Uma Prova Celestial do Teorema Fundamental da Álgebra

Hugo Cattarucci Botós

Instituto de Ciências Matemáticas e de Computação
Universidade de São Paulo
hugocbotos@gmail.com

Resumo

Polinômios são objetos centrais na Matemática, sendo o estudo deles a origem de muitas áreas tais como a Teoria de Grupos, a Teoria de Galois, a Teoria de Invariantes e a Geometria Algébrica. Trataremos de um problema central no estudo de polinômios em uma variável, a busca por raízes. Iniciaremos nossa saga falando de fórmulas por radicais, como a de Bhaskara e de Cardano, até tocarmos superficialmente nos trabalhos de Abel e Galois, e então discutiremos o Teorema Fundamental da Álgebra, o provando usando o sistema solar como nossa musa inspiradora.

1. Solução Radical

> Álgebra é apenas geometria escrita e geometria é apenas álgebra em figuras.
>
> *Sophie Germain*

Nessa primeira parte vamos brincar apenas com equações polinomiais[1] com coeficientes reais.

A equação polinomial mais simples é a equação linear $x + b = 0$, cuja solução é $x = -b$. Em seguida temos a equação de grau dois

$$x^2 + bx + c = 0,$$

que é um pouco mais complicada de se resolver, mas não muito. A solução dessa equação é conhecida desde a antiguidade e é dada pela nossa velha conhecida **Fórmula de Bhaskara**:

$$x = \frac{-b \pm \sqrt{b^2 - 4c}}{2}.$$

Essa fórmula nos diz duas coisas curiosas. A primeira é que precisamos de números complexos para resolvermos todas as equações de grau dois. A segunda é que podemos escrever suas raízes em termos dos coeficientes b e c usando apenas as operações elementares $+$, $-$, $\times$, $\div$ e $\sqrt{\ }$. Nesse caso, dizemos que equações de grau dois tem solução por radical. De forma mais geral, se podemos escrever a formula da raiz de um polinômio genérico de grau n usando apenas as operações básicas $+$, $-$, $\times$, $\div$ e raízes $\sqrt{\ }$, $\sqrt[3]{\ }$, $\sqrt[4]{\ }$, etc, então dizemos que o polinômio tem **solução por radical**.

[1] Como estamos interessados em raízes para equações polinomiais como $a_0 + a_1 x + \cdots + a_n x^n = 0$ com $a_n \neq 0$, podemos supor que o coeficiente a_n é 1, pois podemos dividir a equação polinomial por a_n e isso não altera quem são as raízes.

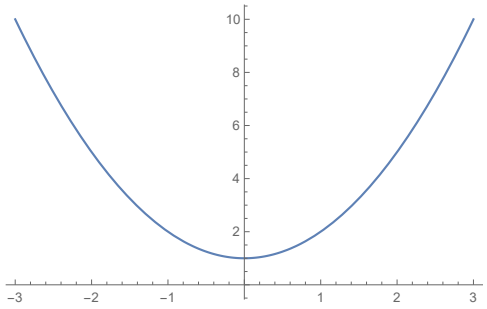


Figura 1: *A equação $x^2 + 1 = 0$ não tem raízes reais, mas tem duas raízes complexas, i e $-i$.*

A necessidade de introduzir números complexos surge, por exemplo, na equação $x^2 + 1 = 0$. Essa equação não tem soluções reais como mostra a Figura 1. As soluções, obtidas pela Fórmula de Bhaskara, são

$$x = \pm\sqrt{-1},$$

que não fazem sentido no contexto dos números reais. Precisamos adicionar um novo número, denotado por i, ao nosso arsenal se quisermos resolver tal equação. Então, estabelecemos i como sendo um número que resolve $x^2 + 1 = 0$, ou seja, $i^2 = -1$.

De certa forma, a introdução do número i lembra bastante a introdução dos números irracionais. Por muito tempo na matemática grega se acreditou que os únicos números que existiam eram os racionais, no entanto, se construirmos um quadrado de lado 1 e calcularmos sua diagonal com o Teorema de Pitágoras obtemos $\sqrt{2}$, que não pode ser representado como fração. Isso forçou os matemáticos da época a aceitarem a existência de números não racionais, isto é, os números irracionais. Da mesma forma, como o número i surge de jeito natural, fomos forçados a aceitá-lo, o que levou alguns séculos, e amá-lo.

Equações gerais de grau três e quatro também podem ser resolvidas por radical. Essas fórmulas são chamadas de Fórmula de Cardano e Fórmula de Ferrari, respectivamente, e foram descobertas por volta de 500 anos atrás. Vejamos como obter as soluções para as equações de grau dois e três. Se temos a equação $x^2 + bx + c = 0$, então a primeira coisa a ser feita é matar o termo de grau um bx, o que pode ser feito com a substituição $x = y - b/2$. Repare que obtemos:

$$x^2 + bx + c = \left(y - \frac{b}{2}\right)^2 + b\left(y - \frac{b}{2}\right) + c = y^2 - \frac{b^2 - 4c}{4},$$

que é igual a zero, ou seja,

$$y^2 = \frac{b^2 - 4c}{4} \Rightarrow y = \pm\frac{\sqrt{b^2 - 4c}}{2},$$

de onde segue a Fórmula de Bhaskara se usarmos que $x = y - b/2$.

Já a equação do terceiro grau é um pouco mais sofisticada. Se temos a equação $x^3 + bx^2 + cx + d = 0$, então fazendo $x = y - b/3$ obtemos uma equação da forma $y^3 + py + q = 0$, ou seja, eliminamos o fator de grau dois do polinômio original. Agora, para resolver essa equação temos de usar a seguinte identidade[2] que vale para todos números y, r, s:

$$y^3 + r^3 + s^3 - 3yrs = (y + r + s)(y^2 + r^2 + s^2 - yr - ys - rs). \tag{1}$$

[2]Essa identidade segue de jeito natural se você brincar com o determinante de $\begin{bmatrix} y & r & s \\ s & y & r \\ r & s & y \end{bmatrix}$, ou você pode prová-la desenvolvendo o termo da direita até obter o da esquerda.

Repare que o fator a esquerda da Identidade (1) e nosso polinômio $y^3 + py + q = 0$ são parecidos, ambos não têm o fator y^2. Procuremos por r e s satisfazendo

$$r^3 + s^3 = q \quad \text{e} \quad -3rs = p,$$

o que pode ser escrito como

$$r^3 + s^3 = q \quad \text{e} \quad r^3 s^3 = -\frac{p^3}{27}.$$

Talvez o leitor repare que essas identidades lembram as relações de soma e produto de uma equação do segundo grau. Se temos uma equação $w^2 + bw + c = 0$ com raízes w_1 e w_2, então escrevendo $(w - w_1)(w - w_2) = w^2 + bw + c$ e desenvolvendo o termo da esquerda, obtém-se as relações $w_1 + w_2 = -b$ e $w_1 w_2 = c$. Pelo mesmo princípio, resolvendo a equação $w^2 - qw - p^3/27 = 0$, obtemos r^3 e s^3. Assim, usando a Fórmula de Bhaskara se obtém

$$r^3 = \frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}} \quad \text{e} \quad s^3 = \frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}},$$

ou seja,

$$r = \sqrt[3]{\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}} \quad \text{e} \quad s = \sqrt[3]{\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}}.$$

Voltando a Identidade (1), temos

$$y^3 + py + q = y^3 + r^3 + s^3 - 3yrs = (y + r + s)(y^2 + r^2 + s^2 - yr - ys - rs),$$

nos dizendo que $y = -(r + s)$ é raiz de $y^3 + py + q = 0$. Então, a raiz é dada por essa fórmula horrenda, chamada **Fórmula de Cardano**,

$$y = -\sqrt[3]{\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}} - \sqrt[3]{\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}}.$$

Veja que apenas encontramos a solução de $y^3 + py + q = 0$. Para acharmos a solução de $x^3 + bx^2 + cx + d = 0$, precisamos escrever p e q em função de b, c, d, relação obtida após fazermos $x = y - b/3$. Mas vou parar por aqui, as contas já estão ficando grandes demais. No entanto, repare no seguinte: para resolvermos a equação de terceiro grau tivemos, durante o percurso, que resolver uma de segundo grau. O mesmo ocorre para a equação de quarto grau. Fazemos um mesmo tipo de troca de variável no começo para eliminarmos o termo de ordem três e depois fazemos vários malabarismos algébricos até cairmos numa equação de terceiro grau, que já sabemos resolver.

