Desenvolvendo o Critério de Eisenstein computacionalmente

Bruno Cezar Steinmetz

19 de dezembro de 2016

1 Introdução

Este trabalho visa o desenvolvimento de um estudo sobre polinômios com coeficientes inteiros, mais especificamente, a irredutibilidade desses polinômios sobre o corpo dos racionais $\mathbb{Q}$. Para isso, buscou-se elaborar um algoritmo que, pelo critério de Eisenstein, defina a irredutibilidade de um dado polinômio com as características necessárias para tal performance – esse polinômio deve pertencer ao anel dos polinômios dos inteiros $\mathbb{Z}$. Para grande parte dos polinômios, é possível observar a irredutibilidade a partir do critério citado acima, o qual é um dos resultados primordiais da Álgebra no estudo de extensões de corpos, grupos e geometrias, principalmente. Tendo em vista essa importância, será apresentado um algoritmo na linguagem de programação Julia, que trata da verificação da irredutibilidade de polinômios com coeficientes inteiros sobre o corpo dos racionais pelo critério de Eisenstein. É importante destacar que nem todo polinômio pode ser observada a irredutibilidade a partir dos critérios acima, há outras ferramentas mais específicas para essa conclusão.

2 Polinômios

Para uma maior apreciação do estudo, é preciso habituar-se no contexto de estudo a ser explorado. Muitas vezes a pergunta "O que é um polinômio?"nos incomoda. Alguns dizem que é uma expressão algébrica, aquela que possui incógnitas multiplicadas por letras cujas parcelas somam-se. Ou ainda, um polinômio é uma função tal que, para cada valor variável, a expressão assume um determinado valor. Mas afinal, o que é?

Conforme [1], um polinômio nada mais é do que uma upla sequência de números $(a_0, a_1, \dots, a_n, \dots)$, em que $a_i \neq 0$ somente para um número finito de índices. Com isso, fica fácil estabelecer relações de operações entre polinômios.

Para somar e multiplicar dois polinômios podemos estabelecer a soma e multiplicação entre uplas. Observe:

- $(a_0, a_1, \dots, a_n, \dots) + (b_0, b_1, \dots, b_n, \dots) = (a_0 + b_0, a_1 + b_1, \dots, a_n + b_n, \dots)$.
- $(a_0, a_1, \dots, a_n, \dots) \cdot (b_0, b_1, \dots, b_n, \dots) = (c_0, c_1, \dots, c_n, \dots)$,
  onde $c_k = a_0b_k + a_1b_{k-1} + \cdots + a_{k-1}b_1 + a_kb_0$.

Essa escrita facilitará o processo de identificação de um polinômio na linguagem Julia de programação.

2.1 Teorema de Eisenstein para a irredutibilidade de polinômios

Ao situar-se no ambiente de polinômio como uma upla sequência de números, trabalharemos a irredutibilidade de um polinômio através do Critério de Eisenstein. Situamos um polinômio irredutível como aquele que não pode ser reduzido para um produto de fatores de grau menor, caso contrário dizemos que o polinômio é redutível.

A redutibilidade ou irredutibilidade de polinômios facilita na identificação das raízes que compõem um polinômio, sendo essencial no estudo de aneis, ideais, corpos e extensões, geometrias e afins.

Abaixo está contemplado o resultado de Eisenstein para a verificação da irredutibilidade de polinômios.

Teorema 2.1. *Critério de Eisenstein Seja* $f(x) = a_0 + a_1x + \cdots + a_nx^n \in \mathbb{Z}[x]$ *representado pela upla* $(a_0, a_1, \ldots, a_n)$*, em que cada* $a_i \in \mathbb{Z}$*. Se existir um primo* p *tal que:*

- $p \nmid a_n$*;*
- $p \mid a_i$*,* $i = 0, \ldots, n-1$*;*
- $p^2 \nmid a_0$*,*

então $f(x)$ *é irredutível sobre o corpo dos racionais* $\mathbb{Q}$*.*

Vale destacar que esse critério não soluciona todos os problemas de irredutibilidade de polinômios, mas sim grande parte deles.

