BULLETIN (New Series) OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 36, Number 1, January 1999, Pages 99–101
S 0273-0979(99)00768-5

Finite fields, by Rudolf Lidl and Harald Niederreiter, Second edition, Cambridge University Press, 1997, xiv + 755 pp., \$95.00, ISBN 0-521-39231-4

Finite fields are fields that have only a finite number of elements. The simplest examples are the rings of integers modulo a prime number p. The origins and history of finite fields can be traced back to the 17th and 18th centuries, but there, these fields played only a minor role in the mathematics of the day. In more recent times, however, finite fields have assumed a much more fundamental role and in fact are of rapidly increasing importance because of practical applications in a wide variety of areas including information science. More generally, finite fields play vital roles in computer science, coding theory, cryptography, algebraic geometry, number theory and group theory as well as in a variety of areas of discrete mathematics.

It unfortunately does not seem to be widely known in the mathematical community how important finite fields really are. They provide a truly beautiful meeting ground for good theoretical problems as well as very practical applications. Because of this interaction between theory and application, finite fields offer a fertile area where mathematicians, engineers and computer scientists can all work, each to the benefit of the others.

The initial edition of this book was published by Addison-Wesley in 1983 and was the first book devoted solely to finite fields; however, that edition was never reviewed in the *Bulletin of the American Mathematical Society.* Considering the immense impact of the original volume, which has often been called the Bible on finite fields, it is indeed important that a full review be written at this time.

One point of clarification is that this current volume was listed by the new publisher, Cambridge University Press, as a second edition unbeknown to the authors. This is misleading, as the current volume is just a reprint of the original version with some minor corrections.

Since the publication of the original volume in 1983, there has been an explosion of finite field publications in both theoretical and applied aspects. *Mathematical Reviews* lists as appearing since 1983 more than 700 papers with the words “finite fields” in their titles, and since that time there have also been more than 20 books as well as 5 conference proceedings on the subject (see also D. Wan’s review in the A.M.S. Bulletin **30**(1994), 284-290, of several finite field related books). In addition, there is now an international conference on the theory and application of finite fields which has been held every two years since 1991. In 1995 Academic Press began publication of a new research journal *Finite Fields and Their Applications.* These observations should help convince the reader that finite fields are indeed very important mathematical structures and that interest in them is growing rapidly.

The authors have done a masterful job in first digesting an enormous amount of material and then organizing it in an efficient way to make for a clear and readable treatise on finite fields. There were very few errors or typos in the original edition and I suspect almost none in this second corrected edition.

1991 *Mathematics Subject Classification.* Primary 11Txx; Secondary 05Bxx, 11B37, 94A55, 94Bxx.

We very briefly summarize each of the chapter contents: 1. "Algebraic Foundations" is a review of some basic algebraic material with an emphasis on rings and fields; 2. "Structure of Finite Fields" discusses bases, primitive elements, trace and norm functions, cyclotomic polynomials and Wedderburn's theorem; 3. "Polynomials over Finite Fields" considers the concept of order (or exponent) of polynomials, irreducible and primitive polynomials, linearized polynomials as well as various properties of binomials and trinomials; 4. "Factorization of Polynomials" considers algorithms (Berlekamp's for example) for the factorization of polynomials in a single indeterminate over small fields, algorithms for factorization over large fields (where large means that the number of elements in the field is substantially larger than the degree of the polynomial to be factored) and methods of root finding; 5. "Exponential Sums" provides a careful and detailed treatment of various kinds of exponential sums including Gauss, Jacobi and Kloosterman sums and gives proofs of Weil's theorems for polynomial arguments; 6. "Equations over Finite Fields" deals with the number of solutions to various types of equations over finite fields, including quadratic and diagonal equations, and also discusses the elementary method of Stepanov; 7. "Permutation Polynomials" provides criteria for and classes of permutation polynomials in one and several variables and discusses groups of permutation polynomials; 8. "Linear Recurring Sequences" gives a thorough discussion of the theory of linear recurring sequences over finite fields; 9. "Applications of Finite Fields" provides an introduction to coding theory and combinatorics including projective and affine planes and geometries, mutually orthogonal latin squares, Hadamard matrices, block designs, difference sets and linear modular systems; 10. "Tables" provides tables of logarithms and exponentials for hand calculations in small finite fields and lists of irreducible polynomials of small degrees over small prime fields and a primitive polynomial of each degree n over the field of p elements where $p^n < 10^9$ with $p < 50$.

The Bibliography consists of 160 pages and approximately 2,500 references. This is a very complete bibliography through 1983 (the date of publication of the first edition) and as such it is one of the most valuable parts of the book. There is also an author index, a list of symbols, and a subject index.

Other very valuable parts of the book are the detailed Notes given at the end of each chapter. In these notes the authors describe historical perspectives as well as provide a quick review of the literature related to that chapter's material. In particular, they give brief statements of the main results of most of the references referred to in that chapter.

In an effort to enhance the attractiveness of their monograph as a textbook, the authors have included numerous worked-out examples. Additionally, each of the first nine chapters contains a set of exercises that either illustrate the theory or provide extensions and alternative proofs of some of the results within that chapter. These exercises are well chosen and as such they could provide excellent homework problems. (For a more textbook-oriented version of this book, I refer to the related book by the authors entitled *Introduction to finite fields and their applications*, Revised edition, Cambridge University Press, 1994.)

One could argue that various additional topics should have been included in the original volume. In his *Mathematical Review* 86c:11106 of the original volume, S.D. Cohen mentions several such omissions including function field theory, non-Desarguesian geometry, and cryptography. Another missing topic which is very important for computational work is that of finite field algorithms and their complexities. Of course, entire volumes could be written about each of these topics; thus the inclusion of all or even any of these topics would have made the current volume unmanageably large.

This monograph has already become the standard reference on finite fields; indeed, it is referenced in nearly every paper related to finite fields. The book is extremely valuable for the nonspecialist or the practitioner wanting to learn and work in the general area of finite fields and their applications. Moreover, because of its very extensive bibliography, it is also an excellent starting point for a literature search by someone well-versed in finite field theory. Every college, university, and institute library needs a copy, and since, in my experience, the library copy is likely to be signed out when the book is needed, individuals should consider buying a personal copy. I predict it will be used many times.

Gary L. Mullen
The Pennsylvania State University
E-mail address: `mullen@math.psu.edu`