

# Teoria de Números

M. Lurdes Teixeira  
Dep. Matemática  
Univ. Minho

2<sup>o</sup> semestre de 2019/2020

## 1 Introdução

## 2 Divisibilidade

- Algoritmo da divisão
- Máximo Divisor Comum
- Algoritmo de Euclides
- Algoritmo de Euclides estendido
- Números primos entre si
- Mínimo Múltiplo Comum

Teoria de Números é uma área da Matemática cujo objetivo é estudar propriedades dos números inteiros relacionadas com a divisibilidade, tais como: paridade, primalidade, fatorização, multiplicatividade, aditividade, etc..

### Aplicações recentes ...

em computação e em tecnologias de informação.

### Áreas atuais de aplicação:

Física, Química, Biologia, Computação, Criptografia, Comunicação Digital, Música, ...

## Temas centrais

- Aritmética Modular
- Primalidade e Fatorização

- Aritmética Modular
- Primalidade e Fatorização



## PROVA

Vamos provar algumas das alíneas do teorema anterior.

Sejam  $a, b, c, d \in \mathbb{Z}$ .

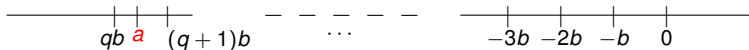
3. Se  $a|b$  e  $b|c$ , então existem  $k_1, k_2 \in \mathbb{Z}$  tais que  $b = a k_1$  e  $c = b k_2$ , pelo que  $c = a k_1 k_2$ .
5. Se  $a|b$  e  $c|d$ , então existem  $k_1, k_2 \in \mathbb{Z}$  tais que  $b = a k_1$  e  $c = d k_2$ , pelo que  $bd = a c k_1 k_2$ , ou seja,  $ac|bd$ .
6. Se  $a|b$  e  $b|a$ , então existem  $k_1, k_2 \in \mathbb{Z}$  tais que  $b = a k_1$  e  $b = a k_2$ , pelo que  $ab = ab k_1 k_2$ , ou seja  $k_1 k_2 = 1$ . Então  $k_1 = k_2 = 1$  ou  $k_1 = k_2 = -1$ .
7. Se  $a|b$  e  $b \neq 0$ , então existe  $k \in \mathbb{Z}$  tal que  $b = a k$  e, como  $|k| \geq 1$ , resulta que  $|b| = |a k| = |a| |k| \geq |a|$ .
8. Se  $a|b$  e  $a|c$ , então existem  $k_1, k_2 \in \mathbb{Z}$  tais que  $b = a k_1$  e  $c = a k_2$ , pelo que  $bx + cy = a k_1 x + a k_2 y = a(k_1 x + k_2 y)$ , pelo que  $a|(bx + cy)$  para quaisquer  $x, y \in \mathbb{Z}$ .

$$a = bq + r.$$

- caso  $a > 0$



- caso  $a < 0$  (notar que  $q < 0$ )



