



UNIVERSIDADE ESTADUAL PAULISTA “JÚLIO DE MESQUITA FILHO”
Instituto de Geociências e Ciências Exatas
Campus de Rio Claro

A Irrracionalidade e Transcendência do Número e

Getulio de Assis Vasconcelos

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 Rizzioli

2013

512 Vasconcelos, Getulio de Assis
V33li A Irracionalidade e Transcendência do Número e / Getulio de Assis Vasconcelos- Rio Claro: [s.n.], 2013.
39 f.: il.

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

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

TERMO DE APROVAÇÃO

Getulio de Assis Vasconcelos

A IRRACIONALIDADE E TRANSCENDÊNCIA DO NÚMERO e

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 Rizzioli
Orientadora

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

Prof. Dr. Thiago de Melo
Departamento de Matemática-IGCE-UNESP/Rio Claro

Rio Claro, 28 de Janeiro de 2013

Dedicado a minha esposa Anna e a meu filho João Vicente

Agradecimentos

Agradeço, primeiramente, a minha família querida, minha esposa Anna Paula Almeida Vasconcelos e meu filho João Vicente Almeida Vasconcelos pelo incentivo e paciência de suportar a minha ausência em finais de semana e férias para que a conclusão do curso e desse trabalho fossem realizados.

Aos meus pais: Rivair de Assis Vasconcelos e Maria Aparecida Vasconcelos e minha irmã Valéria de Assis Vasconcelos que sempre me incentivaram, principalmente no início, onde eu tinha dúvidas se conseguiria conciliar a vida de trabalhador com a vida de estudante de Pós-Graduação.

A minha sogra Cleuza dos Santos Almeida por sempre rezar muito pelo meu sucesso pessoal e profissional, e pelo meu cunhado Arnaldo Jorge de Almeida Junior por me aconselhar e me orientar devido a sua experiência de Mestre formado na academia e na vida.

Agradecimentos também aos meus colegas de turma do Profmat 2011 da Unesp Rio Claro por compartilhar experiências e conhecimentos ao longo de 2 anos, fundamentais para o meu sucesso acadêmico.

E por último e mais importante, agradeço a Deus, por me dar a oportunidade de nascer e viver nesse mundo e me iluminar em todas as minhas decisões, estas que me fizeram crescer e evoluir na vida.

Obrigado a todos!

Percebendo que não há nada mais trabalhoso na prática da matemática, nem que mais prejudique e atrapalhe os calculadores, do que as multiplicações, as divisões, as extrações do quadrado e do cubo dos números muito grandes...comecei a considerar em minha mente através de que tipo de arte certa e rápida poderia remover essas dificuldades.

John Napier, Mirifici logarithmorum canonis descriptio(1614)

Resumo

Quando John Napier desenvolveu seu estudo sobre logaritmo, ele com certeza não imaginou as implicações futuras de suas descobertas. O número e tem importância estratégica nas aplicações de várias áreas do conhecimento científico. Esse trabalho tem como objetivo apresentar o número e como limite infinito de uma sequência, demonstrar sua existência, irracionalidade e transcendência.

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

Abstract

When John Napier developed his study of logarithm, he certainly did not imagine the future implications of their findings. The number e has strategic importance in applications from various areas of scientific knowledge. This work aims to present the number e as the limit of infinite sequence, demonstrating its existence, irrationality and transcendence.

Keywords: Algebra, Number Theory, Algebraic Numbers.

Sumário

1	Introdução	8
2	Sobre Números Algébricos e Transcendentes	10
3	Existência e Irracionalidade do Número e	23
3.1	Existência do Número e	23
3.2	O Número e é Irracional	25
4	O Número e é Transcendente	28
5	Sugestão de Aula para o Ensino Médio	36
	Referências	39

1 Introdução

Para apresentarmos a história do número e é preciso emprestar a história de outro objeto importante para a evolução da matemática, a saber, os Logaritmos.

Logaritmo: palavra de origem grega formada de \logos (razão, evolução, discurso) e $arithmós$ (número). Logaritmo significa, literalmente, a evolução de um número. O símbolo log , contração de $logarithm$, é devido ao astrônomo Kepler.

Os logaritmos foram inventados por John Napier (1550-1617). Seu objetivo era obter uma forma menos trabalhosa de fazer cálculos. E, na época, uma multiplicação entre números grandes, por exemplo, era um verdadeiro sacrifício, a ideia era obter o resultado de uma multiplicação através de uma operação mais fácil: a soma.

Neper ou Napier construiu suas tábuas de logaritmos e publicou um tratado: *Mirifici logarithmorum canonis descriptio*. Posteriormente, outro matemático, Henry Briggs (1561-1631) sugeriu o uso da base 10, cujas tabelas com a notação log de N na base 10 é usada até hoje.

E na sequência, depois do logaritmo decimal, ensinava-se logaritmos em outras bases, em especial o famoso $\ln x$, significando logaritmos natural ou logaritmo na base e , ou ainda, logaritmo neperiano.

Para apresentar o número e , vamos supor uma situação bastante hipotética. Imagine que um banco pague juros de 100 por cento ao ano, após esse 1 ano, teríamos o montante de 2 reais para cada 1 real aplicado.

E se os juros fossem creditados semestralmente, ao final de um ano teríamos 2,25 reais. A expressão para esse cálculo é a seguinte:

$$\left(1 + \frac{1}{n}\right)^n = \left(1 + \frac{1}{2}\right)^2 = 2,25$$

Para o crédito trimestral, temos $n=4$ e o resultado é 2,44141. Ao calcularmos o resultado para o crédito instantâneo, ou seja, n tendendo para infinito, esse limite é um número irracional chamado número e (número de Euler).

Em termos matemáticos:

$$\lim_{n \rightarrow \infty} \left(1 + \frac{1}{n}\right)^n = e$$

$$e = 2,71828182845904523536028747135266\dots$$

Quem efetivamente calculou o número e foi Leonhard Euler, e dizem que a designação decorre da inicial do seu sobrenome, mas também existe a versão do que o e se dava à inicial de "exponencial".

Se aquele banco quisesse creditar juros instantâneos à sua aplicação de 1 real, a 100 por cento ao ano, você teria ao final de um ano o valor de 2,718 reais aproximadamente.

Esse número é importante em quase todas as áreas do conhecimento, a função $x \mapsto e^x$, modela fenômenos de vital importância nos mais variados campos da ciência: físico-químicas, biológicas, econômicas, agrônômicas, geográficas, médicas, sociais, etc.

Este trabalho foi organizado da seguinte maneira: reservamos o capítulo 1 para esta introdução, o capítulo 2 versa sobre números algébricos e transcendentos, capítulo 3 aborda a existência e irracionalidade de e , e dedicamos o capítulo 4 para mostrar sua transcendência. E finalmente no capítulo 5 apresentamos uma aula aplicada ao Ensino Médio envolvendo os elementos tratados nos capítulos anteriores.

2 Sobre Números Algébricos e Transcendentes

Para ser possível tratar dos números algébricos primeiramente devemos introduzir definições e propriedades acerca dos números inteiros.

Definição 2.1. 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 2.1. $a = 2, b = 4; 4 = q2 \implies q = 2$.

