AULA 6

Algoritmo da Divisão

META:

Apresentar o algoritmo da divisão e do cálculo do MDC entre dois números

OBJETIVOS:

Ao fim da aula os alunos deverão ser capazes de:

Executar de maneira correta os algoritmos da divisão e do cálculo do MDC.

Entender os critérios de divisibilidade.

PRÉ-REQUISITOS

Divisibilidade.

6.1 Introdução

Prezado aluno, nesta aula aprenderemos o algoritmo que realizamos no ensino fundamental para divisão entre 2 números inteiros. Veremos também os famosos critérios de divisibilidade que é exposto no ensino fundamental sem a preocupação de o porque e saberemos com escrever o números em outros sistemas de numeração posicionais.

6.1.1 Divisão Euclidiana

Teorema 6.1. *Dado $x, y \in \mathbb{Z}$, $y \neq 0$, existem únicos inteiros q, r chamados respectivamente de quociente e resto, tais que*

$$x = qy + r, \ 0 \leq r < |y|$$

OBS 6.1. O algoritmo acima é chamado **Algoritmo da Divisão de Euclides**

Demonstração.

Caso 1. $y > 0$: Neste caso considere $B = \{x - ay;\ a \in \mathbb{Z},\ x - ay \geq 0\}$. Note que B é não vazio pois $x - (-|x|y) = x + |x|y \geq x + |x| \geq 0$. Claramente B é limitado inferiormente. Pelo Princípio d Boa Ordem B possui um menor elemento, digamos r. Portanto existe $q \in \mathbb{Z}$ tal que $r = x - qy$. Para mostrar que $r < |y| = y$, note que $r = y \Rightarrow x = (1 + q)y \Rightarrow r = 0 \Rightarrow y = 0$ $(\rightarrow\leftarrow)$. $r > y \Rightarrow \exists\sigma;\ r = y + \sigma$, onde $0 < \sigma < r$. Assim $y + \sigma = x - qy \Rightarrow \sigma = x - (q + 1)y \in B$, o que é um absurdo, pois r é o menor elemento de B. Logo $0 \leq r < |y|$

Mostraremos agora que q, r são unicamente determinados: Suponha que $x = qy + r = \widetilde{q}y + \widetilde{r}$, com $0 \leq r, \widetilde{r} \leq |y| = y$. Neste caso

$0 \leq |r - \widetilde{r}| < y$. Por outro lado, $\widetilde{q}y + \widetilde{r} = qy + r \Rightarrow (\widetilde{q} - q)y = r - \widetilde{r} \Rightarrow |q - \widetilde{q}|y = |r - \widetilde{r}|$. Se fosse $r \neq \widetilde{r}$, teríamos $|q - \widetilde{q}| \geq 1$. Daí $y \leq |q - \widetilde{q}|y = |r - \widetilde{r}| < y$. $(\rightarrow\leftarrow)$. Portanto $r = \widetilde{r}$ e, consequentemente, $q = \widetilde{q}$.

Caso 2. $y < 0$. Para $y < 0$, aplicamos o caso anterior com $x, |y|$. Assim existem únicos $q, r \in \mathbb{Z}$ tais que $x = q|y| + r$, com $0 < r \leq |y|$. Se pomos $q_1 = -q$, então $x = q_1 y + r$, com $0 < r \leq |y|$. Claramente, q_1 é unicamente determinado.

■

Bézout 6.1. *Dados dois números inteiros x, y não simultaneamente nulos, se $d = mdc(x, y)$, então existem inteiros m, n tais que $d = mx + ny$.*

Demonstração. Sejam x, y, d como na hipótese do teorema e considere o conjunto $A = \{ax + by;\ a, b \in \mathbb{Z}\}$ e $B = A \cup \mathbb{N}$. B é não vazio pois x, y não são simultaneamente nulos. Pelo Princípio d Boa Ordem, B tem um menor elemento, digamos δ. Assim existem $m, n \in \mathbb{Z}$ tais que $\delta = mx + ny$. Como $d|x$ e $d|y$, $d|mx + ny$, isto é, $d|\delta$. Assim $d \leq \delta$. Mostraremos que $\delta|x$ e $\delta|y$. De fato, dados $a, b \in \mathbb{Z}$ existem $q, r \in \mathbb{Z}$ tais que $ax + by = q\delta + r,\ 0 \leq r < \delta$, ou seja, $ax + by = q\delta + r \Rightarrow (a - qm)x + (b - qn)y = r$. Logo $r \in A$ e $r \geq 0$. Se fosse $r > 0$, então $r \in B$, o que é um absurdo, pois δ é o menor elemento de B. Logo $r = 0$. Então $\delta|ax + by$ para todo $a, b \in \mathbb{Z}$. Em particular $\delta|x$ e $\delta|y$, donde $\delta|d$. Portanto $\delta \leq d$. Concluímos que $mx + ny = \delta = d$ ■

