# Contents

## Preface

### 1 Number Theory Begins

- Pierre de Fermat
- Pythagorean Triangles
- Babylonian Mathematics
- Sexagesimal Numbers
- Regular Numbers
- Square Numbers
- Primitive Pythagorean Triples
- Infinite Descent
- Arithmetic Progressions
- Fibonacci’s Approach
- Problems

### 2 Euclid

- Greek Mathematics
- Triangular Numbers
- Tetrahedral and Pyramidal Numbers
- The Axiomatic Method
- Proof by Contradiction
- Euclid’s Self-Evident Truths
- Unique Factorization
- Pythagorean Tuning
- Problems

### 3 Divisibility

- The Euclidean Algorithm
- The Greatest Common Divisor
- The Division Algorithm
- Divisibility
- The Fundamental Theorem of Arithmetic
- Congruences
- Divisibility Tests
- Continued Fractions
- Problems
# Contents

4 Diophantus  
**The *Arithmetica***  
Problems from the *Arithmetica*  
A Note in the Margin ⋆  
Diophantine Equations ⋆  
Pell’s Equation  
Continued Fractions  
Problems  

5 Fermat  
Christmas Day, 1640 ⋆  
Fermat’s Little Theorem ⋆  
Primes as Sums of Two Squares ⋆  
Sums of Two Squares ⋆  
Perfect Numbers ⋆  
Mersenne Primes  
Fermat Numbers  
Binomial Coefficients ⋆  
“Multi Pertransibunt et Augebitur Scientia”  
Problems  

6 Congruences  
Fermat’s Little Theorem ⋆  
Linear Congruences ⋆  
Inverses ⋆  
The Chinese Remainder Theorem  
Wilson’s Theorem ⋆  
Two Quadratic Congruences  
Lagrange’s Theorem  
Problems  

7 Euler and Lagrange  
A New Beginning ⋆  
Euler’s Phi Function ⋆  
Primitive Roots ⋆  
Euler’s Identity ⋆  
Quadratic Residues ⋆  
Lagrange  
Lagrange’s Four Squares Theorem ⋆  
Sums of Three Squares  
Waring’s Problem  
Fermat’s Last Theorem ⋆  
Problems
Contents

8 Gauss
The Young Gauss 227
Quadratic Residues 229
The Legendre Symbol 231
Euler’s Criterion 232
Gauss’s Lemma 234
Euler’s Conjecture 238
The Law of Quadratic Reciprocity 239
Problems 250

9 Primes I
Factoring 258
The Quadratic Sieve Method 261
Is \( n \) Prime? 267
Pseudoprimes 269
Absolute Pseudoprimes 270
A Probabilistic Test 271
Can \( n \) Divide \( 2^n - 1 \) or \( 2^n + 1 \)? 272
Mersenne Primes 273
Problems 276

10 Primes II
Gaps Both Large and Small 285
The Twin Prime Conjecture 286
The Series \( \sum_{p \leq x} \frac{1}{p} \) 287
Bertrand’s Postulate 292
Goldbach’s Conjecture 296
Arithmetic Progressions 297
Problems 299

11 Sophie Germain
Monsieur LeBlanc 307
Germain Primes 309
Germain’s Grand Plan 312
Fermat’s Last Theorem 316
Problems 317

12 Fibonacci Numbers
Fibonacci 324
The Fibonacci Sequence 325
The Golden Ratio 328
Fibonacci Numbers in Nature 331
<table>
<thead>
<tr>
<th>Contents</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Binet’s Formula ★</td>
<td>334</td>
</tr>
<tr>
<td>Tiling and the Fibonacci Numbers</td>
<td>337</td>
</tr>
<tr>
<td>Fibonacci Numbers and Divisibility</td>
<td>343</td>
</tr>
<tr>
<td>Generating Functions</td>
<td>347</td>
</tr>
<tr>
<td>Problems</td>
<td>349</td>
</tr>
<tr>
<td>13 Cryptography</td>
<td>364</td>
</tr>
<tr>
<td>Secret Codes on Mount Everest</td>
<td>365</td>
</tr>
<tr>
<td>Caesar and Vigenère Ciphers ★</td>
<td>366</td>
</tr>
<tr>
<td>Unbreakable Ciphers</td>
<td>368</td>
</tr>
<tr>
<td>Public-Key Systems ★</td>
<td>369</td>
</tr>
<tr>
<td>Problems</td>
<td>374</td>
</tr>
<tr>
<td>14 Continued Fractions</td>
<td>379</td>
</tr>
<tr>
<td>The Golden Ratio Revisited</td>
<td>379</td>
</tr>
<tr>
<td>Finite Continued Fractions ★</td>
<td>381</td>
</tr>
<tr>
<td>Infinite Continued Fractions ★</td>
<td>393</td>
</tr>
<tr>
<td>Approximation</td>
<td>402</td>
</tr>
<tr>
<td>Pell’s Equation</td>
<td>409</td>
</tr>
<tr>
<td>Problems</td>
<td>424</td>
</tr>
<tr>
<td>15 Partitions</td>
<td>433</td>
</tr>
<tr>
<td>Euler ★</td>
<td>434</td>
</tr>
<tr>
<td>Generating Functions</td>
<td>437</td>
</tr>
<tr>
<td>Euler’s Pentagonal Number Theorem</td>
<td>440</td>
</tr>
<tr>
<td>Ferrers Graphs</td>
<td>446</td>
</tr>
<tr>
<td>Ramanujan</td>
<td>450</td>
</tr>
<tr>
<td>Problems</td>
<td>457</td>
</tr>
<tr>
<td>Hints for Selected Problems</td>
<td>463</td>
</tr>
<tr>
<td>Solutions to Selected Problems</td>
<td>481</td>
</tr>
<tr>
<td>Brief Introduction to Sage</td>
<td>559</td>
</tr>
<tr>
<td>Suggestions for Further Reading</td>
<td>563</td>
</tr>
<tr>
<td>Pronunciation Guide</td>
<td>569</td>
</tr>
<tr>
<td>Table of Primes</td>
<td>571</td>
</tr>
<tr>
<td>Index</td>
<td>573</td>
</tr>
</tbody>
</table>