TEORIA DOS NÚMEROS

RENATO BELINELO BORTOLATTO

TEORIA DOS NÚMEROS

Uma abordagem didática com aplicações à criptografia

EDITORA UNICAMP

SISTEMA DE BIBLIOTECAS DA UNICAMP
DIVISÃO DE TRATAMENTO DA INFORMAÇÃO
Bibliotecária: Gardênia Garcia Benossi – CRB-8ª / 8644

B648t Bortolatto, Renato Belinelo
Teoria dos números : uma abordagem didática com aplicações à criptografia / Renato Belinelo Bortolatto – Campinas, SP : Editora da Unicamp, 2025.

1. Matemática. 2. Ensino. 3. Teoria dos números. 4. Criptografia. I. Título.

CDD – 510
– 371.3
– 511
– 511.8

ISBN: 978-85-268-1795-1

Foi feito o depósito legal.

Editora associada à

Associação Brasileira das Editoras Universitárias

Direitos reservados a

Editora da Unicamp
Rua Sérgio Buarque de Holanda, 421 – 3º andar
Campus Unicamp
CEP 13083-859 – Campinas – SP – Brasil
Tel.: (19) 3521-7718 / 7728
www.editoraunicamp.com.br – vendas@editora.unicamp.br

Para meus companheiros de viagem,
os que estão próximos e os que estão longe.

"*Dois problemas se misturam:*
a verdade do universo e a prestação que vai vencer."

Raul Seixas e Paulo Coelho
"Eu Também Vou Reclamar"

Sumário

Apresentação

Este é um livro didático de introdução à teoria dos números. Desta forma, não tem objetivo de apresentar um tratamento conciso, completo ou apenas formal do assunto. Para o leitor interessado na abordagem mais direta, a referência mais popular é o livro de Hardy e Wright, que, apesar de já ter certa idade, foi revisto recentemente por Silverman, um dos mais importantes especialistas da área.

Para explicar melhor a origem deste livro, é conveniente começarmos com uma breve digressão. Meu interesse por teoria dos números, como é o caso de muitos estudantes, remete aos meus tempos de colégio; minha memória mais forte é da oitava série, com a leitura de *O homem que calculava*, de Malba Tahan, motivado pelo professor João, um engenheiro de formação que em algum momento descobriu grande paixão pelo ensino de Matemática. Há pouco tempo também me lembrei de ter lido *O último teorema de Fermat*, de Simon Singh, quando eu estava no colegial, e de ter tentado provar que a equação cúbica não admitia soluções inteiras. Eu pensava que esse caso particular não podia ser tão difícil de mostrar, mas logo desisti. Um colega de colegial, hoje também matemático, comentou comigo anos depois que fazia iniciação científica nessa área, mas não me lembrei de perguntar para ele como resolver esse caso. No apêndice deste livro, apresento uma prova do teorema de Fermat no caso $n = 3$, prova que só foi possível graças ao livro *Fermat's last theorem for amateurs*, de Paulo Ribenboim, obra a que tive acesso apenas nos últimos anos. A prova, além de ter como pré-requisito a maior parte deste livro, é a que considero mais difícil de todo o texto. Então, se você tiver dificuldade em entendê-la, está em boa companhia.

Apesar de meus estudos terem aos poucos convergido para outros assuntos, eu continuei por conta própria a ler livros e artigos relacionando à teoria dos números e a outros assuntos conforme os anos passavam. Quando vim para o ITA, havia a possibilidade de ofertar disciplinas eletivas de nosso interesse, o que foi para mim uma escolha natural. Após aprovação da ementa e no momento certo, consegui ofertar a disciplina... por três semanas. Era o começo da pandemia de covid-19.

A primeira versão deste livro foi escrita principalmente nesse período, sendo a única forma razoável que eu conseguiria administrar para interagir com os estudantes. Eu já tinha, sim, um rascunho inicial de curso, mas este texto divergiu bastante do original em diversos aspectos. Quando comecei a primeira revisão do material digitado, encontrei poucos pontos importantes que precisaram ser mudados drasticamente, o que me surpreendeu, pois muita coisa foi escrita diretamente no teclado e com sérias restrições de tempo.

O estilo da escrita é bastante discursivo, buscando sempre motivar cada resultado e explicitar ideias dentro de demonstrações. Isso foi planejado, é claro, para funcionar como um substituto da aula presencial ou em vídeo, mas quero notar que vejo isso como uma forma de comunicação natural em livros didáticos, principalmente quando os estudantes estão entrando em contato pela primeira vez com conceitos abstratos e com a forma de argumentação própria da cultura matemática.

