
Contents

Preface	xi
Chapter 1. Primes and factorization	1
§1.1. Groups	1
§1.2. Rings	4
§1.3. Integral domains and fields	6
§1.4. Divisibility: primes and irreducibles	9
§1.5. Ideals and Principal Ideal Domains (PIDs)	12
§1.6. Greatest common divisors	13
§1.7. Unique factorization	15
§1.8. Euclidean domains	17
§1.9. Exercises	21
Chapter 2. Primes in the integers	27
§2.1. The infinitude of primes	27
§2.2. Bertrand's postulate	32
§2.3. How many primes are there?	38
§2.4. Exercises	41
Chapter 3. Congruences in rings	45
§3.1. Congruences and quotient rings	45

§3.2.	The ring $\mathbb{Z}/n\mathbb{Z}$	49
§3.3.	Prime ideals and maximal ideals	51
§3.4.	Primes in the Gaussian integers	55
§3.5.	Exercises	58
Chapter 4.	Primes in polynomial rings: constructing finite fields	63
§4.1.	Primes in the polynomial ring over a field	63
§4.2.	An analogue of the proof of Bertrand's postulate	68
§4.3.	An analogue of Euler's proof	71
§4.4.	Möbius inversion and a formula for $\pi(n; \mathbb{F}_q)$	74
§4.5.	Exercises	79
Chapter 5.	The additive and multiplicative structures of finite fields	83
§5.1.	More about groups: cyclic groups	83
§5.2.	More about groups: Lagrange's theorem	87
§5.3.	The additive structure of finite fields	90
§5.4.	The multiplicative structure of finite fields	95
§5.5.	Exercises	97
Chapter 6.	Understanding the structure of $\mathbb{Z}/n\mathbb{Z}$	99
§6.1.	The Chinese Remainder Theorem	99
§6.2.	The structure of the multiplicative group $(\mathbb{Z}/n\mathbb{Z})^\times$	103
§6.3.	Existence of primitive roots mod p^ℓ : Proof of Theorem 6.10	105
§6.4.	Exercises	108
Chapter 7.	Combinatorial applications of finite fields	111
§7.1.	Sidon sets and perfect difference sets	111
§7.2.	Proof of Theorem 7.3	116
§7.3.	The Erdős-Turán bound—Proof of Theorem 7.4	117
§7.4.	Perfect difference sets—Proof of Theorem 7.8	121
§7.5.	A little more on finite fields	124
§7.6.	De Bruijn sequences	126
§7.7.	A magic trick	129

§7.8. Exercises	130
Chapter 8. The AKS Primality Test	135
§8.1. What is a rapid algorithm?	135
§8.2. Primality and factoring	137
§8.3. The basic idea behind AKS	141
§8.4. The algorithm	143
§8.5. Running time analysis	144
§8.6. Proof of Lemma 8.8	145
§8.7. Generating new relations from old	146
§8.8. Proof of Theorem 8.9	147
§8.9. Exercises	152
Chapter 9. Synopsis of finite fields	155
§9.1. Exercises	161
Bibliography	165
Index	169