Mínimo múltiplo comum

Sejam $a, b \in \mathbb{Z} \setminus \{0\}$. Sabemos que

$$a \mid ab \quad e \quad b \mid ab$$

pelo que podemos dizer que

$$\{k \in \mathbb{N} : a \mid k \text{ e } b \mid k\} \quad \text{é não vazio}$$

Pelo Princípio da boa ordenação de $\mathbb{N}$, existe

$$\min \{k \in \mathbb{N} : a \mid k \text{ e } b \mid k\}$$

A este mínimo chamamos o mínimo múltiplo comum de a e de b.

__Definição__: Sejam $a, b \in \mathbb{Z} \setminus \{0\}$. Chama-se mínimo múltiplo comum de a e b, e representa-se por $m.m.c\,(a,b)$, ao inteiro positivo m tal que:

(i) $a \mid m$ e $b \mid m$

(ii) se $c \in \mathbb{N}$ é tal que $a|c$ e $b|c$ então $m \leq c$.

Se $a=0$ ou $b=0$ então $m.m.c(a,b) = 0$.

<u>Observação</u>: Para quaisquer inteiros a,b $m.m.c(a,b) \leq |ab|$.

<u>Lema</u> Sejam $a,b \in \mathbb{Z} \setminus \{0\}$ e $m \in \mathbb{Z}$. Então $m = m.m.c(a,b)$ sse:

(i) $a|m$ e $b|m$

(ii) se $c \in \mathbb{Z}$ tal que $a|c$ e $b|c$ então $m|c$.

<u>Demonst</u>: Análoga à que foi feita para $m.d.c(a,b)$.

<u>Teorema</u> Para quaisquer inteiros positivos a e b

$$m.m.c(a,b) = \frac{ab}{m.d.c(a,b)}$$

Demonst: Começamos por observar que sendo $a, b > 0$, temos que $m.d.c\,(a,b) \neq 0$.

Sendo $d = m.d.c(a,b)$, existem $x, y \in \mathbb{Z}$ tais que $a = dx$ e $b = dy$ e $x', y' \in \mathbb{Z}$ tais que $d = ax' + by'$.

Consideremos $m = \frac{ab}{d}$. Queremos provar que $m = m.m.c\,(a,b)$

Então:

(i) $m = \frac{ab}{d} = \frac{dxb}{d} = xb \Rightarrow b \mid m$

$m = \frac{ab}{d} = \frac{ady}{d} = ay \Rightarrow a \mid m$

(ii) Se $c \in \mathbb{N}$ é tal que $b \mid c$ e $a \mid c$ então existem $u, v \in \mathbb{Z}$ tais que $c = bu$ e $c = av$

Assim:

$$\frac{c}{m} = \frac{c}{\frac{ab}{d}} = \frac{cd}{ab} = \frac{c(ax' + by')}{ab} =$$

$$= \frac{cax'}{ab} + \frac{cby'}{ab} = \frac{cx'}{b} + \frac{cy'}{a} = ux' + vy' \in \mathbb{Z}$$

$$\frac{c}{m} \in \mathbb{Z} \iff m \mid c.$$

Por (i) e (ii) e o lema anterior $m = \dfrac{ab}{m.d.c(a,b)} = m.m.c(a,b)$

$\square$

<u>Corolário</u> Dados $a, b \in \mathbb{N}$, temos que

$$m.m.c(a,b) = ab \iff m.d.c(a,b) = 1$$

<u>Demonst:</u> Imediata do teorema anterior.

$\square$

Números primos

Definição Um inteiro $p>1$ diz-se um número primo se 1 e p forem os únicos divisores de p.

Um inteiro $k>1$ diz-se um número composto se não for um número primo.

Teorema: Sejam $a, b, p \in \mathbb{Z}$. Se p é um número primo e $p \mid ab$, então $p \mid a$ ou $p \mid b$.

