

Inhaltsverzeichnis

Vorwort	7
Einführung	11
Einführung	11
Grundlagen über ganze Zahlen	15
1 Teilbarkeit	19
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 φ -Funktion	57
1.4.3 DIRICHLET-Faltung und MÖBIUS-Inversion . .	59
1.4.4 Vollkommene und befreundete Zahlen	67
2 Kongruenzen	77
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
3	Quadratische Reste	123
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
4	DIOPHANTISCHE GLEICHUNGEN	153
4.1	Pythagoreische Tripel und FERMATs letzter Satz . . .	154
4.2	Summen von Quadraten	167
4.3	Primzahlen als Werte von Polynomen	174
5	DARSTELLUNGEN RATIONALER UND REELLER ZAHLEN	181
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
6	QUADRATISCHE FORMEN	215
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
A	Grundlegende Konzepte aus der Algebra	255
A.1	Ringe	255
A.2	Gruppen	258
B	Lösungen und Hinweise zu Übungsaufgaben	261
	Namensverzeichnis	273
	Stichwortverzeichnis	277
	Symbolverzeichnis	281
	Literaturverzeichnis	285