

Finite Fields: Theory and Computation

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

by

Igor E. Shparlinski

*School of Mathematics, Physics, Computing and Electronics,
Macquarie University,
Sydney, New South Wales, Australia*



Kluwer Academic

A C.I.P. Catalogue record for this book is available from the Library of Congress.

ISBN 978-90-481-5203-2

ISBN 978-94-015-9239-0 (eBook)

DOI 10.1007/978-94-015-9239-0

Printed on acid-free paper

All Rights Reserved

© 1999 Kluwer Academic Publishers

Softcover reprint of the hardcover 1st edition 1999

No part of the material protected by this copyright notice may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying, recording or by any information storage and retrieval system, without written permission from the copyright owner.

CONTENTS

Preface	ix
Acknowledgments	xi
Notation	xiii
Introduction	1
Links flowchart	13
Chapter 1. Polynomial Factorization	17
1. Univariate factorization	17
2. Counting the number of points on curves and varieties and multivariate factorization	34
3. Other polynomial decompositions	42
Chapter 2. Finding Irreducible and Primitive Polynomials	45
1. Construction of irreducible polynomials	45
2. Construction of primitive polynomials and generating sets	52
Chapter 3. The Distribution of Irreducible, Primitive and Other Special Polynomials and Matrices	65
1. Irreducible, primitive and other special polynomials and matrices of special form	65
2. Irreducible and primitive polynomials of small height and weight	86
3. Sparse polynomials	91
4. Applications to algebraic number fields	97

Chapter 4. Bases and Computation in Finite Fields	99
1. Construction of some special bases for finite fields	99
2. Discrete logarithm and Zech's logarithm	112
3. Polynomial multiplication and multiplicative complexity in finite fields	117
4. Linear algebra, polynomial interpolation and other algorithms in finite fields	127
Chapter 5. Coding Theory and Algebraic Curves	149
1. Codes and points on algebraic curves	149
2. Codes and exponential sums	185
3. Codes and lattice packings and coverings	205
Chapter 6. Elliptic Curves	215
1. Some general properties	215
2. Finding the group structure of elliptic curves	231
Chapter 7. Recurrence Sequences in Finite Fields and Cyclic Linear Codes	239
1. Distribution of values of recurrence sequences	239
2. Applications of recurrence sequences	245
3. BCH and other cyclic linear codes and recurrence sequences	255
Chapter 8. Finite Fields and Discrete Mathematics	265
1. Cryptography, pseudo-random numbers, and permutation polynomials	265
2. Permutation polynomials and other polynomial mappings	282
3. Graph theory, Boolean functions, combinatorial configurations, and integration nets	297
4. Enumeration problems in finite fields	319
Chapter 9. Congruences	325
1. Optimal coefficients and pseudo-random numbers	325
2. Residues of exponential functions	329
3. Modular arithmetic	345
4. Other applications	349
Chapter 10. Some Related Problems	361
1. Integer factorization, primality testing, and the greatest common divisor	361

2. Computational algebraic number theory	372
3. Algebraic complexity theory	376
4. Polynomials with integer coefficients	387
Appendix 1	403
Appendix 2	405
Appendix 3	407
References	409
Index	525