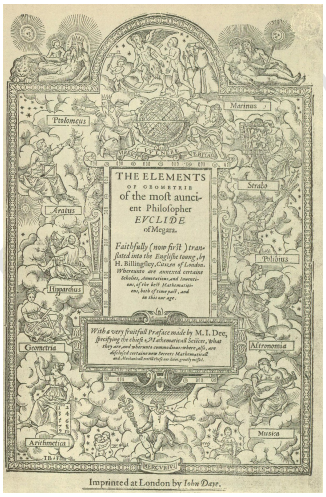
Aula 6. O Algoritmo de Euclides

6.1 Lema de Euclides

Na Aula passada a gente definiu o máximo divisor comum (mdc) entre dois inteiros dados a e b. Do curso secundário, a gente conhece o método para determinar o mdc de dois números usando a decomposição deles em fatores primos (que trataremos brevemente nas próximas Aulas). Porem, quando se trata de números muito grandes, pode ser bem difícil encontrar essa decomposição. O método que damos a seguir é baseado apenas em divisões sucessivas e aparece no livro sétimo dos Elementos de Euclides; porém, há evidências históricas de que o método seja ainda anterior a essa obra.



Os Elementos

O método de Euclides é baseado na seguinte lema.

Lemma 6.1

Sejam a, b inteiros com $b \neq 0$, e sejam q, r o quociente e o resto da divisão de a por b, respectivamente. Então,

$\mathrm{Div}(a,b) = \mathrm{Div}(b,r)$, e assim

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

Prova

Podemos escrever $a = bq + r$. Seja $x \in \mathrm{Div}(a,b)$. Então, $x \mid a$ e $x \mid b$. Mas $r = a - bq$ e x divide cada um dos somados, logo $x \mid r$. Mostra mos, assim, que

$$D(a,b) \subset D(b,r).$$

A inclusão contrária segue de forma análoga, donde resulta a igualdade dos conjuntos.
Se os conjuntos são iguais, assim seus máximos também coincidem, ou seja

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

Segue do lema acima que o problema de achar o $\mathrm{mdc}(a,b)$ reduz-se a achar o $\mathrm{mdc}(b,r)$.

Naturalmente, pode-se repetir esse processo. Fazendo divisões

sucessivas, teremos:

$$\begin{aligned}
a &= bq + r_1, \quad 0 \leq r_1 < b,\\
b &= r_1q_2 + r_2, \quad 0 \leq r_2 < r_1,\\
r_1 &= r_2q_3 + r_3, \quad 0 \leq r_3 < r_2,\\
&\cdots \quad \cdots\\
r_{n-2} &= r_{n-1}q_n + r_n, \quad 0 \leq r_n < r_{n-1},\\
r_{n-1} &= r_nq_{n+1}.
\end{aligned}$$

Como o resto diminui a cada passo, o processo não pode continuar indefinidamente, e alguma das divisões deve ser exata. Suponhamos então que r_{t+1} seja o primeiro resto nulo, como está indicado antes. Do lema, temos que

$$\text{mdc}(a,b) = \text{mdc}(b,r_1) = \text{mdc}(r_1,r_2) = \cdots = \text{mdc}(r_{n-1},r_n).$$

Finalmente, como $r_n \mid r_{n-1}$ é fácil ver que $\text{mdc}(r_{n-1},r_n) = r_n$ logo, $\text{mdc}(a,b) = r_n$.

Demonstramos assim que, nesse processo, o máximo divisor comum de a e b é **o último resto diferente de zero**.

Na pratica vamos colocar os números que intervêm no processo de cálculo do $\text{mdc}(a,b)$ na seguinte tabela:

	q_1	q_2	q_3	$\cdots\cdots$	$\cdots\cdots$	q_n	q_{n+1}
a	b	r_1	r_2	$\cdots$	r_{n-2}	r_{n-1}	r_n
r_1	r_2	r_3	$\cdots$	$\cdots$	r_n	0	

Exemplo 6.1

Sejam $a = 36$, $b = 30$, assim

$$\begin{aligned}
36 &= 30 \cdot 1 + 6, \quad \Rightarrow \quad \text{mdc}(36,30) = \text{mdc}(30,6),\\
30 &= 6 \cdot 5 + 0, \quad \Rightarrow \quad \text{mdc}(30,6) = \text{mdc}(6,0) = 6.
\end{aligned}$$

Como ultimo resto não nulo é 6 e $\text{mdc}(36,30) = \text{mdc}(30,6) = 6$.
Colocando na tabela, temos:

		1	5
36	30	6	
6	0		

Por outro lado se $a = 1128$ e $b = 336$, assim

	3	2	1	4
1128	336	120	96	24
120	96	24	0	

$\text{mdc}(1128,336) = \text{mdc}(336,120) = \text{mdc}(120,96) = \text{mdc}(96,24) = \text{mdc}(24,0) = 24.$

