Jochen Ziegenbalg

LEHRBUCH

Elementare Zahlentheorie

Beispiele, Geschichte, Algorithmen

2. Auflage

Springer Spektrum

Elementare Zahlentheorie

Jochen Ziegenbalg

Elementare Zahlentheorie

Beispiele, Geschichte, Algorithmen

2., überarbeitete Auflage

Springer Spektrum

Jochen Ziegenbalg
Institut für Mathematik und Informatik
Pädagogische Hochschule Karlsruhe
Karlsruhe, Deutschland

ISBN 978-3-658-07170-7 ISBN 978-3-658-07171-4 (eBook)
DOI 10.1007/978-3-658-07171-4

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.d-nb.de abrufbar.

Springer Spektrum

1. Auflage 2002: Wissenschaftlicher Verlag Harri Deutsch GmbH, Frankfurt am Main

Springer Spektrum ist eine Marke von Springer DE. Springer DE ist Teil der Fachverlagsgruppe Springer Science+Business Media
www.springer-spektrum.de

Vorwort

Die „Erfindung“ des Zählens stellt eine der faszinierendsten Leistungen des menschlichen Geistes dar; Zahlen und Zahlschreibweisen sind eng mit unserer Kulturgeschichte verwoben. Ohne Zahlen gäbe es (ob zum Besseren oder zum Schlechteren sei dahingestellt) keine Mathematik, keine Naturwissenschaften, keine Technik, keine Medizin und keine Ingenieurwissenschaften in der Form, wie wir sie kennen. Die vom Menschen geprägte Welt wäre eine völlig andere.

Zahlen sind einfach und kompliziert zugleich. Das Zählen stellt sich beim Menschen „fast automatisch“ ein; die meisten Kinder können schon zählen, bevor sie in die Schule kommen. Aber die Zahlen sind zugleich auch der Stoff, der (zusammen mit der räumlichen Anschauung) den menschlichen Geist zur Konstruktion gedanklicher Gebäude anregt, deren Untersuchung zu den hochgradig abstrakten Strukturen der modernen Mathematik geführt hat.

Zahlen sind zugleich anschaulich und abstrakt. Vermutungen über zahlentheoretische Gesetzmäßigkeiten entstehen oft durch das Betrachten von konkreten Beispielen und insbesondere von strukturierten Punkt- oder Flächenmustern, den sogenannten „figurierten“ Zahlen. Der Satz des Pythagoras gab so Anlass zur Fermatschen Vermutung, welche die Mathematiker Jahrhunderte lang beschäftigte und die Entwicklung zur modernen abstrakten Algebra maßgeblich beeinflusste.

Zahlen machen Spaß. Spiele mit Zahlen und Zahlenrätsel faszinieren immer wieder Menschen aus allen Altersschichten und mit der unterschiedlichsten Vorbildung.

Das Thema „Zahlen“ ist zugleich alt und jung. Schon die frühesten menschlichen Kulturen verfügten über Zahlen (man kann sich fragen, ob es ohne Zahlen überhaupt menschliche Kulturen gegeben hätte) und einige der bemerkenswertesten jüngsten Ergebnisse der Wissenschaft sind Ergebnisse über Zahlen.

Ein besonderes Merkmal dieser Einführung in die elementare Zahlentheorie ist nicht zuletzt auch die bewusste inhaltliche Beschränkung. Der Umfang dieser Darstellung entspricht etwa dem, was ich im Sommersemester in einer einführenden Basisvorlesung von zwei Semesterwochenstunden behandeln kann. Im

Rahmen eines modular aufgebauten Vorlesungsprogramms ist dies ein Baustein, auf dem andere Lehrveranstaltungen aufbauen können.

Möglichkeiten zur Weiterführung, Vertiefung und zum Ausbau sind in vielfältiger Weise gegeben; hier einige Anregungen:

- Faszination Zahl: Figurierte Zahlen, Fibonacci Zahlen, Pythagoreische Zahlen, Zahlen und Kombinatorik
- Zahlen in Natur und Kultur: der Goldene Schnitt, Phyllotaxis (die Lehre von den Blatt-Ständen von Pflanzen), Zahlen und Kalender (historisches Beispiel: die Ermittlung des Osterdatums nach Gauß)
- Praktische Anwendungen: Prüfziffern (EAN, ISBN, ...), Geheimcodes, Verschlüsselungssysteme (insbesondere: Public Key Cryptography, RSA Verfahren), Primzahltests, Kalenderrechnungen, Planung von Tournieren
- Zahlentheoretische Spielereien: Kartentricks mit zahlentheoretischen Erklärungen, Auszählverfahren, Magische Quadrate, Zahlentheorie zur Ermittlung von Gewinnstrategien in Spielen aller Art (z.B. NIM)
- Bruch-Zahlen: ägyptische Brüche, Dezimal- und Systembrüche, Kettenbrüche, Irrationalität, Kommensurabilität
- Zahlentheoretische Vertiefungen: Diophantische Gleichungen, zahlentheoretische Funktionen, Primzahlsätze, Siebmethoden, Gitterpunktverfahren, quadratische Reste, p-adische Zahlen
- Algebra: Restklassenringe, Gruppe der primen Restklassen, Quadratische Erweiterungen, Ring der Gaußschen Zahlen, Polynomringe, Euklidische Ringe, Hauptidealringe, faktorielle Ringe, Integritätsringe
- Zahlentheorie und Informatik bzw. algorithmische Zahlentheorie: Algorithmen in der Zahlentheorie, Zahlentheorie in Codierung und Kryptologie, computerbasierte Experimente in der Zahlentheorie, internetbasierte Methoden in der Zahlentheorie (wie z.B. das Projekt GIMPS – Great Internet Mersenne Prime Search)
- Geschichte der Mathematik: Entstehung der Zahlensysteme, zahlentheoretische Fragestellungen in Antike, Mittelalter, Renaissance und Neuzeit

Sowohl zum Basistext als auch zu den weiterführenden Themen habe ich im Internet neben themenbezogenen Computeralgebra-Quelltexten auch eine Reihe interaktiver Seiten zum Experimentieren zur Verfügung gestellt. Näheres dazu ist im „Verzeichnis der internetbasierten Materialien des Autors“ im An-

schluss an das Abbildungsverzeichnis zusammengestellt; grundsätzlich sind alle diese Materialien unter der Adresse www.ziegenbalg.ph-karlsruhe.de (als „Wurzel“) zu finden.

Der vorliegende Text ist aus einem Manuskript zu meiner Vorlesung „Basiswissen Zahlentheorie“ am Institut für Mathematik und Informatik der Pädagogischen Hochschule Karlsruhe hervorgegangen. Er stellt einen ersten Einstieg in die Zahlentheorie dar und ist, wie oben erläutert, die Basis für vielfältige Ausbaumöglichkeiten.

Bei der Überarbeitung des Buches konnte ich auch Erfahrungen einfließen lassen, die ich im Zusammenhang mit der von der Humboldt Universität zu Berlin organisierten Sommerschule „Lust auf Mathematik“ und mit Schülergruppen des Heinrich-Hertz-Gymnasiums in Berlin gewinnen konnte.

Die Voraussetzungen für das Verständnis dieses Buchs sind bewusst niedrig gehalten. Einige Details zum Thema „Vorwissen“ sind kompakt in den Anhängen zusammengestellt. In Anhang 8.1 sind die in diesem Buch verwendeten Beweisprinzipien aufgeführt. Anhang 8.2 kann auch als kleine Einführung in das Prinzip der vollständigen Induktion genutzt werden. Zielgruppe des Buches ist nicht die „scientific community“ sondern es sind Leser, die sich nicht unbedingt als Berufsmathematiker verstehen. Die Bereitschaft zum Mitdenken und Mitarbeiten muss für eine sinnverstehende Lektüre des Buches allerdings vorhanden sein.

Von Ludwig Wittgenstein stammt der Ausspruch „*Wenn du wissen willst, was ein Satz besagt, schau nach, was sein Beweis beweist*“. So richtig dies grundsätzlich ist, so ergänzungsbedürftig ist es im Hinblick auf das Erlernen von Mathematik bei Menschen, die erst am Anfang ihres mathematischen Lebenswegs stehen. Formale mathematische Beweise sind für sie oft undurchsichtige Rituale. Wirkliches Verständnis kommt bei ihnen selten aus einem abstrakten Beweis sondern viel öfter aus einem gut ausgewählten, typischen Beispiel. Die richtigen Beispiele auszuwählen, ist eine Kunst; gute Beispiele geben der Mathematik etwas von der Sinnlichkeit des Lebens. Manche Wissenschafts-Schulen der Mathematik sind geneigt, die Bedeutung von Beispielen herunterzuspielen. Für die Phasen des Mathematik-*Lernens* meine ich aber im Gegensatz dazu, dass die Bedeutung guter Beispiele kaum überbetont werden kann.

Zum Adressatenkreis dieses Buches gehören natürlich auch die Studierenden, insbesondere in den Lehramtsstudiengängen. Der Zielgruppe entsprechend, stand bei der Konzeption die Redundanzfreiheit des Textes nicht im Vordergrund. Viele formal sehr kompakt beschreibbare Begriffe wurden durch erläuternde Beschreibungen, durch geeignete Beispiele oder durch graphische Veranschaulichungen verständlich gemacht.

Das Interesse am Thema „Zahlen“ scheint universell zu sein. Kürzlich war ich bei einer Hochzeit eingeladen. Das Datum bot sich an, um spontan eine Verbindung zu den „perfekten Zahlen“ herzustellen. Im Laufe des Abends wurde ich dann immer wieder von verschiedenen Hochzeitsgästen gebeten, die vollkommenen Zahlen noch etwas näher zu erläutern. Bei vielen Menschen ist also offenbar ein ganz natürliches Bedürfnis da, etwas mehr über die Zahlen zu erfahren als sie von ihrer Schulzeit her wissen.

Meinen Kollegen Kurt Neubert (Reutlingen) und Erich Wittmann (Dortmund) bin ich für viele und vielfältige Anregungen und Diskussionen inhaltlicher und methodologischer Art dankbar.

Für die verlegerische Unterstützung bei der vorliegenden Neuauflage dieses Buches danke ich Frau Ulrike Schmickler-Hirzebruch vom Verlag Springer Spektrum und ebenso Herrn Klaus Horn vom damals noch existierenden Verlag Harri Deutsch für die entsprechende Unterstützung bei der ersten Auflage.

Über Anmerkungen, Kommentare und Rückmeldungen aller Art freue ich mich. Per electronic mail bin ich unter der Adresse

ziegenbalg@ph-karlsruhe.de

erreichbar.

Berlin, im August 2014 Jochen Ziegenbalg

Inhaltsverzeichnis

1 Geschichtliches zu Zahl und Zahldarstellung

1.1 Zahlen und Zahldarstellungen: Vorgeschichte

> Die ganzen Zahlen hat der liebe Gott gemacht. Alles andere ist Menschenwerk.
>
> Leopold Kronecker (1823–1891)

Wenn man heute irgendwo auf der Welt den symbolischen Ausdruck 90217 sieht, so vermutet man (in der Regel meist zu Recht), dass es sich dabei um eine bestimmte Zahl im Zehnersystem handelt. Die Art und Weise, wie wir heute üblicherweise Zählen und die Zahlen aufschreiben, ist jedoch beileibe nicht selbstverständlich; sie hat sich erst im Laufe eines langen Entwicklungsprozesses herauskristallisiert.

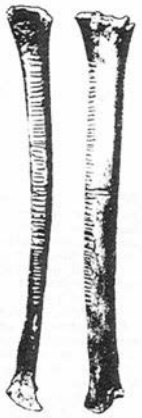


Abb. 1.1: Wolfsknochen mit Einkerbungen *Quelle*: siehe Abbildungsverzeichnis

Ein wesentliches strukturelles Kennzeichen unserer Art und Weise, die Zahlen aufzuschreiben, ist die Methode der *Stellenwertdarstellung*. Sie wurde etwa im 6. Jahrhundert n. Chr., also menschheitsgeschichtlich gesehen relativ spät, in Indien entwickelt und setzte sich danach erst im Verlaufe eines außerordentlich langwierigen historischen Prozesses durch. Eine entscheidende Voraussetzung dafür, dass eine konsequente Stellenwertdarstellung überhaupt möglich wird, ist die Existenz eines Symbols für das *Nichts*. Die Erfindung eines solchen Symbols in der Form der Zahl *Null* ist eine der großen Leistungen der indischen Mathematik.

Zunächst war die Zahlschreibweise jedoch rein additiv. Man verwendete feste Symbole für bestimmte Zahlenwerte und setzte diese Symbole additiv nebeneinander. Da es sich in der Frühzeit noch nicht um eine Stellenwertdarstellung handelte, spielte es z.B.

J. Ziegenbalg, *Elementare Zahlentheorie*, DOI 10.1007/978-3-658-07171-4_1

auch keine Rolle, in welcher Reihenfolge die Zahlsymbole aufgeschrieben wurden.

Erste menschliche Zahldarstellungen (Einkerbungen in Tierknochen, Hölzern u.ä.) sind aus der Steinzeit bekannt. Ihr Alter wird auf etwa 20.000–30.000 Jahre geschätzt (vgl. Wußing 2008). Einer der ältesten Funde ist ein im Jahre 1937 in Dolni Véstonice (Unter-Wisternitz), in der damaligen Tschechoslowakei (Mähren), gefundener Wolfsknochen mit 55 Einkerbungen in zwei Serien mit jeweils 25 und 30 Kerben (vgl. Abb. 1.1). Sein Alter wird auf 12.000 bis 20.000 Jahre geschätzt.

Die Perioden der Steinzeit waren in grober Datierung:

Altsteinzeit (*Paläolithikum*): ab etwa 2 Mill. Jahren bis etwa 10. Jahrtausend v. Chr.

Jungsteinzeit (*Neolithikum*): ab etwa 10. Jahrtausend bis etwa 4. Jahrtausend v. Chr.

1.2 Die Entstehung von Mathematik und Zahlensystemen in den ersten Hochkulturen

Die **Ägypter** (ca. 3000–500 v. Chr.) verwendeten Zehnerpotenzen (Einer, Zehner, Hunderter, Tausender, ...) zur Darstellung der natürlichen Zahlen.

						
1	10	100	1000	10000	100000	1000000
133FA	13386	13362	131BC	130AD	13190	13068
Strich	Joch für Rind	Seil-rolle	Lotus, Wasser-lilie	Finger	Kaul-quappe, Frosch	Gott der Unendlich-keit

Abb. 1.2: Ägyptische Zahlzeichen mit ihren Unicode Werten in der 3. Zeile (zum Thema "Unicode": vgl. Kapitel 6)

Ihre Zahlschreibweise war jedoch rein additiv und enthielt noch keine Elemente einer Stellenwertdarstellung. Die Multiplikation zweier natürlicher Zahlen führten sie mit Hilfe eines sehr effizienten Verfahrens der Halbierung

und Verdopplung durch. Sie entwickelten eine interessante Form der Bruchrechnung. Aufgrund ihrer Notation konnten sie (mit Ausnahme des Bruches $\frac{2}{3}$) nur „Stammbrüche“ aufschreiben, also nur Brüche der Form $\frac{1}{n}$. Dies führte zu dem folgenden Problem (in moderner Sprechweise): Wie kann man einen beliebigen Bruch möglichst „optimal“ als eine Summe von Stammbrüchen darstellen? Dabei entsteht automatisch die Frage, welche Optimalitätskriterien man hierbei zugrunde legen sollte. Algorithmische Fassungen der ägyptischen Multiplikation und Bruchrechnung sind in Ziegenbalg 2010, Abschnitt 4.1.2 und 5.3, in größerem Detail dargestellt.

Griechische Geschichtsschreiber (Herodot, Demokrit) berichten, dass die ägyptischen Landvermesser das „gespannte Seil“ als Werkzeug benutzten. Es wird vermutet, dass ein Seil mit den durch Knoten markierten äquidistanten Teilungen an den Teilungspunkten 3, 4 und 5 in geeigneter Form von drei Seilspannern („*Harpedonapten*“) auseinander gezogen wurde, um einen rechten Winkel zu erzeugen. Die ägyptischen Seilspanner wandten somit schon sehr früh den erst später voll formulierten und bewiesenen *Satz des Pythagoras* an (genauer: sie nutzten die Umkehrung des pythagoreischen Satzes).

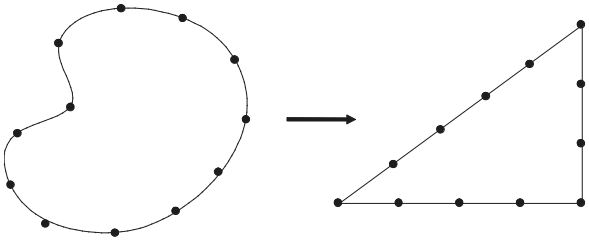


Abb. 1.3: Die ägyptische Seilspanner-Methode (der "Harpedonapten") zur Erzeugung eines rechten Winkels

Die **Babylonier** (ca. 3000–200 v. Chr.) verfügten über eine für diese Zeit außerordentlich hochstehende Mathematik. Die Basis des numerischen Rechnens bildete ein Sechzigersystem, das bereits deutliche Ansätze eines Stellenwertsystems aufwies (es fehlte im wesentlichen nur ein Symbol für die Null).

Dieses Zahlensystem war den anderen Zahlensystemen in der Antike derart überlegen, dass es auch in späteren Zeiten und anderen Kulturen für wissenschaftliche Arbeiten verwendet wurde – so z.B. von dem um etwa 100 n. Chr. in Alexandria wirkenden hellenistischen Mathematiker und Astronomen Klaudios Ptolemaios der mit seinem *Almagest* das bedeutendste astronomische Werk der Antike schuf. Auf dieses babylonisch-ptolemäische Sechzigersystem geht z.B. noch die in unserer Zeitrechnung (und unseren Uhren) verwendete Sechziger-Teilung zurück.

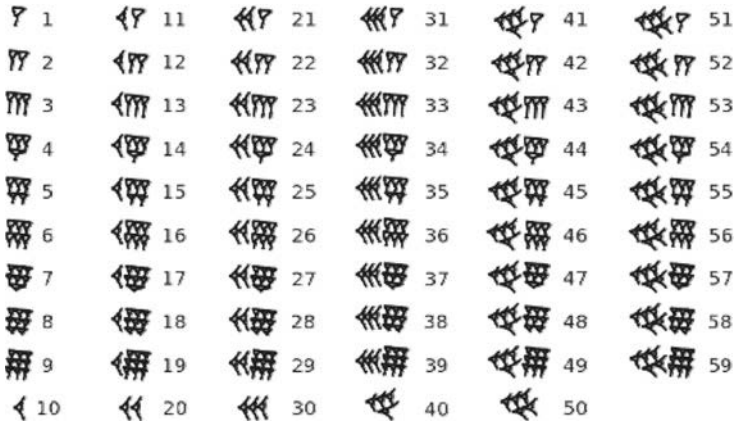


Abb. 1.4: Babylonische Keilschrift-Zahlzeichen
Quelle: siehe Abbildungsverzeichnis

Die Babylonier waren weiterhin gute „Algebraiker“ (der Begriff der Algebra wurde jedoch erst sehr viel später geprägt). Eine Keilschrift aus der Epoche von Hammurapi (um ca. 1700 v. Chr.) dokumentiert ihre Fähigkeit, Quadratwurzeln auf eine sehr effiziente Weise zu ziehen und quadratische Gleichungen zu lösen.

Die **Chinesen** (die kulturgeschichtliche Entwicklung setzte ab etwa 2000 v. Chr. ein) verwendeten für das Rechnen eine Form des *Abakus* (ein frühes Recheninstrument), den sogenannten *Suan-pan,* der in seiner Urform bis in das 11. Jahrhundert v. Chr. zurückverfolgt werden kann. Eine weiterentwickelte

Version dieses Abakus war noch bis vor wenigen Jahren in vielen Regionen Asiens in Gebrauch. Dieser Abakus kann durchaus als eine der frühesten Urformen des modernen Computers angesehen werden.

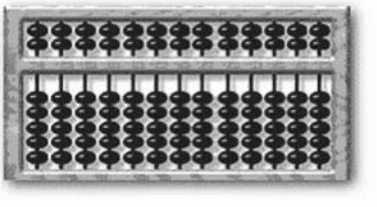


Abb. 1.5: Chinesisches Rechengerät Suan-pan
Quelle: siehe Abbildungsverzeichnis

Die Chinesen entwickelten besondere Fähigkeiten zum Lösen von Systemen linearer Gleichungen und simultaner Kongruenzen (vgl. Kapitel 5). Sie verfügten über ein algorithmisch durchgearbeitetes Verfahren zur Lösung linearer Gleichungssysteme. Der heute als *Chinesischer Restsatz* bekannte mathematische Satz von großer Bedeutung in Algebra und Zahlentheorie geht auf *Sun-Tse* (etwa 3. Jahrhundert n. Chr.) zurück. Eine typische Aufgabe, die mit diesen Kenntnissen gelöst wurde, lautete (vgl. Scheid 1972):

> Eine Bäuerin geht mit einem Korb Eier auf den Markt. Ein Pferd tritt auf den Korb und alle Eier zerbrechen. Der Reiter will für den Schaden aufkommen und fragt, wieviel Eier im Korb waren. Die Bäuerin erinnert sich nicht genau, sie weiß nur noch folgendes: „Wenn ich die Eier zu je zwei, drei, vier, fünf oder sechs aus dem Korb nahm, blieb jedesmal genau eines übrig. Wenn ich sie aber zu je sieben aus dem Korb nahm, blieb keines übrig."

Die **Maya** (ab dem 3. Jahrtausend v. Chr.), eine mittelamerikanische Hochkultur der Frühzeit, verfügten über ein sehr gut entwickeltes Zahlensystem (zur Basis 20), das sie insbesondere auch für ihre präzisen Kalenderberechnungen nutzen konnten.

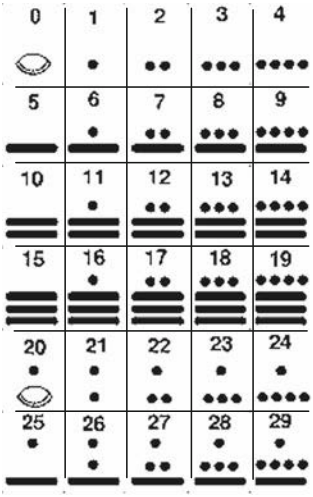


Abb. 1.6:
Zahlzeichen der Maya
Quelle: siehe Abbildungsverzeichnis

P. Beckmann schreibt in dem Buch *A History of* π (1971) „... it is clear that with a positional notation closely resembling our own of today, the Maya could outcalculate the Egyptians, the Babylonians, the Greeks, and all Europeans up to the Renaissance“.

Unter den **Griechen** (die Epoche der griechischen Antike umfasst etwa den Zeitraum von 800 v. Chr. bis 600 n. Chr.) setzte eine erhebliche Vertiefung und die erste systematische „wissenschaftliche“ Beschäftigung mit der Mathematik ein. Sie prägten auch den Begriff der Mathematik; für sie bedeutete

mathema: das Lernen, die Kenntnis, die Wissenschaft

Im Folgenden sind die Beiträge einzelner herausragender griechischer Forscherpersönlichkeiten dargestellt – vorrangig (aber nicht ausschließlich) aus der Perspektive der Zahlentheorie.

• *Thales von Milet* (ca. 624–547 v. Chr.) war Kaufmann, erster griechischer Astronom, Mathematiker und Philosoph. Auf seinen ausgedehnten Reisen lernte er die assyrisch-babylonische Astronomie des Zweistromlandes kennen.

Thales von Milet war einer der ersten, die versuchten, mathematische Sätze „streng“ zu beweisen und ihre Begründung nicht einfach der Anschauung oder der Empirie zu überlassen.

• *Pythagoras von Samos* (ca. 569–475 v. Chr.) war in der Antike eher als Mystiker, Prophet und Begründer eines Geheimbundes denn als Mathematiker bekannt. Die Schule (oder besser: der Geheimbund) der Pythagoreer beschäftigte sich mit Harmonielehre und elementarer Zahlentheorie (pythagoreische Zahlentripel, vollkommene und befreundete Zahlen, figurierte Zahlen, Lehre von Gerade und Ungerade). Erkennungszeichen des Geheimbundes der Pythagoreer war das aus den Diagonalen des regelmäßigen Fünfecks gebildete Sternfünfeck (Pentagramm), für dessen Konstruktion der *Goldene Schnitt* eine Rolle spielt. Die später erkannte Inkommensurabilität von Seite und Diagonale des Pentagramms führte zu einer philosophischen Grundlagen-Krise. Ob der „Satz des Pythagoras“ wirklich von Pythagoras stammt, muss eher als ungewiss angesehen werden. Die Mathematiker Theodorus, Theaitetos und Eudoxos waren maßgeblich an der Ausformung und Vervollkommnung der pythagoreischen Ideen beteiligt.

• *Theodorus von Kyrene* (ca. 465–398 v. Chr.) bewies, unter Verwendung der „Wurzelschnecke" (in unserer heutigen Sprache formuliert) die Irrationalität

der Zahlen $\sqrt{3},\sqrt{5},\ldots,\sqrt{17}$. Als wesentliches Hilfsmittel verwendete er die später auch von Euklid im „Euklidischen Algorithmus“ eingesetzte Methode der *Wechselwegnahme*.

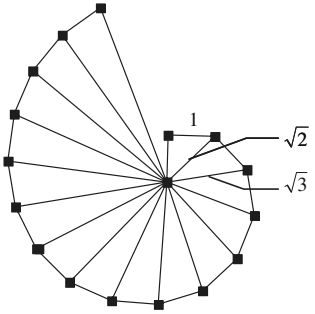


Abb. 1.7: Die Wurzelschnecke des Theodorus von Kyrene

• *Theaitetos von Athen* (ca. 417–369 v. Chr.) schuf, aufbauend auf Theodorus, eine umfassende Lehre von den *Irrationalitäten*. Seine Ergebnisse bilden den Inhalt des Buches X der „Elemente“ des Euklid.

• *Eudoxos von Knidos* (ca. 408–355 v. Chr.) ist der Begründer der *Größen-* bzw. *Proportionenlehre* – unter Einbezug auch irrationaler („inkommensurabler“) Größen. Wesentliche Ergebnisse von ihm gingen in Buch V und XII der Elemente des Euklid ein. Die später von Archimedes zur Bestimmung des Flächeninhalts von Parabelsegmenten herangezogene und für die moderne Analysis (Integralrechnung) bedeutsame *Exhaustionsmethode* geht auf Eudoxos zurück.

