Buchrezension

Elementary Number Theory, Cryptography and Codes

Eine Rezension zu
M.W. Baldoni, C.Ciliberto, G.M. Piacentini Cattaneo
Elementary Number Theory, Cryptography and Codes

Springer Verlag 2008, 522 Seiten, Taschenbuch, 53,45€, ISBN-13: 978-3-540-69199-0

Rezensiert von Peter Patzt

Zahlentheorie und Algebra wurden oft unterstellt Bereiche der Mathematik zu sein, die rein theoretischen Nutzen haben. Dies hat sich aber vorallem im 20. Jahrhundert stark geändert, in dem beide Gebiete grundlegend für Krytographie und Codes verwendet wurden. Beides ist heute in unserer Gesellschaft mit DVDs, Online-Banking und Weltraumfahrten nicht mehr wegzudenken. „Elementray Number Theory, Cryptography and Codes“ zeigt also nicht nur die theoretischen Hintergrunde der Zahlentheorie und Algebra auf, sondern vermittelt auch ihre praktische Anwendung und erläutert sehr eingängig die verschiedenen wichtigen Verfahren der Kryptographie und Codierungstheorie, die heutzutage verwendet werden.

Das Buch enthält neun Kapitel, die klar aufeinander aufbauen. Da sich das Buch ohne weitere Hilfsmittel verstehen lassen will, fängt es im 1. Kapitel mit den mathematischen Grundlagen an. Die vollständige Induktion, der euklidische Algorithmus und ähnliche grundlegenede Werkzeuge werden erklärt.

Das 2. Kapitel dreht sich komplett um die Komplexität von Algorithmen. Die Landaunotation wird eingeführt und an Beispielen weiter erläutert. Dieses Kapitel setzt die Grundlage dafür, dass in den weiteren Kapiteln immer wieder nach der Effizienz von Algorithmen gefragt wird. So werden die Effizienz von Primzahltest und Faktorisierungsmethoden im 6. Kapitel näher beleuchtet und bilden damit eine Voraussetzung für spätere kryptographische Methoden.

In den Kapiteln 3-5 wird nunmehr im Detail auf die Mathematik der Zahlentheorie und Algebra, insbesondere der der endlichen Körper, eingegangen. Das 3. Kapitel führt zunächst die Rechnung mit Restklassen ein und behandelt das Thema der Teilbarkeit mit diesen Mitteln. Im 4. Kapitel werden als erstes wesentliche Eigenschaften von Primzahlen besprochen und danach Primzahlen auf den algebraischen Strukturen der Ringe allgemeiner betrachtet. Die Frage welche Art Ringe die Primzahlstruktur der ganzen Zahlen wiederspiegelt wird u.a. beantwortet. Auch das 5. Kapitel ist zweiteilig. Zunächst wird etwas Körpertheorie eingeführt. Anschließend geht es vor allem um quadratische Kongruenzen und die damit verbundenen Legendre- und Jacobi-Symbole.

Das 6. Kapitel geht, wie bereits erwähnt, auf Methoden bzw. Algorithmen für Primzahltests und Faktorisierungen einer Zahl ein. Hierbei werden die klassischen Primzahltests, sowie der wichtige AKS-Primzahltest vorgestellt. Außerdem werden Faktorisierungsmethoden wie die Fermat-Faktorisierung, das Quadratische Sieb und die ρ-Methode erläutert.

Die anschließenden Kapitel 7-9 enthalten sehr praktischen Beschreibungen der Algorithmen für Kryptographie und Codierungstheorie. Das 7. Kapitel befasst sich umfassend mit der Kryptographie von ihren Anfängen bis hin zu den modernen und heutzutage angewandten Methoden assymetrischer Verschlüsselungen wie RSA oder elliptischer Kurven. Das 8. Kapitel gibt nun einen Einblick in die Codierungstheorie, die Fehler in der Übertragung erkennen und verbessern soll. Es werden einige wichtige Schranken bewiesen und Beispiele für effiziente Codes konstruiert. Zuletzt

wird im 9. Kapitel eine Vorstellung vermittelt, wie Quanten-Computer funktionieren könnten und welche Einflüsse dessen Existenz vor allem auf die Kryptographie haben kann.

Im Ganzen wirkt das Buch sehr gut durchdacht und gewinnt auch durch die zahlreichen Übungsaufgaben, sowie Programmieraufgaben zusätzlich an Reiz. Diese werden aber auch an zahlreichen Stellen genutzt um einfache Aussagen im Text nicht bis ins kleinste auszuformulieren. Dieser Ansatz macht sich besonders gut für Studenten die sich in das Thema einarbeiten wollen, da es so das Verständnis fördert. Aber auch für fortgeschrittene Leser ist es vorteilhaft leichte oder ihnen bekannte Aussagen schnell zu überlesen. Durch die hervorragende Darstellung der Algorithmen lässt sich dieses Buch auch als Nachschlagewerk verwenden.

Zusammenfassend lässt sich sagen, dass sich das Buch sowohl zum Selbststudium als auch zur Vorbeitung einer Vorlesung zu diesen Themen sehr gut eignet. Trotz einiger Stolpersteiner in der Übersetzung aus dem Italienischen lassen sich die Inhalte gut verstehen und sehr viele Beispiele und Übungsaufgaben tragen zum weiteren Verständnis bei.