Definição 2.2. Um número $p \in \mathbb{N}$ e $p \neq 1$, 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 $p \in \mathbb{Z}$, $p \neq 0$, $p \neq 1$, $p \neq -1$ é **primo** se os únicos números inteiros que o dividem são $|p|$, -1 e 1 .

Exemplo 2.2. $p = 7, \quad b|7 \iff b = 7 \text{ ou } b = 1$.

Definição 2.3. Seja $a \in \mathbb{Z}$. Um número inteiro b é chamado **múltiplo** de a se $b = aq$, para algum $q \in \mathbb{Z}$.

Exemplo 2.3. $a = 6, q = 3; \quad b = 6.3 \implies b = 18$.

Definição 2.4. Dados $a, b \in \mathbb{Z}$, um número natural d é chamado **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 2.4. $a = 16, b = 32 \quad m.d.c.(16, 32) = 16 = d$. 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 2.1. O $m.d.c(a, 0)$ não existe caso a seja **nulo**. Além disso, assumimos que $m.d.c(a, 0) = 1$, se $a \neq 0$.

Teorema 2.1. (*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,

$$a = qb + r. \quad (1)$$

Demonstração. (i) **Existência.**

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

$$\dots -3b < -2b < -b < 0 < b < 2b < 3b\dots$$

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

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

com $q \in \mathbb{Z}$.

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

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 $r < (q+1)b - qb = b$.

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

$$a = q'|b| + r. \quad (2)$$

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 $a = q_1b + r_1$, com $0 \leq r < |b|$ e $0 \leq r_1 < |b|$.

Assim,

$$qb + r = q_1b + r_1 \Rightarrow$$

$$r - r_1 = (q_1 - q)b \quad (3)$$

Afirmamos que $r = r_1$.

Com efeito, se $r \neq r_1$, então: $0 < |r_1 - r|$.

Além disso, $|r_1 - r| < b$. Pois, podemos admitir, sem perda de generalidade que $r < r_1$, conseqüentemente $r_1 - r > 0$ 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,

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

Portanto, do acima 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 2.5. $a = 11, b = 5; \quad q = 2 \quad r = 1 \implies 11 = 2 \cdot 5 + 1.$

Teorema 2.2. *Dados $a, b \in \mathbb{Z}$ (pelo menos um deles não nulos) 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. 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 algoritmo da divisão aos elementos a e d :

$$a = dq + r \quad (0 \leq r < d).$$

Das duas últimas igualdades segue que

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

ou, ainda

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

o que vem mostrar que $r \in L$. Sendo r positivo e levando em conta a escolha do elemento 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 $d = m.d.c(a, b)$. \square

Lema 2.1. *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 2.1) implica que existe $q \in \mathbb{Z}$, tal que $a = dq$. Também (pela definição 2.1) $d|b$ 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, $ax_0 + by_0 = dK$, $K \in \mathbb{Z}$, ou seja,

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

\square

Exemplo 2.6. $2|4$ e $2|6 \Rightarrow 2|(4x_0 + 6y_0), \forall x_0, y_0 \in \mathbb{Z}$.

Lema 2.2. *Seja $r \in \mathbb{N}$ um número primo, e $a, b \in \mathbb{Z}$. Se r divide o produto ab então r divide a ou 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 2.2, existem $x_0, y_0 \in \mathbb{Z}$ tais que $ax_0 + ry_0 = 1$.

Assim,

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

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

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

Portanto de (I) segue que $r|b$.

\square

Exemplo 2.7. 1. $r = 3$, $a = 9$, $b = 5$, temos que $3|9 \cdot 5$ e também $3|9$.

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

Proposição 2.1. *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,

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

Além disso, observe que $\mathcal{P}(2)$ também é válida pois se $r|p^2$, e se $r|p.p$, então $r|p$ ou $r|p$, i. 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, de $\mathcal{P}(2)$, 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 $r|p$ ou $r|p$, i. é, $r|p$.

□

Definição 2.5. Qualquer solução de uma equação da forma

$$x^n + a_{n-1}x^{n-1} + \dots + a_1x + a_0 = 0 \quad (1)$$

onde cada coeficiente $a_i \in \mathbb{Z}, \forall i \in \{0, 1, \dots, n-1\}$, é chamado inteiro algébrico.

Exemplo 2.8. 1. Seja $b \in \mathbb{Z}$, então b é um inteiro algébrico, pois b é solução da equação $x - b = 0$, a qual é do tipo (1), para $n = 1$ e $a_0 = -b$.

2. $\sqrt{7}$ é um inteiro algébrico, já que é solução de $x^2 - 7 = 0$.

3. $\sqrt{2 + \sqrt{3}}$ é um inteiro algébrico.

Uma vez que é solução de uma equação do tipo (1).

Abaixo descrevemos como obtê-la. Temos que $x = \sqrt{2 + \sqrt{3}}$, para chegar a uma equação do tipo (1), precisamos aplicar duas quadraturas.

Aplicando a primeira quadratura :

$$x = \sqrt{2 + \sqrt{3}} \Rightarrow x^2 = (\sqrt{2 + \sqrt{3}})^2 \Rightarrow x^2 = 2 + \sqrt{3}.$$

Para eliminar o radical que restou, aplicamos outra quadratura:

$$x^2 = 2 + \sqrt{3} \Rightarrow$$

$$x^2 - 2 = \sqrt{3} \Rightarrow$$

$$(x^2 - 2)^2 = (\sqrt{3})^2 \Rightarrow$$

$$x^4 - 4x^2 + 4 = 3 \implies$$

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

Portanto, $x^4 - 4x^2 + 1 = 0$, é a equação procurada.

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

De fato,

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

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

5. 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 2.2. 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 2.3. *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 (1), ou seja:

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

Então,

$$\left(\frac{p}{q}\right)^n + a_{n-1}\left(\frac{p}{q}\right)^{n-1} + \dots + a_1\left(\frac{p}{q}\right) + a_0 = 0 \Rightarrow$$

$$\frac{p^n}{q^n} + a_{n-1}\frac{p^{n-1}}{q^{n-1}} + \dots + a_1\frac{p}{q} + a_0 = 0 \Rightarrow$$

$$\frac{p^n}{q^n} = -a_{n-1}\frac{p^{n-1}}{q^{n-1}} - \dots - a_1\frac{p}{q} - a_0 \Rightarrow$$

$$p^n = q^n\left(-a_{n-1}\frac{p^{n-1}}{q^{n-1}} - \dots - a_1\frac{p}{q} - a_0\right) \Rightarrow$$

$$p^n = (-a_{n-1}p^{n-1}q - \dots - a_1pq^{n-1} - a_0q^n) \Rightarrow$$

$$p^n = q(-a_{n-1}p^{n-1} - \dots - a_1pq^{n-2} - a_0q^{n-1}).$$

Considerando,

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

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 $p = q$); então r divide p^n e pela Proposição 2.1 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 (1)).

□

Definição 2.6. (a) Qualquer solução de uma equação polinomial da forma

$$a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0 = 0, \quad a_i \in \mathbb{Z}, \text{ para todo } i \in \{0, \dots, n\}$$

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 seja algébrico é chamado **transcendente**.

Os números algébricos possuem algumas propriedades de fechamento, as quais são listadas abaixo.

