Undergraduate Texts in Mathematics

Undergraduate Texts in Mathematics

Undergraduate Texts in Mathematics are generally aimed at third- and fourth-year undergraduate mathematics students at North American universities. These texts strive to provide students and teachers with new perspectives and novel approaches. The books include motivation that guides the reader to an appreciation of interrelations among different aspects of the subject. They feature examples that illustrate key concepts as well as exercises that strengthen understanding.

More information about this series at http://www.springer.com/series/666

Ramin Takloo-Bighash

A Pythagorean Introduction to Number Theory

Right Triangles, Sums of Squares, and Arithmetic

Springer

Ramin Takloo-Bighash
Department of Mathematics, Statistics,
and Computer Science
University of Illinois at Chicago
Chicago, IL, USA

ISSN 0172-6056 ISSN 2197-5604 (electronic)
Undergraduate Texts in Mathematics
ISBN 978-3-030-02603-5 ISBN 978-3-030-02604-2 (eBook)
https://doi.org/10.1007/978-3-030-02604-2

Library of Congress Control Number: 2018958346

Mathematics Subject Classification (2010): 11-01, 11A25, 11H06, 11H55, 11D85

This Springer imprint is published by the registered company Springer Nature Switzerland AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

To Paria, Shalizeh, and Arad.
In the memory of my father.

Preface

This book came out of an attempt to explain to a class of motivated students at the University of Illinois at Chicago what sorts of problems I thought about in my research. In the course, we had just talked about the integral solutions to the Pythagorean Equation and it seemed only natural to use the Pythagorean Equation as the context to motivate the answer. Basically, I motivated my own research, the study of rational points of bounded height on algebraic varieties, by posing the following question: What can you say about the number of right triangles with integral sides whose hypotenuses are bounded by a large number X? How does this number depend on X? In attempting to give a truly elementary explanation of the solution, I ended up having to introduce a fair bit of number theory, the Gauss circle problem, the Möbius function, partial summation, and other topics. These topics formed the material in Chapter 13 of the present text.

Mathematicians never develop theories in the abstract. Despite the impression given by textbooks, mathematics is a messy subject, driven by concrete problems that are unruly. Theories never present themselves in little bite-size packages with bowties on top. Theories are the afterthought. In most textbooks, theories are presented in beautiful well-defined forms, and there is in most cases no motivation to justify the development of the theory in the particular way and what example or application that is given is to a large extent artificial and just "too perfect." Perhaps students are more aware of this fact than what professional mathematicians tend to give them credit for—and in fact, in the case of the class I was teaching, even though the material of Chapter 13 was fairly technical, my students responded quite well to the lectures and followed the technical details enthusiastically. Apparently, a bit of motivation helps.

What I have tried to do in this book is to begin with the experience of that class and take it a bit further. The idea is to ask natural number theoretic questions about right triangles and develop the necessary theory to answer those questions. For example, we show in Chapter 5 that in order for a number to be the length of the hypotenuse of a right triangle with coprime sides, it is necessary and sufficient that all prime factors of that number be of the form $4k + 1$. This result requires determining all numbers that are sums of squares. We present three proofs of this fact:

using elementary methods in Chapter 5, using geometric methods in Chapter 10, and using linear algebra methods in Chapter 12. Since primes of the form $4k + 1$ are relevant to this discussion, we take up the study of such primes in Chapter 6. This study further motivates the Law of Quadratic Reciprocity which we state in Chapter 6 and prove in Chapter 7. We also determine which numbers are sums of three or more squares in Chapters 9, 10, 11, and 12.

When I was in high school, I used to think of number theory as a kind of *algebra*. Essentially everything I learned involved doing algebraic operations with variables, and it did not look like that number theory would have anything to do with areas of mathematics other than algebra. In reality, number theory as a field of study sits at the crossroads of many branches of mathematics, and that fact already makes a prominent appearance in this modest book. Throughout the book, there are many places where geometric, topological, and analytic considerations play a role. For example, we need to use some fairly sophisticated theorems from analysis in Chapter 14. If you have not learned analysis before reading this book, you should not be disheartened. If anything, you should take delight in the fact that now you have a real reason to learn whatever theorem from analysis that you may not otherwise have fully appreciated.