Demonst: Seja p um primo tal que $p \mid ab$. Se $p \mid a$, não há nada a mostrar. Se $p \nmid a$ então $m.d.c(a, p) = 1$

Logo pelo Lema de Euclides, $p \mid b$. $\square$

Corolário Sejam $n \in \mathbb{N}$ e $p, a_1, a_2, \dots, a_n \in \mathbb{Z}$. Se p é primo e $p \mid a_1 a_2 \cdots a_n$ então $p \mid a_k$ para algum $k \in \{1, 2, \dots, n\}$.

Corolário Sejam $n \in \mathbb{N}$, $p, q_1, q_2, \dots, q_n \in \mathbb{Z}$ números primos tais que $p \mid q_1 q_2 \cdots q_n$ então $p = q_k$, para algum $k \in \{1, 2, \dots, n\}$.

Teorema (Teorema Fundamental da aritmética)

Todo o número inteiro $n > 1$ se pode escrever como produto de um número finito de primos. Esta representação é única (a menos da ordem dos factores primos).

Demonst: Ver sebenta.

$\square$

Corolário Todo o número inteiro $n > 1$ pode escrever-se, de modo único, como $n = p_1^{k_1} p_2^{k_2} \cdots p_R^{k_R}$ onde para $i \in \{1, \ldots, R\}$, $k_i \in \mathbb{N}$ e p_i é primo e

$$p_1 < p_2 < \cdots < p_R.$$

Proposição Sejam $a = \prod_{i=1}^{k} p_i^{a_i}$ e $b = \prod_{i=1}^{k} p_i^{b_i}$ onde para todo $i \in \{1, \ldots, k\}$, $a_i \geq 0$, $b_i \geq 0$ e p_i é primo.

Para cada $i \in \{1, 2, \ldots, k\}$, sejam $c_i = \min\{a_i, b_i\}$ e $d_i = \max\{a_i, b_i\}$. Então:

$$m.d.c(a,b) = \prod_{i=1}^{k} p_i^{c_i} \quad e \quad m.m.c(a,b) = \prod_{i=1}^{k} p_i^{d_i}.$$

__Demonst:__ Exercício.

$\square$

__Exemplo:__ Consideremos $a = 990$ e $b = 462$.

I) $990 = 2 \times \underline{462} + \underline{66}$

$462 = 7 \times 66 + 0$ $\qquad$ $m.d.c(990, 462) = 66$

$$m.m.c(a, b) = \frac{990 \times 462}{66} = 6930$$

II)

$$\begin{array}{r|l} 990 & 2 \\ 495 & 5 \\ 99 & 3 \\ 33 & 3 \\ 11 & 11 \\ 1 & \end{array} \qquad\qquad \begin{array}{r|l} 462 & 2 \\ 231 & 3 \\ 77 & 7 \\ 11 & 11 \\ 1 & \end{array}$$

$990 = 2 \times 3^2 \times 5 \times 11$ $\qquad$ $462 = 2 \times 3 \times 7 \times 11$

$m.d.c(a, b) = 2 \times 3 \times 11 = 66$ $\qquad$ $m.m.c(a, b) = 2 \times 3^2 \times 5 \times 7 \times 11 = 6930$

Proposição Todo número composto $a \in \mathbb{N}$ tem um divisor primo p tal que $p \leq \sqrt{a}$.

Demonst: Seja $a = a_1 a_2$ com $a_1, a_2 \in \mathbb{N} \setminus \{1\}$ (pois a não é primo). Suponhamos que $a_1 \leq a_2$. Então $a_1^2 \leq a_1 a_2 = a$ logo $a_1 \leq \sqrt{a}$.

Como $a_1 > 1$, pelo TFA (teorema fundamental da aritmética) existe p primo tal que $p \mid a_1$. Logo $p \leq a_1 \leq \sqrt{a}$.

Note-se que $p \mid a_1 \Rightarrow p \mid a$.

$\square$

Exemplo Consideremos 509. Como

$$22^2 = 484 \leq 509 \leq 529 = 23^2$$

Temos que $22 < \sqrt{509} < 23$ $\quad (\sqrt{509} \simeq 22, \ldots)$

Pela proposição anterior os primos que devemos testar são os primos até 22, ou seja, 2, 3, 5, 7, 11, 13, 17 e 19.

