MuPAD Lectures

Friedrich Schwarz

Einführung in die Elementare Zahlentheorie

Einführung in die Elementare Zahlentheorie

Von Dr. rer. nat. Friedrich Schwarz
Universität-Gesamthochschule Paderborn

B.G.Teubner Stuttgart · Leipzig 1998

Dr. rer. nat. Friedrich Schwarz

Geboren 1937 in Hartmanitz. Studium der Mathematik, Physik und Astronomie in Würzburg. 1966 Promotion in Mathematik (Würzburg), von 1965 bis 1974 Assistent und Akademischer Rat an der Universität Saarbrücken, seit 1974 Akademischer Oberrat an der Universität Paderborn. Koautor (mit K. Kiyek) des Lehrbuchs „Mathematik für Informatiker I und II".

Die Deutsche Bibliothek – CIP-Einheitsaufnahme

Einführung in die elementare Zahlentheorie / von Friedrich Schwarz. – Stuttgart ; Leipzig : Teubner
(MuPAD lectures)

Additional material to this book can be downloaded from http://extra.springer.com.

ISBN-13: 978-3-519-02193-3 e-ISBN-13: 978-3-322-84813-0
DOI: 10.1007/978-3-322-84813-0

Buch. 1998
kart.
CD-ROM. 1998

Vorwort

Dieses Buch ist aus Vorlesungen "Mathematik am Computer" entstanden, die ich an der Universität Paderborn seit 1988 mehrmals gehalten habe. Diese Vorlesungen sind für Studierende der Diplomstudiengänge Mathematik und Technomathematik und des Lehramtsstudiengangs Mathematik für die Sekundarstufe II im zweiten oder dritten Semester obligatorisch; ihr Ziel ist es, die Hörer an Hand eines mathematischen Stoffs mit einem Computer-Algebra-System vertraut zu machen oder umgekehrt, ihnen mit Hilfe eines Computer-Algebra-Systems einen mathematischen Stoff näher zu bringen. Die Themen, die dabei behandelt wurden, entstammten der Linearen Algebra, der Kombinatorik und insbesondere der Elementaren Zahlentheorie; das Computer-Algebra-System war zuerst Maple und seit dem Sommersemester 1993 MuPAD.

Dieses Buch ist eine Einführung in die Elementare Zahlentheorie, wobei besonderer Wert auf Algorithmen und ihre praktische Umsetzung in Computerprogramme gelegt wird. Es gibt bereits Bücher mit einer ähnlicher Zielsetzung, nämlich das Buch [43] von P. Giblin, das Pascal als Programmiersprache verwendet, und das Buch [34] von O. Forster, für das eine eigene Software entwickelt wurde. Ich versuche in diesem Buch zu zeigen, daß sich auch ein Computer-Algebra-System wie MuPAD für die Behandlung der Algorithmen, an denen die Elementare Zahlentheorie überaus reich ist und die bereits dem Anfänger in diesem Gebiet der Mathematik gut zugänglich sind, hervorragend eignet. Selbstverständlich ist die Elementare Zahlentheorie nicht das einzige Gebiet, in dem sich zeigt, wie fruchtbar der Einsatz eines Computer-Algebra-Systems für das Verständnis von Mathematik ist. Daß Computer und insbesondere Computer-Algebra-Systeme in der Ausbildung von Mathematikern und auch und vielleicht ganz besonders in der Ausbildung von Mathematiklehrern eine wichtige Rolle spielen müssen, wird niemand bezweifeln. Wer anfängt, darüber nachzudenken, sollte einige der in [56] gesammelten Aufsätze von D. E. Knuth lesen; eigenes Tun wird ebenso überzeugen.

