Ciclo 4 – Encontro 1

ALGORITMO DO MDC DE EUCLIDES, RELAÇÃO DE BÉZOUT E APLICAÇÕES, EQUAÇÕES DIOFANTINAS LINEARES

Nível 3
PO: Márcio Reis
11º Programa de Iniciação Científica Jr.

Algoritmo do mdc de Euclides, Relação de Bézout e aplicações, equações diofantinas lineares

- Apostila 1: INICIAÇÃO À ARITMÉTICA, de Abramo Hefez.

  Seções 3.8 a 3.10:

  Algoritmo do mdc de Euclides;

  Aplicações da Relação de Bézout;

  Equações diofantinas lineares.

- Apostila: ENCONTROS DE ARITMÉTICA, de F. Dutenhefner, L. Cadar.

  Seções 4.1 e 4.2:

  Cálculo do mdc - Algoritmo de Euclides – partes 1 e 2.

O Lema de Euclides

O Lema de Euclides: *Dados inteiros a e b, os divisores comuns de a e b são os mesmos que os divisores comuns de a e $b - c \times a$, para todo número inteiro c fixado.*

Demonstração. Se d é um divisor comum de a e b, é claro que d é divisor comum de a e de $b - c \times a$.

Reciprocamente, suponha que d seja divisor comum de a e de $b - c \times a$. Logo, d é divisor comum de $b - c \times a$ e de $c \times a$ e, portanto, pelo Problema 3.13(c), tem-se que d é divisor de b. Assim, d é divisor comum de a e b. □

O Lema de Euclides

O Lema de Euclides nos diz que os divisores de comuns de a e b são os mesmos divisores comuns de a e $b - a \times c$, logo tomando o maior divisor comum em ambos os casos, obtemos a fórmula:

$$\text{mdc}(a, b) = \text{mdc}(a, b - a \times c),$$

Algoritmo de Euclides para o cálculo do mdc

Nada melhor do que um exemplo para entender o método.

Vamos calcular $\mathrm{mdc}(a, b)$, onde $a = 162$ e $b = 372$.

Pelo Lema de Euclides, sabemos que o mdc de a e b é o mesmo que o de a e de b menos um múltiplo qualquer de a. Otimizamos os cálculos ao tomarmos o menor dos números da forma b menos um múltiplo de a e isto é realizado pelo algoritmo da divisão:

$$372 = 162 \times 2 + 48.$$

Assim, $\mathrm{mdc}(372, 162) = \mathrm{mdc}(372 - 162 \times 2, 162) = \mathrm{mdc}(48, 162)$.

Algoritmo de Euclides para o cálculo do mdc

$$162 = 48 \times 3 + 18.$$

$$\begin{aligned} \mathrm{mdc}(372, 162) &= \mathrm{mdc}(162, 48) \\ &= \mathrm{mdc}(162 - 48 \times 3, 48) \\ &= \mathrm{mdc}(18, 48). \end{aligned}$$

$$48 = 18 \times 2 + 12.$$

$$\mathrm{mdc}(372, 162) = \mathrm{mdc}(48, 18) = \mathrm{mdc}(48 - 18 \times 2, 18) = \mathrm{mdc}(12, 18).$$

$$18 = 12 \times 1 + 6.$$

$$\mathrm{mdc}(372, 162) = \mathrm{mdc}(18, 12) = \mathrm{mdc}(18 - 12 \times 1, 12) = \mathrm{mdc}(6, 12).$$

Algoritmo de Euclides para o cálculo do mdc

$$\text{mdc}(372, 162) = \text{mdc}(12, 6) = \text{mdc}(12 - 6 \times 2, 6) = \text{mdc}(0, 6) = 6.$$

$$\boxed{\text{mdc}(372, 162) = 6.}$$

Algoritmo de Euclides para o cálculo do mdc

Exemplo 1: Calcule mdc(18, 60).

Algoritmo de Euclides para o cálculo do mdc

Exemplo 1: Calcule mdc(18, 60).

