R. P. BURN

A pathway into number theory

Second edition
CONTENTS

Preface to the second edition xi
Introduction xiii

1 The fundamental theorem of arithmetic 1
1-24 Division algorithm 1
25-42 Greatest common divisor and Euclidean algorithm 7
43-61 Unique factorisation into primes 9
62-66 Infinity of primes 13
67 Mersenne primes 13
Summary 14
Historical note 14
Notes and answers 16

2 Modular addition and Euler’s $\phi$ function 22
1-18 Congruence classes and the Chinese remainder theorem 22
19-38 The groups $(\mathbb{Z}_n, +)$ and their generators 27
39-56 Euler’s $\phi$ function 33
57-64 Summing Euler’s function over divisors 36
Summary 37
Historical note 38
Notes and answers 39

3 Modular multiplication 48
1-20 Fermat’s theorem 48
21-25 Wilson’s theorem 53
26-33 Linear congruences 53
34-42 Fermat–Euler theorem 54
43-44 Simultaneous linear congruences 55
45-57 Lagrange’s theorem for polynomials 56
58-74 Primitive roots 61
75-87 Chevalley’s theorem 64
88-95 RSA codes 66
Contents

Summary .......................... 67
Historical note ...................... 68
Notes and answers ................. 70

4 Quadratic residues .............. 79
1-29 Quadratic residues and the Legendre symbol .... 79
30-43 Gauss' lemma ................ 81
44-65 Law of quadratic reciprocity .. 84
Summary .......................... 87
Historical note ...................... 88
Notes and answers ................. 89

5 The equation $x^n + y^n = z^n$, for $n = 2, 3, 4$ .... 97
1-18 The equation $x^2 + y^2 = z^2$ ............... 97
19-23 The equation $x^4 + y^4 = z^4$ .............. 100
24-26 The equation $x^2 + y^2 + z^2 = t^2$ ....... 101
27-68 The equation $x^3 + y^3 = z^3$ .............. 102
Summary .......................... 108
Historical note ...................... 108
Notes and answers ................. 110

6 Sums of squares .................. 119
1-36 Sums of two squares ............ 119
37-52 Sums of four squares .......... 123
53-54 Sums of three squares ........ 126
55-61 Triangular numbers .......... 126
Summary .......................... 127
Historical note ...................... 129
Notes and answers ................. 130

7 Partitions ......................... 140
1-15 Ferrers' graphs ................. 140
16-35 Generating functions .......... 141
36-47 Euler's theorem ............... 145
Summary .......................... 147
Historical note ...................... 147
Notes and answers ................. 148

8 Quadratic forms ................. 154
1-20 Unimodular transformations ...... 154
21-31 Equivalent quadratic forms .... 158
32-43 Discriminant ................. 162
44-52 Proper representation ........ 164
53-72 Reduced forms ............... 165
73-77 Automorphs of definite quadratic forms .. 168
Summary .......................... 169
Historical note ...................... 170
Notes and answers ................. 171
Contents

9 Geometry of numbers 187
  1–28 Subgroups of a square lattice 187
  29–46 Minkowski’s theorem in two dimensions 192
  47–66 Subgroups of a cubic lattice 197
  67–73 Minkowski’s theorem in three dimensions 200
  74–86 Legendre’s theorem on $ax^2 + by^2 + cz^2 = 0$ 201
    Summary 204
    Historical note 204
    Notes and answers 206

10 Continued fractions 214
  1–7 Irrational square roots 214
  8–25 Convergence 214
  26–53 Purely periodic continued fractions 220
  54–71 Pell’s equation 223
  72–77 Lagrange’s theorem on quadratic irrationals 226
  78–82 Automorphs of the indefinite form $ax^2 - by^2$ 227
    Summary 229
    Historical note 230
    Notes and answers 232

11 Approximation of irrationals by rationals 242
  1–10 Naive approach 242
  11–22 Farey sequences 243
  23–33 Hurwitz’ theorem 245
  34–43 Liouville’s theorem 247
    Summary 250
    Historical note 250
    Notes and answers 251

Bibliography 257
Index 260