Vorwort zur 1. Auflage

Die professionelle Konzeption, Implementierung und Anwendung von Informations- und Kommunikationstechnologien ist heutzutage mehr denn je ohne mathematische Grundlagen undenkbar. Professioneller und privater Einsatz und Gebrauch von Medien und Geräten wie z. B. das Internet, Handys, Audio- und Video-CDs, digitaler Rundfunk und digitales Fernsehen, sind nur deshalb in der vorhandenen Qualität möglich, weil mathematisch abgesicherte Verfahren zu deren Sicherstellung zur Verfügung stehen und eingesetzt werden.

Dieses Buch vermittelt Einsichten in grundlegende mathematische Konzepte und Methoden, auf denen diese Verfahren beruhen. Das Buch richtet sich an Studierende der Informatik sowie an Studierende der Mathematik in Haupt- oder Nebenfach. Es gibt eine Einführung in grundlegende mathematische Begriffe und Prinzipien wie Mengen, Logik, Relationen und Funktionen sowie in Induktion und Rekursion, und es beschäftigt sich darauf aufbauend intensiv mit zahlentheoretischen und algebraischen Grundlagen.

An zwei Themen, die für die eingangs genannten Anwendungen von großer Bedeutung sind, nämlich an der Verschlüsselung und Signatur sowie an der Codierung von Informationen, wird gezeigt, wie diese mathematischen Konzepte und Methoden eingesetzt werden, um Qualitäten wie Sicherheit, Vertraulichkeit, Verbindlichkeit und Fehlertoleranz zu erreichen.

Das Studium dieses Buches vermittelt Ihnen nicht nur die erwähnten Einsichten, sondern die Auseinandersetzung mit seinen Inhalten schult Ihre Fähigkeiten, abstrakt und logisch zu denken, sich klar und präzise auszudrücken, neue Probleme anzugehen und zu wissen, wann Sie ein Problem noch nicht vollständig gelöst haben. Es liefert Ihnen ein zeitinvariantes methodisches Rüstzeug für die Beschreibung und die Lösung von Problemen.

Ich habe versucht, die mathematischen Darstellungen durch informelle Zwischentexte zu motivieren und zu erläutern, so dass das Buch nicht nur als Begleitung und Ergänzung von mathematischen Lehrveranstaltungen nützlich, sondern insbesondere auch zum Selbststudium geeignet ist.

Das Schreiben und das Publizieren eines solchen Buches ist nicht möglich ohne die Hilfe und ohne die Unterstützung von vielen Personen, von denen ich an dieser

Stelle allerdings nur einige nennen kann: Als Erstes erwähne ich die Autoren der Lehrbücher, die ich im Literaturverzeichnis aufgeführt habe. Alle dort aufgeführten Bücher habe ich für den einen oder anderen Aspekt verwendet. Ich kann sie Ihnen allesamt für weitere ergänzende Studien empfehlen. Zu Dank verpflichtet bin ich auch vielen Studierenden, deren kritische Anmerkungen in meinen Lehrveranstaltungen zu Themen dieses Buches ich beim Schreiben berücksichtigt habe. Namentlich erwähnen möchte ich hier cand. inf. Harald Deuer, der mir nicht nur wertvolle inhaltliche Hinweise gegeben hat, sondern der mir auch jederzeit bei Problemen der Textverarbeitung hilfreich zur Seite gestanden hat. Trotz dieser Hilfen wird das Buch Fehler und Unzulänglichkeiten enthalten. Diese verantworte ich allein — für Hinweise zu deren Beseitigung bin ich dankbar.

Die Publikation eines Buches ist nicht möglich ohne einen Verlag, der es herausgibt. Ich danke dem Vieweg-Verlag für die Bereitschaft der Publikation und insbesondere Frau Schmickler-Hirzebruch für ihre Unterstützung und ihre Geduld bei der Entstehung des Buches.

Mein größter und herzlichster Dank gilt allerdings meiner Familie für den Freiraum, den sie mir für das Schreiben dieses Buches gegeben hat.

Bedburg, im Mai 2001

K.-U. W.