1998, 1999, 2000, 2001, 2002, 2003, 2004, 2005, 2006, 2007, 2008, 2009, 2010, 2011, 2012, 2013, 2014, 2015, 2016, 2017, 2018, 2019, 2020, 2021, 2022, 2023, 2024, 2025, 2026, 2027, 2028, 2029, 2030, 2031, 2032, 2033, 2034, 2035, 2036, 2037, 2038, 2039, 2040, 2041, 2042, 2043, 2044, 2045, 2046, 2047, 2048, 2049, 2050, 2051, 2052, 2053, 2054, 2055, 2056, 2057, 2058, 2059, 2060, 2061, 2062, 2063, 2064, 2065, 2066, 2067, 2068, 2069, 2070, 2071, 2072, 2073, 2074, 2075, 2076, 2077, 2078, 2079, 2080, 2081, 2082, 2083, 2084, 2085, 2086, 2087, 2088, 2089, 2090, 2091, 2092, 2093, 2094, 2095, 2096, 2097, 2098, 2099, 2100, 2101, 2102, 2103, 2104, 2105, 2106, 2107, 2108, 2109, 2110, 2111, 2112, 2113, 2114, 2115, 2116, 2117, 2118, 2119, 2120, 2121, 2122, 2123, 2124, 2125, 2126, 2127, 2128, 2129, 2130, 2131, 2132, 2133, 2134, 2135, 2136, 2137, 2138, 2139, 2140, 2141, 2142, 2143, 2144, 2145, 2146, 2147, 2148, 2149, 2150, 2151, 2152, 2153, 2154, 2155, 2156, 2157, 2158, 2159, 2160, 2161, 2162, 2163, 2164, 2165, 2166, 2167, 2168, 2169, 2170, 2171, 2172, 2173, 2174, 2175, 2176, 2177, 2178, 2179, 2180, 2181, 2182, 2183, 2184, 2185, 2186, 2187, 2188, 2189, 2190, 2191, 2192, 2193, 2194, 2195, 2196, 2197, 2198, 2199, 2200, 2201, 2202, 2203, 2204, 2205, 2206, 2207, 2208, 2209, 2210, 2211, 2212, 2213, 2214, 2215, 2216, 2217, 2218, 2219, 2220, 2221, 2222, 2223, 2224, 2225, 2226, 2227, 2228, 2229, 2230, 2231, 2232, 2233, 2234, 2235, 2236, 2237, 2238, 2239, 2240, 2241, 2242, 2243, 2244, 2245, 2246, 2247, 2248, 2249, 2250, 2251, 2252, 2253, 2254, 2255, 2256, 2257, 2258, 2259, 2260, 2261, 2262, 2263, 2264, 2265, 2266, 2267, 2268, 2269, 2270, 2271, 2272, 2273, 2274, 2275, 2276, 2277, 2278, 2279, 2280, 2281, 2282, 2283, 2284, 2285, 2286, 2287, 2288, 2289, 2290, 2291, 2292, 2293, 2294, 2295, 2296, 2297, 2298, 2299, 2300, 2301, 2302, 2303, 2304, 2305, 2306, 2307, 2308, 2309, 2310, 2311, 2312, 2313, 2314, 2315, 2316, 2317, 2318, 2319, 2320, 2321, 2322, 2323, 2324, 2325, 2326, 2327, 2328, 2329, 2330, 2331, 2332, 2333, 2334, 2335, 2336, 2337, 2338, 2339, 2340, 2341, 2342, 2343, 2344, 2345, 2346, 2347, 2348, 2349, 2350, 2351, 2352, 2353, 2354, 2355, 2356, 2357, 2358, 2359, 2360, 2361, 2362, 2363, 2364, 2365, 2366, 2367, 2368, 2369, 2370, 2371, 2372, 2373, 2374, 2375, 2376, 2377, 2378, 2379, 2380, 2381, 2382, 2383, 2384, 2385, 2386, 2387, 2388, 2389, 2390, 2391, 2392, 2393, 2394, 2395, 2396, 2397, 2398, 2399, 2400, 2401, 2402, 2403, 2404, 2405, 2406, 2407, 2408, 2409, 2410, 2411, 2412, 2413, 2414, 2415, 2416, 2417, 2418, 2419, 2420, 2421, 2422, 2423, 2424, 2425, 2426, 2427, 2428, 2429, 2430, 2431, 2432, 2433, 2434, 2435, 2436, 2437, 2438, 2439, 2440, 2441, 2442, 2443, 2444, 2445, 2446, 2447, 2448, 2449, 2450, 2451, 2452, 2453, 2454, 2455, 2456, 2457, 2458, 2459, 2460, 2461, 2462, 2463, 2464, 2465, 2466, 2467, 2468, 2469, 2470, 2471, 2472, 2473, 2474, 2475, 2476, 2477, 2478, 2479, 2480, 2481, 2482, 2483, 2484, 2485, 2486, 2487, 2488, 2489, 2490, 2491, 2492, 2493, 2494, 2495, 2496, 2497, 2498, 2499, 2500, 2501, 2502, 2503, 2504, 2505, 2506, 2507, 2508, 2509, 2510, 2511, 2512, 2513, 2514, 2515, 2516, 2517, 2518, 2519, 2520, 2521, 2522, 2523, 2524, 2525, 2526, 2527, 2528, 2529, 2530, 2531, 2532, 2533, 2534, 2535, 2536, 2537, 2538, 2539, 2540, 2541, 2542, 2543, 2544, 2545, 2546, 2547, 2548, 2549, 2550, 2551, 2552, 2553, 2554, 2555, 2556, 2557, 2558, 2559, 2560, 2561, 2562, 2563, 2564, 2565, 2566, 2567, 2568, 2569, 2570, 2571, 2572, 2573, 2574, 2575, 2576, 2577, 2578, 2579, 2580, 2581, 2582, 2583, 2584, 2585, 2586, 2587, 2588, 2589, 2590, 2591, 2592, 2593, 2594, 2595, 2596, 2597, 2598, 2599, 2600, 2601, 2602, 2603, 2604, 2605, 2606, 2607, 2608, 2609, 2610, 2611, 2612, 2613, 2614, 2615, 2616, 2617, 2618, 2619, 2620, 2621, 2622, 2623, 2624, 2625, 2626, 2627, 2628, 2629, 2630, 2631, 2632, 2633, 2634, 2635, 2636, 2637, 2638, 2639, 2640, 2641, 2642, 2643, 2644, 2645, 2646, 2647, 2648, 2649, 2650, 2651, 2652, 2653, 2654, 2655, 2656, 2657, 2658, 2659, 2660, 2661, 2662, 2663, 2664, 2665, 2666, 2667, 2668, 2669, 2670, 2671, 2672, 2673, 2674, 2675, 2676, 2677, 2678, 2679, 26

