

# Inhaltsverzeichnis

Vororientierung	xiii
- Was nicht vorkommen wird	xiii
- Einige Voraussetzungen in Kurzform	xiv
- Was stattdessen behandelt wird	xvii
0 Grundlegende Beweistechniken	1
0.1 Worum es in diesem Kapitel geht	1
0.2 Der direkte Beweis	2
0.3 Der indirekte Beweis	3
0.4 Der Beweis durch Kontraposition	5
0.5 Der Beweis durch vollständige Induktion	7
0.6 Zum Beweisen von Äquivalenzen	14
1 Die Teilbarkeitsrelation	16
1.1 Definition	16
1.2 Eigenschaften	17
1.3 Teilmengen	21
1.4 Hasse-Diagramme	23
2 Der Hauptsatz der elementaren Zahlentheorie	26
2.1 Vorüberlegungen	26
2.2 Der Hauptsatz	27
2.3 Folgerungen aus dem Hauptsatz	32

3	Primzahlen	41
3.1	Die Unendlichkeit der Menge $\mathbb{P}$	41
3.2	Verfahren zur Bestimmung von Primzahlen	44
3.3	Bemerkenswertes über Primzahlen	49
4	ggT und kgV	53
4.1	Zur Problemstellung	53
4.2	Definitionen	55
4.3	ggT, kgV und Primfaktorzerlegung	57
4.4	ggT, kgV und Hasse-Diagramme	64
4.5	Der euklidische Algorithmus	66
	Anschauliche Beschreibung des euklidischen Algorithmus	71
4.6	Die Menge der Vielfachen des ggT(a,b) und der Linearkombinationen von a und b	73
4.7	Lineare diophantische Gleichungen mit zwei Variablen	77
	Lösen von Anwendungssituationen zu linearen diophantischen Gleichungen	80
5	Kongruenzen und Restklassen	86
5.1	Vorüberlegungen	86
5.2	Definition der Kongruenz	88
5.3	Eigenschaften	90
5.4	Restklassen	95
5.5	Rechnen mit Restklassen	99
5.6	Anwendungen der Kongruenz- und Restklassenrechnung	108
	Teilbarkeitsüberlegungen	108
	Lösen linearer diophantischer Gleichungen	110
	Teilbarkeitsregeln	112
	Rechenproben	117

6	Kryptologie	121
6.1	Grundlegende Begriffe und erste einfache Beispiele	122
6.2	Symmetrische und asymmetrische Verfahren	125
6.3	Mathematische Grundlagen des RSA-Algorithmus	127
6.4	Der RSA-Algorithmus	130
6.5	Die Sicherheit des RSA-Algorithmus	133
7	Stellenwertsysteme	135
7.1	Zahldarstellungen	135
	Das ägyptische Zahlensystem	135
	Das römische Zahlensystem	136
	Das babylonische Zahlensystem	137
	Das Dezimalsystem	140
7.2	b-adische Ziffernsysteme	143
7.3	Die Grundrechenarten in b-adischen Stellenwertsystemen	148
7.4	Teilbarkeitsregeln in b-adischen Stellenwertsystemen	151
8	Alternative Rechenverfahren	160
8.1	Zur Einführung	160
8.2	Schriftliche Addition und Subtraktion	161
8.3	Schriftliche Multiplikation	164
	Die Gittermethode	165
	Das Verdoppelungsverfahren	168
	„Russisches Bauernmultiplizieren“	169
8.4	Schriftliche Division	170
	Das Subtraktionsverfahren	171
	Das Verdoppelungsverfahren	173

---

Literatur	174
Primzahltable	175
Stichwortverzeichnis	177