Aula 5. Máximo divisor comum

5.1 Divisores comuns

Definição

Sejam a, b dois inteiros. Dizemos que um inteiro c é *divisor comum* de a e b, se $c \mid a$ e $c \mid b$.

Por exemplo 2 é divisor comum de 6 e 10, pois $2 \mid 6$ e $2 \mid 10$. Por outro lado 3 não é divisor comum de 6 e 10. Neste caso temos que $3 \mid 6$ mas $3 \nmid 10$.

Na teoria o máximo divisor comum entre dois inteiros a e b desempenha o papel fundamental.

Definição

Sejam a e b dois inteiros. Um inteiro não-negativo d é chamado *máximo divisor comum* de a e b se:

i) $d \mid a$ e $d \mid b$.

ii) se c é divisor comum de a e b, assim $c \mid d$.

Na definição acima temos que a condição i) diz que o inteiro d é divisor comum entre a e b. E a condição ii) pode ser interpretada como a condição de *maximalidade*.

No exemplo acima temos que o máximo divisor comum entre 6 e 10 é 2. Além disso através a definição é claro que o maximo divisor comum entre 0 e 0 é 0, pois

i) $0 \mid 0$ e $0 \mid 0$.

ii) qualquer inteiro c é divisor de zero, e $c \mid 0$.

5.2 Unicidade e Teorema de Bézout

Perguntas naturais:

- O máximo divisor comum de a e b existe?
- Se existir o máximo divisor comum de a e b assim ele é único?

Primeiramente vamos responder a segunda pergunta.

Lemma 5.1

Sejam a, b dois inteiros não nulos. Se d, d' dois máximos divisores comuns de a e b assim, $d = d'$.

Prova

Como d, d' são divisores comuns de a, b assim temos que

$$d \mid d', \quad d' \mid d.$$

Agora pelo proposição da Aula passada segue que $d = \pm d'$. Mas ambos d e d' são positivos, assim $d = d'$.

Observação 5.1

Pelo lema anterior, temos que se existir o máximo divisor comum, assim ele é único. Denotaremos esse numero por $\text{mdc}(a, b)$.

Agora pelo o seguinte teorema a gente mostre que o mdc de dois numeros sumpre existe.

Theorem 5.1: (Teorema de Bézout)

Sejam a, b dois inteiros. Assim existem dois inteiros r, s, tais que

$$\text{mdc}(a, b) = a \cdot r + b \cdot s.$$

Prova

Considere o seguinte conjunto

$$S = \{ax + by \mid x, y \in \mathbb{Z}, \quad ax + by \geq 0\}.$$

O conjunto S não é vazio, pois se $x = a$ e $y = b$ assim

$$a \cdot a + b \cdot b = a^2 + b^2 \geq 0.$$

Além disso S é formado pelos inteiros não-negativos. Assim pelo (PBO) (veja Aula 1) existe elemento minimal em $d = \min S$. Como $d \in S$ assim

$$d = a \cdot r + b \cdot s,$$

para alguns inteiros r, s. Vamos mostrar que $d = \text{mdc}(a, b)$. Precisamos verificar que

(i) $d \mid a$ e $d \mid b$.

(ii) se c é divisor comum de a e b, assim $c \mid d$.

Pelo algoritmo da divisão de a por d, temos que

$$a = d \cdot q + r_1,$$

com $0 \leq r_1 < d$. Se $d \nmid a$, assim $r_1 > 0$. Agora

$$r_1 = a - d \cdot q = a - (a \cdot r + b \cdot s) \cdot q = a \cdot (1 - r \cdot q) + b(-s).$$

Ou seja $r_1 \in S$, pois tem forma $r_1 = a \cdot x + b \cdot y$, com $x = (1 - r \cdot q)$ e $y = (-s)$. Mas $r_1 < d = \min S$, é contradição! Assim $d \mid a$. Analogamente $d \mid b$. Assim d cumpre condição (i).

Agora seja $c \mid a$ e $c \mid b$, assim (veja Aula 4) temos que $c \mid an + bm$ para todos n e m inteiros. Em particular $c \mid ar + bs = d$. Assim d cumpre condição (ii). Ou seja $d = \text{mdc}(a, b)$.