Como nenhum destes números divide 509 então podemos concluir que 509 é primo.

<u>Exemplo</u> Consideramos 2093. Como

$$45^2 = 2025 \leq 2093 \leq 46^2 = 2116$$

$(\sqrt{2093} \simeq 45, \ldots)$ então $45 \leq \sqrt{2093} \leq 46$

Consideramos então o números primos até 45: 2, 3, 5, 7, 11, 13, 19, 23, 29, 31, 37, 41 e 43. Verificamos que:

$$2 \nmid 2093, \quad 3 \nmid 2093, \quad 5 \nmid 2093 \quad \text{mas} \quad 7 \mid 2093.$$

Na verdade $2093 = 7 \times 299$

Consideramos 299.

$$17^2 = 289 < 299 < 324 = 18^2$$

Logo $17 < \sqrt{299} < 18$.

Consideramos os primos $2, 3, 5, 7, 11, 13$ e 17.

Temos que $2 \nmid 299$, $3 \nmid 299$, $5 \nmid 299$, $7 \nmid 299$, $11 \nmid 299$

mas $299 = 13 \times 23$

Como 23 é primo então $2093 = 7 \times 13 \times 22$

que é a decomposição em fatores primos de 2093.

Crivo de Eratóstenes

Algoritmo para determinar os números primos inferiores a um dado número natural n.

1º passo: Listam-se os números naturais de 2 até n seguindo a ordem usual

2º passo: eliminam-se sistematicamente todos os números compostos cancelando todos os múltiplos de p com p tal que $p \leq \sqrt{n}$.

3º passo: Os elementos restantes (ie, os números que não passaram no crivo) são os primos inferiores a n.

Exemplo: Determinar todos os primos até 100

$q \leq \sqrt{100} = 10 \qquad q \in \{2, 3, 5, 7\}$

	2	3	~~4~~	5	~~6~~	7	~~8~~	~~9~~	~~10~~
11	~~12~~	13	~~14~~	~~15~~	~~16~~	17	~~18~~	19	~~20~~
~~21~~	~~22~~	23	~~24~~	~~25~~	~~26~~	~~27~~	~~28~~	29	~~30~~
31	~~32~~	~~33~~	~~34~~	~~35~~	~~36~~	37	~~38~~	~~39~~	~~40~~
41	~~42~~	43	~~44~~	~~45~~	~~46~~	47	~~48~~	~~49~~	~~50~~
~~51~~	~~52~~	53	~~54~~	~~55~~	~~56~~	~~57~~	~~58~~	59	~~60~~
61	~~62~~	~~63~~	~~64~~	~~65~~	~~66~~	67	~~68~~	~~69~~	~~70~~
71	~~72~~	73	~~74~~	~~75~~	~~76~~	~~77~~	~~78~~	79	~~80~~
~~81~~	~~82~~	83	~~84~~	~~85~~	~~86~~	~~87~~	~~88~~	89	~~90~~
~~91~~	~~92~~	~~93~~	~~94~~	~~95~~	~~96~~	97	~~98~~	~~99~~	~~100~~

Portanto: os primos p com $p \leq 100$ são: 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97.

Teorema: Existe uma infinidade de primos.

Demonst: Por redução ao absurdo. Suponhamos que existe p primo tal que $2, 3, 5, 7, 11, \ldots, p$ $(*)$ é uma sucessão finita de todos os números primos, ou seja, p é o maior de todos os primos.

Consideramos $s = 2 \times 3 \times 5 \times 7 \times 11 \times \cdots \times p$.

Como $s+1 > 1$ então admite pelo TFA um divisor primo q, ou seja, admite um divisor na lista $(*)$

Temos $q \mid s+1$ e $q \mid s$

Logo $q \mid (s+1) - s$, ou seja, $q \mid 1$. Logo $q = 1$, o que é absurdo. $\square$