3 Implementação computacional

Para obter sucesso na caracterização de polinômios, abaixo será apresentado um algoritmo que envolve o Critério de Eisenstein na busca por um número primo que satisfaz as condições do teorema de Eisenstein e, caso tal primo não exista, será necessário buscar outros métodos para a verificação.

Antes de estabelecer o algoritmo de Eisenstein, é preciso apresentar um algoritmo que calcula a primalidade de um número natural qualquer. Segue abaixo:

Algoritmo 1: Primalidade

Entrada: $n \in \mathbb{N}$
Saída: Primalidade de n

```
1 início
2 |  para i = 2 : (n − 1) faça
3 |  |  se n | i = 0 retorna Falso
4 |  fim
5 |  retorna Verdadeiro
6 fim
```

Para facilitar o desenvolvimento do algoritmo de Eisenstein, utilizou-se a notação de polinômio como uma upla sequência numérica dos coeficientes inteiros que caracterizam um polinômio. Também fora utilizado o Algoritmo 1 como auxílio. Segue abaixo.

Algoritmo 2: Critério de Eisenstein

Entrada: $v = [a_0 \quad a_1 \quad \dots \quad a_n]$ vetor dos coeficientes do polinômio
Saída: Irredutibilidade do polinômio associado à v

início
  n **tamanho** de v
  M **máximo** entre a_0 e a_{n-1}
  para $p = 2 : M$ **faça**
    se primo(p) = Falso
    continua
    se $a_n \mid p = 0$
    continua
    se $a_0 \mid p^2 = 0$
    continua
    se todo $v[a_0 : a_{n-1}] \mid p = 0$
    retorna *O polinômio é irredutível por Eisenstein para o primo p*
  fim
fim

3.1 Código do Algoritmo

Segue o código utilizando para desenvolver o algoritmo.

```
function primo(n)
    for i = 2 : (n − 1)
        if n%i == 0
            return false
        end
    end
    return true
end

function eisenstein(v) #v = [a_0  a_1  a_2  a_3  ...  a_n]
    n = length(v)
    M = maximum(v[1 : end − 1])
    for p = 2 : M
        if primo(p) == false
            continue
        end
            if v[end]%p == 0
                continue
            end
                if v[1]%p^2 == 0
                    continue
                end
                    if all(v[1 : end − 1]%p. == 0 )
```

```
                return ("O polinômio é irredutível por Eisenstein para o primo p = p")
            else
            end
    end
end
```

3.2 Exemplos

A partir do Algoritmo 2, abaixo serão apresentados alguns exemplos de polinômios irredutíveis testados.

Exemplo 3.1. *Considedere o polinômio* $f(x) = 2 + x^3$.

Esse polinômio pode ser representado pelo vetor $v = [2 \quad 0 \quad 0 \quad 1]$. *Nesse caso, pelo Algoritmo 1 e Algoritmo 2, calculamos o Critério de Eisenstein em* v.

O algoritmo do Critério de Eisenstein retorna: "O polinômio é irredutível para o primo 2".

De fato, pois

- $2 \nmid 1$;
- $2 \mid 2$ *e* $2 \mid 0$;
- $2^2 \nmid 2$.

Logo, notamos a eficácia do algoritmo na verificação da irredutibilidade de $f(x)$ *sobre o corpo dos racionais* $\mathbb{Q}$, *ou seja, o polinômio não possui nenhum raiz racional.*

Exemplo 3.2. *Considere o polinômio* $g(x) = 7 + 14x + 21x^2 + 63x^4 + 49x^5 + 11x^7$.

Esse polinômio pode ser representado pelo vetor $w = [7 \quad 14 \quad 21 \quad 0 \quad 63 \quad 49 \quad 0 \quad 11]$. *Nesse caso, pelo Algoritmo 1 e Algoritmo 2, calculamos o Critério de Eisenstein em* w.

