



CRITÉRIO DE EISENSTEIN

1

Marília Martins Cabral
Orientador: Igor Lima

NOTAÇÕES

- $a \mid b \Leftrightarrow$ “a” divide “b”.
- $a \nmid b \Leftrightarrow$ a não divide “b”
- $x^n \Leftrightarrow$ a variável x elevado a potência n.
- $a_n \Leftrightarrow$ coeficiente de x^n

INTRODUÇÃO: POLINÔMIOS EM UMA VARIÁVEL

- Dadas as notações, define-se um polinômio de grau $n \geq 1$, com coeficientes inteiros, isto é:

$$P(x) = a_n \cdot x^n + a_{n-1} \cdot x^{n-1} + \cdots a_1 \cdot x + a_0$$

onde os $a_k \in \mathbb{Z}$.

DIVISIBILIDADE E DIVISÃO EUCLIDIANA

- Dados polinômios $d(x)$ e $a(x)$, dizemos que $d(x)$ divide $a(x)$ (e usamos a notação $d(x)|a(x)$) se existe um polinômio $c(x)$ tal que $a(x) = d(x)c(x)$.
- Esta relação de divisibilidade possui as mesmas propriedades que são válidas para os números inteiros. Em particular, se $d(x)|a(x)$ e $d(x)|b(x)$, então $d(x)|a(x)c_1(x) + b(x)c_2(x)$ para quaisquer $c_1(x)$ e $c_2(x)$.

MDC

- Com a relação de divisibilidade entre polinômios, podemos definir o mdc de dois polinômios.
- Dados $a(x)$ e $b(x)$, dizemos que $d(x)$ é um mdc de $a(x)$ e $b(x)$ se:
 - 1. $d(x)|a(x)$;
 - 2. $d(x)|b(x)$;
 - 3. $d(x)$ tem grau máximo entre todos os polinômios que cumprem as duas condições anteriores.

POLINÔMIOS IRREDUTÍVEIS

- Dizemos que o polinômio não constante $p(x)$ é irredutível em $R[x]$ (ou irredutível sobre R , onde $R = \mathbb{C}, \mathbb{R}, \mathbb{Q}$ ou $\mathbb{Z}$) se é impossível expressar $p(x)$ como um produto $a(x)b(x)$ de dois polinômios $a(x)$ e $b(x)$ em $R[x]$ cujos graus são ambos maiores ou iguais a 1.

OBSERVAÇÃO

- Não faz sentido dizer que um dado polinômio $p(x)$ é irredutível, simplesmente.
- Para nos convenceremos disso, basta olharmos um exemplo. Seja $p(x) = x^2 + 1$. É fácil ver que $p(x)$ é irredutível sobre $\mathbb{R}$. De fato, se fosse possível escrever $x^2 + 1 = (ax + b)(cx + d)$, com $(ax + b)$ e $(cx + d)$ de grau 1 e com coeficientes reais, então $x^2 + 1$ teria duas raízes reais, o que não é o caso.
- Por outro lado, sabemos que $x^2 + 1$ não é irredutível sobre $\mathbb{C}$, pois

$$x^2 + 1 = (x + i)(x - i).$$

OBSERVAÇÃO

- Polinômios irredutíveis são importantes porque eles representam, entre os polinômios, o mesmo papel que os números primos representam em $\mathbb{Z}$.

CRITÉRIOS DE IRREDUTIBILIDADE

- De acordo com o Teorema Fundamental da Álgebra os únicos polinômios irredutíveis em $\mathbb{C}[x]$ são os polinômios de grau 1. Segue desse fato que os polinômios irredutíveis em $\mathbb{R}[x]$ têm grau 1 ou 2 e um polinômio $ax^2 + bx + c \in \mathbb{R}[x]$ de grau 2 é irredutível se, e somente se, $\Delta = b^2 - 4ac < 0$.

LEMA (GAUSS)

- Se $p(x) \in \mathbb{Z}[x]$ é um polinômio irreduzível sobre $\mathbb{Z}$, então $p(x)$ também é um polinômio irreduzível sobre $\mathbb{Q}$.
- A demonstração pode ser encontrada no livro “Introdução à Álgebra”, de Adilson Gonçalves.

FERDNAND GOTTHOLD MAX EISENSTEIN

- Matemático e professor nascido e morto em Berlim, admirado por Gauss, apesar de sua vida breve, 30 anos, contribuiu em estudos com números primos, formas quadráticas e cúbicas, o teorema de reciprocidade de resíduos cúbicos e partição quadrática de números primos.



CRITÉRIO DE EISENSTEIN

- O Critério de Eisenstein é uma "regra" que permite classificar alguns polinômios com coeficientes inteiros como irredutíveis.

CRITÉRIO DE EISENSTEIN

- Teorema (Critério de Eisenstein): Seja $f(x) \in \mathbb{Z}[x]$, com

$$f(x) = a_n \cdot x^n + a_{n-1} \cdot x^{n-1} + \cdots a_1 \cdot x + a_0.$$

- Suponha que exista um primo p tal que:

- $p \nmid a_n$;
- $p \mid a_i, \forall i = \{0, 1, \dots, n-1\}$;
- $p^2 \nmid a_0$.

Então $f(x)$ não se escreve como produto de polinômios de grau $n \geq 1$ com coeficientes inteiros. Em particular, $f(x)$ é irredutível em $\mathbb{Q}$.

