
Inhaltsverzeichnis

1	Die Peano-Axiome	1
2	Die Grundrechnungs-Arten	9
3	Die Fibonacci-Zahlen	16
4	Der Euklidische Algorithmus	22
5	Primfaktor-Zerlegung	32
6	Der Restklassenring $\mathbb{Z}/m\mathbb{Z}$	44
7	Die Sätze von Fermat, Euler und Wilson	53
8	Die Struktur von $(\mathbb{Z}/m\mathbb{Z})^*$, Primitivwurzeln	58
9	Pseudo-Zufalls-Generatoren	67
10	Zur Umkehrung des Satzes von Fermat	73
11	Quadratische Reste, quadratisches Reziprozitätsgesetz	80
12	Probabilistische Primzahltests	92
13	Die Pollard'sche Rho-Methode	99
14	Die $(p-1)$ -Faktorisierungs-Methode	107
15	Das RSA-Kryptographie-Verfahren	116
16	Quadratische Erweiterungen	123
17	Der $(p+1)$ -Primzahltest, Mersenne'sche Primzahlen	133
18	Die $(p+1)$ -Faktorisierungs-Methode	141
19	Schnelle Fourier-Transformation	147
20	Faktorisierung mit dem quadratischen Sieb	163
21	Der diskrete Logarithmus	184
22	Elliptische Kurven	199
23	Faktorisierung mit elliptischen Kurven	212
24	Quadratische Zahlkörper	221
25	Der Vier-Quadrate-Satz von Lagrange	230
26	Kettenbrüche	239
27	Die Pell'sche Gleichung	253
28	Idealklassen quadratischer Zahlkörper	262
29	Faktorisierung mit der Klassengruppe	278
30	Der AKS-Primzahltest	287
	Kurzanleitung für Aribas	302
	Literaturverzeichnis	306
	Namens- und Sachverzeichnis	311



<http://www.springer.com/978-3-658-06539-3>

Algorithmische Zahlentheorie

Forster, O.

2015, VIII, 314 S. 7 Abb., Softcover

ISBN: 978-3-658-06539-3