

1 Teoria dos Números

Propriedades dos números inteiros \mathbb{Z} com respeito às operações elementares.

Equação diofantina: Equação polinomial que permite a duas ou mais variáveis assumirem apenas valores inteiros.

2 Conceitos Fundamentais

2.1 Divisão Euclidiana

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

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

2.2 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:

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

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

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

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

2.4 Mínimo Múltiplo Comum

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

$$\begin{aligned} a \mid m \wedge b \mid m \\ \forall m' : a \mid m' \wedge b \mid m' \implies m \mid m' \end{aligned}$$

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

2.5 Números Primos

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

Lema: Seja $p \in \mathbb{Z}$ primo, e $x_1, \dots, x_n \in \mathbb{Z}$.

Se $p \mid (x_1 \cdot \dots \cdot x_n)$, 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 $n \in \mathbb{Z}$ com $n \neq 0, \pm 1$.

Sejam $p_1, \dots, p_n \in \mathbb{Z}$ primos.

Sejam $h_1, \dots, h_n \in \mathbb{Z}$ maiores que 0.

n pode ser escrito como $n = \pm \left(p_1^{h_1} + \dots + p_n^{h_n} \right)$