Inhaltsverzeichnis

	Vorwort	vii
	Installation und Gebrauch der Software	ix
1	Die Peano-Axiome	1
2	Die Grundrechnungsarten	9
3	Die Fibonacci-Zahlen	16
4	Der euklidische Algorithmus	22
5	Primfaktor-Zerlegung	33
6	Der Restklassen-Ring $\mathbb{Z}/m\mathbb{Z}$	45
7	Die Sätze von Fermat, Euler und Wilson	54
8	Die Struktur von $(\mathbb{Z}/m\mathbb{Z})^*$, Primitivwurzeln	59
9	Pseudo-Zufalls-Generatoren	72
10	Zur Umkehrung des Satzes von Fermat	78
11	Quadratische Reste, quadratisches Reziprozitäts-Gesetz	85
12	Probabilistische Primzahltests	98
13	Die Pollard'sche Rho-Methode	105
14	Die (p−1)-Faktorisierungs-Methode	113
15	Das RSA-Kryptographie-Verfahren	123
16	Quadratische Erweiterungen	130
17	Der (p+1)-Primzahltest, Mersenne'sche Primzahlen	140
18	Die (p+1)-Faktorisierungs-Methode	148
19	Faktorisierung mit elliptischen Kurven	154
20	Schnelle Fourier-Transformation und die Multiplikation großer Zahlen	172
21	Kettenbrüche	189
22	Faktorisierung mit Kettenbrüchen	204
23	Quadratische Zahlkörper	218
24	Der Vier-Quadrate-Satz von Lagrange	228
25	Die Pell'sche Gleichung	238
26	Idealklassen quadratischer Zahlkörper	247
	Literaturverzeichnis	271
	Namens- und Sachverzeichnis	274
	Funktions-Index	277