Contents

1 Concepts and History 1

1.1 Basic Concepts . . . 1

1.1.1 Prime Numbers . . . 2

1.1.2 Amicable and Perfect Numbers . . . 10

1.1.3 Amicable k-Tuplets . . . 19

1.1.4 Aliquot k-Cycles . . . 21

1.2 The History of Amicable Numbers . . . 24

1.2.1 Ancient Times . . . 25

1.2.2 Around Euler's Time . . . 28

1.2.3 The Modern Computer Era . . . 31

1.3 Brief History of Perfect and Sociable Numbers . . . 34

2 Mathematical Tools 39

2.1 Computational Complexity Theory . . . 39

2.2 Primality Testing . . . 46

2.2.1 Basic Idea . . . 46

2.2.2 Probable Primes and Strong Pseudoprimality Tests . . . 48

2.2.3 Lucas Sequences and Lucas Tests . . . 54

2.2.4 Primality Testing in Maple . . . 63

2.2.5 Elliptic Curve Test . . . 67

2.2.6 Computational Complexity of Primality Testing . . . 71

2.3 Integer Factorization . . . 74

2.3.1 Computational Complexity of Integer Factorization . . . 74

2.3.2 Factoring by Trial Divisions . . . 77

2.3.3 Continued FRACtion Method (CFRAC) . . . 80

2.3.4 Pollard's "*rho*" and "$p-1$" Algorithms . . . 84

2.3.5 Lenstra's Elliptic Curve Algorithm . . . 87

2.3.6 Progress on Factoring Fermat Numbers . . . 89

2.3.7 Integer Factorization in Maple 92
2.4 Diophantine Equations 97
2.4.1 Continued Fraction Approach 98
2.4.2 Combinatorial Approach 100

3 Exhaustive Numerical Methods 103
3.1 Numerical Methods for Perfect Numbers 104
3.2 Computing Different Types of Perfect Numbers 107
3.3 Computing Odd Perfect Numbers 111
3.4 Numerical Methods for Amicable Numbers 113
3.5 te Riele's Seminumerical Method for Amicable Pairs 118
3.6 Computing Reduced Amicable Pairs 121
3.7 Numerical Methods for Aliquot k-Cycles 128

4 Algebraic Assumption Methods 137
4.1 Thabit's Algebraic Assumption Method 137
4.2 Euler's Version of Thabit's Method 140
4.3 Analogue of Thabit's Method 146
4.4 Some Conjectures on Amicable Pairs 151
4.5 Algebraic Rules for Aliquot k-Cycles 153
4.5.1 Algebraic Rule for Aliquot 3-Cycles 154
4.5.2 Algebraic Rules for Aliquot 4-Cycles 163

5 Algebraic Constructive Methods 169
5.1 A Special Algebraic Constructive Method 169
5.2 A General Algebraic Constructive Method 180
5.3 Two Other More General Constructive Methods 189
5.3.1 Forward Methods 190
5.3.2 Backward Methods 199
5.4 Algebraic Methods for Amicable k-Tuplets 201
5.4.1 Methods for Amicable Triplets 202
5.4.2 Methods for Amicable k-Tuplets 203
5.5 A Practical Application in Cryptography 207

6 Conclusions and Open Problems 215
6.1 Summary 215
6.1.1 The History of Amicable Numbers 215
6.1.2 Mathematical Tools for Amicable Numbers 217
6.1.3 Exhaustive Numerical and Semi-numerical Methods . . . 219

6.1.4 Algebraic Assumption Methods 220
6.1.5 Algebraic Constructive Methods 221
6.1.6 Computer-Aided Proof 221
6.2 Some Open Problems 222
6.2.1 Problems Related to Amicable Numbers 222
6.2.2 Problems in General Computational Number Theory . . 225

Bibliography **233**

A Basic Number Theory **245**
A.1 What is Number Theory 245
A.2 Divisibility 248
A.3 Euclid's Algorithm 252
A.4 Arithmetic Functions 256
A.5 Congruences 259

B Introduction to the Maple `numtheory/combinat` Packages **267**
B.1 Basic Concepts 267
B.2 Number-Theoretic Functions 268
B.2.1 Basic Arithmetic Functions 270
B.2.2 Modular Arithmetic Functions 272
B.2.3 Primality Testing Related Functions 273
B.2.4 Integer Factorization Related Functions 278
B.2.5 Continued Fractions 281
B.2.6 Legendre/Jacobi Symbols 287
B.3 Combinatorial Functions 289
B.4 Programming in Maple 293

C Selected Maple Programs **299**
C.1 Programs for Numerical Methods 299
C.2 Programs for Algebraic Assumption Methods 307
C.3 Programs for Algebraic Constructive Methods 316

Index **335**