Nem az a fontos, hogy tudjuk-e formálni a követ, hanem, hogy mivé.†

Melocco Miklós

Vorwort

Ich habe in dem akademischen Jahr 1990/91 die Ehre gehabt, auf Einladung von Prof. Dr. Johannes Buchmann eine Vorlesung über Computeralgebra an der Universität des Saarlandes halten zu können. Die Notizen zu dieser Vorlesung bilden die Grundlage des vorliegenden Buches. Dieses Material wurde zwar ergänzt und umstrukturiert, aber die Grundkonzeption blieb unverändert.

Dieses Buch befaßt sich mit algebraischen Algorithmen vom Gesichtspunkt der Arithmetik. Ich konzentriere mich auf solche algebraischen Begriffe und Methoden, welche sich als anwendbar erwiesen haben für die Lösung arithmetischer, insbesondere Diophantischer Aufgaben.

Die Grundalgorithmen der Arithmetik, die Operationen über den ganzen Zahlen, haben ihre heutige, wohlbekannte Form nach einer mehrere tausend Jahre dauernden Entwicklung bekommen. Der Bedarf für fehlerfreie Rechnung mit potentiell beliebig großen ganzen Zahlen hat sogar auf diesem Gebiet neue, unerwartete Kenntnisse geliefert. Die Entdeckung von A. Karatsuba und später von A. Schönhage und V. Strassen, daß wesentlich schnellere Multiplikationsalgorithmen existieren als die 'Grundschulmethode', war mir richtungsgebend bei der Wahl des Stoffes. Die Betrachtung klassischer Begriffe und Konstruktionen vom algorithmischen Gesichtspunkt führt oft zu interessanten neuen Entdeckungen. Ich möchte hier als Beispiel die Primzahltests, die effiziente Faktorisierung ganzer Zahlen und Polynome, die Bestimmung von Basen von Gittern und Polynomidealen mit günstigen Eigenschaften nennen. Solche Entdeckungen bereichern die Mathematik durch neue Fragestellungen und durch die Entwicklung neuer oder fast vergessener Gebiete. Ich denke hier zum Beispiel an die Theorie der endlichen Körper.

Die Computeralgebra, das heißt die Theorie der algebraischen Algorithmen, entwickelte sich in den letzten Jahren aus einem Forschungsgebiet weniger Wissenschaftler zu einer weit verbreiteten Technologie. Durch die Implementierung algebraischer Algorithmen entstanden die Computeralgebra-Systeme. Die Benutzer haben heute schon eine große Auswahl. Sie können wählen zwischen allgemeinen Systemen, wie DERIVE, MAGMA, MAPLE, MATHEMATICA,... Für die Lösung spezieller Aufgaben stehen ebenfalls viele Systeme zur Verfügung, wie GAP, KANT, PARI, SIMATH, UBASIC,... Die Entwicklung der Theorie und Technologie der Computeralgebra-Systeme wurde durch die leistungsfähigen und allgemein zugänglichen Rechenmaschinen wesentlich beschleunigt. Ich beschäftige mich in diesem

†'Die Frage ist nicht die, ob wir den Stein formen können, sondern wozu.' Mit diesem Gedanken des ungarischen Bildhauers Miklós Melocco möchte ich meine tiefste Verehrung dem Andenken meines Vaters und jedem Steinmetz ausdrücken.

Buch nicht mit den Implementierungen, aber ich richte die Aufmerksamkeit auf die Darstellungsmöglichkeiten der betrachteten Objekte. Ich lege ebenfalls einen besonderen Wert auf die Analyse der Algorithmen.

