

# Inhalt

|                                                                 |           |
|-----------------------------------------------------------------|-----------|
| Vorwort zur zweiten Auflage                                     | vii       |
| Vorwort zur ersten Auflage                                      | ix        |
| Einleitung                                                      | xiii      |
| <br>                                                            |           |
| <b>I Grundlagen</b>                                             | <b>1</b>  |
| <br>                                                            |           |
| <b>1 Natürliche Zahlen und Primzahlen</b>                       | <b>3</b>  |
| 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        |
| <br>                                                            |           |
| <b>2 Algorithmen und Komplexität</b>                            | <b>29</b> |
| 2.1 Algorithmen . . . . .                                       | 29        |
| 2.2 Algorithmisch lösbare und unlösbare Probleme . . . . .      | 37        |
| 2.3 Effizienz von Algorithmen und die Klasse <b>P</b> . . . . . | 42        |
| 2.4 Wer wird Millionär? Die Klasse <b>NP</b> . . . . .          | 51        |
| 2.5 Randomisierte Algorithmen . . . . .                         | 55        |
| <br>                                                            |           |
| <b>3 Zahlentheoretische Grundlagen</b>                          | <b>65</b> |
| 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        |

|           |                                                         |            |
|-----------|---------------------------------------------------------|------------|
| <b>4</b>  | <b>Primzahlen und Kryptographie</b>                     | <b>103</b> |
| 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        |
| <b>II</b> | <b>Der AKS-Algorithmus</b>                              | <b>123</b> |
| <b>5</b>  | <b>Der Ausgangspunkt: Fermat für Polynome</b>           | <b>125</b> |
| 5.1       | Eine Verallgemeinerung des Satzes von Fermat . . . . .  | 125        |
| 5.2       | Die Idee des AKS-Algorithmus . . . . .                  | 131        |
| 5.3       | Der Agrawal-Biswas-Test . . . . .                       | 134        |
| <b>6</b>  | <b>Der Satz von Agrawal, Kayal und Saxena</b>           | <b>139</b> |
| 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        |
| <b>7</b>  | <b>Der Algorithmus</b>                                  | <b>153</b> |
| 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        |
| <b>A</b>  | <b>Offene Fragen über Primzahlen</b>                    | <b>163</b> |
| <b>B</b>  | <b>Lösungen und Hinweise zu wichtigen Aufgaben</b>      | <b>175</b> |
|           | <b>Notationsverzeichnis</b>                             | <b>201</b> |
|           | <b>Stichwortverzeichnis</b>                             | <b>203</b> |
|           | <b>Literaturverzeichnis</b>                             | <b>209</b> |

Primzahltests für Einsteiger  
Zahlentheorie – Algorithmik – Kryptographie  
Waldecker, R.; Rempe-Gillen, L.  
2016, XX, 211 S., Softcover  
ISBN: 978-3-658-11216-5