

Contents

	Preface	ix
1	Prologue	1
2	Euclidean Domains and Euclid's Algorithm	3
3	Unique Factorization in Euclidean Domains	13
4	Building Fields from Euclidean Domains	19
5	Abstract Properties of Finite Fields	29
6	Finite Fields Exist and are Unique	55
7	Factoring Polynomials over Finite Fields	75
8	Trace, Norm, and Bit-Serial Multiplication	97
9	Linear Recurrences over Finite Fields	123
10	The Theory of m -Sequences	151
11	Crosscorrelation Properties of m -Sequences	169
	Bibliography	201
	Index	203