

<b>Part I</b>	
<b>INTEGERS</b>	<b>1</b>
Chapter 1	
Numbers	3
Chapter 2	
Induction; the Binomial Theorem	7
A. Induction	7
B. Another Form of Induction	11
C. Well-ordering	13
D. The Binomial Theorem	14
Chapter 3	
Unique Factorization into Products of Primes	19
A. Euclid's Algorithm	19
B. Greatest Common Divisors	22
C. Unique Factorization	26
D. Exponential Notation; Least Common Multiples	28
Chapter 4	
Primes	31
A. Euclid	31
B. Some Analytic Results	32
C. The Prime Number Theorem	35

Chapter 5	
Bases	37
A. Numbers in Base $a$	37
B. Operations in Base $a$	39
C. Multiple Precision Long Division	41
D. Decimal Expansions	44
Chapter 6	
Congruences	47
A. Definition of Congruence	47
B. Basic Properties	48
C. Divisibility Tricks	49
D. More Properties of Congruence	51
E. Congruence Problems	52
F. Round Robin Tournaments	54
Chapter 7	
Congruence Classes	56
Chapter 8	
Rings and Fields	62
A. Axioms	62
B. $\mathbb{Z}_m$	65
Chapter 9	
Matrices and Vectors	68
A. Matrix Multiplication	68
B. The Ring of $n \times n$ Matrices	70
C. Linear Equations	73
D. Determinants and Inverses	75
E. Row Operations	76
F. Subspaces, Bases, Dimension	80
Chapter 10	
Secret Codes, I	84
Chapter 11	
Fermat's Theorem, I: Abelian Groups	90
A. Fermat's Theorem	90
B. Abelian Groups	91
C. Euler's Theorem	94
D. Finding High Powers mod $m$	95
E. The Order of an Element	96
F. About Finite Fields	97
G. Nonabelian Groups	98
Chapter 12	
Repeating Decimals, I	101

Contents	xi
Chapter 13 Error Correcting Codes, I	105
Chapter 14 The Chinese Remainder Theorem	112
A. The Theorem	112
B. A Generalization of Fermat's Theorem	116
Chapter 15 Secret Codes, II	118
Part II POLYNOMIALS	123
Chapter 1 Polynomials	125
Chapter 2 Unique Factorization	129
A. Division Theorem	129
B. Greatest Common Divisors	132
C. Factorization into Irreducible Polynomials	134
Chapter 3 The Fundamental Theorem of Algebra	136
A. Irreducible Polynomials in $\mathbb{C}[x]$	136
B. Proof of the Fundamental Theorem	138
Chapter 4 Irreducible Polynomials in $\mathbb{R}[x]$	142
Chapter 5 Partial Fractions	144
A. Rational Functions	144
B. Partial Fractions	145
C. Integrating	148
D. A Partitioning Formula	151
Chapter 6 The Derivative of a Polynomial	157
Chapter 7 Sturm's Algorithm	160
Chapter 8 Factoring in $\mathbb{Q}[x]$ , I	166
A. Gauss's Lemma	166
B. Finding Roots	168
C. Testing for Irreducibility	169

Chapter 9	
Congruences Modulo a Polynomial	173
Chapter 10	
Fermat's Theorem, II	175
A. The Characteristic of a Field	175
B. Applications of the Binomial Theorem	176
Chapter 11	
Factoring in $\mathbb{Q}[x]$ , II: Lagrange Interpolation	180
A. The Chinese Remainder Theorem	180
B. The Method of Lagrange Interpolation	181
Chapter 12	
Factoring in $\mathbb{Z}_p[x]$	185
Chapter 13	
Factoring in $\mathbb{Q}[x]$ , III: Mod $m$	193
A. Bounding the Coefficients of Factors of a Polynomial	194
B. Factoring Modulo High Powers of Primes	198
Part III	
FIELDS	205
Chapter 1	
Primitive Elements	207
Chapter 2	
Repeating Decimals, II	212
Chapter 3	
Testing for Primeness	218
Chapter 4	
Fourth Roots of One in $\mathbb{Z}_p$	222
A. Primes	222
B. Finite Fields of Complex Numbers	223
Chapter 5	
Telephone Cable Splicing	226
Chapter 6	
Factoring in $\mathbb{Q}[x]$ , IV: Bad Examples Mod $p$	229
Chapter 7	
Congruence Classes Modulo a Polynomial: Simple Field Extensions	231

Chapter 8	
Polynomials and Roots	237
A. Inventing Roots of Polynomials	237
B. Finding Polynomials with Given Roots	238
Chapter 9	
Error Correcting Codes, II	242
Chapter 10	
Isomorphisms, I	255
A. Definitions	255
B. Examples Involving $\mathbb{Z}$	257
C. Examples Involving $F[x]$	259
D. Automorphisms	261
Chapter 11	
Finite Fields are Simple	264
Chapter 12	
Latin Squares	267
Chapter 13	
Irreducible Polynomials in $\mathbb{Z}_p[x]$	273
A. Factoring $x^{p^n} - x$	273
B. Counting Irreducible Polynomials	275
Chapter 14	
Finite Fields	280
Chapter 15	
The Discriminant and Stickelberger's Theorem	282
A. The Discriminant	282
B. Roots of Irreducible Polynomials in $\mathbb{Z}_p[x]$	287
C. Stickelberger's Theorem	288
Chapter 16	
Quadratic Residues	291
A. Reduction to the Odd Prime Case	291
B. The Legendre Symbol	293
C. Proof of the Law of Quadratic Reciprocity	296
Chapter 17	
Duplicate Bridge Tournaments	300
A. Hadamard Matrices	300
B. Duplicate Bridge Tournaments	302
C. Bridge for 8	303
D. Bridge for $p + 1$	306
Chapter 18	
Algebraic Number Fields	309

Chapter 19	
Isomorphisms, II	314
Chapter 20	
Sums of Two Squares	316
Chapter 21	
On Unique Factorization	320
Exercises Used in Subsequent Chapters	323
Comments on the Starred Problems	325
References	332
Index	335