REVISTA DE CIÊNCIA ELEMENTAR

O algoritmo de Euclides

João Nuno Tavares

CMUP/ Universidade do Porto

jntavar@fc.up.pt

CITAÇÃO
Tavares, J. N. (2018)
O algoritmo de Euclides,
Rev. Ciência Elem., V6(03):056.
doi.org/10.24927/rce2018.056

EDITOR
José Ferreira Gomes,
Universidade do Porto

EDITOR CONVIDADO
João Lopes dos Santos,
Universidade do Porto

RECEBIDO EM
20 de setembro de 2018

ACEITE EM
22 de setembro de 2018

PUBLICADO EM
04 de outubro de 2018

rce.casadasciencias.org

Consideremos uma fração, por exemplo, $\frac{1876434}{983451}$. Será irredutível? Isto é, o numerador e o denominador admitem, como divisor comum, apenas o número 1?

Para responder a esta questão, podemos pensar em enumerar todos os divisores, quer do numerador, quer do denominador, e depois ver quais os que são comuns. No entanto, para números muito grandes, a enumeração dos seus divisores pode ser um problema complicado. De facto, não se conhece um algoritmo eficiente que o faça!

Surpreendentemente, é muito mais fácil calcular os divisores comuns a dois números dados a e b, e, portanto, calcular o maior deles, - o chamado Máximo Divisor Comum de a e b: MDC(a, b). Para simplificar a discussão vamo-nos restringir a números inteiros positivos a e b.

O método foi proposto por Euclides, e, por isso, chama-se o algoritmo de Euclides, e foi exposto, há mais de 2000 anos, na sua grande obra Os Elementos, Livro VII, proposição 2. Em que consiste? Sumariamente, Euclides propõe, nas suas próprias palavras, subtrair sucessivamente o menor número do maior. Mais formalmente, para calcular, por exemplo, MDC(15, 9) fazemos

$$\textbf{MDC}(15, 9) = \textbf{MDC}(9, 6) = \textbf{MDC}(6, 3) = \textbf{MDC}(3, 3) = 3$$

Algoritmo de Euclides: dados dois números inteiros positivos a e b, com $a > b$, para calcular MDC(a, b), substituímos o par (a, b) por $(b, a - b)$, e repetimos sucessivamente esta operação as vezes necessárias até obter um par de números iguais. Este número comum é a solução.

Este algoritmo pode ser implementado através de um dos códigos seguintes:

M é o máximo divisor comum

```
u := a; v := b;
while u ≠ v do
   begin
     if u > v then u := u - v
     else v := v - u
   end
M := u
```

Código da função MDC(a, b)

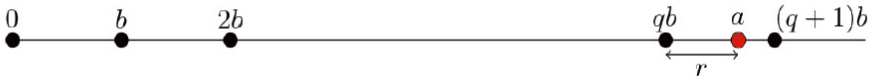
```
if a = b then M = a
   else
     begin
     if a > b then M := MDC(a - b; b)
     else M := MDC(a; b - a)
     end
```

Para provar que este algoritmo funciona, observamos os factos seguintes:

1. Se d é um divisor comum dos inteiros positivos a e b, com $a > b$, então d é também um divisor comum dos inteiros positivos b e a - b.
2. O algoritmo produz sucessivamente inteiros positivos cada vez mais pequenos, e, portanto, termina com um numero inteiro ≥ 1.

O algoritmo de Euclides, tal como ele o enunciou nos *Elementos*, pode não ser muito eficiente. Por exemplo, se tentarmos encontrar MDC$(101, 10^{100} + 1)$ por subtração repetida, teremos que subtrair 101 de $10^{100} + 1$ quase 1098 vezes, o que não é, evidentemente, muito rápido.

No entanto, subtrair repetidamente b de a, até que a diferença, $r = a$ - b, seja menor do que b, é o mesmo que dividir a por b e obter o resto r, como se ilustra na figura seguinte.



Isto dá origem ao seguinte *algoritmo de divisão Euclideana*: Dados dois números naturais a e b, com $a > b$ e $b \neq 0$, existem números naturais q e r, "quociente" e "resto", tais que:

$$a = qb + r \quad \text{onde} \quad 0 \leq r < b$$

A propriedade de divisão é visualmente óbvia, como se ilustra na figura acima, porque qualquer número natural a deve estar entre múltiplos sucessivos de b - na figura, entre qb e $(q + 1)b$. Em particular, a sua distância r, ao múltiplo menor, qb, e menor do que a distância b entre eles.

A vantagem do algoritmo de divisão euclideana, é que, em geral, é muito mais rápido do que a subtração repetida. Cada divisão de um número natural b por um número $a < b$, com k algarismos, "cancela" cerca de k algarismos em b, e conduz a um resto r com no máximo k algarismos. Portanto, o número de divisões e no máximo igual ao número total de dígitos dos números com que começámos. Resumindo

$$\text{MDC}(a, b) = \text{MDC}(b, r), \quad \text{onde} \quad a = qb + r$$

Por exemplo

$$\text{MDC}(1345, 24) = \text{MDC}(24, 1) = 1$$

já que $1345 = 24 \times 56 + 1$. Em geral, podemos calcular M = MDC(a, b) através do código seguinte:

```
u := a; v := b;
while v > 0 do
    begin
      r := u mod v;
      u := v;
      v := r;
    end
M := u
```