O método de Diofanto e a curva $a^b = b^a$

Maria Pires de Carvalho[1], *Alberto Cavaleiro Pacheco*[2]

Centro de Matemática da Universidade do Porto
Faculdade de Ciências da Universidade do Porto
Rua do Campo Alegre 687
4169-007 Porto, Portugal
e-mail: `mpcarval@fc.up.pt`; `up201605820@fc.up.pt`

Resumo: A curva descrita pelos pares (a, b) no plano tais que a, $b > 0$, $a \neq b$ e $a^b = b^a$ é parametrizável pelos declives $0 < t \neq 1$ do feixe de rectas de equações cartesianas $y = tx$, o que permite descrever facilmente os pontos do traço desta curva cujas coordenadas são ambas números algébricos, ou inteiros algébricos ou racionais. Em particular, uma tal parametrização fornece um método simples de encontrar coordenadas de pontos desta curva que são números transcendentes.

Abstract: The curve described by the pairs (a, b) in the plane satisfying a, $b > 0$, $a \neq b$ and $a^b = b^a$ is parameterizable by the slopes $0 < t \neq 1$ of the straight lines whose Cartesian equations are given by $y = tx$. This information allows us to easily detect those pairs whose coordinates are algebraic over the field of the rational numbers, or are algebraic integers, or else are both rational. In particular, such a parametrization provides a simple criterium to find coordinates of points of this curve which are transcendental numbers.

palavras-chave: Número algébrico sobre $\mathbb{Q}$; inteiro algébrico.
keywords: Algebraic number over $\mathbb{Q}$; algebraic integer.

---

[1]MC tem sido financiada pelo CMUP (UID/MAT/00144/2013), que é suportado financeiramente pela FCT com fundos nacionais (MEC) e europeus, através dos programas FEDER e no âmbito do acordo PT2020. Os autores agradecem ao revisor os comentários e sugestões.

[2]Este artigo foi escrito no âmbito do *Programa Novos Talentos em Matemática*, da Fundação Calouste Gulbenkian.

1 A equação $a^b = b^a$, para a, $b > 0$

Para que valores reais de $a, b > 0$ se tem $a^b = b^a$? A igualdade é óbvia quando $a = b$. Para valores distintos de a e b, se reescrevermos a equação $a^b = b^a$ como $a^{\frac{1}{a}} = b^{\frac{1}{b}}$ e esboçarmos o gráfico da função $x > 0 \mapsto f(x) = x^{\frac{1}{x}}$, ilustrado na Figura 1, teremos uma ideia aproximada dos valores da imagem de f que são obtidos mais do que uma vez (e, nesse caso, exactamente duas vezes).

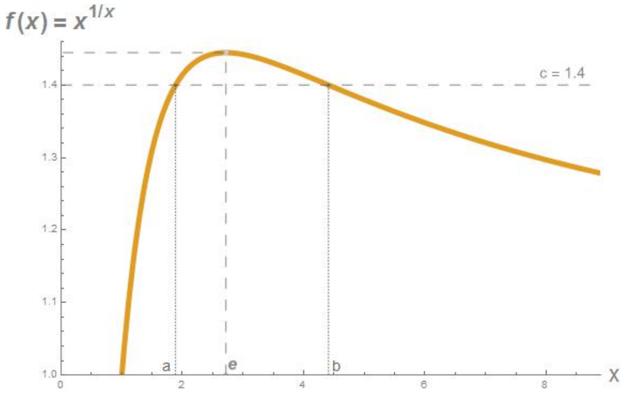


Figura 1: Gráfico da função f.

Esta função tem um máximo global $e^{\frac{1}{e}}$, atingido apenas em $x = e$, e é estritamente crescente em $]0, e[$ e estritamente decrescente em $]e, +\infty[$. Além disso,

$$\lim_{x\to 0^+} f(x) = 0^+ \quad \text{e} \quad \lim_{x\to +\infty} f(x) = 1^+.$$

Logo, cada recta horizontal $y = c$ com $1 < c < e^{\frac{1}{e}}$ (e só para estes valores de c) intersecta o gráfico de f em dois pontos cujas abcissas determinam dois reais positivos distintos a e b tais que $a^{\frac{1}{a}} = b^{\frac{1}{b}}$, ou seja, $a^b = b^a$. Mais precisamente, dado $c \in \,]1, e^{\frac{1}{e}}[$, existe um e um só $b > e$ tal que $f(b) = b^{\frac{1}{b}} = c$; se agora resolvermos a equação $a^{\frac{1}{a}} = c$ com a incógnita $a \in \,]1, e[$, determinamos o outro valor a do domínio de f tal que $f(a) = f(b) = c$.

Para descrever o lugar geométrico de tais pares (a, b) com $a \neq b$, usemos o feixe de rectas $y = tx$ com declive $t \in \mathbb{R}^+ \setminus \{1\}$ que, como um radar, permite detectá-los no 1º quadrante de $\mathbb{R}^2$ (veja-se em [2] outra instância em que este método, atribuído a Diofanto, é usado). Para cada t, determinamos a intersecção das condições $y = tx$ e $x^y = y^x$ resolvendo em conjunto as equações

$$\frac{y}{x} = t \quad \text{ e } \quad x^{\frac{y}{x}} = y.$$

Obtemos então $x^t = tx$, logo $x = t^{\frac{1}{t-1}}$; e, como $y = tx = x^t$, tem-se $y = t^{\frac{t}{t-1}}$. As soluções descrevem a curva α em $\mathbb{R}^+ \times \mathbb{R}^+$, cujo traço está esboçado na Figura 2, parametrizada por

$$\alpha\colon t \in \mathbb{R}^+ \setminus \{1\} \quad \mapsto \quad \left(t^{\frac{1}{t-1}}, t^{\frac{t}{t-1}}\right).$$

Observe-se que o traço de α, que designaremos por $\mathcal{T}_\alpha$, é simétrico relativamente à bissectriz do 1º quadrante (a semirecta de equação $y = x$, $x \geq 0$) uma vez que, se fixarmos $t > 0$ e o par correspondente $\alpha(t) = (a_t, b_t) = \left(t^{\frac{1}{t-1}}, t^{\frac{t}{t-1}}\right)$ de α, então $\frac{1}{t}$ determina o ponto $\alpha(\frac{1}{t}) = (b_t, a_t)$ da mesma curva. Além disso, $\alpha(t)$ converge para (e, e) quando t tende para 1. Note-se ainda que as coordenadas dos pontos desta curva são ambas estritamente maiores do que 1, propriedade que resulta de só surgirem tais pares com abcissas no subconjunto $]1, +\infty[$ do domínio da função f.