Um dos objetivos deste curso é fazer uma primeira apresentação de aspectos computacionais da teoria dos números, tanto dos algoritmos de resolução no papel quanto da sua implementação, além de apresentar questões sobre a complexidade computacional das soluções. Como percebi que os estudantes se sentem muito intimidados com a programação, apenas escrevi códigos quando julguei que adicionam algo fundamental para a explicação. Nesse caso os códigos são apresentados sem especificação de linguagem, o que deve facilitar o entendimento e servir de modelo para exercícios nessa linha. Para estudantes de Ciência da Computação, por exemplo, é possível que o professor peça até mesmo exercícios-programa em sua avaliação.

Enfatizo a interpretação geométrica dos problemas, em especial na direção de interpretá-los com auxílio de *lattices*, que são frequentemente

traduzidos como *reticulados* em português. Permeei a história da Matemática por muitos temas, servindo de fator motivador de muitas discussões e passando por diversas regiões geográficas e épocas. Também são feitas referências a resultados mais atuais como direcionamento de estudo e remetendo à história quase que atual da Matemática.

Ainda com a intenção de apresentar a teoria de forma mais contemporânea, introduzi rapidamente a linguagem de funções aritméticas e faço referências à base de pesquisa OEIS. Alguns resultados sobre a média de funções aritméticas são discutidos no texto, usando resultados de Cálculo. Por outro lado, tomamos caminhos bastante clássicos quando iniciamos com uma abordagem axiomática, tomamos o tempo que julgamos necessário para definir congruências e fazemos o estudo da equação biquadrada diretamente com ideias de Fermat.

Este contraste entre modernidade e antiguidade que cerca a teoria dos números e guia o livro reflete o público para o qual foi pensado. Os estudantes que assistem ao curso são muito interessados em matemática e dominam seus aspectos elementares. Muitos já participaram, e ainda participarão, de olimpíadas e sabem usar congruências, por exemplo, com grande habilidade, apesar de terem dificuldade em entender esse conceito como parte de uma teoria. Enquanto sabem aplicar muito rapidamente critérios de divisibilidade em base 10, relatam nunca terem feito a prova desses fatos, provas essas que são bastante elementares.

Para os estudantes em estágios mais avançados, incluí no final de cada capítulo um tema avançado em continuação natural à discussão do tema. Há pouco *hand-holding* nessas seções, de forma proposital: espera-se que o leitor as leia com lápis e computador na mão e preencha os detalhes omitidos. Os estudantes que estão entrando em contato com a teoria pela primeira vez podem evitar essas seções ou passar por elas de forma breve, sem prejuízo do entendimento do restante do texto. Procedendo dessa forma, creio que o resultado final é acessível ao público geral, respeitando a maturidade de cada leitor, e por qualquer trajeto escolhido não deixa de abordar assuntos interessantes e não elementares que frequentemente não são discutidos em cursos iniciais.

Os exercícios foram escolhidos de forma a cobrir os assuntos com extensão e em quantidade compatível com as horas de estudo esperadas,

sem exageros. Há uma boa quantidade de exercícios puramente práticos que consistem em aplicação de algoritmos, um passo necessário antes de maiores abstrações. Os exercícios teóricos começam fáceis, pensados para treinar o aluno a escrever provas, e progridem em dificuldade conforme o curso avança. Todos têm respostas no formato de dicas, de forma que o estudante tenha ao menos um roteiro para entender o que precisa fazer em cada um. Só recomendo a leitura das dicas após o esgotamento do tempo ou de ideias para a resolução do problema.

Os estudantes são incentivados a continuar seus estudos a partir de temas que julguem interessantes, e há indicação de bibliografia para isso. São incentivados também a continuar a estudar para participar de olimpíadas, razão pela qual uso os termos *gcd* e *lcm* em vez de *mdc* e *mmc*, respectivamente. Acredito também que a extensão e a profundidade dos temas abordados aqui formam uma base adequada para o aluno iniciar a leitura de algum artigo simples em iniciação científica, daí o motivo da inclusão de cada um dos temas, ainda que as discussões finais apresentem uma dificuldade considerável para um primeiro curso.

Para a referência do professor, considerando aulas de dúvidas, eventuais feriados e avaliações, creio que o conteúdo é adequado para um curso semestral de quatro horas-aula semanais, sendo os capítulos dedicados a temas cuja duração pode variar entre uma e duas semanas, dependendo do que julgar interessante omitir ou destacar para a turma. Penso que estudantes do ensino médio que tenham interesse pela teoria dos números e por competições olímpicas podem fazer uma primeira leitura focada nos capítulos de 1 a 7. Turmas de graduação em matemática podem ir até o capítulo 10, eventualmente fazendo apenas uma apresentação breve do teorema da reciprocidade quadrática. Turmas de computação podem fazer o mesmo, mas incluindo uma apresentação do capítulo 11, para isso podendo, se necessário, pular o primeiro capítulo. Os capítulos 6 e 12 podem ser lidos de forma independente pelos estudantes como atividade extra se houver restrições de tempo. Estudantes que tenham interesse em participar de olimpíadas universitárias ou de uma pós-graduação devem ler o texto na íntegra, incluindo os tópicos adicionais que podem ser considerados atividade extra-sala para os outros.

