text{ então } r|p, \forall n \in \mathbb{N}\text{”}.$$

Façamos isso.

Note que, obviamente, $\mathcal{P}(1)$ é válida,

$$\mathcal{P}(1): r|p \Longrightarrow r|p.$$

Além disso, observe que $\mathcal{P}(2)$ também é válida pois se $r|p^2$, pelo Lema 1.2, se $r|p.p$, então $r|p$ ou $r|p$, isto é, $r|p$.

Hipótese de Indução . Seja $k \in \mathbb{N}$, qualquer.

$$\mathcal{P}(k): \text{“Se } r|p^k, \text{ então } r|p.\text{”}$$

Usando a Hipótese de Indução queremos mostrar que $\mathcal{P}(k+1)$ é válida, ou seja,

$$\text{“Se } r|p^{k+1}, \text{ então } r|p.\text{”}$$

Observe que $r|p^{k+1}$ é o mesmo que $r|p^k.p$.

Agora, pelo Lema 1.2, segue que $r|p^k$ ou $r|p$.

Por outro lado, temos por Hipótese de Indução que $r|p^k$ implica que $r|p$.

Portanto, $r|p^{k+1}$ implica $r|p^k$ ou $r|p$, isto é, $r|p$. □

2 Números Algébricos e Números Transcendentes

Neste capítulo apresentamos elementos essenciais para o tratamento dos próximos capítulos.

Qualquer solução de uma equação polinomial da forma

$$x^n + a_{n-1}x^{n-1} + ... + a_1x + a_0 = 0, \tag{2.1}$$

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

Exemplo 2.1. :

1) Qualquer número inteiro b é inteiro algébrico pois a equação

$$x - b = 0 \tag{2.2}$$

tem b por solução.

2) $\sqrt{3}$ e $-\sqrt{3}$ são inteiros algébricos, pois eles são as soluções da equação

$$x^2 - 3 = 0. \tag{2.3}$$

3) Podemos verificar que $\sqrt{2+\sqrt{3}}$ é um inteiro algébrico pois é uma solução da equação

$$x^4 - 4x^2 + 1 = 0. \tag{2.4}$$

Para obtermos a equação (2.4), basta escrever $x = \sqrt{2+\sqrt{3}}$ e mediante duas quadraturas consecutivas livrar-se dos radicais. Apesar de usarmos no presente capítulo inteiros algébricos que sejam números reais, chamamos a atenção para o fato que há inteiros algébricos complexos.

4) $i = \sqrt{-1}$ e $-i$ são inteiros algébricos, pois são as raízes de $x^2 + 1 = 0$.

5) Todo número da forma $\sqrt{2n}$, com $n \in \mathbb{N}$, é um inteiro algébrico.

De fato,

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

e esta última é uma equação do tipo (2.1), para $n = 1,\ a_0 = -2n$.

6) Para cada $a \in \mathbb{Z}^*$, o número complexo $i\sqrt{a}$ é um inteiro algébrico, pois é solução da equação $x^2 + a = 0$.

Observação 2.1. Dos exemplos acima, podemos observar que todos os números Inteiros são Inteiros Algébricos. Também, vimos que, existem Inteiros Algébricos **Irracionais** e **Complexos**.

Nesse momento, vale a pena ressaltar que $\sqrt{3}$ é um número irracional, como demonstraremos a seguir. Para isso, antes precisamos do seguinte resultado.

Lema 2.1. . *Se p^2 é múltiplo de 3, então p é múltiplo de 3.*

Demonstração. Vamos provar, usando a contrapositiva, que se p **não** é múltiplo de 3, então p^2 **não** é múltiplo de 3 .

Note que p não múltiplo de 3, pelo Teorema 1.5, significa que $p = 3q + r$, onde $q \in \mathbb{Z}$ e $0 < r < 3$.

Daí,

$$\begin{array}{rcll} p^2 & = & (3q + r)^2 & \Rightarrow \\ p^2 & = & 9q^2 + 6qr + r^2 & \Rightarrow \\ p^2 & = & 3(3q^2 + 2qr) + r^2 & \Rightarrow \\ p^2 & = & 3q' + r^2 & \end{array}$$

onde $q' = (3q^2 + 2qr) \in \mathbb{Z}$.

Estudemos o resto r, $0 < r < 3$:

(i) $r = 1$

$$p^2 = 3q' + 1.$$

Logo, neste caso, p^2 não é múltiplo de 3.

(ii) $r = 2$

$$p^2 = 3q' + 4 \Rightarrow p^2 = 3q' + 3 + 1 \Rightarrow p^2 = 3q'' + 1$$

onde $q'' = (q' + 3) \in \mathbb{Z}$.

Também, neste caso, p^2 não é múltiplo de 3.

Portanto, por (i) e (ii), segue que p^2 não é múltiplo de 3. □

Observação 2.2. De modo geral, usando o Algoritmo da Divisão como acima, é possível mostrar que, se p^2 é múltiplo de c, então p também o é.

Lema 2.2. *$\sqrt{3}$ é um número irracional.*

Demonstração. Suponhamos por absurdo que $x = \sqrt{3}$ é um número racional. Logo, existem $p, q \in \mathbb{Z}$, com $q > 1$ e $(p, q) = 1$, tal que $x = \frac{p}{q}$.

Assim:

$$\begin{array}{rcll} x^2 & = & \left(\frac{p}{q}\right)^2 & \Rightarrow \\ (\sqrt{3})^2 & = & \left(\frac{p}{q}\right)^2 & \Rightarrow \\ 3 & = & \frac{p^2}{q^2} & \Rightarrow \\ 3q^2 & = & p^2. & \end{array} \tag{2.5}$$

De (2.5), segue que p^2 é múltiplo de 3. Logo, p é múltiplo de 3. Consequentemente, p pode ser escrito da forma $p = 3a$, para algum $a \in \mathbb{Z}$.

Substituindo $p = 3a$ em (2.5), temos,

$$\begin{array}{rcll} 3q^2 & = & 9a^2 & \Rightarrow \\ \frac{3q^2}{3} & = & \frac{9a^2}{3} & \Rightarrow \\ q^2 & = & 3a^2. & \end{array}$$

Logo, q^2 é múltiplo de 3, e assim, q é múltiplo de 3.

Portanto, p e q são múltiplos de 3, o que é absurdo, já que por hipótese p e q são primos entre si. □

O Teorema a seguir caracteriza os Inteiros Algébricos **Reais**.

Teorema 2.1. *Todo número inteiro algébrico real é um número inteiro ou irracional.*

Demonstração. Para provar que um inteiro algébrico não pode ser um número racional não inteiro, usaremos o tipo de demonstração indireta, a saber, redução ao absurdo. Suponha por absurdo, que o número racional $x = \frac{p}{q}$ $[(p, q \in \mathbb{Z})$, e $q > 1$ e $(p, q) = 1]$ satisfaça a equação do tipo (2.1), ou seja:

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

Então,

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

Considerando,

$$j = (-a_{n-1}p^{n-1} - ... - a_1pq^{n-2} - a_0q^{n-1}),$$

temos que $j \in \mathbb{Z}$ (pois vale a lei do fechamento, da adição e multiplicação em $\mathbb{Z}$) e que $p^n = qj$, ou seja, $q|p^n$

Agora, seja r um fator primo de q, $r \neq 1$ (observe que se q for primo podemos considerar $r = q$); então r divide p^n e pelo Corolário 1.1 isso implica que $r|p$.

Portanto obtemos que, $r|q$ e $r|p$, o que contradiz o fato de $(p, q) = 1$, (o absurdo ocorre quando admitimos $\frac{p}{q}$ como solução da equação do tipo (2.1)). □

Definição 2.1. ***(a)*** *Qualquer solução de uma equação polinomial da forma*

$$a_nx^n + a_{n-1}x^{n-1} + ... + a_1x + a_0 = 0,\ a_i \in \mathbb{Z},\ \textit{para todo } i \in \{0, ..., n\}$$

é chamado um ***número algébrico****. Ou seja, um número α é algébrico quando é possível encontrar uma equação polinomial com coeficientes inteiros, da qual α seja raiz.*

(b) *Um número que não é algébrico é denominado* ***transcendente****.*

Exemplo 2.2. :

1) Qualquer número racional $\alpha = \frac{p}{q}$, é algébrico porque α é a raiz da equação $qx - p = 0$.

