

Inhaltsverzeichnis

1	Typische Fragestellungen	1
2	Grundwissen über ganze Zahlen	7
2.1	$\mathbb{Z}$ als geordneter Euklidischer Bereich	8
2.2	ggT und kgV	9
2.3	Euklidischer Algorithmus	10
2.4	Chinesischer Restsatz	11
2.5	Primfaktorzerlegung	12
3	Weitere Eigenschaften ganzer Zahlen	13
3.1	Primzahlverteilung	13
3.2	Zahlentheoretische Funktionen	18
3.2.1	Perfekte Zahlen	19
3.2.2	Summatorfunktionen	21
3.2.3	Die Eulersche φ -Funktion	24
3.3	Darstellungen ganzer und rationaler Zahlen	26
4	Kongruenzen	31
4.1	Grundlagen aus der Gruppentheorie	32
4.2	Folgerungen aus dem Satz von Euler-Fermat	34

4.3	Anwendung in der Kryptographie	41
4.3.1	Caesar-Chiffre	41
4.3.2	RSA-Kryptosystem	42
4.4	Primzahltests	44
4.4.1	Schnelle Exponentiation	44
4.4.2	Pseudoprimzahlen und Carmichael-Zahlen	45
4.4.3	AKS-Primzahltest	50
4.5	Faktorisierung	52
5	Prime Restklassen	53
5.1	Primitivwurzeln	57
5.2	Diskreter Logarithmus	63
5.3	Anwendung in der Kryptographie	64
6	Quadratische Reste	65
6.1	QR modulo einer ungeraden Primzahl	69
6.2	Das Legendre-Symbol	70
6.3	Das quadratische Reziprozitätsgesetz	75
7	Partitionen	79
8	Diophantische Gleichungen	83
8.1	Lineare diophantische Gleichungen	84
8.2	Quadratische diophantische Gleichungen	85
8.2.1	Eine Unbekannte	85
8.2.2	Zwei Unbekannte	87
8.2.3	Drei Unbekannte	94