Teoria dos Números

Textuniversitários 33

Hemar Godinho
Salahoddin Shokranian
Marcus Soares

Teoria dos Números
(3ª edição)

LF Editorial
São Paulo — 2025

3a. Edição

Editor: Victor Pereira Marinho / José Roberto Marinho
Projeto gráfico e diagramação: Thiago Augusto Silva Dourado
Capa: Fabrício Ribeiro

Texto em conformidade com as novas regras ortográficas do Acordo da Língua Portuguesa.

Dados Internacionais de Catalogação na Publicação (CIP)
(Câmara Brasileira do Livro, SP, Brasil)

Godinho, Hemar

Teoria dos números / Hemar Godinho, Salahoddin Shokranian, Marcus Soares. –– 3. ed. –– São Paulo : LF Editorial, 2025. –– (Textuniversitários ; 33)

ISBN 978-65-5563-653-6

1. Teoria dos números I. Shokranian, Salahoddin. II. Soares, Marcus. III. Título. IV. Série.

25-304578.0 CDD–512.7

Índices para catálogo sistemático:

1. Teoria dos números : Matemática 512.7

Eliete Marques da Silva – Bibliotecária – CRB-8/9380

Impresso no Brasil
Printed in Brazil

www.lfeditorial.com.br
Visite nossa livraria no Instituto de Física da USP
www.livrariadafisica.com.br
Telefones:
(11) 2648-6666 | Loja do Instituto de Física da USP
(11) 3936-3413 | Editora

"Dedicamos este trabalho às nossas famílias, e a todas as pessoas que encontram alegria no desvendar dos mistérios escondidos nos números"

Prefácio

Teoria dos Números é a ciência na qual se estudam propriedades e relações entre os números. Esta é uma área de matemática muito antiga, cujo desenvolvimento, como todas as outras partes da ciência, está diretamente ligado ao processo de civilização do ser humano.

A pesquisa hoje em teoria dos números está muito efervescente, e suas aplicações estão se multiplicando rapidamente em vários outros campos de matemática, tanto pura como aplicada. E estes fatos mostram que esta teoria merece um estudo profundo e detalhado, e é isso que nos motivou a escrever este livro a nível elementar, com a intenção de despertar as mentes mais jovens para esta empolgante área. Grande parte do material contido neste livro foi ensinado pelos autores em diversas ocasiões, na Universidade de Brasília, desde 1984.

A leitura deste livro não exige nenhum pré-requisito específico e todos os assuntos tratados aqui são explicados com uma linguagem clara, na tentativa de tornar este trabalho acessível a todos. Assim, mesmo um estudante iniciando seu curso superior poderá fazer bom uso deste livro.

Este livro é uma introdução à Teoria dos Números num nível elementar, mas abordamos também alguns métodos mais modernos que têm se provado úteis em todas as áreas desta teoria. Os primeiros quatro capítulos são introdutórios e fundamentais, podendo ser usados como texto para um curso básico de graduação de um semestre. Os últimos três capítulos apresentam assuntos mais

avançados, formando uma boa base para futuros estudos em nível de pós-graduação. Estes três últimos capítulos são independentes entre si, e a leitura de qualquer um destes capítulos finais pode ser iniciada após o capítulo 4.

Nós gostaríamos de agradecer à Editora Universidade de Brasília, à Tania Sertão pelos trabalhos de digitação, e aos nossos alunos que ajudaram a trazer maior clareza a algumas explanações. Os três autores contavam com auxílio financeiro do CNPq durante a elaboração deste livro.

Brasília, junho de 1994.

Prefácio da Segunda Edição

Nesta segunda edição, buscamos corrigir todos os erros óbvios, além de melhorar muitas das demonstrações e explanações. Aproveitamos para agradecer a todos os leitores, alunos e colegas pelas sugestões apresentadas.

Brasília, junho de 1998.

Prefácio da Terceira Edição

Esta terceira edição é resposta ao interesse e incentivo manifestado por diversos professores e estudantes que procuram encontrar em nosso texto os aspectos básicos da teoria dos números inteiros, e os conteúdos mais avançados presentes nos capítulos finais, como a introdução aos números p-ádicos e à geometria dos números, bem como a apresentação elementar da teoria de curvas elípticas.