• *Euklid*[1] *von Alexandria* (ca. 325–265 v. Chr.) wird heute als Autor des enzyklopädischen Werks „Die Elemente“ angesehen. Die Existenz seiner Person bleibt jedoch im Dunkeln. Es wird gelegentlich sogar die These vertreten, dass es sich bei Euklid nicht um einen einzigen sondern um eine Gruppe von Autoren handelt. Insgesamt scheinen Mathematikhistoriker mehrheitlich aber

[1] Die Geschichte der Wissenschaft kennt zwei Männer des Namens *Euklid*: Den um 400 v. Chr. lebenden Philosophen aus Megara und den etwa ein Jahrhundert später in Alexandria wirkenden Mathematiker. Über letzteren berichtet sein Kommentator *Proklos Diadochos* (um 450 n. Chr.): *Wenig jünger als diese Mathematiker der Akademie ist Euklid, der die Elemente schrieb, der dabei vieles aus Eudoxos verwendete, vieles von Theaitetos Behandelte zum Abschluss brachte und, was von den Früheren nur oberflächlich dargestellt war, durch unanfechtbare Beweise stützte. Dieser Mann lebte zur Zeit des ersten Ptolemaios (*), denn Archimedes, der nach dem ersten kam, erwähnt den Euklid; auch erzählt man, dass Ptolemaios ihn einmal nach einem kürzeren Weg durch die Geometrie als das Elementwerk gefragt habe; er habe darauf geantwortet, einen besonderen Zugang für Könige zur Geometrie gebe es nicht.* (nach Clemens Thaer 1991, S 415)
(*) Der erste von insgesamt 15 hellenistisch geprägten Herrschern Ägyptens nach dem Zerfall des von Alexander dem Großen eroberten Weltreichs

der Auffassung zu sein, dass ein Mathematiker namens Euklid in Alexandria wirkte, also in der von Alexander dem Großen gegründeten Stadt, die sich rasch zu einem bedeutenden Wissenschaftszentrum der Antike entwickelte. Er fasste das gesamte mathematische Wissen seiner Zeit in den „Elementen" zusammen, einem aus dreizehn Büchern bestehenden Werk, das vielfach als eines der einflussreichsten Bücher der gesamten Weltliteratur bezeichnet wird und das mitunter bis ins 19. Jahrhundert hinein unverändert als Lehrbuch für Mathematik verwendet wurde. (Es war zweifellos das langlebigste und eines der erfolgreichsten Lehrbücher aller Zeiten.) In diesem Buch, das uns nur indirekt über Bearbeitungen und Kommentare seiner Nachfolger bekannt ist, trug er vieles von dem Wissen seiner Vorgänger zusammen und fügte eigene Erkenntnisse hinzu. Was im Einzelfall von ihm selbst stammt und was er übernommen hat, ist nicht immer mit Sicherheit zu sagen. Das auf dem Prinzip der *Wechselwegnahme* basierende Verfahren zur Bestimmung des größten gemeinsamen Teilers zweier natürlicher Zahlen ist heute untrennbar mit seinem Namen verbunden (*Euklidischer Algorithmus*) – ebenso wie der Satz, dass es unendlich viele Primzahlen gibt. Euklid verwendet sogar genauer die folgende hochinteressante Formulierung, mit der er den Begriff der („aktual") unendlichen Menge vermeidet (Neuntes Buch, §20): *Es gibt mehr Primzahlen als jede vorgelegte Anzahl von Primzahlen.*

• *Archimedes von Syrakus* (ca. 287–212 v. Chr.) war zweifellos der größte Wissenschaftler des Altertums und einer der größten Wissenschaftler aller Zeiten (Zitat nach van der Waerden 1966). Er nahm durch die systematische Anwendung der *Exhaustionsmethode* zur Ermittlung des Flächeninhalts von Parabelsegmenten die erst weit über tausend Jahre später formulierten Grundideen der Integralrechnung vorweg. Durch genialen Einsatz des Hebelgesetzes gelang es ihm, das Volumen der Kugel zu bestimmen. Eingekleidet in die Aufgabe, alle Sandkörner im Universum zu zählen, entwickelte er mit dem „Sandrechner" eine Systematik, um beliebig große Zahlen darzustellen (für die Griechen war ansonsten die Myriade, also 10.000, die größte benannte Zahl.)

• *Eratosthenes von Kyrene* (ca. 276–194 v. Chr.) lehrte, dass die Erde eine Kugel sei. Er bestimmte den Erdumfang mit erstaunlich hoher Genauigkeit auf 250000 „Stadien". Dies entspricht etwa der Strecke von 46000 Kilometern (heute wird als Wert für den Umfang des Äquators das Maß von 40075 Kilometern verwendet). Sein Name ist in der Zahlentheorie verbunden mit dem *Sieb des Eratosthenes,* dem Verfahren zur Ermittlung von Primzahlen.

• *Apollonius von Perge* (ca. 262–190 v. Chr.) war nach Archimedes einer der kreativsten Mathematiker der griechischen Antike. Er verfasste ein berühmtes achtbändiges Werk über Kegelschnitte (die *Konika*), in dem er – ohne Koordinatengeometrie und Formeln – als erster die einheitliche Herleitung aller Kegelschnitte durch ebene Schnitte ein und desselben Kegels beschrieb.

• *Heron von Alexandria* lebte um etwa 60 n. Chr. Seine Werke stellen eine Art Enzyklopädie in angewandter Geometrie, Optik und Mechanik dar. Sie haben oft den Charakter einer Formelsammlung. Viele der ihm zugeschriebenen Formeln und Verfahren waren schon vorher bekannt – so soll die „Heronsche Formel" für den Flächeninhalt von Dreiecken von Archimedes stammen; das „Heron-Verfahren" zum Wurzelziehen wurde schon Jahrhunderte vorher von den Babyloniern praktiziert.

• *Klaudios Ptolemaios* (ca. 85–165 n. Chr.) schuf mit dem *Almagest* das bedeutendste astronomische Werk der Antike; er benutzte dafür die babylonischen Zahlen (also das 60-er System) und trug dadurch zu ihrer Verbreitung bei. Die Auswirkungen davon sind bis in unsere heutige Zeit festzustellen; am direktesten in der 60-er Teilung unserer heutigen Uhren oder auch in der Winkelmessung (1 Stunde = 60 Minuten; 1 Vollkreis = 360 Grad).

• *Diophantos von Alexandria* (etwa 200–284 n. Chr.) knüpfte an die babylonische Tradition der Algebra und Zahlentheorie an. Er entwickelte Verfahren zur Lösung ganzzahliger Gleichungen, die ihm zu Ehren heute als *Diophantische Gleichungen* bezeichnet werden. Sein Hauptwerk, die *Arithmetika* (ein 13-bändiges Werk, von dem sechs Bände in Griechisch erhalten sind), ist der einzige erhaltene umfassende Text zu Algebra, Arithmetik und Zahlentheorie aus der griechischen Antike. Es beeinflusste maßgeblich die Entwicklung von Algebra und Zahlentheorie sowohl im arabisch-islamischen Kulturkreis als auch (wesentlich später) im christlichen Abendland.

Die Zahlschreibweise der Griechen hatte jedoch nicht den hohen Stand ihrer Mathematik (insbesondere ihrer Geometrie). Die griechische, auf Buchstaben basierende Zahlschreibweise eignete sich nicht zum Rechnen; Astronomen (wie Ptolemaios) verwendeten die babylonischen Zahlen für ihre umfangreichen Berechnungen. Und wenn es nicht um das konkrete Zahlenwerte ging sondern um allgemeine Aussagen („Gesetze") zahlentheoretischer Natur, dann stellten sie sich die Zahlen sowieso als Strecken, Flächen oder Punktmengen („figurierte" Zahlen) vor.

Den **Indern** verdanken wir unser Zehnersystem in seiner heutigen Form. Ihr entscheidender Beitrag zur vollen Ausbildung dieses Stellenwertsystems war die Verwendung eines Symbols für die Zahl Null („Erfindung der Null“). Die Entstehung der ersten indischen mathematischen Werke setzte ab etwa 500 n. Chr. ein. Die Inder waren darüber hinaus gute Algebraiker; sie entwickelten hochstehende Verfahren zum Lösen von Gleichungen.

Im Folgenden sind einige der führenden Forscherpersönlichkeiten aus dieser frühen Periode beschrieben:

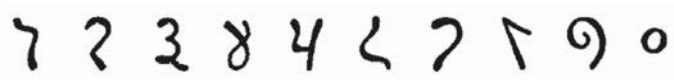
- *Aryabhata I* schrieb etwa im Jahre 500 die für die Folgezeit einflussreiche Abhandlung *Aryabhatiya* über die indische Astronomie und Mathematik.
- *Brahmagupta* verfasste etwa im Jahre 628 das in Versen geschriebene Werk *Brahmasphuta Siddhanta* (Vervollkommnung der Lehre Brahmas), in dem er Themen aus Arithmetik, Algebra und Geometrie behandelte.
- Der von *Bhaskara II* um 1150 verfasste *Siddhanta siromani* (Der Kranz der Wissenschaften) stellt einen Höhepunkt der indischen Mathematik dar. In ihm wird das damalige Wissen in den Gebieten Arithmetik, Geometrie, Algebra und Astronomie zusammengefasst.

In den folgenden Zeilen ist die Verbreitung der „indischen“ Ziffern skizziert. Die Araber hatten an diesem historischen Prozess einen großen Anteil. Sie trugen entscheidend zur Verbreitung der indischen Zahlschreibweise bei. Gelehrte des europäischen Mittelalters lernten diese Zahlen über Kontakte zu den Arabern (sei es durch Reisen in arabische Länder, wie z.B. Leonardo von Pisa, oder sei es über Kontakte zu herausragenden Stätten der arabischen Gelehrsamkeit in Spanien – besonders Cordoba, Sevilla, Granada) kennen. Deshalb werden die Zahlen in unserer heutigen Schreibweise auch als die „arabischen“ Zahlen bezeichnet.

Skizze zur Entwicklung der Zahlschreibweise im Zehnersystem:

Die Brahmi-Ziffern (1 2 3 4 5 6 7 8 9), etwa ab dem 3. Jahrhundert v.Chr.:

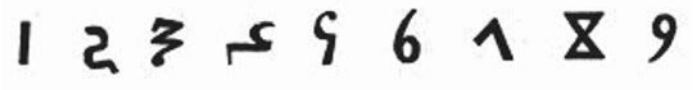
Die Gwalior-Ziffern, Indien, (1 2 3 4 5 6 7 8 9 0), etwa ab dem 8. Jahrhundert n. Chr.:



Die Devanagari-Ziffern (0 1 2 3 4 5 6 7 8 9), etwa ab dem 9. Jahrhundert n.Chr.:

Die ostarabischen Ziffern (0 1 2 3 4 5 6 7 8 9), etwa ab dem 9. Jahrhundert n.Chr.:

Die westarabischen (Gobar-) Ziffern (1 2 3 4 5 6 7 8 9), etwa ab dem 9. Jahrhundert n.Chr.:



Die Gutenberg-Ziffern (0 1 2 3 4 5 6 7 8 9), 15. Jahrhundert:

Die Ziffern nach Dürer (1 2 3 4 5 6 7 8 9 0), 16. Jahrhundert:

Abb. 1.8: Entwicklung der Zahlzeichen des Zehnersystems

Die Mathematik der **Araber** bzw. die Mathematik in den Ländern des *Islam* (ab ca. 750 n. Chr.): Gegen Ende des 6. Jahrhunderts entstand die Religionsbewegung des Islam auf der arabischen Halbinsel und breitete sich sehr schnell in den Ländern des Nahen Ostens, im Zweistromland, über Persien bis

nach Indien hinein und über Nordafrika bis auf die Iberische Halbinsel aus. Durch die Kontakte mit der indischen Kultur lernten die Araber das indische Zahlensystem kennen, das sie im Laufe der Zeit übernahmen. Da dieser Prozess über Jahrhunderte hinweg verlief, veränderte sich die Zahlschreibweise, ohne dass aber am Prinzip des Zehnersystems gerüttelt wurde. Die Araber assimilierten vieles von dem Wissen der eroberten oder benachbarten Kulturkreise (Perser, Ägypter, Inder) und insbesondere von der sich im Niedergang befindenden griechischen Kultur. Sie übersetzten wichtige griechische Werke der Wissenschaft ins Arabische. So blieben z.B. die Elemente des Euklid nur deshalb erhalten, weil sie als arabische Übersetzung überliefert sind.

In der Epoche der *Abbasiden-Dynastie* (etwa Mitte des 8. bis Mitte des 13. Jahrhunderts) erlebte die arabische Wissenschaft ihre Glanzzeit. In der Blütezeit (ca. 750–1000) entwickelte sich Bagdad unter den Kalifen *al-Mansur* und (dem aus den *Märchen aus 1001 Nacht* bekannten) *Harun al Raschid* zum Wissenschaftszentrum. Nach griechischem Vorbild wurde in Bagdad eine Akademie (genannt „Haus der Weisheit“) eingerichtet, zu deren Aufgaben es gehörte, in systematischer Weise die überlieferten griechischen, ägyptischen, persischen und indischen Quellen durch Übersetzung ins Arabische zu erschließen. Es entstanden langfristige astronomische und geographische Forschungsprogramme. In der Physik, Chemie, Medizin, Pharmakologie, Zoologie, Botanik, Mineralogie und Philosophie setzte sowohl in Bagdad als auch in anderen Zentren des arabisch-islamischen Raumes (insbesondere in Cordoba, Granada und Sevilla) eine rege Forschungstätigkeit ein. In den arabischen Zentren der Wissenschaft im Süden des heutigen Spaniens lernten später abendländische Mönche (Gerbert, Johannes von Sevilla, Adelard von Bath) die arabische und mit ihr auch die griechische Wissenschaft kennen und brachten sie von dort in die Länder des europäischen Abendlandes.

Einige herausragende mathematische Forscherpersönlichkeiten aus jener Zeit:

- Der persisch-arabische Mathematiker *al-Khwarizmi* (auch: al-Khowarizmi, al-Hwarizmi), ca. 790–850 n. Chr., erkannte den Wert der indischen Zahlschreibweise und schrieb das einflussreiche, später unter dem Titel „Über die indischen Ziffern“ (lateinisch: de numero indorum) bekannt gewordene Rechenbuch, das sehr viel zur Verbreitung und Popularisierung der indischen Ziffern beigetragen hat. Al-Khwarizmi war Autor weiterer berühmter und einflussreicher Bücher über Algebra und Astronomie; die Begriffe *Algorithmus* und *Algebra* gehen auf sein Wirken zurück.

Abb. 1.9: Statue von Al-Khwarizmi in Khiva (Usbekistan)
Quelle: siehe Abbildungsverzeichnis

• *Ibn al-Haitam* (ca. 965 – ca. 1039), auch Alhazen genannt, war Mathematiker, Astronom, Naturwissenschaftler und Arzt. Er formulierte (ohne Beweis) den heute nach J. Wilson benannten Satz: „Ist p eine Primzahl, dann ist $1+(p-1)!$ durch p teilbar“ (siehe Kapitel 7). Mit Hilfe seiner Ergebnisse über die Summation von Potenzen natürlicher Zahlen gelang ihm die Berechnung der Rauminhalte von Rotationskörpern.

• Unter *al-Biruni* (973–1048) und *al-Tusi* (1201–1274) entwickelte sich die Trigonometrie zu einem eigenständigen Zweig der Mathematik. In der Präzision der Berechnung astronomischer und trigonometrischer Tabellen (Sinustafel) ging er weit über Ptolemaios hinaus.

• *Al-Mu'taman ibn Hud* war von 1081 bis 1085 Herrscher des muslimischen Reiches von Zaragoza. Er unternahm den Versuch, mit dem *Istikmal* ein der Zeit gemäßes Nachfolgewerk für die Elemente des Euklid zu schreiben.

• *Al-Kashi* (1390–1450) war der letzte bedeutende Mathematiker des islamischen Mittelalters. Er berechnete die Kreiszahl π mit großer Genauigkeit (auf 17 Dezimalstellen) auf der Basis eines dem Kreis umbeschriebenen $3\cdot 2^{28}$–Ecks und einer hochgradig effizienten iterativen Berechnung von

$\sin 1^\circ$. Sein Verdienst besteht besonders auch in der systematischen Abhandlung und Verallgemeinerung wichtiger Ergebnisse und Verfahren früherer mittelalterlicher Gelehrter.

Die Zeitepoche der **Römer** und das **europäische Mittelalter**: Das Niveau der mathematisch-naturwissenschaftlichen Wissenschaften war in dieser Zeit durchweg sehr bescheiden und fiel weit hinter den Stand der Griechen zurück. Das römische Zahlensystem eignete sich für in Stein gemeißelte Inschriften; zum Rechnen war es höchst ungeeignet. Bestimmte Anwendungen (Militär, Handel, Architektur) erzwangen bestenfalls eine rudimentäre Beschäftigung mit mathematischen Fragestellungen.

Der römische Philosoph *Boethius* (ca. 480–525) übersetzte und kommentierte u.a. Schriften von Aristoteles, Euklid und des Neupythagoreers Nikomachos. Der für den Lehrbetrieb des Mittelalters prägende Begriff des „Quadriviums“ (Arithmetik, Geometrie, Musik, Astronomie) soll auf ihn zurückgehen. Er verfasste eine Schrift zur Arithmetik, die ihm im Mittelalter zu einem relativ hohen Bekanntheitsgrad verhalf; diesem Umstand ist vermutlich sein Einbezug in die historische Darstellung „Arithmetica, Pythagoras und Boethius“ in der Enzyklopädie *Margarita Philosophica* von Gregor Reisch zu verdanken (vgl. Abb. 1.12).

Der Mönch *Gerbert* (946–1003), der im Jahre 999 den päpstlichen Thron bestieg, lernte in Spanien die indisch-arabischen Ziffern kennen. Er erfasste ihren eigentlichen Sinn jedoch nicht und verwendete sie nur, um sie auf runde Scheiben („Apices“) aufzutragen und dann auf einem herkömmlichen Rechenbrett zu verwenden, ähnlich wie die schon vorher in Gebrauch befindlichen Rechensteine.

Umfangreichere Teile der islamischen Mathematik flossen im 12. Jahrhundert nach Europa ein – solche, die ursprünglich griechischer Herkunft waren und nun aus dem Arabischen ins Lateinische übersetzt wurden, und solche, die das Ergebnis eigenständiger Entwicklungen im Bereich des Islam darstellten. Dabei spielte die Übersetzerschule von *Toledo* eine herausragende Rolle. Um 1140 wurde das Rechenbuch des *al-Khwarizmi* durch *Johannes von Sevilla* (auch: Johannes Hispalensis bzw. Johannes Hispaniensis) ins Lateinische übertragen, und damit wurden die indisch-arabischen Ziffern den Europäern im Prinzip zugänglich. Eine arabische Euklid-Auswahl wurde durch *Adelard von Bath* um 1150 übersetzt. Die systematische Erschließung der wis-

senschaftlichen Werke der Antike unter bewusstem Rückgriff auf die griechischen Originaltexte (soweit noch vorhanden) erfolgte aber erst während der Periode der Renaissance.

1.3 Zur Entwicklung der schriftlichen Rechenverfahren

It is like coining the Nirvana into dynamos.

Der Mathematikhistoriker G. B. Halsted
– zur Erfindung der Null durch die Inder

In der Folgezeit nach *al-Khwarizmi* entwickelten sich die schriftlichen Rechenverfahren in einem sehr langwierigen Prozess, der schließlich zu einer allmählichen Überwindung des Abakus-Rechnens führte. Es kam zum Methodenstreit zwischen Abakisten und Algorithmikern (im Sinne von „Ziffernrechnern“) – von Gregor Reisch (ab 1503) in der Enzyklopädie *Margarita Philosophica* (vgl. Abb. 1.12) versinnbildlicht.

Das Rechnen mit den Ziffern setzte sich nur sehr langsam und gegen großen Widerstand gegenüber dem Rechnen am Rechenbrett (Abakus) durch. *Protagonisten* des Ziffernrechnens waren:

- *Leonardo von Pisa* („Fibonacci“, 1170–1250), Autor des Buches *Liber Abaci* (1202), mit dem er entscheidend zur Popularisierung der indisch-arabischen Zahlschreibweise beitrug. Eine außerordentlich kenntnisreiche Darstellung davon ist in dem Buch *Leonardi Pisani Liber Abaci ...* von H. Lüneburg zu finden.
- Die „Rechenmeister“, die an Rechenschulen den Umgang mit Zahlen, ihren Schreibweisen, Addition, Subtraktion, Multiplikation, Division sowie die Anwendungen auf Probleme des täglichen Lebens (Handel, Geldgeschäfte, ...) lehrten, so z.B. die

Abb. 1.10: Leonardo von Pisa ("Fibonacci")
Quelle: siehe Abbildungsverzeichnis

– *Practica welsch* (französisch-italienische Praktik)

oder die

– *Arte dela Mercandantia* (die Kunst der Kaufmannschaft)

Diese Formen des kaufmännischen Rechnens sind auch der Ursprung von Begriffen wie *Saldo*, *Diskont*, *Bilanz*, *Kredit*, *Valuta*, *Netto*, *Tara*, *Konto* und *Bankrott*.

- Populäre Rechenbücher und ihre Autoren:
  - das Bamberger Rechenbuch (1483)
  - Widmann: Behende und hubsche Rechenung auf allen kauffmannschafft (Leipzig, 1489)
  - Köbels Rechenbuch (1514)
  - *Adam Ries* oder auch *Riese* (1492–1559): Autor der weit verbreiteten Rechenbücher:
    * Rechnung auff der Linihen (1518)
    * Rechnung auff der Linien und Federn (1522)
    * Rechenung nach der lenge auff den Linihen und Feder (1550)

Abb. 1.11:
Adam Ries Denkmal in Erfurt
Quelle: siehe Abbildungsverzeichnis

Die *Widerstände* gegen das Ziffernrechnen hatten vor allem folgende Ursachen:

- die über tausendjährige Tradition des Abakus-Rechnens

- die Ablehnung des Ziffernrechnens durch Theologen („heidnische Praxis, Teufelswerk“) – dies führte z.B. im Jahre 1299 zum Verbot der indisch-arabischen Ziffern in Florenz
- die (vermeintlich) größeren Fälschungsmöglichkeiten beim Ziffernrechnen (aber Fälschungen waren auch mit den römischen Ziffern möglich; sprichwörtlich geworden ist der Ausdruck „*Jemandem ein* X *für ein* U *vormachen*“, der auf die römische Schreibweise für die Zahlen fünf (römisch: V, auch gelesen als U) und zehn (römisch: X) zurückgeht).
- der ungewohnte Gebrauch der Null
- die fehlende Einheitlichkeit in der Ziffernschreibweise

Der Höhepunkt der Auseinandersetzung zwischen *Abakisten* und *Algorithmikern* lag etwa in der Zeit zwischen Ende des 15. und Anfang des 16. Jahrhunderts. Zwar blieben die Rechentische noch lange in Gebrauch (zum Teil bis ins 18. Jahrhundert hinein); aber allmählich setzte sich das schriftliche Rechnen mit den indisch-arabischen Ziffern durch. Ein wichtiges Motiv für die Verwendung der Ziffern war der Umstand, dass man in den Handelskontoren, Schreib- und Rechenstuben der Kaufleute mit diesen Ziffern nicht nur *rechnen*, sondern die Rechnungen zugleich auch *dokumentieren* konnte. Damit wurde es im großen Stil möglich, Abrechnungsbücher und Konten zu führen.

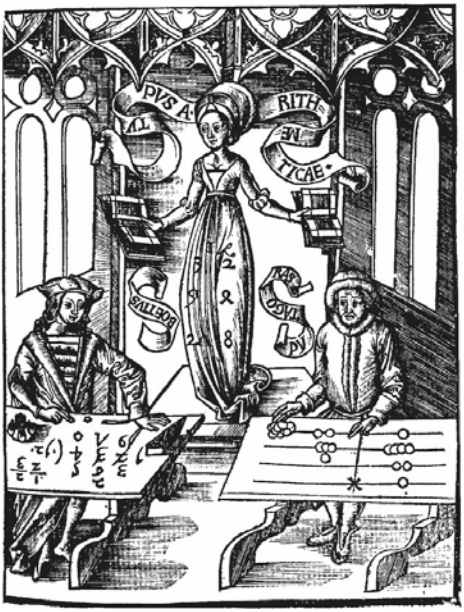


Abb. 1.12: Gregor Reisch, Margarita Philosophica
Quelle: siehe Abbildungsverzeichnis

Die Abbildung mit Pythagoras, Boethius und der Dame Arithmetica von Gregor Reisch (Abb. 1.12), aus der Enzyklo-

pädie *Margarita Philosophica* (ab 1503) symbolisiert diesen Streit zwischen den Abakisten und den Algorithmikern.

Die Zahldarstellung im Zehnersystem bot sich in hervorragender Weise für den weiteren Ausbau des Ziffernrechnens an. Die wichtigsten Stationen waren dabei:

- die Einführung der Dezimalbrüche durch Simon Stevin (1548–1620, Holland), Autor des Buches De Thiende (1585)
- die Entwicklung des logarithmischen Rechnens durch
  - Michael Stifel (ca. 1487–1567), Autor des Buches *Arithmetica integra* (1544)
  - Jost Bürgi (1552–1632, Uhrmacher und Feinmechaniker)
  - Lord John Napier bzw. Neper (1550–1617, Schottland): Autor der Schrift *Mirifici logarithmorum canonis descriptio* (Beschreibung einer Tafel wunderbarer Rechnungszahlen) aus dem Jahre 1614.
  - Henry Briggs (1561–1630, England): ab etwa 1615 Übergang zu den dekadischen Logarithmen

1.4 Erste Höhepunkte der neuzeitlichen Entwicklung

Pierre de Fermat (1601–1665), Jurist und Mathematiker, gab der Zahlentheorie wichtige neue Impulse. Nach ihm ist der „kleine Fermatsche Satz“ benannt: Ist p eine Primzahl, die kein Teiler von a ist, so gilt: $a^{p-1} \equiv 1 \pmod{p}$.

Eine Serie von Primzahlen (heute als Fermatsche Primzahlen bezeichnet, vgl. Abschnitt 4.7) ist nach ihm benannt. Mit seinem (von ihm nicht bewiesenen) „großen Fermatschen Satz“ bzw. seiner „Fermatschen Vermutung“:

> *Die Gleichung* $x^n + y^n = z^n$ *hat für* $n > 2$ *in der Menge der natürlichen Zahlen* (*größer oder gleich* 1) *keine Lösungen.*

Abb. 1.13:
Pierre de Fermat
Quelle: siehe Abbildungsverzeichnis

beeinflusste er die Entwicklung von Mathematik und Zahlentheorie über Jahrhunderte hinweg. Ganze Bereiche der modernen Algebra, besonders die Ring- und Körpertheorie, verdanken ihre Entstehung dem Versuch, die Fermatsche Vermutung zu beweisen. Die Aussage wurde erst kürzlich „mit sehr schwerem Geschütz“ bewiesen. Den Schlussstein auf die extrem lange Beweiskette, an der die besten Mathematiker aller Zeiten beteiligt waren, setzte der englische Mathematiker *Andrew Wiles*.

Gottfried Wilhelm Leibniz (1646–1716) wird wegen seiner Aktivitäten als Mathematiker, Philosoph, Theologe, Rechtsgelehrter, Naturwissenschaftler, Geologe, Geschichts- und Sprachforscher heute als einer der „letzten Universalgelehrten“ bezeichnet. Vielfach ist er primär wegen seines Prioritätenstreits mit dem großen englischen Mathematiker und Physiker Isaac Newton (1643–1727) über die Erfindung des Infinitesimalkalküls bekannt. Auf ihn geht aber noch eine Vielzahl anderer bedeutender Ideen zurück, welche die Entwicklung der Mathematik (und später der Informatik) massiv beeinflusst haben – und zwar sowohl im theoretischen als auch im praktischen Bereich.

Abb. 1.14: G.W. Leibniz
Quelle: siehe Abbildungsverzeichnis

1673 konstruierte er in London eine der ersten Vierspezies-Rechenmaschinen mit Staffelwalze. Es gab jedoch feinmechanische Probleme durch relativ große Fertigungstoleranzen, so dass die Maschine erst später als Nachbau entsprechend seinen Originalplänen wirklich funktionierte.