2) Qualquer inteiro algébrico é um número algébrico.

No que segue, estamos interessados em mostrar a existência de números transcendentes. Para tal necessitamos de alguns conceitos.

Definição 2.2. *Um conjunto A é enumerável se seus elementos podem ser colocados em correspondência biunívoca com os números naturais. Mais precisamente, A é enumerável se existir uma função bijetiva, $f : \mathbb{N} \to A$.*

Exemplo 2.3. :

1) O conjunto dos números pares positivos é enumerável:
Seja $P = \{2n, n \in \mathbb{N}\}$, e considere a seguinte função

$$\begin{array}{rccc} f: & \mathbb{N} & \longrightarrow & P \\ & n & \longmapsto & 2n \end{array}$$

(i) f é injetora, pois:
Suponha que $f(x) = f(y)$. Queremos mostrar que $x = y$.
Como

$$f(x) = f(y) \Rightarrow 2x = 2y \Rightarrow x = y$$

Portanto f, é injetora.
(ii) f é sobrejetora, isto é $f(\mathbb{N}) = P$. De fato:
- $f(\mathbb{N}) \subset P$ pela definição de imagem.
-$P \subset f(\mathbb{N})$, pois seja $b \in P$, qualquer, então $b = 2n_0$ para algum $n_0 \in \mathbb{N}$. Tomando $x = n_0$, temos que $f(x) = f(n_0) = 2n_0 = b$, ou seja, $b \in f(\mathbb{N})$, logo $b = f(x)$.
Portanto f é sobrejetora.
Logo por (i) e (ii), f é bijetora.

2) O conjunto dos números ímpares positivos é enumerável. Basta considerar a função

$$f: N \longrightarrow I$$

$$n \longmapsto 2n - 1$$

onde $I = \{2n - 1, n \in N.\}$
A demontração pode ser feita de modo análogo ao exemplo (1).

3) O conjunto $\mathbb{Z}$ é enumerável. Observe a correspondência abaixo

$$\begin{array}{ccccccccc} ..., & -3, & -2, & -1, & 0, & 1, & 2, & 3, & ... \\ & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \\ ... & 7, & 5, & 3, & 1, & 2, & 4, & 6, & ... \end{array}$$

Esta correspondência pode ser descrita pela função definida por partes

$$\begin{array}{rccc} f: & \mathbb{Z} & \longrightarrow & \mathbb{N} \\ & n & \longmapsto & f(n) \end{array}$$

onde

$$f(n) = \begin{cases} 2n, & \text{se } n > 0 \\ -2n + 1, & \text{se } n \leq 0 \end{cases}$$

(i) f é injetora, isto é, $x \neq y \Rightarrow f(x) \neq f(y)$, pois:

- se $x, y > 0$, $f(x) = 2x \neq 2y = f(y)$

- se $x, y < 0$, $f(x) = -2x + 1 \neq -2y + 1 = f(y)$

- se $x > 0$ e $y < 0$, temos que $f(x) = 2x$ e$f(y) = -2y + 1$

daí, $f(x) = 2x \neq 2y \neq -2y \neq -2y + 1 = f(y)$;

-se $x < 0$ e $y > 0$, idem item anterior;

-se $x = 0$ e $y > 0$ (ou $y = 0$ e $x > 0$), então $f(x) = f(0) = 1$ e $f(y) = 2y$, daí $f(y) = 2y \neq 1 = f(0) = f(x)$

- se $x = 0$ e $y < 0$ (ou $y = 0$ e $x < 0$), então $f(x) = f(0) = 1$ e $f(y) = -2y + 1$, daí $f(y) = -2y + 1 \neq 1 = f(0) = f(x)$

Portanto, pelos casos considerados acima, f é injetora.

(ii) f é sobrejetora, isto é, $f(\mathbb{Z}) = \mathbb{N}$. De fato,

- $f(\mathbb{Z}) \subset \mathbb{N}$ pela definição de imagem;

- $\mathbb{N} \subset f(\mathbb{Z})$, pois:

seja $n \in \mathbb{N}$. Se n é **par**, então $n = 2k, k \in \mathbb{N}$. Logo, tomando $x = k$, temos que

$$n = 2k = f(k) = f(x) \in f(\mathbb{Z}).$$

Se n é **ímpar**, então $n = 2k + 1, k \in \mathbb{N}$, logo tomando $x = -k$, temos que

$$n = 2k + 1 = -2(-k) + 1 = f(-k) = f(x) \ \in f(\mathbb{Z}).$$

Portanto por (i) e (ii), segue que f é sobrejetora.

Logo por (i) e (ii), f é bijetora.

Como f é bijetora, existe $g^{-1} : \mathbb{N} \to \mathbb{Z}$, assim basta tomarmos $f = g^{-1}$

4) O conjunto dos números racionais é enumerável.

Mostremos primeiramente que o conjunto dos números racionais positivos é enumerável.

$$\begin{array}{ccccccccccc}
\frac{1}{1} & \to & \frac{1}{2} & & \frac{1}{3} & \to & \frac{1}{4} & & \frac{1}{5} & \to & \cdots \\
 & \swarrow & & \nearrow & & \swarrow & & \nearrow & & & \\
\frac{2}{1} & & \frac{2}{2} & & \frac{2}{3} & & \frac{2}{4} & & \frac{2}{5} & & \cdots \\
 & \nearrow & & \swarrow & & \nearrow & & \swarrow & & & \\
\frac{3}{1} & & \frac{3}{2} & & \frac{3}{3} & & \frac{3}{4} & & \frac{3}{5} & & \cdots \\
 & \swarrow & & \nearrow & & \swarrow & & \nearrow & & & \\
\frac{4}{1} & & \frac{4}{2} & & \frac{4}{3} & & \frac{4}{4} & & \frac{4}{5} & & \cdots \\
 & \nearrow & & \swarrow & & \nearrow & & \swarrow & & & \\
\frac{5}{1} & & \frac{5}{2} & & \frac{5}{3} & & \frac{5}{4} & & \frac{5}{5} & & \cdots \\
 & \swarrow & & & & & & & & & \\
\vdots & & \vdots & & \vdots & & \vdots & & \vdots & &
\end{array}$$

Observe que todos os números da forma $\frac{p}{q}$, com $p, q \in \mathbb{N}$ e $q \neq 0$ aparecem no quadro anterior. Se o percorrermos seguindo as flechas temos uma ordenação desse conjunto, a função f

$$\begin{array}{rccc} f: & \mathbb{N} & \longrightarrow & \mathbb{Q}^+ \\ & n & \longmapsto & f(n) \end{array}$$

é definida como $f(n) = n$-ésimo elemento que encontramos seguindo as flechas. Assim, mostramos que o conjunto $\mathbb{Q}^+ = \{x \in \mathbb{Q}, x > 0\}$ é enumerável.

A enumerabilidade de $\mathbb{Q}$ segue do item (i) do próximo Teorema, lembrando que $\mathbb{Q} = \mathbb{Q}^+ \cup \mathbb{Q}^- \cup \{0\}$, onde $\mathbb{Q}^- = \{x \in \mathbb{Q} : x < 0\}$.

A seguir demonstramos algumas propriedades sobre conjuntos enumeráveis.

Teorema 2.2. ***(i)*** *A união de um conjunto finito e um conjunto enumerável é enumerável;*

(ii) *A união de dois conjuntos enumeráveis é enumerável;*

(iii) *A união de um número finito de conjuntos enumeráveis é enumerável;*

(iv) *A união de um conjunto enumerável de conjuntos finitos é enumerável;*

(v) *A união de um conjunto enumerável de conjuntos enumeráveis é enumerável.*

Demonstração. **(i)** Seja $A = \{a_1, a_2, ..., a_n\}$ conjunto finito e $B = \{b_1, b_2, ...\}$ o conjunto enumerável. O conjunto $A \cup B$ é enumerável.