Solução:

mdc(18, 60) = mdc(18, 60 − 18) = mdc(18, 42) = mdc(18, 42) = mdc(18, 42 − 18) = mdc(18, 24) = mdc(18, 24) = mdc(18, 24 − 18) = mdc(18, 6) = 6.

Algoritmo de Euclides para o cálculo do mdc

	C	C'	C''			
A	B	R	R'	...		= mdc
R	R'	R''			0	

$$A = B \times C + R$$
$$B = R \times C' + R'$$
$$R = R' \times C'' + R''$$
$$\dots$$
$$R_{n-1} = R_n \times C_n + 0$$

$$R_n = mdc$$

Algoritmo de Euclides para o cálculo do mdc

372	162

372 = 162 x 2 + 48

	2	
372	162	48
48		

162 = 48 x 3 + 18

	2	3	
372	162	48	18
48	18		

48 = 18 x 2 + 12

	2	3	2	
372	162	48	18	12
48	18	12		

18 = 12 x 1 + 6

	2	3	2	1	2
372	162	48	18	12	6=mdc
48	18	12	6	0	

12 = 6 x 2 + 0

Algoritmo de Euclides para o cálculo do mdc

O Algoritmo de Euclides usado de trás para frente nos dá uma informação adicional fundamental.

Das igualdades acima podemos escrever:

$$\textcircled{6} = 18 - 12 \times 1$$

$$12 = 48 - 18 \times 2$$

$$18 = 162 - 48 \times 3$$

$$48 = 372 - 162 \times 2$$

Algoritmo de Euclides para o cálculo do mdc

Donde,

$$\begin{aligned} \textcircled{6} = 18 - 12 \times 1 &= 18 - (48 - 18 \times 2) \\ &= 18 \times 3 - 48 \\ &= (162 - 48 \times 3) \times 3 - 48 \\ &= 162 \times 3 - 48 \times 10 \\ &= 162 - (372 - 162 \times 2) \times 10 \\ &= 162 \times 23 - 372 \times 10. \end{aligned}$$

Assim, podemos escrever:

$$\textcircled{6} = \text{mdc}(372, 162) = 162 \times 23 + 372 \times (-10).$$

Relação de Bézout

Este método sempre se aplica conduzindo ao seguinte importante resultado:

Teorema 3.3 (Relação de Bézout)**.** *Dados inteiros a e b, quaisquer, mas não ambos nulos, existem dois inteiros n e m tais que*

$$\mathrm{mdc}(a, b) = a \times n + b \times m.$$

Relação de Bézout

Exemplo 2: Calcule mdc(18, 60) e os inteiros *n* e *m* tais que mdc(a, b) = a×n+b×m.

Relação de Bézout

Exemplo 2: Calcule mdc(18, 60) e os inteiros *n* e *m* tais que mdc(a, b) = a×n+b×m.

	3	3
60	18	6
6	0	

$6 = 60 - 18 \times 3$

mdc(a,b) = a×n+b×m
6 = 60(1)+18(-3)

ATENÇÃO!

Ler o capítulo **3.9 Aplicações da Relação de Bézout** da Apostila 1: INICIAÇÃO À ARITMÉTICA, de Abramo Hefez. Ficar atento às ***proposições***!

Equações diofantinas lineares

A resolução de muitos problemas de aritmética depende da resolução de equações do tipo $ax + by = c$, onde a, b e c são números inteiros dados e x e y são incógnitas a serem determinadas em $\mathbb{Z}$. Um exemplo típico de um problema modelado por este tipo de equação é o seguinte:

Problema 3.54. De quantos modos podemos comprar selos de cinco e de três reais, de modo a gastar cinquenta reais?

Equações diofantinas lineares

Dada uma equação, as perguntas naturais que se colocam são as seguintes:

1) Quais são as condições para que a equação possua solução?

2) Quantas são as soluções?

3) Como calcular as soluções, caso existam?

Daremos a seguir respostas a essas perguntas no caso das equações em questão.

A primeira pergunta admite a resposta a seguir.