A pergunta natural é se equações de grau cinco arbitrárias tem solução por radicais. Surpreendente, a resposta é não. Isso foi descoberto independentemente por dois jovens matemáticos no início do século 19, um deles foi o rapaz francês Evariste Galois (1811 – 1832), que mostrou a impossibilidade de tal fórmula estudando simetrias nas raízes de polinômios, um tipo de raciocínio que revolucionou a Matemática dos séculos seguintes com a introdução do conceito de grupo, que é a entidade algébrica que codifica simetria de coisas. A outra prova foi dada pelo rapaz norueguês Niels Henrik Abel (1802 – 1829), que deu uma prova bem diferente e mais geométrica. A mesma impossibilidade vale também para equações de grau maior do que cinco. A prova de Abel foi a primeira a ser aceita pela comunidade matemática, em 1824, e por isso o teorema que garante a impossibilidade de uma fórmula por radicais para equações de grau cinco ou maior leva o nome de Teorema de Abel. A prova de Galois só foi aceita duas décadas depois, no entanto,

seus trabalhos fundaram a ciência que hoje chamamos de Teoria de Galois, que resolveu vários problemas clássicos além desse que estamos a descrever. Por exemplo, com essa tecnologia é possível provar resultados que perturbaram os matemáticos desde a Grécia antiga, tais como o problema da trissecção do ângulo e o da duplicação do cubo.

Evariste Galois

Niels Henrik Abel

Wikipedia: [Gal] e [Abl].

Tanto Galois quanto Abel tiveram vidas muito trágicas. Galois era, além de matemático, um revolucionário, sendo expulso da universidade e preso algumas vezes. Encontrou seu fim em um duelo com apenas 20 anos de idade. Felizmente para nós, prevendo sua morte, conseguiu que seus textos matemáticos atingissem grandes matemáticos de sua época, fazendo com que seu legado fosse preservado. No entanto, devido a complexidade de seus argumentos, matemáticos como Siméon Poisson (1781 – 1840) julgaram seu trabalho como incompreensível, ficando esse engavetado até ser redescoberto pelo grande matemático Joseph Liouville (1809 – 1882) anos depois, que compreendeu a genialidade de Galois. Já Abel morreu de tuberculose aos 26 anos, pobre e desempregado, antes que seus trabalhos fossem reconhecidos. No entanto, como disse o matemático Charles Hermite (1822 – 1901),

"Abel deixou aos matemáticos o suficiente para deixá-los ocupados por quinhentos anos."

Em homenagem ao Abel hoje temos o Prêmio Abel, que assim como a Medalha Fields, é um prêmio de altíssimo prestígio na comunidade matemática.

Bem, voltemos aos polinômios. Até o fim do século 18 não se tinha certeza sequer se polinômios sempre tinham raízes. Veja que esse é um problema em essência mais simples que o de encontrar raízes escritas em termos de radicais. Apenas se deseja saber se polinômios tem raízes, sem se importar com encontrá-las explicitamente.

Por exemplo, se pegarmos uma equação polinomial com coeficientes reais de grau cinco dada por $x^5 + bx^4 + cx^3 + dx^2 + ex + f = 0$ e considerarmos a função $p(x) = x^5 + bx^4 + cx^3 + dx^2 + ex + f$, então, plotando seu gráfico, reparamos que essa função cresce para ∞ quando x vai para ∞, isto é,

$$\lim_{x \to \infty} p(x) = \infty,$$

e vai para $-\infty$ quando x vai para $-\infty$,

$$\lim_{x\to-\infty} p(x) = -\infty.$$

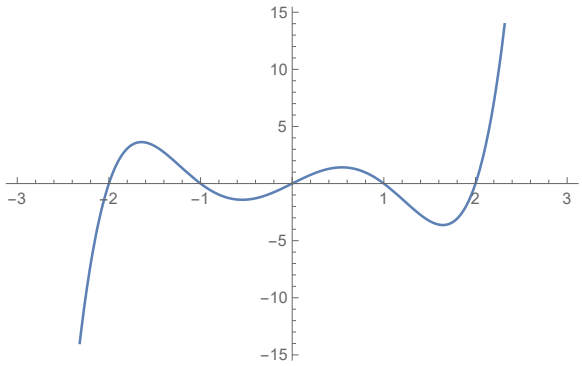


Figura 2: *O polinômio* $p(x) = x^5 - 5x + 4$ *corta o eixo* x *em pelo menos um ponto.*

Isso quer dizer que em algum ponto x_0 o gráfico corta o eixo x, nos garantindo $p(x_0) = 0$, ou seja, a equação $x^5 + bx^4 + cx^3 + dx^2 + ex + f = 0$ tem a solução real $x = x_0$. Em outras palavras, equações polinomiais podem ter raízes mesmo que não exista uma fórmula em radicais para essas soluções. Repare também que esse mesmo argumento gráfico garante que polinômios de grau ímpar com coeficientes reais sempre tem ao menos uma raiz real. No entanto, a equação $x^6 - x + 1 = 0$ não tem solução real como mostra a Figura 3.

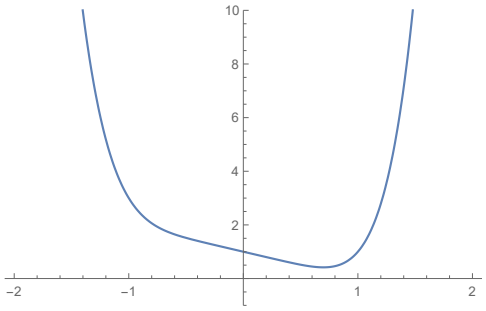


Figura 3: *Gráfico de* $p(x) = x^6 - x + 1$

Por outro lado, se precisarmos desesperadamente de soluções basta usarmos um computador e facilmente obtemos soluções aproximadas. As raízes de $x^6 - x + 1 = 0$, por exemplo, são aproximadamente

$$-0.945402 - 0.611837i, \quad -0.945402 + 0.611837i,$$
$$0.154735 - 1.03838i, \quad 0.154735 + 1.03838i,$$
$$0.790667 - 0.300507i, \quad 0.790667 + 0.300507i.$$

Olhando bem para essas raízes se observa um fenômeno curioso: as raízes aparecem em pares conjugados, isto é, se $a + bi$ é uma raiz, onde $a, b \in \mathbb{R}$, então $a - ib$ também é raiz. Você, caro leitor, consegue ver de onde vem esse fenômeno? Vou deixar essa investigação a seus cuidados.

Agora presenciaremos um milagre chamado **Teorema Fundamental da Álgebra**. Adicionando esse número i aos números reais, necessário para resolver $x^2 + 1 = 0$, podemos resolver todas as equações polinomiais. Esse é um resultado de Carl Friedrich Gauss (1777 – 1855), que deu várias provas desse fato.

