
Contents

Preface	ix
Chapter 1. Numbers	1
Chapter 2. The Problem $Ax + B = C$	7
Chapter 3. Congruences	11
Chapter 4. Double Congruences and the Euclidean Algorithm	17
Chapter 5. The Augmented Euclidean Algorithm	23
Chapter 6. Simultaneous Congruences	29
Chapter 7. The Fundamental Theorem of Arithmetic	33
Chapter 8. Exponentiation and Orders	37
Chapter 9. Euler's ϕ -Function	43
Chapter 10. Finding the Order of $a \bmod c$	45
Chapter 11. Primality Testing	51

Chapter 12.	The RSA Cipher System	57
Chapter 13.	Primitive Roots mod p	61
Chapter 14.	Polynomials	67
Chapter 15.	Tables of Indices mod p	71
Chapter 16.	Brahmagupta's Formula and Hypernumbers	77
Chapter 17.	Modules of Hypernumbers	81
Chapter 18.	A Canonical Form for Modules of Hypernumbers	87
Chapter 19.	Solution of $A\Box + B = \Box$	93
Chapter 20.	Proof of the Theorem of Chapter 19	99
Chapter 21.	Euler's Remarkable Discovery	113
Chapter 22.	Stable Modules	119
Chapter 23.	Equivalence of Modules	123
Chapter 24.	Signatures of Equivalence Classes	129
Chapter 25.	The Main Theorem	135
Chapter 26.	Modules That Become Principal When Squared	137
Chapter 27.	The Possible Signatures for Certain Values of A	143
Chapter 28.	The Law of Quadratic Reciprocity	149
Chapter 29.	Proof of the Main Theorem	153
Chapter 30.	The Theory of Binary Quadratic Forms	155
Chapter 31.	Composition of Binary Quadratic Forms	163

Contents vii

Appendix. Cycles of Stable Modules	169
Answers to Exercises	179
Bibliography	207
Index	209