- (i) A soma de dois números algébricos é um algébrico;
- (ii) O produto de dois números algébricos é um algébrico;
- (iii) O simétrico $-\alpha$ de um número algébrico α é algébrico;
- (iv) O inverso α^{-1} de um número algébrico $\alpha \neq 0$ é um algébrico.

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

Definição 2.7. 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, (isto é, uma função injetiva e sobrejetiva), $f: \mathbb{N} \rightarrow A$.

Exemplo 2.9. (a) O conjunto dos números pares positivos é enumerável:

Seja $P = \{2n, n \in \mathbb{N}\}$, e considere a seguinte função

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

(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 $b = 2n_o$ para algum $n_o \in \mathbb{N}$. Tomando $x = n_o$, temos que $f(x) = f(n_o) = 2n_o = b$, ou seja, $b \in f(\mathbb{N})$, logo $b = f(x)$.

Portanto f é sobrejetora.

Logo por (i) e (ii), f é bijetora.

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

$$f: \mathbb{N} \longrightarrow I$$

$$n \longmapsto 2n - 1$$

onde $I = 2n - 1, n \in \mathbb{N}$.

A demonstração pode ser feita de modo análogo ao exemplo (a).

(c) O conjunto \mathbb{Z} é enumerável. Observe a correspondência abaixo

$$\begin{array}{cccccccc} \dots, & -3, & -2, & -1, & 0, & 1, & 2, & 3, & \dots \\ & \downarrow & \\ \dots & 7, & 5, & 3, & 1, & 2, & 4, & 6, & \dots \end{array}$$

Esta correspondência pode ser descrita pela função definida por partes

$$f: \mathbb{Z} \longrightarrow \mathbb{N}$$

$$n \longmapsto f(n)$$

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

$$n = 2k = f(k) = f(x).$$

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

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

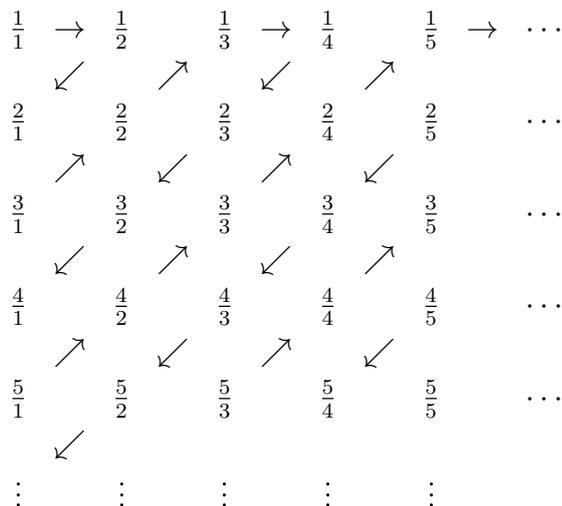
portanto por (i) e (ii), segue que f é sobrejetora.

Logo por (i) e (ii), f é bijetora.

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

(d) O conjunto dos números racionais é enumerável.

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



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

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

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 2.4. (i) A união de um conjunto finito e um conjunto enumerável é um conjunto 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) Sejam $A = \{a_1, a_2, \dots, a_n\}$ conjunto finito e $B = \{b_1, b_2, \dots\}$ o conjunto enumerável. O conjunto $A \cup B$ é enumerável.

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

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

(ii) Sejam $A = \{a_1, a_2, \dots\}$ e $B = \{b_1, b_2, \dots\}$, 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, \dots, A_n conjuntos enumeráveis, queremos mostrar que $A_1 \cup A_2 \cup \dots \cup A_n$, 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, \dots, A_k são enumeráveis então $A_1 \cup A_k$ é enumerável.

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

A_1, \dots, A_k, A_{k+1} são enumeráveis, então

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

é enumerável.

Note que

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

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

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

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

Portanto $A_1 \cup \dots \cup A_k \cup A_{k+1}$ é enumerável.

Logo pelo Princípio de Indução Finita, (iii) é válida.

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

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

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

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

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

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

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

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

Suponha que

$$\begin{aligned}
A_1 &= \{a_{11}, a_{12}, a_{13}, \dots\} \\
A_2 &= \{a_{21}, a_{22}, a_{23}, \dots\} \\
A_n &= \{a_{n1}, a_{n2}, a_{n3}, \dots\}
\end{aligned}$$

Disponha os elementos de A_1, A_2, \dots, A_n como a tabela

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

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 $A_1 \cup A_2 \cup \dots \cup A_n \cup \dots$ e conseqüentemente provamos que é um conjunto enumerável. \square

Teorema 2.5. *O conjunto \mathbb{R} dos números reais não é enumerável.*

Demonstração. Demonstramos que o conjunto dos números reais $x \in [0, 1)$, (isto é, $0 \leq x < 1$) 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

$$0 \ a_1 \ a_2 \ a_3 \dots, \quad (*)$$

onde a_j é um dos algarismos 1, 2, 3, 4, 5, 6, 7, 8 ou 9. Alguns números tem duas representações da forma (*), 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 (*) que a partir de uma certa ordem todos os elementos são 9. Suponhamos que as decimais tipo (*), ou que os números reais no intervalo $[0, 1)$, formam um conjunto enumerável.

$$\begin{array}{cccccc}
0 & a_{11} & a_{12} & a_{13} & \dots & \\
0 & a_{21} & a_{22} & a_{23} & \dots & \\
0 & a_{31} & a_{32} & a_{33} & \dots & \\
& & \vdots & & \dots &
\end{array} \quad (**)$$

Agora forme o decimal $0, b_1 b_2 b_3 \dots$ 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 $0, b_1 b_2 b_3 \dots \neq 0, a_{n1} a_{n2} a_{n3} \dots$, para todo n , pois $b_n \neq a_{nn}$. Logo $0, b_1 b_2 b_3 \dots$ não está na tabela (**), o que é um absurdo, já que é um número real entre 0 e 1. \square

Com os resultados anteriores provaremos a existência de números transcendentos no seguinte teorema.

Teorema 2.6. *Existem números transcendentos.*

Demonstração. Dado um polinômio não nulo com coeficientes inteiros com $a_n \neq 0$,

$$P(x) = a_n x^n + \dots + a_1 x + a_0 \quad (*)$$

definimos sua altura como sendo o número natural

$$|P| = |a_n| + \dots + |a_1| + |a_0| + n \quad (**)$$

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 (*) 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 (**)).

Logo, as raízes de todos os polinômios de uma dada altura formam um conjunto finito, conseqüentemente 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 $|P| = |3| + |-1| + |0| + |1| + |-5| + 4$, pelo Teorema Fundamental da Álgebra $P(x)$ possui quatro raízes complexas e com essa altura podem existir até treze polinômios).

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 transcendentais reais. Assim, como o conjunto \mathbb{R} não é enumerável, o conjunto dos transcendentais reais deve ser não enumerável, já que, caso contrário, pelo item (ii) do Teorema 2.4, \mathbb{R} seria enumerável. Conseqüentemente, existe um conjunto infinito não enumerável de números reais transcendentais. \square

3 Existência e Irrracionalidade do Número e

Primeiramente provamos que o número e existe e mais ainda está compreendido entre 2 e 3.