Se a $\mathcal{T}_\alpha$ juntarmos a semirecta $\{(a, a) : a \in \mathbb{R}^+\}$, obtemos o conjunto $\mathfrak{X}$ de todos os pares $(a, b) \in \mathbb{R}^+ \times \mathbb{R}^+$ tais que $a^b = b^a$. Os conjuntos $\mathcal{T}_\alpha$ e $\mathfrak{X}$ estão representados na Figura 2. (Esta figura consta do artigo [1], onde se analisaram as soluções reais e complexas da equação $a^b = b^a$.) Os dois ramos de $\mathfrak{X}$ intersectam-se precisamente no ponto (e, e) e dividem $\mathbb{R}^+ \times \mathbb{R}^+$ em quatro regiões em cada uma das quais o sinal da diferença $a^b - b^a$, que varia continuamente com a e b, se mantém constante. Em particular, como a recta vertical $x = e$ só intersecta as regiões em que este sinal é positivo (uma vez que são gráficos de funções, $\mathcal{T}_\alpha$ e $\mathfrak{X}$ intersectam cada recta vertical quando muito uma vez), concluímos que, para todos os valores de $0 < x \neq e$, se tem $e^x > x^e$ (por exemplo, $e^\pi > \pi^e$).

Designemos por $\mathcal{A}$ o conjunto de números reais algébricos sobre $\mathbb{Q}$ e por $\mathcal{A}_\mathbb{Z}$ o seu subconjunto dos inteiros algébricos (definições na Secção 2). O objectivo deste texto é o de localizar pontos de $\mathcal{T}_\alpha$ cujas coordenadas sejam ambas racionais, ou ambas números algébricos. Recorde-se que, uma vez que o ponto do traço de α determinado por $\frac{1}{t}$ é (b_t, a_t), bastará analisar estas coordenadas para $t \in]0, 1[$. A tabela seguinte resume o que de mais relevante

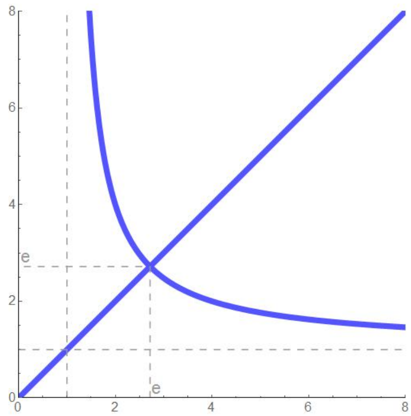


Figura 2: Os conjuntos $\mathcal{T}_\alpha$ e $\mathfrak{X}$.

aqui se provará sobre as coordenadas dos pontos (a_t, b_t) de $\mathcal{T}_\alpha$ para valores de $t \in]0, +\infty[\setminus\{1\}$:

1. (a_t, b_t) tem ambas as coordenadas algébricas se e só se $t \in \mathbb{Q}^+ \setminus \{1\}$.
2. (a_t, b_t) tem ambas as coordenadas racionais se e só se $t = \frac{n}{n+1}$ ou $t = \frac{n+1}{n}$ para algum $n \in \mathbb{N}$.
3. (a_t, b_t) tem ambas as coordenadas inteiras algébricas se e só se $t = 1/n$ ou $t = n$ para algum $n \in \mathbb{N} \setminus \{1\}$.

$0 < t < 1$	Domínio a que pertence (a_t, b_t)	a_t	b_t
$\frac{n}{m}$ $(n, m \in \mathbb{N})$	$\mathcal{A} \times \mathcal{A}$	$\left(\frac{m}{n}\right)^{\frac{m}{m-n}}$	$\left(\frac{m}{n}\right)^{\frac{n}{m-n}}$
$\frac{n}{n+1}$ $(n \in \mathbb{N})$	$\mathbb{Q} \times \mathbb{Q}$	$\left(\frac{n+1}{n}\right)^{n+1}$	$\left(\frac{n+1}{n}\right)^{n}$
$\frac{1}{m}$ $(m \in \mathbb{N},\ m > 1)$	$\mathcal{A}_\mathbb{Z} \times \mathcal{A}_\mathbb{Z}$	$\sqrt[m-1]{m^m}$	$\sqrt[m-1]{m}$
$\frac{1}{2}$	$\mathbb{N} \times \mathbb{N}$	4	2

Em particular, resulta deste estudo que, quando a é um natural maior do que 1 e b é um real positivo tal que $a^b = b^a$, então $a = b$ ou $\{a, b\} = \{2, 4\}$ ou b é um número transcendente.

2 O corpo $\mathcal{A}$ dos números algébricos

Um número real diz-se algébrico sobre $\mathbb{Q}$ (ou, simplesmente, *algébrico*) se for zero de um polinómio não nulo com coeficientes racionais. Por exemplo, os números racionais são algébricos (pois a fracção irredutível $\frac{p}{q}$, com $p \in \mathbb{Z}$ e $q \in \mathbb{N}$, anula o polinómio $qx - p$); $\sqrt{2}$ é algébrico uma vez que é raiz de $x^2 - 2$; e $\sqrt{2} + \sqrt{3}$ também é algébrico já que é zero do polinómio $x^4 - 10x^2 + 1$:

$$\begin{aligned} \left(\sqrt{2}+\sqrt{3}\right)^2 &= 5 + 2\sqrt{6} \\ \left([\sqrt{2}+\sqrt{3}]^2 - 5\right)^2 &= 24 \\ \left(\sqrt{2}+\sqrt{3}\right)^4 - 10\left(\sqrt{2}+\sqrt{3}\right)^2 + 1 &= 0. \end{aligned}$$

O *grau* de um número algébrico z é o menor natural n tal que z é zero de um polinómio não nulo com coeficientes racionais e grau n. Por exemplo, os racionais são os algébricos de grau 1; $\sqrt{2}$ tem grau 2; $\sqrt{2} + \sqrt{3}$ é de grau 4.

Parece difícil demonstrá-lo, por a noção de número algébrico depender de propriedades da família dos polinómios, mas o conjunto dos números algébricos sobre $\mathbb{Q}$ com a soma e produto usuais forma um corpo, que designaremos por $\mathcal{A}$, que até é fechado para a operação de exponenciação por potências racionais. Demonstrações detalhadas destas e de outras propriedades de $\mathcal{A}$ podem ser lidas em [12] ou [14]. Resumiremos aqui o essencial deste argumento. Consideremos $z, w \in \mathcal{A}$, e sejam

$$\mathcal{P}\colon x \in \mathbb{R} \mapsto c_n x^n + \cdots + c_1 x + c_0 \quad \text{e} \quad \mathcal{Q}\colon x \in \mathbb{R} \mapsto d_m x^m + \cdots + d_1 x + d_0$$

dois polinómios não nulos com coeficientes racionais que se anulam, respectivamente, em z e em w. Então:

1. Se $\mathcal{P}^-$ é o polinómio definido por $x \in \mathbb{R} \mapsto \mathcal{P}(-x)$, então P^- tem coeficientes racionais (os mesmos de $\mathcal{P}$, a menos de sinal nas parcelas de grau ímpar) que se anula em $-z$. Assim sendo, $-z$ é algébrico.

