

Inhaltsverzeichnis

Inhaltsverzeichnis	3
1 Primzerlegung	7
1.1 Einführung und Motivation	7
1.2 Elementare Teilbarkeitslehre in integren Ringen	10
1.3 Primzerlegung in Euklidischen Ringen, Faktorielle Ringe	12
2 Arithmetische Funktionen	19
2.1 Einführung	19
2.2 Dirichlet-Reihen	20
2.3 Arithmetische Funktionen allgemein	20
2.4 Multiplikative arithmetische Funktionen	22
3 Kongruenzen und Restklassenringe	29
3.1 Zyklische Gruppen	33
3.2 Primitivwurzeln	36
3.3 Zifferndarstellung nach Cantor	39
3.4 Simultane Kongruenzen	40
3.4.1 Prinzip des Parallelen Rechnens	40
3.4.2 Der Chinesische Restsatz	41
3.5 Ausgewählte Anwendungen von Kongruenzen	44
3.5.1 Diophantische Gleichungen	44
3.5.2 Interpolation	45
3.5.3 Rechnen im Computer mit großen ganzen Zahlen	45
3.6 Struktur der Primrestklassengruppe mod m	46
4 Endliche Körper und der Satz von Chevalley	49
4.1 Untersuchung eines endl. Körpers L mit $\#L = q$	49
4.2 Die Sätze von Chevalley und Waring	52
5 Quadratische Kongruenzen	57
5.1 Einführende Diskussion	57
5.2 Grundaussagen über Potenzreste	58
5.3 Quadratische Reste und das quadratische Reziprozitätsgesetz	59
5.3.1 Jacobi-Symbol	65
6 Primzahltests	67
6.1 Anwendung der EZT in der Kryptographie	71
7 Ganzzahlige lineare Gleichungen und Moduln über euklidischen Ringen	73
7.1 Der Elementarteileralgorithmus	73
7.1.1 Matrizen über euklidischen Ringen	73
7.2 Ganzzahlige Lösungen eines ganzzahligen linearen Gleichungssystems	78

8	Ganzzahlige quadratische Formen	81
8.1	Grundbegriffe und Bezeichnungen	81
8.2	Die Diskriminante	82
8.3	Darstellung von Zahlen durch QFen	83
8.4	Reduktion der definiten Formen	85
8.5	Reduktion indefiniter Formen	87
8.6	Automorphismengruppen	90

Bezeichnungen und Voraussetzungen

- Logische Zeichen: \implies , \iff , \forall , \exists , \exists^1 (es gibt genau ein), \wedge (und), \vee (oder)
- Zeichen der Mengenlehre: z.B. \cup , \cap , $\mathbb{N} := \{x \in \mathbb{Z} | x \geq 0\}$
- Induktion als Beweistechnik
- $\#M$ Kardinalität der Menge M , z.B. $\#\mathbb{N} = \infty$
- $\mathbb{N} = \{0, 1, 2, 3, \dots\}$, $\mathbb{N}_+ = \{1, 2, 3, 4, \dots\}$ (natürliche Zahlen)
- $\mathbb{Z} = \{0, \pm 1, \pm 2, \pm 3, \dots\}$ (Ring der ganzen Zahlen)
- $\mathbb{Q} = \{\frac{z}{n} | z \in \mathbb{Z}, n \in \mathbb{N}_+\}$ (Körper der rationalen Zahlen)
- \mathbb{R} Körper der reellen Zahlen
- \mathbb{F}_q Körper mit $q < \infty$ Elementen ($= GF(q)$ in der Informatik)
- $\mathbb{P} = \{2, 3, 5, 7, 11, 13, 17, 19, 23, \dots\}$ Menge aller Primzahlen