O teorema de Bézout foi provado pelo um matemático francês Étienne Bézout, e garante a existência de $\text{mdc}(a, b)$ para dois inteiros dados a e b. Mas na pratica calcular o $\text{mdc}(a, b)$ através o Teorema de Bézout não é fácil, pois não é claro como encontrar os inteiros r e s do Teorema (vamos explicar isso nas aulas futuras).

Étienne Bézout (1730 – 1783)

5.3 *Divisores e o máximo divisor comum*

Nessa seção vamos explicar uma ideia ingênuo como encontrar o máximo divisor comum.

Definição

Sejam a um inteiro. Defina

$$\text{Div}(a) = \{c \in \mathbb{Z} \mid c \text{ divide } a\},$$

como conjunto de todos divisores de inteiro a.

Por exemplo

$$\mathrm{Div}(6) = \{-6, -3, -2, -1, 1, 2, 3, 6\}.$$

Observem que o único caso quando $\mathrm{Div}(a)$ não é conjunto limitado é quando $a = 0$. Neste caso $\mathrm{Div}(0) = \mathbb{Z}$, pois qualquer inteiro divide 0. E se $a \neq 0$, assim $\mathrm{Div}(a)$ é limitado, pois se $c \mid a$, assim $|c| \leq |a|$, logo

$$\mathrm{Div}(a) \subseteq \{-|a|, -|a|+1, \ldots, 0, \ldots, |a|-1, |a|\}.$$

Dados dois inteiros a e b definamos $\mathrm{Div}(a, b)$ como sendo o seguinte conjunto

$$\mathrm{Div}(a, b) = \mathrm{Div}(a) \cap \mathrm{Div}(b) = \{c \in \mathbb{Z} \mid c \text{ divide } a, \text{ e } c \text{ divide } a\}.$$

Assim $\mathrm{Div}(a, b)$ é conjunto de todos divisores comuns de a e b. Por exemplo, se $a = 6$ e $b = 10$, temos

$$\mathrm{Div}(6) = \{-6, -3, -2, -1, 1, 2, 3, 6\},$$
$$\mathrm{Div}(10) = \{-10, -5, -2, -1, 1, 2, 5, 10\}.$$

e assim

$$\mathrm{Div}(6, 10) = \{-2, -1, 1, 2\}.$$

É logico esperar que o máximo divisor comum mdc entre dois inteiros dados a e b é o elemento maximal do conjunto $\mathrm{Div}(a, b)$. E isso é exatamente a afirmação da seguinte proposição.

Proposição 5.1

Sejam a e b dois inteiros não ambos nulos. Assim

$$\mathrm{mdc}(a, b) = \max \mathrm{Div}(a, b).$$

Prova

Observem que $\mathrm{Div}(a, b)$ é conjunto não-vazio, pois $1 \in \mathrm{Div}(a)$ e $1 \in \mathrm{Div}(b)$, assim $1 \in \mathrm{Div}(a, b)$. Sejam

$$d = \mathrm{mdc}(a, b), \quad d' = \max \mathrm{Div}(a, b).$$

Ambos d e d' são não-negativos, vamos provar que eles são iguais.

Como $d = \mathrm{mdc}(a, b)$, assim $d \mid a$ e $d \mid b$, logo $d \in \mathrm{Div}(a, b)$, logo $d \leq d' = \max \mathrm{Div}(a, b)$.

Por outro lado, $d' \mid a$ e $d' \mid b$ logo (pelo condição (ii) do mdc) temos que $d' \mid d$, assim $d' \leq d$.

Como $d \leq d'$ e $d' \leq d$, assim $d = d'$.

