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

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

<u>Lema</u>: 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 $\text{mdc}(b, r)$.

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

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

<u>Lema de Euclides</u>: 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 $a, b, c \neq 0$

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

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

1.5 Fatoração

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

1.6 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 $x_1, \ldots, x_n \in \mathbb{Z}$.
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:

- $\mathrm{mdc}(a, b) = p_1^{d_1} \cdot \ldots \cdot p_n^{d_n}$, onde $d_i = \min(h_i, k_i)$
- $\mathrm{mmc}(a, b) = p_1^{d_1} \cdot \ldots \cdot p_n^{d_n}$, 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 $\sqrt{p} \in \mathbb{Q}$.

Teorema: Não há forma polinomial que gere apenas números primos.

Teorema: Sejam $a, b \in \mathbb{N}^+$ com $\mathrm{mdc}(a, b) = 1$, então a sequência $(an + b)_{n=0}^{\infty}$ contém infinitos primos.

A função para o número de primos menores que $x \in \mathbb{R}$ é

$$\pi(x) \sim \frac{x}{\ln x}$$

1.6.1 Números de Fermat

Os números de Fermat são dados pela função

$$F : \mathbb{N}^+ \to \mathbb{N}^+$$
$$F(n) = 2^{2^n} + 1$$

Teorema: Nem todos números de Fermat são primos.

Teorema: Seja $a \geq 2 \in \mathbb{Z}$ e $a^2 + 1$ primo. Então a é par e $n = 2^m$.

Teorema: $\forall\, k \in \mathbb{Z}, n \in \mathbb{N}^+ : \text{mdc}(F(n), F(n+k)) = 1$.
Ou seja, todos números de Fermat são co-primos entre si.

Corolário: Como $F(1), \ldots, F(n)$ são co-primos, entre seus fatores há ao menos n números primos distintos.

1.6.2 Números de Mersenne

Os números de Mersenne são dados pela função

$$M : \mathbb{P} \to \mathbb{N}^+$$
$$M(p) = 2^p - 1$$

Teorema: Nem todos números de Mersenne são primos.

Teorema: Seja $a \in \mathbb{Z}$ com $a \geq 1$. Então $a^n - 1$ é primo se e somente se $a = 2$ e n é primo.

2 Congruências

2.1 Relações de Equivalência

Uma relação sobre um conjunto A é um subconjunto $R \subset A \times A$.
Dizemos que aRb se $(a, b) \in R$.

Uma relação pode ter as seguintes propriedades:

- Reflexividade: se $\forall\, a \in A : aRa$.
- Simetria: se $\forall\, a, b \in A : aRb \implies bRa$.
- Transitividade: $\forall\, a, b, c \in A : aRb \wedge bRc \implies aRc$.
- Antissimetria: se $\forall\, a, b \in A : aRb \wedge bRa \implies a = b$.
- Totalidade: se $\forall\, a, b \in A : aRb \oplus bRa$.

Definição: Uma relação R sobre A é de equivalência se ela é reflexiva, simétrica e transitiva.

2.2 Classes de Equivalência

Seja $a \in A$ e R uma relação de equivalência sobre A. Definimos a classe de equivalência de a como

$$[a]_R := \{x \in A \mid aRx\} = \{x \in A \mid xRa\}$$

Propriedades:

- $\forall\, a \in A : a \in [a]_R$
- $[a]_R = [b]_R \iff aRb$
- $[a]_R \cap [b]_R = \varnothing \iff a\not R b$
- As classes de equivalência de um conjunto formam uma partição deste: $\forall\, A : A = \bigsqcup\limits_{a \in A} [a]_R$

Seja R uma relação de equivalência sobre A. Denotamos o conjunto das classes de equivalência de R

$$A_{/R} := \{[a]_R \mid a \in A\}$$

2.3 Congruência

Seja $m \in \mathbb{Z}$ com $m > 1$. Dizemos que a é congruente b módulo m se $m \mid (a - b)$. Denota-se

$$a \equiv_m b$$

Teorema: Para qualquer $m > 1$, $\equiv_m$ forma uma relação de equivalência sobre $\mathbb{Z}$.

- $\forall\, a \in \mathbb{Z} : a \equiv_m a$.
- $\forall\, a, b \in \mathbb{Z} : a \equiv_m b \implies b \equiv_m a$.
- $\forall\, a, b, c \in \mathbb{Z} : a \equiv_m b \land b \equiv_m c \implies a \equiv_m c$.

Propriedades:

- $a \equiv_m 0 \iff m \mid a$.
- $a \equiv_m b \iff -a \equiv_m -b$.
- $a \equiv_m b \,\land\, a' \equiv_m b' \implies (a + a') \equiv_m (b + b')$.
- $a \equiv_m b \,\land\, a' \equiv_m b' \implies (a \cdot a') \equiv_m (b \cdot b')$.
- $\forall\, k \neq 0 \in \mathbb{Z} : a \equiv_m b \iff ka \equiv_m kb$.

Teorema: Seja $m \in \mathbb{Z}$ com $m > 1$. Então $\mathbb{Z}_{/m} = \{[0]_m, [1]_m, \dots [m-1]_m\}$
Portanto, $\left|\mathbb{Z}_{/m}\right| = m$.

Corolário: Seja $p(x)$ um polinômio com coeficientes inteiros. Então $a \equiv_m b \implies p(a) \equiv_m p(b)$.

2.3.1 Inverso Aritmético

Sejam $a, n \in \mathbb{Z}$. O inverso mod n de a é um número a' tal que

$$a \cdot a' \equiv_n 1$$

Teorema: O inverso de a existe se e somente se $\mathrm{mdc}(a, n) = 1$.

2.3.2 Equações Lineares de Congruência

Sejam $a, b, n \in \mathbb{Z}$ com $n \neq 0$. Uma equação linear de congruência é da forma

$$ax \equiv_n b$$

Duas equações lineares de congruência são equivalentes se o conjunto solução de ambas é o mesmo.

Teorema: Uma equação linear de congruência $ax \equiv_n b$ possui solução inteira se e somente se

$$\text{mdc}(a, n) \mid b$$

Se a equação possui uma ou mais soluções inteiras, e seja $d = \text{mdc}(a, n)$.
Então, esta equação é equivalente à equação reduzida

$$\frac{a}{d} \cdot x \equiv_{\frac{n}{d}} \frac{b}{d}$$

Seja $ax \equiv_n b$ uma equação de congruência reduzida ($\text{mdc}(a, n) = 1$).
Seja a' um inverso aritmético mod n de a.
Então, a equação é equivalente a

$$x \equiv_n a \cdot a'$$

3 Resíduo

Seja $n \in \mathbb{N}^*$ e $a \in \mathbb{Z}$. O resíduo r de a mod n é o resto da divisão euclidiana de a por n.

$$r \equiv_n a$$

Portanto, o resíduo é único e mínimo.