CONTENTS

Introduction 1

1 The fundamental theorem of arithmetic 5

1–24 Division algorithm 5

25–42 Greatest common divisor and Euclidean algorithm 11

43–61 Unique factorisation into primes 13

62–66 Infinity of primes 17

67 Mersenne primes 17

Notes and answers 18

Historical note 23

2 Modular addition and Euler's ϕ function **24**

1–18 Congruence classes and the Chinese remainder theorem **24**

19–38 The groups $(\mathbf{Z}_n, +)$ and their generators 29

39–56 Euler's ϕ function 35

57–64 Summing Euler's function over divisors 38

Notes and answers 40

Historical note 47

3 Modular multiplication 50

1–20 Fermat's theorem 50

21–25 Wilson's theorem 55

26–33 Linear congruences 55

34–42 Fermat–Euler theorem 56

43–44 Simultaneous linear congruences 57

45–57 Lagrange's theorem for polynomials 58

58–74 Primitive roots 63

75–87 Chevalley's theorem 66

Notes and answers 69

Historical note 76

4 Quadratic residues 77

1–29 Quadratic residues and the Legendre svmbol 77

30–43 Gauss' lemma 79

44–65 Law of quadratic reciprocity 82

Notes and answers 86

Historical note 93

5 The equation $x^n + y^n = z^n$, for $n = 2, 3, 4$ 95

1–18 The equation $x^2 + y^2 = z^2$ 95

19–23 The equation $x^4 + y^4 = z^4$ 97

24–26 The equation $x^2 + y^2 + z^2 = t^2$ 98

27–68 The equation $x^3 + y^3 = z^3$ 99

Notes and answers 105

Historical note 113

6 Sums of squares 115

1–36 Sums of two squares 115

37–52 Sums of four squares 119

53–54 Sums of three squares 121

Notes and answers 122

Historical note 130

7 Partitions 131

1–15 Ferrers' graphs 131

16–35 Generating functions 132

36–47 Euler's theorem 136

Notes and answers 138

Historical note 143

8 Quadratic forms 144

1–20 Unimodular transformations 144

21–31 Equivalent quadratic forms 148

32–43 Discriminant 152

44–52 Proper representation 154

53–72 Reduced forms 155

73–77 Automorphs of definite quadratic forms 158

Notes and answers 160

Historical note 175

9 Geometry of numbers 176

1–28 Subgroups of a square lattice 176

29–46 Minkowski's theorem in two dimensions 181

47–66 Subgroups of a cubic lattice 186

67–73 Minkowski's theorem in three dimensions 189

74–86 Legendre's theorem on $ax^2 + by^2 + cz^2 = 0$ 190

Notes and answers 193

Historical note 201

10 Continued fractions 202

1–7 Irrational square roots 202

8–25 Convergence 202

26–53 Purely periodic continued fractions 208
54–71 Pell's equation 211
72–77 Lagrange's theorem on quadratic irrationals 214
78–82 Automorphs of the indefinite form $ax^2 - by^2$ 215
Notes and answers 218
Historical note 228
11 Approximation of irrationals by rationals 229
1–10 Naive approach 229
11–22 Farey sequences 230
23–33 Hurwitz' theorem 232
34–43 Liouville's theorem 234
Notes and answers 238
Historical note 243
Bibliography 244
List of definitions and theorems 246
Index 255