A raiz do ~~problema~~ polinômio

Thiago Landim

Julho 2020

História

Quem provou o Teorema Fundamental da Álgebra?

História

Quem provou o Teorema Fundamental da Álgebra?

- Girard?

História

Quem provou o Teorema Fundamental da Álgebra?

- Girard?
- Foi o primeiro e enunciar o Teorema Fundamental da Álgebra! (1629)

História

Quem provou o Teorema Fundamental da Álgebra?

- Girard?
- D'Alembert?

História

Quem provou o Teorema Fundamental da Álgebra?

- Girard?
- D'Alembert?

- Primeiro a "demonstrar" o TFA!

História

Quem provou o Teorema Fundamental da Álgebra?

- Girard?
- D'Alembert?

- Primeiro a "demonstrar" o TFA!
- Assumiu um teorema que só iria ser provado um século depois **cuja demonstração usa o TFA**...

História

Quem provou o Teorema Fundamental da Álgebra?

- Girard?
- D'Alembert?
- Euler?

História

Quem provou o Teorema Fundamental da Álgebra?

- Girard?
- D'Alembert?
- Euler?

- Ideia genial... mas falha

História

Quem provou o Teorema Fundamental da Álgebra?

- Girard?
- D'Alembert?
- Euler?

- Ideia genial... mas falha
- "Um polinômio de grau 2^n pode ser fatorado em dois polinômios de grau 2^{n-1}."

História

Quem provou o Teorema Fundamental da Álgebra?

- Girard?
- D'Alembert?
- Euler?
- Lagrange?

História

Quem provou o Teorema Fundamental da Álgebra?

- Girard?
- D'Alembert?
- Euler?
- Lagrange?

- Primeira solução satisfatória?

História

Quem provou o Teorema Fundamental da Álgebra?

- Girard?
- D'Alembert?
- Euler?
- Lagrange?
- Gauss?

História

Quem provou o Teorema Fundamental da Álgebra?

- Girard?
- D'Alembert?
- Euler?
- Lagrange?
- Gauss?

- "Todas as soluções anteriores assumiam a *existência* de raízes..."

História

Quem provou o Teorema Fundamental da Álgebra?

- Girard?
- D'Alembert?
- Euler?
- Lagrange?
- Gauss?

- "Todas as soluções anteriores assumiam a *existência* de raízes..."
- Dá uma demonstração geométrica!

História

Quem provou o Teorema Fundamental da Álgebra?

- Girard?
- D'Alembert?
- Euler?
- Lagrange?
- Gauss?

- "Todas as soluções anteriores assumiam a *existência* de raízes..."
- Dá uma demonstração geométrica!
- Infelizmente também incompleta...

História

Quem provou o Teorema Fundamental da Álgebra?

- Girard?
- D'Alembert?
- Euler?
- Lagrange?
- Gauss?
- Argand!

História

Quem provou o Teorema Fundamental da Álgebra?

- Girard?
- D'Alembert?
- Euler?
- Lagrange?
- Gauss?
- Argand!

- Primeira demonstração completa!

História

Quem provou o Teorema Fundamental da Álgebra?

- Girard?
- D'Alembert?
- Euler?
- Lagrange?
- Gauss?
- Argand!

- Primeira demonstração completa!
- Nova ideia

TFA à Argand

Teorema

Todo polinômio $p \in \mathbb{C}[z]$ *tem raiz complexa.*

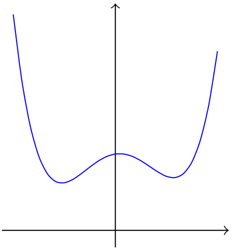
TFA à Argand

Teorema

Todo polinômio $p \in \mathbb{C}[z]$ tem raiz complexa.

- Se $|z| \to \infty$, então $|p(z)| \to \infty$;

$$|z^3 - z| = |z|^3 \left|1 - \frac{1}{z^2}\right|$$



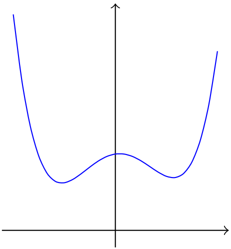
TFA à Argand

Teorema

Todo polinômio $p \in \mathbb{C}[z]$ tem raiz complexa.

- Se $|z| \to \infty$, então $|p(z)| \to \infty$;
- Existe $z_0 \in \mathbb{C}$ tal que $p(z_0) = \min|p(z)|$;

$$|z^3 - z| = |z|^3 \left|1 - \frac{1}{z^2}\right|$$

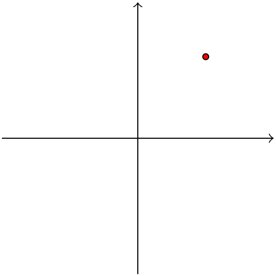


TFA à Argand

Teorema

Todo polinômio $p \in \mathbb{C}[z]$ tem raiz complexa.

- Se $|z| \to \infty$, então $|p(z)| \to \infty$;
- Existe $z_0 \in \mathbb{C}$ tal que $p(z_0) = \min|p(z)|$;

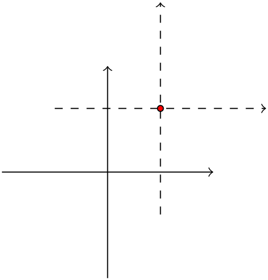


TFA à Argand

Teorema

Todo polinômio $p \in \mathbb{C}[z]$ tem raiz complexa.