Die Stoffe, von denen dieses Buch handelt, sind zum größeren Teil Stoffe, die wohl in jeder Einführung in die Zahlentheorie vorkommen. Im ersten Kapitel ist von der Teilbarkeit im Ring $\mathbb{Z}$ und von Primzahlen die Rede. Das zweite Kapitel behandelt die Restklassenringe von $\mathbb{Z}$ und ihre Einheitengruppen; die dabei hergeleiteten Ergebnisse über Potenzreste dienen im dritten Kapitel der ausführlichen Diskussion des stochastischen Primzahltests von M. O. Rabin. Dieses Kapitel behandelt außerdem die einfachsten Methoden zur Erzeugung von Zufallszahlen und beschreibt in aller Kürze aus dem weiten Feld

der Kryptologie die bekanntesten der public-key-Systeme, deren Beschreibung, Begründung und Diskussion ohne die Elementare Zahlentheorie nicht möglich sind. Im vierten Kapitel ist von den quadratischen Resten die Rede und im fünften Kapitel von den Kettenbrüchen. Dabei werden die endlichen Kettenbrüche zur Begründung des von R. S. Lehman angegebenen Faktorisierungsverfahren für natürliche Zahlen verwendet; die im Anschluß daran hergeleiteten Resultate über unendliche und insbesondere periodische Kettenbrüche erlauben die vollständige Diskussion eines berühmten Typs Diophantischer Gleichungen, nämlich der Pellschen Gleichungen. Die mathematischen Kenntnisse, die vorausgesetzt werden, gehen nicht über das hinaus, was man in den Vorlesungen des ersten Semesters lernt; dem Leser sollten jedenfalls die Begriffe Gruppe, Ring und Körper vertraut sein. Die nötigen Ergebnisse über endliche abelsche Gruppen werden im dritten Kapitel hergeleitet.

Das Buch ist auch eine Einführung in den Gebrauch eines Computer-Algebra-Systems und zwar des Computer-Algebra-Systems MuPAD. Von den selbstverständlichen Fertigkeiten, die ein Benutzer eines Computers im allgemeinen und von MuPAD im besonderen verfügen muß, wird dabei nicht gesprochen, auch nicht über die Grundregeln des Programmierens; über alles, was MuPAD betrifft, informiert das ausfürliche Online-Manual. Vielmehr wird in den Umgang mit MuPAD und insbesondere in das Programmieren mit MuPAD an Hand von Beispielen eingeführt; von Anfang wird der Leser in den zahlreichen Aufgaben zum Experimentieren und zu selbständigem Programmieren aufgefordert. Die Aufgaben sind ein wichtiger Teil des Buchs: Den Umgang mit einem Computer-Algebra-System lernt man nur an konkreten Beispielen und durch eigenes Tun.

Das Computer-Algebra-System MuPAD wird seit 1989 an der Universität Paderborn von einer überaus engagierten und kompetenten Arbeitsgruppe unter der Leitung von Professor Dr. Benno Fuchssteiner und seit kurzem auch von der daraus hervorgegangenen Firma SciFace Software entwickelt und betreut. Ohne die Hilfe aller Mitglieder dieser Gruppe hätte dieses Buch nicht geschrieben werden können. Ich danke allen für ihre tatkräftige Hilfe und für die Geduld, mit der sie meine Anregungen, Fragen und Klagen angehört haben, auch die, die nicht vernünftig oder nicht sachkundig waren.

Ich widme dieses Buch der Erinnerung an meinen Doktorvater Professor Dr. Hermann Schmidt (Merkendorf 22.7.1902 – 26.2.1993 Würzburg). Von ihm habe ich zum ersten Mal von Kettenbrüchen und quadratischen Formen gehört. Er hat in allen Gebieten der Mathematik, mit denen er sich beschäftigt hat, und besonders auch in der Zahlentheorie immer die algorithmischen Aspekte herausgearbeitet und den Hörern seiner Vorlesungen näher gebracht.