Each chapter of the book has a few exercises. I recommend that the reader tries all of these exercises, even though a few of them are quite difficult. Because of the nature of this book, many of the ideas are not fully developed in the text, and the exercises are included to augment the material. For example, even though the Möbius function is introduced in Chapter 13, nowhere in the text is the standard Möbius Inversion Formula presented, though a version of it is derived as Lemma 13.3. We have, however, presented the Möbius Inversion Formula and some applicants in the exercises to Chapter 13. Many of these exercises are problems that I have seen over the years in various texts, jotted down in my notebooks or assigned in exams, but do not remember the source. The classical textbooks by Landau [L], Carmichael [Car], and Mossaheb [M] are certainly the sources for a few of the exercises throughout the text. A few of the exercises in the book are fairly non-trivial problems. I have posted some hints for a number of the exercises on the book's website at

http://www.math.uic.edu/~rtakloo

In addition to exercises, each chapter has a Notes section. The contents of these sections vary from chapter to chapter. Some of them are concerned with the history of the subject, some others give references to more advanced topics, and a few describe connections to current research.

Numerical experiments and hands-on computations have always been a cornerstone of mathematical discovery. Before computers were invented, or were so commonplace, mathematicians had to do their numerical computations by hand. Even today, it is hard to exaggerate the importance of doing computations by hand —the most efficient way to understand a theorem is to work out a couple of small examples with pen and paper. It is of course also extremely important to take advantage of the abundant computational power provided by machines to do

numerical computations, run experiments, formulate conjectures, and test strategies to prove these conjectures. I have included a number of computer-based exercises in each chapter. These exercises are marked by (✠). These exercises are not written with any particular computer programming language or computational package in mind. Many of the standard computational packages available on the market can do basic number theory; I highly recommend SageMath—a powerful computer algebra system whose development is spearheaded by William Stein in collaboration with a large group of mathematicians. Beyond its technical merits, SageMath is also freely available both as a Web-based program and as a package that can be installed on a personal computer. Appendix C provides a brief introduction to SageMath as a means to get the reader started. What is in this appendix is enough for most of the computational exercises in the book, but not all. Once the reader is familiar with SageMath as presented in the appendix, he or she should be able to consult the references to acquire the necessary skills for these more advanced exercises.

This is how the book is organized:

- We present a couple of different proofs of the Pythagorean Theorem in Chapter 1 and describe the types of number theoretic problems regarding right triangles we will be discussing in this book.
- Chapter 2 contains the basic theorems of elementary number theory, the theory of divisibility, congruences, the Euler ϕ-function, and primitive roots.
- We find the solutions of the Pythagorean Equation in integers in Chapter 3 using two different methods, one algebraic and the other geometric. We then apply the geometric method to find solutions to some other equations. We also discuss a special case of *Fermat's Last Theorem*.
- In Chapter 4, we study the areas of right triangles with integer sides.
- Chapter 5 is devoted to the study of numbers that are side lengths of right triangles. Our analysis in this section is based on Gaussian integers which we briefly review. We also discover the relevance of prime numbers of the form $4k + 1$ to our problem.
- Chapter 6 contains a number of theorems about the infinitude of primes of various special forms, including primes of the form $4k + 1$. This chapter also makes a case for a study of squares modulo primes, leading to the statement of the *Law of Quadratic Reciprocity*.
- We present a proof of the Law of Quadratic Reciprocity in Chapter 7 using *quadratic Gauss sums*.
- Gauss sums are used in Chapter 8 to study the solutions of the Pythagorean Equation modulo various integers.
- In Chapter 9, we extend the scope of our study to include analogues of the Pythagorean Equation in higher dimensions and prove several results about the distribution of integral points on circles and spheres in various dimensions. In this chapter, we state a theorem about numbers which are sums of two, three, or more squares.
- Chapter 10 contains a geometric result due to Minkowski. We use this theorem to prove the theorem on sums of squares.

- Chapter 11 presents the theory of quaternions and uses these objects to give another proof of the theorem on sums of four squares.
- Chapter 12 deals with the theory of quadratic forms. We use this theory to give a second proof of the theorem on three squares.
- Chapters 13 and 14 are more analytic in nature than the chapters that precede them. In Chapter 13, we prove a classical theorem of Lehmer from 1900 that counts the number of primitive right triangles with bounded hypotenuse. This requires developing some basic analytic number theory.
- In Chapter 14, we introduce the notion of height and prove that rational points of bounded height are equidistributed on the unit circle with respect to a natural measure.
- Appendix A contains some basic material we often refer to in the book.
- Appendix B reviews the basic properties of algebraic integers. We use these basic properties in our proof of the Law of Quadratic Reciprocity.
- Finally, Appendix C is a minimal introduction to SageMath.