3.1 Existência do Número e

Teorema 3.1. *O $\lim_{n \rightarrow \infty} (1 + \frac{1}{n})^n$ existe e está compreendido entre 2 e 3.*

Demonstração. Vamos provar que o $\lim_{n \rightarrow \infty} (1 + \frac{1}{n})^n$ existe.

$$\text{Seja } u_n = (1 + \frac{1}{n})^n$$

Qualquer que seja n inteiro e positivo, (u_n) é uma potência de base positiva, portanto, também positiva. Vamos mostrar que u_n é crescente, desenvolvendo o termo geral segundo a fórmula do binômio de Newton:

$$u_n = 1 + n \frac{1}{n} + \frac{n(n-1)}{2!} \frac{1}{n^2} + \dots + \frac{n(n-1)(n-2) \dots 2 \cdot 1}{n!} \frac{1}{n^n}$$

$$u_n = 1 + \frac{1}{1!} + \frac{1}{2!} \frac{n(n-1)}{n^2} + \frac{1}{3!} \frac{n(n-1)(n-2)}{n^3} + \dots + \frac{1}{n!} \frac{n(n-1)(n-2) \dots 2 \cdot 1}{n^n}$$

ou ainda

$$u_n = 1 + \frac{1}{1!} + \frac{1}{2!} (1 - \frac{1}{n}) + \frac{1}{3!} (1 - \frac{1}{n})(1 - \frac{2}{n}) + \dots + \frac{1}{n!} (1 - \frac{1}{n})(1 - \frac{2}{n}) \dots (1 - \frac{n-1}{n})$$

temos então:

$$u_n > 1 + \frac{1}{1!} + \frac{1}{2!} (1 - \frac{1}{n-1}) + \frac{1}{3!} (1 - \frac{1}{n-1})(1 - \frac{2}{n-1}) + \dots \\ \dots \frac{1}{(n-1)!} (1 - \frac{1}{n-1})(1 - \frac{2}{n-1}) \dots (1 - \frac{n-2}{n-1}) = u_{n-1}$$

Conclui-se que $u_n > u_{n-1}$ para n inteiro e positivo qualquer. Logo a sucessão u_n é crescente.

Demonstraremos agora que a sucessão de termo geral u_n é limitada superiormente.

$$u_n = \left(1 + \frac{1}{n}\right)^n < 1 + \frac{1}{1!} + \frac{1}{2!} + \cdots + \frac{1}{n!}$$

e como $n! > 2^{n-1}$ para $n \geq 3$ inteiro, temos:

$$u_n \leq 1 + 1 + \frac{1}{2} + \frac{1}{2^2} + \cdots + \frac{1}{2^{n-1}} = 1 + 2 - \frac{1}{2^{n-1}} \leq 3$$

que prova ser 3 maior que qualquer sucessão e, portanto, esta é limitada superiormente. Então a sucessão de termo geral $u_n = \left(1 + \frac{1}{n}\right)^n$ sendo crescente e limitada superiormente tem limite finito.

Vamos provar que $2 \leq \lim_{n \rightarrow \infty} \left(1 + \frac{1}{n}\right)^n < 3$

Sabemos que $u_n < 3$ para todo n inteiro e positivo, portanto

$$\lim_{n \rightarrow \infty} \left(1 + \frac{1}{n}\right)^n \leq 3$$

e

$$u_n = \left(1 + \frac{1}{n}\right)^n \geq 1 + \frac{1}{1!} = 2$$

□

3.2 O Número e é Irracional

Para mostrar a irracionalidade de e fazemos uso de uma interessante caracterização deste, objeto do próximo Lema.

Lema 3.1.

$$e = 1 + \frac{1}{1!} + \frac{1}{2!} + \dots + \frac{1}{q!} + \dots \quad (I)$$

Demonstração. Toda função de classe C^∞ pode ser escrita como um polinômio de Taylor:

$$f(x) = f(x_0) + \frac{f'(x_0)}{1!}(x - x_0) + \frac{f''(x_0)}{2!}(x - x_0)^2 + \dots + \frac{f^{(n)}(x_0)}{n!}(x - x_0)^n + \dots$$

ou

$$f(x) = f(x_0) + \sum_{n=1}^{\infty} \frac{f^{(n)}(x_0)}{n!}(x - x_0)^n.$$

No caso particular de $f(x) = e^x$, em torno da origem (ou seja $x_0 = 0$), temos:

$$f(x) = f(0) + \frac{f'(0)}{1!}(x) + \frac{f''(0)}{2!}(x^2) + \dots + \frac{f^{(n)}(0)}{n!}(x^n) + \dots \quad (II)$$

Sabe-se que $f^{(n)}(x) = e^x$, $\forall n \in 1, 2, \dots$, ou seja, $f'(x) = e^x$, $f''(x) = e^x$, $f'''(x) = e^x$ e assim por diante.

Em particular para $x_0 = 0$ tem-se $f^{(n)}(0) = e^0 = 1 \quad \forall n \in 1, 2, 3, \dots$

Note ainda que $f(0) = e^0 = 1$.

Da observação acima e de (II), segue que $e^x = 1 + \frac{x}{1!} + \frac{x^2}{2!} + \frac{x^3}{3!} + \dots + \frac{x^n}{n!} + \dots \quad \square$

Teorema 3.2. *O número e é Irracional*

Demonstração. É demonstrado no Lema anterior que:

$$e = 1 + \frac{1}{1!} + \frac{1}{2!} + \dots + \frac{1}{q!} + \dots \quad (I)$$

Suponha que e seja um número racional, isto é, e pode ser escrito da forma $\frac{p}{q}$ com $p, q \in \mathbb{Z}$. Suponha ainda que $\frac{p}{q}$ seja a forma irredutível, isto é, $(p, q) = 1$.

De (I), segue que:

$$\begin{aligned} \frac{p}{q} &= \left(1 + \frac{1}{1!} + \frac{1}{2!} + \dots + \frac{1}{q!}\right) + \frac{1}{(q+1)!} + \dots \implies \\ 0 &< \frac{p}{q} - \left(1 + \frac{1}{1!} + \frac{1}{2!} + \dots + \frac{1}{q!}\right) = \frac{1}{(q+1)!} + \frac{1}{(q+2)!} + \dots = \end{aligned}$$

$$\sum_{j=q+1}^{\infty} \frac{1}{j!} \quad (II)$$

mas observe que,

$$\begin{aligned} \frac{1}{(q+1)!} &= \frac{1}{(q+1)q!} \\ \frac{1}{(q+2)!} &= \frac{1}{(q+2)(q+1)q!} \\ \frac{1}{(q+3)!} &= \frac{1}{(q+3)(q+2)(q+1)q!} \\ &\vdots \\ &\vdots \\ &\vdots \end{aligned}$$

assim,

$$\begin{aligned} \sum_{j=q+1}^{\infty} \frac{1}{j!} &= \\ \frac{1}{(q+1)!} + \frac{1}{(q+2)!} + \frac{1}{(q+3)!} + \dots &= \\ \frac{1}{q!} \left(\frac{1}{(q+1)} + \frac{1}{(q+2)(q+1)} \right) + \dots &\leq \\ \frac{1}{q!} \left(\frac{1}{(q+1)} + \frac{1}{(q+1)^2} + \frac{1}{(q+1)^3} \right) + \dots & \quad (III) \end{aligned}$$

pois

$$\begin{aligned} (q+1) < (q+2) < (q+3) < \dots &\implies \\ \dots < \frac{1}{(q+3)} < \frac{1}{(q+2)} < \frac{1}{(q+1)} \end{aligned}$$

logo

$$\begin{aligned} \frac{1}{(q+2)(q+1)} &< \frac{1}{(q+1)(q+1)} = \frac{1}{(q+1)^2}, \\ \frac{1}{(q+3)(q+2)(q+1)} &< \frac{1}{(q+1)(q+1)(q+1)} = \frac{1}{(q+1)^3}, \end{aligned}$$

e assim sucessivamente...