Ein fundamentaler theoretischer Beitrag zur Mathematik und Informatik ist die von Leibniz formulierte Idee einer logisch-mathematischen Universalsprache, in der alle Probleme kalkülhaft „durch Nachrechnen“ gelöst werden können („*Ich hätte gehofft, eine Art allgemeiner Charakteristik zu geben, in der alle Vernunftwahrheiten auf eine Art von Kalkül zurückgeführt würden. Dies könnte gleichzeitig eine Art universeller Sprache oder Schrift sein, doch wäre sie unendlich verschieden von allen denen, die man bislang projektiert hat ...*“, Zitat nach Specht 1979).

Für die Entwicklung der Zahlentheorie war seine die Entdeckung des *Zweiersystems* (vgl. Kapitel 6) von Bedeutung, mit der Leibniz darüber hinaus noch eine der theoretischen Grundlagen für die heutige Computertechnik (lange vor ihrer technischen Realisierung) vorbereitete.

Leonhard Euler (1707–1783) erzielte bahnbrechende Resultate auf fast allen damals bearbeiteten mathematischen Gebieten.
In der Zahlentheorie verallgemeinerte und korrigierte er manche Ergebnisse von Fermat. Die dabei entwickelte *Eulersche Funktion* trägt heute seinen Namen. Euler zeigte u.a. auch. dass die „Fermatsche“ Zahl

$$F_5 = 2^{2^5} + 1 = 2^{32} + 1 = 4294967297$$

den Teiler 641 hat und somit (im Gegensatz zu Fermats Vermutung) keine Primzahl ist.

Abb. 1.15: Leonhard Euler, Sowjetische Briefmarke 1957

Euler entwickelte bei der Lösung des ihm von Kant[2] gestellten *Königsberger Brückenproblems* das neue Gebiet der Graphentheorie. Seine Entdeckung des später nach ihm benannten *Eulerschen Polyedersatzes* war der Ausgangspunkt für die Entwicklung der neuen mathematischen Disziplin der „Topologie“.

[2] Immanuel Kant (1724–1804), deutscher Philosoph

Carl Friedrich Gauß (1777–1855), einer der größten Mathematiker aller Zeiten, bereicherte die Mathematik und Astronomie durch tiefliegende Ergebnisse auf allen Gebieten.

Gauß wurde im Alter von sieben Jahren in die Katharinen-Schule in Braunschweig geschickt. Schon als Schüler in der Elementarschule entdeckte er zur Überraschung seines Lehrers die Methode des „kleinen Gauß“:

Abb. 1.16: Carl Friedrich Gauß, Briefmarke DDR 1977

Um die Schulklasse des kleinen Gauß eine Weile lang zu beschäftigen, gab ihr der Lehrer J. G. Büttner eines Tages die Aufgabe, die natürlichen Zahlen von 1 bis 100 aufzuaddieren. Völlig überraschend für den Lehrer kam Gauß nach kurzer Zeit mit der (richtigen) Antwort nach vorn. Er hatte mit den zu addierenden Zahlen folgendermaßen gespielt: Zu berechnen war der Ausdruck

$$1 + 2 + 3 + \ldots + 98 + 99 + 100 \,.$$

Gauß schrieb noch den Ausdruck in umgekehrter Reihenfolge dazu

$$\begin{aligned} &1 + 2 + 3 + \ldots + 98 + 99 + 100 \\ &100 + 99 + 98 + \ldots + 3 + 2 + 1 \,. \end{aligned}$$

Wenn er alle Zahlen in diesem doppelzeiligen Schema addierte, so erhielt er das Doppelte der gesuchten Summe. Er entdeckte, dass die Spaltensummen alle gleich waren, und zwar jeweils gleich 101. Insgesamt gab es 100 Spalten, jede mit der Summe 101. Durch spaltenweise Addition erhielt er also die Gesamtsumme $101 \cdot 100$ (=10100) für das doppelzeilige Schema. Das war das

Doppelte dessen, was der Lehrer berechnet haben wollte. Die Antwort auf die vom Lehrer gestellte Frage lautete also:

```
1 + 2 + 3 + ... + 98 + 99 + 100  =  101 • 50  =  5050 .
```

Gauß hatte auf diese Weise als junger Schüler eine *paradigmatische* Begründung für die folgende Formel entdeckt:

$$1 + 2 + 3 + ... + (n\text{-}2) + (n\text{-}1) + n = \frac{1}{2} \cdot n \cdot (n+1) \qquad (* \text{ G } *)$$

Abb. 1.17: Gauß auf 10 DM Schein

Sein Lehrer erkannte bald das Talent des jungen Gauß und bemühte sich, ihn zu fördern. Im Alter von etwa 20 Jahren, zu Beginn seines Studiums, löste Gauß das Jahrhunderte alte Problem der Konstruktion des regelmäßigen 17-Ecks mit Zirkel und Lineal. Dieses (nicht zuletzt im Hinblick auf sein Alter) grandiose Erlebnis motivierte ihn, sein Berufsleben der mathematischen Forschung zu widmen.

Auf Gauß gehen weitere bahnbrechende Entdeckungen und Ergebnisse zurück im Zusammenhang mit den Themen: Kongruenzen, quadratische Formen, Kreisteilung, komplexe Zahlen, Großer Primzahlsatz (Vermutung), Fundamentalsatz der Algebra, Funktionentheorie, konforme Abbildungen, Reziprozitätsgesetz für quadratische Reste, nichteuklidische Geometrie, Astronomie (Bahnberechnung des Planetoiden Ceres), Vermessungskunde, Methode der kleinsten Quadrate, Differentialgeometrie u.v.m.

Sein zahlentheoretisches Hauptwerk, die *Disquisitiones arithmeticae* (1801) ist eines der bedeutendsten mathematischen Werke aller Zeiten. Mit dem Erscheinen dieses Werkes durfte die Zahlentheorie als selbständige, systematisch

geordnete Disziplin gelten und ihre weitere Entwicklung nahm einen rasanten Verlauf. Von Gauß soll auch das Bonmot stammen: Die Mathematik ist die Königin der Wissenschaften und die Arithmetik (Zahlentheorie) ist die Königin der Mathematik.

Zur Leistung großer Mathematiker (z.B. Fermat, Gauß, Riemann[3], Hilbert[4] u.a.) gehören nicht nur die von ihnen bewiesenen „Sätze" sondern gelegentlich auch berühmte und zukunftsweisende Vermutungen. Der von Gauß vermutete „große Primzahlsatz" konnte erst nach über 100 Jahren vollständig bewiesen werden, und zwar, aufbauend auf Ergebnissen des russischen Mathematikers P. L. Chebyshev (1821–1894), unabhängig voneinander durch die französischen Mathematiker J. Hadamard (1865–1963) und C. de la Vallée-Poussin (1866–1962).

Ab Mitte des 19. Jahrhunderts entwickelte sich die Zahlentheorie durch die Verschmelzung mit den Methoden und Gebieten der modernen Algebra (Körpertheorie, Idealtheorie, algebraische Zahlentheorie) in neue Richtungen. Diese Entwicklung ist mit der Arbeit einer großen Zahl von brillanten Mathematikern verbunden (Kummer[5], Kronecker[6], Dedekind[7], Hensel[8], Minkowski[9] und anderen). David Hilbert, einer der größten Mathematiker des 20. Jahrhunderts schuf mit seinem vielbeachteten *Zahlbericht* im Jahre 1897 eine Plattform, von der aus die Entwicklung der Zahlentheorie im 20. Jahrhundert konsequent weiter ging.

Abb. 1.18:
David Hilbert
Quelle: siehe Abbildungsverzeichnis

Dieser kleine historische Einblick in die Geschichte der Zahlentheorie soll nicht beendet werden, ohne Hinweis auf eine der faszinie-

[3] Bernhard Riemann (1826–1866)
[4] David Hilbert (1862–1943)
[5] Ernst Eduard Kummer (1810–1893)
[6] Leopold Kronecker (1823–1891)
[7] Richard Dedekind (1831–1916)
[8] Kurt Hensel (1861–1941)
[9] Hermann Minkowski (1864–1909)

rendsten Persönlichkeiten in der Zahlentheorie: Srinivasa Ramanujan. Ramanujan wurde 1887 in Süd-Indien geboren. Er brachte sich als Schüler autodidaktisch ein erstaunliches mathematisches Wissen bei, das ihn teilweise bis an die Grenzen der mathematischen Forschung führte. Da er fast völlig isoliert arbeitete, praktizierte er hochgradig unübliche Notations-, Darstellungs- und Argumentationsformen. Als er versuchte, mit Mathematikern in England in Kontakt zu treten, scheiterte dies fast an der Unverständlichkeit dessen, was er aufgeschrieben hatte. Nur der große englische Zahlentheoretiker Godfrey H. Hardy (1877–1947) erkannte Ramanujans Talent, holte ihn nach Cambridge, förderte ihn und begann eine mathematisch außerordentlich fruchtbare Kooperation mit ihm, die allerdings durch den frühen Tod von Ramanujan bereits im Jahre 1920 beendet wurde.

Abb. 1.19:
Srinivasa Ramanujan
Quelle: siehe Abbildungsverzeichnis

Abb. 1.20:
G. H. Hardy
Quelle: siehe Abbildungsverzeichnis

2 Die Division mit Rest und die Teilbarkeitsrelation

Zahl ist die aus Einheiten zusammengesetzte Menge.
Euklid, Die Elemente VII. Buch, Definition 2

Vorbemerkung: Einige für das folgende wichtige Begriffsbildungen und Voraussetzungen sind im Anhang zusammengestellt; insbesondere in Anhang 8.1: Allgemeine Beweisprinzipien und Beweisverfahren, Anhang 8.2: Axiomatische Beschreibung der natürlichen Zahlen, Anhang 8.3: Mengentheoretische Grundbegriffe

2.1 Die Division mit Rest

Fundamental für die gesamte Zahlentheorie ist der

Satz 2.1 (Division mit Rest):
Zu je zwei natürlichen Zahlen a und b (mit $b \neq 0$) gibt es stets eindeutig bestimmte nichtnegative ganze Zahlen q und r mit der Eigenschaft

$a = q \cdot b + r$ und $0 \leq r < b$

Bemerkungen:

- Der Satz drückt (etwas formaler aufgeschrieben) den Sachverhalt der aus dem Grundschulunterricht bekannten Division mit Rest aus. Wenn man eine natürliche Zahl a durch eine natürliche Zahl b dividiert, dann bezeichnet man die Vielfachheit, mit der b „ganz“ in a aufgeht, als den *Quotienten* q. Bei dieser Division bleibt unter Umständen ein *Rest* r übrig, wie z.B. im Falle $17 = 3 \cdot 5 + 2$ ($a = 17$; $b = 5$; $q = 3$; $r = 2$). Ist der Rest gleich Null, wie etwa im Falle $24 = 4 \cdot 6 + 0$, dann sagt man auch, dass die Zahl b die Zahl a (ohne Rest) *teilt* – man vergleiche dazu die Ausführungen zur Teilbarkeitsrelation weiter unten.
- Die Bedeutung des Satzes für die gesamte Schulmathematik – und darüber hinaus – kann kaum überschätzt werden (nicht zuletzt deswegen werden im Folgenden auch zwei Beweise gegeben); die Division mit Rest tritt später im Zusammenhang mit der Division von Polynomen wieder auf; sie spielt in der gesamten Algebra (Ringtheorie) eine große Rolle.

J. Ziegenbalg, *Elementare Zahlentheorie*, DOI 10.1007/978-3-658-07171-4_2

Im Folgenden werden zwei Beweise für den Satz angegeben; der erste basiert auf dem Prinzip des kleinsten Elements, der zweite auf dem Verfahren der vollständigen Induktion. Auf diese Weise soll auch die Austauschbarkeit der beiden Beweisprinzipien an einem konkreten Beispiel demonstriert werden.

Erster Beweis des Satzes von der Division mit Rest (mit dem Prinzip des kleinsten Elements):

Zunächst zur *Existenzaussage* (d.h. zu dem Teil des Satzes, der besagt: *„Es gibt ...“*). Wir betrachten die Menge

$A := \{x \in \mathbb{N}_0 :\ x = a - k \cdot b \ \text{ mit } \ k \in \mathbb{N}_0\}$.

Die Menge A ist eine nichtleere Teilmenge von $\mathbb{N}_0$ (denn mit $k = 0$ ist z.B. $a \in A$); sie enthält also ein kleinstes Element – es sei mit r bezeichnet.
Dieses r entsteht, anschaulich gesprochen, dadurch, dass man von a alle Vielfachen von b abzieht: a, $a-b$, $a-2b$, $a-3b$, $a-4b$, ... Die entstehende Differenz wird dabei immer kleiner, und irgendwann auch einmal negativ; r ist die letzte (kleinste) nichtnegative Zahl unter diesen Differenzen.

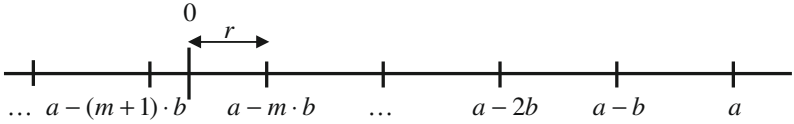


Abb. 2.1: kleinstes Element

Notwendigerweise gilt $r < b$, denn sonst wäre $r' := r - b$ eine noch kleinere zu A gehörende Zahl (im Widerspruch zu der Annahme, dass r das kleinste Element von A sei). Es gilt also $r = a - m \cdot b$ für eine ganze Zahl m. Mit r und $q := m$ haben wir genau die Zahlen gefunden, deren Existenz im Satz von der Division mit Rest behauptet wird.

Nun zur *Eindeutigkeitsaussage* (also zu dem Teil der Aussage, der besagt: „ ... gibt es *eindeutig bestimmte* ...“):
Angenommen, es sei $a = q_1 \cdot b + r_1$ und $a = q_2 \cdot b + r_2$ mit $0 \le r_1 < b$ und $0 \le r_2 < b$. Dann ist: $q_1 \cdot b + r_1 = q_2 \cdot b + r_2$. (*)

Zwischenbehauptung: Die Faktoren q_1 und q_2 können nicht verschieden sein. Denn sonst wäre einer davon größer, etwa $q_1 > q_2$. Dann wäre aber auch $q_1 \cdot b > q_2 \cdot b$. Wegen $r_2 < b$ wäre sogar $q_1 \cdot b > q_2 \cdot b + r_2$ und so-

mit erst recht $q_1 \cdot b + r_1 > q_2 \cdot b + r_2$ – im Widerspruch zur anfangs gemachten Annahme (*). Also sind die Faktoren q_1 und q_2 gleich.

Dann folgt aber sofort aus (*), dass auch die Reste r_1 und r_2 gleich sein müssen und die Eindeutigkeitsaussage ist bewiesen.

Bemerkung und *Übung*: Die in der Existenzaussage gegebene Konstruktion des Elements r ist auch gültig für die Fälle, wo $a = b$ oder $a < b$ ist. Geben Sie für diese beiden Fälle die im Satz von der Division mit Rest genannten Größen q und r an.

Zweiter Beweis des Satzes von der Division mit Rest (mit vollständiger Induktion):

Zunächst zur *Existenzaussage*: Der Beweis wird mit vollständiger Induktion (nach *a*) geführt. Die (natürliche) Zahl b sei im Folgenden beliebig (aber fest) gewählt. (Wegen $b \in \mathbb{N}$ ist insbesondere $b \geq 1$.)
Induktionsverankerung: Es ist zunächst zu zeigen, dass die Aussage für $a = 1$ richtig ist. Wir führen eine Fallunterscheidung durch.

1. *Fall*: Es sei $b = 1$. Dann ist die Aussage richtig mit $q = 1$ und $r = 0$.

2. *Fall*: Es sei nun $b > 1$. Dann ist die Aussage richtig mit $q = 0$ und $r = 1$.

Induktionsschritt: Die Aussage gelte für $a = k$ (*Induktionsannahme*). Es ist zu zeigen, dass dann die Aussage auch für $k+1$ gilt (*Induktionsschluss*).

Nach *Induktionsannahme* ist also $a = q \cdot b + r$ mit $0 \leq r < b$. Es ist zu zeigen: $a + 1 = q' \cdot b + r'$ für geeignete natürliche Zahlen q' und r' mit $0 \leq r' < b$. (*Bemerkung*: Der „Strich" hat hier nicht die Bedeutung der in den Peano-Axiomen auftretenden Nachfolgerfunktion; er soll jeweils einfach ein alternatives q bzw. r andeuten.)

Wir machen eine Fallunterscheidung bezüglich der Variablen *r*:

1. *Fall*: r sei so groß wie möglich, d.h., es sei $r = b - 1$.
   Dann ist $a + 1 = q \cdot b + r + 1 = q \cdot b + b = (q+1) \cdot b + 0$ und die Aussage ist richtig mit $q' = q + 1$ und $r' = 0$.

2. *Fall*: r sei nicht so groß wie möglich, d.h., es sei $r < b - 1$.
   Dann ist $a + 1 = q \cdot b + (r + 1)$ und die Aussage ist ebenfalls richtig, denn dann ist $r' := r + 1 < b$.

Die *Eindeutigkeitsaussage* wird wie oben bewiesen.

Wegen der Eindeutigkeit der Darstellung kann man q und r auch als Funktionswerte geeigneter *Funktionen* deuten. Häufig (so z.B. auch in den meisten Programmiersprachen) werden diese Funktionen als *Div* und *Mod* bezeichnet:

$$\begin{aligned} Div: \quad (a,b) &\rightarrow Div(a,b) = q \\ Mod: \quad (a,b) &\rightarrow Mod(a,b) = r \end{aligned}$$

Der Satz von der Division mit Rest kann also auch folgendermaßen ausgedrückt werden:

$$a = Div(a,b) \cdot b + Mod(a,b)$$

Veranschaulichung

Im folgenden Beispiel sei $a = 17$ und $b = 5$ gewählt. Die nach dem Satz von der Division existierenden Zahlen q und r haben dann die Werte $q = 3$ und $r = 2$. Die in dem Satz auftretende Gleichung lautet dann $17 = 3 \cdot 5 + 2$. Ergänzend zum formalen Beweis ist die *Veranschaulichung* des Sachverhalts von großer Bedeutung. Dazu stellen wir uns die Zahlen a und b, ganz im Sinne der Griechen, als *Strecken* vor; a möge die größere und b die kleinere Strecke sein. Dann kann man b einmal oder mehrmals auf a abtragen (bzw. „von a wegnehmen“), bis nichts mehr übrig bleibt oder bis ein Rest übrig bleibt, der kleiner ist als b.

Die im obigen Satz auftretende Zahl q ist die *Vielfachheit* (bzw. der *Quotient*), mit der man b „ganz“ auf a abtragen kann; r ist der *Rest*, der danach übrig bleibt. Es ist offensichtlich, dass r kleiner als b ist (wie im Satz formuliert). Wenn $r = 0$ ist sagt man auch, dass die Strecke b die Strecke a *misst* bzw. dass die Zahl b die Zahl a *teilt*.

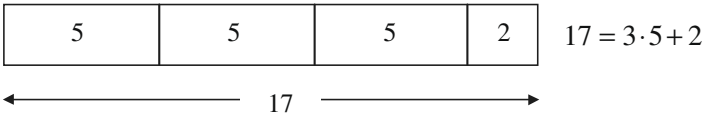


Abb. 2.2: Division mit Rest

Diese Veranschaulichung macht deutlich, warum die Division häufig als „iterierte“ (wiederholte) Subtraktion erklärt und eingeführt wird.

Vorsicht

Veranschaulichung ist zwar wichtig, sie kann gelegentlich aber auch zu Täuschungen Anlass geben. Hier eine kleine Warnung vor allzu blindem Vertrauen in die Anschauung:

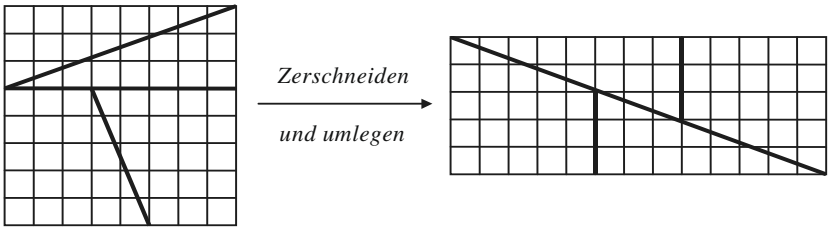


Abb. 2.3: Zerschneiden und Umlegen ... Konsequenz ?

2.2 Die Teilbarkeitsrelation

Zur Wiederholung der Grundbegriffe Menge, Relation, Relationseigenschaften, Äquivalenzrelation, Ordnungsrelation siehe Anhang 8.3.

Definition 2.1: Die (ganze) Zahl b *teilt* die (ganze) Zahl a, wenn es eine (ganze) Zahl n gibt mit der Eigenschaft $a = n \cdot b$.

(Entsprechendes kann man auch bezogen auf die Menge der natürlichen Zahlen formulieren; überall, wo „ganze“ Zahl steht, ist dann jeweils „natürliche“ Zahl einzusetzen.)

Im Zeichen: $b \mid a$

Gleichwertige *Sprechweisen*: b teilt a,
b misst a,
b ist ein Teiler von a,
a ist ein Vielfaches von b

Mit anderen Worten: b teilt a, wenn der im Satz von der Division mit Rest auftretende Divisionsrest bei der Division von a durch b gleich Null ist.

Aufgabe 2.1:

- Jede natürliche Zahl a hat die „trivialen“ Teiler 1 und a (wie viele sind das?).

- Für welche Zahlen x gilt $1 \mid x$, $x \mid 1$, $0 \mid x$, $x \mid 0$?

Man sagt, eine natürliche Zahl ist *gerade*, wenn sie von der Zahl 2 geteilt wird (anders ausgedrückt: wenn sie ein Vielfaches von 2 ist); andernfalls wird sie als *ungerade* bezeichnet.

Eine ganze Zahl a heißt *Quadratzahl*, wenn es eine ganze Zahl b gibt mit der Eigenschaft: $a = b \cdot b =: b^2$

Aufgabe 2.2: $1,\ 1+3=4=2^2,\ 1+3+5=9=3^2,\ 1+3+5+7=16=4^2$ sind Quadratzahlen. Zeigen Sie (einmal durch eine geeignete Visualisierung, einmal durch vollständige Induktion), dass die Summe aufeinanderfolgender ungerader Zahlen, beginnend bei 1, stets eine Quadratzahl ist.

Teilermengen und Vielfachenmengen

Im Folgenden sei mit $\mathbb{G}$ diejenige „Grundmenge“ bezeichnet, in deren Kontext die Teilbarkeitsrelation jeweils diskutiert wird; also z.B. $\mathbb{G} = \mathbb{N}$, $\mathbb{G} = \mathbb{N}_0$ oder $\mathbb{G} = \mathbb{Z}$.

Wir definieren:

$T(a) = \{x \in \mathbb{G} :\ x \mid a\}$ = Menge aller Teiler von a

$V(a) = \{x \in \mathbb{G} :\ a \mid x\}$ = Menge aller Vielfachen von a

Aufgabe 2.3: Diskutieren Sie die Frage, für welche Werte von $\mathbb{G}$ und für welche Werte von a die Mengen $T(a)$ und $V(a)$ jeweils endlich oder unendlich sind.

Zur Darstellung von Teilermengen

- *Venn-Diagramme*[10]
  Beispiel: T(432)

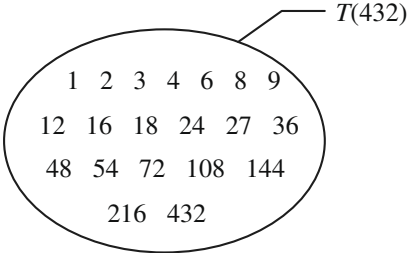


Abb. 2.4: Venn-Diagramm

Während Venn-Diagramme eine relativ unübersichtliche Darstellung der je-

[10] John Venn (1834–1923), englischer Mathematiker

weiligen Teilermenge liefern, sind Hasse-Diagramme (sofern anwendbar) wesentlich besser strukturiert.

- *Hasse-Diagramme*[11]

Beispiel: T(432)

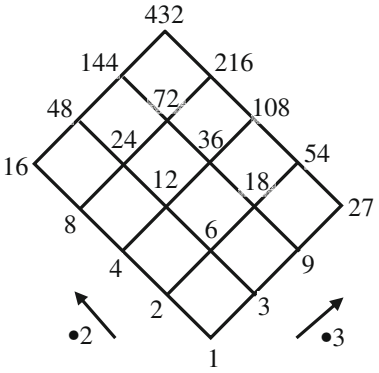


Abb. 2.5: Hasse-Diagramm

Ein weiteres Beispiel: $T(1400)$

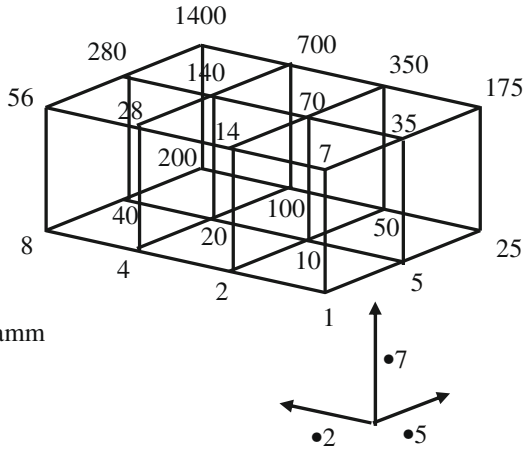


Abb. 2.6: Hasse-Diagramm mit drei Primteilern

Die Beispiele machen deutlich, dass Hasse-Diagramme für die Darstellung der Teilermengen von natürlichen Zahlen geeignet sind, die maximal drei Primteiler besitzen. (Zum Begriff des Primteilers: siehe Kapitel 4).

[11] Helmut Hasse (1898–1979), deutscher Mathematiker

Erste Beobachtungen zur Teilbarkeits-Relation

- Teiler treten in der Regel *paarweise* auf: Ist $a = b \cdot c$ $(a, b, c \in \mathbb{G})$ so ist mit b stets auch c ein Teiler von a. Welche Konsequenzen hat das?

  Zusatzbemerkung: Ist $a = b \cdot c$, so gilt: $b \le \sqrt{a}$ oder $c \le \sqrt{a}$

  (Nicht beide Faktoren können größer als $\sqrt{a}$ sein. Und entsprechend können auch nicht beide Faktoren kleiner als $\sqrt{a}$ sein.)

  Beweis: Übung

  Ist $a = b \cdot c$ mit $b \neq c$, so nennt man b und c auch *Komplementärteiler*.

- Teilermengen mit *ungerader* Elementezahl

  Aufgabe 2.4: Welche Zahlen passen zum nebenstehenden Teilerdiagramm?

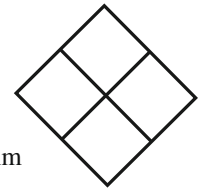


Abb. 2.7: Hasse-Diagramm mit ungerader Teilerzahl

Aufgabe 2.5: Zeichnen Sie ein Hasse-Diagramm zu den Teilern von 128.

Aufgabe 2.6: Zeigen Sie: Für jede natürliche Zahl n gilt $(1-x) \mid (1-x^n)$ und bestimmen Sie den Komplementärteiler.

Allgemeine Eigenschaften der Teilbarkeitsrelation

Bezogen jeweils auf die Grundmenge der *natürlichen* oder der *ganzen* Zahlen gilt:

- *Transitivität der Teilbarkeitsrelation*

  (T-1) Aus $a \mid b$ und $b \mid c$ folgt $a \mid c$.

  Beispiel: Es gilt $6 \mid 18$ und $18 \mid 72$. Deshalb gilt auch $6 \mid 72$.

