

## Inhaltsverzeichnis

<b>1</b>	<b>Die Menge der ganzen Zahlen</b>	<b>1</b>
1.1	Die Rechenstruktur $\mathbb{Z}$ . . . . .	1
1.2	Teilbarkeit . . . . .	3
1.2.1	Division mit Rest . . . . .	3
1.2.2	Division ohne Rest . . . . .	5
1.2.3	Restklassen . . . . .	9
1.3	Größter gemeinsamer Teiler . . . . .	12
1.3.1	Definitionen und elementare Eigenschaften . . . . .	12
1.3.2	Das Lemma von Bézout . . . . .	14
1.3.3	Algorithmen zur Berechnung des größten gemeinsamen Teilers . . . . .	16
1.4	Primzahlen . . . . .	21
1.5	Kleinstes gemeinsames Vielfaches . . . . .	27
<b>2</b>	<b>Gruppen</b>	<b>31</b>
2.1	Grundlegende Eigenschaften von Rechenstrukturen . . . . .	33
2.2	Definitionen und Beispiele . . . . .	35
2.3	Elementordnungen . . . . .	41
2.4	Untergruppen . . . . .	44
2.4.1	Elementare Eigenschaften . . . . .	44
2.4.2	Zyklische Gruppen . . . . .	46
2.5	Faktorisierung von Gruppen . . . . .	48
2.5.1	Nebenklassen . . . . .	49
2.5.2	Faktorgruppen . . . . .	50
2.5.3	Satz von Lagrange . . . . .	52
2.6	Gruppenhomomorphismen . . . . .	55
2.6.1	Beispiele und Definitionen . . . . .	55
2.6.2	Kerne von Homomorphismen . . . . .	61
2.6.3	Der Homomorphiesatz für Gruppen . . . . .	64
<b>3</b>	<b>Ringe, Integritätsbereiche und Körper</b>	<b>69</b>
3.1	Ringe . . . . .	69
3.2	Integritätsbereiche . . . . .	72
3.3	Körper . . . . .	75
3.4	Unterringe, Unterkörper, Ring- und Körperhomomorphismen . . . . .	78
3.5	Körpererweiterungen . . . . .	79
3.6	Restklassengruppen und die Sätze von Euler und Fermat . . . . .	83
3.7	Polynomringe . . . . .	86
3.8	Irreduzible und prime Elemente . . . . .	88
3.9	Teilbarkeit von Polynomen . . . . .	91
3.9.1	Größter gemeinsamer Teiler von Polynomen . . . . .	91
3.9.2	Polynomringe und Irreduzibilität . . . . .	95
3.9.3	Nullstellen . . . . .	99

<b>4</b>	<b>Erweiterungen endlicher Körper</b>	<b>105</b>
4.1	Beispiele . . . . .	105
4.2	Grundlegende Definitionen und Eigenschaften . . . . .	109
4.3	Minimalpolynome . . . . .	111
4.4	Einheitengruppen endlicher Körper . . . . .	112
4.5	Charakteristik von Körpern . . . . .	113
<b>5</b>	<b>Modulare Arithmetik</b>	<b>119</b>
5.1	Chinesischer Restsatz . . . . .	119
5.2	Modulare Addition und Multiplikation . . . . .	124
5.3	Effizientes Potenzieren . . . . .	126
5.4	Primitivwurzeln und diskrete Logarithmen . . . . .	129
<b>6</b>	<b>Primzahltests</b>	<b>137</b>
6.1	Das Sieb des Eratosthenes . . . . .	137
6.2	Wilson-Test . . . . .	139
6.3	Lucas-Test . . . . .	140
6.4	Fermat-Test . . . . .	141
6.5	Carmichael-Zahlen . . . . .	147
6.6	Miller-Rabin-Test . . . . .	151
6.7	Der AKS-Test . . . . .	159
<b>7</b>	<b>Asymmetrische Verschlüsselung</b>	<b>165</b>
7.1	Einwegfunktionen . . . . .	166
7.2	Das RSA-Verfahren . . . . .	168
7.3	Der Diffie-Hellman-Schlüsselaustausch . . . . .	175
7.4	Das ElGamal-Verfahren . . . . .	176
7.5	Signaturen . . . . .	177
<b>A</b>	<b>Anhang</b>	<b>181</b>
A.1	Zahlenmengen . . . . .	181
A.2	Alphabete, Wörter, Sprachen . . . . .	181
A.3	Relationen und Funktionen . . . . .	182
A.4	Spezielle Funktionen sowie Summen und Produkte . . . . .	183
A.5	Vektorräume . . . . .	185
	<b>Lösungen zu den Aufgaben</b>	<b>187</b>
	<b>Literatur</b>	<b>215</b>
	<b>Stichwortverzeichnis</b>	<b>217</b>



<http://www.springer.com/978-3-658-04074-1>

Algebraische und zahlentheoretische Grundlagen für  
die Informatik

Gruppen, Ringe, Körper, Primzahltests, Verschlüsselung

Witt, K.-U.

2014, VIII, 220 S., Softcover

ISBN: 978-3-658-04074-1