Exemplo 6.2

Vamos fazer mais um exemplo com numeros a, e b bem grandes, para mostrar a eficiência do algoritmo. Assim sejam $a = 42823$, $b = 6409$.

$$\begin{aligned} 42823 &= 6409 \cdot 6 + 4369, && \Rightarrow && \text{mdc}(42823, 6409) = \text{mdc}(6409, 4369) \\ 6409 &= 4369 \cdot 1 + 2040, && \Rightarrow && \text{mdc}(6409, 4369) = \text{mdc}(4369, 2040) \\ 4369 &= 2040 \cdot 2 + 289, && \Rightarrow && \text{mdc}(4369, 2040) = \text{mdc}(2040, 289) \\ 2040 &= 289 \cdot 7 + 17, && \Rightarrow && \text{mdc}(2040, 289) = \text{mdc}(289, 17) \\ 289 &= 17 \cdot 17 + 0 && \Rightarrow && \text{mdc}(289, 17) = 17. \end{aligned}$$

E precisam de fazer apenas 5 divisões para encontrar o mdc neste caso.

Theorem 6.1: (Lame, 1844)

O numero dos divisões em aplicação do Algoritmo de Euclides é menor igual do que 5 vezes numero dos dígitos em menor numero.

Por exemplo o numero dos divições para buscar

$$\text{mdc}(117035, 35688479)$$

é menor igual que $5 \cdot 6 = 30$.

6.2 *Alguns exercícios*

Exercício 6.1: (Primeira Olimpíada Internacional, 1959)

Prove que a fração $\dfrac{21n+4}{14n+3}$ é irredutível para todo número natural n.

Solução 6.1

O problema é mostrar que $21n+4$ e $14n+3$ não tem os divisores comuns, isto é precisamos mostrar que

$$\text{mdc}(21n+4, 14n+3) = 1, \quad n \geq 0.$$

Temos

$$\begin{aligned} 21n+4 &= (14n+3) \cdot 1 + (7n+1), \\ 14n+3 &= (7n+1) \cdot 2 + 1, \\ 7n+1 &= (7n+1) \cdot 1 + 0. \end{aligned}$$

Assim,

$$\begin{aligned} \text{mdc}(21n+4, 14n+3) &= \text{mdc}(14n+3, 7n+1) \\ &= \text{mdc}(7n+1, 1) = 1, \end{aligned}$$

para todos $n \geq 0$

Proposição 6.1

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

Prova

Como $\text{mdc}(a, b) = 1$ pelo Teorema de Bezout existem inteiros r, s tais que

$$1 = ar + bs.$$

Multiplicando por c temos

$$c = arc + bsc.$$

Agora temos que a obviamente é divisor de acr por outro lado a divide bc (pela condição), assim a divide bcs. Como a divide acr e bcs, assim a divide a soma $arc + bsc = c$.

Proposição 6.2

Se $\text{mdc}(c, b) = 1$, assim

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

Prova

Vamos mostrar que $\text{Div}(ac, b) = \text{Div}(a, b)$ se $\text{mdc}(c, b) = 1$.
Se $d \mid a$ e $d \mid b$ assim $d \mid ac$, portando qualquer divisor de a e b é divisor de ac e b também, assim

$$\text{Div}(a, b) \subset \text{Div}(ac, b).$$

Por outro lado, pelo teorema de Bezout existes r, s tais que

$$br + cs = 1,$$

assim temos que

$$abr + acs = a.$$

Se $d \mid ac$ e $d \mid b$, temos que pelo $d \mid acs$ e $d \mid bra$, assim d divide $abr + acs = a$ também ou seja

$$\text{Div}(ac, b) \subset \text{Div}(a, b).$$

Rezumindo, temos que

$$\text{Div}(a, b) = \text{Div}(ac, b).$$

ou seja $\text{mdc}(ac, b) = \text{mdc}(a, b)$.

Exercício 6.2

Mostre que

$$\text{mdc}(n^2, 2n + 1) = 1,$$

para todos $n \geq 1$.

Solução 6.2

È difícil dividir n^2 por $2n+1$. Observem, que $2n+1$ é numero impar assim

$$\text{mdc}(2n+1, 2) = 1.$$

Isso pode ser visto através o processo de Euclides. Temos que

$$2n+1 = 2 \cdot (n) + 1,$$

assim

$$\text{mdc}(2n+1, 2) = \text{mdc}(2, 1) = 1.$$

Assim pela Proposição acima, temos

$$\text{mdc}(n^2, 2n+1) = \text{mdc}(2n^2, 2n+1).$$

Agora

$$\begin{aligned} \text{mdc}(n^2, 2n+1) &= \text{mdc}(2n^2, 2n+1), && (\text{mdc}(2n+1, 2) = 1) \\ &= \text{mdc}(2n+1, -n), && (2n^2 = n(2n+1) + (-n)) \\ &= \text{mdc}(2n+1, n), \\ &= \text{mdc}(n, 1) = 1. \end{aligned}$$