De fato a correspondência biunívoca entre $A \cup B$ e $\mathbb{N}$ será assim:

$$\begin{array}{ccccccc} a_1, & ..., & a_n, & b_1, & b_2, & ... \\ \updownarrow & & \updownarrow & \updownarrow & \updownarrow & \\ 1 & & n & n+1 & n+2 & \end{array}$$

(ii) Sejam $A = \{a_1, a_2, ...\}$ e $B = \{b_1, b_2, ...\}$, dois conjuntos enumeráveis, então $A \cup B$ é enumerável, já que possui a seguinte correspondência biunívoca,

$$\begin{array}{ccccc} a_1, & b_1, & a_2, & b_2, & a_3 \\ \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow \\ 1 & 2 & 3 & 4 & 5 \end{array}$$

(iii) Sejam $A_1, A_2, ..., A_n$ conjuntos enumeráveis, queremos mostrar que $A_1 \cup A_2 \cup ... \cup A_n$, é enumerável, $\forall\ n \in \mathbb{N}$.

Para isso usamos o Princípio de Indução Finita.

(a) $k = 1$ é válida pois A_1 é enumerável.

(b) $k = 2$ é válida pelo item (ii).

Hipótese de Indução: Suponha que seja válida para k, ou seja, se $A_1, A_2, ..., A_k$ são enumeráveis então $A_1 \cup ... \cup A_k$ é enumerável.

Provemos então que a propriedade é válida para $k + 1$.

Ou seja, se $A_1, ..., A_k, A_{k+1}$ são enumeráveis, então

$$A_1 \cup A_2 \cup ... \cup A_k \cup A_{k+1}$$

é enumerável.

Note que

$$A_1 \cup A_2 \cup ... \cup A_k \cup A_{k+1} = (A_1 \cup ... \cup A_k) \cup A_{k+1}$$

Considere $A = (A_1 \cup ... \cup A_k)$, então

$$A_1 \cup A_2 \cup ... \cup A_k \cup A_{k+1} = A \cup A_{k+1}.$$

Agora A é enumerável por Hipótese de Indução e $A \cup A_{k+1}$ é enumerável por (ii).

Portanto $A_1 \cup ... \cup A_k \cup A_{k+1}$ é enumerável. Logo pelo Princípio de Indução Finita, (iii) é válida.

(iv) Seja $\{A_1, A_2, ..., A_n, ...\}$ um conjunto enumerável onde cada A_i é um conjunto finito, para qualquer $i \in \{1, ..., n, ...\}$.

Queremos mostrar que $A_1 \cup A_2 \cup ... \cup A_n \cup ...$ é enumerável.

Suponha que $A_1 = \{a_{11}, a_{12}, ..., a_{1l_1}\}$, $A_2 = \{a_{21}, a_{22}, ..., a_{2l_2}\}$, ..., $A_n = \{a_{n1}, a_{n2}, ..., a_{nl_n}\}$

Então,

$$A_1 \cup A_2 \cup ... \cup A_n \cup ... = \{a_{11}, a_{12}, ..., a_{1l_1}, a_{21}, a_{22}, ..., a_{2l_2}, a_{n1}, a_{n2}, ..., a_{nl_n}, ...\}$$

Defina a seguinte correspondência entre $A_1 \cup A_2 \cup ... \cup A_n \cup ... \subset \mathbb{N}$.

$$\begin{array}{ccccccccccccc} a_{11}, & ..., & a_{1l_1}, & a_{21}, & ..., & a_{2l_2}, & ..., & a_{n1}, & ..., & a_{nl_n}, & ... \\ \updownarrow & & \updownarrow & \updownarrow & & \updownarrow & & \updownarrow & & \updownarrow & \\ 1, & ..., & l_1, & l_1+1, & ..., & l_1+l_2, & ..., & l_1+...+l_{n-1}+1, & ..., & l_1+...+l_{n-1}+l_n, & ... \end{array}$$

Logo, $A_1 \cup A_2 \cup ... \cup A_n \cup ...$ é enumerável.

(v) Seja $\{A_1, A_2, ..., A_n, ...\}$ um conjunto enumerável onde cada A_i é um conjunto enumerável para qualquer $i \in \{1, .., n, ...\}$.

Suponha que

$$A_1 = \{a_{11}, a_{12}, a_{13}, ...\}$$

$$A_2 = \{a_{21}, a_{22}, a_{23}, ...\}$$

$$\vdots$$

$$A_n = \{a_{n1}, a_{n2}, a_{n3}, ...\}$$

Disponha os elementos de $A_1, A_2, ..., A_n$ como a tabela

$$\begin{array}{cccc} a_{11}, & a_{12}, & a_{13}, & ... \\ a_{21}, & a_{22}, & a_{23}, & ... \\ \vdots & \vdots & \vdots & \\ a_{n1}, & a_{n2}, & a_{n3}, & ... \\ . & . & . & \\ . & . & . & \\ . & . & . & \end{array}$$

Formando flechas como feito em $\mathbb{Q}^+$ definimos f dada por $f(n) = n$-ésimo elemento que encontramos seguindo as flechas. Dessa forma definimos uma correspondência biunívoca entre $A_1 \cup A_2 \cup ... \cup A_n \cup ...$ e consequentemente provamos que é um conjunto enumerável. □

Observação 2.3. Se A é enumerável e $B \subset A$ é um conjunto infinito, então B também é enumerável, pois como A é enumerável existe uma correspondência biunívoca, f, entre $\mathbb{N}$ e A, então basta considerar a restrição $f|_B : B \to \mathbb{N}$.

Teorema 2.3. *O conjunto $\mathbb{R}$ dos números reais não é enumerável.*

Demonstração. Demonstramos que o conjunto dos números reais $x \in [0, 1)$, não é enumerável, em virtude da observação acima segue que $\mathbb{R}$ também não é enumerável. Façamos isso, primeiro note que os números $x \in [0, 1)$ tem uma representação decimal da forma

$$0,\ a_1\ a_2\ a_3... \tag{2.6}$$

onde a_j é um dos algarismos $0, 1, 2, 3, 4, 5, 6, 7, 8$ ou 9. Alguns números tem duas representações da forma (2.6), por exemplo, $\frac{1}{2}$ é igual $0,50...$ ou $0,499...$

Para tais números, escolhemos a representação decimal que termina. Em outras palavras, eliminamos as decimais (2.6) que a partir de uma certa ordem todos os elementos são 9. Suponhamos que as decimais tipo (2.6), ou que os números reais no intervalo $[0, 1)$, formam um conjunto enumerável.

$$\begin{array}{ccccc} 0 & a_{11} & a_{12} & a_{13} & ... \\ 0 & a_{21} & a_{22} & a_{23} & ... \\ 0 & a_{31} & a_{32} & a_{33} & ... \\ & & \vdots & & ... \end{array} \tag{2.7}$$

Agora forme o decimal $0, b_1 b_2 b_3...$ do seguinte modo: todos os b_i's são diferentes de 0 ou 9 e $b_1 \neq a_{11}$, $b_2 \neq a_{22}$. É claro que $0, b_1 b_2 b_3 \ldots \neq 0, a_{n1} a_{n2} a_{n3} \ldots$, para todo n, pois $b_n \neq a_{nn}$. Logo $0, b_1 b_2 b_3 \ldots$ não está na tabela (2.7) o que é um absurdo, já que é um número real entre 0 e 1. □

Com os resultados anteriores provamos a existência de números transcedentes no seguinte teorema.

Teorema 2.4. *Existem números transcendentes.*

Demonstração. Dado um polinômio com coeficientes inteiros,

$$P(x) = a_n x^n + ... + a_1 x + a_0 \tag{2.8}$$

Definimos sua altura como sendo o número natural

$$|P| = |a_n| + ... + |a_1| + |a_0| + n \tag{2.9}$$

O Teorema Fundamental da Álgebra nos diz que $P(x) = 0$, tem exatamente n raízes complexas. Todas, algumas ou nenhuma delas podem ser reais. Agora o número de polinômios do tipo (2.8) com uma dada altura é apenas um número finito (observe que é para essa afirmação que incluímos a parcela n na definição da altura em (2.9)).

