Algoritmo de Euclides Estendido, Relação de Bézout e Equações Diofantinas

O Algortimo de Euclides Estendido

Tópicos Adicionais

Tópicos Adicionais
O Algoritmo de Euclides Estendido

1 Exercícios Introdutórios

Exercício 1. Aplique o Algoritmo de Euclides para encontrar $mdc(2322, 654)$.

Exercício 2. Calcule $mdc(42823, 6409)$.

Exercício 3. O Algoritmo de Euclides pode ser sintetizado de forma prática em uma tabela, como ilustrado abaixo.

	7	1	1	4
272	36	20	16	4
20	16	4	4	0

Os valores da tabela correspondem as seguintes divisões sucessivas:

$$\begin{aligned} 272 &= (36 \cdot 7) + 20 \\ 36 &= (20 \cdot 1) + 16 \\ 20 &= (16 \cdot 1) + 4 \\ 16 &= (4 \cdot 4) + 0 \end{aligned}$$

Repita o procedimento representado na tabela anterior para calcular $mdc(695, 135)$.

2 Exercícios de Fixação

Exercício 4. Calcule:

a) $mdc(n, n^2 + n + 1)$.

b) $mdc(3 \times 2012, 2 \times 2012 + 1)$.

c) $mdc\left(\frac{2^{40}+1}{2^8+1}, 2^8 + 1\right)$.

Exercício 5. No planeta X, existem apenas dois tipos de notas de dinheiro: \$5 e \$78. É possível pagarmos exatamente \$7 por alguma mercadoria? E se as notas fossem de \$ 3 e \$ 78?

Exercício 6. Encontre inteiros a e b tais que

$$1235a + 415b = mdc(1235, 415)$$

Exercício 7. Encontre inteiros a e b tais que

$$42823a + 6409b = 17$$

3 Exercícios de Aprofundamento e de Exames

Exercício 8. Seja S um conjunto infinito de inteiros não negativos com a seguinte propriedade: dados dois quaisquer de seus elementos, o valor absoluto da diferença entre eles também pertence a S. Se d é o menor elemento positivo de S, prove que S consiste de todos os múltiplos de d.

Exercício 9. Três máquinas I, R, S imprimem pares de inteiros positivos em tickets. Para a entrada (x, y), as máquinas I, R, S imprimem respectivamente $(x - y, y), (x + y, y), (y, x)$. Iniciando com o par $(1, 2)$ podemos alcançar

a) (819, 357)?

b) (19, 79)?

Exercício 10. Prove que $\frac{21n+4}{14n+3}$ é irredutível para todo número natural n.

Exercício 11. Se x e y são inteiros tais que $2xy$ divide $x^2 + y^2 - x$, prove que x é um quadrado perfeito

Exercício 12. A sequência $a_1, a_2, \ldots$ de naturais satisfaz $mdc(a_i, a_j) = mdc(i, j)$ para todo $i \neq j$ Prove que $a_i = i$ para todo i.

Exercício 13. Mostre que $mdc(2^{120} - 1, 2^{100} - 1) = 2^{20} - 1$.

Exercício 14. Encontre $mdc(2n + 13, n + 7)$

Exercício 15. Prove que a fração $\frac{12n+1}{30n+2}$ é irredutível.

Exercício 16. Prove que, para todo natural n,

$$mdc(n! + 1, (n + 1)! + 1) = 1.$$

Exercício 17. Sejam a, b, c, d inteiros não nulos tais que $ad - bc = 1$. Prove que $\frac{a+b}{c+d}$ é uma fração irredutível.

Respostas e Soluções.

1.

$$\begin{aligned} 2322 &= 654 \cdot 3 + 360 \\ 654 &= 360 \cdot 1 + 294 \\ 360 &= 294 \cdot 1 + 66 \\ 294 &= 66 \cdot 4 + 30 \\ 66 &= 30 \cdot 2 + 6 \\ 30 &= 6 \cdot 5 \end{aligned}$$

Portanto, $mdc(2322, 654) = 6$.

