Wilfried Nöbauer, TU Wien

Algorithmen und ihre Komplexität

Das Wort "Algorithmus" ist ein mathematischer Fachausdruck, der in den letzten Jahrzehnten wieder zunehmend an Bedeutung gewonnen hat. Dabei ist keineswegs klar festgelegt, was mit diesem Fachausdruck gemeint ist. Im mathematischen Wörterbuch von Naas-Schmidt aus dem Jahre 1967 beginnt das Stichwort "Algorithmus" folgendermaßen:

"Ein Algorithmus in einer Menge X von Zeichenreihen (Wörtern) ist ein Verfahren zur "effektiven" (schrittweisen) Umformung von Zeichenreihen, wobei man von jeder Zeichenreihe Z' in endlich vielen Schritten feststellen kann, ob sie aus einer gegebenen Zeichenreihe Z durch Anwendung des Algorithmus erhalten werden kann oder nicht. Es gibt bisher im wesentlichen die folgenden beiden Präzisierungen des Begriffs eines Algorithmus:" Hierauf werden die Postsche und die Markowsche Definition des Algorithmus angegeben.

Arthur Engel hingegen beginnt das Einleitungskapitel seines Buches "Elementarmathematik vom algorithmischen Standpunkt" so:

"Die Haupttätigkeit des Menschen ist das systematische Lösen von Problemen. Ein Problem wird in zwei Schritten erledigt. Zuerst konstruiert man eine genau definierte Folge von Anweisungen zur Lösung des Problems. Dies ist eine interessante und geistreiche Tätigkeit. Dann kommt die Ausführung der Anweisungen. In der Regel ist dies eine zeitraubende, langweilige Arbeit, die man einem Rechner überläßt. Eine Folge von Anweisungen zur Lösung eines Problems nennt man einen Algorithmus. Der Begriff des Algorithmus überlappt sich stark mit den Begriffen Rezept, Prozedur, Prozeß, Methode, Rechenverfahren.

Algorithmen kann man in der natürlichen Sprache formulieren. In der Regel verwendet man präzisere Sprachen, die sich zur Darstellung von Prozeßabläufen besser eignen. Die Darstellung eines Algorithmus in einer präzisen formalisierten Sprache nennt man ein Programm."

Zweifellos ist die von Engel gegebene Umschreibung des Begriffes "Algorithmus" wesentlich umfassender. Algorithmen in dem von Engel gemeinten Sinne treten schon seit der Entstehung der ersten Hochkulturen auf. Schon im alten Ägypten begann man, Probleme durch Zahlen zu beschreiben und ihre Lösung auf die Bestimmung gewisser Zahlen zurückzuführen. Probleme, bei denen dies möglich war, traten etwa auf im Zusammenhang mit der Ausführung von Großbauwerken, insbesondere von Bewässerungsbauten. Die Ausführung dieser Bauten erforderte den koordinierten Einsatz großer Menschenmassen; diese Koordination wurde geleistet von einer bereits hochentwickelten Bürokratie, und im Bereich dieser Bürokratie haben sich wohl auch die ersten Algorithmen entwickelt. So verwendeten die Ägypter etwa folgenden Algorithmus zur Multiplikation zweier Zahlen: Sie stellten den Multiplikator als Summe von Zweierpotenzen dar, berechneten das Produkt des Multiplikanden mit einer Zweierpotenz durch wiederholte Verdoppelung und addierten die erhaltenen Teilprodukte. So berechneten sie etwa 37·11 so:

37	1'
74	2'
148	4
296	8'
407	

Die Division führten sie durch Umkehrung dieser Methode aus, das heißt, sie führten vom Divisor ausgehend wiederholte Verdoppelung durch, bis sie auf eine Zahl kamen, die mindestens so groß wie der Dividend war, und konnten daraus den Quotienten

und den Rest ablesen. Die Division 753:26 verläuft nach dieser Methode so:

1	26	
2	52	25
4'	104	129
8'	208	337
16'	416	753
	832	

Man subtrahiert also 416 von 753, das gibt 337, davon subtrahiert man 208, das gibt 129, davon subtrahiert man 104, das gibt 25<26. Also ist der Quotient 16+8+4=28, und der Rest ist 25.

Auch die Hochkulturen in Babylonien verfügten zweifellos schon über beträchtliche Rechenfertigkeit und über gewisse Algorithmen - es ist darüber aber nicht sehr viel erhalten. Sie rechneten im Hexagesimalsystem, das sich in der Winkelmessung und der Zeiteinteilung bis heute erhalten hat, und verwendeten auch schon Tabellen, etwa solche der Quadrate und der Quadratwurzeln. Auf sie geht also vor allem das Prinzip zurück, immer wieder benötigte Rechenergebnisse, wenn man sie einmal gefunden hat, zu "speichern" und nach Bedarf "abzurufen", das in der weiteren Entwicklung des Rechnens eine wichtige Rolle spielte.

In der Kutlurperiode der Antike - genauer gesprochen der griechischen Antike - entstand die Wissenschaft Mathematik. Allerdings betrieben sie die Griechen fast ausschließlich als "reine" Wissenschaft, die nach Erkenntnissen, aber nicht nach praktischen Anwendungen strebte. Dementsprechend sahen sie das elementare Rechnen ebenso wie die Technik als eine untergeordnete Tätigkeit an, mit der sich die vornehmen Leute nicht beschäftigten, sondern die sie Taglöhnern oder Sklaven überließen. Zwar erforderte die Astronomie umfangreiche Berechnungen, die im

babylonischen Hexagesimalsystem durchgeführt wurden. Zum praktischen Rechnen aber, wie es im Geschäftsleben benötigt wurde, verwendete man ein "technisches" Hilfsmittel, nämlich den Abakus, das Rechenbrett (dessen Ursprung nicht geklärt ist und das erstmalig aus der Antike überliefert ist). Das Wort Abakus kommt wohl von dem griechischen "Abax", was etwa "fußloses Brett" heißt. Auf diesem Brett, das in senkrechte Spalten unterteilt ist, wobei jeder Spalte ein bestimmter Stellenwert zukommt, werden die Zahlen, mit denen gerechnet wird, mit Steinchen (lateinisch: calculi) gelegt, und mit einer relativ einfachen Technik können Zahlen addiert und subtrahiert werden; Multiplikationen und Divisionen sind auch ausführbar, wenn auch wesentlich komplizierter.

