Preface

This book arose out of my experiences with teaching Math 62DM at Stanford, a course which I developed in 2016 and have taught over the last several years. The course is aimed primarily at highly motivated first-year students at Stanford who were potential honors math majors. The traditional first-year honors sequence targeted to these undergraduates was a year-long three quarter sequence covering multivariable calculus and linear algebra, differential forms, and ordinary differential equations. Some years back, together with several colleagues, we felt that an alternative sequence aimed at introducing ideas of modern mathematics with a discrete flavor might also be welcome to incoming students, especially those with an interest in computer science. This alternative sequence focuses on linear algebra (lectures shared with the traditional sequence students) with applications to combinatorics in the first quarter, finite fields and applications (the subject of this book, and the middle quarter of the sequence), and probability and random processes in the third quarter.

The prerequisites for reading this book are minimal: familiarity with proof writing, some linear algebra (mainly a little familiarity with vector spaces over a field), and one variable calculus is assumed. The book then develops from scratch the theory of finite fields, constructing all of these, and showing why these are unique (up to isomorphism). The

topic of finite fields is used to introduce the student to ideas from algebra and number theory. As a payoff, several combinatorial applications of finite fields are given: Sidon sets and perfect difference sets, De Bruijn sequences and a magic trick of Persi Diaconis, and the polynomial time algorithm for primality testing due to Agrawal, Kayal and Saxena. The book forms the basis for a one quarter (ten weeks) intensive course at Stanford, with students meeting five days a week (four lectures plus a discussion session). Students can expect to develop familiarity with ideas in algebra (groups, rings and fields), and elementary number theory, which would help with later classes where these are developed in greater detail. Past students of the course have enjoyed seeing the marquee primality test application tying together the many disparate topics from the course.

I am grateful to the many students at Stanford who took this course. This book was shaped by my interactions with them. I am also grateful to the wonderful TA's who helped with the course, including Jonathan Love, Graham White, Sarah Peluse, Vivian Kuperberg, and Max Xu. I am especially indebted to Vineet Gupta, Emmanuel Kowalski, Vivian Kuperberg, and Jonathan Love who read drafts of the book, and offered detailed and extremely helpful suggestions. Thanks are due to Ina Mette for her patience, and to the STML series editorial board for their valuable feedback on early drafts of this project. While writing this book, I have been supported by grants from the National Science Foundation, and a Simons Investigator award from the Simons Foundation.

Finally, I am grateful to the Staats- und Universitäts Bibliothek (SUB) Göttingen for kindly permitting me to use the table from Gauss's Nachlass that appears on page 39 (call number SUB Göttingen, Cod. Ms. Gauss Math. 18, fol. 2r.).

Kannan Soundararajan