  Beweis: $a \mid b$ bedeutet: Es gibt eine ganze Zahl n mit $n \cdot a = b$.

  $b \mid c$ bedeutet: Es gibt eine ganze Zahl k mit $k \cdot b = c$.

  Daraus folgt: $c = k \cdot b = k \cdot n \cdot a = r \cdot a$ (mit $r = k \cdot n$). Also gilt: $a \mid c$.

- *Verträglichkeit der Teilbarkeitsrelation mit der Multiplikation*

  (T-2) Aus $a \mid b$ folgt $a \cdot c \mid b \cdot c$. (Beweis: Übung)

  Beispiel: Es gilt $15 \mid 45$. Deshalb gilt auch $15 \cdot 4 \mid 45 \cdot 4$, also $60 \mid 180$.

  Folgerung: Aus $a \mid b$ und $c \mid d$ folgt $a \cdot c \mid b \cdot d$.

  Beweis: Aus $a \mid b$ folgt nach (T-2) $a \cdot c \mid b \cdot c$. Ebenso folgt aus $c \mid d$ die Gültigkeit von $b \cdot c \mid b \cdot d$. Aus der Transitivität der Teilbarkeitsrelation folgt schließlich $a \cdot c \mid b \cdot d$.

  Aufgabe 2.7: Zeigen Sie für $c \neq 0$: Aus $a \cdot c \mid b \cdot c$ folgt $a \mid b$.

- *Die Teilbarkeitsrelation in Verbindung mit Addition und Subtraktion*

  (T-3) Aus $a \mid b$ und $a \mid c$ folgt $a \mid (b + c)$ und $a \mid (b - c)$.

  Beispiel: Es gilt $6 \mid 78$ und $6 \mid 54$. Deshalb gilt auch $6 \mid 78 + 54$ und $6 \mid 78 - 54$, also $6 \mid 132$ und $6 \mid 24$.

  Beweis: Die Aussage $a \mid b$ bedeutet, es gibt eine ganze Zahl n mit $n \cdot a = b$; $a \mid c$ bedeutet, es gibt eine ganze Zahl k mit $k \cdot a = c$.

  Also gilt: $b + c = n \cdot a + k \cdot a = (n + k) \cdot a = r \cdot a$ (mit $r = n + k$), d.h. $a \mid (b + c)$.

  Folgerung: Aus $a \mid b$ und $a \mid c$ folgt für beliebige ganze Zahlen q und r: $a \mid (q \cdot b + r \cdot c)$.

  Beispiel und *Beweis*: Übung

- *Die Teilbarkeitsrelation und die Durchschnittsbildung*

  (T-4) In der Menge der ganzen Zahlen $\mathbb{Z}$ gilt:
  $T(a) \cap T(b) = T(a - b) \cap T(b)$

  Beispiel: $T(54) = \{1, 2, 3, 6, 9, 18, 27, 54\}$; $T(24) = \{1, 2, 3, 4, 6, 8, 12, 24\}$

  $54 - 24 = 30$; $T(30) = \{1, 2, 3, 5, 6, 10, 15, 30\}$;

  $T(54) \cap T(24) = \{1, 2, 3, 6\}$; $T(30) \cap T(24) = \{1, 2, 3, 6\}$.

  Beweis: (1.) zunächst wird gezeigt: $T(a) \cap T(b) \subseteq T(a - b) \cap T(b)$. Sei also $t \in T(a) \cap T(b)$. Dies bedeutet $t \mid a$ und $t \mid b$. Damit teilt t

aber nach (T-3) auch $a-b$. Somit gilt $t \in T(a-b) \cap T(b)$, wie zu zeigen war.

(2.) Es ist noch zu zeigen: $T(a-b) \cap T(b) \subseteq T(a) \cap T(b)$. Sei also $t \in T(a-b) \cap T(b)$. Dies bedeutet $t \mid a-b$ und $t \mid b$. Damit teilt t auch $(a-b)+b$, also a. Und somit gilt $t \in T(a) \cap T(b)$.

- *Die Teilbarkeitsrelation und Absolutbeträge*

  Der Absolutbetrag $Abs(\mathrm{x})$ oder $|x|$ einer ganzen (oder reellen) Zahl x ist definiert durch:

$$Abs(x) = |x| = \begin{cases} x & \text{falls } x \geq 0 \\ -\mathrm{x} & \text{falls } \mathrm{x} < 0 \end{cases}$$

  Beispiel: $|18| = |-18| = Abs(18) = Abs(-18) = 18$

  (T-5) In $\mathbb{Z}$ gilt: $a \mid b \Leftrightarrow a \mid Abs(b) \Leftrightarrow Abs(a) \mid Abs(b)$

  Beispiel: $-5 \mid 5$, denn $5 = (-1) \cdot (-5)$

  Beweis: Übung

  Aufgabe 2.8: Zeichnen Sie das Schaubild der Funktion *Abs*.

Spezielle Eigenschaften der Teilbarkeitsrelation

Bezogen auf die Grundmenge der **natürlichen Zahlen** $(\mathbb{N})$ gilt:

- *Teilbarkeit und die gewöhnliche „kleiner-gleich"-Relation*

  (T-6) Aus $a \mid b$ folgt $a \leq b$. Dies folgt unmittelbar aus der Definition der Teilbarkeitsrelation.

- *Antisymmetrie der Teilbarkeitsrelation*

  (T-7) Aus $a \mid b$ und $b \mid a$ folgt $a = b$.

  Beweis: $a \mid b$ heißt nach Definition: Es gibt eine natürliche Zahl n mit $n \cdot a = b$. Entsprechend heißt $b \mid a$: Es gibt eine natürliche Zahl k mit $k \cdot b = a$. Daraus folgt: $b = n \cdot a = n \cdot k \cdot b$.

Die einzigen natürlichen Zahlen, welche die letzte Gleichung erfüllen, sind: $n = k = 1$. Also ist $a = b$.

Bemerkung: Diese Argumentation gilt nicht in Bezug auf die Grundmenge der ganzen Zahlen. (Aufgabe: ... warum nicht ?)

In Verbindung mit der oben bewiesenen Transitivität gilt somit: Auf der Menge der natürlichen Zahlen ist die Teilbarkeitsrelation also eine *Ordnungsrelation*.

- Teilbarkeit und *Teilermengen*

  (T-8) Aus $a \mid b$ folgt $T(a) \subseteq T(b)$.

  Beweis: Übung

- *Teilbarkeit und Stellenwert-Schreibweisen*, Endstellen-Regeln, Quersummen-Regeln: Dies wird später (in Kapitel 6) im Zusammenhang mit Stellenwertsystemen und Kongruenzrelationen behandelt.

2.3 Teilerzahl, Teilersumme, Multiplikativität

Die *Teilersumme* $\sigma(a)$ einer natürlichen Zahl a ist, wie der Begriff ausdrückt, gleich der Summe ihrer Teiler: $\sigma(a) = \sum_{x \mid a} x$.

Beispiel: $\sigma(18) = 1 + 2 + 3 + 6 + 9 + 18 = 39$

Die *Teilerzahl* $\tau(a)$ einer natürlichen Zahl a ist gleich der Anzahl ihrer Teiler: $\tau(a) = \sum_{x \mid a} 1$.

Beispiel: $\tau(24) = \sum_{x \mid 24} 1 = 8$ (die Teiler sind: 1, 2, 3, 4, 6, 8, 12, 24)

Ist b ein Teiler von a mit $b \neq a$ (also $b < a$), dann heißt b auch ein *echter Teiler* von a. Gelegentlich ist es günstig, nur die Summe aller echten Teiler zu bilden:

Die Summe der echten Teiler (in der englischsprachigen Fachliteratur: the aliquot parts) von a wird bezeichnet durch $\sigma_0(a) = \sum_{x \mid a \text{ und } x<a} x = \sigma(a) - a$.

Beispiel: $\sigma_0(20) = 1+2+4+5+10 = 22$

Aufgabe 2.9: Zeigen Sie: $\sigma_0(2^n) = 2^n - 1$.

Bemerkung: In der Regel gilt für die Teilersummenfunktion nicht, dass stets $\sigma(a \cdot b) = \sigma(a) \cdot \sigma(b)$ ist.

Beispiel: $a = 6$, $b = 10$, $T(a) = \{1,2,3,6\}$, $T(b) = \{1,2,5,10\}$,
$\sigma(a) = 1+2+3+6 = 12$, $\sigma(b) = 1+2+5+10 = 18$.

Das Produkt $\sigma(a) \cdot \sigma(b) = (1+2+3+6) \cdot (1+2+5+10)$ besteht aus allen Summanden der Form $a_i \cdot b_j$, wo a_i ein Teiler von 6 und b_j ein Teiler von 10 ist. Damit kommen die Produkte $1 \cdot 2$ $(= 2 \cdot 1)$, $2 \cdot 5$ $(= 1 \cdot 10)$, $3 \cdot 2$ $(= 1 \cdot 6)$ und $6 \cdot 5$ $(= 3 \cdot 10)$ mehrfach in $\sigma(a) \cdot \sigma(b)$ vor, während sie in $\sigma(a \cdot b)$ nur jeweils einmal auftreten. Dementsprechend ist $\sigma(6) \cdot \sigma(10) = 12 \cdot 18 = 216$ größer als $\sigma(6 \cdot 10) = \sigma(60) = 168$; genauer:
$\sigma(6 \cdot 10) = 168 = \sigma(6) \cdot \sigma(10) - 2 - 6 - 10 - 30$.

Das soeben beschriebene Phänomen hängt offenbar damit zusammen, dass in den Teilermengen von a und b gleiche Teiler vorkommen, die dann beim distributiven Ausmultiplizieren von

$$\sigma(a) \cdot \sigma(b) = (1+2+3+6) \cdot (1+2+5+10)$$

zu mehrfachen gleichen Summanden führen, während diese in $\sigma(a \cdot b)$ entsprechend der Definition von σ jeweils nur einmal auftreten.

Besitzen a und b jedoch keine gemeinsamen Teiler, so kommt dieses Phänomen der Doppelzählung nicht vor. Die gemeinsamen Teiler von $a \cdot b$ sind dann genau die Produkte der Paare aus dem kartesischen Produkt (vgl. Anhang 8.3) $T(a) \times T(b)$ und es gilt:

Satz 2.2 (Multiplikativität der Teilersummen-Funktion):
Sind a und b teilerfremde natürliche Zahlen, so gilt:
$\sigma(a \cdot b) = \sigma(a) \cdot \sigma(b)$.

Man drückt dies auch folgendermaßen aus (vgl. Kapitel 7): Die Teilersummenfunktion σ ist multiplikativ.

Aufgabe 2.10: Zeigen Sie, dass auch die Teilerzahlfunktion multiplikativ ist, d.h. dass für alle natürlichen Zahlen a und b gilt: $\tau(a \cdot b) = \tau(a) \cdot \tau(b)$.

2.4 Perfekte, abundante, defiziente und befreundete Zahlen

Die Griechen nannten eine natürliche Zahl *vollkommen* (*perfekt*), wenn sie gleich der Summe ihrer echten Teiler war $\sigma_0(a) = a$. Die kleinste perfekte Zahl ist 6, denn 6 = 1+2+3. Weitere niedrige (schon im antiken Griechenland bekannte) vollkommene Zahlen sind 28, 496 und 8128.

Ist $\sigma_0(a) < a$, so nennt man a *defizient* (lateinisch für unzureichend), ist $\sigma_0(a) > a$ so heißt a *abundant* (lateinisch für reichlich).

Beispiele:
10 ist defizient, denn 1+5 < 10 und
12 ist abundant, denn 1+2+3+4+6 > 12.

Aufgabe 2.11:

- Verifizieren Sie durch direktes Ausrechnen der Teilersummen, dass 28, 496 und 8128 perfekte Zahlen sind.
- Finden Sie weitere abundante und defiziente Zahlen.
- Falls entsprechende Programmierkenntnisse vorliegen: Schreiben Sie ein Programm, das ein vorgegebenes Zahlenintervall durchläuft und von jeder Zahl feststellt, ob sie perfekt, abundant oder defizient ist.
- Erweitern Sie das Programm durch einen kleinen Statistik-Modul.

Bemerkung: Es ist derzeit weder bekannt, ob es ungerade vollkommene Zahlen , noch ob es unendlich viele perfekte Zahlen gibt. Man vermutet aber, dass unendlich viele vollkommene Zahlen existieren (siehe Abschnitt 4.8: Spezielle Zahlen und Primzahlen, insbesondere „Mersennesche Primzahlen und vollkommene Zahlen“). Bereits Euklid kannte ein wichtiges Ergebnis über die Struktur vollkommener Zahlen; es wird in Kapitel 4 im Zusammenhang mit den Mersenneschen Primzahlen behandelt.

Definition 2.2: Die *n*-te *Dreieckszahl* ist definiert als $T_n := 1 + 2 + 3 + \ldots + n$.
Das Beispiel T_{100} kennen wir schon von der Geschichte des Grundschülers Gauß.

Aufgabe 2.12: Zeigen Sie, dass allgemein gilt: $T_n = \frac{n \cdot (n+1)}{2}$.

Die Dreieckszahlen lassen sich wie folgt veranschaulichen:

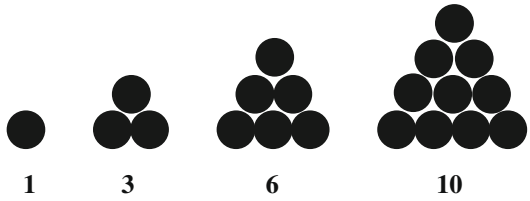


Abb. 2.8: Die ersten vier Dreieckszahlen

Zahlenmuster, besonders in der Form der figurierten Zahlen (Dreieckszahlen, Quadratzahlen, Pentagonalzahlen, Hexagonalzahlen, ...) spielten schon in der griechischen Antike eine große Rolle. Und perfekte Zahlen gaben Anlass für allerlei Zahlenmystik. So spielte die Zahl 6 bereits bei den Pythagoreern eine große Rolle als vollkommene Zahl und als Dreieckszahl.

Ausgehend von der Beobachtung, dass die ersten drei vollkommenen Zahlen auch Dreieckszahlen sind: $6 = 1+2+3 = T_3$, $28 = 1+2+3+4+5+6+7 = T_7$, $496 = 1+2+3+4+\ldots+31 = T_{31}$ lässt sich zeigen, dass jede gerade vollkommene Zahl auch eine Dreieckszahl ist. Im Abschnitt über Mersennesche Zahlen werden wir in Kapitel 4 sehen, dass jede gerade vollkommene Zahl von der Form $2^n \cdot (1+2+4+8+\ldots+2^n)$, also gleich $2^n \cdot (2^{n+1}-1)$ ist.

Aus der Gleichung $2^n \cdot (2^{n+1}-1) = \dfrac{2^{n+1} \cdot (2^{n+1}-1)}{2}$ folgt dann, dass die perfekte Zahl $2^n \cdot (2^{n+1}-1)$ gleich der Dreieckszahl $T_{2^{n+1}-1}$ ist.

Abschließend sei an dieser Stelle noch eine weitere von den Griechen untersuchte Teilbarkeitseigenschaft erwähnt:

Die natürlichen Zahlen a und b heißen *befreundet*, wenn jede der Zahlen gleich der Summe der echten Teiler der jeweils anderen Zahl ist, wenn also $\sigma_0(a) = b$ und $\sigma_0(b) = a$ ist. Das kleinste Paar befreundeter Zahlen besteht aus den Zahlen 220 und 284.

Aufgabe 2.13: Verifizieren Sie, dass 220 und 284 befreundete Zahlen sind und suchen Sie (ggf. unter Nutzung eines Computers) weitere befreundete Zahlen.

3 Euklidischer Algorithmus, größter gemeinsamer Teiler (GGT), kleinstes gemeinsames Vielfaches (KGV)

3.1 Begriffsbeschreibung von GGT und KGV

Die folgende Begriffsbildung bezieht sich auf die Grundmenge $\mathbb{N}$ der natürlichen Zahlen.

Definition 3.1: Es seien a und b natürliche Zahlen mit den Teilermengen $T(a)$ und $T(b)$. Mit $GGT(a,b)$ sei der *größte gemeinsame Teiler* von a und b bezeichnet, also das größte Element der Menge $T(a) \cap T(b)$.

Sind $V(a)$ und $V(b)$ die Vielfachenmengen von a und b, so sei mit $KGV(a,b)$ das kleinste Element von $V(a) \cap V(b)$, also das *kleinste gemeinsame Vielfache* von a und b bezeichnet.

Bemerkung: Die Menge $T(a) \cap T(b)$ ist niemals leer, denn sie enthält in jedem Fall die natürliche Zahl 1. Ist $T(a) \cap T(b) = \{1\}$ (d.h. $GGT(a,b) = 1$), so nennt man die Zahlen a und b *teilerfremd* (oder *relativ prim*).

Aufgabe 3.1: Zeigen Sie, dass auch die Menge $V(a) \cap V(b)$ niemals leer ist.

Beispiele: $GGT(18,24) = 6$; $KGV(18,24) = 72$.

Veranschaulichung im Venn-Diagramm:

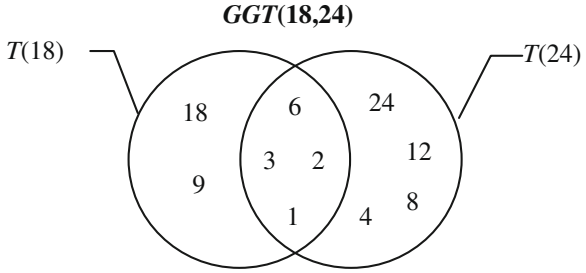


Abb. 3.1: GGT im Venn-Diagramm

J. Ziegenbalg, *Elementare Zahlentheorie*, DOI 10.1007/978-3-658-07171-4_3

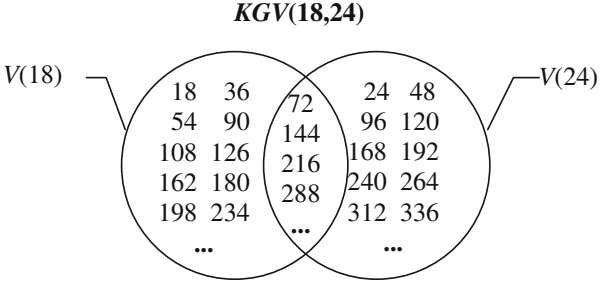


Abb. 3.2: KVG im Venn-Diagramm

Eine Veranschaulichung des GGT im Hasse-Diagramm:
$GGT(864, 972) = 108$

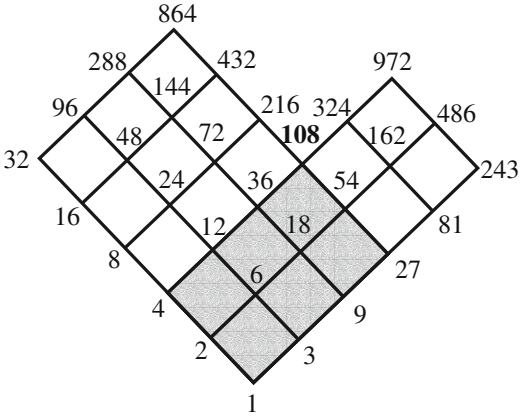


Abb. 3.3: GGT im Hasse-Diagramm

Erste Rechenregeln für den GGT

Satz 3.1 (Eigenschaften des GGT):
Für alle natürlichen Zahlen a und b gilt:

(GGT-1) $GGT(a,b) = GGT(b,a)$

(GGT-2) Ist a ein Teiler von b, so gilt $GGT(a,b) = a$.
Für alle natürlichen Zahlen a gilt $GGT(a,0) = a$.

(GGT-3) Ist $a > b$, so ist $GGT(a,b) = GGT(a-b,b)$.

Beweise:
zu (GGT-1): Dies folgt unmittelbar aus der Definition.
zu (GGT-2): Übung
zu (GGT-3): Nach Kapitel 2, (T-4) gilt $T(a) \cap T(b) = T(a-b) \cap T(b)$.
Dies besagt, dass die Menge der gemeinsamen Teiler von a und b gleich der Menge der gemeinsamen Teiler von $a-b$ und b ist. Damit sind dann aber auch die jeweils größten Elemente, also die größten gemeinsamen Teiler gleich.

Ein *Beispiel* zu (GGT-2):
$a = 52$, $b = 24$. $GGT(52, 24) = 4$, $a - b = 28$, $GGT(28, 24) = 4$.

GGT und der Satz von der Division mit Rest

Erinnerung (Satz von der Division mit Rest): Zu je zwei natürlichen Zahlen a und b ($b \neq 0$) gibt es stets eindeutig bestimmte nichtnegative ganze Zahlen q und r mit der Eigenschaft $a = q \cdot b + r$ und $0 \leq r < b$.

Satz 3.2 (GGT und die Division mit Rest):
(GGT-4) Für alle natürlichen Zahlen a und b gilt:
$GGT(a,b) = GGT(r,b)$,
wobei r der Rest bei der (Ganzzahl-) Division von a durch b ist.

Beweisidee: Iteration von (GGT-3): $a \to a-b,\ a-2b,\ \ldots,\ a - q \cdot b = r$.

Folgerung: $GGT(a,b) = GGT(a,r) = GGT(a, Mod(a,b))$

3.2 Der Euklidische Algorithmus

(*Euklid von Alexandria ca. 365-300 v. Chr.*)

> Nimmt man abwechselnd immer das Kleinere vom Größeren weg, dann muss der Rest schließlich die vorhergehende Größe messen ...
>
> *Euklid*, Die Elemente, Zehntes Buch §3

Vorbemerkung: Der Euklidische Algorithmus ist einer der wichtigsten Algorithmen in der gesamten Mathematik und der Begriff des größten gemeinsamen Teilers spielt eine wichtige Rolle in der Mathematik wie auch im Mathe-

matikunterricht (z.B. in der Bruchrechnung im Zusammenhang mit der Ermittlung des Hauptnenners zweier Brüche, in Verbindung mit dem Kürzen u.s.w.). Es gibt höchst unterschiedliche Verfahren zur Ermittlung des größten gemeinsamen Teilers zweier natürlicher Zahlen a und b:

- Im Schulunterricht wird überwiegend eine Methode praktiziert, die auf der *Primfaktorzerlegung* der Zahlen a und b beruht (vgl. Kapitel 4).
- Historisch, sowie aus Optimalitäts- und innermathematischen Gründen ist der *Euklidische Algorithmus* zur Ermittlung des *GGT* von größter Bedeutung. Er bietet darüber hinaus den Vorteil, dass er sehr anschaulich zu beschreiben ist, dass er im engsten Zusammenhang mit einem grundlegenden Thema des Primarstufenunterrichts steht, nämlich mit dem Verfahren der *Division mit Rest*, dass er intensiv mit anderen wichtigen mathematischen Themen vernetzt ist (Kettenbrüche, Fibonacci-Zahlen, Goldener Schnitt, Restklassenringe, Verschlüsselungsverfahren: Public Key Cryptography, RSA-Verfahren, ...) und dass er in natürlicher Weise zu fundamentalen philosophischen Fragen führt (*Kommensurabilität*).

Die entscheidende Idee des Euklidischen Algorithmus besteht darin, den Satz von der Division mit Rest nach dem Prinzip der *„Wechselwegnahme“* zu iterieren (man vergleiche dazu das Eingangszitat von Euklid) – hilfreich ist auch hierbei wieder die geometrische Deutung der Situation im Sinne der griechischen Mathematik in der Antike (d.h. die Deutung der Zahlen a und b als *Strecken*). Dazu ersetzt man nach der Durchführung der Division mit Rest die ursprünglich größere Strecke a durch die ursprünglich kleinere Strecke b und b durch den Rest r. Mit diesen neuen Zahlen (oder Strecken) a und b führt man wiederum das Verfahren der Division mit Rest durch und erhält ein neues q und ein neues r. Mit diesen Strecken verfährt man wiederum nach dem Prinzip der Wechselwegnahme und nimmt die kleinere so lange von der größeren weg, wie es geht.

Es ist nun an der Zeit, das Verfahren etwas systematischer darzustellen. Mit den Umbenennungen:

$$a_0 := a \quad a_1 := b \quad a_2 := r \quad \text{und} \quad q_1 := q \qquad \text{(* EA-1 *)}$$

geht die Gleichung $a = q \cdot b + r$ über in $a_0 = q_1 \cdot a_1 + a_2$ und die wiederholte Anwendung des Satzes von der Division mit Rest führt zu dem folgenden System von Gleichungen:

$a_0 = q_1 \cdot a_1 + a_2$	$(0 \le a_2 < a_1)$	(Zeile 0)
$a_1 = q_2 \cdot a_2 + a_3$	$(0 \le a_3 < a_2)$	(Zeile 1)
$a_2 = q_3 \cdot a_3 + a_4$	$(0 \le a_4 < a_3)$	(Zeile 2)
…	…	…
$a_{k-1} = q_k \cdot a_k + a_{k+1}$	$(0 \le a_{k+1} < a_k)$	(Zeile k - 1)
$a_k = q_{k+1} \cdot a_{k+1} + a_{k+2}$	$(0 \le a_{k+2} < a_{k+1})$	(Zeile k)
$a_{k+1} = q_{k+2} \cdot a_{k+2} + a_{k+3}$	$(0 \le a_{k+3} < a_{k+2})$	(Zeile k + 1)
…	…	…

Für die Divisionsreste gilt nach dem Satz von der Division mit Rest:

$$b = a_1 > a_2 > a_3 > \ldots > a_{k-1} > a_k > a_{k+1} > \ldots$$

Da alle Divisionsreste nichtnegative ganze Zahlen sind, muss die Kette dieser (streng monoton fallenden) Reste abbrechen; es muss also einen *letzten von Null verschiedenen Divisionsrest* a_n geben. Der nächste auf a_n folgende Divisionsrest ist dann gleich Null: $a_{n+1} = 0$. Die letzten Zeilen des obigen Gleichungssystems lauten also:

	$a_{n-2} = q_{n-1} \cdot a_{n-1} + a_n$	$(0 \le a_n < a_{n-1})$	(Zeile n – 2)
	$a_{n-1} = q_n \cdot a_n + a_{n+1}$	$(a_{n+1} = 0)$	(Zeile n – 1)
d. h.:	$a_{n-1} = q_n \cdot a_n$		

Satz 3.3 (Satz vom Euklidischen Algorithmus):
Der letzte von Null verschiedene Divisionsrest (a_n) im Euklidischen Algorithmus ist der größte gemeinsame Teiler der natürlichen Zahlen a und b: $a_n = GGT(a,b)$.