- Se $|z| \to \infty$, então $|p(z)| \to \infty$;
- Existe $z_0 \in \mathbb{C}$ tal que $p(z_0) = \min |p(z)|$;
- $p(z) = a_0 + a_p z^p + z^{p+1} R(z)$;

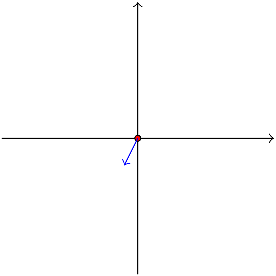


TFA à Argand

Teorema

Todo polinômio $p \in \mathbb{C}[z]$ tem raiz complexa.

- Se $|z| \to \infty$, então $|p(z)| \to \infty$;
- Existe $z_0 \in \mathbb{C}$ tal que $p(z_0) = \min|p(z)|$;
- $p(z) = a_0 + a_p z^p + z^{p+1}R(z)$;



TFA à Argand

Teorema

Todo polinômio $p \in \mathbb{C}[z]$ tem raiz complexa.

- Se $|z| \to \infty$, então $|p(z)| \to \infty$;
- Existe $z_0 \in \mathbb{C}$ tal que $p(z_0) = \min|p(z)|$;
- $p(z) = a_0 + a_p z^p + z^{p+1} R(z)$;

- $a_0 \in \mathbb{R}$ e $a_0 > 0$;

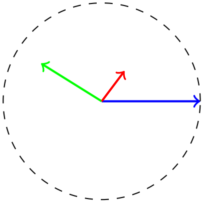
TFA à Argand

Teorema

Todo polinômio $p \in \mathbb{C}[z]$ tem raiz complexa.

- Se $|z| \to \infty$, então $|p(z)| \to \infty$;
- Existe $z_0 \in \mathbb{C}$ tal que $p(z_0) = \min|p(z)|$;
- $p(z) = a_0 + a_p z^p + z^{p+1}R(z)$;

- $a_0 \in \mathbb{R}$ e $a_0 > 0$;



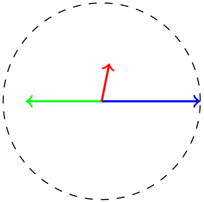
TFA à Argand

Teorema

Todo polinômio $p \in \mathbb{C}[z]$ tem raiz complexa.

- Se $|z| \to \infty$, então $|p(z)| \to \infty$;
- Existe $z_0 \in \mathbb{C}$ tal que $p(z_0) = \min |p(z)|$;
- $p(z) = a_0 + a_p z^p + z^{p+1} R(z)$;

- $a_0 \in \mathbb{R}$ e $a_0 > 0$;



TFA à Argand

Teorema

Todo polinômio $p \in \mathbb{C}[z]$ tem raiz complexa.

- Se $|z| \to \infty$, então $|p(z)| \to \infty$;
- Existe $z_0 \in \mathbb{C}$ tal que $p(z_0) = \min|p(z)|$;
- $p(z) = a_0 + a_p z^p + z^{p+1}R(z)$;

- $a_0 \in \mathbb{R}$ e $a_0 > 0$;
- Ideal: $a_p z^p < 0$;

TFA à Argand

Teorema

Todo polinômio $p \in \mathbb{C}[z]$ tem raiz complexa.

- Se $|z| \to \infty$, então $|p(z)| \to \infty$;
- Existe $z_0 \in \mathbb{C}$ tal que $p(z_0) = \min|p(z)|$;
- $p(z) = a_0 + a_p z^p + z^{p+1} R(z)$;

- $a_0 \in \mathbb{R}$ e $a_0 > 0$;
- Ideal: $a_p z^p < 0$;
- $a_p = r_p e^{i\theta_p}$;

TFA à Argand

Teorema

Todo polinômio $p \in \mathbb{C}[z]$ tem raiz complexa.

- Se $|z| \to \infty$, então $|p(z)| \to \infty$;
- Existe $z_0 \in \mathbb{C}$ tal que $p(z_0) = \min|p(z)|$;
- $p(z) = a_0 + a_p z^p + z^{p+1}R(z)$;

- $a_0 \in \mathbb{R}$ e $a_0 > 0$;
- Ideal: $a_p z^p < 0$;
- $a_p = r_p e^{i\theta_p}$;
- $z = \varepsilon e^{i\pi/p} e^{-i\theta_p/p}$.

TFA à Argand

Teorema

Todo polinômio $p \in \mathbb{C}[z]$ tem raiz complexa.

- Se $|z| \to \infty$, então $|p(z)| \to \infty$;
- Existe $z_0 \in \mathbb{C}$ tal que $p(z_0) = \min |p(z)|$;
- $p(z) = a_0 + a_p z^p + z^{p+1} R(z)$;

- $a_0 \in \mathbb{R}$ e $a_0 > 0$;
- Ideal: $a_p z^p < 0$;
- $a_p = r_p e^{i\theta_p}$;
- $z = \varepsilon e^{i\pi/p} e^{-i\theta_p/p}$.
- $a_p z^p = r_p \varepsilon^p (-1)$

TFA à Argand

Teorema

Todo polinômio $p \in \mathbb{C}[z]$ tem raiz complexa.

- Se $|z| \to \infty$, então $|p(z)| \to \infty$;
- Existe $z_0 \in \mathbb{C}$ tal que $p(z_0) = \min|p(z)|$;
- $p(z) = a_0 + a_p z^p + z^{p+1}R(z)$;

- $a_0 \in \mathbb{R}$ e $a_0 > 0$;
- Ideal: $a_p z^p < 0$;
- $a_p = r_p e^{i\theta_p}$;
- $z = \varepsilon e^{i\pi/p} e^{-i\theta_p/p}$.
- $a_p z^p = r_p \varepsilon^p (-1)$
- $R(z) \leq C$

TFA à Argand

Teorema

Todo polinômio $p \in \mathbb{C}[z]$ tem raiz complexa.