1. *Journal of Management Studies*, 1996, 33, 1, 1-14.

\_\_\_\_\_



## PROVA - continuação

(Unicidade de  $q$  e  $r$ ) Suponhamos que existem  $q, q' \in \mathbb{Z}$  e  $r, r' \in \mathbb{N}_0$  tais que

$$\begin{array}{ll} a = bq + r & \text{e } 0 \leq r < b, \\ a = bq' + r' & \text{e } 0 \leq r' < b. \end{array}$$

Então,

$$bq + r = bq' + r' \implies b|q - q'| = |r' - r| \quad \text{e}$$

$$\left\{ \begin{array}{l} 0 \leq r < b \\ 0 \leq r' < b \end{array} \right\} \implies \left\{ \begin{array}{l} -b < -r \leq 0 \\ 0 \leq r' < b \end{array} \right\} \implies -b < r' - r < b \implies |r' - r| < b$$

Consequentemente,  $b|q - q'| < b$ , o que implica que  $|q - q'| < 1$ . Como  $q - q' \in \mathbb{Z}$ , então  $q - q' = 0$ .

Sendo  $q = q'$  e  $bq + r = bq' + r'$ , então  $r = r'$ .

## Corolário

Dados números inteiros  $a$  e  $b$  com  $b \neq 0$  existem e são únicos os inteiros  $q$  e  $r$  tais que  $0 \leq r < |b|$  e

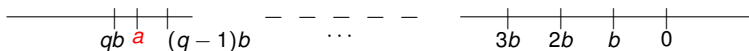
$$a = b \cdot q + r.$$

Graficamente no caso de  $b < 0$ , tem-se:

- caso  $a > 0$  (notar que  $q \leq 0$ )



- caso  $a < 0$  (notar que  $q > 0$ )



## Algoritmo da divisão

## PROVA

Pelo teorema anterior sabemos que existem e são únicos os inteiros  $q'$  e  $r'$  tais que

$$a = |b|q' + r' \text{ e } 0 \leq r' < |b|.$$

Se  $b < 0$ , então

$$a = |b|q' + r' \Leftrightarrow a = -bq' + r' \Leftrightarrow a = b(-q') + r'.$$

Neste caso,  $q = -q'$  e  $r = r'$ .

Se  $b > 0$ , então

$$a = |b|q' + r' \Leftrightarrow a = bq' + r,$$

pelo que  $q = q'$  e  $r = r'$ .