Agora, note que

$$\left(\frac{1}{(q+1)} + \frac{1}{(q+1)^2} + \frac{1}{(q+1)^3} + \dots \right)$$

é a soma dos termos de uma progressão geométrica infinita

$$\left(\frac{1}{(q+1)}, \frac{1}{(q+1)^2}, \frac{1}{(q+1)^3}, \dots \right)$$

cujo primeiro termo é $\left(\frac{1}{(q+1)}\right)$ e a razão é $\left(\frac{1}{(q+1)}\right)$. Logo essa soma é igual a

$$\frac{\frac{1}{(q+1)}}{1 - \left(\frac{1}{(q+1)}\right)} = \frac{1}{(q+1)} \frac{(q+1)}{q} = \frac{1}{q}$$

ou seja,

$$\left(\frac{1}{(q+1)} + \frac{1}{(q+1)^2} + \frac{1}{(q+1)^3} + \dots\right) = \frac{1}{q} \quad (IV)$$

substituindo (IV) em (III) segue que

$$\sum_{j=q+1}^{\infty} \frac{1}{j!} < \frac{1}{q} \frac{1}{q!} \quad (V)$$

substituindo (V) em (II),

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

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

Observe que o segundo termo da esquerda para a direita da desigualdade acima é um número inteiro pois, $p, q \in \mathbb{Z}$, valem as leis do fechamento na multiplicação e adição temos:

$$q! \left(\frac{p}{q} - 1 - \frac{1}{1!} - \frac{1}{2!} - \dots - \frac{1}{q!}\right) =$$

$$q! \left(\frac{(q-1)!(p-q)! - q! - \dots - 1}{q!}\right) =$$

$$((q-1)!(p-q)! - q! - \dots - 1),$$

Mas isso é um absurdo, já que é impossível ter um número inteiro positivo menor que 1.

O absurdo foi supor que e é um número racional. Portanto e é um número irracional.

□

4 O Número e é Transcendente

Para demonstrarmos a transcendência do número e precisaremos utilizar os Lemas 4.1 e 4.2 a seguir.

Lema 4.1. *Seja $P(x)$ um polinômio de grau r . Definimos a função real*

$$F(x) = P(x) + P'(x) + \dots + P^r(x)$$

onde $P^r(x)$ representa a derivada de ordem r de P . então

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

Demonstração.

$$\frac{d}{dx}[e^{-x}F(x)] = \frac{d}{dx}[e^{-x}(P(x) + P'(x) + \dots + P^r(x))] =$$

$$-e^{-x}(P(x) + P'(x) + \dots + P^r(x)) + e^{-x}(P'(x) + \dots + P^r(x) + P^{r+1}(x)) =$$

$$e^{-x}(-P(x) - P'(x) - \dots - P^r(x) + P'(x) + \dots + P^r(x) + P^{r+1}(x)) =$$

$$e^{-x}(-P(x) + P^{r+1}(x)) =$$

$$-e^{-x}(P(x)) =$$

$$-e^{-x}P(x)$$

□

Lema 4.2. *Sejam $F(x)$ e $P(x)$ como no Lema 4.1, então*

$$F(k) - e^k F(0) = -P(k\theta_k)ke^{k(1-\theta_k)},$$

para todo $k > 0$ e onde θ_k é um número entre 0 e 1.

Demonstração. Defina a função

$$\begin{aligned} G : [0, k] &\longrightarrow \mathbb{R} \\ x &\longmapsto G(x) = e^{-x.F(x)} \end{aligned}$$

Note que para $k > 0$, G é contínua em $[0, k]$ e derivável em $]0, k[$ (já que e^x e $F(x)$ têm as mesmas propriedades). Então pelo Teorema do Valor Médio existe $c \in]0, k[$ tal que

$$\begin{aligned} G(k) - G(0) &= G'(c).(k - 0) \Rightarrow \\ e^{-k}F(k) - e^0F(0) &= -e^{-c}P(c)k \Rightarrow \\ e^{-k}F(k) - F(0) &= -k(e^{-c}P(c)) \end{aligned} \quad (*)$$

Observe que como $c \in]0, k[$, $\exists \theta_k \in]0, 1[$, tal que

$$c = k\theta_k. \quad (**)$$

Substituindo $(**)$ em $(*)$, temos

$$e^{-k}F(k) - F(0) = -k(e^{-k\theta_k}P(k\theta_k)).$$

Multiplicando ambos os membros por e^k , tem-se

$$e^k e^{-k}F(k) - e^k F(0) = -e^k k(e^{-k\theta_k}P(k\theta_k)) \Rightarrow F(k) - e^k F(0) = -P(k\theta_k)k e^{k(1-\theta_k)} = A_k$$

□

Corolário 4.1. *Sejam $F(x)$ e A_k definidos nos Lemas 4.1 e 4.2, e suponha que e não seja transcendente, isto é, suponha que e seja algébrico. Então, existem inteiros c_0, c_1, \dots, c_n (com $c_0 > 0$), tais que $c_n e^n + \dots + c_1 e + c_0 = 0$, [caso $c_0 < 0$, considere $(-c_n)e^n + \dots + (-c_1)e + c_0 = 0 \Rightarrow d_n e^n + \dots + d_1 e + d_0 = 0$, onde $d_i = (-c_i), \forall i \in 0, \dots, n$ e $d_0 > 0$], então:*

$$c_0 F(0) + c_1 F(1) + \dots + c_n F(n) = c_1 A_1 + \dots + c_n A_n$$

Demonstração. Pelo Lema 4.2, temos que $A_k = F(k) - e^k F(0)$, então para $k \in 1, \dots, n$, temos:

$$\begin{aligned} c_1 A_1 + \dots + c_n A_n &= \\ c_1 (F(1) - eF(0)) + \dots + c_n (F(n) - e^n F(0)) &= \\ c_1 F(1) + \dots + c_n F(n) - (c_1 e F(0) + \dots + c_n e^n F(0)) &= \\ c_1 F(1) + \dots + c_n F(n) - [F(0)(c_1 e + \dots + c_n e^n)] &= \\ c_0 F(0) + c_1 F(1) + \dots + c_n F(n) & \end{aligned}$$

$$\Rightarrow c_0 F(0) + c_1 F(1) + \dots + c_n F(n) = c_1 A_1 + \dots + c_n A_n$$

□

O objetivo é mostrar que o lado esquerdo dessa igualdade no Corolário 4.1 é um número inteiro não nulo, não divisível por p sendo $p \in \mathbb{Z}$, enquanto o lado direito da igualdade tem módulo menor que 1, caracterizando um absurdo.