- Se $|z| \to \infty$, então $|p(z)| \to \infty$;
- Existe $z_0 \in \mathbb{C}$ tal que $p(z_0) = \min|p(z)|$;
- $p(z) = a_0 + a_p z^p + z^{p+1}R(z)$;
- $$\begin{aligned} |p(z)| &\leq a_0 - r_p\varepsilon^p + C\varepsilon^{p+1} \\ &\leq a_0 - \varepsilon^p(r_p - C\varepsilon) \\ &< a_0. \end{aligned}$$

- $a_0 \in \mathbb{R}$ e $a_0 > 0$;
- Ideal: $a_p z^p < 0$;
- $a_p = r_p e^{i\theta_p}$;
- $z = \varepsilon e^{i\pi/p} e^{-i\theta_p/p}$.
- $a_p z^p = r_p \varepsilon^p(-1)$
- $R(z) \leq C$

Polinômios Simétricos

O que diferencia $f(a,b) = a + b$ de $g(a,b) = a - b$?

Polinômios Simétricos

O que diferencia $f(a,b) = a + b$ de $g(a,b) = a - b$?

Resposta: f é **simétrico** na variáveis a e b.

Polinômios Simétricos

O que diferencia $f(a, b) = a + b$ de $g(a, b) = a - b$?

Resposta: f é **simétrico** na variáveis a e b.

Por que f é simétrico nas variáveis a e b?

Polinômios Simétricos

O que diferencia $f(a,b) = a + b$ de $g(a,b) = a - b$?

Resposta: f é **simétrico** na variáveis a e b.

Por que f é simétrico nas variáveis a e b?

Resposta: Porque ele é o coeficiente de um polinômio com raízes a e b.

Polinômios Simétricos

O que diferencia $f(a,b) = a+b$ de $g(a,b) = a-b$?

Resposta: f é **simétrico** na variáveis a e b.

Por que f é simétrico nas variáveis a e b?

Resposta: Porque ele é o coeficiente de um polinômio com raízes a e b.

Mais ainda, ele é um dos **blocos básicos** *dos polinômios simétricos*!

Polinômios Simétricos - Exemplo 1

Suponha que a e b sejam raízes do polinômio

$$f(x) = x^2 - sx + p,$$

onde $s = a + b$ e $p = ab$.

Polinômios Simétricos - Exemplo 1

Suponha que a e b sejam raízes do polinômio

$$f(x) = x^2 - sx + p,$$

onde $s = a + b$ e $p = ab$.

Qual polinômio tem como raízes a^2 e b^2?

Polinômios Simétricos - Exemplo 1

Suponha que a e b sejam raízes do polinômio

$$f(x) = x^2 - sx + p,$$

onde $s = a + b$ e $p = ab$.

Qual polinômio tem como raízes a^2 e b^2?

$$g(x) = x^2 - (s^2 - 2p)x + p^2,$$

pois $a^2 + b^2 = (a + b)^2 - 2ab = s^2 - 2p$.

Polinômios Simétricos - Exemplo 2

Suponha que a, b e c são as raízes do polinômio

$$f(x) = x^3 - sx^2 + px - q,$$

onde $s = a + b + c$, $p = ab + bc + ca$ e $q = abc$.

Polinômios Simétricos - Exemplo 2

Suponha que a, b e c são as raízes do polinômio

$$f(x) = x^3 - sx^2 + px - q,$$

onde $s = a + b + c$, $p = ab + bc + ca$ e $q = abc$.

Qual polinômio tem raízes $a + b$, $b + c$ e $c + a$?

Polinômios Simétricos - Exemplo 2

Suponha que a, b e c são as raízes do polinômio

$$f(x) = x^3 - sx^2 + px - q,$$

onde $s = a + b + c$, $p = ab + bc + ca$ e $q = abc$.

Qual polinômio tem raízes $a + b$, $b + c$ e $c + a$?

$$g(x) = x^3 - 2sx^2 + (p + s^2)x - (ps - q)$$

Teorema Fundamental dos Polinômios Simétricos

Teorema

Suponha que $r_1, r_2, \ldots, r_n$ *são as raízes do polinômio*

$$f(x) = x^n - a_1 x^{n-1} + \cdots + (-1)^{n-1} a_{n-1} x + (-1)^n a_n,$$

e suponha que o polinômio

$$g(x) = x^m - b_1 x^{m-1} + \ldots + (-1)^{m-1} b_{m-1} x + (-1) b_m$$

tem raízes que dependem de maneira simétrica de $r_1, r_2, \ldots, r_n$*. Então cada* b_i *é um polinômio em* $a_1, a_2, \ldots, a_n$*.*

TFA à Lagrange

Teorema

Todo polinômio $f \in \mathbb{R}[x]$ *tem raiz complexa.*

TFA à Lagrange

Teorema

Todo polinômio $f \in \mathbb{R}[x]$ tem raiz complexa.

Suficiente, pois:

- Se $f(x) = x^n + a_1 x^{n-1} + \cdots + a_n$ tem coeficiente complexos, definimos

$$\overline{f}(x) = x^n + \overline{a_1} x^{n-1} + \cdots + \overline{a_n}.$$

TFA à Lagrange

Teorema

Todo polinômio $f \in \mathbb{R}[x]$ tem raiz complexa.