2. Se $z \neq 0$ e $\mathcal{P}$ tem grau n, com coeficiente $c_j \in \mathbb{Q}$ de x^j para cada $j \in \{0, 1, \cdots, n\}$, seja $\mathcal{P}^{\div}$ o polinómio

$$x \in \mathbb{R} \mapsto \mathcal{P}^{\div}(x) = \begin{cases} x^n\, P(\frac{1}{x}) & \text{se } x \neq 0 \\ c_n & \text{se } x = 0 \end{cases}$$

Então, $\mathcal{P}^{\div}$ tem coeficientes racionais (os mesmos de $\mathcal{P}$, mas c_j é agora coeficiente da potência x^{n-j}, para $0 \leq j \leq n$) que se anula em $\frac{1}{z}$. O que confirma que $\frac{1}{z}$ é algébrico.

3. Sejam $k \in \mathbb{N}$, $k \geq 2$, e $\mathcal{P}^{\wedge}$ o polinómio $x \in \mathbb{R} \mapsto \mathcal{P}(x^k)$. Então, $\mathcal{P}^{\wedge}$ é também um polinómio de coeficientes racionais (os de $\mathcal{P}$) que se anula em $\sqrt[k]{z}$. Logo $\sqrt[k]{z}$ é algébrico. Note-se que esta raiz é um número real para todo o natural ímpar k e, se k é par, quando $z > 0$.

4. Suponhamos que os graus dos polinómios $\mathcal{P}$ e $\mathcal{Q}$ são n e m, respectivamente. Então, existem racionais $(c_i)_{i \in \{0,1,\cdots,n\}}$ e $(d_j)_{j \in \{0,1,\cdots,m\}}$ tais que

$$z^n = c_{n-1}z^{n-1} + \cdots + c_1 z + c_0 \quad \text{e} \quad w^m = d_{m-1}w^{m-1} + \cdots + d_1 w + d_0. \quad (1)$$

Multiplicando a primeira igualdade de (1) por z, concluimos que z^{n+1} é também combinação linear finita sobre o corpo $\mathbb{Q}$ de $\{1, z, \ldots, z^{n-1}\}$. Por indução finita, deduzimos que, para todo o $k \in \mathbb{N}$, a potência z^k é combinação linear finita sobre $\mathbb{Q}$ de $1, z, \ldots, z^{n-1}$. Analogamente se conclui que w^k é combinação linear finita sobre o corpo $\mathbb{Q}$ de $\{1, w, \ldots, w^{m-1}\}$, para todo o $k \in \mathbb{N}$. Mais geralmente, todos os elementos do conjunto $\{1, z + w, (z + w)^2, \ldots, (z + w)^{nm}\}$ são combinações lineares finitas sobre $\mathbb{Q}$ das nm parcelas $z^i\, w^j$, com $i \in \{0, 1, \ldots, n - 1\}$ e $j \in \{0, 1, \ldots, m - 1\}$. Desta forma, temos $mn + 1$ vetores num subespaço vectorial sobre o corpo $\mathbb{Q}$ gerado por mn vetores. E, portanto, esses $mn+1$ vetores são linearmente dependentes sobre $\mathbb{Q}$. Ou seja, existem racionais $e_0, \ldots, e_{mn}$ não todos nulos tais que $e_0 + e_1(z + w) + \cdots + e_{mn}(z + w)^{mn} = 0$. O que prova que $z + w$ é algébrico.

Analogamente, as potências $\{1, zw, (zw)^2, \ldots, (zw)^{nm}\}$ são combinações lineares finitas sobre $\mathbb{Q}$ das nm parcelas $z^i\, w^j$, para $i \in \{0, 1, \ldots, n-1\}$ e $j \in \{0, 1, \ldots, m - 1\}$. Consequentemente, estes $mn + 1$ vetores são linearmente dependentes sobre $\mathbb{Q}$. Isto é, existem racionais $E_0, \ldots, E_{mn}$ não todos nulos tais que $E_0 + E_1\, zw + \cdots + E_{mn}\, (zw)^{mn} = 0$. Logo zw é algébrico.

2.1 O anel $\mathcal{A}_{\mathbb{Z}}$ dos inteiros algébricos

Um número real diz-se um inteiro algébrico sobre $\mathbb{Q}$ (ou, simplesmente, *um inteiro algébrico*) quando é algébrico e zero de um polinómio mónico com coeficientes inteiros. Por exemplo, cada número inteiro z é inteiro algébrico (por ser zero do polinómio $x \in \mathbb{R} \mapsto x - z$); $\sqrt{3}$ também, já que anula o polinómio $x^2 - 3$; e $\sqrt[3]{2} + 1$, que anula o polinómio $(x-1)^3 - 2 = x^3 - 3x^2 + 3x - 3$, também é inteiro algébrico. O conjunto dos inteiros algébricos, que designaremos por $\mathcal{A}_{\mathbb{Z}}$, forma um anel com a soma e produto usuais, que também é fechado para a operação de exponenciação por potências racionais.

Relativamente aos argumentos de (1) e (3) da subsecção anterior, temos apenas de observar que, se $\mathcal{P}$ é mónico e tem coeficientes inteiros, então o mesmo vale para os polinómios $\mathcal{P}^-$ e $\mathcal{P}^\wedge$. Quanto a $\mathcal{P}^\div$, o argumento de (2) não funciona, a não ser que c_0 seja ± 1, pois c_0 é o coeficiente de x^n em $\mathcal{P}^\div$. Por exemplo, apesar de 2 ser inteiro algébrico, o racional $\frac{1}{2}$ não o é porque os zeros racionais de qualquer polinómio mónico com coeficientes inteiros são números inteiros (a propósito, veja-se o início da Secção 6).

