

Algoritmo MDC (Máximo Divisor Comum)

Duas formas:

- Algoritmo trivial
- Algoritmo de Euclides

MDC Trivial

- Obedecer a invariante com condições:
 - $1 \leq d \leq \min(m,n)$
 - $m \% t \neq 0$ ou $n \% t \neq 0$ para todo número inteiro $t \leq d$,
- As condições devem ser válidas todos os valores d
 - $d = [1, \min(m,n)]$

MDC Trivial (Código em C)

```
long mdc_trivial(long m, long n )  
    long d;  
    d = min(m,n);  
    while( m%d != 0 || n%d !=0 ){  
        d--;  
    }  
    return d;  
}
```

Desempenho MDC trivial

- Quantas repetições o algoritmo trivial faz?
 - $\text{MDC}(12, 18)$
 - $\text{MDC}(317811, 514229)$
- Podemos considerar eficiente ?

MDC – Algoritmo de Euclides

- Algoritmo de 2300 anos (cerca de 300 A.C.)
- O $\text{mdc}(m,n)$ para $0 \leq n < m$
 - $\text{mdc}(m,0) == m$;
 - $\text{mdc}(m,n) == \text{mdc}(n, m \% n)$, para $n > 0$.
- Exemplo:
 - $\text{mdc}(12,18) == \text{mdc}(18,12) == \text{mdc}(12,6) == \text{mdc}(6,0) == 6$

Correção MDC Euclides

- Seja m e n números inteiros positivos. Para cada inteiro positivo d tem-se que

$$(m \% d == 0) \text{ e } (n \% d == 0)$$

se e somente se

$$(n \% d == 0) \text{ e } ((m \% n) \% d == 0).$$

- Em outras palavras, o pares m, n e $n, m \% n$ têm o mesmo conjunto de divisores.

MDC Trivial (Código em C)

```
long mdc_euclides( long m, long n){  
    long r;  
    while( n != 0 ){  
        r = m % n;  
        m = n;  
        n = r;  
    }  
    return m;  
}
```

Desempenho MDC Euclides

- Quantas repetições o algoritmo de Euclides faz?
 - $\text{MDC}(12, 18)$
 - $\text{MDC}(317811, 514229)$
- Podemos considerar eficiente ?

Desempenho MDC Euclides

- Quantas repetições o algoritmo de Euclides faz?

`mdc (12, 18)`

`mdc (18, 12)`

`mdc (12, 6)`

`mdc (6, 0)`

- $\text{MDC}(12, 18) = 6$
- 4 repetições

Desempenho MDC Euclides

- Quantas repetições o algoritmo de Euclides faz?

```
_ mdc (317811, 514229)
  mdc (514229, 317811)
    mdc (317811, 196418)
      mdc (196418, 121393)
        mdc (121393, 75025)
          mdc (75025, 46368)
            mdc (46368, 28657)
              mdc (28657, 17711)
                mdc (17711, 10946)
                  mdc (10946, 6765)
                    mdc (6765, 4181)
                      mdc (4181, 2584)
                        mdc (2584, 1597)
                          mdc (1597, 987)
                            mdc (987, 610)
                              mdc (610, 377)
```

Desempenho MDC Euclides

- Quantas repetições o algoritmo de Euclides faz?

```
- mdc (377, 233)
  mdc (233, 144)
    mdc (144, 89)
      mdc (89, 55)
        mdc (55, 34)
          mdc (34, 21)
            mdc (21, 13)
              mdc (13, 8)
                mdc (8, 5)
                  mdc (5, 3)
                    mdc (3, 2)
                      mdc (2, 1)
                        mdc (1, 0)
```

- $\text{MDC}(317811, 514229) = 1$
- 29 repetições

Sumário

- MDC Euclides é notavelmente mais eficiente!
 - Realiza menos instruções computacionais (menos repetições)
- Por exemplo: $\text{MDC}(317811, 514229)$
 - Algoritmo trivial realiza 317811 repetições
 - Algoritmo Euclides realiza 29 repetições
- Referência online:
 - Página do Prof. José Coelho de Pina Jr. – IME – USP
 - <https://www.ime.usp.br/~coelho/algoritmos/aulas/material/aula24.pdf>