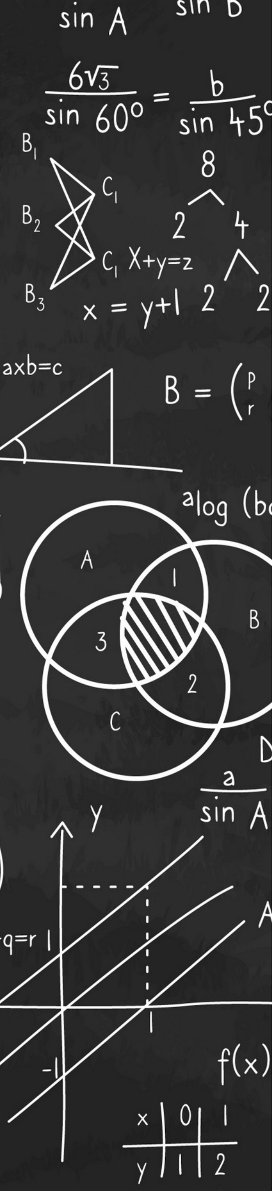

Matemática Discreta 2

Aula 06
MDC e MMC

Cristiane Loesch
cristiane.costa@unb.br

Brasília
2024

DIVISIBILIDADE

$$a = qb + r$$

EXERCÍCIO:

1) Na intenção de trocar minhas moedas do cofrinho, levei-as a uma loja. Como tinha várias moedas de 10 e 25 centavos, a atendente me sugeriu comprar um objeto. Mostre que o preço de qualquer objeto que eu comprar deverá ser divisível por 5 centavos, considerando que não houve troco.

2) Considere que você trabalha em uma loja de chocolates e deve montar caixas de bombom. Sabendo que cada caixa deve conter 8 bombons e que você tem 153 para distribuir entre as caixa, responda:

a) Quantas caixas completas poderá embalar?

b) Quantos bombons vão sobrar, que não couberam nas caixas?

c) Represente as operações anteriores utilizando o algoritmo da divisão, DIV e MOD

PRINCIPIO DA BOA ORDEM

Todo subconjunto, não vazio, de N contém um elemento mínimo

Consequência $\rightarrow$ Proposição:

Não existe $m \in Z$ tal que $a < m < b$, $a,b \in Z$

MÁXIMO DIVISOR COMUM

<u>DEFINIÇÃO</u>

Dados a, b $\in$ Z, não mutuamente nulos, o máximo divisor comum de a e b é o maior d $\in$ Z, qual que d|a e d|b.

→ Notação : mdc(a,b) = d   ou   (a,b)=d

MÁXIMO DIVISOR COMUM

Diz que é possível escrever o MDC de dois números com uma combinação linear destes números

TEOREMA DE BÈZOUT

Dados a,b,d $\in$ Z, se d=mdc(a,b) então existe m, n $\in$ Z tais que

$$d = ma + nb$$

PESQUISAR DEMONSTRAÇÃO

MÁXIMO DIVISOR COMUM

TEOREMA DE BÈZOUT

Dados a,b,d $\in$ Z, se d=mdc(a,b) então existe m, n $\in$ Z tais que

$$d = ma + nb$$

Obs: Observe que o problema nos mostra que d=c. Como c é o menor número positivo pertencente a B, logo ficou provado que d é o menor dentre os positivos de B, que pode ser escrito como combinação linear de a e b.

MÁXIMO DIVISOR COMUM

TEOREMA (1)