Dados  $a, b \in \mathbb{Z}$  os números  $q$  e  $r$  dados pelo algoritmo da divisão dizem-se, respetivamente, **o quociente** e **o resto** da divisão de  $a$  por  $b$ .

Dividir  $a$  por  $b$  significa calcular o quociente e o resto da divisão de  $a$  por  $b$ .

## EXEMPLO 1

$$a=2 \quad b=6 \quad 2=6 \times 0 + 2 \quad q=0 \quad r=2$$

$$a=2 \quad b=-6 \quad 2=-6 \times 0 + 2 \quad q=0 \quad r=2$$

$$a=-2 \quad b=6 \quad -2=6 \times -1 + 4 \quad q=-1 \quad r=4$$

$$a=-2 \quad b=-6 \quad -2=-6 \times 1 + 4 \quad q=1 \quad r=4$$

$$a=9 \quad b=6 \quad 9=6 \times 1 + 3 \quad q=1 \quad r=3$$

$$a=9 \quad b=-6 \quad 9=-6 \times (-1) + 3 \quad q=-1 \quad r=3$$

$$a=-9 \quad b=6 \quad -9=6 \times (-2) + 3 \quad q=-2 \quad r=3$$

$$a=-9 \quad b=-6 \quad -9=-6 \times 2 + 3 \quad q=2 \quad r=3$$

## Proposição

Sejam  $a, b \in \mathbb{Z}$ . Então  $b \mid a$  sse o resto da divisão de  $a$  por  $b$  é zero.

## PROVA

$$b \mid a \Leftrightarrow \exists_{k \in \mathbb{Z}} a = bk \Leftrightarrow \exists_{k \in \mathbb{Z}} a = bk + 0$$

## Máximo Divisor Comum

Sejam  $a, b \in \mathbb{Z}$  e  $D$  o conjunto dos divisores comuns de  $a$  e  $b$ , i.e.,

$$D = \{d \in \mathbb{Z} \mid d \mid a, d \mid b\}.$$

Como  $1 \mid a$  e  $1 \mid b$ , então  $1 \in D$ . Se  $a = b = 0$ , então  $D = \mathbb{N}$ . Senão, se  $d \in D$ , então  $|d| \leq \max\{|a|, |b|\}$  (pela alínea 6. do teorema anterior), pelo que  $D$  é um conjunto finito não vazio.

## Definição

Dados  $a$  e  $b$  inteiros não ambos nulos, chama-se **máximo divisor comum de  $a$  e  $b$**  ao maior inteiro  $d$  que divide  $a$  e divide  $b$ , o qual se representa por **m.d.c.( $a, b$ )**.

## Proposição

Sejam  $a, b \in \mathbb{Z}$  e  $b \neq 0$ .

- 1 m.d.c.( $a, b$ ) = m.d.c.( $|a|, |b|$ ) = m.d.c.( $b, a$ ).
- 2 se  $b \mid a$ , então m.d.c.( $a, b$ ) =  $|b|$ .
- 3 m.d.c.( $0, b$ ) =  $|b|$ .

## Proposição - Igualdade de Bezout

Sejam  $a$  e  $b$  inteiros, não ambos nulos, e  $d = \text{m.d.c.}(a, b)$ . Então existem  $x, y \in \mathbb{Z}$  tais que  $d = ax + by$ .

### PROVA

Suponhamos que  $a \neq 0$ . Seja

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

Notar que  $S \neq \emptyset$  porque, por exemplo,  $a^2 \in S$  ( $a^2 = a \cdot a + b \cdot 0$ ). Pelo Princípio da Boa Ordenação de  $\mathbb{N}$ ,  $S$  tem elemento mínimo  $m$ . Como  $m \in S$ , existem  $x, y \in \mathbb{Z}$  tais que

$$m = ax + by.$$

$m|a$  Como  $m > 0$ , existem inteiros  $q$  e  $r$  tais que  $a = mq + r$  e  $0 \leq r < m$ . Então,

$$0 \leq r = a - mq = a - (ax + by)q = a(1 - x) + b(-yq).$$

Logo, se  $r > 0$ ,  $r \in S$ , pelo que  $m \leq r$ , o que é impossível. Assim,  $r = 0$ .