Equações diofantinas lineares

Demonstração. Suponha que a equação admita uma solução x_0, y_0. Então vale a igualdade $ax_0 + by_0 = c$. Como $\text{mdc}(a, b)$ divide a e divide b, segue que ele divide $ax_0 + by_0$, logo divide c.

Reciprocamente, suponha que $\text{mdc}(a, b)$ divida c, ou seja $c = \text{mdc}(a, b) \times d$, para algum inteiro d. Por outro lado, sabemos que existem inteiros n e m tais que

$$\text{mdc}(a, b) = a \times n + b \times m.$$

Multiplicando ambos os lados da igualdade acima por d, obtemos

$$c = \text{mdc}(a, b) \times d = a \times (n \times d) + b \times (m \times d).$$

Equações diofantinas lineares

Logo, a equação diofantina $ax + by = c$ admite pelo menos a solução

$$x = n \times d \quad \text{e} \quad y = m \times d.$$

Equações diofantinas lineares

Teorema 3.5. *Seja x_0 e y_0 uma solução particular, arbitrariamente dada, da equação $ax + by = c$, onde $\mathrm{mdc}(a, b) = 1$. Então as soluções da equação são da forma $x = x_0 + tb$ e $y = y_0 - ta$, para t variando em $\mathbb{Z}$.*

Equações diofantinas lineares

Por exemplo, a equação $3x + 5y = 50$ admite a solução particular $x_0 = 0$ e $y_0 = 10$. Assim, a solução geral dessa equação é dada por $x = 0 + 5t$ e $y = 10 - 3t$. Se estivermos à procura de soluções não negativas então deveríamos ter $10 - 3t \geq 0$, o que implica que $t = 0, 1, 2$ ou 3. Assim, o Problema 3.54 admite as seguintes soluções:

(a) 10 selos de 5 reais.

(b) 5 selos de 3 reais e 7 selos de 5 reais.

(c) 10 selos de 3 reais e 4 selos de 5 reais.

(d) 15 selos de 3 reais e um selo de 5 reais.

Equações diofantinas lineares

O único verdadeiro trabalho que se tem para resolver uma equação diofantina linear $ax + by = c$ é calcular $\text{mdc}(a, b)$ para verificar se divide ou não c e descobrir uma solução particular x_0, y_0. O primeiro problema se resolve utilizando o algoritmo de Euclides para o cálculo do mdc. Quanto ao segundo, o de determinar uma solução particular da equação, procede-se por inspeção se a e b são números pequenos. Caso a ou b seja grande, podemos usar o algoritmo de Euclides de trás para a frente para determinar inteiros n e m tais que

$$an + bm = \text{mdc}(a, b) = 1,$$

Equações diofantinas lineares

e depois multiplicar ambos os membros da equação acima por c, obtendo

$$a(nc) + b(mc) = c,$$

dando-nos a solução particular $x_0 = nc$ e $y_0 = mc$.

Exercício 1

Calcule $\text{mdc}(n+1, n^2+1)$, para n inteiro.

Exercício 1 - Solução

Solução: $\text{mdc}(n+1, n^2+1) = \text{mdc}\big(n+1, n^2+1-n\cdot(n+1)\big) = \text{mdc}(n+1, -n+1) = \text{mdc}\big(n+1, -n+1+1\cdot(n+1)\big) = \text{mdc}(n+1, 2)$. Assim, se n é par, então $n+1$ é ímpar e, logo, $\text{mdc}(n+1, n^2+1) = \text{mdc}(n+1, 2) = 1$; e se n é ímpar, então $n+1$ é par e, logo, $\text{mdc}(n+1, n^2+1) = \text{mdc}(n+1, 2) = 2$.

Exercício 2

Use o algoritmo do mdc de Euclides para calcular $\text{mdc}(648, -1218)$ e encontre inteiros x e y tais que $\text{mdc}(648, -1218) = 648x + (-1218)y$.