Paderborn, im Mai 1998

Friedrich Schwarz (fritz@uni-paderborn.de)

Der Inhalt der CD

Die dem Buch beiliegende CD enthält

- das Computer-Algebra-System MuPAD Light 1.4.1, zusammen mit allen Programm-Bibliotheken und einem ausführlichen Online-Manual, sowie weiterer Dokumentation,
- eine interaktive Fassung dieses Buchs, zusammen mit den Lösungen der über 80 Aufgaben, und
- zu jedem Paragraphen des Buchs, der Aufgaben enthält, eine Bibliothek der MuPAD-Funktionen, deren Herstellung in den Aufgaben gefordert wird; die Beispiele im Buch und in den Lösungen können per Mausklick in ein MuPAD-Fenster übertragen und dort ausgeführt werden,
- ein interaktives Dokument, in dem beschrieben wird, wie man eine berühmte Aufgabe von Archimedes löst und mit Hilfe von MuPAD eine Lösung berechnet, und
- eine Bibliothek `primelib`, mit deren Hilfe man größere Primzahlen berechnen kann als mit MuPAD allein, nämlich Primzahlen bis zur 2 000 000 000-ten Primzahl 47 055 833 459, und die einige weitere Funktionen zu Verfügung stellt, die beim Umgang mit Primzahlen nützlich sein dürften.

Rechnerkonfiguration: Die Nutzung des Computer-Algebra-Systems MuPAD Light und des interaktiven Buchs erfordert einen PC mit Windows 95 oder Windows NT 4.0 (Pentium empfohlen), 20 MB Hauptspeicher (32 MB empfohlen) und 20 MB freien Festplattenplatz bei minimaler, bzw. 50 MB bei normaler Installation.

Installation: Zur Installation von MuPAD Light und dem interaktiven Buch startet man `setup.exe` im Basisverzeichnis der CD. Das Setup-Programm führt durch die Installation. Der Benutzer hat die Wahl zwischen der normalen Installation, die neben MuPAD Light, dem interaktiven Buch und dem Dokument über die Aufgabe des Archimedes auch die Bibliothek `primelib` installiert, und einer minimalen Installation, die `primelib` nicht installiert. Beide Installationen legen, wenn die Voreinstellungen im Setup-Programm vom Benutzer nicht verändert werden, einen Ordner

`C:\Programme\SciFace\Zahlentheorie mit MuPAD`

an, der einen Ordner `MuPAD Light 1.4.1` und einen Ordner `Zahlentheorie` enthält. Der erste enthält MuPAD Light 1.4.1 selbst und der zweite in einem Ordner `doc` die interaktive Version dieses Buchs und das Dokument über die Aufgabe von Archimedes, sowie in einem Ordner `lib` die Programm-Bibliotheken zu den Lösungen der Aufgaben. Wenn der Benutzer die normale Installation gewählt hat, so enthält der Ordner `Zahlentheorie mit MuPAD` einen weiteren Ordner `primelib`, der in einem Unterordner `lib` die Programme der Bibliothek `primelib` und in einem Unterordner `doc` die Dateien `primelib.dvi`, `primelib.bsp`, `primelib.hyp` und `primelib.lab` enthält.

Gebrauchsanweisung: Zum Start des interaktiven Buchs wählt man entweder `Zahlentheorie` im Startmenü von `Zahlentheorie mit MuPAD` oder aktiviert das Icon `zahlentheorie.dvi` im Ordner `Zahlentheorie\doc`. Das Buch wird daraufhin mit einer Titelseite geöffnet. Mit Hilfe der Schaltflächen in der Kopfleiste kann man vorwärts oder rückwärts blättern und mit Hilfe des Menüs `Targets` zum Inhaltsverzeichnis, zum Index oder zu den Lösungen springen; nach einem solchen Sprung kann man mit Hilfe einer Schaltfläche zum Ausgangspunkt im Text zurückspringen. Auf vielen Seiten, insbesondere dort, wo die Aufgaben des Buchs gelöst werden, findet man farbig markierte Textstellen; ein Mausklick auf eine solche Stelle löst einen Sprung innerhalb des Texts oder ins Literaturverzeichnis aus. Ein doppelter Mausklick auf ein farbig markiertes `>>`-Zeichen startet MuPAD Light, falls es nicht schon vorher gestartet wurde, und überträgt die auf `>>` folgende MuPAD-Eingabe in das MuPAD-Light-Fenster, wo sie durch `Enter` oder `Return` an MuPAD zur Ausführung übergeben wird.
Man kann das interaktive Buch auch aus einer MuPAD-Sitzung heraus starten, indem man vom Menü `Help` aus das Manual startet und darin vom Menü `File` aus die Datei `zahlentheorie.dvi` im Ordner `Zahlentheorie\doc` öffnet.
Das Dokument, das die Aufgabe von Archimedes behandelt, kann man entweder durch Wahl von `Das Rinderproblem` vom Startmenü von `Zahlentheorie mit MuPAD` aus öffnen oder durch Öffnen der Datei `rinderproblem.dvi` im Ordner `Zahlentheorie\doc`.