Propriedade Fundamental do MDC 6.1. *Sejam $x, y, d \in \mathbb{Z}$. Se x, y não são simultaneamente nulos e $d \in \mathbb{Z}_+$ é um divisor comum de x e y. As seguintes afirmações são equivalentes:*

(i) $d = mdc(x, y)$

(ii) Dado $z \in \mathbb{Z}$, *se* $z|x$ *e* $z|y$ *então* $z|d$.

Demonstração. (i) $\Rightarrow$ (ii): Pelo teorema de Bézout, existem $m, n \in \mathbb{Z}$ tais que $d = mx + ny$. Como por hipótese $z|x$ e $z|y$, temos que $z|mx + ny = d$.
(ii) $\Rightarrow$ (i): Seja $\widetilde{d} = mdc(x, y)$. Logo $\widetilde{d}|x$ e $\widetilde{d}|y$. Por hipótese $\widetilde{d}|d$ e portanto $\widetilde{d} \leq d$. Mas d é um divisor comum de x e y. Assim $d \leq \widetilde{d}$, donde concluímos $\widetilde{d} = d = mdc(x, y)$. ■

6.1.2 Sistemas de Numeração Posicionais

Em nosso sistema de numeração natural n é escrito na forma

$$n = a_r 10^r + a_{r-1} 10^{r-1} + ... + a_1 10 + a_0$$

onde $r \geq 0$ e $a_i \in \{0, 1, 2..., 9\}$. O número que representa n é $n = a_r a_{r-1} ... a_1 a_0$

Exemplo 6.1. $641 = 6.10^2 + 4.10 + 1$

O papel que o número 10 representa para nosso sistema é apenas uma opção.

Teorema 6.2. *Seja* b *um número natural,* ≥ 2, *e* $M = \{0, 1, 2, ..., b-1\}$. *Então, todo número natural pode ser representado de forma única da seguinte maneira:*

$$n = a_r b^r + a_{r-1} b^{r-1} + ... + a_1 b + a_0$$

Onde $r \geq 0$, $a_r \neq 0$ *e* $a_i \in M$
Notação: $n = (a_r a_{r-1} ... a_1 a_0)_b$

Demonstração.

. Existência: Se $n < b$, $n = n$. Suponha $n \geq b$ e, por hipótese de indução que todo número q, $1 \leq q < n$ pode ser representado como no teorema. Pelo algoritmo da divisão, existem q e a_0 tais que $n = bq + a_0$. Temos $q < n$. Pois se $q \geq n$, $bq > n$ e isto implica $n = bq + a_0 > n$. Absurdo. Assim por hipótese de indução, $q = a_r b^{r-1} + a_{r-1} b^{r-2} + ... + a_2 b + a_1$. Substituindo q no algoritmo obtemos $n = (a_r b^{r-1} + a_{r-1} b^{r-2} + ... + a_2 b + a_1) b + a_0 = a_r b^r + a_{r-1} b^{r-1} + ... + a_1 b + a_0$, onde $r \geq 0$, $a_r \neq 0$ e $a_i \in M$.

. Unicidade: se $n < b$, ok. Suponha $n \geq b$ e que a unicidade vale para $1 \leq q < n$. Se $n = a_r b^r + a_{r-1} b^{r-1} + ... + a_1 b + a_0 = a'_s b^s + a'_{s-1} b^{s-1} + ... + a'_1 b + a'_0$, então $n = b(a_r b^{r-1} + a_{r-1} b^{r-2} + ... + a_2 b + a_1) + a_0 = b(a'_r b^{s-1} + a'_{s-1} b^{s-2} + ... + a'_2 b + a'_1) + a'_0$. Pela unicidade do algoritmo de euclides, $a_0 = a'_0$ e $a_r b^{r-1} + a_{r-1} b^{r-2} + ... + a_2 b + a_1 = a'_r b^{s-1} + a'_{s-1} b^{s-2} + ... + a'_2 b + a'_1$. Logo por hipótese de indução, $r - 1 = s - 1 \Rightarrow r = s$ e $a_r = a'_r$.