Finalmente, o argumento de (4) também não se apropria pois $\mathbb{Z}$ não é um corpo. Contudo, é ainda verdade que, se z e w são inteiros algébricos, então zw e $z+w$ também o são. Sejam $\mathcal{P}\colon x \in \mathbb{R} \mapsto x^n + \cdots + c_1 x + c_0$ e $\mathcal{Q}\colon x \in \mathbb{R} \mapsto x^m + \cdots + d_1 x + d_0$ dois polinómios não nulos com coeficientes inteiros que se anulam, respectivamente, em z e em w. As funções $\mathcal{P}$ e $\mathcal{Q}$ são os polinómios característicos de duas matrizes quadradas A e B com entradas inteiras, nomeadamente

$$A = \begin{pmatrix} 0 & 0 & 0 & \cdots & 0 & c_0 \\ 1 & 0 & 0 & \cdots & 0 & c_1 \\ 0 & 1 & 0 & \cdots & 0 & c_2 \\ \vdots & & & & & \vdots \\ 0 & 0 & \cdots & 0 & 1 & c_{n-1} \end{pmatrix} \quad \text{e} \quad B = \begin{pmatrix} 0 & 0 & 0 & \cdots & 0 & d_0 \\ 1 & 0 & 0 & \cdots & 0 & d_1 \\ 0 & 1 & 0 & \cdots & 0 & d_2 \\ \vdots & & & & & \vdots \\ 0 & 0 & \cdots & 0 & 1 & d_{m-1} \end{pmatrix}.$$

Formemos o produto de Kronecker[3] entre as matrizes A e B; obtemos uma matriz quadrada $A \otimes B$, de dimensões $mn \times mn$, cujo conjunto de valores próprios contém zw. Além disso, como a matriz $A \otimes B$ tem entradas inteiras,

[3] O produto de Knonecker de duas matrizes $C = (c_{ij})_{i=1,\cdots,m;\, j=1,\cdots,n}$ e $D = (d_{k\ell})_{k=1,\cdots,p;\, j=1,\cdots,q}$, com dimensões $m \times n$ e $p \times q$, é a matriz $C \otimes D$ que tem mp linhas e nq colunas e cujas entradas são dadas por $e_{\theta\eta} = c_{ij}\, d_{k\ell}$, onde $\theta = p(i-1) + k$ e $\eta = q(j-1) + \ell$. Por exemplo, o produto de Kronecker entre uma matriz C quadrada

o seu polinómio característico é não nulo, mónico e tem coeficientes inteiros, o que prova que zw é inteiro algébrico. Analogamente, se considerarmos a soma de Kronecker $A \otimes Id_{m\times m} + Id_{n\times n} \otimes B$, onde $Id_{k\times k}$ designa a matriz identidade com k linhas, que tem entradas inteiras e $z+w$ como valor próprio, concluimos que $z+w$ é inteiro algébrico.

Por exemplo, consideremos $z = \sqrt{2}$, $w = \sqrt[3]{5}$, $\mathcal{P}(x) = x^2 - 2$ e $\mathcal{Q}(x) = x^3 - 5$. Então

$$A = \begin{pmatrix} 0 & 2 \\ 1 & 0 \end{pmatrix} \quad \text{e} \quad B = \begin{pmatrix} 0 & 0 & 5 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$$

e o produto zw é valor próprio da matriz

$$A \otimes B = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 10 \\ 0 & 0 & 0 & 2 & 0 & 0 \\ 0 & 0 & 0 & 0 & 2 & 0 \\ 0 & 0 & 5 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

O polinómio característico de $A \otimes B$ é $x^6 - 200$, cujas raízes reais são precisamente $\pm\sqrt{2}\,\sqrt[3]{5}$. No Capítulo VI de [14] pode ler-se um outro argumento, usando funções simétricas, para demonstrar que $\mathcal{A}_{\mathbb{Z}}$, com a soma e produto usuais em $\mathbb{R}$, é um anel.

2.2 $\mathbb{R} \setminus \mathcal{A}$

O conjunto dos números algébricos sobre $\mathbb{Q}$ é infinito (pois contém $\mathbb{Q}$) e numerável, uma vez que os seus elementos são os da união numerável, indexada por $k \in \mathbb{N}$ e por $(c_0, c_1 \cdots, c_k) \in \mathbb{Q}^k \times (\mathbb{Q} \setminus \{0\})$, dos conjuntos (finitos) dos zeros dos polinómios de grau k com coeficientes $c_0, c_1 \cdots, c_k$. Como a união de dois conjuntos numeráveis é numerável e $\mathbb{R}$ não é numerável (pode ler-se o argumento de Cantor que prova esta última afirmação no primeiro

2×2 e uma matriz D que seja 3×2 é a matriz 6×4 representada por

$$C \otimes D = \begin{pmatrix} c_{11}D & c_{12}D \\ c_{21}D & c_{22}D \end{pmatrix}.$$

capítulo de [13]; uma outra demonstração consta de [3]), o complementar de $\mathcal{A}$ em $\mathbb{R}$, formado pelos números *transcendentes*, é não vazio. Não é fácil exibir exemplos concretos de números transcendentes, e é, em geral, bastante difícil provar que um número em particular é transcendente. Na verdade, ainda há números reais sobre os quais não se sabe se são irracionais, quanto mais se são transcendentes. A dificuldade está na definição deste tipo de números: para se provar que um número é algébrico basta encontrar um polinómio não nulo de coeficientes racionais de que o número seja raiz; pelo contrário, para se garantir que um número é transcendente há que confirmar que ele não anula nenhum polinómio não nulo de coeficientes racionais, e esta família é vasta. Por isso, são úteis os critérios expeditos de verificação da algebricidade de um número, alguns dos quais mencionaremos brevemente de seguida.

Liouville apresentou em [10] uma outra prova da existência de números transcendentes e o seu argumento permite construir exemplos destes números. Liouville demonstrou que, para qualquer número real algébrico z de grau $n > 1$, existe um natural M tal que, para todos os inteiros p e $q > 0$, se tem

$$\left|z - \frac{p}{q}\right| > \frac{1}{M\,q^n}.$$

Daqui resulta que, se um real z for irracional e, para todo o natural m, existirem inteiros p e $q > 1$ tais que $\left|z - \frac{p}{q}\right| < \frac{1}{q^m}$, então z é transcendente. Tais z's muito bem aproximados por racionais chamam-se *números de Liouville*. De facto, suponhamos que um tal z é algébrico de grau n (sendo $n > 1$ por z ser irracional). Então existiria um natural M tal que $\left|z - \frac{p}{q}\right| > \frac{1}{M\,q^n}$ para todos os inteiros p e $q > 0$. Tome-se, porém, um natural k tal que

$$2^k \geq 2^n M$$

que existe porque $\mathbb{N}$ não é majorado, e verifica $k \geq n$ por M ser um natural. Sendo z um número de Liouville, existem inteiros p e $q > 1$ tais que

$$\left|z - \frac{p}{q}\right| < \frac{1}{q^k}$$

e, portanto, devemos ter $\frac{1}{q^k} > \frac{1}{M\,q^n}$, ou seja,

$$M > q^{k-n} \geq 2^{k-n} \geq M.$$

Esta contradição indica que números como os de Liouville não podem ser algébricos.