Gauss: Considerado por muitos o maior matemático de todos.
Wikipedia: [Gau].

No entanto, as provas do Gauss não dizem como achar as soluções, apenas garantem sua existência. Em geral encontrar raízes de um polinômio é uma tarefa árdua, senão impossível, mas ao menos existem técnicas que permitem calculá-las aproximadamente.

Esse é um fenômeno bastante comum em Matemática: muitas vezes podemos mostrar a existência de uma entidade, mas não conseguimos exibi-la explicitamente. Isso não é tão estranho. Se temos, por exemplo, 11 pessoas morando em 10 casas em um vilarejo, então certamente duas pessoas ao menos compartilham uma casa[3]. Veja que temos a existência de uma casa onde ao menos duas pessoas moram, mas não conseguimos dizer qual é a casa.

Meu objetivo nesse texto é explicar porque equações polinomiais sempre tem solução. Não tocarei nos argumento de Galois e de Abel sobre a solução por radicais. Esses argumentos são um tanto sofisticados e não conseguiria expô-los de jeito simples, embora exista uma prova lindíssima de V.I. Arnold (1937 – 2010) que é um tanto geométrica e "elementar", que pode ser encontrada no artigo [Gol] e no livro [Ale].

Mais precisamente, meu objetivo é provar o seguinte teorema:

Teorema 2 (Teorema de Fundamental da Álgebra) *A equação polinomial*

$$x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = 0,$$

onde os coeficientes a_i são números complexos e $n \geq 1$, sempre tem raiz.

Repare que na nossa discussão até agora assumimos que os coeficientes eram reais, mas isso é absolutamente desnecessário. Polinômios como $x^3 + (2+5i)x^2 + 23ix + 1 + i\sqrt{2}$ tem raízes (só não me peça para encontrá-las).

[3]Esse tipo de bom senso se chama Princípio das Casas Dos Pombos.

Esse teorema nos garante algo bem interessante: todo polinômio de grau n tem n raízes $r_1, r_2, \ldots, r_n$, não necessariamente distintas, e se fatora como produto de monômios $x - r_i$, isto é,

$$x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 = (x - r_1)(x - r_2)\cdots(x - r_n).$$

Isso segue do algoritmo da divisão para polinômios: lembre-se que se temos dois polinômios $p(x)$ e $q(x)$, com $q(x) \neq 0$, então existem dois polinômios $s(x)$ e $r(x)$ tais que

$$p(x) = s(x)q(x) + r(x),$$

onde $r(x) = 0$ ou $r(x)$ é um polinômio não nulo com grau menor que o de $q(x)$. Esse algoritmo é similar ao algoritmo da divisão de Euclides: se temos dois números naturais p e q, com q não nulo, então existem naturais s e r tais que $p = sq + r$, onde $0 \leq r < q$.

Agora considere $p(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$. Pelo Teorema Fundamental da Álgebra existe uma raiz r_1 para esse polinômio. Agora apliquemos o algoritmo da divisão para $q(x) = x - r_1$. Temos que existem $p_1(x)$ e $r(x)$ tais que $p(x) = p_1(x)(x - r_1) + r(x)$, onde $r(x)$ é nulo ou é polinômio não nulo com grau inferior ao grau de $x - r_1$, que é 1. Desta forma, $r(x)$ deve ser uma constante, que denotaremos por r, nos dando a expressão

$$p(x) = p_1(x)(x - r_1) + r.$$

No entanto, fazendo $x = r_1$ obtemos $p(r_1) = p_1(r_1)(r_1 - r_1) + r$ e, portanto, $r = 0$. Logo,

$$p(x) = p_1(x)(x - r_1).$$

Aplicando o mesmo procedimento para $p_1(x)$ no lugar de $p(x)$, temos que $p_1(x)$ tem uma raiz r_2 e se escreve como

$$p_1(x) = p_2(x)(x - r_2)$$

e daí segue a identidade

$$p(x) = p_2(x)(x - r_1)(x - r_2).$$

Repetindo esse procedimento k vezes obtemos

$$p(x) = p_k(x)(x - r_1)(x - r_2)\cdots(x - r_k).$$

Se denotarmos o grau de um polinômio por deg temos que $\deg p_1 = \deg p - 1$, $\deg p_2 = \deg p_1 - 1$ e assim por diante, ou seja, o grau dos polinômios $p_k(x)$ reduz 1 a cada estágio do processo, o que nos garante que p_n tem grau zero, o que quer dizer que p_n é um número complexo.

Daí segue que $x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 = p_n(x - r_1)(x - r_2)\cdots(x - r_n)$, mas como o fator x^n a esquerda não tem uma constante multiplicando, temos que p_n tem de ser igual ao polinômio constante 1, e, voilá,

$$x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 = (x - r_1)(x - r_2)\cdots(x - r_n).$$

Assim, polinômios de grau n tem n raízes. Por exemplo, $x^2 + 1 = (x - i)(x + i)$.

Repare que esse tipo de fatoração é a mesma que ocorre em aritmética, em que todo número natural se fatora como produto de números primos. No caso de polinômio complexos, esses "primos" são os monômios $x - r$. Uma pergunta ao leitor: Quem são os "primos" para polinômios com coeficientes reais? Por primos aqui entenda polinômios reais não constantes que não se quebram como produto de dois polinômios reais não constantes, como $x^2 + 1$. Se $x^2 + 1 = p(x)q(x)$, onde p e q são polinômios reais, então p ou q é constante.

A fim de entender a prova do Teorema Fundamental da Álgebra precisamos entender um pouco da geometria dos números complexos, e é sobre isso que falaremos agora.

2. Complexo é Geometria

> O caminho mais curto entre duas verdades no domínio real passa pelo domínio complexo.
>
> *Jacques Hadamard*

Acredito que você, caro leitor, já tenha estudado os números complexos em tempos remotos, e talvez ainda lembre algo sobre eles, mas a fim de me certificar que estamos na mesma página, deixe-me relembrá-lo de alguns fatos da vida, pois relembrar é viver.

Um número complexo é um número da forma $a + bi$, onde $a, b \in \mathbb{R}$ e $i^2 = -1$. Os números a e b são chamados de parte real e parte imaginária de z, respectivamente. O conjunto de todos números complexos é denotado por $\mathbb{C}$ e vale a inclusão $\mathbb{R} \subset \mathbb{C}$, pois todo número real a pode ser escrito como $a + 0i$. Existem duas operações básicas nos números complexos, a adição e a multiplicação: Se $z = a + bi$ e $w = c + di$, então temos

$$z + w = (a + c) + (b + d)i,$$

$$zw = (ac - bd) + (ad + bc)i.$$

Essa segunda fórmula é obtida usando a distributividade:

$$\begin{aligned}(a + bi)(c + di) &= a(c + di) + bi(c + di)\\ &= ac + adi + bci + bdi^2\\ &= ac + adi + bci - bd\\ &= (ac - bd) + (ad + bc)i.\end{aligned}$$

Os números complexos satisfazem as mesmas propriedades básicas de adição e multiplicação que os números reais e racionais tais como a comutatividade e a associatividade.

Se temos um número complexo $z = a + bi$, então podemos representá-lo geometricamente por uma seta como na Figura 4.

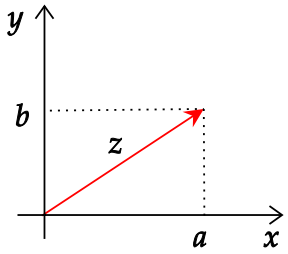


Figura 4: *Denotamos $z = a + ib$ pela seta ligando 0 até (a, b) no plano.*

Denotaremos também o ponto (a, b) no plano acima por $a + bi$. Assim, $a + bi$ pode ser representado pelo ponto (a, b) no plano ou pela seta ligando $(0, 0)$ a (a, b). Chamaremos esse plano de plano complexo.

