Um Curso Básico em Teoria dos Números

Textuniversitários 7

Vandenberg Lopes Vieira

Um Curso Básico em *Teoria dos Números*

Este livro foi finalista do 58º prêmio Jabuti, concorrendo na categoria de Engenharias, Tecnologias e Informática

LF EDITORIAL

Editora Livraria da Física
São Paulo – 2020

1a. Edição

Editor: 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)

Vieira, Vandenberg Lopes
Um curso básico em teoria dos números / Vandenberg Lopes Vieira. – 2. ed. – São Paulo : Editora Livraria da Física, 2020. – (Série textuniversitários ; 7)

Bibliografia.
ISBN 978-85-7861-651-9

1. Teoria dos números I. Título. II. Série.

20-33191 CDD-512.7

Índices para catálogo sistemático:

1. Teoria dos números : Matemática 512.7

Cibele Maria Dias – Bibliotecária – CRB-8/9427

ISBN 978-85-7861-651-9

Impresso no Brasil
Printed in Brazil

LF EDITORIAL

Editora Livraria da Física
Tel./Fax: +55 11 3459-4327 / 3936-3413
www.livrariadafísica.com.br

A minha família

DEDICO

O Senhor com sabedoria fundou a terra,
com inteligência estabeleceu os céus.

Provérbios 3:19

Prefácio da Primeira Edição

A Teoria dos Números foi sem dúvidas o ramo de pesquisa favorito de Gauss, que uma vez disse: *"A Matemática é a rainha das ciências e a Teoria dos Números é a rainha da Matemática"*. Esta notável frase, dada por aquele que é considerado o maior matemático de todos os tempos, resume bem a importância da Teoria dos Números como um ramo da Matemática Pura, cujos problemas a tornam essencialmente diferente de outros ramos.

Os antigos teóricos dos números não desenvolviam resultados com a finalidade de que eles um dia viessem a ser aplicados em problemas do cotidiano. A elegância e desafios desses resultados eram suficientes para atraí-los. Isso também é verdade para os atuais estudiosos da área. Atualmente, aplicações em diversas áreas tais como Física, Química, Acústica, Biologia, Computação, Codificação e Criptografia, fazem da Teoria dos Números mais atraente, ao menos para os leigos que se deleitam em aplicações da Matemática em problemas do dia a dia.

A Teoria dos Números se dedica ao estudo dos números inteiros e suas generalizações. Em geral, esse estudo está relacionado com soluções de problemas diofantinos, ou seja, problemas que requerem solução de equação ou de sistema de equações com valores inteiros para as suas incógnitas. Entre os seus vários ramos, três têm destaque especial: *a Teoria Algébrica*, a *Teoria Analítica* e a *Teoria Elementar*. Em outras palavras, é possível observar o estudo dos números inteiros sob ao menos três pontos de vista diferentes.

Na Teoria Algébrica se estuda os *números algébricos* (números complexos que são raízes de polinômios não nulos com coeficientes racionais) e considera resultados da Álgebra Abstrata a fim de resolver as questões inerentes. A Teoria Analítica emprega resultados da Análise Matemática, tanto real como complexa, quando do estudo mais aprofundado sobre os números primos. Por outro lado, a Teoria Elementar, cujos tópicos estudados se constituem num primeiro contato dos estudantes com as propriedades dos números inteiros, tem por objetivo estudar os conceitos e resultados básicos sobre divisibilidade, primalidade, congruência entre inteiros, frações contínuas, etc. Esses conceitos são essenciais para se estudar os outros ramos da Teoria dos Números.

Objetivos do livro

O objetivo principal deste livro é destacar os resultados básicos e clássicos da Teoria Elementar dos Números, de modo a oferecer um texto para um primeiro curso em Teoria dos Números. O texto não aborda nenhuma parte dedicada a aplicações dos conceitos em outras áreas (algo que pode ser facilmente encontrado nas referências [1], [25] e [38]), mas tem a finalidade de estudá-los de forma mais natural possível, dotando o leitor de conhecimentos necessários para o estudo mais avançado da teoria.