Der Abakus wurde von der europäischen Kultur des Mittelalters übernommen und noch etwas weiter entwickelt. Die Spalten werden nun waagrecht statt senkrecht angeordnet, weshalb man das Rechnen auf dem Rechenbrett auch als "Rechnen auf den Linien" bezeichnete. Dieses Rechnen auf den Linien hielt sich bis zum Beginn der Neuzeit und wurde nur langsam durch eine neue Form des Rechnens verdrängt.

Etwa ab 1200 ist der Abakus auch in China nachgewiesen und fand dort unter dem Namen Suan-Pan weite Verbreitung. Von den Japanern wurde der Suan-Pan zum Soroban weiterentwickelt und hat sich in dieser Form bis in unsere Zeit erhalten, wird nun allerdings zunehmend vom Taschenrechner abgelöst. Auch in der Sowjetunion ist der Abakus noch immer in Verwendung.

Im Abakus tritt neben den Algorithmen und Tabellen erstmalig als drittes Hilfsmittel zur Ausführung von Berechnungen die Anwendung von "Hardware" auf. Aber schon der Abakus erforderte zu seiner Bedienung auch "Software", also Bedienungsregeln, die entwickelt und von den Benützern des Abakus beherrscht werden mußten. Die abwechselnde oder gleichzeitige Anwendung

von Algorithmen, von Tabellen und von "Maschinen" hat seit dem Altertum die Entwicklung des Rechnens bestimmt.

Während nach dem Zusammenbruch der antiken Kultur in Europa ein schwerer kultureller Rückschlag eingetreten war, dessen Auswirkungen die zweite Hälfte des ersten Jahrtausends unserer Zeitrechnung bestimmten, entwickelte sich nach der stürmischen Ausbreitung des Islam im Raum des alten Babylonien erneut eine blühende Kultur, und Bagdad wurde zu einem Zentrum dieser Kultur. In dieser Stadt lebte um 820 der Perser Al-Khwarizmi. Dieser verfaßte ein Lehrbuch mit dem Titel "Hisab Al-Jabr wa'l muquabalah" - ein Buch über die Auflösung von Gleichungen und somit das erste Lehrbuch der "Algebra", deren Name ja aus dem Titel dieses Buches entstanden ist - sowie ein Rechenbuch, in dem er den Gebrauch der indischen Zahlenzeichen (einschließlich der Null) und der indischen dezimalen Zahlenschreibweise, die die Araber kurz vorher von den Indern übernommen hatten, erklärt. Dieses Buch wurde im 12. Jahrhundert in Spanien - wo sich der westarabische Kulturkreis und der aufstrebende Kulturkreis des europäischen Mittelalters berührten - ins Lateinische übersetzt. Die älteste erhalten gebliebene Übersetzung, die des Robert von Chester, beginnt mit den Worten: "Dixit Algoritmi: Laudes deo rectori nostro atque defensori dicamus dignas", also: "Algoritmi hat gesprochen! Lob sei Gott unserm Herrn und Beschützer!". Die neue Art, die Zahlen anzuschreiben, eben mit den arabischen statt den vorher verwendeten "römischen" Ziffern, ermöglichte eine neue Art, zu rechnen, die zum Teil schon im Büchlein des Al-Khwarizmi erklärt wurde, dann aber im Abendland allmählich weiterentwickelt wurde. Diese neue Art des Rechnens, das Rechnen nach der Art des Al-Khwarizmi, wurde nach dem Namen des Mannes, durch dessen Buch sie im Abendland bekannt wurde, als "Algorismus" oder "Algorithmus" bezeichnet.

Mehrere Gelehrte des Mittelalters verfaßten Bücher über diesen Algorithmus, also über das Rechnen in der arabischen Zahlenschreibweise. In einem dieser Werke, dem in Hexametern verfaßten "Carmen de algorismo" des französischen Mönches Alexander de Ville Dieu, heißt es darüber:

> Septem sunt partes, non plures, istius artis:
> Addere, subtrahere, duplare, dimidiare;
> Sextaque dividere, sed quinta multiplicare;
> Radicem extrahere pars septima dicitur esse.

Es treten hier also als Grundrechnungsarten neben dem Addieren, Subtrahieren, Multiplizieren und Dividieren das Verdoppeln, Halbieren und Wurzelziehen auf.

Die Ausbreitung der neuen Rechenverfahren erfolgte aber nicht so sehr durch die Bücher der scholastischen Gelehrten und durch den Einfluß der mittelalterlichen Universitäten, an denen sie unterrichtet wurden, sondern vor allem dadurch, daß sie im oberitalienischen Handel, in dem unsere moderne Geldwirtschaft ihre Wurzeln hat (man denke nur an die vielen italienischen Ausdrücke im Bankwesen) Fuß faßten. Die Anwendungen der neuen Art des Rechnens werden erstmalig dargestellt in dem 1202 erschienenen berühmten "Liber Abaci" des Leonardo von Pisa, auch Fibonacci genannt (der Titel des Buches ist irreführend, denn das Buch beschäftigt sich nicht mit dem Abakus). Allerdings dauerte es noch rund 300 Jahre, bis sich das "algorithmische Rechnen", also das Rechnen mit den neu entwickelten Rechenverfahren für die Grundrechnungsarten, gegenüber dem "Rechnen auf den Linien" durchsetzte. Aus der Zeit um 1500 gibt es eine Reihe von Holzschnitten, auf denen der Wettstreit zwischen den Abakisten und Algorithmikern dargestellt ist. Daß letztere sich durchsetzten, ist vor allem das Verdienst der Rechenmeister, die in dieser Zeit als eine eigene Zunft auftraten, das algorithmische Rechnen unterrichteten und auch Bücher darüber

verfaßten, nicht in Latein, sondern in der jeweiligen Landessprache. Auf deutschem Boden sind hier besonders Johannes Widmann, Adam Ries, Christoff Rudolff (der hauptsächlich in Wien wirkte) und Michael Stifel zu erwähnen.