Gostaríamos de agradecer ao corpo editorial da coleção *Textuniversitários*, em especial ao Prof. Dr. Thiago Augusto Silva Dourado e toda sua equipe, pelo incentivo e pelo excelente trabalho. Sem isso, esta nova edição não se tornaria realidade. Ficamos satisfeitos em perceber

que, mesmo após todos esses anos sem exemplares disponíveis, ainda existia demanda para esse livro.

Nesta edição, corrigimos e melhoramos ainda mais o texto, acrescentamos novos exercícios e também novas referências. Novamente, agradecemos as valiosas sugestões e comentários dos vários colegas e estudantes.

Brasília, agosto de 2025.

Sumário

1

Divisibilidade e Números Primos

Neste primeiro capítulo trataremos de assuntos bastante básicos e ao mesmo tempo indispensáveis a qualquer estudo que se queira fazer em Teoria dos Números. Assumiremos como conhecidas apenas as propriedades mais elementares dos conjuntos numéricos:

$\mathbb{N} = \{1, 2, 3, \ldots\}$, *os números naturais;*

$\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$, *os números inteiros;*

$\mathbb{Q} = \{\frac{m}{n} \mid m, n \in \mathbb{Z},\ n \neq 0\}$, *os números racionais;*

$\mathbb{R} =$ *conjunto dos números reais.*

1.1 Princípio da indução matemática

O princípio da indução matemática serve para provar proposições que dependem de n, um inteiro não negativo, que varia num subconjunto infinito de $\mathbb{Z}$. Este princípio está baseado no seguinte axioma:

Princípio da Boa Ordenação. *Todo subconjunto não vazio A de inteiros não negativos possui um elemento mínimo (isto é, existe $n_0 \in A$ tal que $n_0 \leq n$, para todo $n \in A$).*

Veremos agora como usar este princípio para obtermos uma ferramenta muito útil para lidarmos com inteiros.

Princípio de Indução Matemática (1ª forma). *Seja $N = \{n_0, n_1, \ldots\}$ um conjunto de inteiros não negativos (suponha também $n_0 < n_1 < \cdots$) e seja $S(n)$ uma proposição que depende de $n \in N$, tal que:*

(a) $S(n_0)$ é verdadeira.

(b) Se $m \in N$ e $S(n)$ é verdadeira para todo $n \in N$ tal que $n < m$, então $S(m)$ é verdadeira.

Então $S(n)$ é verdadeira para qualquer $n \in N$.

Demonstração. A demonstração será feita por contradição. Seja

$$F = \{\ell \in N \mid S(\ell) \text{ não é verdadeira}\},$$

e suponha por absurdo que $F \neq \emptyset$. Pelo Princípio da Boa Ordenação, existe $\ell_0 \in F$, $\ell_0 > n_0$ (já que $S(n_0)$ é verdadeira) tal que $\ell_0 \leq \ell$, para todo $\ell \in F$ (isto é, ℓ_0 é um elemento mínimo de F). Isto nos diz que $S(n)$ é verdadeira para todo $n \in N$ tal que $n < \ell_0$ (a não validade desta afirmação comprometeria a minimalidade de ℓ_0). Pela hipótese (b) temos que $S(\ell_0)$ é verdadeira, uma contradição. Assim, devemos ter $F = \emptyset$ e $S(n)$ é verdadeira para todo $n \in N$. □

Princípio de Indução Matemática (2ª forma). *Sejam $N_0 = \mathbb{N} \cup \{0\}$ e $S(n)$ uma proposição que depende de $n \in N_0$, tal que:*

(a) $S(0)$ é verdadeira.

(b) Para cada $n \in N_0$, o fato de $S(n)$ ser verdadeira implica em $S(n+1)$ também ser verdadeira.

Então $S(n)$ é verdadeira para qualquer $n \in N_0$.

Demonstração. Esta demonstração é completamente análoga à do teorema anterior e o leitor está convidado a fazê-la. Observe também que nada há de especial com o zero e o nosso conjunto N_0 poderia ser do tipo $N_0 = \{n_0, n_0 + 1, n_0 + 2, \ldots\}$ para qualquer $n_0 \in \mathbb{N} \cup \{0\}$. □

Vejamos algumas aplicações destes princípios.