Sendo  $r = 0$ ,  $a = mq$  pelo que  $m|a$ .

$m|b$  Análoga à prova anterior de que  $m|a$ .

$m = d$  Como  $m|a$  e  $m|b$ , então  $m \leq \text{m.d.c.}(a, b) = d$ . Como  $d|(ax + by)$ , então  $d \leq m$ .

Logo,  $d = m = ax + by$ .

## Teorema

Sejam  $a$  e  $b$  inteiros não ambos nulos e  $d \in \mathbb{N}$ . Então  $d = \text{m.d.c.}(a, b)$  sse

- 1  $d \mid a$  e  $d \mid b$ ,
- 2 se  $c \in \mathbb{N}$  e  $c \mid a$  e  $c \mid b$ , então  $c \mid d$ .

## PROVA

Seja  $d = \text{m.d.c.}(a, b)$ . Então, por definição,  $d$  verifica a condição 1.

Seja  $c \in \mathbb{N}$  tal que  $c \mid a$  e  $c \mid b$ . Então  $c \mid ax + by$  para quaisquer  $x, y \in \mathbb{Z}$ . Logo  $c \mid d$ .

A prova da implicação recíproca é proposta como exercício.

O resultado deste teorema serve por vezes como definição do m.d.c. de dois inteiros.

## Teorema

Sejam  $a$  e  $b$  inteiros não ambos nulos. Sendo  $c \in \mathbb{N}$ ,

- 1  $\text{m.d.c.}(ac, bc) = c \text{ m.d.c.}(a, b)$ ;
- 2 se  $c \mid a$  e  $c \mid b$ , então  $\text{m.d.c.}\left(\frac{a}{c}, \frac{b}{c}\right) = \frac{1}{c} \text{m.d.c.}(a, b)$ .

## PROVA

Sejam  $a$  e  $b$  inteiros não ambos nulos e  $d = \text{m.d.c.}(a, b)$ .

- 1 Como  $d \mid a$  e  $d \mid b$ , então  $dc \mid ac$  e  $dc \mid bc$ , pelo que,  $dc \mid \text{m.d.c.}(ac, bc)$ .  
Assim,  $\text{m.d.c.}(ac, bc) = kdc$ , para algum  $k \in \mathbb{N}$  e

$$\left. \begin{array}{l} kdc \mid ac \Rightarrow kd \mid a \\ kdc \mid bc \Rightarrow kd \mid b \end{array} \right\} \Rightarrow kd \mid d \Rightarrow k = 1.$$

- 2  $\text{m.d.c.}(a, b) = \text{m.d.c.}\left(c\frac{a}{c}, c\frac{b}{c}\right) = c \times \text{m.d.c.}\left(\frac{a}{c}, \frac{b}{c}\right)$ . Então,

$$\frac{1}{c} \text{m.d.c.}(a, b) = \text{m.d.c.}\left(\frac{a}{c}, \frac{b}{c}\right).$$



## Proposição

Dados  $a$  e  $b$  inteiros, se  $q$  e  $r$  são inteiros tais que  $a = b \cdot q + r$ , então  $\text{m.d.c.}(a, b) = \text{m.d.c.}(b, r)$ .

## PROVA

Seja  $c$  um divisor comum de  $a$  e de  $b$ . Então,

$$c \mid (a - bq).$$

Logo,  $c$  é um divisor comum de  $b$  e de  $r$ .

Reciprocamente, se  $c$  um divisor comum de  $b$  e de  $r$ , então,

$$c \mid (a - bq).$$

Como  $c \mid b$ , conclui-se que  $c \mid a$ . Logo,  $c$  é um divisor comum de  $a$  e de  $b$ .

Em resumo, os divisores comuns de  $a$  e  $b$  são os divisores comuns de  $b$  e  $r$ . Então,  $\text{m.d.c.}(a, b) = \text{m.d.c.}(b, r)$ .

O algoritmo de Euclides tem por objetivo o cálculo do máximo divisor comum de dois inteiros e baseia-se nesta proposição.

