

Mínimo múltiplo comum

Dados dois números inteiros não nulos a e b , denotamos por

$$\text{mmc}\{a, b\}$$

o seu **mínimo múltiplo comum**.

Teorema 1.3.4: (Existência e unicidade do mmc)

Dados dois números inteiros não nulos a e b , existe um único número natural m (designado por **mínimo múltiplo comum** de a e b) tal que:

- ① $a|m$ e $b|m$; (m é múltiplo de a e b)
- ② Se $c \in \mathbb{Z}$ é tal que $a|c$ e $b|c$ então $m|c$. (m é o menor múltiplo de a e b , positivo)

Exemplos:

- $mmc\{6, 9\} = 18 = mmc\{-6, 9\}$
- $mmc\{32, 60\} = ?$

Decompor em factores Primos

$$\begin{array}{r|l} 32 & 2 \leftarrow \\ 16 & 2 \leftarrow \\ 8 & 2 \\ 4 & 2 \\ 2 & 2 \\ 1 & \end{array}$$

$$32 = 2^5$$

$$\begin{array}{r|l} 60 & 2 \leftarrow \\ 30 & 2 \leftarrow \\ 15 & 3 \\ 5 & 5 \\ 1 & \end{array}$$

$$60 = 5 \times 3 \times 2^2$$

$$mmc\{32, 60\} = 5 \times 3 \times 2^5$$
$$= 480$$

(Factores diferentes
e
Factores comuns
com maior grau)

Recordar:

$$mdc\{32, 60\} = 2 \times 2 = 4 \quad (\text{Factores comuns com menor grau})$$

- $\text{mmc}\{32060, 31652\} = ?$

Decompôr em factores Primos

32060		2	
16030		2	
8015		5	
1603		7	!!!!!!
229		?	

- $mmc\{32060, 31652\} = ?$

Decompor em factores Primos

$$\begin{array}{r|l}
 32060 & 2 \\
 16030 & 2 \\
 8015 & 5 \\
 1603 & 7 \\
 229 & 229 \\
 1 &
 \end{array}$$

$$32060 = 229 \times 5 \times 7 \times 2^2$$

$$\begin{array}{r|l}
 31652 & 2 \\
 15826 & 2 \\
 7913 & 41 \\
 193 & 193 \\
 1 &
 \end{array}$$

$$31652 = 193 \times 41 \times 2^2$$

$$\begin{aligned}
 mmc\{32060, 31652\} &= \\
 &= 229 \times 5 \times 7 \times 193 \times 41 \times 2^2 \\
 &= 253690780.
 \end{aligned}$$

Teorema 1.3.5: *Dados dois inteiros não nulos a e b , então*

$$\text{mmc}\{a, b\} = \frac{|ab|}{\text{mdc}\{a, b\}}.$$

● $\text{mmc}\{32060, 31652\} = ?$

Recorrendo ao algoritmo de Euclides

$$32060 = 31652 \times 1 + 408$$

$$31652 = 408 \times 77 + 236$$

$$408 = 236 \times 1 + 172$$

$$236 = 172 \times 1 + 64$$

$$172 = 64 \times 2 + 44$$

$$64 = 44 \times 1 + 20$$

$$44 = 20 \times 2 + 4$$

$$20 = 4 \times 5 + 0,$$

$$\text{mmc}\{32060, 31652\} =$$

$$= \frac{32060 \times 31652}{4}$$

$$= 253690780.$$

- $mmc\{32060, 31652\} = ?$

32060	2		31652	2	
16030	2		15826	2	
8015	5		7913	41	$31652 = 193 \times 41 \times 2^2$
1603	7		193	193	
229	229		1		
1					



$32060 = 229 \times 5 \times 7 \times 2^2$



$31652 = 193 \times 41 \times 2^2$

$mdc\{32060, 31652\} = 2^2$

$$\begin{aligned}
 \frac{32060 \times 31652}{4} &= \frac{(229 \times 5 \times 7 \times 2^2)(193 \times 41 \times 2^2)}{4} \\
 &= 229 \times 5 \times 7 \times 193 \times 41 \times 2^2 = mmc\{32060, 31652\}
 \end{aligned}$$

Definição 1.3.6:

- ① Um número inteiro p diz-se *primo* se $p > 1$ e p apenas possui como divisores positivos 1 e p .
- ② Dois números inteiros não nulos a e b dizem-se *primos entre si* se

$$\text{mdc}\{a, b\} = 1.$$

Curiosidades:

- Estudados, desde a antiguidade. Nomeadamente, quanto à procura de uma regularidade ou lei de formação destes números. Mas, passado milénios, os matemáticos ainda não a descobriram. Um facto que está provado é que *são em número infinito* (Euclides, no século III a.c.).
- No século III antes da nossa era, o matemático grego *Eratóstenes* “inventou” um método, ainda actual, que permite determinar os números primos inferiores a um dado número. A este método dá-se o nome de *Crivo de Eratóstenes*.

- No século III antes da nossa era, o matemático grego Eratóstenes inventou um método, ainda actual, que permite determinar os números primos inferiores a um dado número. A este método dá-se o nome de **Crivo de Eratóstenes**.

Números primos inferiores a 100

1	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

Definição 1.3.6:

- ① Um número inteiro p diz-se *primo* se $p > 1$ e p apenas possui como divisores positivos 1 e p .
- ② Dois números inteiros não nulos a e b dizem-se *primos entre si* se
$$\text{mdc}\{a, b\} = 1.$$

Observações:

- (0) 0 e 1 não são primos;
- (1) O número 2 é o único primo que é par;
- (2) Se $a|b$ e $a|c$ então $a|(b+c)$;
- (3) Se $a|b$ então $a|(kb)$, com k inteiro;
- (4) Se a é primo e $a \nmid b$ então $\text{mdc}\{a, b\} = 1$.

Lema

Sejam a e b dois números inteiros não nulos e primos entre si. Seja $c \in \mathbb{Z}$ tal que $a|bc$. Então $a|c$.

Demonstração. Atendendo à Igualdade de Bezout, existem inteiros m e n tais que

$$1 = am + bn.$$

Donde $c = amc + bnc$. Como $a|bc$, então em particular $a|bnc$. Além disso, claramente, $a|amc$. Logo $a|(amc + bnc)$, ou seja, $a|c$. □

Lema

Seja p um número primo e sejam $a_1, a_2, \dots, a_n \in \mathbb{Z}$ (com $n \in \mathbb{N}^*$) tais que $p|a_1a_2 \cdots a_n$. Então $p|a_i$, para algum $i \in \{1, \dots, n\}$.

Demonstração. Por indução em n . Para $n = 1$ é imediato. Admitamos então o resultado válido para $n - 1$, para certo $n > 1$. Sejam $a_1, a_2, \dots, a_n \in \mathbb{Z}$ tais que $p|a_1a_2 \cdots a_n$. Ora, se $p|a_1a_2 \cdots a_{n-1}$, por hipótese de indução, $p|a_i$, para algum $i \in \{1, \dots, n - 1\}$. Se, pelo contrário $p \nmid a_1a_2 \cdots a_{n-1}$, então

$$\text{mdc}\{p, a_1a_2 \cdots a_{n-1}\} = 1,$$

visto que p é um número primo. Neste caso, pelo lema anterior, deduzimos que $p|a_n$. □

Teorema 1.3.7: (Teorema Fundamental da Aritmética)

Todo o número inteiro maior do que um pode ser escrito como um produto de números primos (com um só factor, no caso do número ser primo). Além disso, uma tal decomposição em números primos é essencialmente única, i.e. duas decomposições apenas diferem na ordem pela qual os primos são escritos.

$$n = p_1^{r_1} p_2^{r_2} \cdots p_k^{r_k}, \quad p_1, p_2, \dots, p_k \text{ são números primos}$$

Exemplo: Escrever $n=51975$ como o produto de números primos.

Decompor em factores primos

51975	3
17325	3
5775	5
1155	3
385	5
77	11
7	7
1	



$$51975 = 3 \times 3 \times 3 \times 5 \times 5 \times 11 \times 7$$

$$= 3^3 \cdot 5^2 \cdot 11 \cdot 7 = 5^2 \cdot 3^3 \cdot 7 \cdot 11$$

$$= 3^3 \cdot 5^2 \cdot 7 \cdot 11$$

forma standard de n
(Base crescente)