6.3 *Algoritmo de Euclides e Teorema de Bézout*

Notamos, agora, que o processo de Euclides também permite determinar inteiros r e s nas condições do Teorema de Bézout. De fato, da primeira das divisões, temos que

$$r_1 = a - q_1 b$$

isto é, r_1 foi escrito como uma combinação linear de a e b. Substituindo r_1 pelo seu valor na segunda, temos: $b = (a - q_1 b) q_2 + r_2$; $\log 0$, $r_2 = -q_2 a + (1 + q_1 q_0) b$ Novamente, pudemos escrever r_2 como combinação linear de $a \in b$. Na igualdade seguinte poderemos substituir $t_1 e r_2$ pelas expressões achadas e escrever r_3 cm função de a c b. Reiterando o processo, obtermos finalmente uma expressão para r_{11} como combinação lincar de a e b. Escrevendo explicitamente as divisões, no caso do exemplo com $a = 1128$ e $b = 336$ temos:

$$1128 = 3 \cdot 336 + 120, \tag{6.1}$$

$$336 = 2 \cdot 190 + 96, \tag{6.2}$$

$$120 = 1 \cdot 96 + 24, \tag{6.3}$$

$$96 = 4 \cdot 24. \tag{6.4}$$

Em (6.1), obtemos $120 = 1128 - 3 \cdot 336$. Substituindo em (6.2). vem que $336 = 2 \cdot (1128 - 3 \cdot 336) + 96$, logo, $96 = -2 \cdot 1128 + 7 \cdot 336$.

Finalmente, em (6.3) obteremos

$$1128 - 3 \times 336 = 1 \cdot (-2 \cdot 1128 + 7 \cdot 336) + 24,$$

logo

$$24 = 3 \cdot 1128 - 10 \cdot 336.$$

Assim, um par de inteiros r, s nas condições do Teorema de Bézout
ê dado por $r = 3$ e $s = -10$.

Exemplo 6.3

Vamos encontrar r, s tais que

$$994r + 399s = \text{mdc}(994, 399).$$

Primeiramente vamos encontrar $\text{mdc}(994, 399)$.

$$\begin{aligned} 994 &= 399 \cdot 2 + 196, &\Rightarrow\quad & \text{mdc}(994, 399) = \text{mdc}(399, 196), \\ 399 &= 196 \cdot 2 + 7, &\Rightarrow\quad & \text{mdc}(399, 196) = \text{mdc}(196, 7), \\ 96 &= 7 \cdot 24, &\Rightarrow\quad & \text{mdc}(196, 7) = 7. \end{aligned}$$

Temos

$$7 = 399 - 196 \cdot 2$$

Por outro lado

$$196 = 994 - 399 \cdot 2$$

Assim

$$7 = 399 - (994 - 399 \cdot 2) \cdot 2$$

o que pode ser escrito como

$$7 = 994 \cdot (-2) + 399 \cdot 5$$

Assim $r = -2$, e $s = 5$.

Exemplo 6.4

Sejam $a = 273$, $b = 94$. Pelo algoritmo de Euclides temos

$$\begin{aligned} 273 &= 94 \cdot 2 + 85 \quad 94 &&= 85 \cdot 1 + 9 \\ 85 &= 9 \cdot 9 + 4 \\ 9 &= 4 \cdot 2 + 1 \\ 4 &= 1 \cdot 4 \end{aligned}$$

Temos:

$$1 = 9 - 4 \cdot 2, \quad 4 = 85 - 9 \cdot \quad 84$$

ou seja

$$1 = 9 - (85 - 9 \cdot 9) \cdot 2 = 85 \cdot (-2) + 9 \cdot 19$$

Agora $9 = 94 - 85$, ou seja

$$1 = 85 \cdot (-2) + (94 - 85) \cdot 19 = 94 \cdot 19 + 85 \cdot (-21)$$

Finalmente $85 = 273 - 94 \cdot 2$ ou seja

$$1 = 94 \cdot 19 + (273 - 94 \cdot 2) \cdot (-21) = 274 \cdot (-21) + 91 \cdot (61).$$

Assim $r = -21$, e $s = 61$.

Exercício 6.3: (Trabalho p/ casa)

Encontre o máximo divisor comum d de 93 e 42 e encontre os inteiros r e s resolvendo a equação

$$93r + 42s = d.$$

Resposta: $93 \cdot 5 + 42 \cdot (-11) = 3$..

Exercício 6.4: (Trabalho p/ casa)

Encontre o máximo divisor comum d de 1310 e 108 e encontre os inteiros r e s resolvendo a equação

$$1310r + 108s = d.$$

Resposta: $1310 \cdot (-23) + 108 \cdot (279) = 2$..

Exercício 6.5: (Trabalho p/ casa)

Mostre que

$$\text{mdc}(n^2, n^2 + n + 1) = 1,$$

para todos n.

Exercício 6.6: (Trabalho p/ casa)

Mostre que se

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

assim

$$\text{mdc}(ab, c^2) = 1.$$