O comprimento dessa seta, denotada por $|z|$, é calculado pelo Teorema de Pitagoras. Note que na Figura 4 temos um triângulo retângulo com catetos a, b, e hipotenusa $|z|$, nos garantindo a fórmula

$$|z| = \sqrt{a^2 + b^2}.$$

A soma de $z = a + bi$ com $w = c + di$ é dada pela Figura 5. A partir das setas z e w obtemos o paralelogramo desenhado. O número complexo $z + w$ é representado pela seta indicada que vai da origem 0 até o vértice $(a + c, b + d)$, oposto ao 0 no paralelogramo.

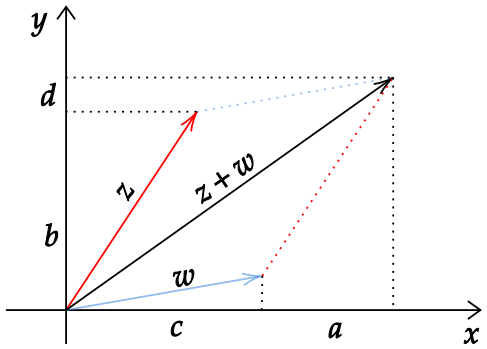


Figura 5: *Regra do paralelogramo.*

Um exercício que talvez interesse o leitor é provar geometricamente a identidade

$$(z_1 + z_2) + z_3 = z_1 + (z_2 + z_3).$$

A multiplicação já é um pouco mais complicada de se entender geometricamente.

Primeiramente, repare que multiplicar um número complexo $z = a + bi$ por um número real $c > 0$ é o mesmo que dilatar (esticar) z por um fator c sem mudar sua direção e seu sentido. Por outro lado, se multiplicarmos por $c < 0$, então a dilatação ocorre, preservando a direção, mas mudando o sentido, a seta cz apontará para direção oposta a aquela de z, como ilustra a Figura 6.

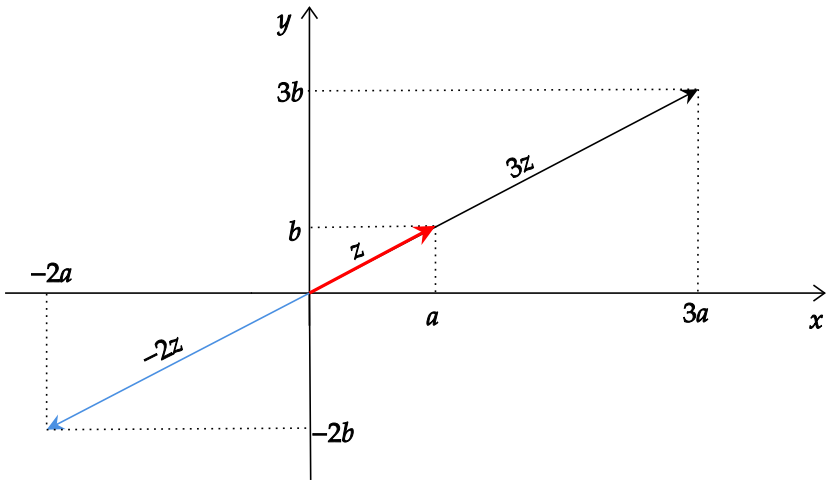


Figura 6: *Multiplicar z por $c \in \mathbb{R}$ estica z de acordo com o valor de c sem mudar a direção, mas podendo mudar o sentido de acordo com o sinal de c.*

A multiplicação por i é bem mais curiosa. Ela faz a seta z girar 90 no sentido anti-horário [4], como mostra a Figura 7.

[4] sentido contrário ao do relógio.

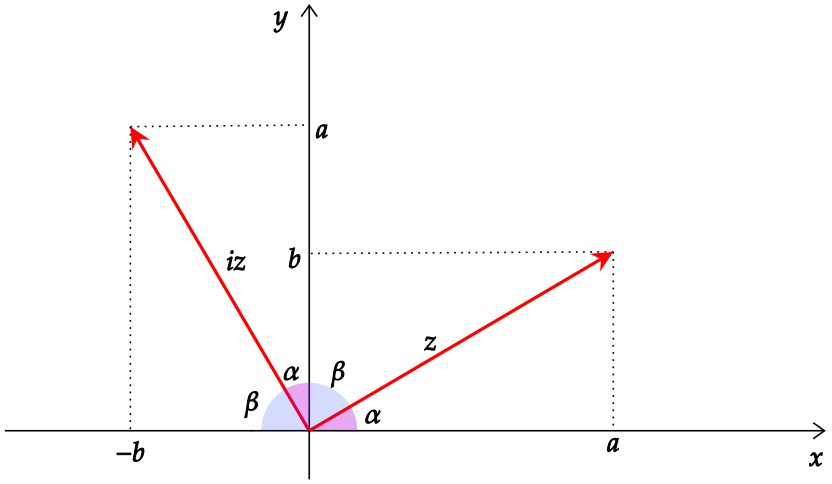


Figura 7: *Multiplicar z por i gira z no sentido anti-horário.*

Para ver que o ângulo entre z e iz é de fato $\pi/2$, basta reparar que esse ângulo, de acordo com a Figura 7, é $\alpha + \beta$, e que $2\alpha + 2\beta = \pi$.

Com isso estamos prontos para descrever a multiplicação geometricamente. Considere as setas $z = a + bi$ e $w = c + di$ de acordo com a Figura 8.

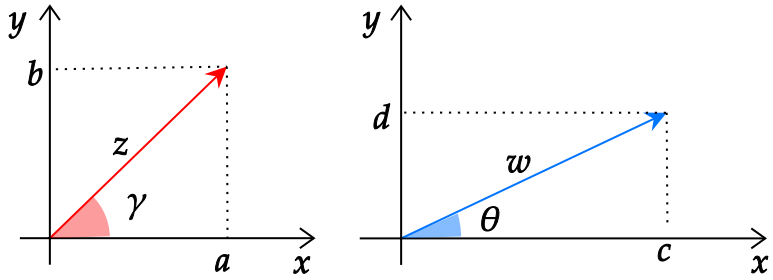


Figura 8: *Números z e w com seus respectivos angulos, γ e θ, com respeito ao eixo x.*

Repare que $zw = cz + idz$. Então temos a soma de cz, que é a dilatação de z pelo fator c, com idz, que é dz girado 90 no sentido anti-horário, como ilustra a Figura 9.

O triângulo retângulo com vértices 0, cz e idz é semelhante ao triângulo retângulo dado por w com vértices 0, w e c, pois temos $|cz| = |z||c|$ e $|idz| = |z||d|$, ou seja, o primeiro triângulo retângulo é obtido do segundo dilatando seus lados pelo fator $|z|$. Como a hipotenusa do primeiro triângulo é zw e o segundo tem hipotenusa w, temos que $|zw| = |z||w|$. Assim, o comprimento da seta zw é $|z||w|$. O ângulo entre zw e o eixo x é a soma dos ângulos de z e w, isto é, $\gamma + \theta$. Assim, ao multiplicarmos z e w obtemos um número complexo que é representado geometricamente pela seta apontando na direção obtida ao somarmos os ângulos de z e w, e com comprimento $|z||w|$.

