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 Algoritmos 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

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

2.2 Divisibilidade

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

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

Propriedades:

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

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

$$d \,|\, a \ \wedge \ d \,|\, b$$

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

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 $\mathrm{mdc}(a, b)$, se existe, é igual a $\mathrm{mdc}(b, r)$.

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

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

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

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

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

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