Suficiente, pois:

- Se $f(x) = x^n + a_1 x^{n-1} + \cdots + a_n$ tem coeficiente complexos, definimos

$$\overline{f}(x) = x^n + \overline{a_1} x^{n-1} + \cdots + \overline{a_n}.$$

- $\mathfrak{z}$ é raiz de f se e somente se $\overline{\mathfrak{z}}$ é raiz de $\overline{f}$.

TFA à Lagrange

Teorema

Todo polinômio $f \in \mathbb{R}[x]$ tem raiz complexa.

Suficiente, pois:

- Se $f(x) = x^n + a_1 x^{n-1} + \cdots + a_n$ tem coeficiente complexos, definimos

$$\overline{f}(x) = x^n + \overline{a_1} x^{n-1} + \cdots + \overline{a_n}.$$

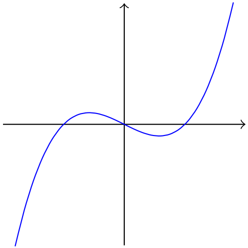
- $\mathfrak{z}$ é raiz de f se e somente se $\bar{\mathfrak{z}}$ é raiz de $\overline{f}$.
- f tem raiz se e somente se $f \cdot \overline{f} \in \mathbb{R}[x]$ tem raiz

TFA à Lagrange

Teorema

Todo polinômio $f \in \mathbb{R}[x]$ tem raiz complexa.

- Pelo Teorema do Valor Intermediário, se o grau de f é ímpar, então sabemos que existe raiz (real).



TFA à Lagrange

Teorema

Todo polinômio $f \in \mathbb{R}[x]$ tem raiz complexa.

- Podemos escrever o grau de f por $m \cdot 2^n$ para algum número ímpar m.

TFA à Lagrange

Teorema

Todo polinômio $f \in \mathbb{R}[x]$ tem raiz complexa.

- Podemos escrever o grau de f por $m \cdot 2^n$ para algum número ímpar m.
- Vamos fazer indução em n.

TFA à Lagrange

Teorema

Todo polinômio $f \in \mathbb{R}[x]$ tem raiz complexa.

- Podemos escrever o grau de f por $m \cdot 2^n$ para algum número ímpar m.
- Vamos fazer indução em n.
- O caso $n = 0$ já foi feito!

TFA à Lagrange

Teorema

Todo polinômio $f \in \mathbb{R}[x]$ tem raiz complexa.

- Podemos escrever o grau de f por $m \cdot 2^n$ para algum número ímpar m.
- Vamos fazer indução em n.
- O caso $n = 0$ já foi feito!
- Intuição por trás: Em $\mathbb{C}$, toda equação de grau 2 tem solução, o que nos permitirá reduzir a paridade.

TFA à Lagrange

Teorema

Todo polinômio $f \in \mathbb{R}[x]$ tem raiz complexa.

- Seja $f(x) = x^n + a_1 x^{n-1} + \cdots + a_n$ de grau $d = m \cdot 2^n$ e digamos que ele tenha raízes $r_1, \ldots, r_d$ em algum *corpo* maior.

TFA à Lagrange

Teorema

Todo polinômio $f \in \mathbb{R}[x]$ tem raiz complexa.

- Seja $f(x) = x^n + a_1 x^{n-1} + \cdots + a_n$ de grau $d = m \cdot 2^n$ e digamos que ele tenha raízes $r_1, \ldots, r_d$ em algum *corpo* maior.
- Para cada $c \in \mathbb{C}$, formamos o polinômio $g_c(z)$ cujas raízes são os números da forma $r_i + r_j - c r_i r_j$.

TFA à Lagrange

Teorema

Todo polinômio $f \in \mathbb{R}[x]$ tem raiz complexa.

- Seja $f(x) = x^n + a_1 x^{n-1} + \cdots + a_n$ de grau $d = m \cdot 2^n$ e digamos que ele tenha raízes $r_1, \ldots, r_d$ em algum *corpo* maior.
- Para cada $c \in \mathbb{C}$, formamos o polinômio $g_c(z)$ cujas raízes são os números da forma $r_i + r_j - c r_i r_j$.
- Como as raízes de g_c dependem de maneira simétrica dos r_i, seus coeficientes são polinômio em a_j, logo estão em $\mathbb{R}$.

TFA à Lagrange

Teorema

Todo polinômio $f \in \mathbb{R}[x]$ tem raiz complexa.

- O grau de g_c é $\binom{d}{2} = m(d-1)2^{n-1}$, logo por indução tem raiz complexa.

TFA à Lagrange

Teorema

Todo polinômio $f \in \mathbb{R}[x]$ tem raiz complexa.

- O grau de g_c é $\binom{d}{2} = m(d-1)2^{n-1}$, logo por indução tem raiz complexa.
- Assim, para cada $c \in \mathbb{C}$, existe um par (i,j) tal que $r_i + r_j - cr_ir_j$ está em $\mathbb{C}$.

TFA à Lagrange

Teorema

Todo polinômio $f \in \mathbb{R}[x]$ tem raiz complexa.

- O grau de g_c é $\binom{d}{2} = m(d-1)2^{n-1}$, logo por indução tem raiz complexa.
- Assim, para cada $c \in \mathbb{C}$, existe um par (i,j) tal que $r_i + r_j - cr_ir_j$ está em $\mathbb{C}$.
- Temos infinitos números complexos e apenas uma quantidade finita de índices.

TFA à Lagrange

Teorema

Todo polinômio $f \in \mathbb{R}[x]$ tem raiz complexa.

