Contents

0 Prerequisites **0–1**
0.1 The number sets 0–1
0.2 The natural numbers 0–1
0.3 Divisibility 0–2

1 The Fundamental Theorem of Arithmetic **1–1**
1.1 Primes 1–1
1.2 The fundamental theorem 1–1
1.3 Euclid's Algorithm 1–2
1.4 Speeding up the algorithm 1–4
1.5 Example 1–4
1.6 An alternative proof 1–5
1.7 Euclid's Lemma 1–6
1.8 Proof of the Fundamental Theorem 1–6
1.9 A postscript 1–7

2 Euclid's Theorem **2–1**
2.1 Variants on Euclid's proof 2–1
2.2 The zeta function 2–2
2.3 Euler's Product Formula 2–3
2.4 Dirichlet's Theorem 2–5

3 Fermat and Mersenne Primes **3–1**
3.1 Fermat primes 3–1
3.2 Mersenne primes 3–2
3.3 Perfect numbers 3–3

4 Modular arithmetic **4–1**
4.1 The modular ring 4–1
4.2 The prime fields 4–2
4.3 The additive group 4–2
4.4 The multiplicative group 4–3
4.5 Homomorphisms 4–5
4.6 Finite fields 4–5

5 The Chinese Remainder Theorem **5–1**
5.1 Coprime moduli 5–1
5.2 The modular ring 5–2

5.3 The totient function 5–2
5.4 The multiplicative group 5–3
5.5 Multiple moduli 5–4
5.6 Multiplicative functions 5–5
5.7 Perfect numbers 5–5

6 Polynomial Rings **6–1**
6.1 Polynomials 6–1
6.2 Long division 6–1
6.3 Irreducibility 6–1
6.4 The Euclidean Algorithm for polynomials 6–2
6.5 Unique factorisation 6–2
6.6 Quotient fields 6–3
6.7 Gauss' Lemma 6–4
6.8 Euclidean domains, PIDs and UFDs 6–4

7 Finite fields **7–1**
7.1 The order of a finite field 7–1
7.2 On cyclic groups 7–1
7.3 Möbius inversion 7–2
7.4 Primitive roots 7–3
7.5 Uniqueness 7–4
7.6 Existence 7–5

8 Fermat's Little Theorem **8–1**
8.1 Lagrange's Theorem 8–1
8.2 Euler's Theorem 8–1
8.3 Fermat's Little Theorem 8–1
8.4 Carmichael numbers 8–2
8.5 The Miller-Rabin test 8–3
8.6 The AKS algorithm 8–3

9 Quadratic Residues **9–1**
9.1 Introduction 9–1
9.2 Prime moduli 9–1
9.3 The Legendre symbol 9–1
9.4 Euler's criterion 9–2
9.5 Gauss's Lemma 9–2
9.6 Computation of $\left(\frac{-1}{p}\right)$ 9–3
9.7 Computation of $\left(\frac{2}{p}\right)$ 9–4
9.8 Composite moduli 9–4
9.9 Prime power moduli 9–5

10 Quadratic Reciprocity **10–1**
10.1 Gauss' Law of Quadratic Reciprocity 10–1
10.2 Wilson's Theorem 10–1
10.3 Rousseau's proof 10–2

11 Gaussian Integers **11–1**
11.1 Gaussian Numbers 11–1
11.2 Conjugates and norms 11–1
11.3 Units 11–2
11.4 Division in Γ 11–2
11.5 The Euclidean Algorithm in Γ 11–3
11.6 Unique factorisation 11–3
11.7 Gaussian primes 11–4
11.8 Sums of squares 11–6

12 Algebraic numbers and algebraic integers **12–1**
12.1 Algebraic numbers 12–1
12.2 Algebraic integers 12–1
12.3 Number fields and number rings 12–2
12.4 Integral closure 12–3

13 Quadratic fields and quadratic number rings **12–1**
12.1 Quadratic number fields 12–1
12.2 Conjugacy 12–2
12.3 Quadratic number rings 12–2
12.4 Units I: Imaginary quadratic fields 12–3

14 Pell's Equation **14–1**
14.1 Kronecker's Theorem 14–1
14.2 Pell's Equation 14–1
14.3 Units II: Real quadratic fields 14–3

15 $Q(\sqrt{5})$ and the golden ratio **15–1**
15.1 The field $\mathbb{Q}(\sqrt{5})$ 15–1
15.2 The number ring $\mathbb{Z}[\phi]$ 15–1
15.3 Unique Factorisation 15–1
15.4 The units in $\mathbb{Z}[\phi]$ 15–2
15.5 The primes in $\mathbb{Z}[\phi]$ 15–3
15.6 Fibonacci numbers 15–4
15.7 The weak Lucas-Lehmer test for Mersenne primality 15–5

16 $\mathbb{Z}[\sqrt{3}]$ and the Lucas-Lehmer test **16–1**
16.1 The field $\mathbb{Q}(\sqrt{3})$ 16–1
16.2 The ring $\mathbb{Z}[\sqrt{3}]$ 16–1
16.3 The units in $\mathbb{Z}[\sqrt{3}]$ 16–1
16.4 Unique Factorisation 16–2
16.5 The primes in $\mathbb{Z}[\sqrt{3}]$ 16–2
16.6 The Lucas-Lehmer test for Mersenne primality 16–3

17 Continued fractions **17–1**
17.1 Finite continued fractions 17–1
17.2 The p's and q's 17–2
17.3 Successive approximants 17–2
17.4 Uniqueness 17–4

17.5 A fundamental identity 17–4
17.6 Infinite continued fractions 17–5
17.7 Diophantine approximation 17–6
17.8 Quadratic surds and periodic continued fractions 17–7

A Expressing numbers as sums of squares **1–1**
A.1 Sum of two squares 1–1
A.2 Sum of three squares 1–2
A.3 Sum of four squares 1–2

B The Structure of Finite Abelian Groups **2–1**
B.1 The Structure Theorem 2–1
B.2 Primary decomposition 2–1
B.3 Decomposition of the primary components 2–2
B.4 Uniqueness 2–2
B.5 Note 2–3

C RSA encryption **3–1**
C.1 The RSA algorithm 3–1
C.2 Encryption 3–1
C.3 Elliptic curve encryption 3–1

D Quadratic Reciprocity: an alternative proof **4–1**