Aritmética modular, Euler e RSA

Carlos Florentino[1,2]

[1]Departmento de Mathemática, FCUL,
[2]CMAFcIO e GFM Univ. de Lisboa,
(Não se usa o AO 90)

Notas de Matemática Discreta / Finita

Outline

Outline

Conjuntos - Linguagem/Terminologia

- $A = \{a, b, c, \cdots\}$, conjunto definido por extensão, $a \in A$
- $B = \{n \in \mathbb{Z} \mid n^2 > 24\}$, subconjunto definido por propriedade. Temos $4 \notin B$, $B \subset \mathbb{Z}$.
- Se C é subconjunto de D, escreve-se $C \subset D$ (podem ser iguais)

Conjuntos - Linguagem/Terminologia

- $A = \{a, b, c, \cdots\}$, conjunto definido por extensão, $a \in A$
- $B = \{n \in \mathbb{Z} \mid n^2 > 24\}$, subconjunto definido por propriedade. Temos $4 \notin B$, $B \subset \mathbb{Z}$.
- Se C é subconjunto de D, escreve-se $C \subset D$ (podem ser iguais)

Conjuntos fundamentais:

- **Naturais** $\mathbb{N} = \{1, 2, 3, \cdots\}$, $\quad \mathbb{N}_0 = \{0, 1, 2, 3, \cdots\} = \mathbb{N} \cup \{0\}$
- **Inteiros** $\mathbb{Z} = \{\cdots, -2, -1, 0, 1, 2, 3, \cdots\}$
- **Racionais** $\mathbb{Q} = \{\frac{a}{b} \mid a \in \mathbb{Z},\ b \in \mathbb{N}\}$
- **Reais** $\mathbb{R}$, **Complexos** $\mathbb{C}$, etc.

Conjuntos - Linguagem/Terminologia

- $A = \{a, b, c, \cdots\}$, conjunto definido por extensão, $a \in A$
- $B = \{n \in \mathbb{Z} \mid n^2 > 24\}$, subconjunto definido por propriedade. Temos $4 \notin B$, $B \subset \mathbb{Z}$.
- Se C é subconjunto de D, escreve-se $C \subset D$ (podem ser iguais)

Conjuntos fundamentais:

- **Naturais** $\mathbb{N} = \{1, 2, 3, \cdots\}$, $\quad \mathbb{N}_0 = \{0, 1, 2, 3, \cdots\} = \mathbb{N} \cup \{0\}$
- **Inteiros** $\mathbb{Z} = \{\cdots, -2, -1, 0, 1, 2, 3, \cdots\}$
- **Racionais** $\mathbb{Q} = \{\frac{a}{b} \mid a \in \mathbb{Z},\ b \in \mathbb{N}\}$
- **Reais** $\mathbb{R}$, **Complexos** $\mathbb{C}$, etc.

Operações com conjuntos:

- **União** $A \cup B = \{x \mid x \in A \text{ ou } x \in B\}$
- **Intersecção** $A \cap B = \{x \mid x \in A \text{ e } x \in B\}$
- **Complemento** como subconjunto de U, $A^c = U \setminus A$
- **Diferença** $A \setminus B = \{x \in A \mid x \notin B\}$;
- **Diferença simétrica** $A \triangle B := (A \setminus B) \cup (B \setminus A)$
- **União disjunta** $A \sqcup B := A \cup B$, sempre que $A \cap B = \varnothing$
- **Produto (cartesiano)** $A \times B = \{(a, b) \mid a \in A,\ b \in B\}$

Cardinal

O cardinal $|X|$ de um conjunto finito X é o número de elementos.

Cardinal

O cardinal $|X|$ de um conjunto finito X é o número de elementos.

Exemplo:

- $[n] := \{1, 2, 3, \cdots, n\} \subset \mathbb{N}$ tem n elementos: $|[n]| = n$.
- $[n]_0 := \{0, 1, 2, 3, \cdots, n\} \subset \mathbb{N}_0$ tem $n + 1$ elementos.

Cardinal

O cardinal $|X|$ de um conjunto finito X é o número de elementos.

Exemplo:

- $[n] := \{1, 2, 3, \cdots, n\} \subset \mathbb{N}$ tem n elementos: $|[n]| = n$.
- $[n]_0 := \{0, 1, 2, 3, \cdots, n\} \subset \mathbb{N}_0$ tem $n + 1$ elementos.
- $|A \cup B| = |A| + |B| - |A \cap B|$

Cardinal

O cardinal $|X|$ de um conjunto finito X é o número de elementos.
Exemplo:

- $[n] := \{1, 2, 3, \cdots, n\} \subset \mathbb{N}$ tem n elementos: $|[n]| = n$.
- $[n]_0 := \{0, 1, 2, 3, \cdots, n\} \subset \mathbb{N}_0$ tem $n+1$ elementos.
- $|A \cup B| = |A| + |B| - |A \cap B|$
- Numa união disjunta:
$$|A_1 \sqcup A_2 \sqcup \cdots \sqcup A_k| = \sum_j |A_j|$$
- Conjunto **potência** de X (ou conjunto das partes de X):
$$\mathcal{P}(X) = \{A \mid A \subset X\}$$
tem $|\mathcal{P}(X)| = 2^{|X|}$.

