Demonstração Algoritmo de Euclides

Carlos Henrique

Setembro 2025

1 Introdução

O Algoritmo de Euclides é um método resolutivo de *mdc* criado pelo famoso matematico Euclides. O propósito do algoritmo é encontrar o máximo divisor comum entre dois números inteiros. Para isso, ele usufrui das propriedades da divisão e multiplicação para dividir um problema em mini problemas e a partir deles, se acha o mdc.

2 Propriedades

2.1 Coeficientes nulos

Uma das principais propriedades que é fundamental para que o algoritmo de Euclides funcione é a seguinte:

$$mdc(a, 0) = a \tag{1}$$

Essa propriedade nos diz que quando tentamos encontrar o máximo divisor comum entre um número inteiro e um número nulo (igual a 0), o máximo divisor comum sempre será o número inteiro. Isso ocorre devido a natureza do 0, todo número é multiplo de 0. Portanto, o máximo sempre será o limite estabelecido pelo número não nulo.

$$\begin{aligned} mdc(10, 0) &= 10 \\ mdc(25, 0) &= 25 \\ mdc(0, 35) &= 35 \end{aligned} \tag{2}$$

Essas propriedades é interessante quando trabalhamos com essa abordagem de resolução de problemas, pois ela facilita na hora de encontrar a solução para os problemas de grandezas de complexidade inferiores ao problema inicial. A demonstração dela é bem simples na verdade, se todo número é multiplo de 0, Portanto, essa afirmação se torna verdadeira:

$$0 * a = 0 \rightarrow \begin{vmatrix} 10 * 0 \\ 25 * 0 \\ 0 * 35 \end{vmatrix} = \begin{vmatrix} 0 \\ 0 \\ 0 \end{vmatrix} \tag{3}$$

Como você pode ver, todos os números são múltiplos de 0.

2.2 Divisibilidade entre coeficiente e resto

A segunda propriedade e a peça chave em segmentar o problema em problemas menos complexos, é essa. Quando trabalhos com divisão euclidiana, trabalhos dessa forma:

$$a = bq + r \tag{4}$$

Onde:

1. $a =$ dividendo
2. $b =$ divisor
3. $q =$ quociente
4. $r =$ resto

A partir dessa equação, podemos manipular ela pra encontrar diferentes outras equações pra cada monómio.

$$\begin{aligned} a &= bq + r \\ r &= a - bq \\ q &= \frac{a - r}{b} \end{aligned} \tag{5}$$

(TODO $\rightarrow$ equação do divisor)

Portanto, temos a seguinte propriedade:

$$mdc(a, b) = mdc(b, r) = mdc(r, r_2) = mdc(r_2, r_n) = mdc(r_n, 0) = r_n \tag{6}$$

E é possivel provar essa propriedade usando a propriedade dos multiplos. Dessa forma:

$$\begin{gathered} \exists mdc(a, b) \rightarrow mdc(a, b)|a, mdc(a, b)|b \\ mdc(a, b)|a, mdc(a, b)|b \rightarrow \begin{vmatrix} m * mdc(a, b) \\ n * mdc(a, b) \end{vmatrix} = \begin{vmatrix} a \\ b \end{vmatrix} \end{gathered} \tag{7}$$

O primeiro passo seria provar que $mdc(a, b)|r$ também. Daria pra escrever isso de outra forma.

$$mdc(a, b)|(a - bq) \tag{8}$$

No entanto, bq sempre irá gerar um multiplo de b. Portanto, pra facilitar a manipulação, presumimos que $q = 1$. Portanto, precisamos provar que na verdade $mdc(a, b)|(a - b)$. Chamamos de $r = a - b$.

$$\begin{aligned} a - b &= r \\ m * mdc(a, b) = a \quad n * mdc(a, b) &= b \\ m * mdc(a, b) - n * mdc(a - b) &= r \\ mdc(a, b) * (a - b) &= r \\ (a - b) * mdc(a, b) = r * mdc(a, b) &= r \end{aligned} \tag{9}$$

Portanto, podemos dizer que a diferença entre os coeficientes também é um multiplo de $mdc(a, b)$. Portanto, podemos dizer que $mdc(a, b)|r$. No entanto, agora falta demonstrar que b e r também é multiplo de a. Porque se isso for verdade, podemos dizer que:

$$\begin{aligned} &mdc(b, r)|b \\ &mdc(b, r)|r \\ &mdc(b, r)|a \end{aligned} \tag{10}$$

Portanto, se conseguirmos provar isso e chegar nesse conflito de inequação, pois se $mdc(a, b) >= mdc(b, r)$ e $mdc(b, r) >= mdc(a, b)$. Portanto, $mdc(a, b) = mdc(b, r)$. E para provar que $mdc(b, r)|a$, precisamos provar que a também é multiplo de $mdc(b, r)$. Portanto:

$$\begin{aligned} r &= a - b \\ r + b &= r \\ \\ b &= n * mdc(b, r) \\ r &= k * mdc(b, r) \\ \\ a = n * mdc(b, r) + k * mdc(b - r) \\ a &= mdc(b, r) * (n + k) \end{aligned} \tag{11}$$

Assim, fica demonstrado que a também é multiplo de $mdc(b, r)$. Dessa forma, podemos dizer que:

$$mdc(b, r) = mdc(a, b)$$

Porque $mdc(a, b)$ não pode ser maior que $mdc(b, r)$ enquanto $mdc(b, r)$ é maior que $mdc(a, b)$. Portanto, o que resta é eles serem iguais. A partir disso, isso aqui se torna verdade:

$$mdc(a, b) = mdc(b, r) = mdc(r, r_2) = mdc(r_2, r_n) = mdc(r_n, 0) = r_n \tag{12}$$