## EXEMPLO 2

$$\text{m.d.c.}(486, 218) = ?$$

$$486 = 218 \times 2 + 50$$

$$218 = 50 \times 4 + 18$$

$$50 = 18 \times 2 + 14$$

$$18 = 14 \times 1 + 4$$

$$14 = 4 \times 3 + 2$$

$$4 = 2 \times 2 + 0$$

$$\text{m.d.c.}(486, 218) = \text{m.d.c.}(218, 50)$$

$$= \text{m.d.c.}(50, 18)$$

$$= \text{m.d.c.}(18, 14)$$

$$= \text{m.d.c.}(14, 4)$$

$$= \text{m.d.c.}(4, 2)$$

$$= \text{m.d.c.}(2, 0)$$

$$= 2$$

## Teorema

Sejam  $a$  e  $b$  inteiros tais que  $b \neq 0$ . Aplicando sucessivamente o algoritmo da divisão, o processo termina ao fim de  $n + 2$  ( $n \geq -1$ ) etapas, obtendo-se :

$$\begin{array}{lll}
 a = bq_0 + r_0 & q_0, r_0 \in \mathbb{N}_0 & 0 < r_0 < |b| \\
 b = r_0q_1 + r_1 & q_1, r_1 \in \mathbb{N}_0 & 0 < r_1 < r_0 \\
 r_0 = r_1q_2 + r_2 & q_2, r_2 \in \mathbb{N}_0 & 0 < r_2 < r_1 \\
 \vdots & \vdots & \vdots \\
 r_{n-2} = r_{n-1}q_n + r_n & q_n, r_n \in \mathbb{N}_0 & 0 < r_n < r_{n-1} \\
 r_{n-1} = r_nq_{n+1} + r_{n+1} & q_{n+1}, r_{n+1} \in \mathbb{N}_0 & 0 = r_{n+1} < r_n
 \end{array}$$

em que  $n + 1 \geq 0$ , considerando que  $r_{-1} = b$ . Assim, a sequência dos inteiros da forma  $r_i$  é uma sequência finita:

$$(r_{-1}, r_0, r_1, \dots, r_n, 0),$$

e

$$r_n = \text{m.d.c.}(a, b).$$

## Algoritmo de Euclides

Entrada:  $a$  e  $b$ .

- 1  $x = a, y = b$ .
- 2 Se  $y = 0$ , então  $\text{m.d.c.}(a, b) = x$  e terminar.
- 3  $r \leftarrow$  resto da divisão de  $x$  por  $y$ ,  
 $x \leftarrow y$ ,  
 $y \leftarrow r$ ,  
voltar a 2.

Saída:  $\text{m.d.c.}(a, b)$ .

## Algoritmo de Euclides estendido

O algoritmo de Euclides estendido tem por objetivo o cálculo do m.d.c. de dois inteiros  $a$  e  $b$ , bem como de inteiros  $x$  e  $y$  referidos na igualdade de Bezout.

## EXEMPLO 2- continuação

$$\text{m.d.c.}(486, 218) = 2$$

$$\begin{aligned}
 &\downarrow \qquad \qquad \downarrow \\
 486 &= 218 \times 2 + 50 \rightarrow 2 = -218 \times 11 + \underbrace{(486 - 218 \times 2)}_{= 486 \times 48 + 218 \times (-107)} \times 48 \\
 218 &= 50 \times 4 + 18 \rightarrow 2 = 50 \times 4 - \underbrace{(218 - 50 \times 4)}_{= 486 \times 48 + 218 \times (-107)} \times 11 = -218 \times 11 + 50 \times 48 \\
 50 &= 18 \times 2 + 14 \rightarrow 2 = -18 \times 3 + \underbrace{(50 - 18 \times 2)}_{= 486 \times 48 + 218 \times (-107)} \times 4 = 50 \times 4 - 18 \times 11 \\
 18 &= 14 \times 1 + 4 \rightarrow 2 = 14 - \underbrace{(18 - 14 \times 1)}_{= 486 \times 48 + 218 \times (-107)} \times 3 = -18 \times 3 + 14 \times 4 \\
 14 &= 4 \times 3 + 2 \rightarrow 2 = 14 - 4 \times 3 \\
 4 &= 2 \times 2 + 0
 \end{aligned}$$

$$x = 48$$

$$y = -107$$

### EXEMPLO 3

Considere-se a equação linear  $486x + 218y = 2$  nas incógnitas  $x$  e  $y$ .