2. Pelo Algoritmo de Euclides,

$$\begin{aligned} 42823 &= 6 \times 6409 + 4369 \\ 6409 &= 1 \times 4369 + 2040 \\ 4369 &= 2 \times 2040 + 289 \\ 2040 &= 7 \times 289 + 17 \\ 289 &= 17 \times 17. \end{aligned}$$

Portanto, $mdc(42823, 6409) = 17$.

3. As divisões sucessivas do Algoritmo de Euclides produzem a seguinte tabela:

	5	6	1	3
695	135	20	15	5
20	15	5	4	0

Portanto, $mdc(695, 135) = 5$.

4.

(a) Pelo Lema de Euclides, temos

$$\begin{aligned} mdc(n, n^2+n+1) &= mdc(n, n^2+n+1-n(n+1)), \\ &= mdc(n, 1), \\ &= 1. \end{aligned}$$

Outra maneira, seria aplicar o Algoritmo de Euclides:

	$n+1$	n
n^2+n+1	n	1
1	0	

(b)

$$\begin{aligned} mdc(3 \times 2012, 2 \times 2012 + 1) &= \\ mdc(3 \times 2012 - (2 \times 2012 + 1), 2 \times 2012 + 1) &= \\ mdc(2012 - 1, 2 \times 2012 + 1) &= \\ mdc(2012 - 1, 2 \times 2012 + 1 - 2(2012 - 1)) &= \\ mdc(2012 - 1, 3) &= \\ mdc(2012 - 1 - 3 \times 670, 3) &= \\ mdc(2, 3) &= 1. \end{aligned}$$

Outra opção seria observar que o mdc procurado deve dividir o número $3(2 \times 2012 + 1) - 2(3 \times 2012) = 3$ e que $2 \times 2012 + 1$ não é múltiplo de 3.

(c) Como $x^5 + y^5 = (x+y)(x^4 - x^3y + x^2y^2 - xy^3 + y^4)$, escolhendo $x = 2^8$ e $y = 1$, o problema se resume a encontrar

$$mdc\left(2^{32} - 2^{24} + 2^{16} - 2^8 + 1, 2^8 + 1\right)$$

Além disso, sabendo que $x - 1 \mid x^8 - 1$ e que

$$\begin{aligned} 2^{32} - 2^{24} + 2^{16} - 2^8 + 1 &= \\ (2^{32} - 1) - (2^{24} - 1) + (2^{16} - 1) - (2^8 + 1) + 1, & \end{aligned}$$

uma aplicação do Lema de Euclides nos permite concluir que o mdc anterior é igual a

$$mdc(1, 2^8 + 1) = 1.$$

5. Veja que $2 \times 78 - 31 \times 5 = 1$ e consequentemente $14 \times 78 - 217 \times 5 = 7$. Basta darmos 14 notas de de \$ 78 para recebermos 217 notas de \$ 5 como troco na compra de nossa mercadoria. Usando as notas de \$3 e \$78 não é possível, pois o dinheiro pago e recebido como troco por algo sempre é múltiplo de 3 e 7 não é múltiplo de 3.

6. Aplicando o Algortimo de Euclides, obtemos as seguintes equações:

$$\begin{aligned} 1235 &= (415 \cdot 2) + 405 \\ 415 &= (405 \cdot 1) + 10 \\ 405 &= (10 \cdot 40) + 5 \\ 10 &= (5 \cdot 2) + 0 \end{aligned}$$

As equações anteriores mostram que cada resto é uma combinação linear dos dividendos e divisores correspondentes. Por um processo de trocas sucessivas, podemos escrever o último resto como uma combinação linear do dividendo e do divisor da primeira equação:

$$\begin{aligned} 5 &= 405 - 10 \cdot 40 \\ &= 405 - (415 - 405 \cdot 1) \cdot 40 \\ &= 405 \cdot 41 - 415 \cdot 40 \\ &= (1235 - 415 \cdot 2) \cdot 41 - 415 \cdot 40 \\ &= 1235 \cdot 41 - 415 \cdot 122. \end{aligned}$$