Exemplo 1.1.1 Seja $S(n) =$ "a soma dos n primeiros inteiros positivos é $\frac{n(n+1)}{2}$", isto é,

$$1+2+\cdots+n = \frac{n(n+1)}{2}.$$

Vamos utilizar o princípio de indução (2ª forma) com $N_0 = \mathbb{N}$. Observe que $S(1)$ é verdadeira ($1 = \frac{1\cdot(1+1)}{2}$). Vamos mostrar que o fato de $S(n)$ ser verdadeira faz com que $S(n+1)$ também o seja. Com efeito,

$$\begin{aligned} 1+2+\cdots+n+(n+1) &= (1+2+3+\cdots+n)+(n+1) \\ &= \frac{n(n+1)}{2}+(n+1) \\ &= \frac{n(n+1)+2(n+1)}{2} \\ &= \frac{(n+1)(n+2)}{2}. \end{aligned}$$

Logo, $S(n+1)$ é verdadeira.

Exemplo 1.1.2 Vamos mostrar por indução que para todo $x \in \mathbb{R}$, $x \neq 1$, e para todo $n \in \mathbb{N}$, é válida a seguinte identidade

$$\sum_{j=0}^{n-1} x^j = 1+x+\cdots+x^{n-1} = \frac{x^n-1}{x-1}.$$

Seja

$$S(n) = 1+x+\cdots+x^{n-1} = \frac{x^n-1}{x-1}.$$

Temos que $1 = \frac{x-1}{x-1}$, logo, $S(1)$ é verdadeira. Supondo que $S(n)$ seja verdadeira, temos

$$\begin{aligned} 1+x+\cdots+x^{n-1}+x^n &= (1+x+\cdots+x^{n-1})+x^n \\ &= \frac{x^n-1}{x-1}+x^n \\ &= \frac{(x^n-1)+x^n(x-1)}{x-1} \\ &= \frac{x^{n+1}-1}{x-1}. \end{aligned}$$

Assim, pelo princípio da indução (2ª forma), temos $\sum_{j=0}^{n-1} x^j = \frac{x^n-1}{x-1}$, para todo número natural n.

Exercício 1.1.3 Deixamos ao leitor a tarefa de encontrar a falha da seguinte aplicação do princípio de indução. Considere a afirmação

$S(n) =$ "numa turma de n alunos, se um deles é loiro, todos o são".

Esta afirmação é obviamente falsa. Examine esta "demonstração" de que $S(n)$ é verdadeira.

Claro que $S(1)$ é verdadeira. Suponha que $S(n)$ é verdadeira para todo $n < m$, $m \in \mathbb{N}$ e vamos provar que $S(m)$ é verdadeira. Ora, m certamente pode ser escrito como $m = m_1 + m_2$ com $m_1, m_2 \in \mathbb{N}$ e $m_1, m_2 < m$. Separe a turma em duas partes com m_1 alunos na primeira parte e m_2 alunos na segunda. Por hipótese de indução, $S(m_1)$ e $S(m_2)$ são verdadeiras. Logo $S(m)$ é verdadeira.

1.2 Divisibilidade

Nesta seção usamos o princípio de indução matemática para estabelecer um belo resultado sobre os números inteiros, tanto por sua simplicidade, como por suas consequências, dentre elas o estudo de máximo divisor comum entre inteiros não nulos. Comecemos com as definições básicas.

Definição 1.2.1 Sejam $a, b \in \mathbb{Z}$, $b \neq 0$. Dizemos que b *divide* a (ou que b *é divisor de* a ou que a *é múltiplo de* b) quando existe $n \in \mathbb{Z}$ tal que $a = nb$. Representamos esta propriedade por $b \mid a$ (lê-se: b divide a). Representamos o fato de b não dividir a por $b \nmid a$ (lê-se: b não divide a).

Lema 1.2.2 *(i) Para qualquer $b \in \mathbb{Z}$, $b \neq 0$, temos que $b \mid 0$.*

(ii) Se $a, b, c \in \mathbb{Z}$, $b \neq 0$ e $b \mid a$, $b \mid c$, então para quaisquer $r, s \in \mathbb{Z}$ temos $b \mid ra + sc$.

DEMONSTRAÇÃO. Exercício. □

Antes de nos aprofundarmos no estudo da divisibilidade, apresentaremos um resultado de Euclides (matemático grego que viveu por volta de 300 a.C.), o *Algoritmo da Divisão de Euclides*.

Teorema 1.2.3 (Euclides) *Para quaisquer $a, b \in \mathbb{N}$ existem únicos inteiros q e r tais que*

$$a = bq + r \quad e \quad 0 \leq r < b.$$

Em outras palavras, existe um único múltiplo bq de b tal que $bq \leq a < b(q+1)$.

