

# Contents

<b>Preface</b>	<b>vii</b>
<b>1 Natural numbers and integers</b>	<b>1</b>
1.1 Natural numbers . . . . .	2
1.2 Induction . . . . .	3
1.3 Integers . . . . .	5
1.4 Division with remainder . . . . .	7
1.5 Binary notation . . . . .	8
1.6 Diophantine equations . . . . .	11
1.7 The Diophantus chord method . . . . .	14
1.8 Gaussian integers . . . . .	17
1.9 Discussion . . . . .	20
<b>2 The Euclidean algorithm</b>	<b>22</b>
2.1 The gcd by subtraction . . . . .	22
2.2 The gcd by division with remainder . . . . .	24
2.3 Linear representation of the gcd . . . . .	26
2.4 Primes and factorization . . . . .	28
2.5 Consequences of unique prime factorization . . . . .	30
2.6 Linear Diophantine equations . . . . .	33
2.7 *The vector Euclidean algorithm . . . . .	35
2.8 *The map of relatively prime pairs . . . . .	38
2.9 Discussion . . . . .	40
<b>3 Congruence arithmetic</b>	<b>43</b>
3.1 Congruence mod $n$ . . . . .	44
3.2 Congruence classes and their arithmetic . . . . .	45
3.3 Inverses mod $p$ . . . . .	48

3.4	Fermat's little theorem . . . . .	51
3.5	Congruence theorems of Wilson and Lagrange . . . . .	53
3.6	Inverses mod $k$ . . . . .	55
3.7	Quadratic Diophantine equations . . . . .	57
3.8	*Primitive roots . . . . .	59
3.9	*Existence of primitive roots . . . . .	62
3.10	Discussion . . . . .	63
<b>4</b>	<b>The RSA cryptosystem</b>	<b>66</b>
4.1	Trapdoor functions . . . . .	66
4.2	Ingredients of RSA . . . . .	69
4.3	Exponentiation mod $n$ . . . . .	70
4.4	RSA encryption and decryption . . . . .	72
4.5	Digital signatures . . . . .	73
4.6	Other computational issues . . . . .	74
4.7	Discussion . . . . .	74
<b>5</b>	<b>The Pell equation</b>	<b>76</b>
5.1	Side and diagonal numbers . . . . .	77
5.2	The equation $x^2 - 2y^2 = 1$ . . . . .	78
5.3	The group of solutions . . . . .	80
5.4	The general Pell equation and $\mathbb{Z}[\sqrt{n}]$ . . . . .	81
5.5	The pigeonhole argument . . . . .	84
5.6	*Quadratic forms . . . . .	87
5.7	*The map of primitive vectors . . . . .	90
5.8	*Periodicity in the map of $x^2 - ny^2$ . . . . .	95
5.9	Discussion . . . . .	99
<b>6</b>	<b>The Gaussian integers</b>	<b>101</b>
6.1	$\mathbb{Z}[i]$ and its norm . . . . .	102
6.2	Divisibility and primes in $\mathbb{Z}[i]$ and $\mathbb{Z}$ . . . . .	103
6.3	Conjugates . . . . .	105
6.4	Division in $\mathbb{Z}[i]$ . . . . .	107
6.5	Fermat's two square theorem . . . . .	109
6.6	Pythagorean triples . . . . .	110
6.7	*Primes of the form $4n + 1$ . . . . .	113
6.8	Discussion . . . . .	115

<b>7</b>	<b>Quadratic integers</b>	<b>117</b>
7.1	The equation $y^3 = x^2 + 2$	118
7.2	The division property in $\mathbb{Z}[\sqrt{-2}]$	119
7.3	The gcd in $\mathbb{Z}[\sqrt{-2}]$	121
7.4	$\mathbb{Z}[\sqrt{-3}]$ and $\mathbb{Z}[\zeta_3]$	123
7.5	*Rational solutions of $x^3 + y^3 = z^3 + w^3$	126
7.6	*The prime $\sqrt{-3}$ in $\mathbb{Z}[\zeta_3]$	129
7.7	*Fermat's last theorem for $n = 3$	132
7.8	Discussion	136
<b>8</b>	<b>The four square theorem</b>	<b>138</b>
8.1	Real matrices and $\mathbb{C}$	139
8.2	Complex matrices and $\mathbb{H}$	141
8.3	The quaternion units	143
8.4	$\mathbb{Z}[\mathbf{i}, \mathbf{j}, \mathbf{k}]$	145
8.5	The Hurwitz integers	147
8.6	Conjugates	149
8.7	A prime divisor property	151
8.8	Proof of the four square theorem	152
8.9	Discussion	154
<b>9</b>	<b>Quadratic reciprocity</b>	<b>158</b>
9.1	Primes $x^2 + y^2$ , $x^2 + 2y^2$ , and $x^2 + 3y^2$	159
9.2	Statement of quadratic reciprocity	161
9.3	Euler's criterion	164
9.4	The value of $\left(\frac{2}{q}\right)$	167
9.5	The story so far	169
9.6	The Chinese remainder theorem	171
9.7	The full Chinese remainder theorem	173
9.8	Proof of quadratic reciprocity	175
9.9	Discussion	178
<b>10</b>	<b>Rings</b>	<b>181</b>
10.1	The ring axioms	182
10.2	Rings and fields	184
10.3	Algebraic integers	186
10.4	Quadratic fields and their integers	189
10.5	Norm and units of quadratic fields	192
10.6	Discussion	194

<b>11 Ideals</b>	<b>196</b>
11.1 Ideals and the gcd . . . . .	197
11.2 Ideals and divisibility in $\mathbb{Z}$ . . . . .	199
11.3 Principal ideal domains . . . . .	202
11.4 A nonprincipal ideal of $\mathbb{Z}[\sqrt{-3}]$ . . . . .	205
11.5 A nonprincipal ideal of $\mathbb{Z}[\sqrt{-5}]$ . . . . .	207
11.6 Ideals of imaginary quadratic fields as lattices . . . . .	209
11.7 Products and prime ideals . . . . .	211
11.8 Ideal prime factorization . . . . .	214
11.9 Discussion . . . . .	217
<b>12 Prime ideals</b>	<b>221</b>
12.1 Ideals and congruence . . . . .	222
12.2 Prime and maximal ideals . . . . .	224
12.3 Prime ideals of imaginary quadratic fields . . . . .	225
12.4 Conjugate ideals . . . . .	227
12.5 Divisibility and containment . . . . .	229
12.6 Factorization of ideals . . . . .	230
12.7 Ideal classes . . . . .	231
12.8 Primes of the form $x^2 + 5y^2$ . . . . .	233
12.9 Discussion . . . . .	236
<b>Bibliography</b>	<b>239</b>
<b>Index</b>	<b>245</b>



<http://www.springer.com/978-0-387-95587-2>

Elements of Number Theory

Stillwell, J.

2003, XII, 256 p., Hardcover

ISBN: 978-0-387-95587-2