

# Inhaltsverzeichnis

<b>Vorwort</b>	<b>7</b>
<b>Einführung</b>	<b>11</b>
Einführung . . . . .	11
Grundlagen über ganze Zahlen . . . . .	15
<b>1 Teilbarkeit</b>	<b>19</b>
1.1 Primzahlen und der Fundamentalsatz der Arithmetik	19
1.2 Der ggT und der EUKLIDISCHE Algorithmus . . . . .	25
1.2.1 Elementare Eigenschaften . . . . .	25
1.2.2 Der EUKLIDISCHE Algorithmus . . . . .	31
1.3 Elementare Primzahlverteilung . . . . .	35
1.3.1 Unendlichkeit der Primzahlen . . . . .	35
1.3.2 Das BERTRANDSche Postulat . . . . .	39
1.3.3 Der große Primzahlsatz . . . . .	46
1.4 Zahlentheoretische Funktionen . . . . .	52
1.4.1 Multiplikative Funktionen . . . . .	52
1.4.2 Die EULERSche $\varphi$ -Funktion . . . . .	57
1.4.3 DIRICHLET-Faltung und MÖBIUS-Inversion . .	59
1.4.4 Vollkommene und befreundete Zahlen . . . . .	67
<b>2 Kongruenzen</b>	<b>77</b>
2.1 Modulare Arithmetik . . . . .	77
2.1.1 Restklassenringe . . . . .	77

2.1.2	Der Chinesische Restsatz . . . . .	82
2.2	Der kleine Satz von FERMAT . . . . .	87
2.2.1	Die Sätze von FERMAT und EULER . . . . .	87
2.2.2	Pseudoprimzahlen und Primzahltests . . . . .	91
2.3	Primitivwurzeln . . . . .	101
2.4	Anwendungen in der Kryptographie . . . . .	113
2.4.1	CAESAR- und VIGENÈRE-Chiffren . . . . .	113
2.4.2	Das RSA-Verfahren . . . . .	116
<b>3</b>	<b>Quadratische Reste</b>	<b>123</b>
3.1	Von allgemeinen zu Primzahlmoduln . . . . .	123
3.2	Das quadratische Reziprozitätsgesetz . . . . .	127
3.3	Anwendungen . . . . .	139
3.3.1	Teiler von FERMAT- und MERSENNE-Zahlen .	139
3.3.2	Der DIRICHLETSche Primzahlsatz . . . . .	142
3.3.3	Das JACOBI-Symbol und Pseudoprimzahlen .	145
<b>4</b>	<b>DIOPHANTISCHE GLEICHUNGEN</b>	<b>153</b>
4.1	Pythagoreische Tripel und FERMATs letzter Satz . . .	154
4.2	Summen von Quadraten . . . . .	167
4.3	Primzahlen als Werte von Polynomen . . . . .	174
<b>5</b>	<b>DARSTELLUNGEN RATIONALER UND REELLER ZAHLEN</b>	<b>181</b>
5.1	Darstellungen zur Basis $g$ . . . . .	182
5.1.1	Existenz der Darstellung . . . . .	182
5.1.2	Perioden rationaler Zahlen . . . . .	186
5.2	Kettenbrüche . . . . .	192
5.2.1	Existenz und Eindeutigkeit . . . . .	192
5.2.2	Die Sätze von EULER und LAGRANGE . . . . .	201
5.2.3	Approximation reeller Zahlen . . . . .	207
<b>6</b>	<b>QUADRATISCHE FORMEN</b>	<b>215</b>
6.1	Allgemeine Konzepte und Notation . . . . .	215
6.2	Reduktionstheorie . . . . .	227
6.2.1	Positiv definite Formen . . . . .	231

6.2.2	Indefinite Formen . . . . .	236
6.3	Ternäre Formen und der Drei-Quadrate-Satz . . . . .	244
6.3.1	Ternäre quadratische Formen . . . . .	244
6.3.2	Ein Beweis des Drei-Quadrate-Satzes . . . . .	250
<b>A</b>	<b>Grundlegende Konzepte aus der Algebra</b>	<b>255</b>
A.1	Ringe . . . . .	255
A.2	Gruppen . . . . .	258
<b>B</b>	<b>Lösungen und Hinweise zu Übungsaufgaben</b>	<b>261</b>
	Namensverzeichnis	273
	Stichwortverzeichnis	277
	Symbolverzeichnis	281
	Literaturverzeichnis	285