Preface

The aim of this book is to provide a brief introduction to finite fields and some of their many fascinating applications. The book arose from lectures of the first author in a course entitled "Finite Fields and Their Applications," which was taught in the Department of Mathematics at The Pennsylvania State University during the Fall semester of 2004. The course was part of the department's Mathematics Advanced Study Semesters (MASS) program. The second author produced an initial online set of notes from these lectures, which have been greatly expanded into the present volume.

The most important chapter of this text is the first, which discusses a variety of properties of finite fields. Many of these properties are used in later chapters where various applications of finite fields are discussed. The chapter begins with a discussion of the basic properties of finite fields and extension fields. It then defines the important trace and norm functions and establishes some of their properties. Bases for extension fields, including dual, normal, and primitive normal bases, are then discussed. The first chapter concludes with a few results concerning polynomials over finite fields. These include a discussion of the order of a polynomial, formulas for the number and orders of irreducible polynomials, and properties of linearized polynomials and permutation polynomials over finite fields.

Chapter 2 includes some combinatorial applications of finite fields. It includes a detailed discussion of latin squares and their applications to affine and projective planes as well as more general block designs. The chapter closes with a brief discussion of Hadamard matrices which arise from an elementary finite field construction.

Chapter 3 deals with algebraic coding theory and includes a discussion of some properties of codes as well as bounds on the parameters of linear codes. Several encoding and decoding methods are also discussed. Constructions for various kinds of codes including Hamming, cyclic, BCH, and Goppa codes are given. A brief discussion of perfect codes is also included. The chapter ends with a discussion of some relations and connections between codes, latin squares, and combinatorial designs.

The final chapter covers some elementary aspects of cryptography. The discussion includes some basic properties of cryptographic systems as well as symmetric key and public key cryptography. The RSA cryptosystem and a double-round quadratic system are presented, along with key exchange systems including the Diffie-Hellman system. The discrete logarithm problem for finite fields is presented in this context. Several threshold systems for distributing secret information are presented, including one based on latin squares. The chapter ends with a brief discussion of digital signatures and several cryptosystems based on Dickson polynomials and elliptic curves over finite fields.

Appendix A provides a brief review of some basic algebraic concepts that are needed for a full understanding of some of the topics covered in the first four chapters. These concepts include topics from number theory, groups, rings and fields, homomorphisms, polynomials and splitting fields. A brief review of a few concepts from the theory of vector spaces, including dual spaces, is presented.

Each chapter, and the first appendix, concludes with a brief set of notes related to that chapter's material. These notes describe a variety of references that provide material for further reading on the topics presented here. Each chapter, and the first appendix, contains a set of exercises of varying levels of difficulty that expand upon

the ideas presented. Appendix B provides hints for many of these exercises.

The first author would like to sincerely thank Sergei Tabachnikov, Director of the MASS program at Penn State, for inviting him to teach a course in the MASS program. Both authors would like to thank Sergei for his encouragement to convert our initial class notes into this text. The first author used this text in his MASS class taught during the Fall semester of 2006. We would like to sincerely thank Charles F. Laywine for his careful reading and many excellent suggestions which greatly improved the readability of our book. A special word of thanks is owed to the 2006 class of MASS students, who provided numerous comments and helpful suggestions for improvements in addition to locating a number of typographical errors. We also thank the publishing staff of the American Mathematical Society who helped bring this book to a successful conclusion.

G. L. Mullen
C. Mummert