

Inhaltsverzeichnis

1	Vollständige Induktion	1
1.1	Das kleinste Element	1
1.2	Das Prinzip vom Maximum	10
1.3	Das Induktionsprinzip	10
1.4	Zusammenfassung	21
2	Euklidischer Algorithmus	25
2.1	Teilen mit Rest	25
2.2	Stellenwertsysteme	28
2.3	Größter gemeinsamer Teiler	35
2.4	Rechnen mit Kongruenzen	44
2.5	Gruppen und Ringe	50
2.5.1	Gruppen	51
2.5.2	Homomorphismen	59
2.5.3	Ringe	66
2.6	Geheimniskrämerei	75
2.7	Primzahlen	80
2.7.1	Natürliche Primzahlen	80
2.7.2	Ein kleiner Spaziergang zum Primzahlsatz	93
2.7.3	Primelemente in anderen Ringen	95
2.8	Der chinesische Restsatz	101
2.9	Die Euler-Funktion	113
3	Der kleine Fermatsche Satz	122
3.1	Kleiner Fermat	122
3.2	Die Ordnung einer Zahl modulo einer Primzahl	127
3.3	Primitivwurzeln	129
3.4	Quadratische Reste	135
3.5	S. Germain's Beitrag zum Problem von Fermat	147
3.6	Verschlüsseln mit dem Kleinen Fermat	151
3.7	Logarithmieren modulo p	153
3.8	Einheiten in Primpotenzmoduln	156
3.9	Fermat in anderen Ringen	161

4	Die Jagd nach großen Primzahlen	165
4.1	Der negative Fermat-Test	165
4.2	Pseudoprimzahlen	171
4.3	Pseudoprimzahlen zur Basis a und Carmichael-Zahlen	177
4.4	Ein probabilistischer Primzahltest	179
4.5	Starke Pseudoprimzahlen	181
4.6	Der Lucas Test	188
4.7	RSA-Verschlüsselung	192