In den Bürgerschulen, die in der Zeit um 1500 den Klosterschulen und den Universitäten an die Seite traten, nahm der Rechenunterricht einen wichtigen Platz ein, und hier wurden auch die Algorithmen für die Grundrechnungsarten, also Verfahren, mit denen man die elementaren Operationen an Zahlen ohne Zuhilfenahme des Abakus ausführen kann, gelehrt. Die Erlernung dieser Algorithmen, vor allem der Algorithmen für die vier Grundrechnungsarten in unserer heutigen Sicht, also für Addieren, Subtrahieren, Multiplizieren und Dividieren, ist bis in unsere Zeit herauf eines der Hauptziele im Rechenunterricht der Grundschule geblieben.

Es dauerte dabei eine gewisse Zeit, bis diese Algorithmen die heute übliche Form angenommen hatten. Insbesondere bei der Entwicklung der Algorithmen für Subtraktion und Division wurde erst mit der "österreichischen Methode", welche erstmalig erwähnt wurde im "Handbuch der Mathematik" von Bittner, erschienen 1821 in Prag, und ausführlich erklärt ist im "Lehrbuch der Arithmetik und Algebra" von Johann Salomon (der als Professor am K.K.Polytechnischen Institut, also der Technischen Hochschule, in Wien wirkte) eine endgültige Form erreicht. Dieses Buch ist in der ersten Hälfte des 19. Jahrhunderts in mehreren Auflagen erschienen. Die österreichische Methode in der Subtraktion besteht im Aufzählen vom Subtrahenden auf den Minuenden, wobei Zehnerstellen auf die nächste Stelle weitergezählt werden, also

2123
1852
271

beziehungsweise bei der Division in der Ausführung der auftretenden Subtraktionen nach der österreichischen Methode, also

7656 : 29 = 264
185
116
0

Die rasche und fehlerfreie Durchführung der Algorithmen für das Multiplizieren und Dividieren beruht allerdings auf der Verwendung von Tabellen, Tabellen, die nicht in schriftlicher Form vorliegen, sondern im Gehirn gespeichert sind - nämlich den Multiplikationstafeln für die Zahlen von 1 bis 9. Das Einspeichern dieser Tabellen erfolgt durch das Erlernen des "Kleinen Einmaleins", das ja zumindest in meiner Volksschulzeit noch einen beträchtlichen Teil des Rechenunterrichtes der 2. und 3. Klasse einnahm.

In der höheren Schule kamen dann zumindest zu meiner Zeit zu den Grundrechnungsalgorithmen noch weitere Algorithmen dazu, die zu erlernen waren: Die Algorithmen für das Quadrieren, Kubieren, Quadratwurzelziehen, Kubikwurzelziehen, sowie die Algorithmen für das Multiplizieren und Dividieren von Polynomen. Als Beispiel für einen derartigen Algorithmus sei an den Algorithmus für das Quadratwurzelziehen erinnert:

Es sei zu berechnen $\sqrt{18378369}$. Der Algorithmus verläuft so:

$\sqrt{18378369} = 4287$
237 : 82.2
7383 : 848.8
59969 : 8567.7
0000

Zweifellos hat die Entdeckung der Algorithmen für die vier Grundrechnungsarten die Grenze des für den Menschen Berechenbaren wesentlich erweitert. Das Dividieren etwa, das mit dem Abakus sehr mühsam war - so schreibt ein mittelalterlicher

Schriftsteller diesbezüglich von "Regulae quae a sudantibus abacistis vix intelliguntur" - also von "Regeln, die von den schwitzenden Abakisten kaum verstanden werden" - wurde durch den Divisionsalgorithmus auf entscheidende Weise erleichtert. Das gesamte Wirtschaftsleben wurde durch die Einführung und Ausbreitung der Algorithmen nachhaltig beeinflußt, da diese die Grundlage für Buchhaltung und Bankwesen bildeten.

Es ist eine seit den Anfängen der Menschheit zu beobachtende Tatsache, daß mit den Möglichkeiten, die sich dem Menschen bieten, seine Wünsche steigen, und so wagten sich die Astronomen - nicht zuletzt im Zusammenhang mit den Auseinandersetzungen "Ptolomäisches versus Kopernikanisches Weltbild" - bei der Auswertung des Beobachtungsmaterials an Berechnungen heran, die ohne die neuen Algorithmen undenkbar gewesen wären, die aber auch mit den Algorithmen zur Multiplikation und Division vor allem deshalb, weil sie in großer Zahl auszuführen waren, sehr mühsam waren.