Para provarmos o lado esquerdo da igualdade usaremos os Lemas 4.3, 4.4, 4.5, 4.6, 4.7 e 4.8. Já para o lado direito da igualdade usaremos os Lemas 4.9 e 4.10 a seguir.

Lema 4.3. *Vamos definir $Q(x)$ uma função polinomial onde:*

$$Q(x) = \sum_{j=0}^r a_j x^j, a_j \in \mathbb{Z}$$

$j = 0, \dots, r$ e $p < r$, então

$$Q^{(i)}(x) = \sum_{j=i}^r \frac{j!}{(j-i)!} a_j x^{j-i}, i \leq r$$

Demonstração. Antes façamos alguns exemplos, para $r = 4$.

$$Q(x) = \sum_{j=0}^4 a_j x^j = a_0 x^0 + a_1 x^1 + a_2 x^2 + a_3 x^3 + a_4 x^4$$

$$Q^{(1)}(x) = a_1 + 2a_2 x^{2-1} + 3a_3 x^{3-1} + 4a_4 x^{4-1}$$

$$Q^{(2)}(x) = (2-1)2a_2 x^{2-2} + (3-1)3a_3 x^{3-2} + (4-1)4a_4 x^{4-2}$$

$$Q^{(3)}(x) = (3-2)(3-1)3a_3 x^{3-3} + (4-2)(4-1)4a_4 x^{4-3}$$

$$Q^{(4)}(x) = (4-3)(4-2)(4-1)4a_4 x^{4-4}$$

Observe que $Q^{(1)}(x)$, onde $j = 1$.

$$\frac{1!}{(1-1)!} = \frac{1!}{0!} = 1$$

$$\frac{2!}{(2-1)!} = 2 \quad \frac{2!}{(2-1)!} a_2$$

$$\frac{3!}{(3-1)!} = \frac{3!}{2!} = 3 \quad \frac{3!}{(3-1)!} a_3$$

$$\frac{4!}{(4-1)!} = \frac{4!}{3!} = 4 \quad \frac{4!}{(4-1)!} a_4$$

Logo podemos escrever

$$Q^{(1)}(x) = \sum_{j=1}^4 \frac{j!}{(j-1)!} a_j x^{j-1}$$

Analogamente para $j = 2$ temos

$$Q^{(2)}(x) = \sum_{j=2}^4 \frac{j!}{(j-2)!} a_j x^{j-2}$$

para $j = 3$ temos

$$Q^{(3)}(x) = \sum_{j=3}^4 \frac{j!}{(j-3)!} a_j x^{j-3}$$

para $j = 4$ temos

$$Q^{(4)}(x) = \sum_{j=4}^4 \frac{j!}{(j-4)!} a_j x^{j-4}$$

Provemos por Indução a expressão para $Q^{(i)}(x)$.

Verifiquemos se $Q^{(i)}(x)$ é válida.

$$\begin{aligned} Q^{(1)}(x) &= [Q(x)]' = \\ &= \left(\sum_{j=0}^r a_j x^j \right)' = (a_0 x^0 + a_1 x^1 + \dots + a_r x^r)' = \\ &= (a_1 x^{1-1} + (2)a_2 x^{2-1} + \dots + (r)a_r x^{r-1}) = \\ &= \frac{1!}{(1-1)!} a_1 x^{1-1} + \frac{2!}{(2-1)!} a_2 x^{2-1} + \dots + \frac{r!}{(r-1)!} a_r x^{r-1} = \\ &= \sum_{j=1}^r \frac{j!}{(j-1)!} a_j x^{j-1} \end{aligned}$$

portanto $Q^{(1)}(x)$ é válida.

Hipótese de Indução: suponha que $Q^{(k)}(x)$ é válida.

$$Q^{(k)}(x) = \sum_{j=k}^r \frac{j!}{(j-k)!} a_j x^{j-k}$$

Queremos provar que

$$Q^{(k+1)}(x) = \sum_{j=k+1}^r \frac{j!}{(j-(k+1))!} a_j x^{j-(k+1)}$$

é válida.

$$\begin{aligned} Q^{(k+1)}(x) &= (Q^{(k)}(x))' = \left(\sum_{j=k}^r \frac{j!}{(j-k)!} a_j x^{j-k} \right)' = \\ &= \left(\frac{k!}{(k-k)!} a_k x^{k-k} + \frac{(k+1)!}{((k+1)-k)!} a_{k+1} x^{(k+1)-k} + \dots + \frac{r!}{(r-k)!} a_r x^{r-k} \right)' = \\ &= (k+1-k) \frac{(k+1)!}{((k+1)-k)!} a_{k+1} x^{(k+1)-k-1} + \dots + (r-k) \frac{r!}{(r-k)!} a_r x^{r-k-1} \end{aligned}$$

Observe que:

$$\frac{(k+1)!}{((k+1)-k)!} = \frac{(k+1)!}{((k+1)-(k+1))!} \quad (I)$$

$$\frac{r!}{(r-k)!} \frac{(r-k)}{(r-(k+1))} = \frac{r!}{(r-(k+1))!} \quad (II)$$

$$(r-k)! = (r-k)(r-(k+1))!$$

então

$$= \frac{(k+1)!}{((k+1)-(k+1))!} a_{k+1} x^{(k+1)-(k+1)} + \dots + \frac{r!}{(r-(k+1))!} a_r x^{r-(k+1)} =$$

$$\sum_{j=k+1}^r \frac{j!}{(j-(k+1))!} a_j x^{j-(k+1)}$$

logo vale a expressão para $Q^{(k+1)}(x)$.

Portanto pelo Princípio de Indução Finita é válida a expressão para $Q^{(i)}(x)$, $i \leq r$ e $r \in \mathbb{N}$.

□

Lema 4.4. *Sob o contexto do Lema 4.3, $\frac{1}{(p-1)!} Q^{(i)}(x)$, para $i \geq p$, é um polinômio com coeficientes inteiros divisíveis por p .*

Demonstração. Substituindo $Q^{(i)}(x)$ dado no Lema 4.3, temos que

$$\frac{1}{(p-1)!} Q^{(i)}(x) = \frac{1}{(p-1)!} \sum_{j=i}^r \frac{j!}{(j-i)!} a_j x^{j-i} =$$

$$\sum_{j=i}^r \frac{1}{(p-1)!} \frac{j!}{(j-i)!} a_j x^{j-1}$$

logo o polinômio dado acima possui cada coeficiente dado por: $b_j = \frac{1}{(p-1)!} \frac{j!}{(j-i)!} a_j$. Queremos mostrar que cada b_j é um número inteiro e divisível por p , ou seja, queremos mostrar existe $k \in \mathbb{Z}$ tal que: $b_j = pk$.

Para isso, observe que $\frac{1}{(p-1)!} = \frac{p}{p!}$, então: $b_j = \frac{p}{p!} \frac{j!}{(j-i)!} a_j = p a_j \frac{j!}{p!(j-i)!}$.

Considerando $k = a_j \frac{j!}{p!(j-i)!}$ resta mostrar que k é um número inteiro. Como já sabemos por hipótese do Lema 4.3, que $a_j \in \mathbb{Z}$, para mostrar que $k \in \mathbb{Z}$, basta mostrar que $\frac{j!}{p!(j-i)!}$ é um número inteiro. Veja que como $j \geq p$, segue que $j! \geq p!$, assim $\frac{j!}{p!(j-i)!} = \frac{j(j-1)(j-2)\dots(p+1)p!}{p!(j-i)!} = \frac{j(j-1)(j-2)\dots(p+1)}{(j-i)!}$, o qual é obviamente um número inteiro.