Für Einsteiger: Lesern dieses Buchs, die noch nicht mit MuPAD zu tun hatten, wird das Studium der Dokumente `erste_schritte.dvi`, `demo.dvi` und `advdemo.dvi` im Ordner `MuPAD Light 1.4.1\doc\dvi` empfohlen. Dazu startet man, wie oben beschrieben, in einer MuPAD-Sitzung vom Menü `Help` aus das Manual und öffnet darin vom Menü `File` aus `erste_schritte.dvi`, `demo.dvi` oder `advdemo.dvi`.

Die Bibliothek `primelib`: Die Bibliothek `primelib` kann auch nachträglich installiert werden. Welche Dateien in welche Ordner zu kopieren sind, fin-

det man weiter oben in dem Abschnitt, der die Installation beschreibt. Man braucht auch nicht alle Primzahltafeln, die zu `primelib` gehören, auf seine Festplatte zu kopieren; dann sollte man aber die Funktionen `prime` und `pi` in `primelib` anpassen.

MuPAD Pro 1.4: Die CD enthält auch eine Vollversion des Computer-Algebra-Systems MuPAD, deren Nutzungsdauer auf 30 Tage beschränkt ist. Zur Installation dieser Demo-Version startet man `setup.exe` im Verzeichnis `MuPAD Pro 1.4` auf der CD. Ein Dokument, das über die Unterschiede zwischen MuPAD Light und MuPAD Pro informiert, kann man entweder durch Wahl von `MuPAD Pro` im Startmenü von `Zahlentheorie mit MuPAD` öffnen oder durch Öffnen der Datei `MuPAD Pro.doc` im Ordner `Zahlentheorie mit MuPAD`.

Registrierung: Die Registrierung von MuPAD Light ist jedem Benutzer empfohlen, schon weil durch sie der für MuPAD Light reservierte Arbeitsspeicher vergrößert wird. Man registiert entweder

- über `http://www.sciface.com`: Der Abschnitt `Download` enthält einen Eintrag `Register`, der ein Formular zur Online-Registrierung bereitstellt, oder
- durch einen Brief oder eine E-mail an die unten angegebene Adresse der Firma SciFace Software.

Die Registrierung ist für Schüler und Lehrer, für Mitarbeiter nicht-kommerzieller Forschungsinstitute, für alle, die an Hochschulen und Universitäten in Lehre und Forschung tätig sind, und natürlich für alle Käufer dieses Buchs kostenfrei.

Anschrift der Firma SciFace Software:

SciFace Software GmbH & Co. KG
Technologiepark 12
D-33100 Paderborn
Tel.: 05251/640751 – Fax: 05251/640799
E-mail: `info@sciface.com`
WWW: `http://www.sciface.com`

Anschrift des Autors:

Dr. Friedrich Schwarz
Universität Paderborn, Fachbereich 17
D-33095 Paderborn
Tel.: 05251/602602
E-mail: `fritz@uni-paderborn.de`

Inhaltsverzeichnis