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*, $a \in A$
- $B = \{n \in \mathbb{Z} \ : \ n^2 > 24\}$, 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** $\mathbb{Q} = \{\frac{a}{b} \ : \ a \in \mathbb{Z}, b \in \mathbb{N}\}$
- **Reais** $\mathbb{R}$, **Complexos** $\mathbb{C}$, etc.

Operações com conjuntos:

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

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.
- $|A \cup B| = |A| + |B| - |A \cap B|$
- $|A \times B| = |A| \cdot |B|$
- 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):

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

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

Exemplo: se $X = \{0, 4, \alpha\}$ então:

$$\mathcal{P}(X) = \{\varnothing, \{0\}, \{4\}, \{\alpha\}, \{0, 4\}, \{0, \alpha\}, \{4, \alpha\}, X\}$$

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 $f(X) = \{f(x) \in Y \ : \ x \in X\} \subset Y$

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

Imagem inversa de $B \subset Y$:

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

Definição

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

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 $x \sim z$.

Divisão inteira e divisibilidade

- Sejam $a, b \in \mathbb{N}$, com $a > b > 1$. Recorde: a **divisão inteira de a por b** é a representação:

$$a = q \cdot b + r$$

onde $r \in \{0, 1, 2, \cdots, b-1\}$ é o **resto** e q o **quociente**, que são únicos!

Exemplo: Dividir 711 por 132: $711 = 5 \cdot 132 + 51$.

Divisibilidade: Para $a, b \in \mathbb{Z}$, dizemos que *"b divide a"*, ou *"b é divisor de a"*, e escreve-se $b \mid a$ (caso contrário $b \nmid a$) se:

- a é múltiplo de b, ou
- $\frac{a}{b} \in \mathbb{Z}$
- o resto da divisão de a por b é zero (no caso $a, b > 0$)

$$\mathrm{Div}(a) := \{\text{divisores positivos de } a\} = \{n \in \mathbb{N} \ : \ n \mid a\}$$

Divisibilidade: Propriedades

- **Propriedades:** • $0 \nmid a$, $1 \mid a$ para todo $a \in \mathbb{N}$
  - Se $a \mid b$ e $b \mid c$ então $a \mid c$.
  - Se $b \mid a$ e $a \mid b$ então $|a| = |b|$.
  - Se $a, b \in \mathbb{N}$ e $a \mid b$, então $a \leq b$ e $a \in \text{Div}(b)$
  - Se $a \mid b$ então $a \mid bc$.
  - Se $a \mid b$ e $a \mid c$ então $a \mid (b + c)$ e $a \mid (b - c)$.

- $p \in \mathbb{N}$ é número ***primo*** se $\text{Div}(p) = \{1, p\}$. Assim, um **primo** se tem apenas 2 divisores. De facto:

$$|\text{Div}(n)| = 2 \qquad \Longleftrightarrow \qquad n \text{ é primo}$$

MDC e O algoritmo de Euclides

- **Máximo divisor comum** entre $a, b \in \mathbb{N}$ é o maior elemento $(a, b) := \mathrm{mdc}(a, b)$, do conjunto:
$$\mathrm{Div}(a) \cap \mathrm{Div}(b).$$

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

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

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

Diz-se que $a, b \in \mathbb{N}$ são ***primos entre si*** se $(a, b) = 1$.

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* $d = (a, b) \mid c$ (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

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

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:

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

- 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 $|\mathrm{Div}(p)| = 2$

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:

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

Princípio de Indução

Proposição: [Princípio de Indução]. Seja $P(n)$ uma proposição (afirmação), $n \in \mathbb{N}$. $P(n)$ é verdadeira $\forall n \in \mathbb{N}$ se:

- [passo base] $P(1)$ é válida e:
- [passo de indução] $P(n)$ implica $P(n+1)$, para todo $n \geq 1$.

Proposição: [Princípio de Indução forte]. Seja $P(n)$ uma proposição (afirmação), $n \in \mathbb{N}$. $P(n)$ é verdadeira $\forall n \geq n_0$ se:

- [passo base] $P(n_0)$ é válida e:
- [passo de indução] $P(n_0), \cdots, P(n)$ implicam $P(n+1)$, para todo $n \geq n_0$.

Exemplo: Mostrar que $\frac{n^2-3n+2}{2}$ é inteiro $\forall n \in \mathbb{N}$.

Passo base $P(1)$: $\frac{1^2-3+2}{2} = 0$ é inteiro

Passo de indução: Temos $P(n+1)$: $\frac{(n+1)^2-3(n+1)+2}{2}$ equivale a $\frac{n^2-3n+2}{2} + \frac{2n+1-3}{2} = \frac{n^2-3n+2}{2} + n - 1$ que é inteiro sempre que $\frac{n^2-3n+2}{2}$ é inteiro. Portanto $P(n) \Rightarrow P(n+1)$.

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 factorizações 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:

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

Exemplo: (1) Sem fazer contas $3^{11}11^3 \neq 5^7 7^5$.
(2) Sem determinar os números $(2^7 5^8 13^4, 4^2 21^3 19^5) = 16$.

Números racionais

- Números racionais são da forma:
$$\frac{a}{b}, \quad a \in \mathbb{Z},\, b \in \mathbb{N}.$$
Se $(a,b)=1$ diz-se **fracção irredutível**. Ex: $\frac{90}{56}=\frac{45}{28}=\frac{5\cdot 3^2}{2^2\cdot 7}$.
- 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 qualquer $x \in \mathbb{Q}$, 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 impomos $b > a \geq 0$.