Exercício 2 - Solução

Solução: Tem-se $\text{mdc}(648, -1218) = \text{mdc}(648, 1218)$. Aplicando o algoritmo do mdc de Euclides, tem-se $1218 = 1 \cdot 648 + 570$, $648 = 1 \cdot 570 + 78$, $570 = 7 \cdot 78 + 24$, $78 = 3 \cdot 24 + 6$ e $24 = 4 \cdot 6 + 0$. Logo, $\text{mdc}(648, -1218) = 6$. Realizando o processo de trás para frente, tem-se $6 = 78 - 3 \cdot 24 = 78 - 3 \cdot (570 - 7 \cdot 78) = -3 \cdot 570 + 22 \cdot 78 = -3 \cdot 570 + 22 \cdot (648 - 570) = 22 \cdot 648 - 25 \cdot 570 = 22 \cdot 648 - 25 \cdot (1218 - 648) = 648 \cdot 47 + (-1218) \cdot 25$. Logo, $x = 47$ e $y = 25$.

Exercício 2 - Solução

	1	1	7	3	4
1218	648	570	78	24	6 = mdc
570	78	24	6	0	

Exercício 3a

a) Encontre todos os inteiros múltiplos de 3 que divididos por 15 deixam resto igual a 8.

Exercício 3a - Solução

Seja n um inteiro múltiplo de 3 que dividido por 15 deixa resto 8. Então, existem inteiros x e y tais que $n = 3x = 15y + 8$. Como $3x = 15y + 8$, obtém-se a equação diofantina $3x - 15y = 8$, que não tem solução porque $\text{mdc}(3, -15) = 3$ não divide 8. Assim, não existem inteiros múltiplos de 3 que divididos por 15 deixam resto igual a 8.

Exercício 3b

b) Encontre todos os inteiros pares que divididos por 15 deixam resto igual a 8.

Exercício 3b - Solução

Seja n um inteiro par que dividido por 15 deixa resto 8. Então, existem inteiros x e y tais que $n = 2x = 15y + 8$. Como $2x = 15y + 8$, obtém-se a equação diofantina $2x - 15y = 8$, que tem solução porque $\text{mdc}(2, -15) = 1$ divide 8. Como $2 \cdot (-7) - 15 \cdot (-1) = 1$, então $2 \cdot (-7 \cdot 8) - 15 \cdot (-1 \cdot 8) = 8$ e, portanto, $x_0 = -7 \cdot 8 = -56$ e $y_0 = -1 \cdot 8 = -8$ é uma solução particular da equação diofantina $2x - 15y = 8$. Assim, a solução geral da equação diofantina é dada por $x = -56 - 15t$ e $y = -8 - 2t$, com t variando no conjunto dos inteiros. Assim, $n = 2x = 2 \cdot (-56 - 15t) = -112 - 30t$, com t variando no conjunto dos inteiros.

Exercício 4

Problema 3.43. Determine $\text{mdc}(a, b)$, $\text{mmc}(a, b)$ e inteiros n e m tais que $\text{mdc}(a, b) = a \times n + b \times m$ para os seguintes pares de números a e b.

(a) $a = 728$ e $b = 1\,496$

(b) $a = 108$ e $b = 294$.

Exercício 4 - Solução

	2	18	5
1496	728	40	8
40	8	0	

8 = 728(37) + 1496(-1)

	2	1	2	1	1	2
294	108	78	30	18	12	6
78	30	18	12	6	0	

6 = 108(-15) + 294(7)

Estudar para o próximo encontro!

Próximo encontro: 08/10, sábado, às 08h30

Assistir às vídeo aulas:
Módulo: "**Métodos de Contagem e Probabilidade**":
http://matematica.obmep.org.br/index.php/modulo/ver?modulo=69
Vídeoaulas: "Aula 17 – Probabilidade condicional", "Aula 18 – Probabilidade condicional", "Aula 19 – Indepêndencia"

Módulo: **"Probabilidade Condicional"**:
http://matematica.obmep.org.br/index.php/modulo/ver?modulo=47
Vídeoaulas: "Probabilidade condicional", "Probabilidade condicional e Multiplicação de Probabilidades – Parte 1", "Probabilidade condicional e Multiplicação de Probabilidades – Parte 2"