- O grau de g_c é $\binom{d}{2} = m(d-1)2^{n-1}$, logo por indução tem raiz complexa.
- Assim, para cada $c \in \mathbb{C}$, existe um par (i, j) tal que $r_i + r_j - cr_ir_j$ está em $\mathbb{C}$.
- Temos infinitos números complexos e apenas uma quantidade finita de índices.
- Existem $c, d \in \mathbb{C}$ distintos tais que $r_i + r_j - cr_ir_j \in \mathbb{C}$ e $r_i + r_j - dr_ir_j \in \mathbb{C}$.

TFA à Lagrange

Teorema

Todo polinômio $f \in \mathbb{R}[x]$ tem raiz complexa.

- $r_i + r_j \in \mathbb{C}$ e $r_i r_j \in \mathbb{C}$

TFA à Lagrange

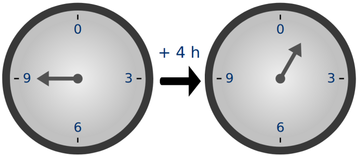
Teorema

Todo polinômio $f \in \mathbb{R}[x]$ tem raiz complexa.

- $r_i + r_j \in \mathbb{C}$ e $r_i r_j \in \mathbb{C}$
- r_i e r_j são raízes de uma equação do 2º grau com coeficientes complexos

Aritmética modular 1.0

Teoria dos Números: Aritmética de relógio



- Os inteiros podem ser complicados
- $\mathbb{Z}/n\mathbb{Z} := \{\overline{0}, \overline{1}, \overline{2}, \dots, \overline{n-1}\}$ (restos na divisão por n)
- Ignora informação inútil e adiciona estrutura boa
- Preserva soma, produto e aplicação por polinômios

Exemplos 1.0

- $\overline{n-1} + \overline{2} = \overline{n+1} = \overline{1}$ em $\mathbb{Z}/n\mathbb{Z}$

Exemplos 1.0

- $\overline{n-1} + \overline{2} = \overline{n+1} = \overline{1}$ em $\mathbb{Z}/n\mathbb{Z}$
- $\overline{n-1}^2 = \overline{n^2 - 2n + 1} = \overline{1}$ em $\mathbb{Z}/n\mathbb{Z}$

Exemplos 1.0

- $\overline{n-1} + \overline{2} = \overline{n+1} = \overline{1}$ em $\mathbb{Z}/n\mathbb{Z}$
- $\overline{n-1}^2 = \overline{n^2 - 2n + 1} = \overline{1}$ em $\mathbb{Z}/n\mathbb{Z}$
- $\overline{2} \cdot \overline{3} = \overline{6} = \overline{1}$ em $\mathbb{Z}/5\mathbb{Z}$

Exemplos 1.0

- $\overline{n-1} + \overline{2} = \overline{n+1} = \overline{1}$ em $\mathbb{Z}/n\mathbb{Z}$
- $\overline{n-1}^2 = \overline{n^2 - 2n + 1} = \overline{1}$ em $\mathbb{Z}/n\mathbb{Z}$
- $\overline{2} \cdot \overline{3} = \overline{6} = \overline{1}$ em $\mathbb{Z}/5\mathbb{Z}$
- $\overline{3} \cdot \overline{5} = \overline{15} = \overline{1}$ em $\mathbb{Z}/7\mathbb{Z}$

Exemplos 1.0

- $\overline{n-1} + \overline{2} = \overline{n+1} = \overline{1}$ em $\mathbb{Z}/n\mathbb{Z}$
- $\overline{n-1}^2 = \overline{n^2 - 2n + 1} = \overline{1}$ em $\mathbb{Z}/n\mathbb{Z}$
- $\overline{2} \cdot \overline{3} = \overline{6} = \overline{1}$ em $\mathbb{Z}/5\mathbb{Z}$
- $\overline{3} \cdot \overline{5} = \overline{15} = \overline{1}$ em $\mathbb{Z}/7\mathbb{Z}$
- Se $p(x) = x^2 - 2$, então $p(\overline{3}) = 0$ em $\mathbb{Z}/7\mathbb{Z}$, pois

$$p(\overline{3}) = \overline{3}^2 - \overline{2} = \overline{9} - \overline{2} = \overline{7} = \overline{0}.$$

Portanto $\overline{3} = \sqrt{2}$ em $\mathbb{Z}/7\mathbb{Z}$.

Aritmética modular 2.0

Polinômios: Não tem mais relógio :(

- Os polinômios **são** complicados
- $\mathbb{C}[x]/(p(x)) := \{\text{restos na divisão por } p(z)\}$
- Ignora informação inútil e adiciona estrutura boa
- $f(\overline{x}) = \overline{f(x)}$ para todo polinômio f

Exemplos 2.0

- $\overline{x}^2 = \overline{x^2 + 1 - 1} = \overline{-1}$ em $\mathbb{C}[x]/(x^2+1)$

Exemplos 2.0

- $\overline{x}^2 = \overline{x^2 + 1 - 1} = \overline{-1}$ em $\mathbb{C}[x]/(x^2 + 1)$
- $\overline{(x-1)} \cdot \overline{(x+1)} = \overline{x^2 - 1} = \overline{0}$ em $\mathbb{C}[x]/(x^2 - 1)$

Exemplos 2.0

- $\overline{x}^2 = \overline{x^2+1-1} = \overline{-1}$ em $\mathbb{C}[x]/(x^2+1)$
- $\overline{(x-1)} \cdot \overline{(x+1)} = \overline{x^2-1} = \overline{0}$ em $\mathbb{C}[x]/(x^2-1)$
- Em $\mathbb{C}[x]/(x^2+1)$, vale que

$$\begin{aligned} \overline{x+3} \cdot \overline{x+7} &= \overline{x^2+10x+21} \\ &= \overline{10x+21-1} \\ &= \overline{10(x+1)} \end{aligned}$$

Extensão de Corpos

O protótipo de toda extensão de corpos é $\mathbb{R} \subset \mathbb{C}$.