Com este critério, Liouville gerou o primeiro número transcendente conhecido: $L = \sum_{j=1}^{+\infty} \frac{1}{10^{j!}}$. Este número é irracional, uma vez que tem uma dízima infinita não periódica, e, dado um natural m, se considerarmos os inteiros $q = 10^{m!}$ e $p = q \sum_{j=1}^{m} \frac{1}{10^{j!}}$, obtemos

$$\begin{aligned}\left|L - \frac{p}{q}\right| &= \left|\sum_{j=1}^{+\infty} \frac{1}{10^{j!}} - \sum_{j=1}^{m} \frac{1}{10^{j!}}\right| = \sum_{j=m+1}^{+\infty} \frac{1}{10^{j!}} < \frac{9}{10^{(m+1)!}} \sum_{j=0}^{+\infty} \frac{1}{10^{j}} \\ &= \frac{10}{10^{(m+1)!}} < \frac{10^{m!}}{10^{(m+1)!}} = \frac{1}{10^{m(m)!}} = \frac{1}{q^m}.\end{aligned}$$

E, portanto, L é um número de Liouville, logo transcendente.

O conjunto $\mathcal{L}$ de números de Liouville é residual (isto é, intersecção numerável de abertos densos) de $\mathbb{R}$, logo é denso em $\mathbb{R}$. Contudo, tem medida de Lebesgue nula: dado $\varepsilon > 0$, existe uma sucessão de intervalos $(I_n)_{n\in\mathbb{N}}$ tal que $\sum_{n=1}^{+\infty} |I_n| < \varepsilon$ e

$$\mathcal{L} \subset \bigcup_{n\in\mathbb{N}} I_n.$$

Pode ler-se mais informação sobre $\mathcal{L}$ nos capítulos 3 e 7 de [12].

Usando outro tipo de argumento, em 1873 Hermite [7] provou que e é transcendente e, pouco depois, Lindemann [9] e Weierstrass [16] generalizaram esse método, demonstrando que π é transcendente, assim encerrando o celebrado problema sobre a impossibilidade de construir, com régua não graduada e compasso, um quadrado com área igual à de um círculo. Por estas referências, ficamos a saber que são também transcendentes os números

- e^x, $\text{sen}(x)$, $\cos(x)$, $\text{tg}(x)$, para todo o número algébrico $x \neq 0$;
- $\log(x)$, $\text{arcsen}(x)$, $\arccos(x)$, $\arctan(x)$, para todo o número algébrico $x \notin \{0, 1\}$ do domínio destas funções.

Estes dois resultados são casos particulares de um teorema posterior, provado em 1934 por A. O. Gelfond [6] e, independentemente, através de uma solução mais elementar, em 1935 por Th. Schneider [15]. Na referência [12] pode ler-se uma demonstração primorosa do que é agora conhecido como Teorema de Gelfond-Schneider. Estes autores resolveram o sétimo problema proposto por Hilbert [8] e criaram um gerador simples de números transcendentes. Ora acontece que os números associados à equação $a^b = b^a$ se encaixam muito bem nesse teorema porque ele garante que, *se a, b são números algébricos, $a \notin \{0,1\}$ e $b \in \mathbb{R} \setminus \mathbb{Q}$, então a^b é transcendente.* Este resultado prova que, por exemplo, são transcendentes os números $2^{\sqrt{2}}$, $\log_{10}(2)$, e^{π}; e os que analisaremos neste texto.

Todavia, sobram ainda reais a que nenhum destes teoremas, ou outros, se aplica, como 2^e ou $\pi + e$. Neste contexto, é curioso referir um resultado de Mahler (veja-se [11] ou [4]) que prova, em particular, que se f é a função $x \in \mathbb{R} \mapsto f(x) = \frac{x(x+1)}{2}$, então é transcendente o número cuja dízima é

$$0.f(1)\,f(2)\,\cdots f(n)\cdots = 0.1361015\cdots.$$

3 A equação $n^x = x^n$, para $n \in \mathbb{N} \setminus \{1\}$ e $x \in \mathbb{R}$

Fixemos um natural $n > 1$. Na Secção 1 verificámos que a equação $n^x = x^n$ tem duas soluções positivas, nomeadamente $x_1(n) = n$ e $x_2(n) = t^{\frac{t}{t-1}}$, sendo t o único real de $]0,1[\cup\{2\}$ tal que $n = t^{\frac{1}{t-1}}$ (cf. Figura 3). Em particular, $x_2(2) = 4$, $x_2(4) = 2$ e $x_2(n) \in\,]1,e[$ se $n \geq 3$, sendo $\lim_{n\to+\infty} x_2(n) = 1^+$.

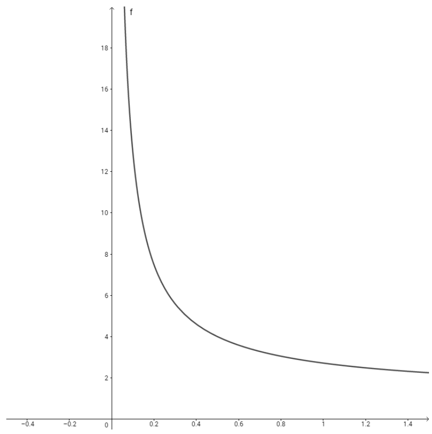
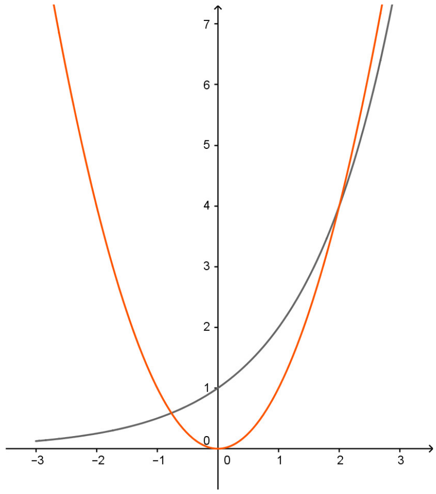


Figura 3: Gráfico da função $t \mapsto t^{\frac{1}{t-1}}$.

Mas, ao contrário do que acontece com a equação geral $a^b = b^a$ em que, para nos mantermos no domínio dos reais, precisamos que a e b sejam positivos, a equação $n^x = x^n$ também é válida para $x \in]-\infty, 0[$ e, dependendo da paridade de n, pode ter soluções neste intervalo. A Figura 4 mostra a existência de uma tal solução negativa quando $n = 2$; na mesma figura à direita podemos notar por que não existem soluções negativas quando $n = 3$. Mais geralmente, quando n é ímpar, a igualdade $n^x = x^n$ não é verificada por nenhum real negativo uma vez que, se $x < 0$, temos $x^n < 0$ e $n^x = e^{x \log n} > 0$.