7. Nesta solução, apresentaremos um procedimento diferente do exercício anterior. Essencialmente, a equação $mdc(x + qy, y) = mdc(x, y)$ nos diz que podemos subtrair q vezes um número de outro sem alterar o máximo divisor comum do par em questão. Realizando esse procedimento sucessivas vezes, subtraindo o número menor do maior, podemos obter pares com números cada vez menores até que chegarmos em um par do tipo (d, d). Como o máximo divisor comum foi preservado ao longo dessas operações, d será o máximo divisor comum procurado. Iremos repetir o exemplo anterior registrando em cada operação quantas

vezes um número é subtraido do outro. Isso será feito através de dois pares de números auxiliares:

$$\begin{array}{rcl} (42823, 6409) & | & (1,0)(0,1) \\ (4369, 6409) & | & (1,-6)(0,1) \\ (4369, 2040) & | & (1,-6)(-1,7) \\ (289, 2040) & | & (3,-20)(-1,7) \\ (289, 17) & | & (3,-20)(-22,147) \\ (17, 17) & | & (355,-2372)(-22,147) \end{array}$$

Da primeira linha para a segunda, como subtraímos 6 vezes o número 6409 de 42823, subtraímos 6 vezes o par $(0,1)$ de $(1,0)$, obtendo: $(1,0) - 6(0,1) = (1,-6)$. Se em uma dada linha, temos:

$$(x, x+qy) \mid (a,b)(c,d);$$

então, a próxima linha deverá ser:

$$(x,y) \mid (a,b)(c-aq, d-bq);$$

porque representará a operação de subtrairmos q vezes o primeiro número do segundo. Veja que o par (a,b) foi subtraido de (c,d) exatamente q vezes. Os números escritos nos últimos dois pares representam os coeficientes dos números originais para cada número do primeiro par. Por exemplo, analisando a linha:

$$(289, 2040) \mid (3,-20)(-1,7);$$

obtemos que:

$$\begin{array}{rcl} 289 & = & 3 \times 42823 - 20 \times 6409, \\ 2040 & = & -1 \times 42823 + 7 \times 6409. \end{array}$$

Em cada linha, essa propriedade é mantida pois a mesma subtração que é realizada no primeiro par também é realizada entre os dois últimos pares. Analisando o último par, podemos escrever 17 como combinação de 42823 e 6409 de duas formas diferentes:

$$\begin{array}{rcl} 17 & = & -22 \times 42823 + 147 \times 6409, \\ 17 & = & 355 \times 42823 + -2372 \times 6409, \end{array}$$

Assim, podemos obter duas soluções $(a,b) = (-22, 147)$ e $(355, -2372)$. Sugerimos o leitor mostrar que existem infinitas soluções (a,b).

8. Considere um elemento m qualquer de S. Pelo algoritmo da divisão, $m = qd + r$ com $0 \leq r < d$. Como todos os números $m-d, m-2d, m-3d, \ldots, m-qd = r$ pertencem a S e d é o menor elemento positivo de tal conjunto, devemos ter obrigatoriamente que $r = 0$. Sendo assim, podemos concluir que todos os elementos de S são múltiplos de d. Resta mostrarmos que todos os múltiplos de d estão em S. Seja kd um múltiplo positivo qualquer de d. Como S é infinito, existe um inteiro $m \in S$ tal que $m = qd > kd$. Assim todos os números $m-d, m-2d, \ldots, m-(q-k)d = kd$ estão em S.

9. Para o item a), calculemos inicialmente $mdc(819, 357)$ usando o Lema de Euclides:

$$\begin{array}{rcl} mdc(819,357) & = & mdc(105,357) \\ & = & mdc(105,42) \\ & = & mdc(21,42) \\ & = & 21. \end{array}$$

Pelo Lema de Euclides, o mdc entre os dois números em um ticket nunca muda. Como $mdc(1,2) = 1 \neq 21 = mdc(819,357)$, não podemos alcançar o par do item a).

Para o item b), indiquemos com $\rightarrow$ uma operação de alguma das máquinas. Veja que: $(2,1) \xrightarrow{R} (3,1) \xrightarrow{S} (1,3) \xrightarrow{R} (4,3) \xrightarrow{R} \ldots \xrightarrow{R} (19,3) \xrightarrow{S} (3,19) \xrightarrow{R} (22,19) \xrightarrow{R} (41,19) \xrightarrow{R} (60,19) \xrightarrow{R} (79,19)$.