Exemplo 5.1

Vamos calcular $\text{mdc}(6,10)$. Temos,

$$\text{Div}(6) = \{\pm 1, \pm 2, \pm 3, \pm 6\},$$
$$\text{Div}(10) = \{\pm 1, \pm 2, \pm 5, \pm 10\}.$$

Logo

$$\text{Div}(6,10) = \text{Div}(6) \cap \text{Div}(10) = \{\pm 1, \pm 2\}.$$

e

$$\text{mdc}(6,10) = \max \text{Div}(6,10) = 2.$$

Exemplo 5.2

Vamos calcular $\text{mdc}(30,36)$. Temos,

$$\text{Div}(30) = \{\pm 1, \pm 2, \pm 3, \pm 5, \pm 6, \pm 10, \pm 15, \pm 30\},$$
$$\text{Div}(36) = \{\pm 1, \pm 2, \pm 3, \pm 4, \pm 6, \pm 9, \pm 12, \pm 18, \pm 36\}.$$

Logo

$$\text{Div}(30,36) = \text{Div}(30) \cap \text{Div}(36) = \{\pm 1, \pm 2, \pm 3, \pm 6\}.$$

e

$$\text{mdc}(30,36) = \max \text{Div}(30,36) = 6.$$

5.4 *Propriedades do* mdc

Nessa seção vamos descobrir vários propriedades do mdc. Começaremos com o seguinte exercícios cujo solução deixamos como a carga para o leitor.

Exercício 5.1: Trabalho p/ casa

Sejam a, b e c números inteiros. Verificar se as afirmações abaixo são verdadeiras ou falsas, dando a demonstração ou um contra-exemplo:

(1) $\text{mdc}(a,b) = \text{mdc}(b,a)$.

(2) $\text{mdc}(\text{mdc}(a,b),c) = \text{mdc}(a,\text{mdc}(b,c))$.

(3) $\text{mdc}(a,1) = 1$.

(4) $\text{mdc}(a,b+c) = \text{mdc}(a,b) + \text{mdc}(a,c)$.

(5) $\text{mdc}(a,bc) = \text{mdc}(a,b) \cdot \text{mdc}(a,c)$.

(6) $\text{mdc}(a,a) = |a|$.

(7) $\text{mdc}(a,bc) = b\,\text{mdc}(a,c)$.

(8) $\text{mdc}(ab,cd) = \text{mdc}(a,c)\cdot\text{mdc}(b,d)$.

(9) $b \mid a \Leftrightarrow \text{mdc}(a,b) = |b|$.

(10) $\text{mdc}(-a,b) = mdc(a,-b) = \text{mdc}(a,b)$.

Resposta: (1),(3), (6), (9), (10) são verdadeiras, os restos são falsas.

Proposição 5.2

Sejam a, b inteiros, $d = \text{mdc}(a,b)$ e c um inteiro não-nulo. Então:

(i) $\text{mdc}(ac,bc) = d|c|$.

(ii) Se $c \mid a$ e $c \mid b$ assim

$$\text{mdc}(a/c, b/c) = d/|c|.$$

Prova

Para (i), mostraremos que $d|c|$ verifica as condições (i) e (ii) da definição do mdc em relação aos inteiros ab e bc
De fato, como $d = \text{mdc}(a,b)$, temos em particular que $d \mid a$, logo $(d|c|) \mid (ac)$. Da mesma forma, $(d|c|) \mid (bc)$, Ainda, do Teorema de Bézout, temos que existem $r, s \in \mathbb{Z}$ tais que $d = ra + sb$. Logo,

$$d|c| = r(a|c|) + s(b|c|)$$

Agora se d' é um inteiro tal que $d' \mid ac$ e $d' \mid bc$, da relação acima vem imediatamente que $d' \mid (d|c|)$.

Para provar (ii), poderíamos usar um raciocínio análogo, mas daremos uma demonstração mais breve, usando o resultado anterior. Seja $x = \text{mdc}(a/c, b/c)$. De (i) temos que

$$\text{mdc}(a,b) = \text{mdc}\left(\frac{a}{c}\cdot c, \frac{b}{c}\cdot c\right) = \text{mdc}\left(\frac{a}{c}, \frac{b}{c}\right)\cdot|c|,$$

isto é, $d = x|c|$, donde $x = d/|c|$.

Exercício 5.2: (Trabalho p/ casa)

Calcule o $\text{mdc}(72,33)$ e $\text{mdc}(14,52)$.

Exercício 5.3: (Trabalho p/ casa)

Sejam a, b, c inteiros. Provar que

(i) Se $a \mid b$ e $\text{mdc}(b,c) = 1$, então $\text{mdc}(a,c) = 1$.

(ii) $\text{mdc}(a,c) = \text{mdc}(b,c) = 1$ se e somente se $\text{mdc}(ab,c) = 1$.