Beweis: Aus dem Zeilenschema des Euklidischen Algorithmus folgt im Zusammenhang mit (GGT-4) bzw. der anschließenden Folgerung:

$$\begin{aligned} GGT(a,b) &= GGT(a_0,a_1) = GGT(a_1,a_2) = GGT(a_2,a_3) = \ldots \\ &= GGT(a_{n-2},a_{n-1}) = GGT(a_{n-1},a_n) = GGT(a_n,a_{n+1}) \\ &= GGT(a_n,0) = a_n \end{aligned}$$

Der Euklidische Algorithmus eignet sich hervorragend zur Abarbeitung mit einem Computer. Die ursprüngliche Form der Wechselwegnahme bezeichnen

wir als die *Subtraktionsform* des Euklidischen Algorithmus. Wir formulieren zunächst in der Umgangssprache:

```
EuklidSubtraktionsform(a, b)
  Solange a und b beide von Null verschieden sind,
    fuehre folgendes aus:
    Wenn a>=b, so ersetze a durch a-b,
               sonst ersetze b durch b-a.
  Die uebrig bleibende von Null verschiedene ganze Zahl ist
  der gesuchte groesste gemeinsame Teiler GGT(a, b).
```

Im Folgenden sind zwei Formulierungen in der Programmiersprache des Computeralgebra Systems *Maxima* (aus der „open source“-Welt) gegeben; zunächst die Subtraktionsform:

```
EuklidSub(a0, b0):=
  block([a : a0, b : b0],
    while not(a*b = 0) do
      /* solange a und b beide von Null verschieden sind */
      (print(a, " ", b),
       if a > b then a : a-b else b : b-a ),
    return(a+b) )         /* Jetzt ist einer der Summanden
                             gleich Null */
```

Bemerkung: Die zwischen den „Klammern“ /* und */ stehende Texte sind Kommentare ohne Auswirkung auf den Programmablauf. Der Print-Befehl im obigen Programm dient nur dazu, die Zwischenergebnisse auszudrucken. Dies kann aus didaktischen Gründen sinnvoll sein, solange man das Programm zu Lernzwecken diskutiert und laufen lässt. In einer (funktionalen) „Arbeits“-Version des Programms sollte man auf den Print-Befehl verzichten, da mit dem Ausdruck oft die Erzeugung unerwünschter Nebeneffekte verbunden ist.

Ein konkreter Aufruf (mit aktivem Print-Befehl):

```
EuklidSub(136, 60)
136   60
 76   60
 16   60
 16   44
 16   28
 16   12
  4   12
  4    8
  4    4
Ergebnis:  4
```

Die folgende graphische Darstellung dieses Beispiels verdeutlicht noch einmal die obige Argumentation, dass der letzte von Null verschiedene Divisionsrest (hier die Zahl 4) jeden der vorangehenden Divisionsreste und schließlich auch die Ausgangszahlen a und b teilt.

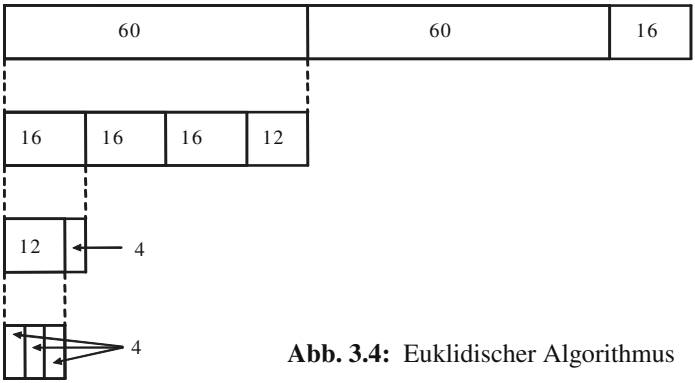


Abb. 3.4: Euklidischer Algorithmus

In der Subtraktionsform des Algorithmus treten u.U. sehr lange Subtraktionsketten auf, bis jeweils ein neuer Divisionsrest entsteht. Dies lässt sich durch die „Divisionsform“ `EuklidDiv`, die dem oben dargestellten Gleichungssystem nachgebildet ist, erheblich beschleunigen.

```
EuklidDiv(a0, b0) :=
  block([a : a0, b : b0],
    while not(a*b = 0) do
      (print(a, " ", b),  /* Print-Befehl ggf. entfernen */
      if a >= b then a : mod(a, b) else b : mod(b, a) ),
    return(a+b) )
```

Ein Aufrufbeispiel (mit aktivem Print-Befehl):

```
EuklidDiv(136, 60)
136   60
 16   60
 16   12
  4   12
Ergebnis:  4
```

Dieses „Laufzeit-Protokoll“ entspricht den Gleichungen:

```
136 = 2 · 60  +  16
 60 = 3 · 16  +  12
 16 = 1 · 12  +   4
 12 = 3 ·  4  +   0
```

Satz 3.4 (Satz von der Vielfachsummendarstellung):

Für jeden der Reste a_k im Zeilenschema des Euklidischen Algorithmus gilt: Es gibt ganze Zahlen x_k und y_k mit der Eigenschaft:

$$a_k = x_k \cdot a + y_k \cdot b .$$

Die Werte von x_k und y_k können dabei wie folgt gewählt werden:

$$x_0 = 1 \qquad y_0 = 0$$
$$x_1 = 0 \qquad y_1 = 1$$

und für $k \geq 2$:

$$x_k = x_{k-2} - q_{k-1} \cdot x_{k-1} \quad \text{bzw.} \quad y_k = y_{k-2} - q_{k-1} \cdot y_{k-1} .$$

Beweis: Der Beweis ergibt sich mit vollständiger Induktion (nach der Zeilenzahl *k*) aus dem Iterationsschema des Euklidischen Algorithmus. (Die vollständige Induktion wird dabei in einer Variante durchgeführt, bei der in der Induktionsannahme von der Gültigkeit der Aussage für die letzten beiden Werte, hier $k-2$ und $k-1$, ausgegangen wird.)

Induktionsverankerung: Die Aussage gilt für $k = 0$ und $k = 1$, denn es gilt

Zeile 0: $a_0 = a$ und mit $x_0 = 1$ und $y_0 = 0$ ist
$$a_0 = x_0 \cdot a + y_0 \cdot b = 1 \cdot a + 0 \cdot b = a .$$

Mit der obigen Definition, siehe (* EA-1 *), folgt weiterhin:

Zeile 1: $a_1 = b$ und $a_1 = x_1 \cdot a + y_1 \cdot b = 0 \cdot a + 1 \cdot b = b .$

Im *Induktionsschritt* ist nun zu zeigen, dass aus der *Induktionsannahme* (d.h. der Gültigkeit der Aussage für die Zeilen $k-2$ und $k-1$) der *Induktionsschluss* (also die Gültigkeit für die Zeile *k*) folgt. Es sei also

$$a_{k-2} = x_{k-2} \cdot a + y_{k-2} \cdot b \text{ und } a_{k-1} = x_{k-1} \cdot a + y_{k-1} \cdot b .$$

Dann ist

$$\begin{aligned} a_k &= a_{k-2} - q_{k-1} \cdot a_{k-1} \\ &= (x_{k-2} \cdot a + y_{k-2} \cdot b) - q_{k-1} \cdot (x_{k-1} \cdot a + y_{k-1} \cdot b) \\ &= (x_{k-2} - q_{k-1} \cdot x_{k-1}) \cdot a + (y_{k-2} - q_{k-1} \cdot y_{k-1}) \cdot b \\ &= x_k \cdot a + y_k \cdot b \end{aligned}$$

Der Satz von der Vielfachsummendarstellung besitzt viele wichtige Anwendungen; meist bezieht man sich dabei jedoch auf die

Folgerung (*Lemma von Bachet*[12] oder auch *Lemma von* Bézout[13])**:** Für alle natürlichen Zahlen a und b gibt es ganze Zahlen x und y mit der Eigenschaft $GGT(a,b) = x \cdot a + y \cdot b$. (* V *)

Beweis: Mit den Bezeichnungen aus dem Euklidischen Algorithmus gilt:

$$GGT(a,b) = a_n = x_n \cdot a + y_n \cdot b = x \cdot a + y \cdot b \quad (\text{mit } x := x_n \text{ und } y := y_n).$$

Bemerkung: Die Bezeichnung „Vielfachsummendarstellung“ ist zwar treffend, aber nicht standardisiert. Die Gleichung (* V *) wird in der Literatur gelegentlich auch als „Linearkombination“ und die ganzzahligen Faktoren x und y werden dementsprechend (nicht falsch, aber ungenau) als „Linearfaktoren“ bezeichnet. Welche Bezeichnung auch immer gewählt wird; es bleibt festzuhalten, dass die Faktoren x und y *nicht eindeutig bestimmt* sind.

Beispiel: Für $a = 136$ und $b = 60$ ergibt sich der folgende Verlauf

Euklidischer Algorithmus	*Vielfachsummendarstellung*
`136 = 2·60 + 16`	`16 = 136 – 2·60`
`60 = 3·16 + 12`	`12 = 60 – 3·16`
	`= 60 – 3·(136 – 2·60)`
	`= (–3)·136 + 7·60`
`16 = 1·12 + 4`	`4 = 16 – 12`
	`= (136 – 2·60)–((–3)·136 + 7·60)`
`12 = 3·4 + 0`	`= 4·136 – 9·60`

Die Darstellung ist jedoch nicht eindeutig; es gilt z.B. auch:

```
4 =  4·136  –   9·60  +  (60·136 – 136·60)
  = 64·136  – 145·60   =  ...
```

Folgerung: Sind die natürlichen Zahlen a und b teilerfremd (d.h. ist $GGT(a,b) = 1$), dann gilt: Es gibt ganze Zahlen x und y mit der Eigenschaft $x \cdot a + y \cdot b = 1$.

Bemerkung: Die Formulierungen $x \cdot a + y \cdot b = 1$ und $b \mid x \cdot a - 1$ sind offensichtlich gleichwertig. In der später einzuführenden Sprache der Kongruenzen (Kapitel 5) drückt man diesen Sachverhalt auch durch die Schreibweise $x \cdot a \equiv 1 \ (mod\ b)$ aus. Man sagt im letzteren Fall auch: x und a sind „invers zueinander modulo b“, bzw. x ist ein Inverses von a modulo b.

---

[12] Claude Gaspar Bachet de Méziriac (1581–1638) französischer Mathematiker
[13] Etienne Bézout (1730–1783) französischer Mathematiker

Für viele Aufgaben (so z.B. im Zusammenhang mit dem Auffinden von inversen Elementen in der Restklassenarithmetik) ist es nicht nur wichtig zu wissen, dass es solche ganze Zahlen x und y gibt, sondern auch konkrete numerische Werte für x und y zu finden. Dies leistet der Berlekamp-Algorithmus, eine naheliegende Verallgemeinerung des Euklidischen Algorithmus, bei der i.w. über die obigen sukzessive gebildeten Vielfachen x_k und y_k „Buch geführt" wird, so dass sie am Ende des Programmlaufs zusammen mit dem größten gemeinsamen Teiler ausgegeben werden können.

Aufgabe 3.2 (für Leser mit entsprechenden Programmierkenntnissen): Formulieren Sie den Berlekamp-Algorithmus und setzen Sie ihn in ein Computerprogramm um.

Hinweis: „Das Lemma von Bachet" in Deutsches Institut für Fernstudien (DIFF), Tübingen), *Computer im Mathematikunterricht*, Heft CM 1, *Algorithmen der elementaren Zahlentheorie*, 30-31.

Wir fahren fort mit der Diskussion grundlegender Eigenschaften des GGT.

(GGT-5) Es gilt $T(a) \cap T(b) = T(GGT(a,b))$.

(*In Worten*: Jeder gemeinsame Teiler von a und b ist ein Teiler des größten gemeinsamen Teilers von a und b und jeder Teiler von $GGT(a, b)$ ist ein gemeinsamer Teiler von a und b.)

Beispiel: $T(18) \cap T(24) = \{1,2,3,6,9,18\} \cap \{1,2,3,4,6,8,12,24\} = \{1,2,3,6\}$

$$= T(6) = T(GGT(18,\ 24))$$

Beweis von GGT-5:

(1.) Zu zeigen: Jeder gemeinsame Teiler t von a und b ist ein Teiler von $GGT(a,b)$.

Aus $t \mid a$ und $t \mid b$ folgt $t \mid a - q \cdot b$, also $t \mid r$, wo q und r die durch die Division mit Rest bestimmten Größe sind. Mit einem entsprechenden Argument folgt, dass t alle im Iterationsverfahren des Euklidischen Algorithmus auftretenden Divisionsreste teilt, insbesondere also den letzen von Null verschiedenen Divisionsrest – und dies ist $GGT(a,b)$.

(2.) Zu zeigen: Jeder Teiler t von $GGT(a,b)$ ist ein gemeinsamer Teiler von a und b.

Dies folgt aber unmittelbar aus der Transitivität der Teilbarkeitsrelation.

Charakterisierung des GGT

In der Mathematik sagt man, eine Eigenschaft *charakterisiert* einen Begriff, wenn die Menge der Elemente, die diese Eigenschaft erfüllen mit derjenigen Menge zusammenfällt, die dem Begriff unterliegen.

(GGT-6) Jeder gemeinsame Teiler von a und b teilt $GGT(a,b)$.

(GGT-7) $GGT(a,b)$ ist durch die Aussage (GGT-6) charakterisiert; d.h., ist t ein gemeinsamer Teiler von a und b, der von jedem gemeinsamen Teiler von a und b geteilt wird, dann gilt: $t = GGT(a, b)$.

Bemerkung: Man kann die Aussage (GGT-7) also folgendermaßen als Beweisstrategie verwenden: Wenn man zeigen will, dass eine natürliche Zahl u der größte gemeinsame Teiler von a und b ist, so zeige man, dass u ein gemeinsamer Teiler von a und b ist, der von jedem gemeinsamen Teiler von a und b geteilt wird.

Beweis: (GGT-6) ist nur noch einmal eine Umformulierung von (GGT-5).

Zu (GGT-7): Sei t ein gemeinsamer Teiler von a und b, der von jedem gemeinsamen Teiler von a und b geteilt wird. Dann wird t insbesondere auch von $GGT(a,b)$ (=: d) geteilt; d.h. $d \mid t$. Andererseits ist (nach Definition) $d \geq t$ und dies ist nur möglich für $d = t$.

Charakterisierung des KGV

(KGV-1) $KGV(a,b)$ teilt jedes gemeinsame Vielfache von a und b.

(KGV-2) $KGV(a,b)$ ist durch die Aussage (KGV-1) charakterisiert; d.h., ist v ein gemeinsames Vielfaches von a und b, das jedes gemeinsame Vielfaches von a und b teilt, dann gilt: $v = KGV(a,b)$.

Beweis: Übung

Weitere Rechenregeln für den GGT

Satz 3.5 (Eigenschaften des GGT):
Für alle natürlichen Zahlen a, b und c (mit $c \neq 0$) gilt:
(GGT-8) $GGT(c \cdot a,\ c \cdot b) = c \cdot GGT(a,b)$

Beispiel: $GGT(126, 168) = 42$

$126 = 7 \cdot 18,\ 168 = 7 \cdot 24,\quad 42 = 7 \cdot 6$

$GGT(7 \cdot 18,\ 7 \cdot 24) = 7 \cdot GGT(18,\ 24)$

Beweis von (GGT-8): Sei $d := GGT(c \cdot a, c \cdot b)$. Da c ein gemeinsamer Teiler von $c \cdot a$ und $c \cdot b$ ist, gilt: $c \mid d$.

Also ist $d_1 := \frac{d}{c}$ eine natürliche Zahl.

Zwischenbehauptung: $d_1 = GGT(a,b)$. (*)

Beweis: 1. Es ist zu zeigen: $d_1 \mid a$ und $d_1 \mid b$.

Nach Definition von d ist $c \cdot a = k \cdot d$ für ein geeignetes k; also gilt $c \cdot a = k \cdot c \cdot d_1$. Durch Kürzen mit c $(c \neq 0)$ folgt sofort $a = k \cdot d_1$, d.h. $d_1 \mid a$.

Ebenso wird gezeigt: $d_1 \mid b$. Also ist d_1 ein gemeinsamer Teiler von a und b.

2. Es bleibt noch zu zeigen: Jeder gemeinsame Teiler von a und b teilt auch d_1.

Sei u ein solcher gemeinsamer Teiler: $u \mid a$ und $u \mid b$. Dann gilt auch: $u \cdot c \mid a \cdot c$ und $u \cdot c \mid b \cdot c$ und somit $u \cdot c \mid d$, denn $d = GGT(c \cdot a, c \cdot b)$.

Daraus folgt $u \mid \frac{d}{c}$ $(= d_1)$.

Damit ist die Zwischenbehauptung bewiesen.

Gleichung (*) besagt nun: $GGT(a,b) = \frac{GGT(c \cdot a,\ c \cdot b)}{c}$ und die Aussage (GGT-8) folgt sofort.

(GGT-9) Aus $c \mid a$ und $c \mid b$ folgt $GGT(\frac{a}{c}, \frac{b}{c}) = \frac{GGT(a,b)}{c}$

Beispiel: $6 \mid 210,\quad 6 \mid 462$

$$GGT(\frac{210}{6}, \frac{462}{6}) = GGT(35,\ 77) = 7 = \frac{42}{6} = \frac{GGT(210,\ 462)}{6}$$

Beweis von (GGT-9): Es sei $a_1 := \frac{a}{c}$ und $b_1 := \frac{b}{c}$; das heißt $a = a_1 \cdot c$ und $b = b_1 \cdot c$. Nach (GGT-8) folgt dann: $GGT(a_1 \cdot c,\ b_1 \cdot c) = c \cdot GGT(a_1, b_1)$,

also $GGT(\frac{a}{c},\frac{b}{c}) = \frac{GGT(a,b)}{c}$.

(GGT-10) Ist $d = GGT(a,b)$, so ist $GGT(\frac{a}{d},\frac{b}{d}) = 1$;

(mit anderen Worten: $GGT(\frac{a}{GGT(a,b)},\frac{b}{GGT(a,b)}) = 1$).

Beweis von (GGT-10): Wendet man (GGT-9) speziell auf den gemeinsamen Teiler $d := GGT(a,b)$ an, so folgt unmittelbar:

$GGT(\frac{a}{d},\frac{b}{d}) = \frac{GGT(a,b)}{d} = \frac{d}{d} = 1$.

Fibonacci-Zahlen

In seinem *Liber Abaci* formulierte Leonardo von Pisa (Fibonacci) im Jahre 1202 das inzwischen als „Kaninchenaufgabe“ berühmt gewordene Problem:

> *Ein Mann hielt ein Paar Kaninchen an einem Ort, der ringsum von einer Mauer umgeben war, um herauszufinden, wie viele Paare daraus in einem Jahr entstünden. Dabei ist es ihre Natur, jeden Monat ein neues Paar auf die Welt zu bringen, und sie gebären erstmals im zweiten Monat nach ihrer Geburt. ...*

Die Mathematisierung dieser Aufgabe führt zu einer der bekanntesten Zahlenfolgen, der Folge der Fibonacci-Zahlen. Sie beginnt folgendermaßen: 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, 233, 377, 610, 987, 1597, 2584, 4181

Die charakteristische Eigenschaft der Fibonacci-Zahlen ist, dass (ab der dritten) jede Zahl die Summe ihrer beiden Vorgänger ist. Die Fibonacci-Zahlen sind eine der am besten untersuchten Folgen überhaupt (es gibt ganze Bücher über die Fibonacci-Zahlen; siehe z.B. Posamentier 2007).

Aufgabe 3.3: Berechnen Sie die Fibonacci-Zahlen mit Hilfe geeigneter Computersoftware

- rekursiv
- iterativ
- mit Hilfe einer Tabellenkalkulationsprogrammes

Führen Sie Laufzeittests durch.

Aufgabe 3.4: Zeigen Sie: Je zwei aufeinanderfolgende Fibonacci-Zahlen sind teilerfremd.

3.3 Exkurs: Paradigmatisches[14] Beweisen und Visualisierung

Eine wichtige *Veranschaulichung* des größten gemeinsamen Teilers der natürlichen Zahlen a und b besteht darin, dass man ihn als die Seitenlänge des größten Quadrats deutet, mit dem ein Rechteck mit den Seitenlängen a und b lückenlos „gepflastert“ werden kann.

Beispiel: $a = 8$, $b = 6$, $d := GGT(a, b) = 2$

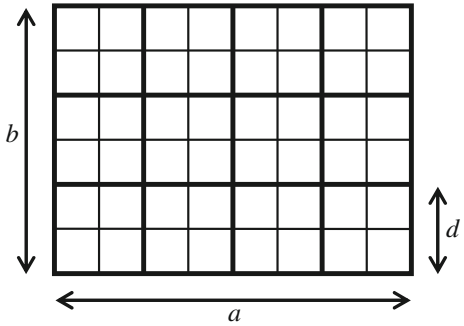


Abb. 3.5: Pflasterung mit GGT-Quadraten

Entsprechend ist das kleinste gemeinsame Vielfache von a und b die Seitenlänge des kleinsten Quadrats, das mit Rechtecken der Seitenlängen a und b lückenlos (wie in der folgenden Abbildung) gepflastert werden kann:

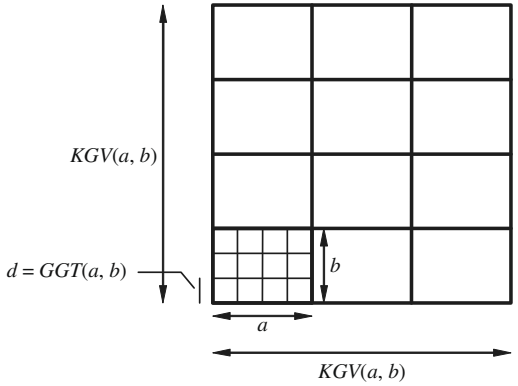


Abb. 3.6: Pflasterung des KGV mit GGT-Quadraten

[14] *Paradigma* (griechisch): Beispiel, Muster
paradigmatisch: von modellhaftem Charakter

Wir wollen diese Veranschaulichung nutzen, um eine paradigmatische Begründung für den folgenden Satz zu geben.

Satz 3.6 (Produkt aus GGT und KGV): $a \cdot b = GGT(a,b) \cdot KGV(a,b)$

Dazu betrachten wir im Rechteck in Abb. 3.5 die folgenden Größen:

- Anzahl der „fett umrahmten" Spalten: $\frac{8}{2}$ $(=4)$; allgemein: $s = \frac{a}{d}$
- Anzahl der „fett umrahmten" Zeilen: $\frac{6}{2}$ $(=3)$; allgemein: $z = \frac{b}{d}$

Daraus folgt

- Anzahl der „fett umrahmten" Quadrate $4 \cdot 3$ $(=12)$; allgemein: $\frac{a}{d} \cdot \frac{b}{d}$.

Wir bezeichnen diese Anzahl mit A: $A := \frac{a}{d} \cdot \frac{b}{d}$.

Die Größe $A \cdot d$ $(= a \cdot \frac{b}{d} = \frac{a}{d} \cdot b)$ ist dann ein gemeinsames Vielfaches von a und b.

Abbildung 3.6 macht deutlich, dass das Quadrat mit der Seitenlänge $V := KGV(a, b)$ mit Quadraten der Seitenlänge d gepflastert werden kann.

Es gilt:

- im Beispiel: $V = d \cdot s \cdot z = d \cdot z \cdot s$
  $V \cdot V = 24 \cdot 24 = (2 \cdot \frac{8}{2} \cdot \frac{6}{2}) \cdot (2 \cdot \frac{6}{2} \cdot \frac{8}{2})$
- allgemein: $V \cdot V = (d \cdot \frac{a}{d} \cdot \frac{b}{d}) \cdot (d \cdot \frac{b}{d} \cdot \frac{a}{d}) = \frac{a \cdot b}{d} \cdot \frac{a \cdot b}{d}$.

Mit $A \cdot d = \frac{a \cdot b}{d}$ folgt $V^2 = (A \cdot d)^2$, und da alle Zahlen positiv sind, gilt: $V = A \cdot d$.

$A \cdot d$ ist also das kleinste gemeinsame Vielfache von a und b und daraus folgt:

$$GGT(a,b) \cdot KGV(a,b) = d \cdot V = d \cdot A \cdot d = d \cdot \frac{a \cdot b}{d} = a \cdot b .$$

Aufgabe 3.5:

- Informieren Sie sich über den Begriff des paradigmatischen Beweisens (ein Literaturhinweis: A. Kirsch, 1979).
- Geben Sie einen geometrisch-anschaulichen Beweis für die vom jungen Gauß entdeckte Formel (* G *) – siehe Kapitel1.
  (*Hinweis*: Treppendarstellung).

Die Methode der Visualisierung ist sowohl für das Erlernen von Mathematik, wie auch für das mathematische Problemlösen grundsätzlich sehr hilfreich. Ein Thema, wo dies besonders deutlich wird, ist der

Satz 3.7 (Satz von Sylvester[15]):
Die natürliche Zahl a ($a > 1$) besitzt genau dann einen ungeraden Teiler, wenn sie sich als Summe aufeinanderfolgender natürlicher Zahlen schreiben lässt.

Beispiele: $a = 30 = 4+5+6+7+8 = 5 \bullet 6$ bzw. $a = 14 = 2+3+4+5 = 2 \bullet 7$

Aufgabe 3.6: Beweisen Sie den Satz von Sylvester.

Hinweise: Überführung der Rechtecksdarstellung in die Treppendarstellung und umgekehrt anhand einer geeigneten „Mittenzahl".

Fallunterscheidungen:

1. Die Anzahl der Summanden ist ungerade: Dann gibt es eine „Mittenzahl". Idee: Verteilung der Nachbarsummanden nach dem Prinzip: links eins mehr, rechts eins weniger, u.s.w.

2. Die Anzahl der Summanden ist gerade. Dann gibt es keine Mittenzahl, aber eine Mitten-Senkrechte. Verteilung der Nachbarsummanden nach dem Prinzip: links 1/2 mehr, rechts 1/2 weniger, u.s.w.

[15] James Joseph Sylvester (1814–1897), englischer Mathematiker

4 Primzahlen

2 is the oddest of all primes.

Zugeschrieben: Philip Hall, englischer Mathematiker (Gruppentheorie) des 20. Jahrhunderts

4.1 Der Begriff der Primzahl

Die Primzahlen sind einer der ältesten und interessantesten Untersuchungsgegenstände der Mathematik. Sie stellen die Bausteine dar, aus denen die natürlichen Zahlen aufgebaut sind. Der *Fundamentalsatz der Zahlentheorie* besagt, dass sich jede natürliche Zahl multiplikativ aus Primzahlen zusammensetzt, wobei diese Darstellung bis auf die Reihenfolge eindeutig ist (vgl. Satz 4.3). Die Primzahlen sind also, multiplikativ gesehen, die Atome, aus denen sich die natürlichen Zahlen zusammensetzen.

Auch für andere Zahlensysteme oder algebraische Systeme sind Primzahlen, Primelemente oder dem Primzahlbegriff nachgebildete Begriffe (wie z.B. Irreduzibilität) von zentraler Bedeutung. Eine faszinierende Eigenschaft der Primzahlen ist die Unregelmäßigkeit, mit der sie in der Zahlenreihe auftreten. Gesetzmäßigkeiten in der Primzahlreihe zu entdecken, war schon immer eine wichtige Forschungsrichtung in der Mathematik.

Ausgangspunkt: Es gibt natürliche Zahlen, die sehr wenige Teiler besitzen; nämlich nur die „trivialen“ Teiler (1 und die Zahl selbst). Solche Zahlen nennt man Primzahlen, wenn sie von 1 verschieden sind. (Es gibt gute Gründe, die Zahl 1 nicht zu den Primzahlen zu rechnen. Einer dieser Gründe wäre, dass bei Einbezug der 1 der Hauptsatz der Zahlentheorie nicht gelten würde.)

Definition 4.1: Eine natürliche Zahl a $(a > 1)$ heißt *Primzahl*, wenn sie (in der Menge der natürlichen Zahlen) nur die beiden (trivialen) Teiler 1 und a besitzt.

Eine natürliche Zahl *a*, die sich schreiben lässt als $a = x \cdot y$ (mit nichttrivialen ganzzahligen Faktoren x und y) heißt *zerlegbar* oder *zusammengesetzt*. Jede natürliche Zahl a $(a > 1)$ ist entweder eine Primzahl oder sie ist zerlegbar. In der Menge der natürlichen Zahlen fallen also die Begriffe *Primzahl* und *unzerlegbare* (*irreduzible*) *Zahl* zusammen.

