UFRJ - Universidade Federal do Rio de Janeiro

Rio de Janeiro, 14 de Março de 2017

- TEOREMA DA DIVISÃO

Dados dois inteiros positivos a e b, existem dois inteiros q e r (chamados de quociente e resto da divisão inteira de a por b) tais que:

$$\begin{cases} a = bq + r \\ 0 \leq r < b \end{cases}$$

Além disso os inteiros q e r que satisfazem estas duas condições são únicos.

EXISTÊNCIA → basta exibirmos uma maneira qualquer de calcular estes valores
Exemplo: Algoritmo "bobo" da divisão.

UNICIDADE → PROVA POR CONTRADIÇÃO: Suponha, por contradição, que existem $q \neq q'$ e $r \neq r'$ tais que:

$$\begin{cases} a = bq + r \\ 0 \leq r < b \end{cases} \qquad \begin{cases} a = bq' + r' \\ 0 \leq r' < b \end{cases}$$

$\therefore a = bq + r$

$(-)\ a = bq' + r'$

$0 = b(q - q') + (r - r')$

$b(q - q') = r - r'$

Suponha, sem perda de generalidade, que $r' \geq r$

$\hookrightarrow r' - r \geq 0$

$r < b$

$r' < b$

$r' - r < b$

$0 \leq r' - r < b$

$0 \leq b(q - q') < b$

↳ $\neq 0$ ↓ menor valor para b

$0 \leq q - q' < 1$

$q - q' = 0$

$q = q'$

$q = q' \ + \ q \neq q' \rightarrow$ contradição

$b \underbrace{(q - q')}_{0} = r' - r$

$r' - r = 0$

$r = r'$

$r = r' \ + \ r \neq r' \rightarrow$ Contradição

Logo, q e r são únicos.

Sejam a e b dois inteiros, com $b \neq 0$, dizemos que b divide a ou b é divisor de a ou b é fator de a ou a é divisível por b ou a é múltiplo de b se existe um número inteiro k tal que $a = b \cdot k$.

DEFINIÇÃO: sejam a e b dois inteiros positivos. O máximo divisor comum entre a e b é o maior inteiro d tal que d é divisor de a e também de b.

- ALGORITMO "INGÊNUO" PARA O CÁLCULO DO MDC:

Dados a e b, calculo a lista de todos os divisores de a, calculo a lista de todos os divisores de b e busco o maior inteiro que aparece nas duas listas. Isso é extremamente lento.

- ALGORITMO MAIS EFICIENTE: ALGORITMO EUCLIDIANO

- EXEMPLO: MDC ENTRE 1234 E 54 MDC (1234, 54) = 2

	22	1	5	1	3
1234	54	46	8	6	2 → MDC
	46	8	6	2	0

- Dividir 1234 por 54 → q = 22
r = 46

- Dividir 54 por 46 → q = 1
r = 8

- Dividir 46 por 8 → q = 5
r = 6

- Dividir 8 por 6 → q = 1
r = 2

- Dividir 6 por 2 → q = 3
r = 0

- MAIS GENERICAMENTE:

$a = b q_1 + r_1 \quad 0 \leq r_1 < b$

$b = r_1 q_2 + r_2 \quad 0 \leq r_2 < r_1$

$r_1 = r_2 q_3 + r_3 \quad 0 \leq r_3 < r_2$

⋮

$r_j = r_{j+1} q_{j+2} + r_{j+2} \quad 0 \leq r_{j+2} < r_{j+1}$

⋮

$r_{n-2} = r_{n-1} q_n + r_n$, $r_n = 0$ → TÉRMINO

- O MDC é o último resto diferente de 0.

→ $MDC(a,b) = r_{n-1}$

tilibra

(11)

- VAMOS MOSTRAR QUE O ALGORITMO SEMPRE TERMINA:

$b > r_1 > r_2 > r_3 > \dots > 0$

Todos os restos são inteiros. Existe uma quantidade finita de inteiros entre b e 0. Logo, em algum momento, algum dos restos da sequência será igual a 0. e o algoritmo terminará.

- VAMOS MOSTRAR QUE O ALGORITMO PRODUZ O RESULTADO CORRETO, ISTO É, QUE O ÚLTIMO RESTO DIFERENTE DE ZERO É REALMENTE O MDC ENTRE A E B:

Para isso precisamos de um lema auxiliar.

LEMA: sejam a, b, g e s inteiros positivos tais que $a = bg + s$. Então, $MDC(a,b) = MDC(b,s)$.

Seja $d_1 = MDC(a,b)$ e $d_2 = MDC(b,s)$. Quero mostrar que $d_1 = d_2$.