How to use this book. The topics in Chapters 2 through 7 are completely appropriate for a first course in elementary number theory. Depending on the level of the students enrolled in the course, one might consider covering the proof of the Four Squares Theorem from either Chapter 10 or Chapter 11. In some institutions, students take number theory as a junior or senior by which time they have, often, already learned basic analysis and algebra. In such instances, the materials in either Chapter 13 or Chapter 14 might be a good end-of-semester topic. When I taught from this book last year, in a semester-long course, I taught Chapters 1, 2, Example 8.6, 3, Chapters 6 and 7, the proofs of the Two Squares and Four Squares Theorems from Chapter 10, Theorem 9.4, and Chapter 13.

The book may also be used as the textbook for a second-semester undergraduate course, or an honors course, or a first-year master's level course. In these cases, I would concentrate on the topics covered in Chapters 8 through 14, though Chapter 4 might also be a good starting point as what is discussed in that chapter is not usually covered in undergraduate classes. Except for the first two sections of Chapter 9 that are referred to throughout the second part of the book, the other chapters are independent of each other and they can be taught in pretty much any order. Many of the major theorems in this book are proved in more than one way. This is aimed to give instructors flexibility in designing their courses based on their own interests, or who is attending the course.

I wish to thank the students of my Foundations of Number Theory class at UIC in the fall term of 2016 for their patience and dedication. These students were Samuel Coburn, William d'Alessandro, Victor Flores, Fayyazul Hassan, Ryan Henry, Robert Hull, Ayman Hussein, McKinley Meyer, Natawut Monaikul, Samantha Montiague, Shayne Officer, George Sullivan, and Marshal Thrasher. They took notes, asked questions, and, in a lot of ways, led the project. Without them, this book would have never materialized.

I also wish to thank Jeffery Breeding-Allison, Antoine Chambert-Loir, Samit Dasgupta, Harald Helfgott, Hadi Jorati, Lillian Pierce, Lior Silberman, William Stein, Sho Tanimoto, Frank Thorne, and Felipe Voloch, as well as the anonymous readers for many helpful suggestions. This book would have never seen the light of the day had it not been for the support and encouragement of my editor Loretta Bartolini.

My work on this project is partially supported by a Collaboration Grant from the Simons Foundation.

This book was written at the Brothers K Coffeehouse in Evanston, IL. The baristas at Brothers K serve a lot more than just *earl gray*. I thank Yelena Dligach who suggested that I write this book and Dr. Joshua Nathan for his care and support during the past few years.

Finally I thank my wife, Paria, and my children, Shalizeh and Arad, for their patience and encouragement. It is to them that this book is humbly dedicated.

Chicago, IL, USA Ramin Takloo-Bighash
July 2018

Contents

Part I Foundational material

1 Introduction . . . 3
- 1.1 The Pythagorean Theorem . . . 3
- 1.2 Pythagorean triples . . . 6
- 1.3 The questions . . . 8
- Exercises . . . 8
- Notes . . . 10

2 Basic number theory . . . 13
- 2.1 Natural numbers, mathematical induction, and the Well-ordering Principle . . . 13
- 2.2 Divisibility and prime factorization . . . 14
- 2.3 The Chinese Remainder Theorem . . . 22
- 2.4 Euler's Theorem . . . 24
- 2.5 Polynomials modulo a prime . . . 30
- 2.6 Digit expansions . . . 32
- 2.7 Digit expansions of rational numbers . . . 39
- 2.8 Primitive roots . . . 41
- Exercises . . . 49
- Notes . . . 53

3 Integral solutions to the Pythagorean Equation . . . 59
- 3.1 Solutions . . . 59
- 3.2 Geometric method to find solutions . . . 61
- 3.3 Geometric method to find solutions: Non-Pythagorean examples . . . 65
- 3.4 Application: $X^4 + Y^4 = Z^4$ . . . 70
- Exercises . . . 72
- Notes . . . 73

4 What integers are areas of right triangles? 81
4.1 Congruent numbers 81
4.2 Small numbers 83
4.3 Connection to cubic equations 84
Exercises 87
Notes 88

5 What numbers are the edges of a right triangle? 91
5.1 The theorem 91
5.2 Gaussian integers 93
5.3 The proof of Theorem 5.2 95
5.4 Irreducible elements in $\mathbb{Z}[i]$ 98
5.5 Proof of Theorem 5.1 99
Exercises 101
Notes 102

6 Primes of the form $4k+1$ 105
6.1 Euclid's theorem on the infinitude of primes 105
6.2 Quadratic residues 107
6.3 An application of the Law of Quadratic Reciprocity 112
Exercises 113
Notes 115