Logo, as raízes de todos os polinômios de uma dada altura formam um conjunto finito, consequentemente o conjunto de todas as raízes de todos os polinômios de todas as alturas formam um conjunto enumerável de conjuntos finitos. (Por exemplo, se $P(x) = 3x^4 - x^3 + x - 5$, então $|P| = |3| + |-1| + |0| + |1| + |-5| + 4$ e pelo Teorema Fundamental da Álgebra $P(x)$ possui quatro raízes complexas). Portanto, podemos concluir que o conjunto dos números algébricos reais é enumerável. Agora, o conjunto dos números reais pode ser considerado como a união do conjunto dos números algébricos reais com o conjunto dos números não-algébricos reais, ou seja, o conjunto dos números reais pode ser considerado como a união do conjunto dos números algébricos reais com o conjunto dos números transcendentes reais. Assim, como o conjunto $\mathbb{R}$ não é enumerável, o conjunto dos transcendentes reais deve ser não enumerável, já que, caso contrário, pelo item (ii) do Teorema 2.2, $\mathbb{R}$ seria enumerável. Consequentemente, existe um conjunto infinito não enumerável de números reais transcendentes. □

Exemplo 2.4. O número

$$\beta = \sum_{j=1}^{\infty} 10^{-j!} = 0,110001000\cdots$$

é transcendental. (Este era um dos números usados por Liouville em 1851 na primeira prova da existência de números transcendentais.)

Demonstração. Suponha que β é algébrico, para que ele satisfaça qualquer equação

$$f(x) = \sum_{j=0}^{n} c_j x^j = 0$$

com coeficientes inteiros. Para qualquer x satisfazendo $0 < x < 1$, temos que, pela desigualdade triangular

$$|f'(x)| = \left| \sum_{j=1}^{n} j c_j x^{j-1} \right| < \sum |j c_j| = C,$$

onde a constante C, definida na equação anterior, depende somente dos coeficientes de $f(x)$. Definimos $\beta_k = \sum_{j=1}^{k} 10^{-j!}$ a fim de que

$$\beta - \beta_k = \sum_{j=k+1}^{\infty} 10^{-j!} < 2 \cdot 10^{-(k+1)!}.$$

Pelo teorema do valor médio,

$$|f(\beta) - f(\beta_k)| = |\beta - \beta_k| \cdot |f'(\theta)|$$

para algum θ entre β e β_k. Conseguimos uma contradição provando que o lado direito é menor que o esquerdo, se k é escolhido suficientemente grande. O lado direito é menor que $2C/10^{(k+1)!}$. Desde que $f(x)$ tenha somente n zeros, podemos tomar k suficientemente grande de modo que $f(\beta_k) \neq 0$. Usando $f(\beta) = 0$ vemos que

$$|f(\beta) - f(\beta_k)| = |f(\beta_k)| = \left| \sum_{j=0}^{n} c_j \beta_k^j \right| \geq \frac{1}{10^{n.k!}},$$

pois $c_j \beta_k^j$ é um número racional com denominador $10^{n.k!}$. Finalmente observamos que $1/10^{n.k!} > 2C/10^{(k+1)!}$ se k é suficientemente grande. □

3 O número π é irracional

O objetivo dessa seção é demonstrar que o número π é irracional, para isso consideremos a função,

$$f(x) = \frac{x^n(1-x)^n}{n!} \tag{3.1}$$

onde n é um numero inteiro positivo.

Lema 3.1. *$D^k f(0)$ é um número inteiro para qualquer $k = 0, 1, 2...$, onde D^k representa a $k-$ésima derivada de f e $D^0 f = f$.*

Demonstração. Vamos utilizar a chamada fórmula de Leibnitz para as derivadas de um produto de duas funções g e h,

$$D^k(gh) = \sum_{j=0}^{k} \binom{k}{j} D^j g D^{(k-j)} h. \tag{3.2}$$

Note que a função (3.1) pode ser escrita como o produto das funções $g(x) = \frac{1}{n!}x^n$ e $h(x) = (1-x)^n$.

Logo aplicando (3.2), temos:

$$D^k f = \frac{1}{n!} \sum_{j=0}^{k} \binom{k}{j} D^j x^n D^{(k-j)}(1-x)^n. \tag{3.3}$$

Agora observe que:

$$D^j x^n|_{x=0} = \begin{cases} 0, & \text{se } j < n \\ n!, & \text{se } j = n \\ 0, & \text{se } j > n \end{cases} \tag{3.4}$$

Substituindo (3.4) em (3.3) segue que

$$D^k f(0) = 0 \text{ se } k < n.$$

e que

$$D^k f(0) = \frac{1}{n!}\binom{k}{n} n! D^{(k-n)}(1-x)^n|_{x=0} = \binom{k}{n} D^{(k-n)}(1-0)^n = \binom{k}{n}, \tag{3.5}$$

se $k \geq n$.

Como os coeficientes binomiais são inteiros segue que expressão no segundo membro de (3.5) é um inteiro. Portanto, como $D^k f(0) = 0$ para $k < n$ e $D^k f(0) = \binom{k}{n}$, para $k \geq n$, segue que $D^k f(0)$ tem número inteiro para qualquer $k = 0, 1, 2, ...$ □

Lema 3.2. *$D^k f(1)$ é um número inteiro para qualquer $k = 0, 1, 2, ...$*

Demonstração. Segue diretamente do lema anterior e da observação de que:

$$f(1-x) = f(x)$$

pois,

$$f(1-x) = \frac{(1-x)^n(1-(1-x))^n}{n!} = \frac{(1-x)^n x^n}{n!} = \frac{x^n(1-x)^n}{n!} = f(x)$$

De fato, como $D^k f(1-x) = D^k f(x)$, temos para $x = 0$, que

$$D^k f(1) = D^k f(0).$$

Como $D^k f(0)$ é um número inteiro segue que $D^k f(1)$ também o é. □

Teorema 3.1. *π é um número irracional.*

Demonstração. Suponha que $\pi^2 = \frac{p}{q}$, onde $\frac{p}{q}$ é uma fração irredutível. Com essa suposição queremos encontrar um absurdo, mostrando assim que π^2 não é racional e consequentemente, π não é racional, pois o quadrado de um número racional necessariamente é racional.

Para isso, defina a função:

$$F(x) = q^n\{\pi^{2n} f(x) - \pi^{(2n-2)} D^2 f(x) + ... + (-1)^n D^{2n} f(x)\},$$

onde $f(x) = \dfrac{x^n(1-x)^n}{n!}$.

Como consequência dos lemas 3.1 e 3.2, e da hipótese $\pi^2 = \frac{p}{q}$, temos que $F(0)$ e $F(1)$ são números inteiros pois:

$$\begin{aligned} F(0) &= q^n\{\left(\tfrac{p}{q}\right)^n f(0) - \left(\tfrac{p}{q}\right)^{(n-1)} D^2 f(0) + ... + (-1)^n D^{2n} f(0)\} = \\ &= -q^n \frac{p^{(n-1)}}{q^{(n-1)}} D^2 f(0) + ... + (-1)^n q^n D^{2n} f(0) = \\ &= qp^{(n-1)} D^2 f(0) + ... + (-1)^n q^n D^{2n} f(0) \end{aligned}$$

e

$$F(1) = -qp^{(n-1)}D^2f(1) + ... + (-1)^n q^n D^{2n} f(1).$$

Agora observe que,

$$\{F'(x)\operatorname{sen}\pi x - \pi F(x)\cos\pi x\}' =$$
$$F''(x)\operatorname{sen}\pi x + \pi^2 F(x)\operatorname{sen}\pi x.$$

Pois,

$$\begin{aligned} \{F'(x)\operatorname{sen}\pi x - \pi F(x)\cos\pi x\}' &= \\ F''(x)\operatorname{sen}\pi x + F'(x)\cos\pi x\pi - \pi[F'(x)\cos\pi x - F(x)\operatorname{sen}\pi x\pi] &= \\ F''(x)\operatorname{sen}\pi x + F'(x)\cos\pi x\pi - \pi F'(x)\cos\pi x + F(x)\operatorname{sen}\pi x\pi^2 &= \\ F''(x)\operatorname{sen}\pi x + \pi^2 F(x)\operatorname{sen}\pi x. \end{aligned}$$