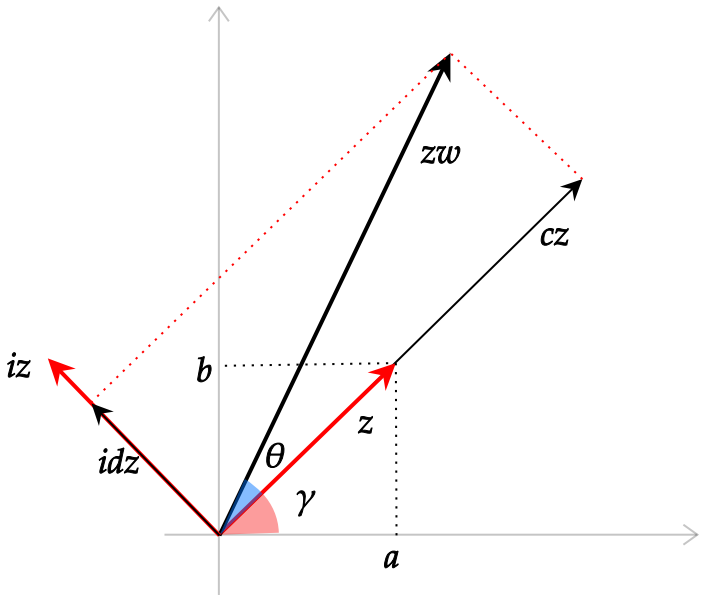


Figura 9: *Geometricamente zw é a seta apontando na direção dada pelo angulo $\gamma + \theta$, e com comprimento $|z||w|$.*

Multiplicar números complexos = somar ângulos + multiplicar comprimentos. (3)

O conjugado de um número complexo $z = a + bi$ é definido por $\bar{z} = a - bi$. Deixarei a interpretação geométrica da fórmula $z\bar{z} = |z|^2$ ao leitor.

Essa descrição visual da multiplicação não é muito prática. Precisamos deixá-la mais algébrica para facilitar nossas contas a seguir, e será isso que faremos até o fim dessa seção.

Existe um número real, um pouco menor que três, chamado número de Euler, denotado por e. Da mesma forma que o π, essa entidade é onipresente na ciência moderna. Como e é um número real, podemos exponenciá-lo a um número real, como, por exemplo, e^{42}. No entanto, o grande matemático suíço Leonhard Euler (1707 – 1783) estendeu a noção de exponencial para números complexos definindo

$$e^{i\theta} := \cos(\theta) + i\text{sen}(\theta). \tag{4}$$

Em particular, essa fórmula relaciona os números mais importantes da Matemática: para $\theta = \pi$ obtemos $e^{i\pi} + 1 = 0$, uma fórmula que envolve $0, 1, i, e, \pi$.

Repare que esse número $e^{i\theta}$ é um ponto no círculo de raio um no plano complexo com inclinação dada pelo ângulo θ. Denotaremos tal círculo por $\mathbb{S}^1$.

$$\mathbb{S}^1 := \{e^{i\theta} \in \mathbb{C} : \theta \in \mathbb{R}\}.$$

Pela nossa discussão geométrica sobre multiplicação, devemos ter que $e^{i\alpha}e^{i\beta} = e^{i(\alpha+\beta)}$, pois ao multiplicarmos números complexos, multiplicamos comprimentos, que são 1, e somamos ângulos. Repare que a notação de exponencial faz todo sentido, pois, como sabemos da escola, exponenciais satisfazem relações tipo $a^x a^y = a^{x+y}$.

Essa fórmula não é só esteticamente bonita, ela resume toda a trigonometria da escola. Se você entende bem como essa fórmula funciona, trigonometria se torna uma trivialidade. Para justificar

essa afirmação, brinquemos com a identidade

$$e^{2i\theta} = e^{i\theta}e^{i\theta}.$$

Pela Fórmula 4 temos

$$\cos(2\theta) + i\text{sen}(2\theta) = (\cos(\theta) + i\text{sen}(\theta))(\cos(\theta) + i\text{sen}(\theta))$$

e desenvolvendo o termo da direita obtemos

$$\cos(2\theta) + i\text{sen}(2\theta) = \cos(\theta)^2 - \sin(\theta)^2 + 2i\text{sen}(\theta)\cos(\theta).$$

Comparando a parte real à parte real, e a parte imaginária à parte imaginária, obtemos as famosas relações de arco duplo da escola.

$$\begin{cases} \cos(2\theta) = \cos(\theta)^2 - \sin(\theta)^2, \\ \text{sen}(2\theta) = 2\text{sen}(\theta)\cos(\theta). \end{cases}$$

Por fim, escrevamos todo número complexo diferente de zero em termos de seu comprimento e seu ângulo. Se pegarmos $z \neq 0$, então podemos dividí-lo por seu comprimento $|z|$, obtendo o ponto $z/|z|$ de $\mathbb{S}^1$. Se o ângulo entre z e o eixo x é γ, então podemos escrever

$$z/|z| = e^{i\gamma} \Rightarrow z = |z|e^{i\gamma}.$$

Assim, escrevendo $z = |z|e^{i\gamma}$ e $w = |w|e^{i\theta}$ temos

$$zw = |z||w|e^{i(\gamma+\theta)},$$

que é a expressão algébrica para afirmação 3.

3. Matemática Experimental

> Matemática é parte da física. A física é uma ciência experimental, parte da ciência natural. A matemática é a parte da física em que os experimentos são baratos.
>
> *Vladimir Arnold*

Como daqui em diante nossos polinômios são complexos, passarei a usar z no lugar de x como variável, pois me parece hediondo usar x como número complexo.

Considere o polinômio $p(z) = z^2$. O que esse polinômio faz quando "andamos em círculos"?

Um ponto z de $\mathbb{S}^1$ pode ser escrito como $e^{i\theta}$, como vimos na seção anterior, onde θ é o ângulo que esse ponto faz com a direção positiva do eixo x. O polinômio p manda $z = e^{i\theta}$ para $z^2 = e^{2i\theta}$, ou seja, conforme você caminha com o ponto z aumentando θ aos poucos, z^2 caminha duas vezes mais rápido. Ao chegarmos em $\theta = \pi$, ou seja, $z = -1$, o ponto z^2 terá percorrido uma volta completa, atingindo $z^2 = 1$. Quando z completar uma volta completa, então teremos que z^2 completou duas voltas. Se pensarmos que z e z^2 são planetas orbitando em órbitas circulares em torno de 0, então a cada volta que z completa, teremos que z^2 completou duas voltas.

Se pegarmos $p(z) = z^3$ algo similar ocorre, z^3 orbita com velocidade três vezes maior do que a de z. Ao darmos uma volta com z temos que z^3 dará três voltas.

De modo geral, temos que $p(z) = z^n$ funciona da mesma forma. Se z der uma volta em sua órbita, então z^n dará n voltas.

Pegamos z no círculo de raio um apenas por conveniência. Se z caminha em um círculo de raio r, então podemos escrever $z = re^{i\theta}$, e assim $p(z) = r^n e^{ni\theta}$. Desta forma, se z der uma volta no círculo de raio r, então z^n dará n voltas no círculo de raio r^n.

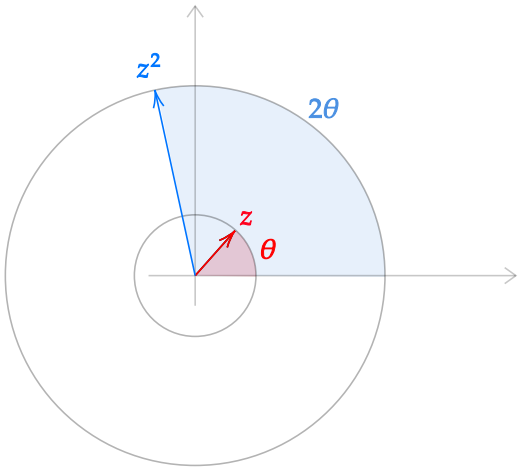


Figura 10: *O ponto z percorrendo um cículo de raio r e* z^2 *percorrendo um círculo de raio* r^2.