O texto foi escrito focalizando principalmente os estudantes de Licenciatura em Matemática, mas levando em consideração que muitos assuntos abordados são estudados por estudantes de outras áreas, tais como Ciência da Computação e Engenharia Elétrica. Isso não significa que o rigor inerente não apenas à Teoria dos Números, mas também à Matemática foi deixado de lado. À luz desse foco, fomos persuadidos a considerar duas coisas essenciais. A primeira concerne à apresentação dos exemplos. É imprescindível que eles sejam abordados com mais detalhes e com grau de dificuldade crescente, o que pode ser decisivo para que o leitor possa assimilar com mais acuidade os conceitos envolvidos. A segunda diz respeito às expressões como "fácil ver" e "é imediato", tão comuns em textos matemáticos, sejam realmente coerentes, sem a conotação de desprezo para com o leitor, mas que expressem o fato de que alguns detalhes superficiais de um determinado resultado foram compactados.

Os tópicos escolhidos para a elaboração do texto são em sua maioria clássicos da teoria, de modo que o que pode diferenciar este livro dos muitos disponíveis é a forma com que cada um deles é apresentado. Ao realizarmos a tarefa de escolha, tivemos o cuidado (ao menos nos esforçamos para isso) de atingir ao máximo os conteúdos relacionados à Teoria Elementar. É claro que, de certa forma, isto exprime um pouco da experiência obtida por meio dos cursos que ministramos em Teoria dos Números, tanto na graduação como no mestrado profissional em Matemática. Isto significa que alguns temas abordados em outros livros podem não ser encontrados neste, mas isso em nada interfere em seu objetivo central.

Outra coisa importante a ser destacada é sobre os pré-requisitos. Seguramente, neste livro, eles são mínimos, pois os conceitos necessários ao seu desenvolvimento são em geral previamente apresentados. Uma ligeira exceção é feita quando da necessidade do uso de resultados relacionados à Análise Matemática (no estudo sobre frações contínuas e equação de Pell), mas na ocasião fazemos esclarecimento a respeito.

Em linhas gerais, acreditamos que o livro é útil a todo estudante, seja de Matemática, Ciência da Computação ou Engenharia Elétrica, que tem o objetivo de fazer um curso de introdução em Teoria Elementar dos Números que aborde os seus principais tópicos.

A estrutura do livro

O livro é constituído de doze capítulos. No que segue, temos uma pequena descrição de cada um deles.

O Capítulo 1 segue o padrão de alguns livros. Ele se inicia efetivamente com uma fundamentação axiomática dos números inteiros, destacando as propriedades relativas à adição e à multiplicação de inteiros, como também as relacionadas à relação de ordem usual. Após isso, são apresentados o Princípio da Boa Ordenação e o Princípio de Indução Finita em suas duas formas. É na verdade um capítulo base e, por isso, importante para se estabelecer resultados de outros capítulos. Ele se encerra com a seção dedicada ao Binômio de Newton.

No Capítulo 2, consideramos o conceito de divisibilidade sobre o conjunto dos números inteiros, sendo o Algoritmo da Divisão seu resultado principal. A Seção 2.3 aborda sistemas de numeração e, a partir de seus resultados, apresentamos alguns critérios de divisibilidade. Esta seção se constitui num intervalo interessante entre a primeira e à que destaca os conceitos de máximo divisor comum e mínimo múltiplo comum.

Os números primos são estudados no Capítulo 3. Seria até possível unir os resultados deste capítulo com os do anterior. Mas, devido à importância do tema, preferimos abordá-los num capítulo à parte. O Teorema Fundamental da Aritmética tem destaque especial, cujo resultado nos mostra de forma implícita que os números primos são os mais importantes números inteiros. Destacamos também o Crivo de Eratóstenes, as funções $\tau(n)$ e $\sigma(n)$, que são exemplos clássicos de funções multiplicativas (conceito este estudado mais adiante), e finalizamos com a seção sobre a distribuição dos números primos. Este último tema se apresenta de forma resumida, pois ele é objeto de estudo da Teoria Analítica. A referência [2] aborda isso com muita propriedade.