Der erste Schritt zur Erleichterung dieser Mühe war die Entdeckung der "prostaphairetischen Methode", die 1514 durch Johannes Werner erfolgte. Diese beruhte auf den Additionstheoremen der trigonometrischen Funktionen. Um etwa das Produkt $a \cdot b$ zu berechnen, stützte man sich auf die Formel

$$\cos(\alpha-\beta)-\cos(\alpha+\beta) = 2\sin\alpha\sin\beta.$$

Man stellte a und b durch Multiplikation bzw. Division mit einer geeigneten Zehnerpotenz als Sinus eines Winkels α bzw. β dar, bestimmte α bzw. β durch Nachschlagen in einer Sinustafel (entsprechend genaue Sinustafeln gab es damals schon), berechnete daraus $\alpha-\beta$ bzw. $\alpha+\beta$, schlug den Cosinus nach, subtrahierte, dividierte durch 2 und machte schließlich die ursprüngliche Veränderung von a und b durch Division bzw. Multiplikation mit den Zehnerpotenzen rückgängig. Es wurde also die Multiplikation ersetzt durch viermaliges Nachschlagen in einer Tafel,

eine Addition und zwei Subtraktionen sowie eine Halbierung, was insgesamt einfacher war als die Multiplikation. Bei der Division ging man unter Verwendung von Secans und Cosecans ähnlich vor.

Die prostaphairetische Methode brachte zwar beträchtliche Vereinfachungen bei umfangreichen Berechnungen mit sich, war aber doch noch wesentlich komplizierter als die Anwendung von Logarithmen. Diese wurden aber erst rund 100 Jahre später von dem Schotten John Neper und dem Schweizer Jost Bürgi unabhängig voneinander entdeckt. Durch die Logarithmen war es möglich, eine Multiplikation bzw. Division zu ersetzen durch dreimaliges Nachschlagen in einer Logarithmentafel und eine Addition bzw. Subtraktion, und die Logarithmen blieben bis in unsere Zeit herauf ein wichtiges Rechenhilfsmittel, das auch im Schulunterricht seinen gebührenden Platz fand.

Die Logarithmen führten praktisch schon zur Zeit ihrer Entdekkung zur Erfindung einer sehr wirksamen Hardware, nämlich des Rechenschiebers, der bis zur Erfindung des Taschenrechners das wichtigste Rechenhilfsmittel des Ingenieurs geblieben ist - den es etwa seit 1850 als allgemein anerkannten selbständigen Beruf gab. So spricht der Dichter Robert Musil, selbst gelernter Maschineningenieur und einige Jahre Bibliothekar an der Technischen Hochschule Wien, davon, daß die Ingenieure den Rechenschieber "wie einen schmalen Strich über dem Herzen tragen" - der Rechenschieber schaute nämlich meist aus der Brusttasche heraus.

Für viele Zwecke war aber die Genauigkeit des Rechenschiebers zu gering. Man hatte allerdings schon bald Ausschau nach anderen Möglichkeiten gehalten, sich die Mühen des Rechnens zu erleichtern. Die erste mechanische Rechenmaschine baute 1623 Johannes Schickhart nach den Ideen des Astronomen Kepler - sie kam nie zum Einsatz. Etwas später entstand die Rechenmaschine von Pascal, von der schon eine größere Serie gebaut wurde; die Staffelwalzenmaschine von Leibniz war zwar schon sehr gut durchdacht,

diese Maschine und Verbesserungen davon konnten sich aber nie richtig durchsetzen - sie blieben unhandlich und schwerfällig. Lediglich im Geschäftsleben, etwa bei Registrierkassen u. dgl., fanden mechanische Rechenmaschinen häufig Anwendung. Für kompliziertere Berechnungen wurden sie zwar auch eingesetzt, etwa in der Flugzeugindustrie, aber nur als elementares Hilfsmittel, mehr konnten sie nicht leisten.

Die Zeit von der Erfindung der Grundrechnungsalgorithmen bis weit in unser Jahrhundert herauf brachte großartige Fortschritte der Mathematik als Wissenschaft und ihrer Anwendungsmöglichkeiten in Physik und Technik. Auch Algorithmen für eine Reihe von mathematischen Aufgaben wurden entwickelt - etwa der bekannte Algorithmus von Gauß zum Auflösen linearer Gleichungssysteme. Allerdings blieben viele dieser Aufgaben trotz der Existenz von Algorithmen zu ihrer Lösung bei größeren Werten der sie bestimmenden Ausgangsgrößen praktisch undurchführbar - der Aufwand zur Durchführung der Algorithmen war zu groß.

Darüber hinaus stellte sich gerade in unserem Jahrhundert heraus, daß es mathematische Problemstellungen gibt, für die überhaupt keine Algorithmen zu ihrer Lösung existieren. Zu dieser Erkenntnis haben insbesondere die grundlegenden Ergebnisse unseres Landsmannes Kurt Gödel aus den frühen dreißiger Jahren beigetragen, der erstmals gezeigt hat, daß es "unentscheidbare" Probleme gibt. Besonders bekannte Ergebnisse in dieser Richtung sind die in den letzten Jahrzehnten erzielten Resultate zum Zehnten Hilbertschen Problem und zum Wortproblem. Ich möchte diese Probleme kurz erläutern:

Eine diophantische Gleichung ist bekanntlich eine Gleichung $p(x_1,x_2,\ldots,x_n)=0$, wobei $p(x_1,x_2,\ldots x_n)$ ein Polynom mit ganzzahligen Koeffizienten ist und als Lösungen nur ganze Zahlen $x_1,x_2,\ldots,x_n$ zugelassen sind. Hilberts Zehntes Problem lautete: Man gebe einen Algorithmus an, der zu entscheiden ermöglicht,

ob eine beliebig gegebene diophantische Gleichung lösbar ist. Matijasevits hat 1970 gezeigt, daß es keinen derartigen Algorithmus gibt.

