APPLICATIONS OF FINITE FIELDS

by

Alfred J. Menezes, *Editor*

Ian F. Blake
XuHong Gao
Ronald C. Mullin
Scott A. Vanstone
Tomik Yaghoobian

KLUWER ACADEMIC PUBLISHERS

Contents

Preface ix

Acknowledgements xi

1 Introduction to Finite Fields and Bases 1

1.1 Introduction 1

1.2 Bases 3

1.3 The Enumeration of Bases 7

1.4 Applications 12

1.5 References 15

2 Factoring Polynomials over Finite Fields 17

2.1 Introduction 17

2.2 A Few Basics 20

2.3 Root Finding 22

2.4 Factoring 26

2.5 Factoring Multivariate Polynomials 34

2.6 References 37

3 Construction of Irreducible Polynomials 39

3.1 Introduction 39

3.2 Specific Irreducible Polynomials 40

3.3 Irreducibility of Compositions of Polynomials 43

3.4 Recursive Constructions 49

3.5 Composed Product of Irreducible Polynomials 55

3.6 A General Approach 60
3.7 References 65

4 Normal Bases 69
4.1 Introduction 69
4.2 Some Properties of Normal bases 70
4.3 Distribution of Normal Elements 76
4.4 Characterization of N-Polynomials 83
4.5 Construction of Normal Bases 86
4.6 Comments 90
4.7 References 90

5 Optimal Normal Bases 93
5.1 Introduction 93
5.2 Constructions 96
5.3 Determination of all Optimal Normal Bases 104
5.4 An Open Problem 110
5.5 References 112

6 The Discrete Logarithm Problem 115
6.1 Introduction 115
6.2 Applications 118
6.3 The Discrete Logarithm Problem: General Remarks . . 122
6.4 Square Root Methods 123
6.5 The Pohlig-Hellman Method 124
6.6 The Index Calculus Method 126
6.7 Best Algorithms 130
6.8 Computational Results 130
6.9 Discrete Logarithms and Factoring 131
6.10 References 136

7 Elliptic Curves over Finite Fields 139
7.1 Definitions 139
7.2 Group Law 141
7.3 The Discriminant and j-Invariant 142

7.4 Curves over K, $\text{char}(K) \neq 2, 3$ 143
7.5 Curves over K, $\text{char}(K) = 2$ 144
7.6 Group Structure 146
7.7 Supersingular Curves 148
7.8 References 149

8 Elliptic Curve Cryptosystems 151
8.1 Introduction 151
8.2 Singular Elliptic Curves 152
8.3 The Elliptic Curve Logarithm Problem 154
8.4 Implementation 163
8.5 References 170

9 Introduction to Algebraic Geometry 173
9.1 Affine Varieties 173
9.2 Plane Curves 175
9.3 Projective Varieties 177
9.4 Projective Plane Curves 179
9.5 Dimension of X 180
9.6 Divisors on X 181
9.7 Differentials on X 184
9.8 Algebraic Curves over a Finite Field 189
9.9 References 190

10 Codes From Algebraic Geometry 191
10.1 Introduction to Coding Theory 192
10.2 Algebraic Geometric Codes 193
10.3 Hermitian Codes 197
10.4 Codes From Elliptic Curves 200
10.5 Codes From Elliptic Curves over F_{2^m} 201
10.6 Decoding Algebraic Geometric Codes 203
10.7 Problems 207
10.8 References 208

Appendix – Other Applications 211

Index 215