■

Exemplo 6.2. (a) $(2102)_3 = 2.3^3 + 1.3^2 + 0.3 + 2 = 65$

(b) $(1001001)_2 = 1.2^6 + 0.2^5 + 0.2^4 + 1.2^3 + 0.2^2 + 0.2 + 1 = 73$

(c) Coloque 4761 na base 8. $4761 = 8.595 + 1$, $595 = 8.74 + 3$, $74 = 8.9 + 2$, $9 = 8.1 + 1$, donde $4761 = (11231)_8$.

Definição 6.1. Seja $n \in \mathbb{Z}$. Dizemos que n é par se $n = 2k$, com $k \in \mathbb{Z}$. Dizemos que n é ímpar se $n = 2k + 1$, com $k \in \mathbb{Z}$.

Exercício 6.1. (1) m é par $\Leftrightarrow m + 2n$ é par.

(2) $m + n$ é ímpar $\Leftrightarrow m - n$ é ímpar.

(3) Mostre que se $a \in \mathbb{Z}$ um dos números $a, a+1, a+2$ é divisível por 3.

(4) Se n é um inteiro par então$mdc(n, n+2) = 2$.

(5) Se n é um inteiro ímpar, então $mdc(n, n+2) = 1$.

(6) Seja m um inteiro cujo resto da divisão por 6 é 5. Mostre que o resto da divisão de m por 3 é 2.

Solução:

(1) Seja $m, n \in \mathbb{Z}$. ($\Rightarrow$): Se m é par, então $m = 2k$, $k \in \mathbb{Z}$. Logo $m + 2n = 2k + 2n = 2(k + n)$ com $k + n \in \mathbb{Z}$. Logo $m + 2n$ é par. ($\Leftarrow$): Reciprocamente, se $m + 2n$ é par, $m + 2n = 2k$, com $k \in \mathbb{Z}$. Assim, $m = 2k - 2n = 2(k - n)$. Logo m é par.

(2) ($\Rightarrow$): Se $m + n$ é ímpar, $m + n = 2k + 1$, com $k \in \mathbb{Z}$. Desse modo $m + n - 2n = 2k + 1 - 2n = 2(k - n) + 1 \Rightarrow m - n = 2(k - n) + 1$, com $k - n \in \mathbb{Z}$. Portanto, $m - n$ é ímpar. ($\Leftarrow$): Se $m - n$ é ímpar, então $m - n = 2k + 1$, com $k \in \mathbb{Z}$, isto é, $m - n + 2n = 2k + 1 + 2n = 2(k + n) + 1 \Rightarrow m + n = 2(k + n) + 1$, com $k + n \in \mathbb{Z}$. Logo, $m + n$ é ímpar.

(3) Pelo algoritmo da divisão, existem $q, r \in \mathbb{Z}$ tais que $a = 3q + r$, com $0 \leq r < 3$. Se $r = 0$, $a = 3q$, portanto $3|a$. Se $r = 1$, então $a = 3q + 1$, portanto $a + 2 = 3(q + 1)$, donde $3|a + 2$. Se $r = 2$, $a + 1 = 3(q + 1)$, donde $3|a + 1$.

(4) Se n é par então $n = 2k$, $k \in \mathbb{Z}$. Observe que $2|n$ e $2|2(k + 1) = n + 2$. Seja $d = mdc(n, n + 2)$. Como $d|n$ e $d|n + 2$, $d|n + 2 - n$, isto é, $d|2$. Mas, como $2|n$ e $2|n + 2$, $2|d$. Logo $d = 2$.

(5) Se n é ímpar, $n = 2k + 1$, $k \in \mathbb{Z}$. Seja $d = mdc(n, n + 2)$. Pelo mesmo motivo de antes, $d|2$, donde $d = 1$ ou $d = 2$. Se

fosse $d = 2$, então, $2|2k+1$, isto é, $1 = 2(j-k)$, com $j \in \mathbb{Z}$. Absurdo. Logo $d = 1$.

(6) Se $m = 6q+5$ para algum $q \in \mathbb{Z}$, então, $m = 3.2.q+3+2 = 3(2q+1)+2$, donde o que queríamos.