Beim Wortproblem - das am einfachsten für Gruppen zu formulieren ist - geht es um folgendes: Gegeben sei eine Gruppe mit endlich vielen Erzeugenden $x_1,x_2,\ldots,x_n$ und mit endlich vielen definierenden Relationen (d. h. Gleichungen zwischen den Erzeugenden) $w_1=w_1',\ldots w_k=w_k'$. Man gebe einen Algorithmus an, der stets zu entscheiden ermöglicht, ob für zwei gegebene Worte - d. h. Ausdrükke - w,w' in den Erzeugenden $x_1,x_2,\ldots,x_n$ die Gleichung $w=w'$ gilt. Auch hier wurde gezeigt, daß es einen derartigen Algorithmus nicht gibt.

Es gibt also Probleme, die grundsätzlich nicht mit Hilfe eines Algorithmus gelöst werden können; nicht wenige derartige Probleme sind tatsächlich bekannt. Andererseits sind wesentlich mehr Probleme bekannt, für deren Lösung ein Algorithmus gefunden wurde - oder sogar mehrere Algorithmen.

Das heißt aber noch lange nicht, daß ein derartiges Problem für alle auftretenden Werte der vorkommenden Ausgangsgrößen tatsächlich gelöst werden kann. Denn die tatsächliche Durchführung eines Algorithmus erfordert Rechenaufwand und damit Zeit und Mühe, und beides steigt mit der Größe der Zahlen, für die der Algorithmus durchgeführt wird. Aus diesem Grund waren vor der Erfindung des Computers viele Algorithmen nur für kleine Werte der darin eingehenden Parameter tatsächlich ausführbar. Durch die Erfindung des Computers hat sich die Fähigkeit des Menschen, Berechnungen auszuführen, in nahezu gigantischer Weise gesteigert. Trotzdem aber wächst der Bedarf an Rechenzeit und Speicherplatz, der zur Ausführung eines Algorithmus erforderlich ist, meist mit der Größe der Ausgangsparameter des Algorithmus so stark, daß schließlich Rechenzeiten in der Größenordnung von Millionen von Jahren auftreten. Für Parameterwerte, bei

denen dies der Fall ist, ist das Problem natürlich praktisch gesehen auch unlösbar, obwohl es theoretisch lösbar wäre. Allerdings hat man die Hoffnung, daß es bei weiteren Fortschritten der Computertechnik - wie sie derzeit etwa das Parallelrechnen in Aussicht stellt - lösbar sein wird, es besteht aber auch die Möglichkeit, daß für das Problem ein "besserer" Algorithmus gefunden werden kann, mit dessen Hilfe das Problem auch mit der derzeit bestehenden Rechenkapazität bewältigt werden kann.

Die Unmöglichkeit, ein Problem, das zwar theoretisch lösbar ist, praktisch zu lösen, weil der Rechenaufwand dafür zu groß ist, wurde bisher fast ausschließlich als Ärgernis empfunden. In den letzten Jahren aber hat man überraschenderweise eine wichtige Anwendung dieses Ärgernisses gefunden, nämlich eine Anwendung in der Kryptologie. Bei der Kryptologie geht es um das Problem des Schutzes von Information vor unbefugtem Zugriff. Die Übertragung und Speicherung von Information ist ja ein entscheidender Faktor für die Entstehung und für den Weiterbestand der menschlichen Zivilisation und Kultur. Seit urdenklichen Zeiten trat dabei das Problem auf, Information geheimzuhalten, also nur bestimmten Personen oder Personengruppen zugänglich zu machen. Dieses Problem gab es nicht nur im militärischen, diplomatischen und politischen Bereich, es spielte auch in der Privatsphäre seit jeher eine wichtige Rolle (wie nicht wenige klassische Liebestragödien zeigen). Speziell in unserer Zeit ist es von großer Bedeutung für das Wirtschaftsleben geworden, denn das Geld, eine zentrale Größe der Wirtschaft, ist heute weitgehend von seinen materiellen Realisierungen losgelöst und tritt immer mehr in Form von Information in Erscheinung.

Geheimzuhaltende Information kann auf zwei Arten an Unbefugte gelangen: Durch Verrat oder durch Spionage. Der Schutz vor Verrat erfolgt durch Setzung entsprechender rechtlicher Normen (von den seit altersher bestehenden Gesetzen gegen Landesverrat

angefangen über das Beichtgeheimnis des Kirchenrechts bis zu den Datenschutzgesetzen unserer Zeit), sowie durch die moralische Ächtung von Verrätern (man denke etwa daran, daß diese in Dantes "Göttlicher Komödie" im untersten Höllenkreis angesiedelt werden). Der Schutz vor Spionage hingegen erfolgt durch technische Maßnahmen (im weitesten Sinn des Wortes). Diese bestehen einerseits in materiellen Vorkehrungen (Aufbewahrung von Geheimpapieren in Tresoren, Übertragung von Information durch Geheimkuriere u. dgl.), andererseits darin, daß man die geheime Information "verschlüsselt", also in einer Form darstellt, in der sie für Unbefugte nicht verständlich ist. Die ersten Methoden der Verschlüsselung sind schon aus dem klassischen Altertum überliefert, und seither hat sich unter dem Namen "Kryptologie" allmählich eine eigene Wissenschaft entwickelt, die sich in ihren beiden Zweigen Kryptographie und Kryptanalyse mit der Entwicklung von Verschlüsselungsmethoden einerseits, mit der Untersuchung ihrer Sicherheit (und in der Praxis mit ihrer "Brechung") andererseits beschäftigt. Dabei spielen mathematische Methoden eine wichtige Rolle, und seit der Entwicklung und Verbreitung der elektromagnetischen und elektronischen Methoden zur Speicherung, Übertragung und Verarbeitung von Information haben sich der Kryptologie neue, vorher ungeahnte Möglichkeiten eröffnet.

