

Aritmética modular, Euler e RSA

Carlos Florentino^{1,2}

¹Departamento de Matemática, FCUL,

²CMAFcIO e GFM Univ. de Lisboa,
(Não se usa o AO 90)

Notas de Matemática Discreta / Finita

Outline

- 1 Conjuntos, Funções e Relações de Equivalência
 - Conjuntos e Cardinalidade
 - Funções e Relações de Equivalência

- 2 Teorema Fundamental da Aritmética
 - Algoritmos, Euclides e Bézout

Outline

- 1 Conjuntos, Funções e Relações de Equivalência
 - Conjuntos e Cardinalidade
 - Funções e Relações de Equivalência

- 2 Teorema Fundamental da Aritmética
 - Algoritmos, Euclides e Bézout

Conjuntos - Linguagem/Terminologia

- $A = \{a, b, c, \dots\}$, 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

- $A = \{a, b, c, \dots\}$, 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** $\mathbb{N} = \{1, 2, 3, \dots\}$, $\mathbb{N}_0 = \{0, 1, 2, 3, \dots\} = \mathbb{N} \cup \{0\}$
- **Inteiros** $\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, 3, \dots\}$
- **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

- $A = \{a, b, c, \dots\}$, 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** $\mathbb{N} = \{1, 2, 3, \dots\}$, $\mathbb{N}_0 = \{0, 1, 2, 3, \dots\} = \mathbb{N} \cup \{0\}$
- **Inteiros** $\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, 3, \dots\}$
- **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** $A \Delta B := (A \setminus B) \cup (B \setminus A)$
- **União disjunta** $A \sqcup B := A \cup B$, sempre que $A \cap B = \emptyset$
- **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:

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

Cardinal

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

Exemplo:

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

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

$$|A_1 \sqcup A_2 \sqcup \dots \sqcup A_k| = \sum_j |A_j|$$

- Conjunto **potência** de X (ou conjunto das partes de X):

$$\mathcal{P}(X) = \{A \mid A \subset X\}$$

tem $|\mathcal{P}(X)| = 2^{|X|}$.

Cardinal

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

Exemplo:

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

$$|A_1 \sqcup A_2 \sqcup \dots \sqcup A_k| = \sum_j |A_j|$$

- 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

$$\mathcal{P}(X) = \{\emptyset, \{0\}, \{3\}, \{\alpha\}, \{0, 3\}, \{0, \alpha\}, \{3, \alpha\}, X\}$$

Funções

Uma **função** $f : X \rightarrow Y$ 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** $f : X \rightarrow Y$ 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 $f: X \rightarrow Y$ 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** $f : X \rightarrow Y$ 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 $f: X \rightarrow Y$ 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 $f: X \rightarrow Y$ 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 $X = \{x, y, \xi, \phi, g, h\}$, podemos tornar equivalentes as letras do mesmo alfabeto - obtém-se a relação $\{\{x, y\}, \{\xi, \phi\}, \{g, h\}\}$.
(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 $X = \{x, y, \xi, \phi, g, h\}$, podemos tornar equivalentes as letras do mesmo alfabeto - obtém-se a relação $\{\{x, y\}, \{\xi, \phi\}, \{g, h\}\}$.
(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 $g \sim h$, 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 $x \sim z$.

Outline

- 1 Conjuntos, Funções e Relações de Equivalência
 - Conjuntos e Cardinalidade
 - Funções e Relações de Equivalência

- 2 Teorema Fundamental da Aritmética
 - Algoritmos, Euclides e Bézout

MDC e O algoritmo de Euclides

- Dados 2 naturais a, b , o seu **máximo divisor comum** é o maior elemento $d := (a, b)$ do conjunto finito:

$$\text{Div}(a) \cap \text{Div}(b).$$

MDC e O algoritmo de Euclides

- Dados 2 naturais a, b , o seu **máximo divisor comum** é o maior elemento $d := (a, b)$ do conjunto finito:

$$\text{Div}(a) \cap \text{Div}(b).$$

- Para o determinar, fazemos uma sucessão de **divisões inteiras**, começando com $a = d_0$, $b = d_1$ (supondo $a > b$):

$$d_0 = q_1 d_1 + d_2$$

$$d_1 = q_2 d_2 + d_3$$

$$\vdots$$

$$d_{k-2} = d_{k-1} q_{k-1} + d_k$$

$$d_{k-1} = d_k q_k + 0$$

MDC e O algoritmo de Euclides

- Dados 2 naturais a, b , o seu **máximo divisor comum** é o maior elemento $d := (a, b)$ do conjunto finito:

$$\text{Div}(a) \cap \text{Div}(b).$$

- Para o determinar, fazemos uma sucessão de **divisões inteiras**, começando com $a = d_0$, $b = d_1$ (supondo $a > b$):

$$d_0 = q_1 d_1 + d_2$$

$$d_1 = q_2 d_2 + d_3$$

$$\vdots$$

$$d_{k-2} = d_{k-1} q_{k-1} + d_k$$

$$d_{k-1} = d_k q_k + 0$$

- No fim obtemos $(a, b) = d_k$.

Equação de Bézout

- Sejam a, b naturais (ou inteiros) e seja $d = (a, b)$ o seu máximo divisor comum. **A equação de Bézout** é:

$$ax + by = d,$$

sendo x, y as incógnitas (em \mathbb{Z}). Uma **solução particular** obtém-se do algoritmo de Euclides estendido.

Equação de Bézout

- Sejam a, b naturais (ou inteiros) e seja $d = (a, b)$ o seu máximo divisor comum. **A equação de Bézout** é:

$$ax + by = d,$$

sendo x, y as incógnitas (em \mathbb{Z}). Uma **solução particular** obtém-se do algoritmo de Euclides estendido.

- Mais geralmente, temos a equação (Diofantina):

$$ax + by = c, \tag{1}$$

sendo a, b, c **dados** (em \mathbb{N} ou \mathbb{Z}) e x, y as **incógnitas** (em \mathbb{Z}).

Equação de Bézout

- Sejam a, b naturais (ou inteiros) e seja $d = (a, b)$ o seu máximo divisor comum. **A equação de Bézout** é:

$$ax + by = d,$$

sendo x, y as incógnitas (em \mathbb{Z}). Uma **solução particular** obtém-se do algoritmo de Euclides estendido.

- Mais geralmente, temos a equação (Diofantina):

$$ax + by = c, \tag{1}$$

sendo a, b, c **dados** (em \mathbb{N} ou \mathbb{Z}) e x, y as **incógnitas** (em \mathbb{Z}).

- A equação (1) tem solução (x_0, y_0) se e só se $(a, b) \mid c$ (quando existem, as soluções são infinitas).

Equação de Bézout

- Sejam a, b naturais (ou inteiros) e seja $d = (a, b)$ o seu máximo divisor comum. **A equação de Bézout** é:

$$ax + by = d,$$

sendo x, y as incógnitas (em \mathbb{Z}). Uma **solução particular** obtém-se do algoritmo de Euclides estendido.

- Mais geralmente, temos a equação (Diofantina):

$$ax + by = c, \tag{1}$$

sendo a, b, c **dados** (em \mathbb{N} ou \mathbb{Z}) e x, y as **incógnitas** (em \mathbb{Z}).

- A equação (1) tem solução (x_0, y_0) se e só se $(a, b) \mid c$ (quando existem, as soluções são infinitas).
- A **solução geral** de (1) é:

$$x = x_0 + k \frac{b}{d}, \quad y = y_0 - k \frac{a}{d}, \quad k \in \mathbb{Z},$$

sendo (x_0, y_0) solução de $ax + by = c = md$.

Equação de Bézout - Exemplo

- Exemplo: determinar todas as soluções $(x, y) \in \mathbb{Z}^2$ de

$$711x + 132y = 6. \quad (2)$$

i	d_i	$-q_i$	x_i	y_i
0	711		1	0
1	132	-5	0	1
2	51	-2	1	-5
3	30	-1	-2	11
4	21	-1	3	-16
5	9	-2	-5	27
6	3	-3	13	-70
7	0		-44	237

Relacionamos as linhas $i + 1$, i e $i - 1$ da seguinte forma:

$$d_{i+1} = d_{i-1} - q_i d_i$$

$$x_{i+1} = x_{i-1} - q_i x_i$$

$$y_{i+1} = y_{i-1} - q_i y_i$$

- Logo

$$6 = 711 \times 26 + 132 \times (-140),$$

e, usando $\frac{132}{3} = 44$ e $\frac{711}{3} = 237$, a solução geral de (2) é:

$$x = x_0 - 44k, \quad y = y_0 + 237k, \quad k \in \mathbb{Z}.$$