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

Exemplos: $\frac{45}{28} = 1 + \frac{17}{28}$, $\quad -\frac{5}{2} = -3 + \frac{1}{2}$.

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: $n = [a_k \cdots a_1 a_0]_m$.

$$\begin{aligned} 25 = [25]_{10} &= 16 + 8 + 1 = 1 \cdot 2^4 + 1 \cdot 2^3 + 1 = [11001]_2 \\ 25 &= 2 \cdot 3^2 + 2 \cdot 3 + 1 = [221]_3 \\ 25 &= 3 \cdot 7 + 4 = [34]_7 \end{aligned}$$

Os números racionais **também se representam em bases:**

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

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

Congruências

Seja m natural ≥ 2, $a, b \in \mathbb{Z}$. Dizemos que "a é congruente com b módulo m"

$$a \equiv b \text{ mod } m$$

se $m \mid (b-a)$ (ie, $b-a$ é múltiplo de m).

Exemplos

- módulo 2: a par $\Leftrightarrow a \equiv 0$ mod 2; a impar $\Leftrightarrow a \equiv 1$ mod 2
- módulo 4: anos bissextos $\equiv 0$ mod 4; mundial de futebol $\equiv 2$ mod 4
- módulo 7: Segunda-feira é dia 2 $\Leftrightarrow$ próximas segundas-feiras são $\equiv 2$ mod 7
- módulo 24: $55 \equiv 7$ mod 24: "55 horas = 2 dias e 7 horas"
- $a \equiv r$ mod m, sempre que $a = mq + r$ é uma divisão inteira de a por m.

Números modulares: $\equiv$ mod m é *relação de equivalência* em $\mathbb{Z}$

$\mathbb{Z}_m :=$ {Classes de equival. de $\equiv$ mod m} $\leftrightarrow \{0, 1, \cdots, m-1\} =: [m]_0$

Regras da Aritmética Modular

Módulo fixo m:

$$a \equiv b \bmod m, \quad c \equiv d \bmod m \quad \Rightarrow \quad \begin{array}{c} a + c \equiv b + d \bmod m \\ ac \equiv bd \bmod m \\ a^k \equiv b^k \bmod m, \quad \forall k \in \mathbb{N} \end{array}$$

Módulos múltiplos:

$$n \mid m \quad a \equiv b \bmod m \quad \Rightarrow \quad a \equiv b \bmod n$$

$$(a, b, m) = d \quad a \equiv b \bmod m \quad \Rightarrow \quad \frac{a}{d} \equiv \frac{b}{d} \bmod \frac{m}{d}$$

- $5 + 23 \equiv 0 \bmod 7$
- $(-2) \cdot 19 \equiv -8 \equiv 2 \bmod 10$
- $4^{23} \equiv (-1)^{23} \equiv -1 \equiv 4 \bmod 5$

Não se verifica a lei do corte: $ab \equiv ac \bmod m \quad \not\Rightarrow \quad b \equiv c \bmod m$

$a \in \mathbb{Z}$ é invertível módulo m (ie $\exists b \in \mathbb{Z}$ com $ab \equiv 1 \bmod m$) se e só se $(a, m) = 1$.

No caso $(a, m) = 1$, já temos $ab \equiv ac \bmod m \quad \Rightarrow \quad b \equiv c \bmod m$.

Anéis

Um **anel** é um conjunto A com elementos especiais $0, 1$ e operações $+, \times$ que satisfazem (para todo $a, b, c, \cdots$):

- $(a+b)+c = a+(b+c)$ (+ é associativa)
- $a+b = b+a$ (+ é comutativa)
- $a+0 = a$ (0 é neutro para $+$)
- Dado a existe $-a$ tal que $a+(-a) = 0$
- $(a \times b) \times c = a \times (b \times c)$ ($\times$ é associativa)
- [se $a \times b = b \times a$, caso em que $\times$ é comutativa, A diz-se comutativo]
- $a \times 1 = 1 \times a = a$ (1 é neutro para $\times$)
- $a \times (b+c) = (a \times b) + (a \times c)$ e $(b+c) \times a = (b \times a) + (c \times a)$ (distributividade)

Exemplos

- $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ e $\mathbb{C}$ são anéis, com as operações usuais.
- Polinómios: $\mathbb{R}[x]$ é um anel
- Matrizes (quadradas): $Mat_{n \times n}$ é um anel (*não comutativo*).
- $\mathbb{Z}_m$ é um anel.

Corpos

Um **corpo** F é um **anel comutativo**: os elementos especiais $0, 1$ e as operações $+, \times$ satisfazem (para todo $a, b, c, \cdots$) todas as propriedades de anel comutativo, e **mais uma propriedade:**

- Para todo $a \neq 0$, existe $1/a \in F$ (também escrito a^{-1}) tal que

$$a \times \frac{1}{a} = \frac{1}{a} \times a = 1$$

Exemplos

- $\mathbb{Q}$, $\mathbb{R}$ e $\mathbb{C}$ são corpos, com as operações usuais.
- $\mathbb{Z}$ não é corpo
- $\mathbb{R}[x]$ não é corpo
- $Mat_{n \times n}$ não é corpo (se $n > 1$)
- $\mathbb{Z}_m$ é corpo se e só se m é primo!

Um corpo verifica a ***lei do corte***: Se $ab = ac$ e $a \neq 0$, então $b = c$.