

Inhalt

1 Was Sie erwartet	9
2 Zahlen und Primzahlen – Eigenschaften	10
2.1 Bezeichnungen und Notationen	10
2.2 Teilbarkeit und Primalität in Integritätsbereichen	10
2.3 Die Menge der Primzahlen	14
2.4 Division mit Rest und Euklidischer Algorithmus	14
3 Das Rechnen mit ganzen Zahlen. Die Langzahlarithmetik und deren Komplexität	18
3.1 Rechnen in Positionssystemen	18
3.2 Ein- und Ausgabe	19
3.3 Vergleich zweier Zahlen	22
3.4 Addition und Subtraktion	23
3.5 Multiplikation	24
3.6 Division mit Rest	26
3.7 Berechnung des größten gemeinsamen Teilers .	28
4 Rechnen mit Resten	29
4.1 Ein Satz über endliche Mengen	29
4.2 Der Restklassenring \mathbb{Z}_m	30
4.3 Der Chinesische Restsatz	32
4.4 Die Gruppe der primen Restklassen	37
5 Primzahl-Testverfahren	40
5.1 Primtest durch Probdivision	40

5.2	Der Fermat-Test	43
5.3	Der Las-Vegas-Ansatz	45
5.4	Carmichael-Zahlen	47
5.5	Der Rabin-Miller-Test	47
5.6	Der Solovay-Strassen-Test	51
6	Primzahl-Zertifikate	56
6.1	Verifikation der Primzahleigenschaft	56
6.2	Primzahl-Zertifikate	57
7	Der Lucas-Test	62
7.1	Quadratische Erweiterungen	62
7.2	Der Ring \mathbb{O}_m	64
7.3	Lucas-Folgen	65
7.4	Eigenschaften von Lucas-Folgen	67
7.5	Lucas-Zertifikate und die Gruppe G_m	69
8	Primzahlrekorde	73
8.1	Fermatzahlen	74
8.2	Mersennezahlen	76
Literatur		80
Index		81