Para a referência dos estudantes, especialmente aqueles que estudarão por conta própria, é importante saber *a priori* que os capítulos finais têm grau de dificuldade elevado. A prova do teorema da reciprocidade quadrática, por exemplo, é delicada e abstrata, mesmo com todo esforço feito para torná-la acessível. O mesmo pode ser dito sobre a caracterização dos casos em que existem raízes λ-primitivas. No entanto, não é esperado que você entenda todos os detalhes e saiba replicar essas provas após uma primeira leitura. São provas difíceis também para os professores e requerem um tempo de preparação de aula adicional. O que é esperado de você é mais próximo das listas de exercícios, que incluem, por exemplo, exercícios de contas. Não deixe de ler esses capítulos, ainda que você sinta que não é possível entendê-los por inteiro em um primeiro momento.

Por fim, gostaria de agradecer a revisão final feita pelo Prof. Samuel Augusto Wainer. Desde o início deste projeto, quis incluir alguém que tivesse mais conhecimento e experiência em Álgebra do que eu para incluir sua percepção, pensando que este também pode ser um curso preparatório para as disciplinas dessa área. Não tenho dúvidas de que o trabalho como apresentado aqui foi enriquecido por sua colaboração.

1 - Inteiros

Neste capítulo iniciamos nosso estudo dos números inteiros a partir de um sistema de axiomas, de forma semelhante ao tratamento de Euclides para a geometria. Discutimos consequências dos axiomas que justificam o tratamento costumeiro da aritmética nos inteiros e terminamos a discussão mostrando e aplicando o princípio da indução finita a que recorremos com frequência em nosso estudo.

Como tópico adicional, fazemos uma primeira apresentação dos conceitos de consistência e completude para sistemas axiomáticos e fazemos menção aos teoremas de Göedel.

1.1 Um sistema axiomático para os inteiros

Um axioma é uma afirmação que assumimos ser verdadeira. O objetivo da abordagem axiomática é conseguir, a partir de uma quantidade razoável de suposições, preferencialmente "pequena", conseguir deduzir, de acordo com a lógica proposicional, novos resultados de natureza mais sofisticada, que chamamos de proposições, lemas e teoremas. A lógica proposicional tem como principal ferramenta o *modus ponens*, que por este momento explicamos como

> Se sabemos que P implica Q e
> Se sabemos que P é verdadeiro
> Então Q é verdadeiro.

O uso do *modus ponens* requer que assumamos que ao menos duas afirmações sejam verdadeiras (no caso "P implica Q" e "P"). Não é

possível, portanto, construirmos uma teoria desta forma sem assumirmos algumas proposições como verdadeiras.

O *modus ponens* é, portanto, apenas uma regra de inferência lógica e, ao mesmo tempo que requer existência de axiomas para ser efetivamente aplicado, não leva em consideração a razoabilidade dos axiomas. Uma escolha cuidadosa de axiomas é o que determina a qualidade de uma teoria. Um exemplo que você já deve conhecer são os axiomas de Euclides para a geometria. Assumimos que:

(E1) Podemos traçar uma reta ligando dois pontos distintos.

(E2) Podemos estender um segmento de reta nas duas direções.

(E3) Podemos construir um círculo com centro e raio prescritos.

(E4) Todos os ângulos retos são iguais.

(E5) Em um plano, dada uma reta r e um ponto P fora dela, é possível determinar uma única reta paralela a r passando por P.

As quatro primeiras afirmações soam de fato tão elementares que mal podemos imaginar como desenvolver qualquer geometria sem elas. São afirmações baseadas inclusive na nossa experiência (você sabe como desenhar uma reta ligando dois pontos!), e fazer uma geometria sem elas levanta questões até sobre sua utilidade.

No entanto, o último axioma (nesta forma, conhecido como axioma de John Playfair) caracteriza a geometria Euclideana. Munidos desses cinco axiomas, podemos, por exemplo, provar o Teorema de Pitágoras, o Teorema de Tales e que a soma dos ângulos internos de um triângulo é π. Nenhuma dessas afirmações é válida sem o axioma de Playfair (ou um axioma equivalente), o que deixa dizer que não são resultados simples. São de fato resultados notáveis, de aplicação prática e não imediatamente intuitivos o suficiente para serem colocados como axiomas.

O tratamento axiomático de Euclides consta em *Os elementos*, escrito por volta de 300 AEC (antes da era comum). A necessidade de um tratamento axiomático para os naturais começa a ficar clara por volta