Die klassischen Verschlüsselungssysteme sind sogenannte Einschlüsselverfahren. Bei diesen wird die Information mit einem bestimmten Verfahren, das von einem veränderlichen Parameter, dem Schlüssel, abhängt, in den "Chiffretext" verwandelt. Dieser wird durch die Umkehrung des Verschlüsselungsverfahrens, die etenfalls vom Schlüssel als Parameter abhängt und sich leicht aus dem Verschlüsselungsverfahren ergibt, entschlüsselt, also in den "Klartext" zurückverwandelt. Der Schlüssel muß natürlich allen zur Teilnahme am Informationsnetz Autorisierten bekannt sein. Je größer dieser Teilnehmerkreis ist, desto größer ist die Gefahr des Verrates, und je umfangreicher das Informations-

netz ist, desto größer ist die Gefahr, daß Chiffretexte von Unbefugten aufgefangen und entschlüsselt werden oder daß Unbefugte gar aus aufgefangenen Chiffretextstücken oder zusammengehörigen Stücken von Klartext und Chiffretext den Schlüssel ermitteln. Man versucht dieser Gefahr vorzubeugen, indem man den Schlüssel häufig wechselt, wobei sich aber Probleme des "Schlüsselmanagements", das heißt der Bekanntgabe des jeweiligen Schlüssels an alle autorisierten Teilnehmer des Informationsnetzes unter Geheimhaltung gegenüber Nichtautorisierten, ergeben.

Im letzten Jahrzehnt aber hat man durch die Entdeckung der "Public-Key-Kryptosysteme" eine neuartige Möglichkeit gefunden, die Sicherheit von Information in umfangreichen Kommunikationsnetzen zu gewährleisten. Bei einem Public-Key-Kryptosystem besitzt jeder autorisierte Teilnehmer A am Kommunikationsnetz einen "öffentlichen Schlüssel" S_A, der in einem allgemein zugänglichen Schlüsselverzeichnis enthalten ist. Dieser ist so beschaffen, daß es unmöglich ist, seine Umkehrung T_A ohne Kenntnis zusätzlicher Information über S_A zu ermitteln. Mit Kenntnis dieser Information aber, über die nur der Teilnehmer A verfügt, kann T_A leicht berechnet werden und wird von A als sein "privater Schlüssel" geheimgehalten. Wenn nun der Teilnehmer B eine Geheiminformation x an A übermitteln will, verschlüsselt er sie mittels S_A zu S_Ax und sendet S_Ax an A. Nur dieser kann S_Ax entschlüsseln, denn nur er kennt die Umkehrung T_A von S_A. Um nun derartige öffentliche Schlüssel herzustellen - man braucht natürlich viele derartige Schlüssel - sucht man Algorithmen, die rasch und bequem ausführbar sind, die aber so beschaffen sind, daß die Berechnung des Umkehralgorithmus ohne Zusatzkenntnisse einen so großen Rechenaufwand erfordert, daß diese Berechnung praktisch unmöglich ist.

Gerade wegen der Anwendungen in der Kryptologie hat das Studium des für die Ausführung von Algorithmen erforderlichen Aufwandes

in den letzten Jahren zunehmend Interesse gefunden, und es hat sich ein eigenes Teilgebiet an den Grenzen von Mathematik, mathematischer Logik und Informatik entwickelt, die Komplexitätstheorie, die die "Komplexität" von Algorithmen untersucht. In der Kryptographie benötigt man ja zur Herstellung von öffentlichen Schlüsseln Algorithmen von geringer Komplexität, für welche die Berechnung des Umkehralgorithmus aber eine ungeheuer große Komplexität besitzt.

Die Komplexitätstheorie ist ein schwieriges Gebiet, das, wenn man es exakt betreibt, beträchtliche Hilfsmittel aus der mathematischen Logik erfordert, und es kann daher hier nicht näher darauf eingegangen werden. Es sollen aber als Beispiele einfacher Komplexitätsabschätzungen drei für die Kryptographie wichtige Algorithmen kurz besprochen werden:

1. Modulares Potenzieren:

Es sei gegeben eine natürliche Zahl m als Modul. Gesucht ist der Wert a^k modulo m, wo a und k natürliche Zahlen sind. Die naheliegendste Art, das zu berechnen, ist die aufeinanderfolgende Berechnung der Potenzen a, a^2, a^3,... a^k, was insgesamt k-1 Multiplikationen modulo m erfordert. In der Kryptographie treten bis zu 200-stellige Exponenten k auf, man würde also auf diese Weise bis zu 10^{200} Multiplikationen modulo m auszuführen haben. Die Anzahl dieser Multiplikationen kann man aber auf folgende Weise wesentlich verringern:
Man stellt k binär dar, also in der Form

$$k = 2^n e_n + 2^{n-1} e_{n-1} + \ldots + 2e_1 + e_0 \qquad 0 \leq e_i \leq 1 \qquad e_n = 1$$

dann ist $x^k = (x^{2^n})^{e_n} (x^{2^{n-1}})^{e_{n-1}} \ldots (x^2)^{e_1} x^{e_0}$.

Man berechnet nun der Reihe nach $x, x^2, (x^2)^2 \ldots x^{2^n}$ modulo m, indem man jeweils die vorhergehende Zahl modulo m quadriert, und multipliziert x^{e_0} mit $(x^2)^{e_1}$, das Ergebnis mit $(x^{2^2})^{e_2}$ usw.

Wieviele Rechenschritte werden insgesamt benötigt? Es gilt

$2^n \leq k < 2^{n+1}$, somit $n \leq ld\, k < n+1$, daraus folgt $n = [ld\, k] \leq ld\, k \leq 4 \log k$.

Um also mit diesem Algorithmus x^k mod m zu berechnen, benötigt man höchstens $4 \log k$ Divisionen durch 2, höchstens $4 \log k$ Quadraturen modulo m und höchstens $4 \log k$ Multiplikationen modulo m, also höchstens $12 \log k$ Rechenoperationen, also bei 200-stelligem k höchstens 2400 Operationen im Gegensatz zu 10^{200}.