$d_1 = MDC(a,b)$ → $a = d_1 \cdot k$

$d_1 = MDC(a,b)$ → $b = d_1 \cdot l$

$a = bg + s$

$a_1 k = d_1 l_g + s$

$d_1 k - d_1 l_g = s$

$\underbrace{d_1 (k - l_g) = s}_{d_1 \text{ DIVIDE } s}$

d_1 divide b
d_1 divide s
} d_1 é divisor comum de b e s.

Como d_2 é o máximo divisor comum de b e s, então $d_1 \leq d_2$

$d_2 = MDC(b,s)$ → $b = d_2 \cdot m$

$d_2 = MDC(b,s)$ → $s = d_2 \cdot n$

$a = bq + s$

$a = d_2 m q + d_2 n = d_2 (mq + n)$

d_2 DIVIDE A

d_2 divide a
d_2 divide b
} d_2 é divisor comum de a e b

Como d_1 é o máximo divisor comum de a e b, então $d_2 \leq d_1$

$d_1 \geq d_2$
$d_2 \geq d_1$
} $d_1 = d_2$

Refinando um pouco mais o algoritmo euclidiano, ele pode nos dar mais dados utéis além do MDC.

↳ ALGORITMO EUCLIDIANO ESTENDIDO (PROPOSTO POR KNUTH)

Dados dois inteiros positivos a e b, quero calcular dois inteiros (não necessáriamente positivos) α e β tais que:

$$\alpha \cdot a + \beta \cdot b = d,$$

onde d é o $MDC(a,b)$

- ALGORITMO SENDO PROVADO GENERICAMENTE (PRÓXIMA PÁGINA)

		(*) (**)
$a = bq_1 + r_1$	$0 \leq r_1 < b$	$r_1 \cdot a + y_1 \cdot b = r_1$
$b = r_1 q_2 + r_2$	$0 \leq r_2 < r_1$	$x_2 \cdot a + y_2 b = r_2$
$r_1 = r_2 q_3 + r_3$	$0 \leq r_3 < r_2$	$x_3 \cdot a + y_3 b = r_3$
⋮	⋮	⋮
$r_{j-2} = r_{j-1} \cdot q_j + r_j$	$0 \leq r_j < r_{j-1}$	$x_j \cdot a + y_j \cdot b = r_j$
$r_{j-1} = r_j \cdot q_{j+1} + r_{j+1}$	$0 \leq r_{j+1} < r_j$	$x_{j+1} \cdot a + y_{j+1} \cdot b = r_{j+1}$
$r_j = r_{j+1} \cdot q_{j+2} + r_{j+2}$	$0 \leq r_{j+2} < r_{j+1}$	$x_{j+2} \cdot a + y_{j+2} \cdot b = r_{j+2}$
⋮	⋮	⋮
$r_{n-3} = r_{n-2} \cdot q_{n-1} + r_{n-1}$	$0 \leq r_{n-1} < r_n$	$x_{n-1} \cdot a + y_{n-1} \cdot b = r_{n-1} \rightarrow MDC(a,b)$
$r_{n-2} = r_{n-1} \cdot q_n + r_n$	$r_n = 0$	$x_{n-1} \rightarrow \alpha$; $y_{n-1} \rightarrow \beta$

$$x_j a + y_j b = (x_{j+1} a + y_{j+1} b) \cdot q_{j+2} + (x_{j+2} a + y_{j+2} b)$$

$$x_j a + y_j b - x_{j+1} a q_{j+2} - y_{j+1} b q_{j+2} = x_{j+2} a + y_{j+2} b$$

$$(x_j - x_{j+1} \cdot q_{j+2}) a + (y_j - y_{j+1} \cdot q_{j+2}) b = x_{j+2} a + y_{j+2} b$$

$$\begin{cases} x_{j+2} = x_j - x_{j+1} \cdot q_{j+2} \\ y_{j+2} = y_j - y_{j+1} \cdot q_{j+2} \end{cases}$$

(*) $x_{-1} \cdot a + y_{-1} b = a \rightarrow x_{-1} = 1 \;/\; y_{-1} = 0$

(**) $x_0 \cdot a + y_0 b = b \rightarrow x_0 = 0 \;/\; y_0 = 1$

EXEMPLO NUMÉRICO: MDC (1234, 54) → PRÓXIMA PÁGINA

RESTO	QUOCIENTE	α ou X	β ou Y
1234	–	1	0
54	–	0	1
46	22	1	-22
8	1	-1	23
6	5	6	-137
2	1	-7	160
0	3	–	–

Daqui sai o MDC e o α e o β