

Contents

| | |
|---|-----------|
| Preface | ix |
| 1 Prime Numbers | 1 |
| 1.1 Prime Factorization | 2 |
| 1.2 The Sequence of Prime Numbers | 10 |
| 1.3 Exercises | 19 |
| 2 The Ring of Integers Modulo n | 21 |
| 2.1 Congruences Modulo n | 22 |
| 2.2 The Chinese Remainder Theorem | 29 |
| 2.3 Quickly Computing Inverses and Huge Powers | 31 |
| 2.4 Primality Testing | 36 |
| 2.5 The Structure of $(\mathbf{Z}/p\mathbf{Z})^*$ | 39 |
| 2.6 Exercises | 44 |
| 3 Public-key Cryptography | 49 |
| 3.1 Playing with Fire | 49 |
| 3.2 The Diffie-Hellman Key Exchange | 51 |
| 3.3 The RSA Cryptosystem | 56 |
| 3.4 Attacking RSA | 61 |
| 3.5 Exercises | 67 |
| 4 Quadratic Reciprocity | 69 |
| 4.1 Statement of the Quadratic Reciprocity Law | 70 |

| | | |
|----------|---|------------|
| 4.2 | Euler's Criterion | 73 |
| 4.3 | First Proof of Quadratic Reciprocity | 75 |
| 4.4 | A Proof of Quadratic Reciprocity Using Gauss Sums | 81 |
| 4.5 | Finding Square Roots | 86 |
| 4.6 | Exercises | 89 |
| 5 | Continued Fractions | 93 |
| 5.1 | The Definition | 94 |
| 5.2 | Finite Continued Fractions | 95 |
| 5.3 | Infinite Continued Fractions | 101 |
| 5.4 | The Continued Fraction of e | 107 |
| 5.5 | Quadratic Irrationals | 110 |
| 5.6 | Recognizing Rational Numbers | 115 |
| 5.7 | Sums of Two Squares | 117 |
| 5.8 | Exercises | 121 |
| 6 | Elliptic Curves | 123 |
| 6.1 | The Definition | 124 |
| 6.2 | The Group Structure on an Elliptic Curve | 125 |
| 6.3 | Integer Factorization Using Elliptic Curves | 129 |
| 6.4 | Elliptic Curve Cryptography | 135 |
| 6.5 | Elliptic Curves Over the Rational Numbers | 140 |
| 6.6 | Exercises | 146 |
| | Answers and Hints | 149 |
| | References | 155 |
| | Index | 161 |