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

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.

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

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**.

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 $x \sim z$.

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:

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

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

$$\begin{array}{rcl} d_0 & = & q_1 d_1 + d_2 \\ d_1 & = & q_2 d_2 + d_3 \\ & \vdots & \\ d_{k-2} & = & d_{k-1} q_{k-1} + d_k \\ d_{k-1} & = & d_k q_k + 0 \end{array}$$

- 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.

- 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

$$711x + 132y = 6. \tag{2}$$

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		13	-70

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

$$\begin{aligned} d_{i+1} &= d_{i-1} - q_i d_i \\ x_{i+1} &= x_{i-1} - q_i x_i \\ y_{i+1} &= y_{i-1} - q_i y_i \end{aligned}$$

- 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:

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

Lema de Euclides

Recorde que $p \in \mathbb{N}$ é **primo** se e só se $|\text{Div}(p)| = 2$

Se $(a, b) = 1$ dizemos que a e b são **primos entre si**.

Sejam a, b, c inteiros não nulos.
Se a é primo com b e com c, então é primo com bc.
Ou seja:
Lema: Se $(a, b) = (a, c) = 1$, então $(a, bc) = 1$.

Lema de Euclides

Seja $a, b \in \mathbb{Z}$. Se p é primo:

$$p \mid ab, \quad \Leftrightarrow \quad p \mid a \text{ ou } p \mid b.$$

Enunciado do TFA

Teorema Fundamental da Aritmética

Seja $n \in \mathbb{N}$.

Versão 1: Existe factorização:

$$n = p_1 \cdots p_m, \qquad p_1, \cdots, p_m \text{ são primos.}$$

Versão 2: Existe factorização:

$$n = p_1^{e_1} \cdots p_k^{e_k}, \qquad p_1, \cdots, p_k \text{ são primos } \textbf{distintos}, \; e_j \in \mathbb{N}.$$

Ambas as factorizaçõs são únicas a menos de reordenação dos factores.

Corolário

Seja $n = p_1^{e_1} \cdots p_k^{e_k} \in \mathbb{N}$. O conjunto dos divisores positivos de n é:

$$\mathrm{Div}(n) = \{p_1^{c_1} \cdots p_k^{c_k} \; : \; c_i \in \{0, \cdots, e_i\}\}$$

Números racionais

- Um número racional é da forma:

$$\frac{a}{b}, \quad a \in \mathbb{Z}, b \in \mathbb{Z} \setminus \{0\}.$$

- Os números racionais formam um **corpo**, denotado $\mathbb{Q}$: temos $+$, $\times$, elementos neutros 0 e 1, distributividade, e podemos dividir dois racionais desde que o denominador não se anule.

Dado um racional $x \in \mathbb{Q}$, existem $n, a, b \in \mathbb{Z}$, com $(a, b) = 1$, tais que:

$$x = n + \frac{a}{b},$$

além disso esta representação é única, se exigirmos $b > a \geq 0$.

- Se $x > 0$, o inteiro n chama-se a parte inteira de x e $\frac{a}{b}$ chama-se a parte própria (ou fraccionária) de x.
- Escrevemos $n = \lfloor x \rfloor$ e $\frac{a}{b} = /x\backslash$.
- Note-se $/x\backslash \in [0, 1[$.

Representação na base m

Seja m um natural ≥ 2.

Teorema

Qualquer natural $n \in \mathbb{N}$ se pode escrever "na base m":

$$n = a_k m^k + a_{k-1} m^{k-1} + \cdots + a_1 m + a_0$$

onde $a_k \in \{0, 1, \cdots, m-1\}$. Abreviadamente: $n = [a_k \cdots a_1 a_0]_m$.

$$\begin{aligned} 25 &= 16 + 8 + 1 = 1 \cdot 2^4 + 1 \cdot 2^3 + 1 = [11001]_2 \\ 25 &= 2 \cdot 3^2 + 2 \cdot 3 + 1 = [221]_3 \\ 25 &= 3 \cdot 7 + 4 = [34]_7 \end{aligned}$$

Podemos fazer o mesmo com números racionais:

$$\begin{aligned} 12,34 &= 12 + \frac{3}{10} + \frac{4}{100} = 10 + 2 \cdot 10^0 + 3 \cdot 10^{-1} + 4 \cdot 10^{-2}, \text{ na base } 10 \\ 1,76 &= \frac{44}{25} = 1 + \frac{3}{5} + \frac{4}{25} = 1 \cdot 5^0 + 3 \cdot 5^{-1} + 4 \cdot 5^{-2} = [1,34]_5 \end{aligned}$$

mas normalmente, vamos obter dízimas infinitas (periódicas)...