EXEMPLOS

- Exemplo (Gauss): Mostremos que $p(x) = x^4 - 2x^3 + 8x + 1$ é irredutível sobre $\mathbb{Q}$.
- Resposta:
- Pelo lema de Gauss, é suficiente ver que o polinômio é irredutível sobre $\mathbb{Z}$. Uma fatoração de $p(x)$ pode ser de dois tipos: um polinômio linear vezes um polinômio de grau 3, ou então o produto de dois polinômios quadráticos.

- Exemplo (Gauss continuação)
- Se existe um polinômio linear que divide $p(x)$, isso quer dizer que $p(x)$ tem uma raiz racional. As únicas possíveis raízes racionais de $p(x)$ são 1 e -1 , e podemos ver facilmente que nenhuma dela é raiz. Logo uma possível fatoração de $p(x)$ só pode ser um produto de dois polinômios quadráticos. Seja então:
 - $p(x) = (x^2 + ax + b)(x^2 + cx + d)$,
 - com a, b, c e d inteiros. Fazendo a distributiva e comparando coeficientes, temos:

- Exemplo(Gauss continuação)
- $bd = 1$
- $ad + bc = 8$
- $ac + b + d = -2$
- $a + c = 0$.
- De $bd = 1$ temos $b = d = 1$ ou $b = d = -1$. Se $b = d = 1$, ficamos com $ac = -4$ e portanto
- $a = -c = \pm 2$ e não podemos ter $ad + bc = 8$. Se $b = d = -1$, obtemos $ac = 0$, logo $a = c = 0$
- e novamente não temos $ad + bc = 8$. Portanto a fatoração como dois polinômios quadráticos também é impossível, e concluimos que o polinômio $p(x)$ é irredutível sobre $\mathbb{Q}$.

Proposição 1.9. *Seja p um número primo. Então o polinômio*

$$f(x) = x^{p-1} + x^{p-2} + \cdots + x + 1$$

é irreduzível em $\mathbb{Q}[x]$.

Demonstração. É um truque: faça a substituição $x = y + 1$. Observe que

$$f(x) \text{ é irreduzível em } \mathbb{Z}[x] \iff f(y) \text{ é irreduzível em } \mathbb{Z}[y]$$

(basta substituir $y = x - 1$ em qualquer fatoração de $f(y)$); e como $f(x) = (x^p - 1)/(x - 1)$, segue-se da fórmula do binômio de Newton que

$$f(y) = \frac{(y+1)^p - 1}{y} = y^{p-1} + \binom{p}{1}y^{p-2} + \binom{p}{2}y^{p-3} + \cdots + \binom{p}{p-2}y + \binom{p}{p-1}.$$

Agora uma grata surpresa: como p é um número primo, temos que p divide $\binom{p}{i}$ para cada $i = 1, \dots, p-1$ (este é um bom exercício!) e logo pelo critério de Eisenstein segue-se que $f(y)$ é irreduzível em $\mathbb{Z}[y]$, terminando a prova. $\square$

- Exemplo 2. De acordo com a preposição anterior, encontrar o polinômio irredutível no qual $\cos(2\pi/7)$ é raiz.
- $w = \zeta_7 =$ raiz primitiva 7-ésima da unidade
 logo
 como $f(x) = x^7 - 1 = (x-1)(x^6 + x^5 + \dots + x + 1)$
 e w é diferente de 1, segue de $f(w) = 0$ que
 $w^6 + w^5 + \dots + w + 1 = 0$.
 Tem-se que $w_- =$ conjugado de $w = w^6$.
 Seja $x = (w + w_-) = 2\cos(2\pi/7)$.

- Exemplo 2(continuação).
- Logo
- $x^2 = w^2 + 2w \cdot w_- + w_-^2 = w^2 + w^5 + 2$
 $x^3 = w^3 + 3w^2 \cdot w_- + 3w \cdot w_-^2 + w_-^3$
 $= w^3 + 3w + 3w^6 + w^4$
 $= w^3 + 3(w + w_-) + w^4$
 $= \text{substituindo os possíveis "x"}$
 $= w^3 + 3x + w^4$
 $(\text{como } w^4 = -(w^6 + w^5 + w^3 + w^2 + w + 1))$
 $= 3x - (w^6 + w) - w^5 - w^2 - 1$
 $= 2x - (w^5 - w^2) - 1$
 $= 2x - (x^2 - 2) - 1$
 $= -x^2 + 2x + 1$
 logo $x^3 + x^2 - 2x - 1$ é tal que $2\cos(2\pi/7)$ é raiz
 assim $(x/2)^3 + (x/2)^2 - 2(x/2) - 1$ é tal que $\cos(2\pi/7)$ é raiz.
 Multiplicando por 8 fica
 $p(x) = x^3 + 2x^2 - 8x - 8$
-
- Esse polinômio é irreduzível por Eisenstein pois $p(x+3)$ é irreduzível.

- Exemplo 3. Tome $f = x^4 + 5x^3 + 10x^2 + 15x + 20$. Pelo Teorema (aplicado com o primo $p = 5$), f não é produto de polinômios não constantes em $\mathbb{Z}[x]$. Mais uma vez, como f é primitivo, f é irreduzível em $\mathbb{Z}[x]$.
- Exemplo 4. Seja $f = 6x^9 + 14x^2 + 28x + 14$. Não podemos aplicar o critério para $p = 2$; mas para $p = 7$ concluímos que f é irreduzível em $\mathbb{Q}[x]$. Note que f é reduzível em $\mathbb{Z}[x]$ (2 é um fator).
- Exemplo 5. O polinômio $x^3 + 3x + 9$ é irreduzível em $\mathbb{Z}[x]$ (considere módulo 2) mas o critério de Eisenstein não se aplica aqui.