10. (Extraído da Olimpíada Internacional de Matemática) Pelo lema de Euclides,

$$\begin{array}{rcl} mdc(21n+4, 14n+3) & = & mdc(7n+4, 14n+3) \\ & = & mdc(7n+1, 7n+2) \\ & = & mdc(7n+1, 1) = 1. \end{array}$$

11. Se $d = mdc(x,y)$, então $x = da$ e $y = db$, com $mdc(a,b) = 1$. Do enunciado, temos:

$$\begin{array}{rl} 2abd^2 \mid d^2a^2 + d^2b^2 - da & \Rightarrow \\ d^2 \mid d^2a^2 + d^2b^2 - da & \Rightarrow \\ d^2 \mid -da & \Rightarrow \\ d \mid a. & \end{array}$$

Logo, $a = dc$, para algum c. Como $x \mid y^2$, obtemos $d^2c \mid d^2b^2$, ou seja, $c|b^2$ e $mdc(c, b^2) = c$. Usando que $mdc(a,b) = 1$ e que todo divisor comum de b e c também é um divisor comum de a e b, podemos concluir que $mdc(c,b) = 1$. Daí, $mdc(c, b^2) = 1$ e $c = 1$. Portanto, $x = d^2c = d^2$.

12. Para qualquer inteiro n, $mdc(a_{2n}, a_n) = mdc(2n, n) = n$, consequentemente $n \mid a_n$. Seja d um divisor qualquer de a_n diferente de n, então $d \mid mdc(a_d, a_n)$. De $mdc(a_d, a_n) = mdc(d,n)$, podemos concluir que $d \mid n$. Sendo assim, todos os divisores de a_n que são diferentes de n são divisores de n. Como já sabemos que $a_n = nk$, para algum k, não podemos ter $k > 1$, pois nk não divide n e assim concluímos que $a_n = n$.

13. Pelo lema de Euclides,

$$\begin{aligned} mdc(2^{120}-1, 2^{100}-1) &= \\ mdc(2^{120}-1-2^{20}(2^{100}-1), 2^{100}-1) &= \\ mdc(2^{20}-1, 2^{100}-1) &= \\ mdc(2^{20}-1, 2^{100}-1-2^{80}(2^{20}-1)) &= \\ mdc(2^{20}-1, 2^{80}-1) &= \\ mdc(2^{20}-1, 2^{80}-1-2^{60}(2^{20}-1)) &= \\ mdc(2^{20}-1, 2^{60}-1) &= \\ mdc(2^{20}-1, 2^{60}-1-2^{40}(2^{20}-1)) &= \\ mdc(2^{20}-1, 2^{40}-1) &= \\ mdc(2^{20}-1, 2^{40}-1-2^{20}(2^{20}-1)) &= \\ mdc(2^{20}-1, 2^{20}-1) = 2^{20}-1. & \end{aligned}$$

14.

$$\begin{aligned} mdc(2n+13, n+7) &= mdc(2n+13-2(n+7), n+7), \\ &= mdc(2n+13-2(n+7), n+7), \\ &= mdc(-1, n+7) = 1 \end{aligned}$$

15.

$$\begin{aligned} mdc(12n+1, 30n+2) &= \\ mdc(12n+1, 30n+2-2(12n+1)) &= \\ mdc(12n+1, 6n) &= \\ mdc(12n+1-2(6n), 6n) &= \\ mdc(1, 6n) = 1. & \end{aligned}$$

16. Pelo lema de Euclides,

$$\begin{aligned} mdc(n!+1, (n+1)!+1) &= \\ mdc(n!+1, (n+1)!+1-(n+1)(n!+1)) &= \\ mdc(n!+1, -n) &= \\ mdc(n!+1-n[(n-1)!], -n) &= \\ mdc(1, -n) &= 1 \end{aligned}$$

17. Seja $f = mdc(a+b, c+d)$. Então $f \mid d(a+b) - b(c+d) = 1$ e consequentemente $f = 1$.

Produzido por Arquimedes Curso de Ensino
contato@cursoarquimedes.com