2. Der Euklidische Algorithmus

Die Abschätzung der Rechenschritte bei diesem klassischen Algorithmus war eines der ersten komplexitätstheoretischen Resultate. Sie wurde durchgeführt von dem französischen Mathematiker Gabriel Lamé im Jahre 1845. Er verwendete dazu die Folge der Fibonacci-Zahlen. Wir wollen hier eine Abschätzung für die Komplexität des Algorithmus auf eine etwas einfachere Weise gewinnen (erhalten dadurch allerdings eine etwas größere Konstante):
Der euklidische Algorithmus zur Bestimmung des größten gemeinsamen Teilers von u und v verläuft folgendermaßen:

$$\begin{aligned}
u &= v\, q_1 + r_1 && 0 < r_1 < v \\
v &= r_1\, q_2 + r_2 && 0 < r_2 < r_1 \\
r_1 &= r_2\, q_3 + r_3 && 0 < r_3 < r_2 \\
r_2 &= r_3\, q_4 + r_4 && 0 < r_4 < r_3
\end{aligned}$$

Dieses Verfahren wird so lange fortgesetzt, bis sich $r_n = 0$ ergibt. Dieser Fall muß wegen $v > r_1 > r_2 > \ldots$ nach endlich vielen Schritten eintreten. Die beiden letzten Gleichungen des Algorithmus lauten dann:

$$\begin{aligned}
r_{n-3} &= r_{n-2} q_{n-1} + r_{n-1} && 0 < r_{n-1} < r_{n-2} \\
r_{n-2} &= r_{n-1} q_n
\end{aligned}$$

Das r_{n-1} ist der größte gemeinsame Teiler von u und v, denn es ist ein gemeinsamer Teiler (Durchlaufen der Gleichungskette von unten nach oben) und durch jeden gemeinsamen Teiler teilbar (Durchlaufen der Gleichungskette von oben nach unten).
Die Komplexität des Verfahrens ist gegeben durch die Anzahl der erforderlichen Divisionen, und die ist n. Wir wollen n abschätzen:

Es gilt entweder $r_1 \leq \frac{v}{2}$ oder $r_1 > \frac{v}{2}$. Im zweiten Fall gilt $q_2=1$ und $r_2 < \frac{v}{2}$, somit gilt $r_2 < \frac{v}{2}$ in jedem Fall. Es gilt entweder $r_3 \leq \frac{r_2}{2}$ oder $r_3 > \frac{r_2}{2}$; im zweiten Falle gilt $q_4=1$ und $r_4 < \frac{r_2}{2}$, also gilt auf jeden Fall $r_4 < \frac{r_2}{2} < \frac{v}{2^2}$. Mit vollständiger Induktion zeigt man, daß $r_{2k} < \frac{v}{2^k}$ für $k=1,2,\ldots$. Sei k die kleinste nichtnegative ganze Zahl mit $\frac{v}{2^k} \leq 1$. Wäre $2k \leq n-1$, dann wäre $r_{2k} \geq 1$, andererseits aber $r_{2k} < \frac{v}{2^k} \leq 1$ Widerspruch. Also gilt $2k > n-1$, daher $n < 2k+1$ und somit $n \leq 2k$.

Wie bestimmt man k? Ist k die kleinste nichtnegative ganze Zahl mit $\frac{v}{2^k} \leq 1$, dann ist k-1 die größte ganze Zahl mit $\frac{v}{2^{k-1}} > 1$, also ist $v > 2^{k-1}$, also ist $k-1 < \mathrm{ld}\, v \leq k$, daraus folgt $k \leq [\mathrm{ld}\, v] + 1$, somit

$$n \leq 2[\mathrm{ld}\, v] + 2 \leq 2\,\mathrm{ld}\, v + 2 \leq 8 \log v + 2 \leq 8\,(\text{Stellenzahl von } v) + 2$$

Ist also v eine 200-stellige Zahl, dann erfordert der euklidische Algorithmus höchstens 1602 Divisionen.

3. Die Primfaktorzerlegung einer natürlichen Zahl n

Auch diese Aufgabe ist algorithmisch stets lösbar. Einen einfachen Algorithmus dafür erhalten wir, wenn wir n der Reihe nach durch die Zahlen $t=2,3,\ldots$ dividieren, bis sich die Division ausgeht, oder bis gilt $t > \sqrt{n}$. Falls die Division einmal ausgeht, dann ist das so erhaltene t eine Primzahl, andernfalls ist n selbst Primzahl. Im ersten Fall wenden wir das gleiche Verfah-

ren auf $\frac{n}{t}$ an usw. Wegen $\frac{n}{t}<n$ bricht der Algorithmus tatsächlich nach endlich vielen Schritten ab und liefert die gesuchte Primzahlzerlegung. Natürlich gibt es wesentlich ausgefeiltere und schnellere Algorithmen zur Primfaktorzerlegung, aber auch diese sind selbst mit den leistungsfähigsten Computern, wie etwa CRAY II, ungeheuer aufwendig. So war der Stand vor etwa zwei Jahren so, daß für die Faktorisierung einer 75-stelligen Zahl ein Tag, einer 100-stelligen Zahl 255 Tage, einer 200-stelligen Zahl $36 \cdot 10^6$ Jahre erforderlich gewesen wären. Selbstverständlich treten aber durch leistungsfähigere Computer und verbesserte Algorithmen immer wieder Reduktionen dieses Aufwandes ein.