Existem soluções inteiras para esta equação? Pelo exposto anteriormente, existe pelo menos uma solução que é

$$x = 48 \text{ e } y = -107.$$

Em geral, qualquer par do tipo

$$\left( 48 + k \frac{218}{2}, -107 - k \frac{486}{2} \right)$$

com  $k \in \mathbb{Z}$ , é solução da equação, porque

$$486 \left( 48 + k \frac{218}{2} \right) + 218 \left( -107 - k \frac{486}{2} \right) = 2$$

$$\Leftrightarrow 486 \times 48 + 486 \times k \frac{218}{2} - 218 \times 107 - 218 \times k \frac{486}{2} = 2$$

$$\Leftrightarrow (486 \times 48 - 218 \times 107) + \left( 486 \times k \frac{218}{2} - 218 \times k \frac{486}{2} \right) = 2$$

$$\Leftrightarrow 2 + 0 = 2$$

### Definição

Dois inteiros  $a$  e  $b$  não ambos nulos, dizem-se **primos entre si** se  $\text{m.d.c.}(a, b) = 1$ .

### Teorema

Dados  $a$  e  $b$  inteiros não ambos nulos, então  $a$  e  $b$  são primos entre si sse existem inteiros  $x$  e  $y$  tais que  $1 = ax + by$ .

### Proposição

Dados  $a$  e  $b$  inteiros não ambos nulos, se  $d = \text{m.d.c.}(a, b)$ , então  $\frac{a}{d}$  e  $\frac{b}{d}$  são primos entre si.

### Proposição

Sejam  $a$  e  $b$  são inteiros primos entre si. Se  $c \in \mathbb{Z}$  é tal que  $a \mid c$  e  $b \mid c$ , então  $ab \mid c$ .

### Lema de Euclides

Sejam  $a$  e  $b$  inteiros primos entre si. Se  $c \in \mathbb{Z}$  é tal que  $a \mid bc$ , então  $a \mid c$ .

#### PROVA

Se  $a$  e  $b$  são inteiros primos entre si, então, existem  $x, y \in \mathbb{Z}$  tais que  $1 = ax + by$ . Assim,

$$c = acx + bcy.$$

Como  $a \mid ac$  e  $a \mid bc$ , então  $a \mid (acx + bcy)$ , ou seja,  $a \mid c$ .

#### EXEMPLO 4

- $15 \mid (2 \times 45)$  e  $15 \mid 45$ .
- $15 \mid 9 \times 10$  mas  $15 \nmid 9$  e  $15 \nmid 10$ .



## Proposição

Sejam  $a, b, c \in \mathbb{Z} \setminus \{0\}$ . Então  $\text{m.d.c.}(a, c) = \text{m.d.c.}(b, c) = 1$  sse  $\text{m.d.c.}(ab, c) = 1$ .

## PROVA

Resumidamente,

- $$\left. \begin{array}{l} \text{m.d.c.}(a, c) = 1 \Rightarrow 1 = ax + cy \\ \text{m.d.c.}(b, c) = 1 \Rightarrow 1 = bx' + cy' \end{array} \right\}$$

$$\Rightarrow 1 = (ax + cy)(bx' + cy') = ab(xx') + c(axy' + bx'y + cyy')$$

$$\Rightarrow \text{m.d.c.}(ab, c) = 1$$
- $$\text{m.d.c.}(ab, c) = 1 \Rightarrow 1 = abx + cy \Rightarrow \begin{cases} 1 = a(bx) + cy \Rightarrow \text{m.d.c.}(a, c) = 1 \\ 1 = b(ax) + cy \Rightarrow \text{m.d.c.}(b, c) = 1 \end{cases}$$

Dados  $a$  e  $b$  inteiros não nulos, o conjunto dos inteiros positivos múltiplos de  $a$  e  $b$  é

$$M = \{x \in \mathbb{N} : a|x, b|x\}$$

Notar que  $M$  é um subconjunto de  $\mathbb{N}$  não vazio, pois  $|ab| \in M$ .