□

Lema 4.5. *Considere o polinômio definido no Lema 4.1 como $P(x) = \frac{1}{(p-1)!}x^{p-1}(1-p)^p \dots (n-x)^p$. Então $P(x)$ é da forma $P(x) = \frac{(n!)^p}{(p-1)!}x^{p-1} + \frac{b_0}{(p-1)!}x^p + \dots$*

Demonstração. Note que

$$\begin{aligned} (1-x)^p &= 1 + p(-x) + \dots + p(-x)^{p-1} + (-x)^p \\ (2-x)^p &= 2^p + p2^{p-1}(-x) + \dots + p2(-x)^{p-1} + (-x)^p \\ (3-x)^p &= 3^p + p3^{p-1}(-x) + \dots + p3(-x)^{p-1} + (-x)^p \\ &\vdots \\ (n-x)^p &= n^p + pn^{p-1}(-x) + \dots + pn(-x)^{p-2} + (-x)^p. \end{aligned}$$

Então,

$$\begin{aligned} P(x) &= \frac{1}{(p-1)!}x^{p-2}(1 + p(-x) + \dots + (-x)^p). \\ (2^p + p2^{p-1}(-x) + \dots + (-x)^p) \cdot (3^p + p3^{p-2}(-x) + \dots + (-x)^p) \cdot (n^p + pn^{p-1}(-x) + \dots + (-x)^p) \\ &= \frac{x^{p-1}}{(p-1)!}(1 \cdot 2^p 3^p \dots n^p + p(-x)p2^{p-1}(-x) + p3^{p-1}(-x) + \dots + pn^{p-1}(-x) + \dots) \\ &= \frac{x^{p-1}}{(p-1)!}((n!)^p + x(-p - p2^{p-1} - p3^{p-1} - \dots - pn^{p-1}) + \dots) = \\ &= \frac{x^{p-1}}{(p-1)!}((n!)^p) + xb_0 + \dots = \frac{(n!)^p}{(p-1)!}x^{p-1} + \frac{b_0x^p}{(p-1)!} + \dots \end{aligned}$$

onde $b_0 = -p - p2^{p-1} - p3^{p-1} - \dots - pn^{p-1}$.

Note que $P^{(i)}(k) = 0$; $k = 1, \dots, n, i < p$, pois analisando $P^{(i)}(x)$ para $x = k$, $k \in 1, \dots, n$ possui termos com sinais alternados, os quais quando agrupados resultam zero.

Ainda veja que $P^{(p-1)}(x) = \frac{(n!)^p}{(p-1)!}(p-1)! + \frac{b_0xp!}{(p-1)!} + (\text{parcelas com a variável } x)$

logo $P^{(p-1)}(0) = (n!)^p(p-1)! + \frac{b_0xp!}{(p-1)!} + (\text{parcelas com } x = 0) = (n!)^p$

Para $i < p - 1$ todas as parcelas de $P^{(i)}(x)$ possuem a variável x , logo quando $x = 0$ $P^{(i)}(0) = 0$.

□

Lema 4.6. *Se d_i , $i = 0, 1, \dots, r$ são inteiros, tais que os d_i , para $i \geq 1$ são divisíveis por p , e d_0 não é divisível por p , então $\sum_{i=0}^r d_i$ não é divisível por p .*

Demonstração. Suponha por absurdo que $\sum_{i=0}^r d_i$ seja divisível por p , ou seja,

$$\{\exists k \in \mathbb{Z} : \sum_{i=0}^r d_i = kp\} \quad (*)$$

Como cada d_i é divisível por p , para $1 \leq i \leq r$, $\{\exists k \in \mathbb{Z} : d_i = k_i p, 1 \leq i \leq r\}$

Assim por (*) e (**), temos que:

$$kp = \sum_{i=0}^r d_i = d_0 + d_1 + \dots + d_r = d_0 + (k_1 p) + \dots + (k_r p) = d_0 + (k_1 + \dots + k_r)p$$

$$\Rightarrow d_0 = (kp) - (k_1 + \dots + k_r)p = (k - (k_1 + \dots + k_r))p$$

Como $L = (k - (k_1 + \dots + k_r)) \in \mathbb{Z}$ e $d_0 = Lp$, segue que d_0 é divisível por p .

O que é um absurdo, pois por hipótese temos que d_0 não é divisível por p . \square

Lema 4.7. $F(k)$ para $k = 1, \dots, n$ é um inteiro divisível por p e $F(0)$ não é divisível por p .

Demonstração. Temos que $F(x) = P(x) + P'(x) + \dots + P^{(p)}(x)$ então

$$F(0) = P(0) + P'(0) + \dots + P^{p-2}(0) + P^{p-1}(0) + P^p(0) = P^{p-1}(0) + P^p(0)$$

Observe que $P^p(x) = \frac{b_0 p!}{(p-1)!} + (\text{parcelas com a variável } x)$ então $P^p(0) = \frac{b_0 p!}{(p-1)!} = b_0 p$.

Assim como sabemos que $P^{(p-1)}(0) = (n!)^p$, segue que, $F(0) = (n!)^p + b_0 p$ o qual não pode ser divisível por p , já que se o fosse teríamos que $(n!)^p$ também seria o que é absurdo pois $p > n$ e p é primo.

$$\text{Agora } F(0) = kp \Rightarrow (n!)^p = kp - b_0 p = p(k - b_0)$$

$(n!)^p = (n(n-1)(n-2)\dots 2 \cdot 1)^p = n^p(n-1)^p(n-2)^p\dots 2^p$, note que nenhum termo deste produto é divisível por p , (por exemplo, se n^p o fosse existiria $L \in \mathbb{Z} : n^p = Lp \Rightarrow nn\dots n = Lp \Rightarrow L = \frac{nn\dots n}{p}$ o qual não é um número inteiro já que $p > n$ e p é primo ($\rightarrow \leftarrow$)).

Mostremos agora que $F(k), k \in 1, \dots, n$ é um inteiro divisível por p . Sabemos que

$$F(k) = P(k) + P'(k) + \dots + P^{(p-1)}(k)P^p(k) = F(k)P^p(k) \quad (*)$$

Pelo Lema 4.4 $P^p(x)$ é um polinômio com coeficientes inteiros divisíveis por p . Substituindo $x = k, k \in 1, \dots, n$ temos que:

$P^p(k)$ é uma soma cuja as parcelas são todas inteiras e divisíveis por p , conseqüentemente $P^p(k)$ é um inteiro divisível por p . Portanto por (*) $F(k)$ é divisível por p . \square

Lema 4.8. Como $0 < c_0 < p$, mostre que $c_0 F(0) + c_1 F(1) + \dots + c_n F(n)$ é um inteiro não divisível por p .

