Computational and Algorithmic Problems in Finite Fields

by

Igor E. Shparlinski

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

SPRINGER SCIENCE+BUSINESS MEDIA, B.V.

ISBN 978-94-010-4796-8 ISBN 978-94-011-1806-4 (eBook)
DOI 10.1007/978-94-011-1806-4

Printed on acid-free paper

All Rights Reserved
© 1992 Springer Science+Business Media Dordrecht
Originally published by Kluwer Academic Publishers in 1992
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

Series Editor's Preface **ix**

Preface **x**

Acknowledgements **xi**

Notations **ix**

Introduction **1**

Chapter 1. Polynomial Factorization **7**

1. Univariate factorization 7
2. Multivariate factorization 16
3. Other polynomial decompositions 20

Chapter 2. Finding irreducible and primitive polynomials **21**

1. Construction of irreducible polynomials 21
2. Construction of primitive polynomials 27

Chapter 3. The distribution of irreducible and primitive polynomials **30**

1. Distribution of irreducible and primitive polynomials 30
2. Irreducible and primitive polynomials of a given height and weight 42
3. Sparse polynomials 46
4. Applications to algebraic number fields 47

Chapter 4. Bases and computation in finite fields **49**

1. Construction of some special bases for finite fields 49
2. Discrete logarithm and Zech's logarithm 54
3. Polynomial multiplication and multiplicative complexity in finite fields 56
4. Other algorithms in finite fields 64

Chapter 5. Coding theory and algebraic curves **72**

1. Codes and points on algebraic curves 72
2. Codes and exponential sums 86
3. Codes and lattice packings and coverings 92

Chapter 6. Elliptic curves **99**

1. Some general properties 99
2. Distribution of primitive points on elliptic curves 105

Chapter 7. Recurrent sequences in finite fields and cyclic linear codes 109
1. Distribution of values of recurrent sequences 109
2. Applications of recurrent sequences 113
3. Cyclic codes and recurrent sequences 116

Chapter 8. Finite fields and discrete mathematics 122
1. Cryptography and permutation polynomials 122
2. Graph theory, combinatorics, Boolean functions 129
3. Enumeration problems in finite fields 136

Chapter 9. Congruences 139
1. Optimal coefficients and pseudo-random numbers 139
2. Residues of exponential functions 143
3. Modular arithmetic 148
4. Other applications 150

Chapter 10. Some related problems 153
1. Integer factorization, primality testing and the greatest common divisor 153
2. Computational algebraic number theory 155
3. Algebraic complexity theory 156
4. Polynomials with integer coefficients 158

Appendix 1 161

Appendix 2 164

Appendix 3 165

Addendum 166

References 191

Index 238