Daí

$$\{F'(x)\operatorname{sen}\pi x - \pi F(x)\cos\pi x\}' = \tag{3.6}$$

$$p^n\pi^2 f(x)\operatorname{sen}\pi x.$$

Agora, aplicamos o teorema fundamental do cálculo integral ["Se $g : [0,1] \to \mathbb{R}$ é uma função contínua em $[0,1]$ e derivável em $(0,1)$, então $\int_0^1 g'(x)dx = g(1) - g(0)$"]. Obtemos para função $g(x) = F'(x)\operatorname{sen}\pi x - \pi F(x)\cos\pi x$. Em virtude de (3.6) obtemos que

$$p^n\pi^2\int_0^1 f(x)\operatorname{sen}\pi x dx = \pi F(1) + \pi F(0),$$

ou seja,

$$\pi p^n\int_0^1 f(x)\operatorname{sen}\pi dx = F(1) + F(0). \tag{3.7}$$

Note que como $F(1)$ e $F(0)$ são números inteiros e o conjunto dos números inteiros é fechado quanto a adição, o lado direito de (3.7) é inteiro. Portanto se mostrarmos que para $n \in N$ conveniente, o lado esquerdo de (3.7) é um número positivo estritamente menor que 1, temos o absurdo procurado. Já que assim temos $0 < F(1) + F(0) < 1$.

Façamos isso, veja que para $0 < x < 1$, temos (lembre-se $f(x)$ é dado em (3.1))

$$0 < f(x) < \frac{1}{n!}. \tag{3.8}$$

Usando a desigualdade (3.8) em (3.7):

$$0 < \pi p^n\int_0^1 f(x)\operatorname{sen}\pi x dx < \pi p^n\int_0^1 \frac{1}{n!}\operatorname{sen}\pi x dx.$$

Mas,

$$\pi p^n \int_0^1 \frac{1}{n!} \operatorname{sen} \pi x dx = \frac{\pi p^n}{n!} \int_0^1 \operatorname{sen} \pi x dx.$$

Com a mudança de variável,

$$u = g(x) = \pi x$$

$$g'(x) = \pi.$$

Temos que

$$\pi p^n \frac{1}{\pi n!} \int_0^\pi \operatorname{sen} u du =$$

$$\frac{p^n}{n!}[-\cos u]|_0^\pi$$

$$\frac{p^n}{n!}[-(\cos \pi) - (-\cos 0)] = \frac{p^n}{n!}[-(-1) + 1] = \frac{2p^n}{n!}.$$

Portanto

$$0 < \pi p^n \int_0^1 f(x) \operatorname{sen} \pi x dx < \frac{2p^n}{n!}.$$

Como $\lim_{n\to\infty} \frac{p^n}{n!} = 0$, temos que $\lim_{n\to\infty} \frac{2p^n}{n!} = 0$, logo podemos encontrar um $n \in \mathbb{N}$ suficientemente grande, tal que $\frac{2p^n}{n!} < 1$.

Ou seja, π é um número irracional. □

No próximo capítulo tratamos da transcendência deste número.

4 O número π é transcendente.

Para mostrar a transcendência de π precisamos de determinados resultados sobre Análise Complexa.

O primeiro trata-se do Teorema da Desigualdade do Valor Médio, para isso exploramos o Teorema do Valor Médio para números reais, a saber, seja $f : [a, b] \to \mathbb{R}$ uma função real contínua definida em um intervalo fechado $[a, b]$, $a, b \in \mathbb{R}$. Suponha que a derivada $f'(x)$ existe para todo x no intervalo aberto (a, b). Então existe λ com $0 < \lambda < 1$ tal que

$$f(b) - f(a) = (b - a)f'(a + \lambda(b - a)).$$

Para obter um teorema de valor médio para funções complexas, utilizaremos algo sobre funções de duas variáveis. Representamos por $\mathbb{C}$ o conjunto dos números complexos, isto é, números da forma $z = x + iy$, onde $x, y \in \mathbb{R}$. Uma função $f : \mathbb{C} \to \mathbb{C}$ tem derivada no ponto z se o limite abaixo existe

$$f'(z) = \lim_{z_0 \to 0} \frac{f(z + z_0) - f(z)}{z_0} \tag{4.1}$$

onde $z_0 \in \mathbb{C}$, e $f'(z)$ é chamada a derivada de f no ponto z. Se uma função f tiver derivadas em todos os pontos de $\mathbb{C}$, então dizemos que ela é analítica em $\mathbb{C}$. Sejam $u(x, y)$ e $v(x, y)$ as partes real e imaginária de $f(z)$, isto é,

$$f(z) = u(x, y) + iv(x, y), \text{ em que } z = x + iy. \tag{4.2}$$

Suponhamos que $f(z)$ seja analítica em $\mathbb{C}$ e calculemos a derivada (4.1) usando valores reais para z_0, $z_0 = h$

$$f'(z) = \lim_{h \to 0} \frac{u(x + h, y) - u(x, y)}{h} + i \lim_{h \to 0} \frac{v(x + h, y) - v(x, y)}{h}$$

ou seja

$$f'(z) = u_x(x, y) + iv_x(x, y). \tag{4.3}$$

(u_x representa a derivada de $u(x, y)$ com relação a primeira variável, e u_y com relação a segunda).

A seguir calculemos a derivada (4.1) usando valores imaginários puros para z_0, $z_0 = ik$:

$$f'(z) = \lim_{k\to 0} \frac{u(x, y+k) - u(x,y)}{ik} + i \lim_{k\to 0} \frac{v(x, y+k) - v(x,y)}{ik}$$

ou seja

$$f'(z) = -iu_y(x,y) + v_y(x,y). \tag{4.4}$$

Identificando (4.3) e (4.4)obtemos as equações de $Cauchy - Riemann$

$$u_x(x,y) = v_y(x,y), u_y(x,y) = -v_x(x,y),$$

para qualquer $z = x + iy$ em $\mathbb{C}$.

Resumindo-se: se f for analítica em $\mathbb{C}$, então as equações de Cauchy-Riemann valem em qualquer ponto de $\mathbb{C}$. Se $f : \mathbb{C} \to \mathbb{C}$ for uma função analítica em $\mathbb{C}$ e se z_2 e z_1 forem números complexos, não é verdade, em geral, que exista λ, $0 < \lambda < 1$, tal que

$$f(z_2) - f(z_1) = (z_2 - z_1)f'(z_1 + \lambda(z_2 - z_1)). \tag{4.5}$$

Como podemos ver através de um contra-exemplo. Seja $P(z) = (z^2 - 2z + 2)(z^2 + 2z + 2)$ cujas raízes são $z_1 = 1 + i$, $z_2 = 1 - i$, $z_3 = -1 + i$, $z_4 = -1 - i$; aplicando (4.5) aos pares de pontos (z_1, z_2), (z_2, z_3), (z_3, z_4), (z_4, z_1), concluímos que $P'(z)$ teria 4 raízes distintas. Isso, porém, contraria o teorema fundamental da álgebra que diz que um polinômio de grau 3 tem exatamente 3 raízes complexas. Portanto, temos de abrir mão da igualdade no teorema do valor médio, e assim teremos:

Teorema 4.1. *Seja $f : \mathbb{C} \to \mathbb{C}$ uma função analítica e sejam $z_1, z_2 \in \mathbb{C}$. Então*

$$|f(z_2) - f(z_1)| \leq 2|z_2 - z_1| sup\{|f'(z_1 + \lambda(z_2 - z_1))| : 0 \leq \lambda \leq 1\} \tag{4.6}$$

onde $|z|$ representa o módulo do complexo $z = x + iy$, isto é, $|z| = +\sqrt{x^2 + y^2}$.