Extensão de Corpos

O protótipo de toda extensão de corpos é $\mathbb{R} \subset \mathbb{C}$.

- Note que $i \notin \mathbb{R}$ e ele adiciona uma raiz à equação $x^2 + 1 = 0$

Extensão de Corpos

O protótipo de toda extensão de corpos é $\mathbb{R} \subset \mathbb{C}$.

- Note que $i \notin \mathbb{R}$ e ele adiciona uma raiz à equação $x^2 + 1 = 0$
- "Todo complexo pode ser escrito da forma $a + bi$" $=$ "Todo resto de $x^2 + 1$ é da forma $a + bx$"

Extensão de Corpos

O protótipo de toda extensão de corpos é $\mathbb{R} \subset \mathbb{C}$.

- Note que $i \notin \mathbb{R}$ e ele adiciona uma raiz à equação $x^2 + 1 = 0$
- "Todo complexo pode ser escrito da forma $a + bi$" $=$ "Todo resto de $x^2 + 1$ é da forma $a + bx$"
- $\mathbb{C} = \mathbb{R}[x]/(x^2 + 1)$

Extensão de Corpos

O protótipo de toda extensão de corpos é $\mathbb{R} \subset \mathbb{C}$.

- Note que $i \notin \mathbb{R}$ e ele adiciona uma raiz à equação $x^2 + 1 = 0$
- "Todo complexo pode ser escrito da forma $a + bi$" $=$ "Todo resto de $x^2 + 1$ é da forma $a + bx$"
- $\mathbb{C} = \mathbb{R}[x]/(x^2 + 1)$
- Note que, em $\mathbb{R}[x]/(x^2 + 1)$, $\overline{x}^2 + 1 = \overline{x^2 + 1} = \overline{0}$

Extensão de Corpos - Continuação

- $\overline{a + bx} + \overline{c + dx} = \overline{(a + b) + (b + d)x}$

Extensão de Corpos - Continuação

- $\overline{a+bx}+\overline{c+dx}=\overline{(a+b)+(b+d)x}$
- $\overline{a+bx}\cdot\overline{c+dx}=\overline{ac+(bc+ad)x+bdx^2}$
  $=\overline{(ac-bd)+(bc+ad)x}$

Extensão de Corpos - Continuação

- $\overline{a+bx} + \overline{c+dx} = \overline{(a+b)+(b+d)x}$
- $\overline{a+bx} \cdot \overline{c+dx} = \overline{ac+(bc+ad)x+bdx^2}$
  $= \overline{(ac-bd)+(bc+ad)x}$
- Assim, $i \in \mathbb{C}$ e $\overline{x} \in \mathbb{R}[x]/(x^2+1)$ exercem o mesmo papel

Extensão de Corpos - Além

Por outro lado, não tem nada de especial no polinômio $x^2 + 1$...

Extensão de Corpos - Além

Por outro lado, não tem nada de especial no polinômio $x^2 + 1$...
Exemplo 2: $\mathbb{R}[x]/(x^2 + x + 1)$

Tem a mesma operação de soma e a "mesma" operação de produto:

- $$\begin{aligned} \overline{a + bx} \cdot \overline{c + dx} &= \overline{ac + (bc + ad)x + bdx^2} \\ &= \overline{(ac - bd) + (bc + ad - bd)x} \end{aligned}$$

Extensão de Corpos - Além

Por outro lado, não tem nada de especial no polinômio $x^2 + 1$...

Exemplo 2: $\mathbb{R}[x]/(x^2 + x + 1)$

Tem a mesma operação de soma e a "mesma" operação de produto:

- $\overline{a + bx} \cdot \overline{c + dx} = \overline{ac + (bc + ad)x + bdx^2}$
  $= \overline{(ac - bd) + (bc + ad - bd)x}$
- Nesse caso, adicionamos uma raiz ao polinômio $x^2 + x + 1$

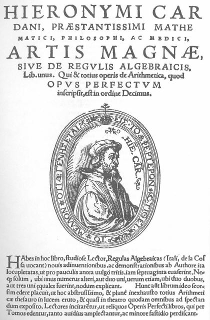
Teorema de Kronecker

Teorema

Seja f um polinômio em $\mathbb{R}[x]$. Existe um corpo K contendo $\mathbb{R}$ tal que f tem raiz em K. Mais geralmente, podemos encontrar um corpo com todas as raízes de f.

História

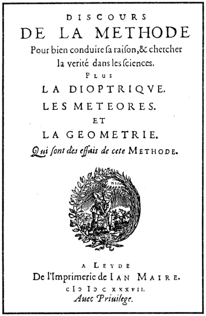
- Idade Média


HIERONYMI CAR
DANI, PRÆSTANTISSIMI MATHE
MATICI, PHILOSOPHI, AC MEDICI,
ARTIS MAGNÆ,
SIVE DE REGVLIS ALGEBRAICIS,
Lib. unus. Qui & totius operis de Arithmetica, quod
OPVS PERFECTVM
inscripsit, est in ordine Decimus.