Vorwort zur 2. Auflage

Zunächst möchte ich all denjenigen Leserinnen und Lesern der 1. Auflage danken, von denen ich kritische Rückmeldungen erhalten habe. Leider hatten sich doch eine Reihe Fehler eingeschlichen, teilweise sogar von fataler Art. Ich habe versucht, mithilfe der Rückmeldungen diese alle zu beseitigen.

Daneben hat das Buch aber auch inhaltliche Überarbeitungen und Veränderungen erfahren. Zum einen habe ich die ersten dreizehn Kapitel über elementare mathematische Grundlagen, die eher einen Vorkurscharakter haben, herausgenommen. Die Kenntnis und das Verständnis dieser ist natürlich Voraussetzung für das Studium dieses Buches. Bei Bedarf finden Sie diese Kapitel unter „Vorkurse" auf der Seite

http://www.inf.fh-bonn-rhein-sieg.de/witt.html

Zum anderen behandele ich als weitere algebraische Strukturen Integritätsbereiche und endliche Körper. Der Grund dafür ist, dass wichtige Rechenstrukturen wie ganze Zahlen und Polynome Integritätsbereiche bilden, und in Integritätsbereichen der für weitergehende Betrachtungen und Anwendungen wesentliche Begriff der Teilbarkeit eingeführt werden kann und dessen Eigenschaften dort untersucht werden können. Die Betrachtungen endlicher Körper in diesem Buch vermitteln nicht nur erste nachhaltige Eindrücke über die Existenz, die Struktur und die Beschreibungsmöglichkeiten endlicher Mengen, in denen uneingeschränkt gerechnet werden kann. Endliche Körper bieten auch die Möglichkeit zur Konstruktion von Codes mit guten Fehlererkennungs- und Fehlerkorrektureigenschaften, wie sie bei der Codierung von CDs und DVDs verwendet werden. Die grundsätzlichen Konzepte und Methoden hierzu werden einführend ebenfalls in dieser Auflage betrachtet.

Bedburg, im November 2004

K.-U. W.

Vorwort zur 3. Auflage

Ich freue mich sehr darüber, dass dieses Buch weiterhin viel Interesse und Nachfrage sowohl bei Studierenden als auch bei Kolleginnen und Kollegen findet, was ich wieder durch viele Rückmeldungen erfahren habe – dafür vielen Dank an alle. Diese Rückmeldungen haben dazu geführt, dass ich weitere Fehler orthografischer oder logischer Art korrigiert habe. Außerdem habe ich einige Umstellungen vorgenommen sowie weitere Querweise eingefügt. Dadurch ist der inhaltliche Aufbau „logischer" geworden, und es soll noch deutlicher werden, dass die geeignete Verknüpfung von Ideen und Konzepten zu neuen theoretischen Kenntnissen und Lösungen von praktischen Problemen führt.

Des Weiteren habe ich eine Reihe weiterer Beweise zu wichtigen Sätzen angegeben, wie z.B. zum Satz, dass die Faktorisierung von Carmichael-Zahlen quadratfrei ist und mindestens drei Primfaktoren enthält, sowie zum Satz, dass der Miller-Rabin-Algorithmus, ein verbreitet angewendeter randomisierter Primzahltest, in einer Runde eine Irrtumswahrscheinlichkeit von höchstens ein Viertel hat. Außerdem habe ich das bisher nur erwähnte effiziente Verfahren zum Potenzieren durch wiederholtes Quadrieren ausführlich mithilfe von Beispielen erklärt; ebenso das Verfahren, mit dem auf der Basis des Chinesischen Restsatzes die Arithmetik sehr großer Zahlen auf das Rechnen mit sehr kleinen Zahlen zurückgeführt werden kann, und ich habe die Lösbarkeit und im gegebenen Fall ein Verfahren für die Berechnung der Lösung von linearen Kongruenzgleichungen für den allgemeinen Fall $ax = b\,(m)$ und nicht nur für den Spezialfall $b = 1$ angegeben.

Durch das Schließen dieser Lücken ist das Buch weiter „abgerundet" worden. Es würde mich sehr freuen, wenn das Buch dadurch noch interessanter für das Studium algebraischer und zahlentheoretischer Grundlagen und deren Anwendung in der Informatik geworden ist.

Bedburg, im Januar 2007

K.-U. W.