6.1.3 Critérios de Divisibilidade

(1) Critério de divisibilidade por 2:

Dado qualquer número natural n podemos escrevê-lo na forma $n = a_r 10^r + a_{r-1}10^{r-1} + ... + a_1 10 + a_0$. Observe que qualquer potência de 10 é um número par, ou seja, $10^r = 2q_r$, $q_r \in \mathbb{N}$. Logo, $n = a_r(2q_r) + a_{r-1}(2q_{r-1}) + ... + a_1(2q_1) + a_0$ e portanto, $n = a_0 + 2(a_1q_1 + ... + a_{r-1}q_{r-1} + a_rq_r)$, ou seja, podemos escrever $n = a_0 + 2q$, com $q \in \mathbb{Z}$. Note que se $2|n$, $2|n-2q$, isto é, $2|a_0$. Assim $a_ra_{r-1}...a_1a_0$ é divisível por 2 se $a_0 \in \{0, 2, 4, 6, 8, ...\}$.

(2) Critério de Divisibilidade por 3:

Já sabemos que um número natural n pode ser escrito na forma $n = a_r 10^r + a_{r-1}10^{r-1} + ... + a_1 10 + a_0$.

Afirmação: $10^k = 3q+1$ com $q \in \mathbb{Z}$, para todo $k \in \mathbb{N}$.

De fato, se $k = 1$ temos que $10 = 3.3+1$. Suponha que $10^k = 3q_1 + 1$ para algum $q_1 \in \mathbb{Z}$. Note que

$$\begin{aligned}10^{k+1} = 10^k.10 \quad &= (3q_1+1)(3.3+1)\\ &= 3.9.q_1 + 3q_1 + 3.3 + 1\\ &= 3(9q_1 + q_1 + 3) + 1\\ &= 3q+1\end{aligned}$$

Portanto pelo princípio de indução $10^k = 3q+1$ com $q \in \mathbb{Z}$, para todo $k \in \mathbb{N}$.

Logo $n = a_r(3q_r+1)+a_{r-1}(3q_{r-1}+1)+...+a_1(3q_1+1)+a_0 = 3(a_rq_r+...+a_1q_1)+(a_r+...+a_1+a_0) = 3q+(a_r+...+a_1+a_0)$. Se $3|n$ então $3|n-3q$, isto é $3|(a_r+...+a_1+a_0)$.

Exemplo 6.3. 343892 não é divisível por 3 pois $3+4+3+8+0+2 = 29$ e $3|29$ (não divide)

(3) Critério de Divisibilidade por 4:

Seja $n = a_r10^r + a_{r-1}10^{r-1} + ... + a_110 + a_0$. temos que $n = 100(a_r10^{r-2}+a_{r-1}10^{r-3}+...+a_2)+a_110+a_0$. Observe que $4|100$. Assim, $4|100$ se, e somente se, $4|n-100(a_r10^{r-2}+a_{r-1}10^{r-3}+...+a_2)$, ou seja, $4|a_110+a_0$. Logo $n = a_ra_{r-1}...a_1a_0$ é divisível por 4 se, e somente se, a_1a_0 é divisível por 4.

6.1.4 Teorema Fundamental da Aritmética

Definição 6.2. Dois números x, y são ditos primos entre si se $mdc(x, y) = 1$.

Exemplo 6.4. Dado $a \in \mathbb{Z}$, temos que a e $a+1$ são primos entre si. Com efeito, seja $d = mdc(a, a+1)$. Assim $d|a$ e $d|a+1$, donde $d|a+1-a$, isto é, $d|1$. Logo, $d = 1$.

Lema de Gauss 6.1. *Sejam x, y, z inteiros não nulos tais que x, y são primos entre si e $x|yz$. Então $x|z$.*

Demonstração. Como $mdc(x, y) = 1$, pelo Teorema de Bézout existem $a, b \in \mathbb{Z}$ tais que $ax + by = 1$. Assim, $axz + byz = z$. Por hipótese, $x|yz$, donde $x|byz$. Como $x|axz$, $x|axz + byz$, isto é, $x|z$.

■

Teorema Fundamental da Aritmética 6.1. *Todo número inteiro maior ou igual a 1 pode ser representado de maneira única (a menos da ordem), como produto de fatores primos.*

Demonstração. Falta mostrar a unicidade. Faremos isto usando o segundo princípio da indução. Seja $n \geq 2$. Se $n = 2$, ok. Suponha que a afirmação sobre a unicidade seja verdadeira para todo número maior que 1 e menor que n. Se n é primo, não há nada o que fazer. Suponha que n seja composto. Seja $n = p_1 p_2 ... p_r = q_1 q_2 ... q_s$ duas fatorações de n. vamos mostrar que $r = s$ e que $p_i = q_j$ para algum i e algum j. Observe que $p_1 | n$ e portanto $p_1 | q_1 q_2 ... q_s$. Logo, p_1 divide algum q_j, digamos q_1, ou seja $p_1 = q_1$. Logo $\widetilde{n} = p_2 ... p_r = q_2 ... q_s$, pois $n = \widetilde{n} p_1 = \widetilde{n} q_1$. Observe que $1 < \widetilde{n} < n$. Logo, por hipótese de indução, $r - 1 = s - 1 \Rightarrow r = s$. Além disso,$p_2 ... p_r = q_2 ... q_r$ são iguais a menos da ordem. Portanto a decomposição $n = p_1 ... p_r$ é única a menos da ordem. ■