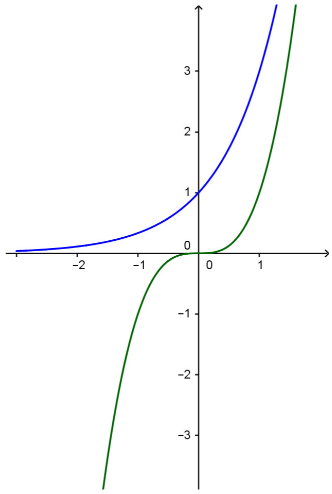


Figura 4: Gráficos das funções $x \in \mathbb{R} \mapsto x^2$ e $x \in \mathbb{R} \mapsto 2^x$; e, à direita, $x \in \mathbb{R} \mapsto x^3$ e $x \in \mathbb{R} \mapsto 3^x$.

Suponhamos agora que n é par e consideremos as funções

$$\mathcal{F}\colon x \in \mathbb{R} \mapsto n^x \quad \text{e} \quad \mathcal{G}\colon x \in \mathbb{R} \mapsto x^n.$$

Então, por n ser par, temos

$$\begin{aligned} (\mathcal{F} - \mathcal{G})(-1) &= \frac{1}{n} - (-1)^n = \frac{1}{n} - 1 < 0 \\ (\mathcal{F} - \mathcal{G})(0) &= 1 - 0 > 0 \end{aligned}$$

e, portanto, como $\mathcal{F} - \mathcal{G}$ é contínua, pelo Teorema do Valor Intermédio existe um zero da função $\mathcal{F} - \mathcal{G}$ em $]-1, 0[$; ou seja, existe um real negativo

$x_3(n) \in]-1,0[$ tal que $n^{x_3(n)} = (x_3(n))^n$. Por outro lado, a derivada de $\mathcal{F} - \mathcal{G}$ é dada por

$$x \in \mathbb{R} \quad \mapsto \quad (\log n)\, n^x - n\, x^{n-1}$$

função que, como $n-1$ é natural ímpar, é positiva no intervalo $]-\infty,0[$. Consequentemente, a restrição a $]-\infty,0[$ da função $\mathcal{F} - \mathcal{G}$ é injectiva e, por isso, o zero $x_3(n)$ em $]-\infty,0[$ de $\mathcal{F} - \mathcal{G}$ é único.

Observe-se, finalmente, que para n par se tem $(x_3(n))^n = (-x_3(n))^n$ e

$$n^{x_3(n)} = (x_3(n))^n \quad \Leftrightarrow \quad \frac{\log n}{n} = \frac{\log(-x_3(n))}{x_3(n)}.$$

Logo, como $\lim_{n\to+\infty} \frac{\log n}{n} = 0$ e $x_3(n) \in]-1,0[$ para todo o n par, devemos ter

$$\lim_{n \text{ par} \to +\infty} x_3(n) = -1.$$

3.1 Irracionalidade de $x_2(n)_{n\neq 1,\,2,\,4}$ e de $x_3(n)_{n \text{ par}}$

Fixemos um natural $n > 1$. No que se segue, verificaremos que $x_2(n)$ é irracional quando $n \neq 2,4$ e que, para n par, $x_3(n)$ é sempre irracional.

Comecemos por analisar o caso de $x_2(n)$. Recorde-se que, para $n \geq 3$, $x_2(n)$ está em $]1,e[$; em particular, $x_2(n)$ é um inteiro se e só se $x_2(n) = 2$, o que é equivalente a $n = 4$. Suponhamos que para algum valor de $n \neq 4$ se tem $x_2(n)$ racional. Se representarmos $x_2(n)$ pela sua fracção irredutível $\frac{p}{q}$, onde $p,q \in \mathbb{N}$ são tais que $mdc\,(p,q) = 1$, a igualdade $n^{\frac{p}{q}} = (\frac{p}{q})^n$ é equivalente a $n^p\, q^{nq} = p^{nq}$, o que implica que $q = 1$ por q ser primo com p. Temos então de resolver em $\mathcal{Z} = \{z \in \mathbb{N}\colon z > 1\}$ a equação $n^p = p^n$. Ora, é uma consequência simples do facto de a equação $n^x = x^n$ só ter duas soluções, nomeadamente $x_1(n) = n$ e $x_2(n) \in]1,e[$ se $n \geq 3$, que as únicas soluções $n,p \in \mathcal{Z}$ desta equação são (n,n), $(2,4)$ e $(4,2)$. Logo, se $n \neq 2,4$, o número $x_2(n)$ é irracional.

Quanto a $x_3(n)$, que só existe quando n é par e está no intervalo $]-1,0[$, se, para algum valor de n, $x_3(n)$ fosse uma fracção irredutível $-\frac{p}{q}$, onde $p,q \in \mathbb{N}$ são tais que $mdc\,(p,q) = 1$, então, como no caso anterior, concluiríamos que $p = 1$ (logo $q > 1$ pois $x_3(n) > -1$) e que q teria de ser solução da equação $n = q^{nq}$. Contudo, para todo o par de números naturais $n,q > 1$, tem-se

$q^n > n$. De facto, é fácil provar por indução finita que, para todo o natural $n > 1$ se tem $2^n > n$: $2^2 > 2$; e se, para um natural $k > 1$ fixado, se tem $2^k > k$, então, como $k > 1$, $2^{k+1} = 2^k \times 2 > 2k > k + 1$. Logo, para todo o natural $q > 1$ e todo o natural $n > 1$, temos $q^n \geq 2^n > n$. Assim sendo, a equação $n = q^{nq}$ não tem soluções em $\mathcal{Z}$ e, portanto, $x_3(n)$ é irracional.

3.2 Transcendência de $x_2(n)_{n \neq 1,2,4}$ e de $x_3(n)_{n \text{ par}}$

Já sabemos que, para cada natural $n > 1$, a coordenada $x_2(n)$ do ponto $(n, x_2(n))$ do traço de α é irracional quando $n \neq 2, 4$ e que, para n par, $x_3(n)$ é sempre irracional. Mas podemos afirmar mais: estes números são transcendentes. Estudemos $x_2(n)$, adaptando-se facilmente o argumento para $x_3(n)$. Suponhamos, pelo contrário, que, para algum natural $1 < n \neq 2, 4$, o número $x_2(n)$ é algébrico. Então, como vimos na Secção 2, a potência $(x_2(n))^n$ também é um número algébrico. Contudo, $n \neq 0, 1$, $x_2(n)$ é irracional (veja-se a Secção 3.1) e, por hipótese, $x_2(n)$ é algébrico. Logo, pelo Teorema de Gelfond-Schneider, $n^{x_2(n)}$ é transcendente, o que não é compatível com a igualdade $(x_2(n))^n = n^{x_2(n)}$. Esta contradição indica que $x_2(n)$ não pode ser algébrico.