No Capítulo 4, apresentamos o conceito de *congruência*, o qual é um dos mais importantes da Teoria dos Números. Para que se possa entender os resultados de capítulos mais substanciais, tais como os dos Capítulos 6 e 8, é necessário que se faça uma leitura com muita acuidade deste. Estudamos de forma detalhada as principais propriedades das congruências, incluindo algumas aplicações. Após isso, as congruências lineares seguem de forma natural e, como não poderia deixar de ser, apresentamos o Teorema Chinês dos Restos, que é um clássico do assunto. Aproveitamos este capítulo para estudar as equações diofantinas lineares com duas incógnitas e finalizamos com a construção de um importante conjunto, não apenas para a Teoria dos Números, como também para a Álgebra Abstrata – o conjunto das classes de congruência módulo m, $\mathbb{Z}_m$ – abordando suas operações de adição e multiplicação com suas propriedades.

Alguns números especiais no sentido dado no texto são apresentados no Capítulo 5. Entre esses, destacamos os números perfeitos, de Fermat e de Mersenne. Esses números despertam interesse especial, pois são fonte de pesquisas científicas. Entre os resultados deste capítulo, há o teorema que caracteriza os números perfeitos pares, devido a Euclides e Euler.

No Capítulo 6 são apresentados três importantes teoremas que envolvem congruências: os Teoremas de Wilson, de Fermat (o pequeno) e o de Euler. O Teorema de Wilson é na verdade um critério de primalidade, embora não seja usado na prática para este fim. Já o de Fermat estabelece uma congruência base importante, assim como o de Euler, o qual generaliza o resultado dado pelo de Fermat. Há uma parte do texto dedicada à função ϕ de Euler com algumas de suas propriedades.

No capítulo 7, consideramos o conceito de função aritmética, objetivando o estudo das funções multiplicativas. Dentre essas, destacamos a função μ de Möbius, que é uma das mais importantes. Essa função desempenha um papel central na fórmula de inversão (um clássico da Teoria dos Números) que relaciona duas funções aritméticas F e f, em que f é arbitrária não necessariamente multiplicativa.

O estudo sobre Ordens e Raízes Primitivas é dado no Capítulo 8, o qual apresenta os resultados clássicos inerentes, incluindo, é claro, a caracterização dos inteiros que possuem raízes primitivas. Ele destaca também alguns resultados sobre o conceito de índice, que foi primeiro introduzido por Gauss em seu *Disquisitiones Arithmeticae* e que está relacionado com o conceito de raiz primitiva. Algumas propriedades de índice são fundamentais para se estudar congruências da forma $x^k \equiv a \pmod{m}$, em que k é um inteiro positivo.

No Capítulo 9 é apresentado um dos mais importantes problemas da Teoria dos Números, a saber, a solução de congruências quadráticas da forma $x^2 \equiv a \pmod{p}$, em que $p > 2$ é primo e a um inteiro tal que $\mathrm{mdc}(a, p) = 1$. Para tanto, faz-se necessário o uso de conceitos e resultados clássicos da área, entre os quais se destaca de modo especial a Lei da Reciprocidade Quadrática, que é uma das grandes contribuições de Gauss à Teoria dos Números.