6.2 Conclusão

Note que os critérios de divisibilidade são meras consequências do Algoritmo da Divisão. Além disso é importante saber, caro aluno, que isso tem com ser explicado de maneira simples no ensino fundamental através de vários exemplos.

RESUMO

..

Algoritmo da Divisão

Dado $x, y \in \mathbb{Z}$, $y \neq 0$, existem únicos inteiros q, r chamados respectivamente de quociente e resto, tais que

$$x = qy + r, \ 0 \leq r < |y|$$

Teorema Fundamental do MDC

Sejam $x, y, d \in \mathbb{Z}$. Se x, y não são simultaneamente nulos e $d \in \mathbb{Z}_+$ é um divisor comum de x e y. As seguintes afirmações são equivalentes:

(i) $d = mdc(x, y)$

(ii) Dado $z \in \mathbb{Z}$, se $z|x$ e $z|y$ então $z|d$.

Teorema Fundamental da Aritmética

Todo número inteiro maior ou igual a 1 pode ser representado de maneira única (a menos da ordem), como produto de fatores primos.

Sistema de Numeração posicional

Seja b um número natural, ≥ 2, e $M = \{0, 1, 2, ..., b - 1\}$. Então, todo número natural pode ser representado de forma única da seguinte maneira:

$$n = a_r b^r + a_{r-1} b^{r-1} + ... + a_1 b + a_0$$

Onde $r \geq 0$, $a_r \neq 0$ e $a_i \in M$

Notação: $n = (a_r a_{r-1} ... a_1 a_0)_b$

PRÓXIMA AULA

Na próxima aula apresentaremos um algoritmo para o cálculo do MDC. Além disso definiremos mínimo múltiplo comum (MMC) entre 2 números inteiros e um algoritmo para se calcular o MMC.

ATIVIDADES

ATIV. 6.1. Se p um número primo e $p|ab$, onde $a, b \in \mathbb{Z}$, então $p|a$ ou $p|b$. (Compare com o exercício 7 da lista 2. É verdadeiro?)

ATIV. 6.2. Seja K um conjunto dos números inteiros, não vazio, fechado em relação a multiplicação e a adição ($a + b, a \cdot b \in K$ se $a, b \in K$) e $K \neq 0$. Mostre que:

a) $0 \in K$;

b) K contém um menor inteiro positivo, digamos m;

c) K contém todos os múltiplos positivos de m;

d) Todo elemento de K é um múltiplo de m.

ATIV. 6.3. Se $a|c$, $b|c$ e $MDC(a, b) = d$, então $ab|cd$.

ATIV. 6.4. Mostre que se $n \geq 2$, então 12^n é divisível por 8. Use este fato para mostra que $n = (a_r a_{r-1} \dots a_1 a_0)_{12}$ é divisível por 8 se, e somente se, $(a_1 a_0)_{12}$ é divisível por 8.

ATIV. 6.5. Na divisão euclidiana de -345 por um inteiro $b > 0$, o resto é 12. Ache o divisor e o quociente em todos os casos possíveis.

ATIV. 6.6. Seja m um inteiro ímpar. Mostre que o resto da divisão de m por 4 é 1 ou 3.

ATIV. 6.7. Sejam a, b e c inteiros arbitrários. Se $MDC(a, b) = 1$ e $c|(a + b)$, prove que $MDC(a, c) = MDC(b, c) = 1$

LEITURA COMPLEMENTAR

LIMA, Elon L., Análise na Reta Vol. 1, IMPA, Projeto Euclides, 5.ed., Rio de Janeiro, 2008.

LIMA, Elon L., Matemática para o Ensino Médio 1, SBM, 5.ed,Rio de Janeiro, 2008.

DOMINGUES, H. Fundamentos de Aritmética, Atual Editora, São Paulo, 2001.

SANTOS, J. P. O. Introdução à Teoria dos Números, IMPA, Rio de Janeiro, 2007

Bahiano, C. Notas de aula. UFBA