Demonstração. Pelo Lema 4.7 temos que $F(k)$ para $k = 1, \dots, n$ é um inteiro divisível por p e $F(0)$ é um inteiro não divisível por p . Conseqüentemente como $c_k \in \mathbb{Z}$ $d_k = c_k F(k)$ para $k = 1, \dots, n$ é um inteiro divisível por p e $d_0 = c_0 F(0)$ é um inteiro não divisível por p , já que $0 < c_0 < p$. Logo pelo Lema 4.6 segue que $\sum_{k=0}^n d_k$ não é divisível por p , mas $\sum_{k=0}^n d_k = d_0 + d_1 + \dots + d_n = c_0 F(0) + c_1 F(1) + \dots + c_n F(n)$.

Portanto $c_0 F(0) + c_1 F(1) + \dots + c_n F(n)$ é um inteiro não divisível por p . \square

Lema 4.9. $|A_k| \leq \frac{e^n n^p (n!)^p}{(p-1)!}$, para $k \leq n$.

Demonstração. Observe que os A_k definidos no Lema 4.2, calculado para o polinômio $P(x)$, definido no Lema 4.5, têm a forma

$$A_k = -k e^{k(1-\theta_k)} \frac{1}{(p-1)!} (k\theta_k)^{p-1} (1-k\theta_k)^p \dots (n-k\theta_k)^p, 0 < \theta < 1.$$

Então,

$$\begin{aligned} |A_k| &= \left| -k e^{k(1-\theta_k)} \frac{1}{(p-1)!} (k\theta_k)^{p-1} (1-k\theta_k)^p \dots (n-k\theta_k)^p \right| = \\ &= \frac{1}{(p-1)!} | -k | | e^{k(1-\theta_k)} | | (k\theta_k)^{p-1} | | (1-k\theta_k)^p | \dots | (n-k\theta_k)^p | \leq \\ &= \frac{1}{(p-1)!} n e^{n(1-\theta_k)} | n\theta_k |^{p-1} | 1-\theta_k |^p \dots | n-\theta_k |^p \leq \\ &= \frac{1}{(p-1)!} n e^n n^{p-1} = \frac{e^n n^p}{(p-1)!} \leq \frac{e^n n^p (n!)^p}{(p-1)!}. \end{aligned}$$

□

Lema 4.10. Se p for um número primo suficiente grande então $|c_1 A_1 + \dots + c_n A_n| < 1$.

Demonstração.

$$\begin{aligned} |c_1 A_1 + \dots + c_n A_n| &\leq |c_1 A_1| + \dots + |c_n A_n| \leq |c_1| \frac{e^n n^p (n!)^p}{(p-1)!} + \dots + |c_n| \frac{e^n n^p (n!)^p}{(p-1)!} = \\ &= (|c_1| + \dots + |c_n|) \frac{e^n n^p (n!)^p}{(p-1)!} \end{aligned}$$

Para p um número primo suficientemente grande temos:

$$|c_1 A_1 + \dots + c_n A_n| \leq (|c_1| + \dots + |c_n|) \frac{e^n n^p (n!)^p}{(p-1)!} < 1$$

□

Teorema 4.1. *O número e é transcendente.*

Demonstração. Pelo Corolário 4.1 supomos que o número e era algébrico, ou seja, existem inteiros c_0, c_1, \dots, c_n (com $c_0 > 0$), tais que $c_n e^n + \dots + c_1 e + c_0 = 0$, temos que $c_0 F(0) + \dots + c_n F(n) = c_1 A_1 + \dots + c_n A_n$, e pelo Lema 4.8, segue que $c_0 F(0) + \dots + c_n F(n)$ é um número inteiro não divisível por p , porém pelo Lema 4.10 temos que nessas mesmas condições que $|c_1 A_1 + \dots + c_n A_n| < 1$, o que é absurdo, já que um número inteiro não nulo tem módulo sempre maior ou igual que 1. O absurdo foi supor que e é um número algébrico. □

5 Sugestão de Aula para o Ensino Médio

Para a sala de aula, a sugestão é uma abordagem dos tópicos estudados através de exemplos. A saber,

Exemplo 5.1. No Capítulo 1 introduzimos a ideia que $\lim_{n \rightarrow \infty} (1 + \frac{1}{n})^n = e$

onde $e = 2,71828182845904523536028747135266\dots$

Com o auxílio de uma calculadora, determine, conforme os exemplos a) e b), o valor da expressão $(1 + \frac{1}{n})^n$ para os seguintes valores de n :

a) $n = 10$

$$(1 + \frac{1}{10})^{10} = 2,5937424601$$

b) $n = 100$

$$(1 + \frac{1}{100})^{100} = 2,70481382942153$$

c) $n = 1000$

d) $n = 10000$

e) $n = 10^5$

f) $n = 6 \cdot 10^{20}$

g) $n = (10!)^{10!}$.

Exemplo 5.2. Mostre que $\sqrt{3}$ é irracional.

Demonstração. Suponhamos por absurdo que $\sqrt{3}$ 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:

$$x^2 = \left(\frac{p}{q}\right)^2 \Rightarrow$$

$$(\sqrt{3})^2 = \left(\frac{p}{q}\right)^2 \Rightarrow$$

$$3 = \frac{p^2}{q^2} \Rightarrow$$

$$3q^2 = p^2.$$

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 $p = 3a$, temos,

$$3q^2 = 9a^2 \Rightarrow$$

$$\frac{3q^2}{3} = \frac{9a^2}{3} \Rightarrow$$

$$q^2 = 3a^2.$$

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. \square

Exercício

Mostre que $\sqrt{2}$ e $\sqrt{5}$ são números irracionais. (Dica: use o Algoritmo da Divisão)

Exemplo 5.3. Usando a definição de Números Algébricos do Capítulo 2, mostre que o número complexo $1 + i$ é algébrico.

Demonstração. Temos que encontrar uma equação do tipo $x^n + a_{n-1}x^{n-1} + \dots + a_1x + a_0 = 0$ com coeficientes inteiros, onde $1 + i$ seja solução. Mas se $1 + i$ é solução, então seu conjugado $1 - i$ também é solução de uma equação do 2º grau. Usando a fórmula da Soma e Produto, temos:

$$(1 + i) + (1 - i) = 2$$

$$(1 + i)(1 - i) = 2$$

consequentemente $1 + i$ e $1 - i$ são soluções da equação $x^2 - 2x + 2 = 0$.

\square

Exercício

Mostre que os números abaixo são algébricos:

-
- a) $-7/3$
b) $2\sqrt{2}$
c) $3 + 5i$
d) $\frac{1 + \sqrt{5}}{2}$ (número áureo)
e) $\sqrt{\sqrt{2} + 3}$.

Exemplo 5.4. Mostre que o número real irracional e não é solução de uma equação do 1º grau com coeficientes inteiros.

Demonstração. Uma equação do 1º grau pode ser escrita da forma $ax + b = 0$, onde $a, b \in \mathbb{Z}$.

Temos que $x = \frac{-b}{a}$, como a e b são inteiros, portanto x é um número racional, ou seja, e que é irracional não pode ser solução dessa equação.

□

Exercício

Mostre que o número real irracional e não é solução de uma Equação do 2º grau com coeficientes inteiros.

Referências

- [1] FIGUEIREDO, Djairo L. Números Irracionais e Transcendentes - 3. ed. SBM, 2002.
- [2] MAOR, Eli e: A História de um Número -Tradução de Jorge Calife - 7. ed. Editora Record, 2012.