HAbes in hoc libro, studiose Lector, Regulas Algebraicas (Itali, de la Cossa uocant) nouis adinuentionibus, ac demonstrationibus ab Authore ita locupletatas, ut pro pauculis antea uulgò tritis, iam septuaginta euaserint. Neq; solum, ubi unus numerus alteri, aut duo uni, uerum etiam, ubi duo duobus, aut tres uni æquales fuerint, nodum explicant. Hunc aũt librum ideo seorsim edere placuit, ut hoc abstrusissimo, & planè inexhausto totius Arithmeticæ thesauro in lucem eruto, & quasi in theatro quodam omnibus ad spectandum exposito, Lectores incitarẽtur, ut reliquos Operis Perfecti libros, qui per Tomos edentur, tanto auidius amplectantur, ac minore fastidio perdiscant.

História

- Idade Média
- Descartes


DISCOURS
DE LA METHODE
Pour bien conduire sa raison, & chercher
la verité dans les sciences.
PLUS
LA DIOPTRIQVE.
LES METEORES.
ET
LA GEOMETRIE.
Qui sont des essais de cete METHODE.

A LEYDE
De l'Imprimerie de IAN MAIRE.
cIↃ IↃ c XXXVII.
Avec Privilege.

História

- Idade Média
- Descartes
- Budan-Fourier

História

- Idade Média
- Descartes
- Budan-Fourier
- Sturm

História

- Idade Média
- Descartes
- Budan-Fourier
- Sturm
- Teorema de Abel-Ruffini

Viète

Em 1593, Adriaen van Roomen desafiou outros matemáticos a encontrarem uma raiz de

$$\begin{aligned} A = \ & x^{45} - 45x^{43} + 945x^{41} - 12300x^{39} + 111150x^{37} - 740259x^{35} \\ & + 3764565x^{33} - 14945040x^{31} + 46955700x^{29} - 117679100x^{27} \\ & + 236030652x^{25} - 37865800x^{23} + 483841800x^{21} - 488494125x^{19} \\ & + 384942237x^{17} - 232676280x^{15} + 105306075x^{13} - 3451207x^{11} \\ & + 7811375x^{9} - 1138500x^{7} + 95634x^{5} - 3795x^{3} + 45x, \end{aligned}$$

Viète

Em 1593, Adriaen van Roomen desafiou outros matemáticos a encontrarem uma raiz de

$$\begin{aligned} A = {} & x^{45} - 45x^{43} + 945x^{41} - 12300x^{39} + 111150x^{37} - 740259x^{35} \\ & + 3764565x^{33} - 14945040x^{31} + 46955700x^{29} - 117679100x^{27} \\ & + 236030652x^{25} - 37865800x^{23} + 483841800x^{21} - 488494125x^{19} \\ & + 384942237x^{17} - 232676280x^{15} + 105306075x^{13} - 3451207x^{11} \\ & + 7811375x^{9} - 1138500x^{7} + 95634x^{5} - 3795x^{3} + 45x, \end{aligned}$$

onde

$$A = \sqrt{\frac{7}{4} - \sqrt{\frac{5}{16} - \sqrt{\frac{15}{8} - \sqrt{\frac{45}{64}}}}}.$$

Regra de Descartes - Exemplos

Exemplo baby: Quantas raízes reais positivas tem o polinômio

$$x^6 + x^4 + x^3 + x + 1 = 0?$$

Regra de Descartes - Exemplos

Exemplo baby: Quantas raízes reais positivas tem o polinômio

$$x^6 + x^4 + x^3 + x + 1 = 0?$$

Exemplo papa: Quantas raízes reais positivas tem o polinômio

$$x^6 + x^4 - x^3 - x - 1 = 0?$$

Regra de Descartes - Enunciado

Denote por $V(a_1, \ldots, a_n)$ a quantidade de mudanças de sinais da sequência $a_1, \ldots, a_n$.
Exemplo: $V(-1, 0, 1, 1, 0, 2, -7) = 2$.

Teorema

Seja $r_+(f)$ a quantidade de raízes reais positivas de $f \in \mathbb{R}[x]$. Então

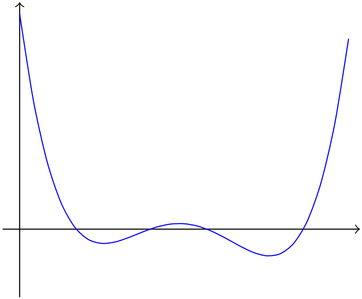
$$r_+(f) \leq V(a_1, \ldots, a_n).$$

Além disso, a diferença entre esses dois números é par.

Regra de Descartes - Demonstração

Escreva $f(x) = a_0 + \ldots + a_n x^n$. Primeiro provaremos a paridade. Para tanto, separaremos em dois casos:

Se $\text{sgn}(a_0) = \text{sgn}(a_n)$**:**

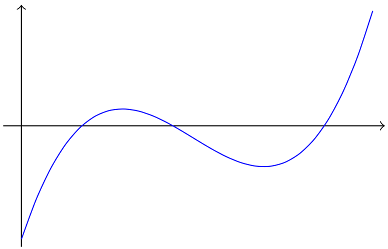


(+,+,-,-,+,-,+)

Regra de Descartes - Demonstração

Escreva $f(x) = a_0 + \ldots + a_n x^n$. Primeiro provaremos a paridade. Para tanto, separaremos em dois casos:

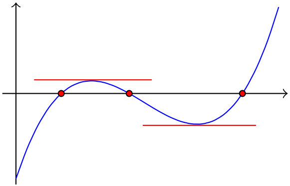
Se $\operatorname{sgn}(a_0) \neq \operatorname{sgn}(a_n)$**:**



(-,+,-,-,+,-,+)

Regra de Descartes - Demonstração

Suponha que f tenha r raízes reais positivas. Então f' tem $r' \geq r - 1$ raízes positivas pelo Teorema de Rolle.