Die folgende Tabelle enthält alle (168) Primzahlen zwischen 0 und 1000:

J. Ziegenbalg, *Elementare Zahlentheorie*, DOI 10.1007/978-3-658-07171-4_4

```
  2,   3,   5,   7,  11,  13,  17,  19,  23,  29,  31,  37,
 41,  43,  47,  53,  59,  61,  67,  71,  73,  79,  83,  89,
 97, 101, 103, 107, 109, 113, 127, 131, 137, 139, 149, 151,
157, 163, 167, 173, 179, 181, 191, 193, 197, 199, 211, 223,
227, 229, 233, 239, 241, 251, 257, 263, 269, 271, 277, 281,
283, 293, 307, 311, 313, 317, 331, 337, 347, 349, 353, 359,
367, 373, 379, 383, 389, 397, 401, 409, 419, 421, 431, 433,
439, 443, 449, 457, 461, 463, 467, 479, 487, 491, 499, 503,
509, 521, 523, 541, 547, 557, 563, 569, 571, 577, 587, 593,
599, 601, 607, 613, 617, 619, 631, 641, 643, 647, 653, 659,
661, 673, 677, 683, 691, 701, 709, 719, 727, 733, 739, 743,
751, 757, 761, 769, 773, 787, 797, 809, 811, 821, 823, 827,
829, 839, 853, 857, 859, 863, 877, 881, 883, 887, 907, 911,
919, 929, 937, 941, 947, 953, 967, 971, 977, 983, 991, 997
```

Die größte im Jahr 2013 bekannte Primzahl war die „Mersennesche“ Primzahl $M_{57885161} = 2^{57885161} - 1$ (die *Mersenneschen Zahlen* werden in Abschnitt 4.8 behandelt). Im Dezimalsystem geschrieben, benötigt sie 17.425.170 Stellen. Geht man davon aus, dass etwa 3000 Ziffern auf eine DIN A4 Seite passen, so benötigte man etwa 5.800 Seiten, um diese Zahl dezimal aufzuschreiben.

Bemerkung zum Auftreten von Primzahlen in Teilermengen: Für jede natürliche Zahl a $(a > 1)$ ist der kleinste von 1 verschiedene Teiler von a stets eine Primzahl. (*Beweis*: Übung)

4.2 Die Unendlichkeit der Primzahlmenge

Die folgende wortgetreue Wiedergabe von Euklids Formulierung (*Euklid von Alexandria*: ca. 365–300 v. Chr.) beruht auf Heibergs Text, aus dem Griechischen übersetzt und herausgegeben von Clemens Thaer (Ostwald‘s Klassiker 1973).

Satz 4.1 (Satz von Euklid): *Die Elemente, Neuntes Buch,* §20:
Es gibt mehr Primzahlen als jede vorgelegte Anzahl von Primzahlen.

Beweis: Die vorgelegten Primzahlen seien a, b, c. Ich behaupte, dass es mehr Primzahlen gibt als a, b, c.

Man bilde die kleinste von a, b, c gemessene Zahl; sie sei DE, und man füge zu DE die Einheit DF hinzu. Entweder ist EF dann eine Primzahl, oder nicht. Zunächst sei es eine Primzahl. Dann hat man mehr Primzahlen als a, b, c gefunden, nämlich a, b, c, EF.

Zweitens sei EF keine Primzahl. Dann muss es von irgendeiner Primzahl gemessen werden; es werde von der Primzahl g gemessen. Ich behaupte, dass g mit keiner der Primzahlen a, b, c zusammenfällt. Wenn möglich, tue es dies nämlich. a, b, c messen nun DE; auch g müsste dann DE messen. Es misst aber auch EF. g müsste also auch den Rest, die Einheit DF messen, während es eine Zahl ist; dies wäre Unsinn. Also fällt g mit keiner der Zahlen a, b, c zusammen; und es ist Primzahl nach Voraussetzung. Man hat also mehr Primzahlen als die vorgelegte Anzahl a, b, c gefunden, nämlich a, b, c, g – q.e.d.

Einige Bemerkungen zum Satz von Euklid und seinem Beweis:

1. Dem Euklidischen Bewies liegt die für die Griechen typische Methode der Deutung von *Zahlen* durch *Strecken* zugrunde:

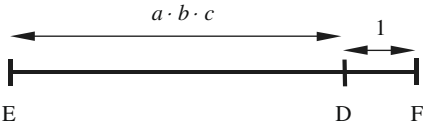


Abb. 4.1: zu Euklids Beweis für den Satz, dass es unendlich viele Primzahlen gibt

2. Streng genommen, beweist der Beweis nicht das, was der Satz aussagt. Denn Euklid spricht im Satz von *jeder* vorgelegten Menge von Primzahlen; er führt den Beweis aber nur anhand einer dreielementigen Menge von Primzahlen aus. Nach den heute in der Mathematik üblichen Gepflogenheiten müsste der Beweis etwa folgendermaßen beginnen:

   Sei $M := \{p_1, \ldots, p_n\}$ *eine beliebige Menge endlich vieler Primzahlen. ...*

   Obwohl der Euklidische Beweis also nicht die Behauptung in voller Allgemeinheit aufgreift, enthält er doch aber alles Wesentliche. Es ist unmittel-

bar klar, dass sich die gegebene Begründung sofort auch auf vorgegebene Mengen von 4, 5, oder einer anderen, beliebigen endlichen Anzahl von Primzahlen übertragen ließe. Der an einem (typischen) Beispiel gegebene Beweis ist ohne weiteres auf jedes beliebige andere Beispiel übertragbar. Beweise bzw. Begründungen oder Argumentationen dieser Art bezeichnet man auch als paradigmatisch.

3. Der Satz des von Euklid und sein Beweis in „moderner" Formulierung:

   Satz: Es gibt unendlich viele Primzahlen.

   Beweis: Wir zeigen, dass zu jeder beliebigen vorgegebenen endlichen Menge von Primzahlen, etwa zur Menge der Primzahlen $\{p_1,\ldots,p_n\}$, eine neue Primzahl konstruiert werden kann, die nicht in dieser Menge enthalten ist. (Damit ist klar, dass die Menge der Primzahlen nicht endlich sein kann, dass sie also *unendlich* ist; d.h., dass sie unendlich viele Elemente enthält). Sei v ein gemeinsames Vielfaches (z.B. das Produkt) dieser vorgegebenen Primzahlen: $v = p_1 \cdot \ldots \cdot p_n$. Man betrachte die Zahl $v+1 = p_1 \cdot \ldots \cdot p_n + 1$. Sie besitzt, wie jede natürliche Zahl (größer als 1), einen kleinsten Primteiler q (dies schließt als Möglichkeit auch den Fall ein, dass $v+1$ selbst eine Primzahl, dass also $v+1 = q$ ist). Die Primzahl q ist von jeder der Primzahlen $p_1,\ldots,p_n$ verschieden, denn die Zahl $v+1$ ist zwar durch q, aber durch keine der Primzahlen $p_1,\ldots,p_n$ teilbar (sie lässt bei der Division durch jede dieser Primzahlen ja offensichtlich den Rest 1). Also haben wir mit q eine neue Primzahl gefunden, die noch nicht unter den ursprünglich gegebenen Primzahlen $p_1,\ldots,p_n$ vorkam.

4. Der Unterschied in der ursprünglichen und modernen Formulierung des Satzes von Euklid ist nicht nur stilistischer Natur – in diesen Formulierungen kommen grundlegende Unterschiede philosophischer Natur zum Ausdruck. Sie betreffen die Frage: *Von welcher Art ist das Unendliche?* Euklid beschreibt mit der Menge der Primzahlen eine unendliche Menge, ohne den Begriff „unendlich" überhaupt zu erwähnen. Die Menge der Primzahlen ist in Euklids Formulierung in dem Sinne unendlich, dass jede vorgegebene endliche Menge von Primzahlen durch neue Primzahlen erweiterbar ist; dass also keine endliche Menge von Primzahlen die Gesamtheit aller Primzahlen erschöpfend umfasst.

Die Unendlichkeit der Primzahlmenge besteht bei Euklid in der Möglichkeit, jede endliche Menge von Primzahlen zu erweitern. Man bezeichnet heute diese Auffassung vom Unendlichen als die des *potentiell*[16] Unendlichen.

Im Gegensatz dazu liegt der Formulierung *„Es gibt unendlich viele Primzahlen“* – oder noch deutlicher der Fassung *„Die Menge der Primzahlen ist unendlich“* die Vorstellung zugrunde, dass es sich bei dieser Menge um etwas Abgeschlossenes handelt; die Menge aller Primzahlen ist in diesem Sinne wie ein (sehr) großer Sack, der alle Primzahlen (und nichts weiter) enthält. Dies sei auch unbeschadet der Tatsache richtig, dass der menschliche Geist diese unendliche Gesamtheit nie auf einmal völlig erfassen kann. Die Idee der *Menge aller Primzahlen* ist eine der Ideen in Platons „Ideenhimmel“, von der wir Menschen immer nur einen Schatten erhaschen können. Wenn man von dieser Vorstellung über die Unendlichkeit ausgeht, dann ist die Menge aller Primzahlen etwas Fertiges, Abgeschlossenes, Aktuales. Man bezeichnet diese Auffassung vom Unendlichen heute als die des *aktual*[17] Unendlichen.

Aufgabe 4.1:

Dem kleinen Fritz kommt die Formulierung

... Man betrachte die Zahl $v+1 = p_1 \cdot \ldots \cdot p_n + 1$ *Sie besitzt, wie jede natürliche Zahl* (*größer als* 1)*, einen kleinsten Primteiler* q *...*

im Beweis des Satzes von Euklid etwas umständlich vor. Nach der Betrachtung einiger Beispiele kommt er zu dem Schluss, dass man nach dem folgenden Schema stets sofort eine neue Primzahl bekommt. Er beginnt mit den Primzahlen 2 und 3 und rechnet:

2•3 + 1 = 7	(Primzahl)
2•3•5 + 1 = 31	(Primzahl)
2•3•5•7 + 1 = 211	(Primzahl)
2•3•5•7•11 + 1 = 2311	(Primzahl)
...	

Überprüfen Sie die Argumentation des kleinen Fritz.

---

[16] *potentiell* (lateinisch): möglich, denkbar

[17] *aktual* (lateinisch): tatsächlich vorhanden; im Gegensatz zu: potentiell

Aufgabe 4.2: Es sei n zusammengesetzte Zahl. Dann hat n einen Primteiler p mit der Eigenschaft $p \le \sqrt{n}$.

4.3 Die Suche nach Primzahlen: Das Sieb des Eratosthenes

Schon im Altertum war man bestrebt, einen möglichst guten Überblick über die Primzahlen zu gewinnen. Euklid zeigte, dass es unendlich viele Primzahlen gibt. Der griechische Mathematiker *Eratosthenes von Kyrene* (ca. 276-194 v. Chr.) gab das folgende Verfahren an, um alle Primzahlen bis zu einer bestimmten vorgegebenen Zahl n zu bestimmen. Es sei hier am Beispiel $n = 20$ erläutert.

1. Schreibe alle Zahlen von 1 bis 20 auf:
   1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20
2. Streiche die Zahl 1 (sie wird aus guten Gründen nicht zu den Primzahlen gerechnet):
   ~~1~~ 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20
3. Unterstreiche die Zahl 2:
   ~~1~~ 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20
4. Streiche alle echten Vielfachen von 2; also die Zahlen 4, 6, 8, 10, 12, 14, 16, 18 und 20:
   ~~1~~ 2 3 ~~4~~ 5 ~~6~~ 7 ~~8~~ 9 ~~10~~ 11 ~~12~~ 13 ~~14~~ 15 ~~16~~ 17 ~~18~~ 19 ~~20~~
5. Unterstreiche die erste „freie“ (d.h. noch nicht unterstrichene oder gestrichene) Zahl; in diesem Fall also die Zahl 3:
   ~~1~~ 2 3 ~~4~~ 5 ~~6~~ 7 ~~8~~ 9 ~~10~~ 11 ~~12~~ 13 ~~14~~ 15 ~~16~~ 17 ~~18~~ 19 ~~20~~
6. Streiche aus den verbleibenden Zahlen alle echten Vielfachen von 3; also die Zahlen 9 und 15:
   ~~1~~ 2 3 ~~4~~ 5 ~~6~~ 7 ~~8~~ ~~9~~ ~~10~~ 11 ~~12~~ 13 ~~14~~ ~~15~~ ~~16~~ 17 ~~18~~ 19 ~~20~~
7. Unterstreiche die kleinste freie Zahl; in diesem Fall also die Zahl 5:
   ~~1~~ 2 3 ~~4~~ 5 ~~6~~ 7 ~~8~~ ~~9~~ ~~10~~ 11 ~~12~~ 13 ~~14~~ ~~15~~ ~~16~~ 17 ~~18~~ 19 ~~20~~
8. Streiche aus den verbleibenden Zahlen alle echten Vielfachen der Zahl 5. Da die in Frage kommenden Zahlen 10, 15 und 20 bereits gestrichen sind, tritt in diesem Fall (Obergrenze = 20) keine Veränderung auf.
9. Setze das Verfahren so lange fort, bis jede der Zahlen entweder unterstrichen oder gestrichen ist.
   ~~1~~ 2 3 ~~4~~ 5 ~~6~~ 7 ~~8~~ ~~9~~ ~~10~~ 11 ~~12~~ 13 ~~14~~ ~~15~~ ~~16~~ 17 ~~18~~ 19 ~~20~~
10. Ende des Verfahrens. Die unterstrichenen Zahlen sind die Primzahlen zwischen 1 und 20.

Durch dieses Verfahren werden, wenn man so will, also genau die Primzahlen „ausgesiebt“. Man nennt das Verfahren deshalb auch das *Sieb des Eratosthenes* bzw. kurz das *Siebverfahren*.

Aufgabe 4.3:

1. Führen Sie das Siebverfahren von Hand für die natürlichen Zahlen von 1 bis 200 durch.
2. Geben Sie eine allgemeine Beschreibung des Siebverfahrens, die von der Zahl 20 unabhängig ist; die Obergrenze sei allgemein mit g bezeichnet.
3. Zeigen Sie: Ist die Zahl a zerlegbar, z.B. $a = x \cdot y$ (mit von 1 verschiedenen Faktoren x und y), so ist einer der Faktoren kleiner oder gleich $\sqrt{a}$.

4. Aufgabenteil 3. hat zur Folge, dass das Siebverfahren *erheblich* verkürzt werden kann, denn man ist mit dem Streichen der Vielfachen schon fertig, wenn die Zahl $\sqrt{g}$ erreicht und verarbeitet ist. Formulieren Sie den Algorithmus so, dass diese Verbesserung der „Laufzeiteffizienz“ realisiert wird.

Eine „dynamische“ Version des Siebverfahrens ist im Internet zu finden unter der Adresse:

http://www.ziegenbalg.ph-karlsruhe.de/materialien-homepage-jzbg/Sieb-des-Eratosthenes/Sieb-des-Eratosthenes-Simulation.htm

Bemerkung: Gelegentlich kann man lesen, dass das Sieb des Eratosthenes dazu dient, *die* Primzahlen (d.h. *alle* Primzahlen) zu ermitteln. Ein Blick auf den Algorithmus genügt aber, um festzustellen, dass er nur dann funktionieren kann, wenn man sich von vorn herein auf einen *endlichen* Zahlenabschnitt beschränkt (im Beispiel: die natürlichen Zahlen von 1 bis 20). Das Sieb des Eratosthenes liefert also stets nur die Primzahlen bis zu einer bestimmten, von vorn herein festzulegenden oberen Grenze. Diese Grenze lässt sich jedoch durch mehrere „Läufe“ des Verfahrens immer weiter nach oben verschieben. Die (unendliche) Menge der Primzahlen wird durch das Sieb des Eratosthenes also als potentiell unendliche Menge erschlossen. Es sei an dieser Stelle nochmals an die weise Formulierung von Euklid erinnert: *Es gibt mehr Primzahlen als jede vorgelegte Anzahl von Primzahlen*.

Aufgabe 4.4 (für Leser mit entsprechenden Programmierkenntnissen):

1. Man kann die Idee von der Menge der Primzahlen als potentiell unendlicher Menge dadurch operationalisieren, dass man die Obergrenze im Sieb des Eratosthenes immer weiter nach oben verschiebt.

   Setzen Sie diese Idee in ein Computer-Programm um. Versuchen Sie dabei, bei der Erhöhung der Obergrenze so vorzugehen, dass die in vorangegangenen Läufen erzielten Ergebnisse nach Möglichkeit übernommen werden (dass sie also nicht vor jedem neuen Lauf „weggeworfen“ werden). Da dies stark von den Möglichkeiten der verwendeten Programmiersprache abhängt, soll an dieser Stelle nicht näher darauf eingegangen werden.

   Damit das Programm überhaupt einmal stoppt, muss an strategisch geeigneter Stelle eine Abfrage („Ende des Verfahrens?: Ja/Nein“) eingebaut werden.

2. Beginnend mit der Primzahl 2 führt das in Euklids Beweis beschriebene Verfahren zu einer eindeutig bestimmten Folge von Primzahlen, wenn man als neue Primzahl immer den *kleinsten* Teiler des um 1 vergrößerten Produkts aller in der jeweiligen Stufe bekannten Primzahlen nimmt.

   Diese Folge wird auch als Euclid-Mullin-Folge bezeichnet. Sie hat die Nr. A000945 in Sloanes On-Line Encyclopedia of Integer Sequences (OEIS, vgl. https://oeis.org/). Die Folge hat das Anfangsstück: 2, 3, 7, 43, 13, 53, 5, 6221671, 38709183810571, 139, 2801, 11, 17, ...

   Schreiben Sie ein Programm zur sukzessiven Berechnung der Glieder der Euclid-Mullin Folge.

4.4 Primeigenschaft und Unzerlegbarkeit

Ein **Fundamental-Lemma**[18] **über Primzahlen**[19]: Teilt eine Primzahl p ein Produkt $a \cdot b$ von zwei natürlichen Zahlen a und b, so teilt p (mindestens) einen der Faktoren.

[18] *Lemma* (griechisch): Hilfssatz (Manches Lemma startet seine Existenz relativ bescheiden – eben als „Hilfs“-Satz. Gelegentlich kommt es aber vor, dass die Bedeutung des zunächst unscheinbaren Lemmas stark zunimmt, und so ist manches Lemma, wie z.B. das vorliegende Fundamental-Lemma oder das Lemma von Sperner oder das Lemma von Zorn, berühmter als mancher Satz.)

Beweis: Wir zeigen: Wenn p einen der Faktoren (z.B. den Faktor b) nicht teilt, so teilt es den anderen Faktor (in diesem Fall also den Faktor a).
Die Primzahl p sei also kein Teiler von b. Dann sind p und b teilerfremd und nach dem Lemma von Bachet gibt es ganze Zahlen x und y mit der Eigenschaft $1 = x \cdot p + y \cdot b$. Daraus folgt $a = a \cdot x \cdot p + y \cdot a \cdot b$. Da p nach Voraussetzung die rechte Seite dieser Gleichung teilt, muss es auch die linke Seite, also a, teilen.

Folgerung: Teilt eine Primzahl p ein Produkt $a_1 \cdot \ldots \cdot a_n$ aus n natürlichen Zahlen $a_1, \ldots, a_n$, so teilt p (mindestens) einen der Faktoren.

Beweis: Übung (Hinweis: vollständige Induktion)

Satz 4.2 (Primzahlkriterium):
Für die natürliche Zahl p $(p > 1)$ sind die beiden folgenden Aussagen gleichwertig:

(P1) p ist eine Primzahl.

(P2) Für alle natürlichen Zahlen a und b gilt:
Aus $p \mid a \cdot b$ folgt $p \mid a$ oder $p \mid b$.

Beweis: Die Teilaussage „aus (P1) folgt (P2)“ ist gerade die Aussage des Fundamentallemmas.

Beweis der Teilaussage „aus (P2) folgt (P1)“: Es ist zu zeigen: Jede natürliche Zahl p mit der Eigenschaft (P2) ist eine Primzahl. Sei d $(d \in \mathbb{N})$ ein Teiler von p. Dann ist also $p = d \cdot n$ für eine natürliche Zahl n; insbesondere gilt dann $p \mid d \cdot n$. Nach Voraussetzung (P2) folgt daraus $p \mid d$ oder $p \mid n$.

1. *Fall*: Es gelte $p \mid d$. Mit $d \mid p$ (wegen $p = d \cdot n$) folgt daraus $d = p$.

2. *Fall*: Es gelte $p \mid n$. Wegen $n \mid p$ $(p = d \cdot n)$ folgt daraus $p = n$ und $d = 1$.

Das heißt: Jeder Teiler d von p ist ein „trivialer“ Teiler und p ist eine Primzahl.

---

[19] Das Fundamental-Lemma wird auch als „Lemma von Euklid“ bezeichnet. Euklid formuliert in den Elementen, Siebentes Buch, §30: „*Wenn zwei Zahlen, indem sie einander vervielfältigen, irgendeine Zahl bilden und irgendeine Primzahl dabei das Produkt misst, dann muss diese auch eine der ursprünglichen Zahlen messen*“.

Primeigenschaft und Unzerlegbarkeit – ein Exkurs zur Begriffsbildung

Die im obigen Fundamentallemma beschriebene Eigenschaft zeichnet die „Rechenbereiche“ der natürlichen und ganzen Zahlen aus. Es gibt andere für die Mathematik bedeutsame Rechenbereiche, wo die entsprechende Aussage nicht gilt.

So gilt z.B. im Rechenbereich $\mathbb{Z}[\sqrt{-5}] := \{a + b \cdot \sqrt{-5} : a, b \in \mathbb{Z}\}$, in dem man ähnlich „rechnen“ kann wie im Bereiche der ganzen Zahlen (siehe untenstehende Bemerkung), für die dort ebenfalls unzerlegbaren Zahlen 2 und 3:

$$2 \cdot 3 = 6 = (1 + \sqrt{-5}) \cdot (1 - \sqrt{-5}).$$

Das heißt also: $2 \mid (1 + \sqrt{-5}) \cdot (1 - \sqrt{-5})$, aber man kann zeigen, dass weder $2 \mid (1 + \sqrt{-5})$ noch $2 \mid (1 - \sqrt{-5})$ gilt.

Man kann sich den Zahlbereich $\mathbb{Z}[\sqrt{-5}]$ als *Erweiterung* der ganzen Zahlen vorstellen, denn für $b = 0$ enthält er auch die gewöhnlichen ganzen Zahlen. Im Bereich der Zahlen $\mathbb{Z}[\sqrt{-5}]$ rechnet man (aus Gründen, die mit dem von *Hermann Hankel*[20] im Jahre 1867 formulierten *Permanenzprinzip* zusammenhängen) folgendermaßen:

Die *Addition*:

$$(a_1 + b_1 \cdot \sqrt{-5}) + (a_2 + b_2 \cdot \sqrt{-5}) := (a_1 + a_2) + (b_1 + b_2) \cdot \sqrt{-5}$$

Das heißt, die Addition wird „komponentenweise“ durchgeführt.

Für die *Multiplikation* gilt: $\sqrt{-5} \cdot \sqrt{-5} = -5$ und

$$(a_1 + b_1 \cdot \sqrt{-5}) \cdot (a_2 + b_2 \cdot \sqrt{-5}) := \\ (a_1 \cdot a_2 - 5 \cdot b_1 \cdot b_2) + (a_1 \cdot b_2 + b_1 \cdot a_2) \cdot \sqrt{-5}$$

Die Motivation für die Definition der Multiplikation besteht offenbar in dem Wunsch, dem in $\mathbb{Z}$ geltenden Distributivgesetz auch in dem neuen, erweiterten Zahlbereich zur Gültigkeit zu verhelfen. Man nennt $\mathbb{Z}[\sqrt{-5}]$ einen *quadratischen Erweiterungsring* der ganzen Zahlen $\mathbb{Z}$; die Bezeichnung „quadratisch“ soll signalisieren, dass gewisse quadratische Gleichungen, die in $\mathbb{Z}$ keine Lösung besitzen, in dem Erweiterungsring lösbar werden; so z.B. die

[20] Hermann Hankel (1839–1873) deutscher Mathematiker

Gleichung $x^2 + 5 = 0$ (mit den Lösungen $x = \sqrt{-5}$ und $x = -\sqrt{-5}$).

In entsprechender Weise lässt sich für jede „quadratfreie“ natürliche Zahl a der Rechenbereich $\mathbb{Z}[\sqrt{-a}]$ konstruierten:

$$\mathbb{Z}[\sqrt{-a}] := \{x + y \cdot \sqrt{-a} : x, y \in \mathbb{Z}\}.$$

Man bezeichnet einen solchen Rechenbereich in der Algebra auch als (kommutativen) *Ring*. Eine natürliche Zahl a heißt dabei *quadratfrei*, wenn 1 $(= 1^2)$ die einzige Quadratzahl ist, von der a geteilt wird. Der Zahlbereich $\mathbb{Z}[\sqrt{-1}]$ wurde intensiv von C. F. Gauß studiert; ihm zu Ehren bezeichnet man $\mathbb{Z}[\sqrt{-1}]$ heute als die *Gaußschen Zahlen*. Die „imaginäre Einheit“ $\sqrt{-1}$ wird oft auch kurz als i geschrieben. Für dieses i gilt dann die fundamentale Gleichung $i^2 = -1$.

Im Venn-Diagramm:

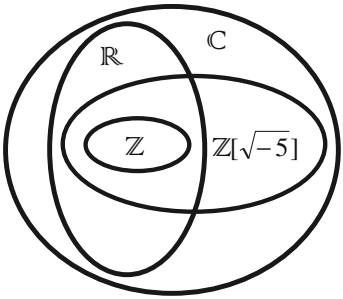


Abb. 4.2: Der Ring der ganzen Zahlen und eine seiner quadratischen Erweiterungen – eingebettet in die reellen und komplexen Zahlen

In den Rechenbereichen der natürlichen und der ganzen Zahlen sind die Primzahlen offenbar durch die beiden folgenden gleichwertigen Eigenschaften ausgezeichnet:

- durch die Eigenschaft (P1) im obigen Primzahlkriterium, die man als (multiplikative) Unzerlegbarkeit bzw. als die „Trivial-Teiler-Eigenschaft“ bezeichnen kann;
- durch die Eigenschaft (P2) im obigen Primzahlkriterium, für die es keine „griffige“ allgemein gebräuchliche Bezeichnung gibt. Umgangssprachlich (und ziemlich „sperrig“) ausgedrückt könnte man sie als die „teilt p ein Produkt, so teilt es (mindestens) einen der Faktoren“ – Eigenschaft bezeichnen.

In Rechenbereichen, wo die Gleichwertigkeit dieser beiden Eigenschaften nicht gilt (wie z.B. in $\mathbb{Z}[\sqrt{-5}]$) wird die erste Eigenschaft des Primzahlkriteriums als *Unzerlegbarkeit* (Irreduzibilität) und die zweite Eigenschaft des Primzahlkriteriums als *Primeigenschaft* bezeichnet. Im Rechenbereich der natürlichen Zahlen gilt mit diesen Bezeichnungen also:

Eine von 1 *verschiedene natürliche Zahl ist genau dann unzerlegbar, wenn sie die Primeigenschaft besitzt.*

4.5 Der Fundamentalsatz der Zahlentheorie

Satz 4.3 (Fundamentalsatz der Zahlentheorie):
Jede natürliche Zahl n $(n > 1)$ ist als Produkt von Primzahlen darstellbar: $n = p_1 \cdot p_2 \cdot \ldots \cdot p_s$. Abgesehen von der Reihenfolge der Faktoren ist diese Darstellung eindeutig.