Das bekannteste Verfahren der Public-key Kryptographie, das RSA-Verfahren (nach seinen Entdeckern Rivest, Shamir, Adleman benannt) baut nun die öffentlichen Schlüssel so auf: Man wählt zwei voneinander verschiedene große (etwa 100-stellige) Primzahlen p_1, p_2 (diese Auswahl kann erfolgen mit einem sogenannten Primzahltest, der nur eine erträgliche Zahl von Potenzierungen modulo der zu testenden Zahl n erfordert), bildet $n=p_1 \cdot p_2$, wählt k so, daß der größte gemeinsame Teiler von k und $(p_1-1)(p_2-1)$ den Wert 1 hat, was jede Primzahl $k>(p_1-1)(p_2-1)$ erfüllt, die man dann noch modulo $(p_1-1)(p_2-1)$ reduzieren kann. Man gibt nun n und k als öffentlichen Schlüssel bekannt. Die Verschlüsselung einer Nachricht erfolgt, indem man sie zunächst durch Zusammenfassen aufeinanderfolgender Teile der Nachricht zu Blöcken in eine Folge von natürlichen Zahlen $<n$ codiert und dann jede dieser Zahlen x in $x^k \bmod n$ verschlüsselt. Das Entschlüsseln erfolgt, indem man l so wählt, daß $k \cdot l \equiv 1 \bmod (p_1-1)(p_2-1)$, was mit dem euklidischen Algorithmus möglich ist, aber nur dann, wenn man $(p_1-1)(p_2-1)$ kennt. Wegen $(x^k)^l \equiv x \bmod n$ erhält man durch Potenzieren mit l aus dem verschlüsselten Text dann den Klartext zurück. Dieses l kann man aber nur berechnen, indem man n faktorisiert, was, wie wir gesehen haben, praktisch unmöglich ist.
Die Sicherheit des RSA-Verfahrens hängt also von der Komplexität der bekannten Faktorisierungsalgorithmen relativ zur vorhandenen Hardware ab.

Wir haben in unseren ersten beiden Beispielen gesehen, daß die Komplexität unseres Potenzierungsalgorithmus linear wächst mit log k, dem Logarithmus des Exponenten, und daß die Komplexität des euklidischen Algorithmus ebenfalls linear wächst mit log v, dem Logarithmus der zweiten Zahl. Allgemein wird die Komplexität eines Algorithmus in der Komplexitätstheorie ausgedrückt durch eine Funktion f(w) des Parameterwertes w, für den der Algorithmus auszuführen ist. Solange diese Funktion beschränkt durch ein Polynom in w ist, kann der Algorithmus akzeptiert werden, wenn diese Funktion aber eine Exponentialfuktion ist, dann wächst seine Komplexität so rasch an, daß er bald nicht mehr ausführbar ist.

Auch in der Schule werden nach wie vor Algorithmen behandelt, sowohl im Mathematikunterricht, als auch im EDV-Unterricht. Es ist dabei durchaus schon möglich, einfache Komplexitätsabschätzungen derartiger Algorithmen durchzuführen, also sich zu überlegen, wie die Anzahl der für den Algorithmus nötigen Einzelschritte von den Ausgangsgrößen des Algorithmus abhängt, und wie daher die Rechenzeit in Abhängigkeit von diesen Ausgangsgrößen anwächst. Dies gibt dem Schüler eine gewisse Ahnung von den Möglichkeiten, aber auch den Grenzen unserer neuzeitlichen Rechentechnik.

Dabei wird sich vielleicht auch die Gelegenheit ergeben, allgemeiner auf die Chancen und Risiken hinzuweisen, die die moderne Informationstechnik für unsere Zivilisation und Kultur mit sich bringt. Zweifellos gibt uns diese Technik viele Vorteile: Mühsame Rechenarbeit wird uns abgenommen, wir können Berechnungen ausführen, die früher weit jenseits des Menschenmöglichen standen, und damit der naturwissenschaftlichen Forschung und der Technik wertvolle Hilfe geben. In der Tat wären ja viele der Errungenschaften dieser Gebiete ohne die moderne Computertechnik unmöglich. Aber auch die Schattenseiten dieser Technik sind nicht zu unterschätzen. Es besteht nämlich die Gefahr,

daß unsere Gesellschaft immer mehr von diesen Hilfsmitteln abhängig wird, und Abhängigkeit schafft auch Verwundbarkeit: Computerkriminalität, Überwachungsstaat, oder gar die Drohung mit dem elektromagnetischen Puls als neuartige Waffe, die mit einem Schlag die gesamte Mikroelektrik funktionsunfähig machen kann, sind Indizien für diese Verwundbarkeit. Natürlich kann man versuchen, sich mit technischen Maßnahmen gegen diese Bedrohungen zu schützen, und man hat hier auch schon Erfolge erzielt. Eine andere Gefahr kam mir sehr deutlich zu Bewußtsein, als ich vor kurzem in einer Eisenhandlung zehn Schrauben zum Stückpreis von 13 Groschen kaufte. Der Verkäufer griff in seine Tasche, nahm den Taschenrechner heraus und berechnete damit das Produkt 10 mal 13 Groschen. Dies ist ein Zeichen dafür, daß die Taschenrechner in ähnlicher Weise zur Denkfaulheit führen können wie das Auto zur Gehfaulheit, und daß damit der Mensch auch auf diese Weise zunehmend abhängig wird von der Technik. So droht auch in diesem Bereich die Gefahr, "sich zu Tode zu amüsieren", die Neil Postman in seinem Bestseller so deutlich ausgemalt hat. Der Gefahr, das Denken immer mehr zu verlernen und das ganze Leben nur noch als riesiges Computerspiel aufzufassen, muß nicht zuletzt die Schule entgegenwirken. So möchte ich meinen Vortrag beschließen mit der Bitte an Sie, sehr geehrte Zuhörer, Ihren Unterricht so zu gestalten, daß Ihre Schüler das Denken, auch das Denken in mathematischen Größen, nicht verlernen, und daß sie in Zukunft auch ohne Hardware nicht total hilflos sind.