Das Buch ist in acht Kapitel gegliedert. In Kapitel 1 führe ich eine Pseudoprogrammiersprache für die Darstellung der Algorithmen ein. Kapitel 2 beschäftigt sich mit der allgemeinen Theorie der Euklidischen Ringe, insbesondere mit der Primfaktorzerlegung und mit der Bestimmung des größten gemeinsamen Teilers. In Kapitel 3 analysiere ich die Grundoperationen ganzer Zahlen. Modulare Methoden, der chinesische Restalgorithmus und endliche Körper werden in Kapitel 4 bearbeitet. Hier stellen wir noch einige Primzahltests und Faktorisierungsmethoden ganzer Zahlen dar. Die Schwerpunkte des langen Kapitels 5 sind die Kettenbruchentwicklung reeller Zahlen und Algorithmen für Gitter. Wir präsentieren hier Methoden für die Lösung Pellscher und Thuescher Gleichungen, sowie die Fincke-Pohst und LLL Algorithmen. Kapitel 6 ist eine Einführung in Polynomringe. Wir analysieren wieder die Grundoperationen und führen mehrere Maßbegriffe ein. Für die Berechnung des größten gemeinsamen Teilers von Polynomen stellen wir zwei Methoden dar; die erste beruht auf polynomialen Restfolgen, die zweite ist eine modulare Methode. Faktorisierung von Polynomen über endlichen Körpern und über $\mathbb{Z}$ ist das Thema von Kapitel 7. In dem letzten Kapitel beschäftigen wir uns mit Polynomidealen. Das Hauptziel ist dabei, den Buchberger Algorithmus für die Berechnung der Gröbner Basen von Polynomidealen zu formulieren. Als Abschluß des Buches behandeln wir einige Anwendungen von Gröbner Basen.

Die Nummern der Gleichungen, Algorithmen, Lemmata, Sätze und Folgerungen haben zwei Glieder. Auf der ersten Position steht die laufende Nummer des Kapitels. Die Zahl auf der zweiten Position ist die laufende Nummer der betreffenden Gleichung, etc. innerhalb des Kapitels. Diese Nummern dienen als Kreuzreferenzen. Nummern in eckigen Klammern verweisen auf das Literaturverzeichnis.

Wir definieren die Begriffe immer. Es kommen aber Sätze vor, welche wir ohne Beweis zitieren. In solchen, wenigen Fällen verweisen wir auf die relevante Literatur. Wir setzen Kenntnisse eines Kurses über Lineare Algebra voraus, etwa den Stoff in den Büchern von F.R. Gantmacher [46] oder G. Fischer [43]. Darüber hinaus soll der Leser über gewisse Programmiererfahrung in einer höheren Programmiersprache verfügen.

In den letzten Jahren sind mehrere Bücher mit verwandtem Thema erschienen. Ich denke an die Bücher Th. Becker und V. Weispfenning [10], B. Buchberger et al. [20], H. Cohen [30], D. Cox et al. [34], J.H. Davenport et al. [37], M. Mignotte [74], M. Pohst und H. Zassenhaus [81], M. Pohst [82] und F. Winkler [113]. Aus diesen, aus den Vorlesungsnotizen von F. Winkler et al. [113, 114] und aus der klassischen Monographie von D.E. Knuth [63] habe ich sehr viel gelernt, und ich kann sie zur Vertiefung der Kenntnisse meinem Leser gerne empfehlen.

Ich habe Algebra zuerst aus dem ausgezeichneten Lehrbuch von T. Szele [105] gelernt. Dieses Buch ist leider nur auf ungarisch erhältlich. Obwohl Professor Szele schon längst verstorben war, als ich mein Studium an der Lajos Kossuth Universität in Debrecen angefangen hatte, kann man seine Wirkung sicherlich auch in diesem Buch spüren. Ich danke meinen Professoren K. Buzási, J. Erdős und K. Győry,

daß sie mir die Welt der Algebra, der Zahlentheorie und der Algorithmen eröffnet haben. Mein bester Dank gilt den Kollegen Professoren J. Buchmann, I. Gaál, K. Győry, M. Mignotte, M. Pohst und H.G. Zimmer. Unsere gemeinsamen Arbeiten und Diskussionen haben zur Ausformung des Stoffes wesentlich beigetragen. I. Gaál und F. Lemmermeyer haben das Manuskript sorgfältig gelesen. Auf ihren Rat habe ich zahlreiche Fehler korrigiert.

Mein besonderer Dank gilt dem Herausgeber, Herrn Prof. Dr. Michael Pohst. Das Rohmanuskript hat er mit riesiger Geduld gelesen und sorgfältig korrigiert. Er hat für die Ausbesserung der Ungenauigkeiten und Inkonsequenzen sehr viele wertvolle Vorschläge gemacht. Ohne seine Hilfe wäre dieses Buch nie erschienen.

Debrecen, den 30. März 1999