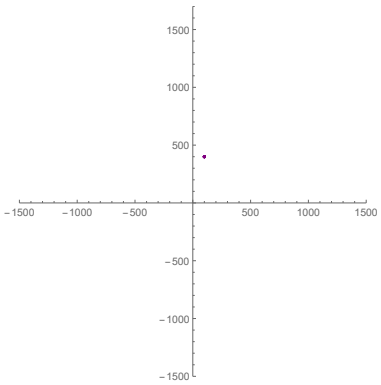
O Teorema Fundamental da Álgebra é obtido comparando o comportamento das funções polinomiais

$$z \mapsto z^n + a_{n-1}z^{n-1} + \cdots + a_1 z + a_0 \quad \text{e} \quad z \mapsto z^n$$

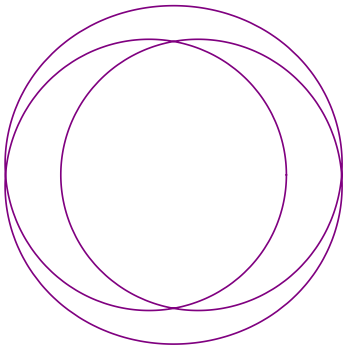
sobre círculos de raio bem grande, como veremos a seguir.

Como matemática é ciência empírica como todas as outras, vejamos alguns experimentos computacionais para ver o que acontece com o polinômio $p(z) = z^5 + 5z^3 - 2z + 100 + 400i$.

Se pegarmos z num círculo pequeno, teremos que z é aproximadamente 0, e, portanto, $p(z) \simeq 100 + 400i$. Na Figura 11, considerou-se z de tamanho 1, que é suficientemente pequeno comparado a $100 + 400i$. Então, ao fazermos z percorrer o círculo de raio 1 em torno de 0, temos uma pequena figura em torno de $100 + 400i$.



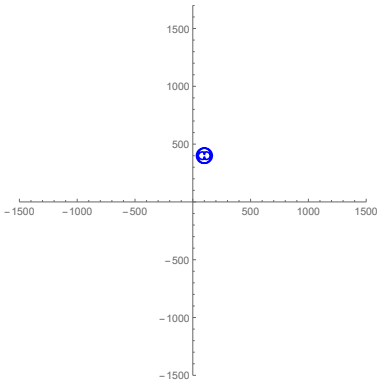
Visto de longe



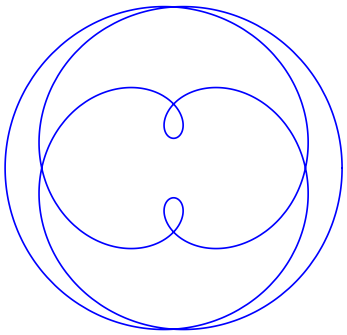
Visto de perto, no microscópio

Figura 11: *Fazendo z percorrer um círculo de raio* 1*, temos que $p(z)$ faz um desenho pequeno em torno de* $100 + 400i$*.*

Agora vamos aumentar o raio para 2. Fazendo z percorrer o círculo de raio 2 centrado em 0 obtemos a seguinte figura:



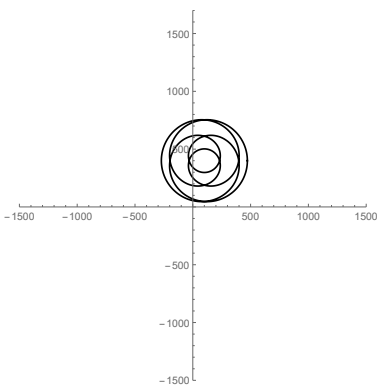
Visto de longe



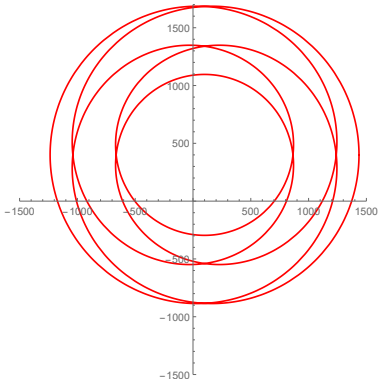
Visto de perto, no microscópio

Figura 12: *Fazendo z percorrer o círculo de raio* 2*, temos que $p(z)$ faz um desenho um pouco maior em torno de* $100 + 400i$*.*

As figuras a seguir correspondem aos casos em que z percorre os círculos de raio 3 e 4. Repare que as figuras já são bem mais visíveis.



Raio $= 3$



Raio $= 4$

Figura 13: *Fazendo z percorrer os círculos de raio 3 e 4, temos que $p(z)$ faz desenhos grandes em torno de $100 + 400i$.*

Note que para o raio igual a 4 já temos um fenômeno interessante: ao percorrermos com z uma volta em torno do círculo de raio 4, temos que $p(z)$ dá 5 voltas em torno de 0. É como se $p(z)$ orbitasse, como um planeta, em torno de 0 com um órbita um tanto peculiar, mas periódica. O número de voltas que esse "planeta"dá, esse número 5, é de fato o grau do polinômio $p(z)$. Assim, obtemos empiricamente evidência para o seguinte fenômeno: se z orbita uma vez em um círculo de raio suficientemente grande, então $p(z)$ dá n voltas em torno de 0, onde n é o grau do polinômio.

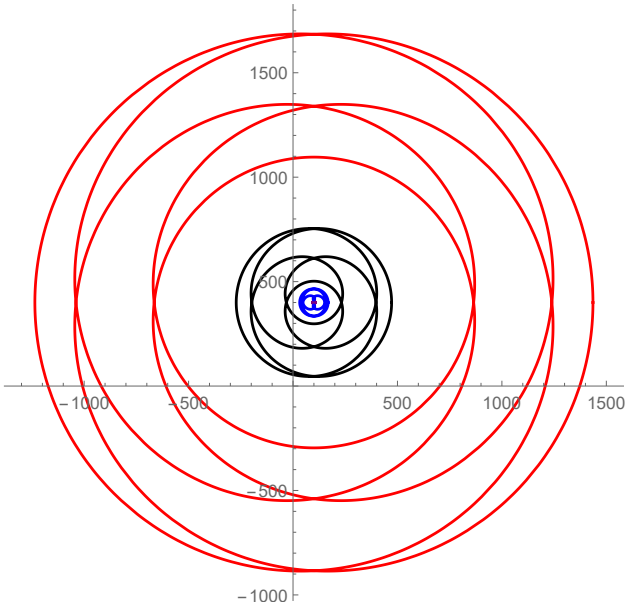


Figura 14: *Todas as orbitas juntas.*

Repare que essa órbita maior, representada na Figura 14 em vermelho, obtida por $p(z)$ com z percorrendo o círculo de raio 4, é bem próxima de um círculo de raio $4^5 = 1024$, que é a trajetória que z^5 percorre quando z percorre esse mesmo círculo de raio 4, como mostra a Figura 15.