O algoritmo do Critério de Eisenstein retorna: "O polinômio é irredutível para o primo 7".

De fato, pois

- $7 \nmid 11$;
- $7 \mid 7$, $7 \mid 14$, $7 \mid 21$, $7 \mid 0$, $7 \mid 63$ *e* $7 \mid 49$;
- $7^2 \nmid 7$.

Logo, notamos a eficácia do algoritmo na verificação da irredutibilidade de $g(x)$ *sobre o corpo dos racionais* $\mathbb{Q}$, *ou seja, o polinômio não possui nenhum raiz racional.*

Exemplo 3.3. *Considere o polinômio* $h(x) = -1 + x^2$.

Esse polinômio pode ser representado pelo vetor $y = [-1 \quad 0 \quad 1]$. *Nesse caso, pelo Algoritmo 1 e Algoritmo 2, calculamos o Critério de Eisenstein em* y.

O algoritmo do Critério de Eisenstein não retorna nada, pois não existe um primo p que satisfaça as condições do teorema de Eisenstein.

Sabe-se que esse polinômio é redutível sobre os racionais, pois suas raízes são $x = \pm 1$. *Daí,*

$$-1 + x^2 = (x - 1) \cdot (x + 1).$$

Vale ressaltar que o fato de o algoritmo não apresentar um número primo que satisfaça o critério de Eisenstein, signifique que o polinômio seja redutível sobre o corpo dos racionais. Observe o exemplo abaixo.

Exemplo 3.4. *Considere o polinômio* $s(x) = 8 + 2x - 3x^2 + 21x^3$.

Esse polinômio pode ser representado pelo vetor $z = [8 \quad 2 \quad -3 \quad 21]$. *Nesse caso, pelo Algoritmo 1 e Algoritmo 2, calculamos o Critério de Eisenstein em* z.

O algoritmo do Critério de Eisenstein não retorna nada, pois não existe um primo p *que satisfaça as condições do teorema de Eisenstein. Mas* $s(x)$ *é irredutível sobre o corpo dos racionais* $\mathbb{Q}$ *e, para averiguar essa afirmação, basta utilizar o polinômio* $\overline{s}(x)$ *em* $\mathbb{Z}_5[x]$, *o qual não possui raízes em* $\mathbb{Z}_5$ *e, portanto,* $s(x)$ *não possui raízes em* $\mathbb{Q}$, *sendo assim irredutível sobre o corpo dos racionais* $\mathbb{Q}$.

4 Conclusões

A elaboração desse projeto proporcionou grande aprendizado na interpretação, desenvolvimento e escrita de um algoritmo na linguagem Julia de programação.

Além disso, ficou clara a ligação entre conceitos da Álgebra e da programação. Inicialmente foi difícil conseguir adaptar uma linguagem para a outra, a escrita e a lógica foram grandes desafiadoras no desenvolvimento dos algoritmos, principalmente.

Os dois algoritmos apresentados no decorrer desse trabalho evidenciam uma solução rápida e simples para a verificação da irredutibilidade de polinômios no anel dos inteiros sobre o corpo dos racionais. O primeiro, além de dar suporte para o segundo, pode ser usado em separado para testar a primalidade de um número qualquer na entrada. O segundo, mais sofisticado, utiliza a primalidade para determinar um número primo que satisfaça as condições do Teorema de Eisenstein.

Portanto, é possível concluir que o estudo e desenvolvimento do projeto situou e formalizou conceitos essenciais da linguagem Julia de programação e da escrita de polinômios para testar sua irredutibilidade, o que implica grande aprendizado para a formação acadêmica no trabalho em sala de aula com o tema principal desse trabalho.

Referências

[1] A. Gonçalves, *Introdução à álgebra*. Rio de Janeiro: Instituto de Matemática Pura e Aplicada, 1979.

[2] A. Garcia e Y. Lequain, *Elementos de álgebra*. Instituto de Matemática Pura e Aplicada, 2003.