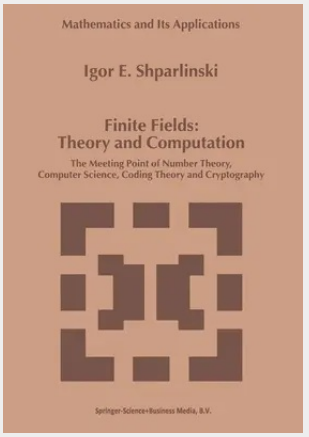
Shparlinski

Finite Fields: Theory and Computation

The Meeting Point of Number Theory, Computer Science, Coding Theory and Cryptography

This book is mainly devoted to some computational and algorithmic problems in finite fields such as, for example, polynomial factorization, finding irreducible and primitive polynomials, the distribution of these primitive polynomials and of primitive points on elliptic curves, constructing bases of various types and new applications of finite fields to other areas of mathematics. For completeness we in clude two special chapters on some recent advances and applications of the theory of congruences (optimal coefficients, congruential pseudo-random number gener ators, modular arithmetic, etc.) and computational number theory (primality testing, factoring integers, computation in algebraic number theory, etc.). The problems considered here have many applications in Computer Science, Cod ing Theory, Cryptography, Numerical Methods, and so on. There are a few books devoted to more general questions, but the results contained in this book have not till now been collected under one cover. In the present work the author has attempted to point out new links among different areas of the theory of finite fields. It contains many very important results which previously could be found only in widely scattered and hardly available conference proceedings and journals. In particular, we extensively review results which originally appeared only in Russian, and are not well known to mathematicians outside the former USSR.

This book is mainly devoted to some computational and algorithmic problems in finite fields such as, for example, polynomial factorization, finding irreducible and primitive polynomials, the distribution of these primitive polynomials and of primitive points on elliptic curves, constructing bases of various types and new applications of finite fields to other areas of mathematics. For completeness we in clude two special chapters on some recent advances and applications of the theory of congruences (optimal coefficients, congruential pseudo-random number gener ators, modular arithmetic, etc.) and computational number theory (primality testing, factoring integers, computation in algebraic number theory, etc.). The problems considered here have many applications in Computer Science, Cod ing Theory, Cryptography, Numerical Methods, and so on. There are a few books devoted to more general questions, but the results contained in this book have not till now been collected under one cover. In the present work the author has attempted to point out new links among different areas of the theory of finite fields. It contains many very important results which previously could be found only in widely scattered and hardly available conference proceedings and journals. In particular, we extensively review results which originally appeared only in Russian, and are not well known to mathematicians outside the former USSR.



213,99 €
199,99 € (zzgl. MwSt.)

Lieferfrist: bis zu 10 Tage

Artikelnummer: 9780792356622
Medium: Buch
ISBN: 978-0-7923-5662-2
Verlag: Springer Netherlands
Erscheinungstermin: 31.05.1999
Sprache(n): Englisch
Auflage: 1. Auflage 1999
Serie: Mathematics and Its Applications
Produktform: Gebunden
Gewicht: 2060 g
Seiten: 528
Format (B x H): 160 x 241 mm

Kundenservice Verlag Dr. Otto Schmidt KG
Neumannstraße 10, 40235 Düsseldorf | kundenservice@otto-schmidt.de | 0221-93738-997 (Inland)