Algumas equações diofantinas são estudadas no Capítulo 10. É um assunto extremamente vasto, de modo que o capítulo traduz uma simples apresentação do mesmo. Caracterizamos as soluções da famosa equação de Pitágoras $x^2 + y^2 = z^2$ e, a partir dela, estudamos outras equações. Apresentamos também o método clássico de descida infinita de Fermat. Finalizamos o capítulo caracterizando as soluções inteiras positivas da equação $x^2 - dy^2 = 1$, em que $d > 1$ não é um quadrado perfeito, que é conhecida como uma equação de Pell. Para este fim, consideramos um ambiente de estudo mais abrangente do que o conjunto dos números inteiros – o conjunto $X_d = \{x + y\sqrt{d} : x, y \in \mathbb{Z}\}$ dotado de suas operações usuais. Isso foi feito devido à fatoração $x^2 - dy^2 = (x + y\sqrt{d})(x - y\sqrt{d})$.

Três problemas diofantinos clássicos são tratados no Capítulo 11: a caracterização dos inteiros que são somas de dois, três e quatro quadrados. Tais problemas sempre despertaram interesse entre os matemáticos, e alguns inerentes ainda são fonte de pesquisas científicas. Os teoremas relativos à soma de dois quadrados e à de quatro quadrados foram provados de uma forma completa. Quanto à soma dos três quadrados, sua caracterização, dada pelo Teorema dos Três Quadrados de Gauss, tem uma prova muito longa e sofisticada. Por isso, foi apresentada apenas a prova da condição necessária.

No Capítulo 12 são estudadas as frações contínuas finitas e as infinitas. Assim como o tema do Capítulo 10, é um tema amplo e, por isso, apresentamos apenas os tópicos básicos e importantes. Destacamos de forma especial um método clássico de obtenção de aproximações de irracionais por racionais. As referências [13], [18] e [29] são excelentes para o leitor se aprofundar nos tópicos estudados no capítulo.

Finalmente, encerramos o livro com um apêndice que destaca o conceito de *relação de equivalência* e outros inerentes. Isso foi feito objetivando o estudo sobre o conjunto das classes de congruência módulo m. Mas é claro que os resultados apresentados são essenciais para a construção formal do conjunto $\mathbb{Z}$ a partir de $\mathbb{N}$, bem como à do conjunto $\mathbb{Q}$ a partir de $\mathbb{Z}$, algo que não foi feito neste livro. Para este fim, indicamos a referência [8].

Os exercícios propostos

Existem 542 exercícios propostos no livro, os quais foram dispostos numa ordem crescente com respeito ao nível de dificuldade. A maioria deles tem a finalidade de fixar a aprendizagem, enquanto uma pequena parte surge como uma forma de acrescentar algo à teoria apresentada no texto. Em geral, os exercícios são apresentados em três níveis: fácil, médio e difícil. Alguns exercícios contêm mais de quatro itens, o que pode tornar algo repetitivo. Mas, resolver todos ou não é uma decisão que só cabe ao estudante. Se ele já se sente seguro sobre os conceitos exigidos em um dado exercício, então não há motivos para que se resolva do item (a) ao item (d), por exemplo. Já ciente disso, ele será automaticamente convidado a encarar seu próximo desafio, um problema de outro nível ou que envolva outros conceitos.

Os exercícios marcados com asterisco ($*$) são os que exigirão um pouco mais de empenho do aluno, forçando-o a obter mais profundidade no trato dos conceitos relacionados. Sabemos o quanto esses são desafiadores para os estudantes e que podem levá-los a certo pânico. No entanto, não foram colocados para este fim, mas foram selecionados para quem deseja gastar um pouco mais de energia.

Muitas vezes nos dedicamos exaustivamente na solução de um problema considerado difícil. Mesmo assim podemos não resolvê-lo. É claro que isso pode trazer algum desânimo, mas quando se dedica um tempo extra na solução de um exercício dessa natureza, mesmo que não haja “sucesso”, é inegável que algo da teoria é assimilada, e isso será útil em ocasião oportuna. Desse modo, o leitor não deve se sentir desencorajado a encarar os exercícios marcados com as famosas estrelinhas.