DEMONSTRAÇÃO. Dividimos a demonstração em duas partes.

Existência de q e r. Seja $M = \{m \in \mathbb{Z} \mid m = a - bt, t \in \mathbb{Z}\}$, e denote por M_+ o subconjunto dos elementos não negativos de M, ou seja $M_+ = \{m \in M \mid m \geq 0\}$. Pelo Princípio da Boa Ordenação existe $r \in M_+$ tal que $r \leq x$, para todo $x \in M_+$ (um elemento mínimo de M_+). Como $r \in M_+ \subset M$ temos $r = a - bq$ para algum $q \in \mathbb{Z}$, e assim $a = bq + r$, com $r \geq 0$ (pois $r \in M_+$). Se tivéssemos $r = (a - bq) \geq b$ isto acarretaria $a - (q+1)b \geq 0$, logo $a - (q+1)b \in M_+$. Mas $a - (q+1)b < a - qb = r$, contradizendo a minimalidade de r. Assim temos $0 \leq r < b$.

Unicidade de q e r. Suponhamos que $a = bq + r$ e também $a = bq' + r'$ com $q, r, q', r' \in \mathbb{Z}$ e $0 \leq r, r' < b$. Suponha, sem perda de generalidade, que $r \geq r'$. Como $bq + r = bq' + r'$, temos que

$$r - r' = b(q' - q).$$

Assim, $0 \leq b(q' - q) < b$, daí $q' - q = 0$ e consequentemente $q = q'$ e $r = r'$. □

Veremos a seguir uma primeira aplicação do algoritmo de Euclides.

Definição 1.2.4 Um subconjunto não vazio $S \subset \mathbb{Z}$ é dito um *módulo de $\mathbb{Z}$* se:

(i) $nr \in S$, para quaisquer $r \in S$ e $n \in \mathbb{Z}$.

(ii) $r_1 \pm r_2 \in S$, para quaisquer $r_1, r_2 \in S$.

Exemplo 1.2.5 Vejamos alguns exemplos de módulos.

1. $S = \{0, \pm 2, \pm 4, \ldots\} = 2\mathbb{Z}$ é um módulo de $\mathbb{Z}$.
2. $S = \{0\}$ e $S = \mathbb{Z}$ são módulos (triviais) de $\mathbb{Z}$.
3. Para $a_1, \ldots a_n \in \mathbb{Z}$ fixos, o conjunto

$$S = \{a_1x_1 + \ldots + a_nx_n \mid x_1, \ldots x_n \in \mathbb{Z}\}$$

é um módulo de $\mathbb{Z}$.

Teorema 1.2.6 *Seja S um módulo de $\mathbb{Z}$. Então existe $g \in S$ tal que*

$$S = \{0, \pm g, \pm 2g, \ldots\} = g\mathbb{Z}.$$

Demonstração. Se $S = \{0\}$, tome $g = 0$ e nada há a demonstrar. Suponha então $S \neq \{0\}$. Seja $S_+ = \{x \in S \mid x > 0\}$. Da propriedade (i) da definição de módulo é fácil ver que $S_+ \neq \emptyset$. Pelo Princípio da Boa Ordenação, seja $g \in S_+$ tal que $g \leq x$, para todo $x \in S_+$.

Se $x \in S_+$ então, pelo algoritmo da divisão de Euclides, existem $q, r \in \mathbb{Z}$ tais que $x = qg + r$ e $0 \leq r < g$. Como $r = x - qg$ temos que $r \in S$, e do fato de r ser não negativo, ou temos $r = 0$ ou $r \in S_+$. A segunda opção comprometeria a minimalidade de g, logo $r = 0$ e $x = qg$, com $q \in \mathbb{Z}$.

Tudo isto mostra que S está contido em

$$\{0, \pm g, \pm 2g, \ldots\}.$$

Como a outra inclusão é trivial, a demonstração está terminada. □

Definição 1.2.7 Sejam $a, b \in Z$ não nulos. Definimos o *máximo divisor comum* (mdc) de a e b, denotado por (a, b), como sendo o maior inteiro que divide a e b simultaneamente.

Nas mesmas condições, definimos o *mínimo múltiplo comum* (mmc) de a e b, denotado por $\langle a, b \rangle$, como sendo o menor inteiro positivo múltiplo comum de a e b.