Exemplo: se $X = \{0, 3, \alpha\}$ então
$$\mathcal{P}(X) = \{\varnothing, \{0\}, \{3\}, \{\alpha\}, \{0, 3\}, \{0, \alpha\}, \{3, \alpha\}, X\}$$

Funções

Uma **função** $f : X \to Y$ é uma associação: a cada $x \in X$, f associa um **único** $y = f(x) \in Y$.

X =**conjunto de partida** (domínio), Y = conjunto de chegada

Imagem de f é $f(X) = \{f(x) \in Y \mid x \in X\} \subset Y$

Imagem de $A \subset X$: $f(A) = \{f(x) \in Y \mid x \in A\} \subset f(X)$

Imagem inversa de $B \subset Y$:

$f^{-1}(B) = \{x \in X \mid f(x) \in B\} \subset X$

Funções

Uma **função** $f : X \to Y$ é uma associação: a cada $x \in X$, f associa um **único** $y = f(x) \in Y$.
X =**conjunto de partida** (domínio), Y = conjunto de chegada
Imagem de f é $f(X) = \{f(x) \in Y \mid x \in X\} \subset Y$
Imagem de $A \subset X$: $\quad f(A) = \{f(x) \in Y \mid x \in A\} \subset f(X)$
Imagem inversa de $B \subset Y$:
$f^{-1}(B) = \{x \in X \mid f(x) \in B\} \subset X$

Definição (Seja $f.X \to Y$ uma função)

f é **injectiva** se $f(x) \neq f(y)$ para $x \neq y$
f é **sobrejectiva** se $f(X) = Y$
f é **bijectiva** se é injectiva e sobrejectiva

Funções

Uma **função** $f : X \to Y$ é uma associação: a cada $x \in X$, f associa um **único** $y = f(x) \in Y$.
X =**conjunto de partida** (domínio), Y = conjunto de chegada
Imagem de f é $f(X) = \{f(x) \in Y \mid x \in X\} \subset Y$
Imagem de $A \subset X$: $f(A) = \{f(x) \in Y \mid x \in A\} \subset f(X)$
Imagem inversa de $B \subset Y$:
$f^{-1}(B) = \{x \in X \mid f(x) \in B\} \subset X$

Definição (Seja $f.X \to Y$ uma função)

f é **injectiva** se $f(x) \neq f(y)$ para $x \neq y$
f é **sobrejectiva** se $f(X) = Y$
f é **bijectiva** se é injectiva e sobrejectiva

Teorema (Seja $f.X \to Y$ uma função)

Se $|X| > |Y|$ então f não pode ser injectiva.
Se $|X| < |Y|$ então f não pode ser sobrejectiva.

Relações de equivalência

Relação de equivalência em X - uma *partição* de X em subconjuntos disjuntos - cada subconjunto fica com os objectos **equivalentes**.

Relações de equivalência

Relação de equivalência em X - uma *partição* de X em subconjuntos disjuntos - cada subconjunto fica com os objectos **equivalentes**.

Exemplos: (1) Com $X = \{x, y, \xi, \phi, \mathfrak{g}, \mathfrak{h}\}$, podemos tornar equivalentes as letras do mesmo alfabeto - obtém-se a relação $\{\{x, y\}, \{\xi, \phi\}, \{\mathfrak{g}, \mathfrak{h}\}\}$.
(2) Seja Y um conjunto de bolas. Dizemos que duas bolas são equivalentes se se usam no mesmo desporto.

Relações de equivalência

Relação de equivalência em X - uma *partição* de X em subconjuntos disjuntos - cada subconjunto fica com os objectos **equivalentes**.

Exemplos: (1) Com $X = \{x, y, \xi, \phi, \mathfrak{g}, \mathfrak{h}\}$, podemos tornar equivalentes as letras do mesmo alfabeto - obtém-se a relação $\{\{x, y\}, \{\xi, \phi\}, \{\mathfrak{g}, \mathfrak{h}\}\}$.
(2) Seja Y um conjunto de bolas. Dizemos que duas bolas são equivalentes se se usam no mesmo desporto.

Usualmente, a relação é descrita por um símbolo de operação binária, por ex. $\sim$. Escrevemos $x \sim y$, $\xi \sim \phi$ e $\mathfrak{g} \sim \mathfrak{h}$, ou $b_1 \equiv b_2$.

Relações de equivalência

Relação de equivalência em X - uma *partição* de X em subconjuntos disjuntos - cada subconjunto fica com os objectos **equivalentes**.

Exemplos: (1) Com $X = \{x, y, \xi, \phi, \mathfrak{g}, \mathfrak{h}\}$, podemos tornar equivalentes as letras do mesmo alfabeto - obtém-se a relação $\{\{x, y\}, \{\xi, \phi\}, \{\mathfrak{g}, \mathfrak{h}\}\}$. (2) Seja Y um conjunto de bolas. Dizemos que duas bolas são equivalentes se se usam no mesmo desporto.

Usualmente, a relação é descrita por um símbolo de operação binária, por ex. $\sim$. Escrevemos $x \sim y$, $\xi \sim \phi$ e $\mathfrak{g} \sim \mathfrak{h}$, ou $b_1 \equiv b_2$.

Proposição: A relação $\sim$ é uma relação de equivalência em X, **se e só se**, para todos $x, y, z \in X$:

- **Reflexiva:** $x \sim x$
- **Simétrica:** se $x \sim y$, então $y \sim x$
- **Transitiva:** se $x \sim y$ e $y \sim z$, então $x \sim z$.