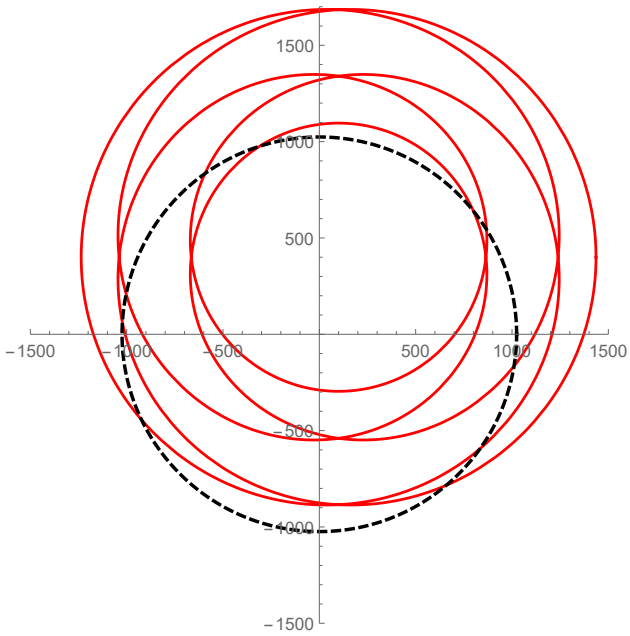
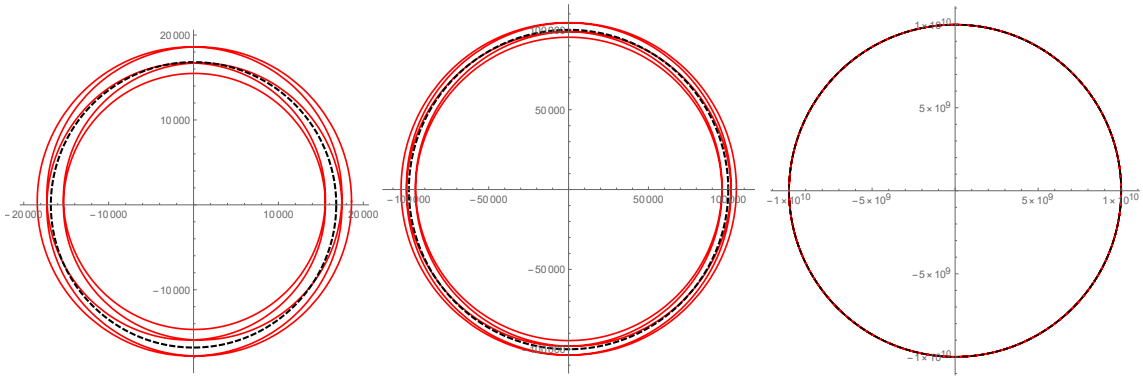


Figura 15: *Na figura temos o trajeto de $z \mapsto p(z)$ e $z \mapsto z^5$ quando z percorre o círculo de raio 4.*

Se pegarmos raios maiores, a proximidade dessas duas órbitas fica ainda mais aparente como mostra a figura a seguir:



Raio $= 7$ *Raio* $= 10$ *Raio* $= 100$

Figura 16: *As órbitas de $z \mapsto z^5$ e $z \mapsto p(z)$ se tornam indistinguíveis ao percorremos z ao longo de círculos de raio grande.*

Você pode não ter percebido, mas já provamos que nosso polinômio $p(z)$ tem raiz. Se pegarmos o círculo de raio $r = 100$, sobre o qual z percorre, e começarmos a diminuir o raio, temos que a órbita dada por $z \mapsto p(z)$ vai se deformando aos pouquinhos, como se fosse um laço feito de barbante e fossemos movendo ele aos poucos, deixando ele cada vez menor. Note que enquanto estamos reduzindo r de 100 até 4 a órbita dada por $p(z)$ continua dando 5 voltas em torno 0, imitando $z \mapsto z^5$. No entanto, quando chegamos no raio $r = 1$, vemos que $p(z)$ não dá nenhuma volta em torno de 0. Ou seja, fomos de um laço que dá 5 voltas em torno de 0 para um laço que não dá nenhuma volta em torno de 0. A única possibilidade é que para algum r entre 4 e 1 o laço

passou sobre o ponto 0. Então, algum ponto z_0 nesse círculo de raio r é levado no 0. Portanto, temos $p(z_0) = 0$.

Assim, o fato de murcharmos um laço que dá 5 voltas em torno do zero, para um laço que não dá voltas em torno de 0 nos garante que para algum z_0 temos $p(z_0) = 0$, ou seja, uma raiz.

Veja que coisa milagrosa: pegamos um polinômio horrível como $p(z) = z^5 + 5z^3 - 2z + 100 + 400i$ e apenas brincando com laços encontramos uma raiz. No entanto, repare que esse argumento não diz nada sobre a raiz, não nos ensina sequer como encontrá-la aproximadamente. Só nos garante a sua existência. Essa é a essência do Teorema Fundamental da Álgebra. Repare também que fomos de 5 voltas para 0 voltas em torno da origem, ou seja, passamos 5 vezes pelo zero, explicando também porque polinômios de grau 5 têm 5 raízes.

4. Um Prova Celestial

> Uma prova se torna uma prova somente depois do ato social de "aceitá-la como prova".
>
> *Yuri Manin*

O argumento empírico dado na seção anterior está em sua essência correto, no entanto, falta a nós entender porque ao carminarmos z em círculos grandes temos z^n perto de $p(z)$, comparado a distância desses pontos ao centro, onde $p(z)$ é agora um polinômio de grau n. Um bom jeito de entender isso é observar o sistema solar. Mais precisamente, olhemos para as órbitas da Terra e da Lua em torno do Sol. Primeiro repare que a Terra gira em torno do Sol em uma órbita que é praticamente circular de raio aproximadamente igual a 150.000.000 km. Já a Lua orbita a Terra em órbita circular de raio aproximadamente igual a 384.400 km. Assim, a distância Terra-Lua é por volta de 390 vezes menor que a distância Terra-Sol.

A órbita da Lua é circular apenas com respeito à Terra. Com respeito ao Sol, sua órbita é bem não circular, fazendo um trajeto de zig-zag em torno da trajetória da Terra, como mostra a figura a seguir.

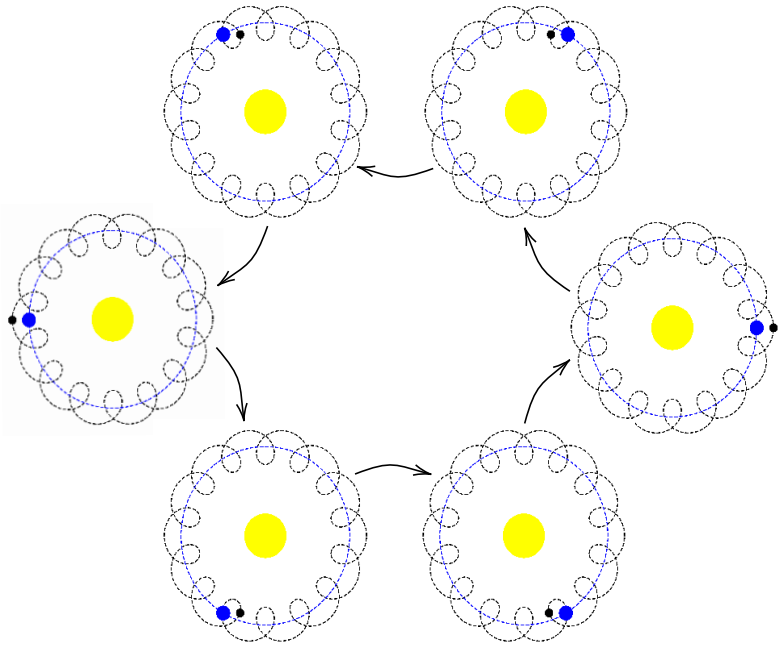


Figura 17: *Movimento da Terra e da Lua em torno do Sol em várias épocas do ano.*

Embora a Lua tenha órbita bem estranha com respeito ao Sol, como ela está presa perto da Terra, sabemos que se a Terra der n voltas em torno do Sol, então a Lua fará o mesmo.