7 Gauss Sums, Quadratic Reciprocity, and the Jacobi Symbol 119
7.1 Gauss sums and Quadratic Reciprocity 119
7.2 The Jacobi Symbol 124
Exercises 129
Notes 130

Part II Advanced Topics

8 Counting Pythagorean triples modulo an integer 133
8.1 The Pythagorean Equation modulo a prime number p 133
8.2 Solutions modulo n for a natural number n 138
Exercises 145
Notes 146

9 How many lattice points are there on a circle or a sphere? 151
9.1 The case of two squares 151
9.2 More than two squares 155
9.3 Integral points on arcs 156
Exercises 162
Notes 164

10 What about geometry? . . . 165
10.1 Lattices in $\mathbb{R}^n$ . . . 165
10.2 Minkowski's Theorem . . . 168
10.3 Sums of two squares . . . 172
10.4 Sums of four squares . . . 173
10.5 Sums of three squares . . . 176
Exercises . . . 180
Notes . . . 182

11 Another proof of the four squares theorem . . . 187
11.1 Quaternions . . . 187
11.2 Matrix representation . . . 189
11.3 Four squares . . . 190
Exercises . . . 192
Notes . . . 193

12 Quadratic forms and sums of squares . . . 195
12.1 Quadratic forms with integral coefficients . . . 195
12.2 Binary forms . . . 200
12.3 Ternary forms . . . 203
12.4 Three squares . . . 206
Exercises . . . 208
Notes . . . 209

13 How many Pythagorean triples are there? . . . 211
13.1 The asymptotic formula . . . 211
13.2 The computation of C_2 . . . 217
Exercises . . . 220
Notes . . . 223

14 How are rational points distributed, really? . . . 227
14.1 The real line . . . 227
14.2 The unit circle . . . 240
Exercises . . . 243
Notes . . . 245

Appendix A: Background . . . 247

Appendix B: Algebraic integers . . . 255

Appendix C: SageMath . . . 261

References . . . 271

Index . . . 277

Notation

The following notations are frequently used in the rest of the text:

- $\mathbb{R}$: The field of real numbers.
- $\mathbb{C}$: The field of complex numbers.
- $\mathbb{Q}$: The field of rational numbers.
- $\mathbb{Z}$: The ring of all integers.
- $\mathbb{N}$: The set of all natural numbers, i.e., all positive integers.
- $R[x]$: For a ring R, this is the ring of all polynomials in the variable x with coefficients in R.
- $[x]$: The integer part of a real number x, i.e., the largest integer m with the property that $m \leq x$.
- $\{x\}$: The fractional part of x, i.e., $x - [x]$.
- $|||x|||$: The distance of x to the closest integer, i.e., $\min(\{x\}, 1 - \{x\})$.
- $a \mid b$ for integers a, b: a divides b, i.e., there is an integer c such that $b = ac$.
- $a \nmid b$ for integers a, b: b is not divisible by a.
- $a \equiv b \mod c$, with a, b, c integers such that $c \neq 0$: $c | a - b$.
- $\mathrm{M}_n(R)$: The ring of $n \times n$ matrices with entries in the set R.
- $\mathrm{GL}_n(\mathbb{Z})$: The group of $n \times n$ integral matrices with determinant equal to ± 1.
- $\mathrm{SL}_n(\mathbb{Z})$: The group of $n \times n$ integral matrices with determinant equal to $+1$.
- $f(x) = O(g(x))$ for real functions f, g: If there is a constant $C > 0$ such that for all x large enough, $|f(x)| \leq C|g(x)|$.
- $f(x) = o(g(x))$ for real functions f, g: If

$$\lim_{x \to \infty} \frac{f(x)}{g(x)} = 0.$$

- $\phi(n)$ for a natural number n: Euler totient function.
- $\sigma(n)$ for a natural number n: The sum of the divisors of n.

- $d(n)$ for a natural number n: The number of divisors of n.
- $sqf(n)$ for a natural number n: The square-free part of n, i.e., the smallest natural number m such that $n = k^2 \cdot m$ for some natural number k.
- δ_{kl}: Kronecker's delta function, equal to 1 if $k = l$, 0 otherwise.
- χ_S for the subset S of a set X: The characteristic function of S, i.e., $\chi_S(x) = 1$ if $x \in S$, $\chi_S(x) = 0$ if $x \in X - S$.
- $\#A$ for a finite set A: The number of elements of the set A.