Seja $d=mdc(a,b)$ e $c>0$ tal que $c|a$ e $c|b$ então $c|d$

MÁXIMO DIVISOR COMUM

Proposição 1

Sejam $a,b,t \in Z$, $t>0$, $mdc(ta, tb) = t\, mdc(a,b)$

MÁXIMO DIVISOR COMUM

Proposição 1

Sejam $a,b,t \in Z$, $t>0$, $mdc(ta, tb) = t\ mdc(a,b)$

DEMONSTRAR – em sala

Proposição 2

Se $c>0$, $c|a$ e $c|b \Rightarrow mdc(a/c, b/c)=1/c\ mdc(a,b)$

DEMONSTRAR - estudo

MÁXIMO DIVISOR COMUM

Corolário

Se $d=mdc(ta, tb) \Rightarrow mdc(a/d, b/d)=1$

DEMONSTRAR - estudo

MÁXIMO DIVISOR COMUM

Corolário

Se $d=mdc(ta, tb) \Rightarrow mdc(a/d, b/d)=1$

DEMONSTRAR - estudo

Exemplo:

a) $mdc(14, 35) = 7$

b) $mdc(18,33)=3$

MÁXIMO DIVISOR COMUM

TEOREMA (2)

Se a,b, x $\in$ Z => mdc(a,b)= mdc(a, b+ax)

DEMONSTRAÇÃO - estudar

Hipotese: d=mdc(a,b) ; h=mdc(a, b+ax)
Tese: d|h e h|d

(T Bezout)

d=ma+nb $\rightarrow$ d=ma+nb+0 $\rightarrow$ d=ma+nb+axn-axn

$\rightarrow$ d=(m-xn)a+n(b+ax) $\rightarrow$ d=k a+n(b+ax)

Como h=mdc(a, b+ax) $\rightarrow$ h|a ^ h|(b+ax) logo h|k a+n(b+ax) => h|d

Como d= mdc(a,b) $\rightarrow$ d|a ^ d|b pela ppdde da divisao d|b+ax
Logo d é divisor comum de a e b+ax => d|h

MÁXIMO DIVISOR COMUM

DEFINIÇÃO

Dizemos que dois números inteiros a e b são **relativamente primos** quando mdc(a,b) =1

MÁXIMO DIVISOR COMUM

TEOREMA DE EUCLIDES

Se a, b, c $\in$ Z tal que a|bc e mdc(a,b)=1 então a|c

DEMONSTRAR - estudo

MÁXIMO DIVISOR COMUM

Proposição 3

Sejam a, b, $c \in Z$ tal que $a|c$, $b|c$ e $mdc(a,b)=1$ então $ab|c$

DEMONSTRAR - estudo

MÁXIMO DIVISOR COMUM

<u>Como calcular o MDC?</u>

MÁXIMO DIVISOR COMUM

ALGORITMO DE EUCLIDES

Dados dois números inteiros a e b, vamos denotar o conjunto de todos os divisores comuns de a e b como:

$$D(a,b) = \{ x \in Z / \ x|a \text{ e } x|b \}$$

Assim, mdc(a,b) = max D(a,b).

MÁXIMO DIVISOR COMUM

ALGORITMO DE EUCLIDES

Dados dois números inteiros a e b, vamos denotar o conjunto de todos os divisores comuns de a e b como:

$$D(a,b) = \{ x \in Z / \ x|a \text{ e } x|b\}$$

Assim, $mdc(a,b) = \max D(a,b)$.

LEMA:

Sejam a, b, q, $r \in Z$, $b \neq 0$, tais que

$$a=bq+r$$

com $0 \leq r < |b|$. $D(a,b) = D(b,r)$, logo $mdc(a,b)=mdc(b,r)$

MÁXIMO DIVISOR COMUM

TEOREMA 4

Sejam a, b $\in$ Z, ambos não nulos, e seja d =mdc(a,b), existem x e y inteiros tais que ax + by = d, ou seja, ax + by = mdc(a,b)