Voltemos ao polinômio $p(z) = z^n + a_{n-1}z^{n-1} + \cdots + a_1 z + a_0$. Seja R o raio do círculo sobre o qual z vai percorrer. Vamos tomar esse R bem grande.

Agora repare que se z está no círculo de raio R, então[5]

$$|p(z) - z^n| = |a_{n-1}z^{n-1} + \cdots + a_1 z + a_0| \leq |a_{n-1}z^{n-1}| + \cdots + |a_1 z| + |a_0|$$

e como $|a_k z^k| = |a_k||z^k| = |a_k|R^k$, temos

$$|p(z) - z^n| \leq R^{n-1}|a_{n-1}| + \cdots + R|a_1| + |a_0|. \tag{5}$$

Desta forma

$$\frac{|p(z) - z^n|}{R^n} \leq \frac{|a_{n-1}|}{R} + \cdots + \frac{|a_1|}{R^{n-1}} + \frac{|a_0|}{R^n}.$$

e tomando R muito grande, podemos supor que cada fator $|a_k|/R^{n-k}$ é bem pequeno.

Assim, para R muito grande temos, por exemplo,

$$\frac{|p(z) - z^n|}{R^n} \leq \frac{1}{390},$$

ou seja,

$$|p(z) - z^n| < \frac{R^n}{390}.$$

[5]Aqui estamos usando a desigualdade $|z_1 + z_2 + \cdots + z_k| \leq |z_1| + |z_2| + \cdots + |z_k|$, que pode ser provada da desigualdade triangular $|z + w| \leq |z| + |w|$, cuja prova deixarei ao cargo do leitor (Dica! Desenhe o triângulo com vértices 0, z e $-w$ e repare que o caminho mais curto entre dois pontos é o segmento de reta que os conecta).

Então, para cada z no círculo de raio R temos que z^n está a uma distância R^n do centro e a distância entre z^n e $p(z)$ é no máximo $R^n/390$. Então, se z der uma volta em torno desse círculo de raio R, então z^n dará n voltas em torno de 0 sobre um círculo de raio R^n. Como $p(z)$ está relativamente próximo de z^n, temos que $p(z)$ dará n voltas em torno de 0. Em outras palavras, o ponto 0 é como o Sol, z^n é como a Terra e $p(z)$ é como a Lua.

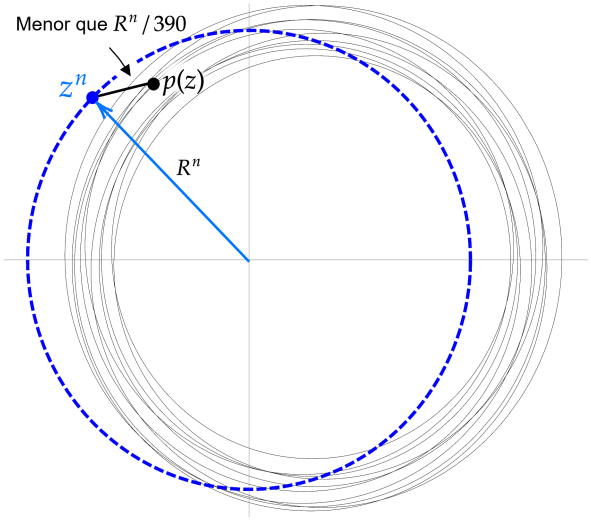


Figura 18: *Movimento da $p(z)$ e z^n em torno do 0 conforme z varia no círculo de raio R.*

Para finalizar o argumento fazemos como na seção anterior, tomamos z em círculos de raios cada vez menores começando em R. Se o polinômio $p(z)$ tiver seu termo a_0 nulo, então não há nada para provar, pois $z = 0$ será raiz. Desta forma, podemos supor que $a_0 \neq 0$. Começando com o raio R temos que $p(z)$ dá n voltas em torno de 0. Já tomando z em um círculo infinitamente pequeno, temos que $p(z)$ fica bem próximo de a_0, ou seja, $p(z)$ não dá nenhuma volta em torno de 0. Então, deve existir algum r entre 0 e R para o qual o laço obtido por $p(z)$, com $|z| = r$, passa por zero. Assim, existe z_0 satisfazendo $|z_0| = r$ e $p(z_0) = 0$.

Repare também que assim como na seção anterior, o procedimento acima explica porque polinômios de grau n tem n raízes.

Isso finaliza a demonstração. Por fim, gostaria de dizer que essa técnica planetária é normalmente conhecida em Matemática como Teorema Rouché, que é estudado nos cursos básicos de cálculo em uma variável complexa com uma roupagem mais sofisticada.

5. Minhas Últimas Palavras

> Qualquer bom teorema deve ter várias provas, quanto mais, melhor.
>
> *Michael Atiyah*

O processo de investigação de zeros de polinômios não para por ai, muito pelo contrário, é o início da Geometria Algébrica. Se considerarmos polinômios em duas variáveis, isto é, funções obtidas a partir de duas variáveis z e w, números complexos e as operações $+$ e $\times$, então podemos também estudar seus zeros. Por exemplo, se nosso polinômio é $z^2 + w^2 + 1$, então podemos estudar o conjunto dos zeros

$$\{(z, w) \in \mathbb{C}^2 : z^2 + w^2 + 1 = 0\}.$$

Ao contrário do que ocorre com uma variável, esse conjunto de zeros é um objeto 2-dimensional e, portanto, infinto dentro de $\mathbb{C}^2$, que é um espaço 4-dimensional. O estudo de espaços desse tipo, dados por zeros de polinômios, é o que se chama de Geometria Algébrica. O Teorema Fundamental da Álgebra é a razão pela qual o conjunto de zeros de um polinômio em duas ou mais variáveis é não vazio, dado que o polinômio não seja constante. Esse teorema se chama Nullstellensatz de Hilbert, que é em essência a versão geral do Teorema Fundamental da Álgebra. No entanto, esse fato não vale se estivermos estudando polinômios sobre os números reais. Por exemplo, o conjunto

$$\{(x, y) \in \mathbb{R}^2 : x^2 + y^2 + 1 = 0\}$$

é vazio.

Por fim deixe me acrescentar que, assim como ocorre com o Teorema de Pitágoras, há dezenas de provas do Teorema Fundamental da Álgebra, como mostra essa bela lista [MO] no mathoverflow. Além disso, o Teorema Fundamental da Álgebra faz com que o estudo da geometria sobre $\mathbb{C}$ seja muito mais fácil em geral que o da geometria sobre $\mathbb{R}$. E isso não se resume a geometria, o mesmo ocorre para as mais diversas áreas da Matemática.

Referências

[Abl] Wikipedia. Niels Henrik Abel.
`https://en.wikipedia.org/wiki/Niels_Henrik_Abel`. Acesso em 29/02/2020.

[Ale] V.B. Alekseev. Abel's Theorem in Problems and Solutions: Based on the lectures of Professor VI Arnold. Springer Science & Business Media, 2004.

[Gal] Wikipedia. Évariste Galois.
`https://en.wikipedia.org/wiki/Evariste_Galois`. Acesso em 29/02/2020.

[Gau] Wikipedia. Carl Friedrich Gauss.
`https://en.wikipedia.org/wiki/Carl_Friedrich_Gauss`. Acesso em 29/02/2020.

[Gol] L. Goldmakher. Arnold's Elementary Proof of the Insolvability of the Quintic.
`www.williams.edu/Mathematics/lg5/394/ArnoldQuintic.pdf`. Acesso em 29/02/2020.

[MO] `www.mathoverflow.net/questions/10535/ways-to-prove-the-fundamental-theorem-of-algebra`. Acesso em 29/02/2020.