Demonstração. Primeiramente, demostraremos que

$$|f(z_0) - f(0)| \leq 2|z_0| sup\{|f'(\lambda z_0)| : 0 \leq \lambda \leq 1\} \tag{4.7}$$

Isso feito, (4.6) segue-se facilmente pela aplicação de (4.7) à função $g(z) = f(z + z_1)$ e ao ponto $z_0 = z_2 - z_1$. Sejam u e v as partes real e imaginária de $f(z)$. Dado $z_0 = x_0 + iy_0$, defina as funções $\phi : \mathbb{R} \to \mathbb{R}$ e $\psi : \mathbb{R} \to \mathbb{R}$ pelas expressões

$$\phi(\lambda) = u(\lambda x_0, \lambda y_0),$$

$$\psi(\lambda) = v(\lambda x_0, \lambda y_0).$$

Aplicando o teorema do valor médio às funções reais ϕ e ψ obtemos

$$\phi(1) - \phi(0) = \phi'(\lambda_1),\ 0 < \lambda_1 < 1, \tag{4.8}$$

$$\psi(1) - \psi(0) = \psi'(\lambda_2),\ 0 < \lambda_2 < 1. \tag{4.9}$$

Para calcular as derivadas de ϕ e ψ, usamos o teorema de derivação das funções compostas e obtemos de (4.8) e (4.9)

$$u(x_0, y_0) - u(0,0) = u_x(\lambda_1 x_0, \lambda_1 y_0)x_0 + u_y(\lambda_1 x_0, \lambda_1 y_0)y_0,$$

$$v(x_0, y_0) - v(0,0) = v_x(\lambda_2 x_0, \lambda_2 y_0)x_0 + v_y(\lambda_2 x_0, \lambda_2 y_0)y_0,$$

e daí

$$f(z_0)-f(0) = u_x(\lambda_1 x_0, \lambda_1 y_0)x_0+u_y(\lambda_1 x_0, \lambda_1 y_0)y_0+i\{v_x(\lambda_2 x_0, \lambda_2 y_0)x_0+v_y(\lambda_2 x_0, \lambda_2 y_0)y_0\}. \tag{4.10}$$

Agora usaremos a desigualdade

$$|z| \leq |x| + |y|,$$

da qual segue que o módulo de um número complexo $z = x + iy$ é menor ou igual que a soma dos valores absolutos de sua parte real e imaginária, bem como a desigualdade de Cauchy-Schwarz

$$|a_1 b_1 + a_2 b_2| \leq \sqrt{a_1^2 + a_2^2}\sqrt{b_1^2 + b_2^2},$$

onde a_1, a_2, b_1, b_2 são números reais quaisquer. Utilizando essas duas desigualdades em (4.10) obtemos

$$|f(z_0) - f(0)| \leq \sqrt{u_x^2(\lambda_1 x_0, \lambda_1 y_0) + u_y^2(\lambda_1 x_0, \lambda_1 y_0)}\sqrt{x_0^2 + y_0^2} \tag{4.11}$$

$$+\sqrt{v_x^2(\lambda_2 x_0, \lambda_2 y_0) + v_y^2(\lambda_2 x_0, \lambda_2 y_0)}\sqrt{x_0^2 + y_0^2}.$$

Em virtude de (4.4) e (4.5) e das equações de Cauchy-Riemann, os radicais em (4.11), envolvendo u e v são precisamente o módulo de f' calculado em certos pontos, isto é,

$$|f(z_0) - f(0)| \leq |f'(\lambda_1 z_0)||z_0| + |f'(\lambda_2 z_0)||z_0|,$$

de onde segue (4.7) imediatamente. E, assim, o teorema 4.1 fica demonstrado. □

Agora sim estamos preparados para demonstrar a transcendência de π. Para tanto, suponhamos por absurdo que π seja um número algébrico.

Logo, $i\pi$ onde $i = \sqrt{-1}$ seria também algébrico como um produto de dois números algébricos. Então $i\pi$ seria raiz de uma equação polinomial com coeficientes inteiros:

$$P_1(x) = 0. \tag{4.12}$$

Representemos as raízes de (4.12) por $\alpha_1 = i\pi$, $\alpha_2, ..., \alpha_n$. Como $e^{i\pi} = -1$, segue que

$$\prod_{j=1}^{n}(1 + e^{\alpha_j}) = 0. \tag{4.13}$$

Se desenvolvermos o produto indicado em (4.13), obteremos uma expressão da forma: 1 + somatório de exponenciais cujos expoentes são:

$$\alpha_1, \alpha_2, ..., \alpha_n \tag{4.14}$$

$$\alpha_i + \alpha_j, \quad \text{para todos} \quad i < j \tag{4.15}$$

$$\alpha_i + \alpha_j + \alpha_k, \quad \text{para todos} \quad i < j < k \tag{4.16}$$

$$\vdots$$

$$\alpha_1 + ... + \alpha_n. \tag{4.17}$$

Observemos que o número de termos em (4.14) é n, em (4.15) é $\binom{n}{2}$, em (4.16) é $\binom{n}{3}$, ..., em (4.17) é $\binom{n}{n} = 1$, em que $\binom{n}{m}$ são os coeficientes binomiais, isto é, $\binom{n}{m} = \dfrac{n!}{m!(n-m)!}$ para $0 \leq m \leq n$.

Agora, do fato de $\alpha_1 + ... + \alpha_n$ satisfazerem uma equação polinomial de grau n com coeficientes inteiros, segue-se (e isso será demonstrado no Apêndice a esse capítulo) que: (a) os números em (4.15) satisfazem uma equação polinomial de grau $\binom{n}{2}$ com coeficientes inteiros

$$P_2(x) = 0; \tag{4.18}$$

(b) os números em (4.16) satisfazem uma equação polinomial de grau $\binom{n}{3}$ com coeficientes inteiros

$$P_3(x) = 0,$$

e assim sucessivamente.

Logo os números em (4.14) ... (4.17) satisfazem a equação polinomial

$$P_1(x)...P_n(x) = 0 \tag{4.19}$$

com coeficientes inteiros e cujo grau é $n + \binom{n}{2} + ... + \binom{n}{n} = 2^n - 1$. Como alguns dos números em (4.14) ... (4.17) podem se anular, podemos supor que m deles sejam diferentes de zero e representemo-los por $\beta_1, ..., \beta_m$. Logo, simplificando de (4.19) os fatores da forma x^q, para $q > 0$, caso haja, (e haverá se $2^n - 1 > m$), obtemos que $\beta_1, ..., \beta_m$ são raízes de uma equação na forma

$$R(x) = cx^m + c_{m-1}x^{m-1} + ... + c_1x + c_0 = 0, \tag{4.20}$$

com coeficientes inteiros.

A seguir, efetuamos o produto de (4.13) e obtemos

$$k + e^{\beta_1} + ... + e^{\beta_m} = 0. \tag{4.21}$$

Considere o polinômio

$$P(x) = \frac{c^s}{(p-1)!} x^{p-1} (R(x))^p, \tag{4.22}$$

onde $s = mp - 1$ e p é um número primo a ser escolhido posteriormente. O grau de P é $r = s + p$. Seja agora

$$F(x) = P(x) + P'(x) + ... + P^{(s+p)}(x). \tag{4.23}$$

Segue que

$$\frac{d}{dx}(e^{-x} F(x)) = -e^{-x} P(x). \tag{4.24}$$

Aplicando o Teorema 4.1 à função $f(z) = e^{-z} F(z)$, temos

$$|e^{-\beta_j} F(\beta_j) - F(0)| \leq 2|\beta_j| \ sup\{|e^{-\lambda \beta_j} P(\lambda \beta_j)| : \ 0 \leq \lambda \leq 1\}, \tag{4.25}$$

para $j = 1, ..., m$. Fazendo

$$\varepsilon_j = 2|\beta_j| \ sup\{|e^{(1-\lambda)\beta_j} P(\lambda \beta_j)| : \ 0 \leq \lambda \leq 1\}, \tag{4.26}$$

obtemos de (4.25) que

$$|F(\beta_j) - e^{\beta_j} F(0)| \leq \varepsilon_j. \tag{4.27}$$

Usando (4.21) e a expressão (4.27) para $j = 1, ..., m$ obtemos

$$|kF(0) + \sum_{j=1}^{m} F(\beta_j)| \ \leq \ \sum_{j=1}^{m} \varepsilon_j. \tag{4.28}$$

Mostraremos, agora, que o lado esquerdo de (4.28) é um inteiro não nulo, e que o lado direito, para p conveniente, é menor que 1.