MÁXIMO DIVISOR COMUM

TEOREMA 4

Sejam $a, b \in Z$, ambos não nulos, e seja

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

existem x e y inteiros tais que

$$ax + by = d,$$

ou seja,

$$ax + by = mdc(a,b)$$

MÁXIMO DIVISOR COMUM

<u>TEOREMA 4</u>

Sejam a, b $\in$ Z, ambos não nulos, e seja

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

existem x e y inteiros tais que

$$ax + by = d,$$

ou seja,

$$ax + by = mdc(a,b)$$

Exercício: Encontre x e y dado MDC(431, 29)=1

MÁXIMO DIVISOR COMUM

TEOREMA 4

Sejam a, b $\in$ Z, ambos não nulos, e seja

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

existem x e y inteiros tais que

$$ax + by = d,$$

ou seja,

$$ax + by = mdc(a,b)$$

Exercício: Encontre x e y dado MDC(431, 29)=1

SUA VEZ! Encontre x e y dados:

a) MDC(351, 28)=1

b) MDC(1128, 336)=1

MÁXIMO DIVISOR COMUM

Observação

Em relação ao teorema 4, não podemos afirmar que a volta será verdadeira, uma vez que para a, b inteiros e não simultaneamente nulos, podemos escolher aleatoriamente dois inteiros x e y, garantimos apenas que, eventualmente, tal combinação será igual ao mdc(a,b)

MÁXIMO DIVISOR COMUM

Observação

Em relação ao teorema 4, não podemos afirmar que a volta será verdadeira, uma vez que para a, b inteiros e não simultaneamente nulos, podemos escolher aleatoriamente dois inteiros x e y, garantimos apenas que, eventualmente, tal combinação será igual ao mdc(a,b)

EXCETO QUANDO:

Sejam a,b inteiros, suponha que existam x, y inteiros tais que

$$ax+by = 1.$$

Mostre que MDC(a,b) =1

MÍNIMO MÚLTIPLO COMUM

Definição

Sejam a, b inteiros, não nulos. Diz-se que m é o mínimo múltiplo comum entre a e b, se:

$a|m \wedge b|m$

$m \in N$

m é o menor número possível

NOTAÇÃO: mmc(a,b)

MÍNIMO MÚLTIPLO COMUM

Obs: nomenclatura

M(a) = conjunto dos múltiplos de a

$$M(a)=\{k \in Z / \ a|k\} = \{\ldots, -2a, -a, 0, a, 2a, 3a, ...\}$$

$M_+(a)$= conjunto dos múltiplos de a positivos

$$M_+(a)=\{k \in Z / \ a|k, a \neq 0\} = \{a, 2a, 3a, ...\}$$

MÍNIMO MÚLTIPLO COMUM

Obs: nomenclatura

M(a) = conjunto dos múltiplos de a

$$M(a)=\{k \in Z / \ a|k\} = \{\dots, -2a, -a, 0, a, 2a, 3a, \dots\}$$

$M_+(a)$= conjunto dos múltiplos de a positivos

$$M_+(a)=\{k \in Z / \ a|k, a \neq 0\} = \{a, 2a, 3a, \dots\}$$

EXEMPLO: mmc(12,18)

$M_+(12)$

$M_+(18)$

MÍNIMO MÚLTIPLO COMUM

Obs: nomenclatura

M(a) = conjunto dos múltiplos de a

$$M(a)=\{k \in Z / \ a|k\} = \{\dots, -2a, -a, 0, a, 2a, 3a, ...\}$$

$M_+(a)$= conjunto dos múltiplos de a positivos

$$M_+(a)=\{k \in Z / \ a|k, a\neq 0\} = \{a, 2a, 3a, ...\}$$

EXEMPLO: mmc(12,18)

$M_+(12) = \{12, 24, 36, 48, 60, ...\}$

$M_+(18)= \{18, 36, 54, ...\}$

MÍNIMO MÚLTIPLO COMUM

Definição 2:

Define-se como o mínimo múltiplo comum de dois inteiros a e b:

$$mmc(a,b) = \min M_+(a,b)$$

em que min $M_+(a,b)$ é o conjunto de todos os inteiros positivos em $M(a,b)$, sendo:

$$M(a,b)=\{c \in Z / \ a|c \ \wedge b|c\}$$

conjunto de todos os múltiplos comuns de a e b.