Exemplo 1.2.8 Vamos calcular o mdc e o mmc de 8 e 12. Para o cálculo de $(8, 12)$ precisamos listar os seus divisores positivos que são:

$$\begin{aligned} &\text{divisores de } 8: \quad 1, 2, 4, 8, \\ &\text{divisores de } 12: \quad 1, 2, 4, 6, 12, \end{aligned}$$

logo o máximo divisor comum é 4.

Agora vamos calcular $\langle 8, 12\rangle$. Os múltiplos positivos de 8 e 12 são da forma $8t$ e $12t$ com $t \in \mathbb{N}$, ou seja,

$$\begin{aligned} &\text{múltiplos de } 8: \quad 8, 16, 24, 32, \ldots, \\ &\text{múltiplos de } 12: \quad 12, 24, 36, 48, \ldots, \end{aligned}$$

portanto vemos que o mínimo múltiplo comum é 24.

O próximo teorema foi provado por Étienne Bézout (1730–1783), e nos mostra uma importante propriedade do mdc.

Teorema 1.2.9 (Bézout) *Sejam $a, b \in \mathbb{Z}$, não nulos e seja $d = (a, b)$. Então existem $r, s \in \mathbb{Z}$ tais que $d = ra + sb$.*

Demonstração. Seja $S = \{xa + yb \mid x, y \in \mathbb{Z}\}$. Sabemos que S é um módulo de $\mathbb{Z}$ e, portanto, pelo teorema 1.2.6, existe $d' \in S$ tal que

$$S = d'\mathbb{Z} = \{0, \pm d', \pm 2d', \ldots\}.$$

Assim, como $a, b \in S$, segue que $a = \alpha d'$ e $b = \beta d'$, para algum par de inteiros α e β. Ou seja, $d' \mid a$ e $d' \mid b$. Como d' é um divisor comum de a e b, por definição, temos que $d' \leq d = (a, b)$.

Por outro lado, segue do lema 1.2.2 que $d \mid na + mb$, para todos os pares $n, m \in \mathbb{Z}$. Em particular, d divide d', e logo temos que $d = d'$, como queríamos demonstrar. □

Euclides, no livro VII de sua célebre obra *Elementos*, apresenta um algoritmo para obtenção do mdc de dois inteiros positivos $a \in b$, que consiste no seguinte.

> Se $a = b$, então $(a, b) = a$. Suponha então que temos $b < a$, e vamos seguir os seguintes passos:

(1) Existem $q_0, r_1 \in \mathbb{N} \cup \{0\}$ tais que
$a = bq_0 + r_1 \in 0 \leq r_1 < b$.

Se $r_1 \neq 0$, então

(2) existem $q_1, r_2 \in \mathbb{N} \cup \{0\}$ tais que
$b = q_1 r_1 + r_2, 0 \leq r_2 < r_1$.

Se $r_2 \neq 0$, então

(3) existem $q_2, r_3 \in \mathbb{N} \cup \{0\}$ tais que
$r_1 = q_2 r_2 + r_3, 0 \leq r_3 < r_2$.

Continuando este processo, caso os r_i anteriores sejam não nulos, no k-ésimo passo teremos:

(k) Existem $q_{k-1}, r_k \in \mathbb{N} \cup \{0\}$ tais que
$r_{k-2} = q_{k-1} r_{k-1} + r_k, 0 \leq r_k < r_{k-1}$.

Como existe um número finito de inteiros entre $0 \in b$, e a cada passo do algoritmo acima, determinamos um r_k onde

$$0 \leq r_k < r_{k-1} < \cdots < r_1 < b,$$

certamente existirá um primeiro inteiro n tal que $r_{n+1} = 0$. Convidamos agora o leitor a mostrar que $r_n = (a, b)$ (veja exercício 5 no final deste capítulo).

Exemplo 1.2.10 Vamos utilizar este algoritmo para calcular o mdc de 60 e 27. Começamos escrevendo

$$\begin{aligned} 60 &= 27 \times 2 + 6 \quad \text{logo} \quad q_0 = 2 \quad \text{e} \quad r_1 = 6, \\ 27 &= 6 \times 4 + 3 \quad \text{logo} \quad q_1 = 4 \quad \text{e} \quad r_2 = 3, \\ 6 &= 3 \times 2 + 0 \quad \text{logo} \quad q_2 = 2 \quad \text{e} \quad r_3 = 0. \end{aligned}$$

Como $r_3 = 0$, concluímos que

$$r_2 = 3 = (60, 27).$$