Devemos, então, calcular as várias derivadas de $P(x)$ nos pontos $0, \beta_1, ..., \beta_m$. O polinômio $P(x)$ definido em (4.22) é da forma

$$P(x) = \frac{c^s}{(p-1)!} \{c_0^p x^{p-1} + b x^p + ...\}.$$

Logo,

$$P^{(i)}(0) = 0, \quad para \quad i < p-1, \quad e \quad P^{(p-1)}(0) = c^s c_0^p. \tag{4.29}$$

Por outro lado, segue-se diretamente de (4.22) que

$$P^{(i)}(\beta_j) = 0, \quad i < p, \quad j = 1, ..., m, \tag{4.30}$$

uma vez que nas derivadas $P^{(i)}(x)$, para i, p, a expressão $R(x)$ é fator comum, e $R(\beta_j) = 0$.

Para as derivadas de ordem $i \geq p$, e de (4.22), concluímos que os coeficientes de

$$P^{(i)}(x), \ i \geq p, \tag{4.31}$$

são inteiros divisíveis por pc^s.

Logo, de (4.29) e (4.31) obtemos

$$F(0) = c^s c_0^p + pc^s k_0, \tag{4.32}$$

onde k_0 é um inteiro, cujo valor não importa para os nossos propósitos. Para os demais $F(\beta_j)$ observamos que

$$\sum_{j=1}^{m} F(\beta_j) = \sum_{j=1}^{m} \sum_{i \geq p} P^{(i)}(\beta_j) = \sum_{i \geq p} \sum_{j=1}^{m} P^{(i)}(\beta_j). \tag{4.33}$$

Agora, na expressão

$$\sum_{j=1}^{m} P^{(i)}(\beta_j) \tag{4.34}$$

para cada i fixado, com $p \leq i \leq s + p$. Por (4.31) o polinômio $P^{(i)}$ tem coeficientes inteiros divisíveis por pc^s. Além disso, como P tem grau $s + p$, segue-se que $P^{(i)}$ tem grau $s + p - i \leq s$, pois $p \leq i$. Logo, a expressão (4.34) pode ser escrita como

$$\sum_{j=1}^{m} P^{(i)}(\beta_j) = pc^s Q(\beta_1, ..., \beta_m), \tag{4.35}$$

onde $Q(\beta_1, ..., \beta_m)$ é um polinômio nos $\beta_i's$ de grau menor ou igual a s, com coeficientes inteiros. Veja ainda que $Q(\beta_1, ..., \beta_m)$ é um polinômio simétrico nos $\beta_i's$ com coeficientes inteiros. Logo, pelo Teorema "A"do Apêndice, existe um polinômio $G(\sigma_1, ..., \sigma_m)$ de grau menor ou igual a s com coeficientes inteiros e onde $\sigma_1, ..., \sigma_m$ são os polinômios simétricos elementares em $\beta_1, ..., \beta_m$, tal que

$$Q(\beta_1, ..., \beta_m) = G(\sigma_1, ..., \sigma_m). \tag{4.36}$$

Por outro lado, temos

$$\sigma_1 = c^{-1} c_{m-1}, \quad \sigma_2 = c^{-1} c_{m-2}, ..., \quad \sigma_m = c^{-1} c_0. \tag{4.37}$$

Logo, de (4.35), (4.36) e (4.37) segue que a expressão (4.34)é um inteiro divisível por p. Voltando a (4.33) concluimos que

$$\sum_{j=1}^{m} F(\beta_j) = pK_1, \tag{4.38}$$

onde K_1 é um inteiro cujo valor é irrelevante para nossos propósitos. A seguir, usando (4.32) e (4.38) obtemos que o lado esquerdo de (4.28) é um inteiro da forma

$$|kc^s c_0^p + pK|, \tag{4.39}$$

onde $K = c^s k_0 + K_1 l$. Agora escolhemos um número primo p de modo que ele seja maior que k, c e c_0. Portanto, o inteiro (4.39) não é divisível por p, e, consequentemente, é um inteiro não nulo.

Para concluir a demonstração, necessitamos fazer a estimativa do termo do lado direito de (4.28). Seja

$$M = max(|\beta_1|, ..., |\beta_m|).$$

Logo,

$$\varepsilon_j \leq 2Me^M \frac{|c|^s}{(p-1)!} sup\{|\lambda\beta_j|^{p-1}|R(\lambda\beta_j)|^p : \quad 0 \leq \lambda \leq 1\}, \tag{4.40}$$

onde usamos que $0 \leq \lambda \leq 1$. Seja a seguir

$$N = max\{|R(z)| : \ |z| < m\},$$

a qual usada em (4.40) fornece

$$\varepsilon_j \leq 2Me^M \frac{|c|^s}{(p-1)!} M^{p-1} N^p.$$

Como o fatorial domina qualquer exponencial, isto é,

$$\lim_{n\to\infty} \frac{A^n}{n!} = 0,$$

para qualquer $A > 0$, segue que, para p suficientemente grande, podemos fazer $\varepsilon_j < \frac{1}{m+1}$. Logo,

$$\sum_{j=1}^{m} \varepsilon_j \leq \frac{m}{m+1} < 1. \tag{4.41}$$

A expressão (4.41) juntamente com o fato que o lado esquerdo de (4.28) é inteiro não nulo resulta em um absurdo. Logo, π é transcendente.

Com este último resultado cumprimos o objetivo deste trabalho.

5 Números Irracionais: Uma Abordagem no Ensino Médio.

Os PCN alertam para a importância e a dificuldade do tratamento dos números, na escola. Não é desejável que os alunos saiam da escola básica sem terem construído os conceitos de números e conjuntos numéricos, estando restritos ao nível utilitário, realizando cálculos segundo regras memorizadas, sem qualquer compreensão a respeito do que estão fazendo.

Ao trabalhar com os números, é preciso criar atividades que explorem diferentes contextos, trabalhar com suas diferentes representações, explorar a ordenação e a comparação e, especialmente, trabalhar com a reta numérica.

Atividades:

Em meio à infinidade do nosso sistema numérico, temos diversos números com suas peculiaridades: entre eles, os números irracionais. O surgimento do conjunto dos números irracionais é proveniente de uma discussão acerca do cálculo da diagonal de um quadrado de lado 1.

Vamos determinar a medida da diagonal d do quadrado ABCD cujo lado mede 1.

Usando o Teorema de Pitágoras no triângulo ABC, temos:

$$\begin{aligned} d^2 &= 1^2 + 1^2 \quad \Rightarrow \\ d^2 &= 1 + 1 \quad \Rightarrow \\ d^2 &= 2 \end{aligned}$$

Qual o número racional positivo cujo quadrado dá 2?

Inicialmente, vamos fazer:

$$1^2 = 1 \text{ e } 2^2 = 4$$

Logo, d está entre 1 e 2 $(1 < d < 2)$.

Em seguida, vamos determinar a primeira casa decimal de d.

$$(1,3)^2 = 1,69 \qquad (1,4)^2 = 1,96 \qquad (1,5)^2 = 2,25$$

Logo, d está entre 1,4 e 1,5, ou seja, $1,4 < d < 1,5$.

Então, 1,4 é o valor aproximado de d, por falta, com uma casa decimal.

Usando o mesmo procedimento, determinamos a segunda casa decimal de d.

$$(1,41)^2 = 1,9881 \qquad (1,42)^2 = 2,0164$$

Logo, d está entre 1,41 e 1,42, ou seja, $1,41 < d < 1,42$.

Aqui, 1,41 é o valor aproximado de d, por falta, com duas casas decimais.

Se repetirmos esse processo, vamos obter quantas casas decimais quisermos, mas encontraremos sempre um valor aproximado para d, por falta, pois esse valor, elevado ao quadrado, é sempre um número menor que 2.

