

Inhalt

Vorwort zur zweiten Auflage	vii
Vorwort zur ersten Auflage	ix
Einleitung	xiii
I Grundlagen	1
1 Natürliche Zahlen und Primzahlen	3
1.1 Die natürlichen Zahlen	3
1.2 Teilbarkeit und Primzahlen	13
1.3 Primfaktorzerlegung	17
1.4 Der Euklidische Algorithmus	21
1.5 Das Sieb des Eratosthenes	24
1.6 Es gibt unendlich viele Primzahlen	26
2 Algorithmen und Komplexität	29
2.1 Algorithmen	29
2.2 Algorithmisch lösbare und unlösbare Probleme	37
2.3 Effizienz von Algorithmen und die Klasse P	42
2.4 Wer wird Millionär? Die Klasse NP	51
2.5 Randomisierte Algorithmen	55
3 Zahlentheoretische Grundlagen	65
3.1 Modularrechnung	65
3.2 Der kleine Satz von Fermat	74
3.3 Ein erster Primzahltest	83
3.4 Polynome	85
3.5 Polynome und Modularrechnung	96

4	Primzahlen und Kryptographie	103
4.1	Kryptographie	103
4.2	RSA	106
4.3	Verteilung von Primzahlen	110
4.4	Beweis des schwachen Primzahlsatzes	113
4.5	Randomisierte Primzahltests	116
II	Der AKS-Algorithmus	123
5	Der Ausgangspunkt: Fermat für Polynome	125
5.1	Eine Verallgemeinerung des Satzes von Fermat	125
5.2	Die Idee des AKS-Algorithmus	131
5.3	Der Agrawal-Biswas-Test	134
6	Der Satz von Agrawal, Kayal und Saxena	139
6.1	Die Aussage des Satzes	140
6.2	Die Beweisidee	141
6.3	Anzahl der Polynome in $\mathcal{P}$	143
6.4	Kreisteilungspolynome	147
7	Der Algorithmus	153
7.1	Wie schnell wächst $\text{ord}_r(n)$?	153
7.2	Der Algorithmus von Agrawal, Kayal und Saxena	155
7.3	Weitere Anmerkungen	158
A	Offene Fragen über Primzahlen	163
B	Lösungen und Hinweise zu wichtigen Aufgaben	175
	Notationsverzeichnis	201
	Stichwortverzeichnis	203
	Literaturverzeichnis	209