# 1 Conceitos Fundamentais

## 1.1 Divisão Euclidiana

Sejam $a, b \in \mathbb{Z}$ com $b \neq 0$, a divisão euclidiana de $a$ por $b$ consiste na identidade

$$a = b \cdot q + r \qquad q, r \in \mathbb{Z} \ \wedge \ 0 \leq r < b$$

## 1.2 Divisibilidade

Sejam $a, b \in \mathbb{Z}$ com $b \neq 0$, dizemos que $b$ divide $a$, denotando $b \mid a$, se

$$\exists\, c \in \mathbb{Z} : \ \ a = b \cdot c$$

Propriedades:

- $\forall\, a \in \mathbb{Z} : \ \ a \mid 0$
- $\forall\, a \in \mathbb{Z} : \ \ \pm 1 \mid a$
- $\forall\, a \in \mathbb{Z} : \ \ \pm a \mid a$
- $\forall\, c \in \mathbb{Z} : \ \ a \mid b \implies ac \mid bc$
- $\forall\, x, y \in \mathbb{Z} : \ \ a \mid b \ \wedge \ a \mid c \implies a \mid (bx + cy)$
- $\forall\, a, b \in \mathbb{Z} : \ \ a \mid b \ \wedge \ b \mid a \implies b = \pm a$

## 1.3 Máximo Divisor Comum

Sejam $a, b \in \mathbb{Z}$ com $(a, b) \neq (0, 0)$, o máximo divisor comum de $a$ e $b$ é um inteiro $d$ tal que

$$d \mid a \ \wedge \ d \mid b$$

$$\forall\, d' : \ \ d' \mid a \ \wedge \ d' \mid b \implies d' \mid d$$

Lema: Sejam $a, b \in \mathbb{Z}$ com $(a, b) \neq (0, 0)$, e $q, r \in \mathbb{Z}$ com $a = b \cdot q + r$.
O $\text{mdc}(a, b)$, se existe, é igual a $\text{mdc}(b, r)$.

Identidade de Bézout: Sejam $a, b \in \mathbb{Z}$ com $(a, b) \neq (0, 0)$, então

$$\exists\, \alpha, \beta \in \mathbb{Z} : \ \ \alpha \cdot a + \beta \cdot b = \text{mdc}(a, b)$$

Lema de Euclides: Sejam $a, b, c \in \mathbb{Z}$ com $a, b, c \neq 0$. Se $a|bc$ e $\text{mdc}(a, b) = 1$, então $a|c$.

Propriedades: Sejam $a, b, c \in \mathbb{Z}$ com $a, b, c \neq 0$

- $\text{mdc}(a, c) = \text{mdc}(b, c) \iff \text{mdc}(ab, c) = 1$
- $\text{mdc}(a, b) = d \iff \text{mdc}\left(\dfrac{a}{d}, \dfrac{b}{d}\right) = 1$
- $a \mid c \ \wedge \ b \mid c \implies \left(\dfrac{ab}{\text{mdc}(a, b)}\right) \Bigg| \, c$
- $(a \mid c \ \wedge \ b \mid c \ \wedge \ \text{mdc}(a, b) = 1) \implies ab \mid c$

## 1.4 Mínimo Multiplo Comum

Sejam $a, b \in \mathbb{Z}$ com $(a, b) \neq (0, 0)$, o mínimo multiplo comum de $a$ e $b$ é um inteiro $m$ tal que

$$a \mid m \ \wedge \ b \mid m$$

$$\forall\, m' : \ \ a \mid m' \ \wedge \ b \mid m' \implies m \mid m'$$

Teorema: $\forall\, a, b \in \mathbb{Z}, (a, b) \neq (0, 0) : \ \ \text{mmc}(a, b) = \dfrac{ab}{\text{mdc}(a, b)}$

## 1.5 Números Primos

Um número $p$ é primo se os únicos divisores de $p$ são $\pm 1$ e $\pm p$.

Lema: Seja $p \in \mathbb{Z}$ primo, e $x_1, \ldots, x_n \in \mathbb{Z}$.
Se $p \mid (x_1 \cdot \ldots \cdot x_n)$, então $p \mid x_i$ para ao menos algum $i \in [1, n] \subset \mathbb{Z}$.

Teorema: Qualquer número natural $n \geq 2$ é produto de um conjunto único e finito de números primos.

Corolário: Seja $a \in \mathbb{Z}$ com $a \neq 0, \pm 1$.
Sejam $p_1, \ldots, p_n \in \mathbb{Z}$ primos.
Sejam $h_1, \ldots, h_n \in \mathbb{Z}$ maiores que 0.
$a$ pode ser escrito como $a = \pm \left( p_1^{h_1} \cdot \ldots \cdot p_n^{h_n} \right)$

Corolário: Seja $a, b \in \mathbb{Z}$ com $a$ e $b \neq 0, \pm 1$.
Sejam $\forall\, i : h_i, k_i \geq 0$, e $p_1, \ldots, p_n \in \mathbb{Z}$ primos tais que
$a = \pm \ p_1^{h_1} \cdot \ldots \cdot p_n^{h_n}$
$b = \pm \ p_1^{k_1} \cdot \ldots \cdot p_n^{k_n}$
Então:

- $\text{mdc}(a, b) = p_1^{d_1} \cdot \ldots \cdot p_n^{d_n}$, onde $d_i = \min(h_i, k_i)$
- $\text{mmc}(a, b) = p_1^{d_1} \cdot \ldots \cdot p_n^{d_n}$, onde $d_i = \max(h_i, k_i)$

Teorema: Há um número infinito de números primos.

Corolário: Seja $p \in \mathbb{Z}$ primo com $p > 0$, então $\sqrt{p} \in \mathbb{Q}$.

## 1.6 Fatoração

Lema: Seja $n = ab \in \mathbb{Z}$ com $n \neq 0, \pm 1$, então $a \leq \lfloor \sqrt{n} \rfloor \ \vee \ b \leq \lfloor \sqrt{n} \rfloor$.