

Vorwort zur zweiten Auflage

Diese zweite Auflage unterscheidet sich von der ersten hauptsächlich durch die Korrektur von kleinen Fehlern. Wir bedanken uns bei allen, die uns auf solche hingewiesen haben, vor allem bei Jörn Peter und Dierk Schleicher, und wir bitten um Verzeihung für jene Ungenauigkeiten, die uns bei der Revision mit Sicherheit noch entgangen sind. Für Hinweise auf Fehler oder veraltete Informationen sind wir weiterhin dankbar.

Die einzige größere Veränderung haben wir in Kapitel 1 vorgenommen: Dort haben wir den Beweis des Fundamentalsatz der Arithmetik vorgezogen, weil uns das im Nachhinein als natürlicher erschien und besser mit dem Vorgehen in Kapitel 3 harmoniert. Außerdem waren im Anhang, aufgrund spannender neuer Entwicklungen in der Zahlentheorie in den letzten Jahren, einige Aktualisierungen erforderlich!

Lasse Rempe-Gillen und Rebecca Waldecker
Sommer 2015

Vorwort zur ersten Auflage

„Forschung in der Mathematik – wie geht das denn?“ Mit dieser Frage werden wir in Gesprächen häufig konfrontiert. Dass in Physik, Chemie, Biologie und weiteren Wissenschaften noch viele Fragen ungelöst sind, ist wohl weithin bekannt. Aber dass dies auch in der Mathematik der Fall ist, scheint selbst mathematikinteressierten Menschen kaum bewusst zu sein.

Das hängt einerseits mit dem Bild der Mathematik in der Gesellschaft zusammen, andererseits aber auch mit der Natur der modernen Mathematik selbst. Etwa besteht eine Schwierigkeit darin, dass aktuelle mathematische Fragestellungen und Ergebnisse für Nichtexperten meist nicht zugänglich sind. Selbst für uns als Mathematiker sind Forschungsergebnisse, welche nicht in unsere Spezialgebiete fallen, kaum zu erschließen. Natürlich gibt es Ausnahmen zu dieser Regel, wie zum Beispiel den in den 1990er Jahren von Andrew Wiles bewiesenen **großen Satz von Fermat**, dessen Formulierung an Einfachheit kaum zu übertreffen ist¹. Doch gerade in diesem Fall ist der Beweis außerordentlich lang und schwierig, und nur wenige Experten weltweit sind wirklich in der Lage, ihn vollständig zu verstehen.

Im Sommer des Jahres 2002 gelang dem indischen Informatik-Professor Manindra Agrawal, gemeinsam mit seinen Studenten Neeraj Kayal und Nitin Saxena, ein Durchbruch im Gebiet der **algorithmischen Zahlentheorie**: Die drei Wissenschaftler beschrieben ein **effizientes** und **deterministisches** Verfahren, um festzustellen, ob eine gegebene natürliche Zahl eine Primzahl ist. (Die Bedeutung dieser Begriffe werden wir im Laufe dieses Buches erklären.) Besonders bemerkenswert an dieser Arbeit ist, dass sie trotz ihrer Bedeutung nur elementare mathematische Grundkenntnisse erfordert, welche Studenten der Mathematik oder Informatik üblicherweise im Grundstudium erwerben. Zusätzlich betrifft dieses Resultat einen Bereich der Mathematik, dessen Relevanz heute aufgrund der Anwendung von Verschlüsselungsverfahren im Internet (von „eBay“ bis zum Online-Banking) unbestritten ist.

Diese Konstellation empfanden wir als einzigartigen Glücksfall, weshalb wir

¹ „Ist $n > 2$, so gibt es keine ganzen Zahlen $a, b, c \neq 0$ mit $a^n + b^n = c^n$.“

im Sommer 2005 im Rahmen der „Deutschen SchülerAkademie“ einen Kurs zu diesem Thema angeboten haben. Dort haben wir über zweieinhalb Wochen hinweg 16 hochmotivierte Oberstufenschüler auf dem Weg von den Grundlagen bis zum Verständnis dieses aktuellen mathematischen Ergebnisses begleitet. Der Spaß, den die Teilnehmenden dabei hatten, und der Enthusiasmus, den sie an den Tag legten, motivierten uns, das vorliegende Buch zum selben Thema zu schreiben. Ein großer Teil des Manuskripts entstand daher zeitnah zur Schülerakademie, von November 2005 bis April 2007, und orientiert sich am Aufbau des Kurses. Wir danken Frau Schmickler-Hirzebruch vom Verlag Vieweg+Teubner für die reibungslose Zusammenarbeit und Helena Mihaljević-Brandt, Katharina Radermacher, Stefanie Söllner und Yasin Zähringer für ihre Hilfe beim Korrekturlesen. Ganz besonderer Dank gilt „unseren“ DSA-Kursteilnehmenden: Andreas, Christian, Coline, Ina, Fabian, Feliks, Haakon, Johannes, Katharina, Kerstin, Hinnerk, Martin und Martin, Tabea, Yasin und Yvonne – ihr wart ein wunderbarer Kurs! Ohne euch wäre dieses Büchlein nie entstanden!

Lasse Rempe und Rebecca Waldecker
Sommer 2009

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