Bemerkung: Nach dem üblichen mathematischen Sprachgebrauch ist der „Index" s eine natürliche Zahl, die auch gleich 1 sein darf. In diesem Fall ist $n = p_1$ selbst eine Primzahl. Auch diese Möglichkeit ist in der obigen Formulierung des Fundamentalsatzes der Zahlentheorie enthalten.

Beweis des Satzes: Es ist sowohl die Existenz als auch die Eindeutigkeit der Primfaktorzerlegung zu zeigen.

(1.) Zur *Existenz* der Primfaktorzerlegung: Wir führen einen Widerspruchsbeweis durch (vgl. Anhang 8.1). Angenommen, die Aussage sei falsch. Dann gibt es gewisse natürliche Zahlen, die keine Primfaktorzerlegung besitzen, die Menge dieser „Verbrecher" ist also nichtleer und es gibt darunter einen kleinsten; dies sei die natürliche Zahl m. Die Zahl m kann keine Primzahl sein, denn sonst wäre sie kein Verbrecher (vgl. obige Bemerkung); m besitzt also nichttriviale Teiler. Der kleinste darunter sei p. Er ist eine Primzahl (denn der kleinste nichttriviale Teiler einer zerlegbaren natürlichen Zahl ist stets eine Primzahl – vgl. Übungen). Es sei etwa $m = p \cdot r$. Jeder der Faktoren p und r ist kleiner als m. Da m der kleinste Verbrecher war, ist r kein Verbrecher; d.h. r besitzt eine Primfaktorzerlegung, etwa $r = q_1 \cdot \ldots \cdot q_j$. Aber dann ist $p \cdot q_1 \cdot \ldots \cdot q_j$ eine Primfaktorzerlegung von m – im Widerspruch zur Annahme, dass m keine Primfaktorzerlegung besitzt.

(2.) Zur *Eindeutigkeit* der Primfaktorzerlegung: Angenommen, dieser Teil

der Aussage sei falsch. Dann gibt es gewisse natürliche Zahlen, die keine eindeutige Primfaktorzerlegung besitzen, die Menge dieser „Verbrecher“ ist also nichtleer und es gibt darunter einen Kleinsten; dies sei die natürliche Zahl m. $m = p_1 \cdot \ldots \cdot p_s$ und $m = q_1 \cdot \ldots \cdot q_t$ seien zwei unterschiedliche Primfaktorzerlegungen von m. Da die Primzahl p_1 das Produkt $q_1 \cdot \ldots \cdot q_t$ teilt, muss sie nach dem Fundamentallemma einen der Faktoren $q_1, \ldots, q_t$ teilen; p_1 teile etwa q_j. Da q_j eine Primzahl ist, muss p_1 gleich q_j sein: $q_j = p_1$.

Die natürliche Zahl $\frac{m}{p_1} = p_2 \cdot \ldots \cdot p_s = \frac{m}{q_j} = q_1 \cdot \ldots \cdot q_{j-1} \cdot q_{j+1} \cdot \ldots \cdot q_t$ ist kleiner als m und ihre Primfaktorzerlegung ist deshalb bis auf die Reihenfolge der Faktoren eindeutig (denn m war der kleinste Verbrecher). Daraus folgt insbesondere, dass die Anzahl der Faktoren gleich ist (d.h. es ist $s - 1 = t - 1$ und somit auch $s = t$) und dass die Primfaktoren $p_2, \ldots, p_s$ und $q_1, \ldots, q_{j-1}, q_{j+1}, \ldots, q_t$ (bis auf die Reihenfolge) übereinstimmen. Aber damit stimmen dann auch sämtliche Primfaktoren der beiden obigen Zerlegungen von m überein, denn die Primfaktorzerlegungen von m ergeben sich aus denjenigen von $\frac{m}{p_1}$, indem man einmal (im ersten Fall) p_1 und einmal (im zweiten Fall) q_j hinzufügt. Wegen $q_j = p_1$ führt dies (abgesehen von der Reihenfolge) zum gleichen Ergebnis – im Widerspruch zur Annahme, dass m unterschiedliche Primfaktorzerlegungen besitze.

Aufgabe 4.5:

1. Begründen Sie: Jede ungerade Primzahl p lässt sich (für eine geeignete ganze Zahl m) in der Form $p = 4 \cdot m + 1$ oder $p = 4 \cdot m + 3$ schreiben.
2. Zeigen Sie: Jedes Produkt $(4 \cdot m_1 + 1) \cdot (4 \cdot m_2 + 1) \cdot \ldots \cdot (4 \cdot m_k + 1)$ von natürlichen Zahlen der Form $4 \cdot m_i + 1$ hat die Form $4 \cdot x + 1$ mit einer geeigneten Zahl x.
3. Zeigen Sie: Sind $p_1, p_2, \ldots, p_k$ Primzahlen der Form $p_i = 4 \cdot m_i + 3$, dann hat die Zahl $a := 4 \cdot p_1 \cdot p_2 \cdot \ldots \cdot p_k - 1$ einen Primteiler q der Form $q = 4 \cdot m + 3$. (*Hinweis*: Nicht alle Primteiler von a können von der Form $4 \cdot m_i + 1$ sein.)
4. Zeigen Sie, dass q mit keinem der p_i übereinstimmt.
5. Zeigen Sie: Es gibt unendlich viele Primzahlen der Form $4 \cdot m + 3$.

4.6 Die kanonische[21] Darstellung der Primfaktorzerlegung

Die Primzahlen sind in natürlicher Weise der Größe nach geordnet: $2 < 3 < 5 < 7 < 11 < \ldots$. Schreibt man die Primfaktorzerlegung einer natürlichen Zahl unter Berücksichtigung dieser Reihenfolge auf, so ist sie völlig eindeutig; z.B. $1960 = 2 \cdot 2 \cdot 2 \cdot 5 \cdot 7 \cdot 7$. Fasst man dann noch gleiche Faktoren unter Verwendung der Potenz-Schreibweise zusammen, so gelangt man zur *kanonischen Primfaktorzerlegung*; im Beispiel: $1960 = 2^3 \cdot 5^1 \cdot 7^2$

Allgemein lässt sich so jede natürliche Zahl a in der *kanonischen Primfaktorzerlegung* darstellen als: $a = p_1^{m_1} \cdot p_2^{m_2} \cdot \ldots \cdot p_r^{m_r}$ mit der natürlichen Zahl r, den Primzahlen $p_1 < p_2 < \ldots < p_r$ und den Exponenten $m_1 \geq 1$, $m_2 \geq 1$, ..., $m_r \geq 1$.

Satz 4.4 (Teilerstruktur und die kanonische Primfaktorzerlegung):
Jeder Teiler t der Zahl a mit der kanonischen Primfaktorzerlegung $a = p_1^{m_1} \cdot p_2^{m_2} \cdot \ldots \cdot p_r^{m_r}$ hat die Form $t = p_1^{k_1} \cdot p_2^{k_2} \cdot \ldots \cdot p_r^{k_r}$ mit $0 \leq k_i \leq m_i$.

Beweis: Offensichtlich ist jede solche Zahl der Form $p_1^{k_1} \cdot p_2^{k_2} \cdot \ldots \cdot p_r^{k_r}$ ein Teiler von a (Übung). Umgekehrt ist noch zu zeigen, dass jeder Teiler t von a eine derartige Form hat. Sei also t ein Teiler von a; t hat seinerseits eine kanonische Primfaktorzerlegung; etwa $t = q_1^{s_1} \cdot q_2^{s_2} \cdot \ldots$. Jeder der Primteiler q_i von t ist wegen der Transitivität der Teilbarkeitsrelation aber auch ein Teiler von a und muss deswegen mit einem Primfaktor p_j aus der kanonischen Primfaktorzerlegung von a übereinstimmen. Der Exponent s_i von q_i kann nicht größer sein als der entsprechende Exponent m_j von p_j, denn sonst hätte zwar die Zahl $t' = \frac{t}{q_i^{m_j}}$ noch den Primteiler q_i – nicht aber das Vielfache $a' = \frac{a}{q_i^{m_j}}$ von t'.

[21] *Kanon* (lat.): Richtschnur, Leitfaden
kanonisch: als Vorbild dienend

Folgerung: Die natürliche Zahl a mit der kanonischen Primfaktorzerlegung $a = p_1^{m_1} \cdot p_2^{m_2} \cdot \ldots \cdot p_r^{m_r}$ hat genau $(m_1 + 1) \cdot (m_2 + 1) \cdot \ldots \cdot (m_r + 1)$ Teiler.

GGT, KGV und die kanonische Primfaktorzerlegung

Auch die kanonische Primfaktorzerlegung kann zur Ermittlung von GGT und KGV herangezogen werden. Im Schulunterricht ist dies häufig (leider) sogar die einzige Methode, die vermittelt wird – „leider" deshalb, weil der Euklidische Algorithmus wesentlich fundamentaler, anschaulicher und effizienter ist. (Man vergleiche dazu auch das Zitat von Stan Wagon, weiter unten.)

Ein Beispiel zur Verdeutlichung:

1. Wir betrachten die natürlichen Zahlen $a = 25480$ und $b = 61740$.
2. Wir schreiben a und b jeweils in der kanonischen Primfaktorzerlegung: $a = 2^3 \cdot 5 \cdot 7^2 \cdot 13$ und $b = 2^2 \cdot 3^2 \cdot 5 \cdot 7^3$.
3. Wir reichern die Primfaktorzerlegungen von a und b so an, dass jeweils alle vorkommenden Primzahlen (notfalls mit dem Exponenten 0) auftreten: $a = 2^3 \cdot 3^0 \cdot 5^1 \cdot 7^2 \cdot 13^1$ und $b = 2^2 \cdot 3^2 \cdot 5^1 \cdot 7^3 \cdot 13^0$.
4. Wir versehen jede der auftretenden Primzahlen mit einem Exponenten, der gleich dem *Minimum* der in den angereicherten Primfaktorzerlegungen auftretenden Exponenten ist: $2^2 \cdot 3^0 \cdot 5^1 \cdot 7^2 \cdot 13^0 = 980$ und erhalten so $GGT(25480,\ 61740)$.
5. Wir versehen jede der auftretenden Primzahlen mit einem Exponenten, der gleich dem *Maximum* der in den angereicherten Primfaktorzerlegungen auftretenden Exponenten ist: $2^3 \cdot 3^2 \cdot 5^1 \cdot 7^3 \cdot 13^1 = 1605240$ und erhalten so $KGV(25480,\ 61740)$.

Aufgabe 4.6: Bestimmen Sie zum Vergleich der beiden Verfahren $GGT(7618,\ 2536)$ einmal mit dem Euklidischen Algorithmus und einmal mit der kanonischen Primfaktorzerlegung – von „Hand".

Man beachte (vgl. obiges Beispiel):

$$a \cdot b = 25480 \cdot 61740 = 1573135200$$

$$GGT(a,b) \cdot KGV(a,b) = 980 \cdot 1605240 = 1573135200 = a \cdot b$$

Aufgabe 4.7: Formulieren und beweisen Sie den im vorangegangenen Beispiel ausgedrückten Sachverhalt in voller Allgemeinheit (unter Verwendung der kanonischen Primfaktorzerlegung). Hilfreich erweist sich dabei der

Hilfssatz: $a+b = Min(a,b)+Max(a,b)$ und
$a\cdot b = Min(a,b)\cdot Max(a,b)$

Beweis des Hilfssatzes: Übung (Fallunterscheidungen)

Satz 4.5 (Produkt aus GGT und KGV):
Für beliebige natürliche Zahlen a und b gilt stets:
$a\cdot b = GGT(a,b)\cdot KGV(a,b)$.

Eine Bemerkung zur Effizienz der Verfahren

In der Divisionsform ist der Euklidische Algorithmus sehr viel schneller als das auf der Primfaktorzerlegung basierende Verfahren zur Ermittlung des größten gemeinsamen Teilers. Stan Wagon schreibt in dem Buch *Mathematica in Action* (sinngemäß):

> *Mit dem Euklidischen Algorithmus (in der Divisionsform) lässt sich der größte gemeinsame Teiler von zwei 500-stelligen Zahlen in wenigen Sekunden ermitteln. Mit dem Verfahren, das auf der Primfaktorzerlegung basiert, würde dies Hunderte von Jahren dauern.*

Im Hinblick auf die Diskussion der Effizienz des Euklidischen Algorithmus sei an dieser Stelle auch auf Ziegenbalg (2010), Abschnitt 5.5, verwiesen.

4.7 Fermatsche Zahlen

Aufgabe 4.8: Zeigen Sie: Die Operation des Potenzierens ist nicht assoziativ. Geben Sie Gegenbeispiele an.

Bemerkung: Da das Potenzieren von natürlichen Zahlen (im Gegensatz zur Addition und Multiplikation) keine assoziative Operation ist, d.h. da *nicht* allgemein $\left(a^b\right)^c = a^{(b^c)}$ gilt, müsste man den Ausdruck a^{b^c} im Prinzip strikt mit Klammern versehen. Es gilt jedoch im allgemeinen die folgende Konvention: Sind *a*, *b*, *c* natürliche Zahlen, so versteht man unter a^{b^c} in der Regel den Ausdruck $a^{(b^c)}$, denn an Stelle von $\left(a^b\right)^c$ schreibt man meistens $a^{b\cdot c}$.

Definition 4.2: Die *Fermatschen Zahlen* (nach Pierre de Fermat, vgl. Kapitel 1) sind definiert durch: $F_n = 2^{2^n} + 1$ (mit $n \in \mathbb{N}_0$).

In den ersten fünf Fällen ($n = 0, 1, 2, 3, 4$) ergeben sich für F_n Primzahlen: $F_0 = 3$, $F_1 = 5$, $F_2 = 17$, $F_3 = 257$, $F_4 = 65537$. Deshalb vermutete Fermat, dass auch alle folgenden Zahlen dieser Art Primzahlen seien. Im Jahre 1732 konnte Leonhard Euler jedoch zeigen, dass F_5 zerlegbar ist:

$$F_5 = 2^{32} + 1 = 4294967297 = 641 \cdot 6700417$$

Ist eine Fermatsche Zahl F_n eine Primzahl, so nennt man sie eine *Fermatsche Primzahl*. Es ist zur Zeit unbekannt, ob es außer den genannten fünf noch weitere Fermatsche Primzahlen gibt.

Seit der griechischen Antike war die Konstruktion regelmäßiger Polygone (*n*-Ecke) mit Zirkel und Lineal ein wichtiges mathematisches Ziel. Im Jahre 1801 konnte C. F. Gauß zeigen, dass ein regelmäßiges *n*-Eck genau dann mit Zirkel und Lineal konstruierbar ist, wenn n eine Fermatsche Primzahl oder ein Produkt Fermatscher Primzahlen ist.

4.8 Mersennesche[22] Zahlen

In seinem Satz über vollkommene Zahlen (s.u.) betrachtete Euklid (für $n \geq 1$) den in der folgenden Tabelle dargestellten Prozess. Er war besonders an denjenigen Summen interessiert, die Primzahlen ergeben.

Exponent n	$1 + 2 + 2^2 + 2^3 + \ldots + 2^n$	*Wert*	*Primzahl?*
1	1+2	3	**ja**
2	1+2+4	7	**ja**
3	1+2+4+8	15	nein
4	1+2+4+8+16	31	**ja**
5	1+2+4+8+16+32	63	nein
6	1+2+4+8+16+32+64	127	**ja**
7	1+2+4+8+16+32+64+128	255	nein

[22] Marin Mersenne (1588–1648), französischer Mönch, Philosoph und Mathematiker

8	1+2+4+8+16+32+64+128+256	511	nein
9	1+2+4+8+16+32+64+...+512	1023	nein
10	1+2+4+8+16+32+64+...+1024	2047	nein
11	1+2+4+8+16+32+64+...+2048	4095	nein
12	1+2+4+8+16+32+64+...+4096	8191	**ja**
13	1+2+4+8+16+32+64+...+8192	16383	nein
14	1+2+4+8+16+32+64+...+16384	32767	nein
15	1+2+4+8+16+32+64+...+32768	65535	nein

Die Summen der Form: $1+2+2^2+2^3+\ldots+2^{n-1}+2^n$ sind also manchmal Primzahlen, manchmal nicht.

Aufgabe 4.9: Zeigen Sie: Für jede natürliche Zahl n gilt

$1+2+2^2+2^3+\ldots+2^{n-1}=2^n-1$ und (*)

$(1+x+x^2+x^3+\ldots+x^{n-1})\cdot(x-1)=x^n-1$ (**)

Der französische Mönch und Mathematiker M. Mersenne beschäftigte sich mit den Zahlen der Form

$1+2+2^2+2^3+\ldots+2^{n-2}+2^{n-1}$

(d.h. mit Zahlen der Form 2^n-1).

Ihm zu Ehren werden heute Zahlen der Form $M_n=2^n-1$ als *Mersennesche Zahlen* bezeichnet.

Mersenne war besonders an der Frage interessiert, wann solche Zahlen Primzahlen sind. Ein erstes Ergebnis lautet:

Abb. 4.3: M. Mersenne

Satz 4.6 (notwendige Bedingung für Mersennesche Primzahlen):

Eine notwendige Bedingung dafür, dass $M_n=2^n-1$ eine Primzahl ist, ist dass auch n eine Primzahl ist.

Beweis: Ist $n = r \cdot s$ eine zusammengesetzte Zahl, so ist auch $2^n - 1 = 2^{r \cdot s} - 1 = (2^r)^s - 1$ zusammengesetzt. Denn wegen (**) ist mit $x = 2^r$

$$2^n - 1 = 2^{r \cdot s} - 1 = (2^r)^s - 1 = (1 + 2^r + 2^{r \cdot 2} + 2^{r \cdot 3} + \ldots + 2^{r \cdot (s-1)}) \cdot (2^r - 1).$$

Für die Primzahlen p = 2, 3, 5, 7, 13, 17, 19, 31, 61, 89, 107, 127, 521, 607, 1279, 2203, 2281, ... ist M_p eine Primzahl; nicht jedoch für *alle* Primzahlen, denn es ist z.B. $M_{11} = 2^{11} - 1 = 2047 = 23 \cdot 89$.

Die Vermutung, dass M_p stets eine Primzahl sei, wenn p eine Primzahl ist, ist also nicht haltbar.

Definition 4.3: Ist eine Mersennesche Zahl $M_p = 2^p - 1$ eine Primzahl, so nennt man sie eine *Mersennesche Primzahl*.

Mersennesche Zahlen eignen sich sehr gut für die Suche nach großen Primzahlen. Die meisten der heute im Zusammenhang mit Primzahlrekorden auftretenden Primzahlen sind Mersennesche Primzahlen. Für diese Suche ist heute der Computer ein unerlässliches Werkzeug. Unter der Abkürzung GIMPS (The Great Internet Mersenne Prime Search) läuft seit einigen Jahren ein Projekt, bei dem im Internet individuelle Arbeitsplatzcomputer zusammengeschaltet werden, um auf der Basis der Parallelverarbeitung nach Mersenneschen Primzahlen zu suchen; siehe:

http://www.mersenne.org und http://primes.utm.edu (The Prime Pages).

Die bis zum Jahr 2013 größte bekannte Primzahl war zugleich eine Mersennesche Primzahl, nämlich: $M_{57885161} = 2^{57885161}-1$ (vgl. Abschnitt 4.1).

Mersennesche Zahlen und vollkommene Zahlen

Schon Euklid behandelte perfekte Zahlen in den „Elementen“ und konnte ein wichtiges Ergebnis über perfekte Zahlen beweisen. Seine Darstellung sei hier zunächst im ursprünglichen Wortlaut wiedergegeben, um einen Eindruck von seiner Formulierungskunst zu vermitteln (die fast 2000 Jahre später entwickelten sprachlichen Mittel der modernen Algebra standen ihm ja nicht zur Verfügung).

Die Sätze von Euklid und Euler über vollkommene Zahlen

1. *In wörtlicher Formulierung* (vgl. Euklid, Die Elemente, neuntes Buch, §36): Verschafft man sich beliebig viele Zahlen, von der Einheit aus in der Reihe nach dem Verhältnis 1 : 2, bis die Summe aus allem eine Primzahl wird, und bildet die Summe, mit dem letzten Glied vervielfältigt, eine Zahl, so muss das Produkt eine vollkommene Zahl sein.

2. *In moderner Formulierung*:

Satz 4.7 (hinreichende Bedingung für vollkommene Zahlen):
Ist $1+2+2^2+2^3+\ldots+2^n$ eine Primzahl, so ist die Zahl $2^n \cdot (1+2+2^2+2^3+\ldots+2^n)$ vollkommen.

Beweis: Es sei $p := 1+2+2^2+2^3+\ldots+2^n$ eine Primzahl und $a = 2^n \cdot (1+2+2^2+2^3+\ldots+2^n)$; d.h.: $a = 2^n \cdot p$. Da p eine Primzahl ist, hat a genau die Teiler 1, 2, 2^2, 2^3, ... , 2^n und p, $2p$, $2^2 p$, $2^3 p$, ... , $2^n p$. Also ist

$$\begin{aligned}\sigma(a) &= (1+2+2^2+2^3+\ldots+2^n) + p \cdot (1+2+2^2+2^3+\ldots+2^n) \\ &= p + p \cdot (1+2+2^2+2^3+\ldots+2^n) \\ &= p + p \cdot (2^{n+1}-1) = p \cdot (1+2^{n+1}-1) \\ &= 2 \cdot 2^n p \\ &= 2 \cdot a\end{aligned}$$

Fast 2000 Jahre später konnte Euler zeigen, dass für gerade vollkommene Zahlen auch die Umkehrung gilt.

Wir erinnern an dieser Stelle an den folgenden Satz (vgl. Abschnitt 2.3): Die Teilersummenfunktion σ ist multiplikativ, d.h. für teilerfremde natürliche Zahlen a und b gilt $\sigma(a \cdot b) = \sigma(a) \cdot \sigma(b)$.

Satz 4.8 (notwendige Bedingung für gerade vollkommene Zahlen):
Ist a eine gerade, vollkommene Zahl, dann ist sie (notwendigerweise) von der Form $2^n \cdot (1+2+2^2+2^3+\ldots+2^n)$, wobei $1+2+2^2+2^3+\ldots+2^n$ eine Primzahl ist.

Beweis: Es sei a eine gerade, vollkommene Zahl. Dann lässt sich a darstellen in der Form $a = 2^s \cdot b$, wobei b eine ungerade Zahl ist.
Für die Teilersumme von a gilt wegen der Multiplikativität von σ

$$\sigma(a) = \sigma(2^s) \cdot \sigma(b). \qquad (*)$$

Aus der Definition der Teilersummenfunktion (vgl. 2.3) folgt unmittelbar: $\sigma(2^s) = 1 + 2 + 2^2 + 2^3 + \ldots + 2^s = 2^{s+1} - 1$.

Da a vollkommen ist, gilt $\sigma(a) = 2 \cdot a = 2^{s+1} \cdot b$. Daraus folgt mit (*) $\sigma(a) = 2^{s+1} \cdot b = (2^{s+1} - 1) \cdot \sigma(b)$. Da $2^{s+1} - 1$ eine ungerade Zahl ist, folgt aus der letzten Gleichung, dass sie ein Teiler von b sein muss; es gibt also eine natürliche Zahl d mit der Eigenschaft: $(2^{s+1} - 1) \cdot d = b$. (**)

In die letzte Gleichung eingesetzt, ergibt das:
$2^{s+1} \cdot (2^{s+1} - 1) \cdot d = (2^{s+1} - 1) \cdot \sigma(b)$; gekürzt: $2^{s+1} \cdot d = \sigma(b)$.

Die Teiler d und b von b treten in $\sigma(b)$ als Summanden auf; also ist

$$2^{s+1} \cdot d = \sigma(b) \geq b + d = (2^{s+1} - 1) \cdot d + d = 2^{s+1} \cdot d.$$

Das erzwingt $\sigma(b) = b + d$ und dies wiederum ist nur möglich, wenn b eine Primzahl und $d = 1$ ist. Aus der Gleichung (**) folgt schließlich

$$b = 2^{s+1} - 1$$

und somit ist

$$a = 2^s \cdot b = 2^s \cdot (2^{s+1} - 1) = 2^s \cdot (1 + 2 + 2^2 + 2^3 + \ldots + 2^s).$$

4.9 Die Goldbachsche Vermutung

Im Jahre 1742 teilte der Mathematiker und Diplomat Christian *Goldbach* (1690–1764) dem führenden Mathematiker Leonhard Euler die folgende Vermutung mit:

Jede gerade Zahl größer als 2 ist als Summe zweier Primzahlen darstellbar.

So ist zum Beispiel: $20 = 3 + 17$.

Es kann auch mehrere solche Darstellungen geben; z.B.: $20 = 7 + 13$.

Die berühmte Vermutung entzog sich über die Jahrhunderte hinweg einer Entscheidung, d.h. einem Beweis oder einer Widerlegung.

Im Jahre 2000 brachten die Verlagshäuser Bloomsbury und Faber & Faber die englische Ausgabe des Buches „Uncle Petros and Goldbach's Conjecture" von Apostolos Doxiadis heraus. Als Publicity-Maßnahme stifteten sie im März 2000 einen Preis von 1 Million U.S. Dollar für die Lösung der Goldbachschen Vermutung. Die Lösung musste allerdings bis März 2002 eingereicht und der vollständige Beweis bis März 2004 veröffentlicht sein. Das Preisgeld wurde nie eingefordert. Der Verkauf des Buches brachte den Verlagen im Jahr 2000 (laut The Guardian, Saturday 3 March 2001) einen Gewinn in Höhe von 256.000 Englische Pfund ein. Bloomsbury und Faber & Faber hätten sich sich aber keine allzu großen Gedanken über die eventuell entstehende Deckungslücke machen müssen. Sie hätten sie leicht mit den Einnahmen aus dem Verkauf von Harry Potter decken können. Ihr Risiko, dass sie den Preis hätten auszahlen müssen, war zudem nicht sehr hoch. Die Vermutung konnte bis heute weder bewiesen noch widerlegt werden.

Die *schwache* (oder *ternäre*) Goldbachsche Vermutung besagt, dass jede ungerade Zahl größer als 5 als Summe dreier (nicht notwendigerweise verschiedener) Primzahlen dargestellt werden kann. Für diese Vermutung legte der peruanische Mathematiker H. Helfgott im Jahre 2013 einen Beweis vor. Bezeichnet man die ursprüngliche Vermutung als *starke* Goldbachsche Vermutung, so gilt: Aus der Gültigkeit der (starken) Goldbachschen Vermutung, würde sofort die der schwachen Goldbach-Vermutung folgen.

Aufgabe 4.10: Begründen Sie die letzte Aussage.

4.10 Formeln und Polynome für Primzahlen

„Ein Problem mathematisch zu lösen" wurde in der Vergangenheit – und wird auch heute noch vielfach – damit identifiziert, „eine Formel (einen Rechenausdruck, ein Polynom, ...) zu finden, welche die Lösung des Problems beschreibt". Polynome, also Ausdrücke der Form

$$P(x) = a_n \cdot x^n + a_{n-1} \cdot x^{n-1} + \ldots + a_3 \cdot x^3 + a_2 \cdot x^2 + a_1 \cdot x + a_0$$

(wobei die „Koeffizienten" a_i in der Regel natürliche, rationale, reelle oder komplexe Zahlen sind) hängen eng mit der Suche nach Primzahlen zusammen. Leonhard Euler untersuchte das Polynom $H(x) = x^2 - x + 41$ und entdeckte, dass die 41 Werte $H(0)$, $H(1)$, $H(2)$, …, $H(40)$ alles Primzahlen sind.