Então, pelo Princípio de Boa Ordenação de  $\mathbb{N}$ ,  $M$  tem elemento mínimo.

### Definição

Dados  $a$  e  $b$  inteiros não nulos, chama-se **mínimo múltiplo comum de  $a$  e  $b$**  ao menor inteiro positivo que é divisível por  $a$  e por  $b$ .

O mínimo múltiplo comum de  $a$  e  $b$  representa-se por **m.m.c.( $a, b$ )**.

## Proposição

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

- ①  $\text{m.m.c.}(a, b) = \text{m.m.c.}(|a|, |b|) = \text{m.m.c.}(b, a)$ .
- ②  $\text{m.m.c.}(a, a) = |a|$ .
- ③ se  $b \mid a$ , então  $\text{m.m.c.}(a, b) = |a|$ .
- ④  $\text{m.d.c.}(a, b) \mid \text{m.m.c.}(a, b)$ .
- ⑤  $\text{m.m.c.}(ka, kb) = |k| \text{m.m.c.}(a, b)$  para qualquer  $k \in \mathbb{Z} \setminus \{0\}$ .

## Teorema

Sejam  $a, b \in \mathbb{Z} \setminus \{0\}$ . Então,  $m = \text{m.m.c.}(a, b)$  sse

- ①  $a \mid m$  e  $b \mid m$ ,
- ② se  $c \in \mathbb{N}$  e  $a \mid c$  e  $b \mid c$ , então  $m \mid c$ .

## PROVA

Seja  $m = \text{m.m.c.}(a, b)$ . Pela definição de mínimo múltiplo comum, a condição 1. é válida.

Pelo algoritmo da divisão, existem inteiros  $q$  e  $r$ , com  $0 \leq r < m$ , tais que

$$c = mq + r.$$

Como  $a \mid m$ ,  $a \mid c$  e  $b \mid m$ ,  $b \mid c$ , então  $a \mid r$  e  $b \mid r$ , respetivamente. Consequentemente,  $r = 0$  ou  $m = \text{m.m.c.}(a, b) \leq r$ . Logo  $r = 0$  e  $m \mid c$ .

Reciprocamente, a condição 1. implica que  $m$  é um múltiplo comum de  $a$  e  $b$ , e a condição 2. implica que  $m \leq c$ , para qualquer múltiplo comum de  $a$  e  $b$ .

O resultado deste teorema serve por vezes como definição do m.m.c. de dois inteiros.

## Teorema

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

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

**PROVA** Sem perda de generalidade, suponhamos que  $a, b > 0$ .

● **Caso  $\text{m.d.c.}(a, b) = 1$**

Como  $ab$  é múltiplo de  $a$  e  $b$ , então  $m \mid ab$ , pelo teorema anterior. Mas, se  $\text{m.d.c.}(a, b) = 1$ ,  $a \mid m$  e  $b \mid m$ , então  $ab \mid m$ . Logo  $m = ab = \frac{|ab|}{\text{m.d.c.}(a, b)}$ .

● **Caso  $\text{m.d.c.}(a, b) = d \in \mathbb{N}$**

Sabemos que  $\text{m.d.c.}(\frac{a}{d}, \frac{b}{d}) = 1$ , o que implica que  $\text{m.m.c.}(\frac{a}{d}, \frac{b}{d}) = \frac{(\frac{a}{d} \cdot \frac{b}{d})}{\text{m.d.c.}(\frac{a}{d}, \frac{b}{d})}$ .

Por outro lado,  $\text{m.m.c.}(a, b) = d \text{ m.m.c.}(\frac{a}{d}, \frac{b}{d})$ , donde se conclui que

$$\text{m.m.c.}(a, b) = d \frac{\left| \frac{a}{d} \cdot \frac{b}{d} \right|}{1} = d \frac{|ab|}{d^2} = \frac{|ab|}{d} = \frac{|ab|}{\text{m.d.c.}(a, b)}.$$