

R. Crandall, C. Pomerance: Prime Numbers. A Computational Perspective. Second Edition. Springer Science+Business Media, Inc., 2005. XV + 597 S., ISBN 0-387-25282-7, H/b.

Dieses Buch, geschrieben von zwei weltbekannten Mathematikern, betrachtet – wie der Name schon sagt – das weite Gebiet der Primzahlen, vor allem aus computationeller und algorithmischer, aber auch aus zahlentheoretischer Sicht.

Im ersten Viertel des Buches wird zum einen eine allgemeine Einführung in Primzahlen (z.B. spezielle Arten von Primzahlen) und die wichtigsten Sätze und Vermutungen dazu gegeben, zum anderen werden die im weiteren Verlauf des Buches benötigten Grundlagen aus der Zahlentheorie dargestellt, wie etwa die modulare und polynomielle Arithmetik usw.

Nach einer Klassifizierung von Primzahlen und Pseudo-Primzahlen und den zugehörigen Algorithmen und Sätze, wie etwa diverse Siebmethoden, werden die wichtigsten Methoden zum Beweis der Primalität vorgestellt.

Die nächsten beiden Kapitel betrachten exponentielle und subexponentielle Faktorisierungsalgorithmen. Nach einem Kapitel über elliptische Kurven und deren Anwendung zum Beweis von Primalität folgt schließlich ein Streifzug durch die verschiedenen Anwendungsgebiete der Primzahlen: Von der Kryptografie, über Zufallszahlen, Quasi-Monte Carlo Methoden, diophantische Analysis bis hin zu Quantencomputern und -algorithmen wird die Relevanz der Theorie der Primzahlen beispielhaft veranschaulicht. Zum Abschluß des Buches findet sich schließlich noch ein Kapitel über effiziente Algorithmen für die Arithmetik mit großen Integer-Zahlen.

Neben dem sehr gut geschriebenen Text zur Theorie gibt es zu jedem Abschnitt zahllose Übungsaufgaben, die an normale Studenten gerichtet sind, sowie zusätzlich etliche Forschungsaufgaben von noch nicht gelösten Problemen zum jeweiligen Abschnitt. Außerdem sind die im Buch als Pseudocode vorgestellten Algorithmen als Mathematica-Paket "Prime Kit" auf der Homepage der von Crandall gegründeten Firma "Perfectly Scientific Inc." zum Download verfügbar (<http://www.perfsci.com/>).

R. Kainhofer (Wien)