4 $\mathcal{T}_\alpha \cap (\mathbb{Q} \times \mathbb{Q})$

Já sabemos que no traço $\mathcal{T}_\alpha$ da curva α não há pontos (n, y) com $n \in \mathbb{N}$ e $y \in \mathbb{Q}$, com excepção de $(2, 4)$ e $(4, 2)$. E quanto a pontos com ambas as coordenadas racionais? Suponhamos que um tal ponto da intersecção do traço de α com $\mathbb{Q}^+ \times \mathbb{Q}^+$ é (a, b). Como vimos na Secção 1, existe $t \in \mathbb{R}^+ \setminus \{1\}$ tal que $a = a_t = t^{\frac{1}{t-1}}$ e $b = b_t = t^{\frac{t}{t-1}}$. Ora, sendo a e b racionais e distintos, o declive t da recta que une $(0, 0)$ e (a, b) está em $\mathbb{Q}^+ \setminus \{1\}$. Pela simetria do conjunto $\mathcal{T}_\alpha$ relativamente à recta $y = x$, basta prosseguir a análise no caso em que $a > e$, sendo que então se tem $1 < b < e$ e $0 < t < 1$.

Consideremos a fracção irredutível de t, digamos $\frac{n}{m}$, onde $n, m \in \mathbb{N}$, $n < m$ e $mdc\,(n, m) = 1$. Então

$$a = \left(\frac{m}{n}\right)^{\frac{m}{m-n}} \qquad \text{e} \qquad b = \left(\frac{m}{n}\right)^{\frac{n}{m-n}}. \tag{2}$$

Comecemos por notar que, se $m - n$ dividir n e m, então os expoentes de $\frac{m}{n}$ em a e em b são inteiros e, portanto, a e b são racionais. Ora, como n e m

são primos entre si, para $m-n$ dividir ambos os naturais n e m devemos ter $m-n=1$. Ou seja, para todos os valores racionais de $t=\frac{n}{n+1}$, os pontos $(a,b)=\left(t^{\frac{1}{t-1}},\, t^{\frac{t}{t-1}}\right)$ do traço de α têm ambas as coordenadas racionais. Por exemplo,

$n \in \mathbb{N}$	$t=\frac{n}{n+1}$	$a_t=\left(\frac{n}{n+1}\right)^{n+1}$	$b_t=\left(\frac{n}{n+1}\right)^{n}$
1	$\frac{1}{2}$	4	2
2	$\frac{2}{3}$	$\frac{27}{8}$	$\frac{9}{4}$
3	$\frac{3}{4}$	$\frac{254}{81}$	$\frac{64}{27}$

Haverá outros pares $(a,b)\in\mathcal{T}_\alpha$ com ambas as coordenadas racionais? Voltemos à expressão (2) de a e b determinados por $t=\frac{n}{m}$, para $n,m\in\mathbb{N}$, $n<m$ e $mdc\,(n,m)=1$. Note-se que, como $b=ta$ e t é racional, basta determinar para que valores de n e m pode a ser racional. Estando a em $\mathbb{Q}$, existem $r,s\in\mathbb{N}$ tais que $r>s$, $mdc\,(r,s)=1$ e $a=\frac{r}{s}$. Então, elevando a primeira igualdade de (2) ao expoente $m-n$, resulta que

$$\left(\frac{m}{n}\right)^m=\left(\frac{r}{s}\right)^{m-n}.$$

Observe-se que, como n e m são primos entre si, tem-se $mdc\,(m^m,n^m)=1$: de facto, se p fosse um divisor primo de m^m e de n^m, então dividiria n e m; mas estes naturais são, por hipótese, primos entre si. Analogamente se conclui que $mdc\,(r^{m-n},s^{m-n})=1$. Então as duas fracções

$$\frac{m^m}{n^m} \quad \text{e} \quad \frac{r^{m-n}}{s^{m-n}}$$

são escritas em fracção irredutível do mesmo racional. Consequentemente, devemos ter

$$m^m=r^{m-n} \quad \text{e} \quad n^m=s^{m-n}.$$

Mas então existem naturais u,v tais que

$$m=u^{m-n} \quad \text{e} \quad n=v^{m-n}$$

sendo $u > v$ porque $n < m$. Vejamos como encontrar tais u e v.

Como $m > 1$, para determinarmos u basta considerar a factorização de m em primos. Seja p um primo que divide m e surge na factorização de m com potência $\beta \in \mathbb{N}$. Então, como $m^m = r^{m-n}$, o primo p tem também de dividir r, ocorrendo na factorização de r com uma potência máxima $\gamma \in \mathbb{N}$. Como a factorização em primos é única, concluimos que

$$\beta\, m = \gamma\,(m-n).$$

Ora m e $m-n$ são primos entre si e, portanto, esta igualdade implica que $m-n$ divide β; isto é, existe $d \in \mathbb{N}$ tal que $\beta = d\,(m-n)$. E, portanto, todos os primos da factorização de m ocorrem em m com potência que é divisível por $m-n$. Então, se $m = p_1^{\beta_1} \cdots p_k^{\beta_k}$ é a factorização de m em primos distintos e $\beta_i = d_i\,(m-n)$ para todo o $i \in \{1, \cdots, k\}$, tem-se

$$m = \left(p_1^{\beta_1} \cdots p_k^{\beta_k}\right) = p_1^{d_1\,(m-n)} \cdots p_k^{d_k\,(m-n)} = \left(p_1^{d_1} \cdots p_k^{d_k}\right)^{m-n}$$

e $u = p_1^{d_1} \cdots p_k^{d_k}$. Um argumento análogo permite concluir que ou $n = 1$, caso em que $v = 1$, ou $n > 1$ e se constrói v como u para m. Daqui resulta que

$$m - n = u^{m-n} - v^{m-n}$$

onde, recorde-se, $u > v$ e $m - n \geq 1$. Contudo, se $m - n \geq 2$, então

$$\begin{aligned} m-n &= u^{m-n} - v^{m-n} \\ &= (u-v)\left(u^{m-n-1} + u^{m-n-2}\,v + \cdots + u\,v^{m-n-2} + v^{m-n-1}\right) \\ &> m-n \end{aligned}$$

uma vez que na soma de naturais $u^{m-n-1}+u^{m-n-2}\,v+\cdots+u\,v^{m-n-2}+v^{m-n-1}$ há $m-n$ parcelas de números naturais das quais pelo menos uma, u^{m-n-1}, é estritamente maior do que 1. Consequentemente, devemos ter $m - n = 1$, ou seja,

$$t = \frac{n}{n+1}, \quad a = \left(\frac{n+1}{n}\right)^{n+1} \quad \text{e} \quad b = \left(\frac{n+1}{n}\right)^{n}.$$

Note-se ainda que $\lim_{n\to+\infty} t = 1$ e $\lim_{n\to+\infty} a = \lim_{n\to+\infty} b = e$.