Representamos o valor exato para a medida da diagonal do quadrado de lado 1 por $\sqrt{2}$.

$$\sqrt{2} = 1,414213562373095048801688724209 7...$$

Esse valor tem uma infinidade de casas decimais que não se repetem, portanto não é uma dízima periódica. Assim, $\sqrt{2}$ não é um número racional. É um número irracional.

Um exemplo interessante da aplicação do conceito de números racionais e números irracionais é uma questão do vestibular da Unicamp de 1992.

Exemplo 5.1. Considere duas circunferências, uma delas tendo o raio com medida racional e a outra com medida irracional. Suponha que essas circunferências tem centros fixos e estão se tocando de modo que a rotação de uma delas produz uma rotação na outra, sem deslizamento. Mostre que os dois pontos (um de cada circunferência) que coincidem no início da rotação, nunca mais voltarão a se encontrar.

Resolução.

Sejam as circunferências denotadas por C_1 e C_2 e seus pontos de encontro A e B, respectivamente. Sejam r e R os raios de C_1 e C_2, respectivamente. Logo, r é racional e R é irracional.

Se o ponto A andar um arco de comprimento x, o ponto B também irá andar essa distância, já que não há deslizamento entre elas.

Suponhamos que após n voltas completas de A e m voltas completas de B, os pontos se encontram novamente. Nesse caso, teremos:

$$n2\pi r \quad = \quad m2\pi R,$$

pois ambas deverão percorrer o mesmo arco. Logo,

$$\begin{aligned} nr &= mR \\ R &= \left(\frac{n}{m}\right) r \end{aligned}$$

Como n, m são inteiros, $\left(\frac{n}{m}\right)$ é racional, assim como r. Isso é um absurdo, pois o produto de dois racionais é também um racional, mas R é irracional.

Assim, não existem n e m que cumprem as condições e, portanto, os dois pontos nunca mais se encontram.

Outras aplicações importantes envolvendo tais números podem ser encontradas na literatura científica.

Referências

[1] FIGUEIREDO, D. G.: *Números Irracionais e Transcendentes*, Terceira Edição, Julho, 2002. Sociedade Brasileira de Matemática.

[2] DOMINGUES, HYGINO H., IEZZI, GELSON : *Álgebra Moderna*, Segunda Edição, São Paulo, 1982. Atual.

[3] HEFEZ, ABRAMO: *Elementos de Aritmética*, Segunda Edição, Rio de Janeiro, 2011. SBM.

[4] NIVEN, I., ZUCKERMAN, H. S. and MONTGOMERY, H. L. R.: *An Introduction to the Theory of Numbers*, 5th ed.,New York, 1991.

[5] GIOVANNI, J. R., BONJORNO, J. R.: *Matemática Fundamental: uma nova abordagem*, São Paulo, 2002. FTD.

6 Apêndice

Teorema A. Seja $f(t_1, ..., t_n)$ um polinômio simétrico de grau d com coeficientes em A. Então, existe um polinômio $g(s_1, ..., s_n)$ de peso menor ou igual a d com coeficientes em A, onde

$$\begin{aligned} s_1 &= \sum_{j=1}^{n} t_j \\ s_2 &= \sum_{i<j} t_i t_j \\ s_3 &= \sum_{i<j<k} t_i t_j t_k \\ &\vdots \\ s_n &= t_1 t_2 ... t_n \end{aligned}$$

são os polinômios simétricos elementares em $t_1 t_2 ... t_n$, tal que

$$f(t_1, ..., t_n) = g(s_1, ..., s_n).$$

Demonstração. (Por indução em n): Para $n = 1$, o teorema é óbvio, pois nesse caso $s_1 = t_1$. Suponhamos, agora, que o teorema seja válido para polinômios em $t_1, ..., t_{n-1}$. Representemos por $\overline{s}_1, ..., \overline{s}_{n-1}$ os polinômios simétricos elementares em $t_1, ..., t_{n-1}$:

$$\begin{aligned} \overline{s}_1 &= \textstyle\sum_{j=1}^{n-1} t_j && && (6.1.1) \\ \overline{s}_2 &= \textstyle\sum t_i t_j, && 1 \leq i < j \leq n-1 && (6.1.2) \\ \overline{s}_3 &= t_i t_j t_k, && 1 \leq i < j < k \leq n-1 && (6.1.3) \\ &\vdots \\ \overline{s}_{n-1} &= t_1 ... t_{n-1} && && (6.1.n) \end{aligned}$$

os quais podem ser obtidos das funções correspondentes, fazendo $t_n = 0$.

Agora, para provar que o teorema vale para polinômios em $t_1, ..., t_n$, procedemos por indução nos graus d desses polinômios. Para $d = 0$, o resultado é trivial, pois teríamos apenas os polinômios constantes. Suponha que o resultado seja válido para polinômios de grau menor que d, e provemos que ele se verifica para polinômios de grau d. Seja,

$f(t_1, ..., t_n)$ um polinômio de grau d. Pela hipótese de indução, existe um polinômio de peso menor ou igual a d, $g_1(\overline{s}_1, ..., \overline{s}_{n-1})$, tal que

$$f(t_1, ..., t_{n-1}, 0) = g_1(\overline{s}_1, ..., \overline{s}_{n-1}). \tag{6.2}$$

Assim $g_1(s_1, ..., s_{n-1})$ é um polinômio em $t_1...t_n$, cujo grau é menor ou igual a d. Vemos que $g_1(\overline{s}_1, ..., \overline{s}_{n-1})$ é um polinômio simétrico em $t_1...t_n$. Logo,

$$f_1(t_1, ..., t_n) = f(t_1, ..., t_n) - g_1(s_1, ..., s_{n-1}) \tag{6.3}$$

é um polinômio simétrico em $t_1...t_n$. Provemos agora que $f_1(t_1...t_n)$ é da forma (6.4), abaixo, com f_2 de grau menor que d, para então usarmos a hipótese de indução. Agora, se fizermos $t_n = 0$ em (6.3), obtemos, em virtude de (6.2), que

$$f_1(t_1, ..., t_{n-1}, 0) = 0.$$

Consequentemente, t_n é um fator comum em $f_1(t_1, ..., t_n)$. Agora, do fato que $f_1(t_1, ..., t_n)$ é simétrico em $t_1, ..., t_n$, segue-se que t_j, para todo $j = 1, ..., n$, é fator comum de $f_1(t_1, ..., t_n)$. Logo

$$f_1(t_1, ..., t_n) = s_n f_2(t_1, ..., t_n), \tag{6.4}$$

e daí segue que o grau de f_2 é $\leq d - n < d$. Aplicando a hipótese de indução, temos que existe um polinômio $g_2(s_1, ..., s_n)$ de peso menor ou igual a $d - n$, tal que

$$f_2(t_1, ..., t_n) = g_2(s_1, ..., s_n). \tag{6.5}$$

Finalmente de (6.3), (6.4) e (6.5) obtemos

$$f(t_1, ..., t_n) = s_n g_2(s_1, ..., s_n) + g_1(s_1, ..., s_{n-1}),$$

o que mostra que $f(t_1, ..., t_n)$ é igual a um polinômio simétrico em $s_1, ..., s_n$: $g(s_1, ..., s_n) = s_n g_2(s_1, ..., s_n) + g_1(s_1, ..., s_{n-1})$. O peso de $g(s_1, ..., s_n)$ é menor ou igual a d.

E a demonstração do Teorema A está concluída. □

Exemplo 6.1. :

1) (n = 2). O polinômio $f(t_1, t_2) = t_1^2 + t_2^2 + 6t_1t_2$ é simétrico, e vemos que

$$t_1^2 + t_2^2 + 6t_1t_2 = (t_1 + t_2)^2 + 4t_1t_2$$

logo, o polinômio $g(s_1, s_2)$ nesse caso será $g(s_1, s_2) = s_1^2 + 4s_2$.

2) (n = 3). O polinômio $f(t_1, t_2, t_3) = t_1^2 + t_2^2 + t_3^2 + t_1t_2t_3$ é simétrico, e, nesse caso,

$$g(s_1, s_2, s_3) = s_1^2 - 2s_2 + s_3.$$