No final do livro estão as respostas de alguns exercícios, os que não têm caráter demonstrativo. É aconselhável que uma consulta a essa parte seja considerada como último recurso e que seja feita após algumas tentativas de solução. Não é conveniente que o estudante ao menor sinal de dificuldade recorra automaticamente às repostas dadas. Isso pode trazer prejuízo ao seu aprendizado, podendo levá-lo a ser um simples espectador.

Uma palavra aos estudantes

A partir da nossa experiência como estudante e principalmente agora como professor, queremos chamar a atenção de todo aquele que porventura venha a estudar por este livro. As seções dos exercícios propostos de um livro-texto despertam muito interesse nos alunos, sendo um atrativo à parte. Por isso, é perfeitamente compreensível que os mais afoitos busquem o mais rápido possível se debruçar nos exercícios.

Por mais delineados que sejam ministrados os conteúdos, é quase que impossível para o professor apresentar todos os detalhes de um dado tópico em sala de aula. Após cada aula sobre um determinado conteúdo, é razoável que o estudante estabeleça o hábito de se fazer um estudo do que foi visto, analisando com bastante atenção os exemplos trabalhados, uma vez que, em geral, eles são uma fonte de informações que pode auxiliar nas resoluções dos problemas e ajudar a fixar se não todas, mas as principais ideias. Em seguida, ele deve procurar resolver os exercícios propostos, começando com os mais fáceis, e quem sabe, indo até aos mais difíceis. Na medida do possível, é apropriado estabelecer um procedimento de estudo, tornando-o o mais agradável e interessante possível. Isso pode ser útil e decisivo em seu aprendizado.

Leia cada seção do texto pausadamente, reescrevendo sempre que necessário cada definição e resultado. Às vezes, você terá que ler uma parte do texto mais de uma vez, revendo os exemplos, teoremas, demonstrações, etc. Se houver necessidade para isso, faça com dedicação.

Agradecimentos

Algumas pessoas contribuíram para a apresentação final do livro e desejamos por isso agradecê-las. Expressamos nossos sinceros agradecimentos aos colegas professores Vilmar Vaz, José Ginaldo e Luciana Roze, que se dispuseram em ler partes do texto. Suas sugestões e críticas contribuíram de forma significativa, melhorando-o em alguns aspectos, além de nos permitir corrigir erros minuciosos. Agradecemos ainda a Wanderson Guimarães e a Kézia Patrícia pelas contribuições nas ilustrações, e ao Professor Euler Franco pelas sugestões em algumas citações.

Finalmente, nossa gratidão aos alunos do curso de Licenciatura Plena em Matemática da Universidade Estadual da Paraíba – UEPB, bem como a todos os autores dos livros que foram base para a elaboração deste texto.

Críticas e sugestões

Desde já agradecemos ao leitor que se dispuser em nos comunicar sobre os erros contidos no texto que porventura venham a ser detectados, os enviando para os e-mails: `vandenberglv@uepb.edu.br` ou `vandenberglv@yahoo.com.br`. O leitor poderá também enviar seus comentários, críticas, correções e sugestões. Todos serão bem-vindos e analisados com bastante atenção, podendo ser incorporados na próxima edição.

VANDENBERG LOPES VIEIRA
Campina Grande, agosto de 2015

Prefácio da Segunda Edição

O que essencialmente diferencia esta edição da primeira são sutis mudanças em algumas partes do texto, inclusão de outras e correções de erros de digitação. Agradecemos aos leitores que colaboraram neste sentido. Também é notória a alteração no tamanho da fonte, visando melhor adequação ao número de páginas.

Aproveitamos, também, para apresentar alguns exercícios acrescidos de mais de 50 exemplos, objetivando dar mais suporte ao leitor na resolução dos exercícios propostos.

Nossa gratidão a todos os professores e alunos que adotaram o livro como livro-texto. A boa aceitação do mesmo é para nós motivo de alegria, quando desejamos que ele siga desempenhando o papel que lhe fora outorgado. Por fim, agradecemos à LF Editorial pela contribuição e confiança.

Vandenberg Lopes Vieira

Campina Grande, março de 2020

Sumário