5 $\mathcal{T}_\alpha \cap (\mathcal{A} \times \mathcal{A})$

Dadas as propriedades que referimos na Secção 2 sobre o corpo dos números algébricos, sabemos que, para cada número racional $t \in \mathbb{R} \setminus \{1\}$, o par (a, b) tal que $a = t^{\frac{1}{t-1}}$ e $b = t^{\frac{t}{t-1}}$ tem ambas as coordenadas algébricas. Reciprocamente, suponhamos que o par $(a, b) = \left(t^{\frac{1}{t-1}}, t^{\frac{t}{t-1}}\right)$ de $\mathcal{T}_\alpha$ tem ambas as coordenadas algébricas. Então devemos ter $t \in \mathbb{Q}$, caso contrário, pelo Teorema de Gelfond-Schneider, $b = a^t$ seria transcendente.

6 $\mathcal{T}_\alpha \cap (\mathcal{A}_\mathbb{Z} \times \mathcal{A}_\mathbb{Z})$

Comecemos por notar que $\mathcal{A}_\mathbb{Z} \cap \mathbb{Q} = \mathbb{Z}$, uma vez que os zeros racionais de um polinómio mónico $x \in \mathbb{R} \mapsto x^n + c_{n-1}x^{n-1} + \cdots + c_1 x + c_0$ com coeficientes $c_i \in \mathbb{Z}$, para $i = 0, 1, \ldots, n$, são fracções irredutíveis $\frac{r}{s}$ tais que $r \in \mathbb{Z}$, $s \in \mathbb{N}$, $mdc\,(r, s) = 1$, s divide o coeficiente 1 de x^n e r divide c_0; e, portanto, $s = 1$ e $\frac{r}{s} = r$ é um inteiro.

Consideremos um ponto $(a, b) = \left(t^{\frac{1}{t-1}}, t^{\frac{t}{t-1}}\right)$ de $\mathcal{T}_\alpha$, onde $t \in \,]0, 1[$, e suponhamos que as suas coordenadas são inteiros algébricos (o argumento é análogo para $t \in \,]1, +\infty[$). Então, como vimos na Subsecção 5, o declive t é racional, digamos, $t = \frac{n}{m}$ com $n, m \in \mathbb{N}$, $n < m$ e $mdc\,(n, m) = 1$. Observe-se que, como a é inteiro algébrico, a^{m-n} também é; além disso, a^{m-n} é racional porque

$$a^{m-n} = \left(t^{\frac{1}{t-1}}\right)^{m-n} = \left(\frac{m}{n}\right)^m.$$

Logo a^{m-n} é inteiro, e portanto $n = 1$. Consequentemente, $t = \frac{1}{m}$ para algum natural $m \geq 2$.

Reciprocamente, quando $t = \frac{1}{m}$ para algum natural $m \geq 2$, o par $(a, b) = \left(t^{\frac{1}{t-1}}, t^{\frac{t}{t-1}}\right)$ tem coordenadas que são inteiros algébricos. Efectivamente, neste caso,

$$a = \sqrt[m-1]{m^m} \quad \text{e} \quad b = \sqrt[m-1]{m}$$

e estes números são, respectivamente, zeros dos polinómios mónicos de coeficientes inteiros

$$\mathcal{P}(x) = x^{m-1} - m^m \quad \text{e} \quad \mathcal{Q}(x) = x^{m-1} - m.$$

Por exemplo,

m	t	$a_t = t^{\frac{1}{t-1}}$	$b_t = t^{\frac{t}{t-1}}$	$\mathcal{P}$	$\mathcal{Q}$
2	$\frac{1}{2}$	4	2	$x-4$	$x-2$
3	$\frac{1}{3}$	$3\sqrt{3}$	$\sqrt{3}$	x^2-27	x^2-3
4	$\frac{1}{4}$	$4\sqrt[3]{4}$	$\sqrt[3]{4}$	x^3-256	x^3-4

Referências

[1] Associação Atractor, *Dinâmica de uma família de exponenciais*, Gazeta de Matemática 181 (2017) 3–7.

[2] M. Carvalho, *O método das cordas*, Bol. Soc. Port. Mat. Número especial do tricentenário de Leonard Euler (2008) 61–72.

[3] M. Carvalho, S. Cavadas, *Jogando no limite*, Bol. Soc. Port. Mat. 69 (2013) 1–19.

[4] J. H. Cadwell, *Topics in Recreational Mathematics*, Cambridge University Press, 1980.

[5] L. Euler, *De formulis exponentialibus replicatis*, Acta Academiae Scientarum Imperialis Petropolitinae 1 (1778) 38–60.

[6] A. O. Gelfond, *Sur le septieme problème de D. Hilbert*, Doklady Akad. Nauk. 2 (1934) 1–6.

[7] C. Hermite, *Sur la fonction exponentielle*, C. R. Acad. Sci. Paris 77 (1873) 18–24.

[8] D. Hilbert, *Sur les problèmes futures des mathématiques*, C. R. Deuxième Congrès International des Mathématiciens, Paris, 1900, 58–114.

[9] F. Lindemann, *Ueber die Zahl p*, Math. Annalen 20 (1882) 213–225.

[10] J. Liouville, *Sur des classes très-étendues de quantités dont la valeur n'est ni rationnelle ni même réductible à des irrationnelles algébriques*, C. R. Acad. Sci. Paris 18 (1844) 883–885; J. Math. Pures Appl. 16:1 (1851) 133-142.

[11] K. Mahler, *Lectures on Transcendental Numbers*, LNM 546, Springer New York, 1976.

[12] I. Niven, *Irrational Numbers*, Wiley New York, 2012.

[13] J. C. Oxtoby, *Measure and Category*, Springer New York, 1980.

[14] H. Pollard, H. G. Diamond, *The Theory of Algebraic Numbers*, Carus Mathematical Monographs 9, MAA, 1975.

[15] Th. Schneider, *Transzendenzuntersuchungen periodischer Funktionen I*, Journal fur Mathematik 172 (1935) 65–69.

[16] K. Weierstrass, *Math. Werke II* (1895) 341–362.