MÍNIMO MÚLTIPLO COMUM

LEMA:

Sejam a, b $\in Z^*$, então

$$mmc(a,b)|c \qquad \forall c \in M(a,b)$$

Sejam ma, m2 $\in$ M(a,b) tal que

$a|m1, a|m2 \quad => a|(m1+m2)$

$b|m1, b|m2 \quad => b|(m1+m2)$

Logo,

m1+m2 é um múltiplo comum de a e b $\rightarrow$ m1+m2 $\in$ M(a,b)

Dado n $\in$ Z

$a|m1 => a \mid n\, m1$

$b|m1 => b \mid n\, m1$

Logo, $n.m1 \in M(a,b)$

Tais características garantem que o mmc de a e b sempre existe.

MÍNIMO MÚLTIPLO COMUM

LEMA:

Sejam a, b $\in Z^*$, então

$$mmc(a,b)|c \qquad \forall c \in M(a,b)$$

Sejam ma, m2 $\in$ M(a,b) tal que

$a|m1, a|m2 \Rightarrow a|(m1+m2)$

$b|m1, b|m2 \Rightarrow b|(m1+m2)$

Logo,

m1+m2 é um múltiplo comum de a e b $\rightarrow$ m1+m2 $\in$ M(a,b)

Dado n $\in$ Z

$a|m1 \Rightarrow a \mid n\, m1$

$b|m1 \Rightarrow b \mid n\, m1$

Logo, $n.m1 \in M(a,b)$

Tais características garantem que o mmc de a e b sempre existe.

Mas, mmc pode ser menor do que zero?

Pelo lema a resposta é não!

Pois se c< 0, tem-se

$-c = c\,(-1) \in M(a,b)$

MÍNIMO MÚLTIPLO COMUM

TEOREMA:

Sejam a, b naturais,

$$mmc(a,b) \cdot mdc(a,b) = a.b$$

DEMONSTRAR - estudo

MÍNIMO MÚLTIPLO COMUM

TEOREMA:

Sejam a, b naturais,

$$mmc(a,b) \, . \, mdc(a,b) = a.b$$

Obs:

Se a, b inteiros $\rightarrow$ $mmc(a,b) \, . \, mdc(a,b) = |a.b|$

MÍNIMO MÚLTIPLO COMUM

TEOREMA:

Sejam a, b naturais,

$$mmc(a,b) \cdot mdc(a,b) = a.b$$

EXEMPLO:

Determine o mmc(1128, 336) sabendo que mdc(1128, 336) =24

EXTRA

Obs:

mdc(a,b,c) =

mdc(a_1, a_2, a_3, …, a_n)

mmc(a,b,c) =

mmc(a_1, a_2, a_3, …, a_n)

EXTRA

Obs:

$\text{mdc}(a,b,c) = \text{mdc}((a,b), c)$ *recursividade

$\text{mdc}(a_1, a_2, a_3, \ldots, a_n)$

$\text{mmc}(a,b,c) =$

$\text{mmc}(a_1, a_2, a_3, \ldots, a_n)$

EXTRA

<u>Obs:</u>

$mdc(a,b,c) = mdc((a,b), c)$ *recursividade

Por indução:

$mdc(a_1, a_2, a_3, \dots, a_n) = mdc((a_1, a_2, a_3, \dots, a_{n-1}), a_n)$

$mmc(a,b,c) =$

$mmc(a_1, a_2, a_3, \dots, a_n)$

EXTRA

Obs:

$mdc(a,b,c) = mdc((a,b), c)$ *recursividade

Por indução:

$mdc(a_1, a_2, a_3, \ldots, a_n) = mdc((a_1, a_2, a_3, \ldots, a_{n-1}), a_n)$

Analogamente,

$mmc(a,b,c) = mmc((a,b),c)$

$mmc(a_1, a_2, a_3, \ldots, a_n) = mmc((a_1, a_2, a_3, \ldots, a_{n-1})\ a_n)$

EXERCÍCIOS

1) mostre que dois inteiros consecutivos são primos entre si

2) calcule o mmc (n, n+1), para n $\in$ N

3) determinar inteiros positivos a e b, tais que: a.b = 9900 e mmc(a,b)=330