$f'(x) = a_1 + 2a_2x + \cdots + na_nx^{n-1}$ tem $v' \leq V(a_1, \ldots, a_n)$ mudanças de sinais.

$$r - 1 \leq r' \leq v' \leq v$$

Regra de Descartes - Além

A regra de Descartes nos diz mais do que superficialmente aparenta.

Regra de Descartes - Além

A regra de Descartes nos diz mais do que superficialmente aparenta.

- Se queremos saber as raízes negativas de $f(x) \in \mathbb{R}[x]$, então aplicamos a regra de Descartes para $f(-x)$.
  Exemplo: Quantas raízes negativas tem

$$x^4 + x^3 + x + 1 = 0?$$

Regra de Descartes - Além

A regra de Descartes nos diz mais do que superficialmente aparenta.

- Se queremos saber as raízes negativas de $f(x) \in \mathbb{R}[x]$, então aplicamos a regra de Descartes para $f(-x)$.
  Exemplo: Quantas raízes negativas tem
  $$x^4 + x^3 + x + 1 = 0?$$
- Se queremos saber a quantidade de raízes reais $> a$ para algum $a \in \mathbb{R}$, basta aplicar a regra de Descartes para $f(x+a)$.

Teorema de Budan - germes

Fixado um polinômio $f \in \mathbb{R}[x]$, vamos denotar por $V_f(h)$ a quantidade de variações dos coeficientes de $f(x+h)$.

Teorema de Budan - germes

Fixado um polinômio $f \in \mathbb{R}[x]$, vamos denotar por $V_f(h)$ a quantidade de variações dos coeficientes de $f(x+h)$.

Se $V_f(a) = 1$, sabemos que f possui exatamente uma raiz $> a$, e se $V_f(b) = 0$ para $b > a$, então garantimos que existe uma única solução em $(a, b]$.

Teorema de Budan

Teorema

Seja $f \in \mathbb{R}[x]$ um polinômio e $r_{(a,b]}$ a quantidade de raízes de f no intervalo $(a, b]$. Então

$$V_f(b) - V_f(a) - r_{(a,b]}$$

é um número par não-negativo.

Teorema de Budan

Teorema

Seja $f \in \mathbb{R}[x]$ um polinômio e $r_{(a,b]}$ a quantidade de raízes de f no intervalo $(a, b]$. Então

$$V_f(b) - V_f(a) - r_{(a,b]}$$

é um número par não-negativo.

- Esse teorema nos permite **isolar** as raízes reais de um polinômio!

Teorema de Sturm

Intuição: Se $f = (x-a_1)^{m_1}\cdots(x-a_n)^{m_n}Q$, onde Q não tem raiz real

$$\frac{f'}{f} = \frac{m_1}{x-a_1} + \frac{m_2}{x-a_2} + \cdots + \frac{m_n}{x-a_n} + \frac{Q'}{Q}.$$

Teorema de Sturm

Intuição: Se $f = (x - a_1)^{m_1} \cdots (x - a_n)^{m_n} Q$, onde Q não tem raiz real

$$\frac{f'}{f} = \frac{m_1}{x - a_1} + \frac{m_2}{x - a_2} + \cdots + \frac{m_n}{x - a_n} + \frac{Q'}{Q}.$$

- Esse quociente de certa forma armazena a informação a respeito das raízes de f.

Teorema de Sturm

Intuição: Se $f = (x - a_1)^{m_1} \cdots (x - a_n)^{m_n} Q$, onde Q não tem raiz real

$$\frac{f'}{f} = \frac{m_1}{x - a_1} + \frac{m_2}{x - a_2} + \cdots + \frac{m_n}{x - a_n} + \frac{Q'}{Q}.$$

- Esse quociente de certa forma armazena a informação a respeito das raízes de f.
- Queremos uma função linear que dê 1 em $1/(x - a)$ e 0 em Q'/Q se Q não tem raiz real.

Teorema de Sturm

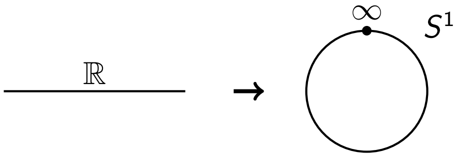
Dizemos que a é um polo de $\frac{P}{Q}$ se ele for um zero de Q, e chamamos o excesso em a por

$$E_a \frac{P}{Q} := \begin{cases} 1, & \text{se } \frac{P}{Q} \text{ muda de } -\infty \text{ para } +\infty \text{ em } a, \\ -1, & \text{se } \frac{P}{Q} \text{ muda de } +\infty \text{ para } -\infty \text{ em } a, \\ 0, & \text{caso contrário.} \end{cases}$$

Teorema de Sturm

Dizemos que a é um polo de $\frac{P}{Q}$ se ele for um zero de Q, e chamamos o excesso em a por

$$E_a \frac{P}{Q} := \begin{cases} 1, & \text{se } \frac{P}{Q} \text{ muda de } -\infty \text{ para } +\infty \text{ em } a, \\ -1, & \text{se } \frac{P}{Q} \text{ muda de } +\infty \text{ para } -\infty \text{ em } a, \\ 0, & \text{caso contrário.} \end{cases}$$



Teorema de Sturm

$$E_a^b \; \frac{P}{Q} = \text{soma dos } E_a \frac{P}{Q} \text{ em [a,b]}$$

Teorema de Sturm

Defina
$V_a^b(P_1, \ldots, P_n) = V(P_1(a), \ldots, P_n(a)) - V(P_1(b), \ldots, P_n(b))$.

Teorema

"Números de raízes de P entre a e b $= V_a^b(P, P', \ldots)$