Es gilt jedoch der folgende

Satz 4.9 (Primzahlen und Polynome):
Es existiert kein Polynom
$P(x) = a_n \cdot x^n + a_{n-1} \cdot x^{n-1} + \ldots + a_3 \cdot x^3 + a_2 \cdot x^2 + a_1 \cdot x + a_0$
mit ganzzahligen Koeffizienten $a_i \ \{i = 0, \ldots, n\}$ vom Grad $n \geq 1$, das für alle $x \in \mathbb{Z}$ Primzahlwerte annimmt.

Beweis: 1. *Fall*: Ist $P(0) = a_0$ keine Primzahl, so sind wir fertig.

2. *Fall*: Es sei also $P(0) = a_0 = q$ eine Primzahl.

Für jede natürliche Zahl m sei $b = \sum_{i=1}^{n} a_i \cdot m^i \cdot q^{i-1}$. Die Zahl b lässt sich deuten als der Wert des Polynoms

$$Q(x) = m \cdot (a_n \cdot x^{n-1} + a_{n-1} \cdot x^{n-2} + \ldots + a_3 \cdot x^2 + a_2 \cdot x + a_1)$$

an der Stelle $x = m \cdot q$.

Für alle natürlichen Zahlen m gilt

$$\begin{aligned} P(m \cdot q) &= a_n (m \cdot q)^n + a_{n-1} (m \cdot q)^{n-1} + \ldots + a_1 (m \cdot q) + a_0 \\ &= q \cdot b + a_0 \\ &= q \cdot b + q \\ &= q \cdot (b + 1) \end{aligned}$$

Dieser Wert ist eine zusammengesetzte Zahl, d.h. eine Nicht-Primzahl, falls b von Null verschieden ist. Ein solches b gibt es, denn das Polynom $Q(x)$ ist nicht das Nullpolynom (nach Voraussetzung ist $a_n \neq 0$) und besitzt nach dem Fundamentalsatz der Algebra höchstens $n-1$ Nullstellen. Es muss also natürliche Zahlen m geben mit $Q(m \cdot q) \neq 0$. Wählt man ein solches m, so ist b von Null verschieden und $P(m \cdot q) = q \cdot (b + 1)$ ist keine Primzahl.

4.11 Die Verteilung der Primzahlen

Besonders faszinierend an den Primzahlen ist die Unregelmäßigkeit, mit der sie auftreten. Es gibt zwar unendlich viele davon, diese sind aber sehr ungleichmäßig auf der Zahlengeraden „verstreut“. Wie werden sehen, dass es in

den natürlichen Zahlen einerseits beliebig große primzahlfreie Lücken gibt, dass aber auch sehr viele sehr eng benachbarte Primzahlen, „Primzahlzwillinge“ genannt, vorkommen. Ob es unendlich viele solcher Primzahlzwillinge gibt, ist derzeit eine offene Frage.

Empirische Untersuchungen zeigen, dass es sich mit den Primzahlen ähnlich verhält wie mit der Luft: je weiter man „nach oben“ steigt, desto „dünner“ wird ihre Konzentration (ihre „Dichte“, wie man auch sagt).

Ein beliebter Zeitvertreib, angesiedelt zwischen Unterhaltungsmathematik und Zahlentheorie, besteht darin, Primzahlen nach bestimmten (geometrischen) Mustern darzustellen – und auf diese Weise Gesetzmäßigkeiten über sie zu entdecken.

Es gibt auch eine sportliche Variante in Verbindung mit den Primzahlen. So werden seit Jahrhunderten Listen mit Primzahlrekorden geführt (was ist die größte bekannte Primzahl, welches sind die größten bekannten Primzahlzwillinge, was ist die größte bekannte Mersennesche Primzahl, u.s.w.). Der Mathematiker P. Ribenboim hat sogar ein ganzes Buch unter diesem Aspekt geschrieben: *The Book of Prime Number Records*; Springer Verlag, New York / Berlin 1989. Es wurde im Jahre 1997 aktualisiert und erschien unter dem Titel *The New Book of Prime Number Records*.

Da solche Rekorde sehr rasch veralten, bietet es sich heute an, die Rekordlisten auf elektronischer Basis im Internet zu führen, wo sie sehr schnell zu aktualisieren und praktisch jederzeit und von jedem Ort aus einzusehen sind. Eine besonders ergiebige Quelle für alles, was Primzahlen betrifft, findet sich unter der Internetadresse der University of Tennessee (U.S.A.):

http://www.utm.edu/research/primes/

Satz 4.10 (Primzahl-Lücken):

Zu jeder natürlichen Zahl n gibt es n aufeinanderfolgende natürliche Zahlen, die keine Primzahlen sind.

Beweis: Man betrachte die n Zahlen $(n+1)!+2$, $(n+1)!+3$, ... , $(n+1)!+n$ und $(n+1)!+(n+1)$. Die erste dieser Zahlen ist durch 2, die zweite durch 3, ... , die vorletzte durch n und die letzte durch $n+1$ teilbar; es sind also alles keine Primzahlen.

Primzahlzwillinge

Primzahlpaare der Form $\{p,\ p+2\}$ heißen *Primzahlzwillinge*; so sind z.B. die Paare $\{5, 7\}$, $\{11, 13\}$ und $\{101, 103\}$ Primzahlzwillinge. Das im Jahr 2011 gefundene Zahlenpaar $3756801695685 \cdot 2^{666669} \pm 1$ (im Dezimalsystem geschrieben mit jeweils 200.700 Stellen) ist bis heute (August 2014) das größte bekannte Paar von Primzahlzwillingen. Es ist derzeit unbekannt, ob es nur endlich viele oder unendlich viele Primzahlzwillinge gibt. Es gilt jedoch (auf den Beweis muss an dieser Stelle verzichtet werden):

(1.) Die (unendliche) Summe aus den Reziproken der Primzahlen ist divergent; d.h. die Summe

$$\frac{1}{2}+\frac{1}{3}+\frac{1}{5}+\frac{1}{7}+\frac{1}{11}+\frac{1}{13}+\frac{1}{17}+\frac{1}{19}+\frac{1}{23}+\frac{1}{29}+\frac{1}{31}+\frac{1}{37}+\frac{1}{41}+\frac{1}{43}+\frac{1}{47}+...$$

besitzt keinen Grenzwert.

(2.) Die Summe aus den Reziproken der Primzahlzwillinge ist endlich oder konvergent; bzw. etwas genauer: Die Summe

$$(\frac{1}{3}+\frac{1}{5})+(\frac{1}{5}+\frac{1}{7})+(\frac{1}{11}+\frac{1}{13})+(\frac{1}{17}+\frac{1}{19})+(\frac{1}{29}+\frac{1}{31})+(\frac{1}{41}+\frac{1}{43})+...$$

besitzt einen Grenzwert B (Bruns[23] Konstante: $B \approx 1{,}902160583104$).

Im Jahre 2013 bewies der chinesisch-amerikanische Mathematiker Yitang Zhang, dass es unendlich viele Primzahlpaare gibt, die höchstens den Abstand $a = 70.000.000$ voneinander haben. Danach setzte eine intensive Jagd nach kleineren solchen Grenzen ein. James Maynard (University of Montreal) konnte den Wert von a auf 600 drücken. Im Rahmen des kollaborativen Projekts *polymath8* gelang es, den Abstand immer weiter zu verkleinern. Derzeit liegt der von Terence Tao (University of California, Los Angeles, Fields Medaille 2006) erzielte Rekord bei $a = 246$ (vgl. PolyMath homepage / polymath8). Mit der unteren Grenze $a = 2$ wäre schließlich der Nachweis der Existenz unendlich vieler Primzahlzwillinge erbracht.

Überraschenderweise haben Primzahlzwillinge bei der Aufdeckung von Fehlern in der Architektur bestimmter Mikroprozessoren eine entscheidende Rolle

[23] Viggo Brun, 1885–1978, norwegischer Mathematiker

gespielt. Hier eine Darstellung dazu aus dem Jahrbuch der Mathematik 1996/97, 135–143:

Das 470 Millionen Dollar Zwillingspaar
(824 633 702 441, 824 633 702 443)

Primzahlzwillingsforschung ist mathematische Grundlagenforschung, eine direkte Anwendung gibt es - zumindest zur Zeit - nicht. Trotzdem waren es letztendlich Primzahlzwillinge, die die wahrscheinlich teuerste Rückrufaktion der Welt auslösten. Mitte 1994 begann der amerikanische Mathematiker Thomas R. Nicely, Primzahlzwillinge zu zählen. Zunächst setzte er einige PCs älterer Bauart ein, im März 1995 kam dann ein Rechner mit dem Pentium-Prozessor der amerikanischen Firma Intel hinzu. Nach Problemen mit Speichermodulen und Compilerfehlern, die zu Beginn seiner Berechnungen aufgetreten waren, hatte er sich dazu entschlossen, sämtliche Teilrechnungen auf jeweils zwei Maschinen unterschiedlicher Bauart laufen zu lassen. Dabei trat plötzlich eine Diskrepanz bei der Berechnung der Summe über die reziproken Primzahlzwillinge zutage. Die Ursache dieser Diskrepanz fand sich schließlich im Prozessor selbst. Der Pentium verrechnete sich beim Bilden der Kehrwerte des Paares (824 633 702 441, 824 633 702 443). Ein Fehler in der sogenannten FPU (floating point unit) des Pentiums führte zu gelegentlich auftretenden Ungenauigkeiten. Dieser Fehler zwang Intel schließlich dazu, die Prozessoren durch korrigierte Versionen auszutauschen. Insgesamt soll diese Umtauschaktion etwa 470 Millionen Dollar gekostet haben.

Primzahldrillinge, Primzahl-Cousinen und sexy Primzahlen

Primzahltripel der Form $\{p,\ p+2,\ p+4\}$ heißen *Primzahldrillinge*.

Aufgabe 4.11: Zeigen Sie, dass die Zahlen 3, 5 und 7 das einzig mögliche Primzahldrillings-Tripel bilden.

Weitere Primzahl-„Verwandtschaften“ geben zu vielerlei Untersuchungen Anlass: Primzahlpaare der Form (p, p+4), also z.B. (3, 7), (7, 11), (13, 17), ... werden als *Primzahl-Cousinen* und Primzahlpaare der Form (p, p+6), also z.B. (5, 11), (7, 13), (11, 17), ... werden aus offensichtlichen Gründen als *sexy Primzahlen* bezeichnet (vgl. mathworld.wolfram.com/TwinPrimes.html).

Einige empirische Befunde

> It is a capital mistake to theorise before one has data.
> *Sir Arthur Conan Doyle*
>
> Für große Mathematiker war das Betrachten konkreter Beispiele schon immer eine wichtige Quelle der Intuition.
> *Srinivasa Ramanujan*, genialer indischer Mathematiker (erste Hälfte des 20. Jahrhunderts)

Mathematisches Wissen entwickelt sich häufig durch das „freie Spielen“ mit mathematischen Objekten (Zahlen, Linien, Kurven, Konfigurationen, ...). Am Anfang stehen dabei spontane Entdeckungen an konkreten Beispielen. Man bewegt sich dabei zunächst völlig im Bereiche der empirischen Arbeitsweise. Durch dieses freie Spiel kommt man zu ersten (empirischen) Entdeckungen, Vermutungen, Hypothesen. So arbeiteten und arbeiten selbst berühmte Mathematiker; eine ganze Serie berühmter Vermutungen (Fermat, Gauß, Riemann u.v.m.) ist so entstanden.

Das Aufstellen und Verifizieren von Hypothesen setzt i.a. ein solides Studium der dem Problem zugrundeliegenden „Daten“ voraus. Solche Experimente sollte man zunächst „von Hand“ ausführen. Bei etwas komplexerer Sachlage wird aber sehr bald der (mit geeigneter Software ausgestattete) Computer ein unverzichtbares Werkzeug beim Experimentieren. In der Zahlentheorie ist der Computer und seine Software (meist in der Form von Computeralgebra Systemen) insbesondere auch bei der Untersuchung „großer“ Zahlen unentbehrlich.

Ein Beispiel möge dies belegen: Es dauerte fast 100 Jahre, bis die Zerlegbarkeit der Fermatschen Zahl

$$F_5 = 2^{32} + 1 = 4294967297 = 641 \cdot 6700417$$

nachgewiesen werden konnte und es forderte das Talent eines der genialsten Mathematiker aller Zeiten – Leonhard Euler. Heute findet ein Computeralgebra System die Zerlegung auf einem ganz normalen PC in kaum messbarer Zeit.

Im Folgenden sind einige Primzahltabellen angegeben, die (sei es in der vorliegenden oder in ähnlicher Form) als Vorstudien bei der Erstellung der Hypothese des „großen Primzahlsatzes“ eine Rolle gespielt haben. Auch

große Mathematiker verbrachten z.T. viel Zeit mit der Erstellung solcher Tabellen. Heute ist das Aufstellen derartiger Tabellen oft eine gute Programmierübung, ein kleiner Beitrag zur „algorithmischen Zahlentheorie“.

Die folgende Tabelle gibt an, wie viele Primzahlen es „unterhalb“ von gewissen natürlichen Zahlen gibt. Dabei sei $\pi(n)$ die Anzahl der Primzahlen unterhalb von n.

n	$\pi(n)$
10	4
100	25
1.000	168
10.000	1229
100.000	9592
1.000.000	78498
10.000.000	664579
100.000.000	5761455
1.000.000.000	50847534

Die nächste Tabelle gibt an, wie viele Primzahlen es in den ersten „Hunderttausender-Intervallen“ natürlicher Zahlen gibt.

Intervall	*Anzahl der Primzahlen in dem Intervall*
0 – 100.000	9592
100.000 – 200.000	8392
200.000 – 300.000	8013
300.000 – 400.000	7863
400.000 – 500.000	7678
500.000 – 600.000	7560
600.000 – 700.000	7445
700.000 – 800.000	7408
800.000 – 900.000	7323
900.000 – 1.000.000	7224

Diese, wie auch die nächste Tabelle sind ein empirischer Beleg dafür, dass die Primzahlen mit der Größe des Zahlbereichs, den wir betrachten, tendenziell in

immer geringerer Anzahl auftreten, dass also, wie man auch sagt, die *Dichte* der Primzahlen mit wachsender Größe abnimmt.

Hier noch einige weitere Daten (mit der Intervallgröße: 1000, einer sog. *Chiliade*):

Intervall	*Anzahl der Primzahlen in der Chiliade*
0 – 1000	168
1000 – 2000	135
2000 – 3000	127
3000 – 4000	120
4000 – 5000	119
5000 – 6000	114
6000 – 7000	117
7000 – 8000	107
8000 – 9000	110
9000 – 10000	112
$10^4 - 10^4 + 1000$	106
$10^5 - 10^5 + 1000$	81
$10^6 - 10^6 + 1000$	75
$10^7 - 10^7 + 1000$	61
$10^8 - 10^8 + 1000$	54
$10^9 - 10^9 + 1000$	49

Bemerkung: C. F. Gauß war nicht nur ein genialer Mathematiker sondern auch ein vorzüglicher „Rechner“ (was bei weitem nicht immer dasselbe ist). Gauß scheint seine Untersuchungen über Primzahlen etwa im Alter von 14 Jahren begonnen zu haben und setzte sie sein ganzes Leben lang fort. In einem Brief an den Astronomen Encke erzählt er, wie gern er ab und zu ein Viertelstündchen damit verbringe, die Primzahlen einer Chiliade von Zahlen auszuzählen.

Satz 4.11 (Der große Primzahlsatz von Gauß): $\lim_{x\to\infty}\left(\frac{\pi(x)}{x/\ln x}\right)=1$

Der im Jahre 1792 von Gauß vermutete „große Primzahlsatz“ konnte erst nach über 100 Jahren im Jahre 1896 vollständig bewiesen werden, und zwar, auf-

bauend auf Ergebnissen des russischen Mathematikers P. L. Chebyshev (1821–1894). Dies gelang unabhängig voneinander dem französischen Mathematiker Jacques Hadamard (1865–1963) und dem belgischen Mathematiker Charles de la Valleé-Poussin (1866–1962).

Schaubilder zum großen Primzahlsatz

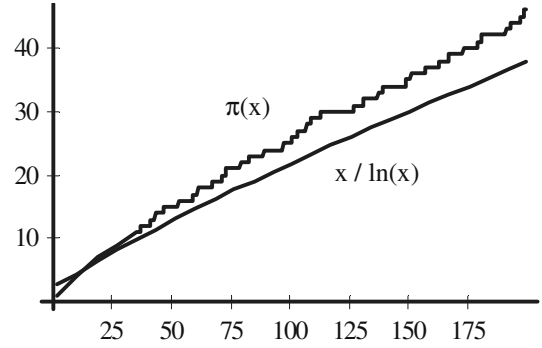


Abb. 4.4: Primzahlfunktion und Logarithmus

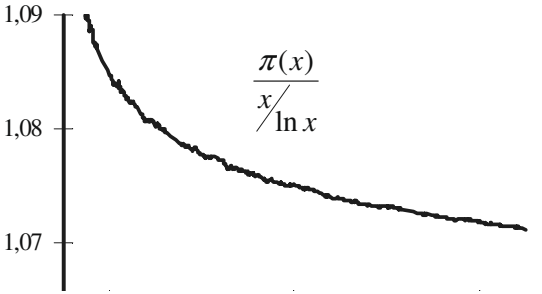


Abb. 4.5: zum Gaußschen Primzahlsatz

Dass die Mathematik eine hochgradig „lebendige“ Wissenschaft ist, in der es noch vieles zu entdecken und erforschen gibt, zeigt die folgende Liste mit offenen Primzahl-Problemen, die in den Internetseiten der University of St Andrews (Schottland) zu finden ist:

http://www-history.mcs.st-andrews.ac.uk/HistTopics/Prime_numbers.html

5 Kongruenzen und Restklassen

Kontext: Die folgenden Überlegungen spielen sich stets in der Grundmenge der ganzen Zahlen $\mathbb{Z}$ ab, falls nichts anderes festgelegt ist.

5.1 Die Kongruenzrelation

Definition 5.1: Es seien a, b und m ganze Zahlen; $m \geq 0$. Man vereinbart die folgende Schreib- und Sprechweise:

$a \equiv b \pmod{m} \Leftrightarrow m \mid (b-a)$.

Andere Schreibweise: $a \equiv b\,(m)$ an Stelle von $a \equiv b \pmod{m}$

In Worten: $a \equiv b \pmod{m}$: a ist kongruent zu b modulo m

Die Zahl m wird der *Modul* der Kongruenz genannt.

Als Moduln wollen wir im Folgenden nur nichtnegative ganze Zahlen betrachten; *wenn also von einem Modul* m *die Rede ist*, *so wird stets stillschweigend vorausgesetzt*, *dass* $m \geq 0$ (*und in der Regel sogar* $m \geq 2$) *ist*.

Hilfssatz: Für $a, b \in \mathbb{N}$ gilt $a \equiv b \pmod{m}$ genau dann, wenn a und b bei der Division durch m denselben Rest haben. (Beweis: Übung)

Die folgende Abbildung kann als Veranschaulichung dieses Sachverhalts angesehen werden.

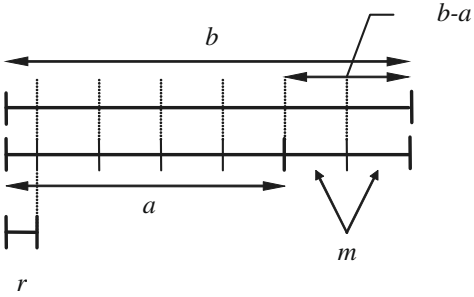


Abb. 5.1: zur Kongruenz von natürlichen Zahlen modulo m

Satz 5.1 (Die Kongruenz ist eine Äquivalenzrelation):
Die Relation „a ist kongruent zu b modulo m“ ist eine Äquivalenzrelation.

J. Ziegenbalg, *Elementare Zahlentheorie*, DOI 10.1007/978-3-658-07171-4_5

Beweis: Übung

Definition 5.2: $\overline{a} := \{x \in \mathbb{Z}:\ x \equiv a \pmod m\}$, also die Menge der zu a modulo m kongruenten ganzen Zahlen, heißt die *Restklasse* von a modulo m.

Bemerkungen:

1. Es ist $\overline{a} := \{a, a \pm m, a \pm 2m, a \pm 3m, \dots, a \pm k \cdot m, \dots\}$. Jede der Zahlen $a + v \cdot m$ kann als Repräsentant dieser Restklasse verwendet werden; insbesondere (im Falle $v = 0$) auch a selbst. Die Zahl a ist also einer der (i.a. unendlich vielen) *Repräsentanten* dieser Restklasse.
2. Die Menge *aller* Restklassen modulo m wird (bei festem Modul m) auch durch R_m bzw. durch $\mathbb{Z}/m \cdot \mathbb{Z}$ oder auch $\mathbb{Z}/(m)$ bezeichnet.
3. Eine Menge ganzer Zahlen $\{a_1, a_2, \dots, a_m\}$ mit der Eigenschaft, dass die Menge der Restklassen $\{\overline{a_1}, \overline{a_2}, \dots, \overline{a_m}\}$ mit der Menge $\mathbb{Z}/m \cdot \mathbb{Z}$ übereinstimmt, nennt man ein *vollständiges Repräsentantensystem* von R_m. Im Falle $m \geq 2$ gibt es für jede Restklasse stets unendlich viele Repräsentanten (siehe Bemerkung 1.) und dementsprechend auch unendlich viele Repräsentantensysteme.
4. Für jedes m $(m \geq 2)$ stellt die Menge $\{0, 1, 2, 3, \dots, m-1\}$ ein vollständiges Repräsentantensystem von $\mathbb{Z}/m \cdot \mathbb{Z}$ dar (Übung); man nennt es auch das *kanonische* Repräsentantensystem.
5. Ist $\{a_1, a_2, \dots, a_m\}$ ein weiteres vollständiges Repräsentantensystem, so gilt $\{\overline{a_1}, \overline{a_2}, \dots, \overline{a_m}\} = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \dots, \overline{m-1}\}$
   Die *Mengen* $\{\overline{a_1}, \overline{a_2}, \dots, \overline{a_m}\}$ und $\{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \dots, \overline{m-1}\}$ sind dann also gleich – allerdings nicht notwendigerweise „elementweise“ in der aufgeschriebenen Reihenfolge. Ist dies der Fall, so sagt man auch: Die Mengen $\{a_1, a_2, \dots, a_m\}$ und $\{0, 1, 2, 3, \dots, m-1\}$ stimmen *modulo m* überein bzw. sie sind *modulo m* gleich.

Ein Beispiel: $m = 6$

Das kanonische Repräsentantensystem ist dann $\{0, 1, 2, 3, 4, 5\}$. Ein anderes vollständiges Repräsentantensystem wäre z.B. die Menge

$\{13, 77, 118, 32, 24, 51\}$. Anders ausgedrückt ist

$$R_6 = \mathbb{Z}/_{6\cdot\mathbb{Z}} = \mathbb{Z}/_{(6)} = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}\} = \{\overline{13}, \overline{77}, \overline{118}, \overline{32}, \overline{24}, \overline{51}\}.$$

Die Restklassen dieses Restesystems stimmen *modulo 6* folgendermaßen paarweise überein:

$$\bar{0} = \overline{24}, \quad \bar{1} = \overline{13}, \quad \bar{2} = \overline{32}, \quad \bar{3} = \overline{51}, \quad \bar{4} = \overline{118}, \quad \bar{5} = \overline{77}.$$

Aufgabe 5.1:

1. Was bedeuten die folgenden Aussagen
   - $a \equiv b \pmod 0$
   - $a \equiv b \pmod 1$
2. Wie viele Elemente haben die folgenden Mengen von Restklassen
   - $\mathbb{Z}/_{0\cdot\mathbb{Z}}$
   - $\mathbb{Z}/_{1\cdot\mathbb{Z}}$
3. Geben Sie der folgenden Aussage einen konkreten Sinn:
   Kongruent zu sein modulo 2 heißt, dieselbe „Parität“ zu besitzen.
4. Machen Sie sich den folgenden Sachverhalt an einem typischen Beispiel klar und zeigen Sie allgemein:

   Aus $k \mid m$ und $x \equiv y \pmod m$ folgt $x \equiv y \pmod k$.

   Aus der Perspektive der Informationstheorie könnte man dies auch folgendermaßen ausdrücken: Bezüglich eines „größeren“ Moduls kongruent zu sein, ist aussagekräftiger (hat einen höheren Informationsgehalt) als bezüglich eines „kleineren“ Moduls. (Hierbei wird als natürliche Ordnungsrelation die Teilbarkeitsrelation verwendet).

Satz 5.2 (vollständige Repräsentantensysteme):
Jedes System von Repräsentanten *modulo m*, das m Elemente enthält, von denen keine zwei *modulo m* gleich sind, ist ein vollständiges Repräsentantensystem von R_m.

Beweis. Übung

Satz 5.3 (Verträglichkeit der Kongruenzrelation mit der Addition und Multiplikation):
Die Relation „a ist kongruent zu b modulo m“ ist *verträglich* mit den Rechenoperationen der Addition und der Multiplikation, d.h., für alle ganzen Zahlen a, b, und c gilt:

(1) Aus $a \equiv b \pmod{m}$ folgt $a + c \equiv b + c \pmod{m}$.

(2) Aus $a \equiv b \pmod{m}$ folgt $a \cdot c \equiv b \cdot c \pmod{m}$.

Beweis: Zu (1): Zu zeigen ist: Aus $m \mid (b - a)$ folgt $m \mid (b + c) - (a + c)$. Wenn irgendwo die Sprechweise „das ist trivial“ angebracht ist, dann in diesem Fall. Entsprechendes gilt für (2).

Folgerungen: Für alle ganzen Zahlen a, b, c und d und alle natürlichen Zahlen n gilt:

(1) Aus $a \equiv b \pmod{m}$ folgt $a - c \equiv b - c \pmod{m}$.

(2) Aus $a \equiv b \pmod{m}$ und $c \equiv d \pmod{m}$
folgt $a + c \equiv b + d \pmod{m}$.

(3) Aus $a \equiv b \pmod{m}$ und $c \equiv d \pmod{m}$
folgt $a - c \equiv b - d \pmod{m}$.

(4) Aus $a \equiv b \pmod{m}$ und $c \equiv d \pmod{m}$
folgt $a \cdot c \equiv b \cdot d \pmod{m}$.

(5) Aus $a \equiv b \pmod{m}$ folgt $a^n \equiv b^n \pmod{m}$.

Beweis: Übung

Bemerkung: Diese Folgerungen besagen, informell gesprochen, dass man in Bezug auf Addition, Multiplikation (sowie den daraus abgeleiteten Operationen der Subtraktion und der Potenzierung) mit Restklassen und Kongruenzen „praktisch genau so rechnen kann“ wie mit gewöhnlichen natürlichen Zahlen und der Gleichheitsrelation.

Die Division bildet jedoch eine Ausnahme, der in den folgenden Ergebnissen Rechnung getragen wird.

Hilfssatz: Aus $a \mid b \cdot c$ und $GGT(a, b) = 1$ folgt $a \mid c$.

Beweis: Nach dem Lemma von Bachet gibt es ganze Zahlen x und y mit der

Eigenschaft $1 = x \cdot a + y \cdot b$. Somit ist $c = c \cdot x \cdot a + c \cdot y \cdot b$. Da a nach Voraussetzung die rechte Seite der letzten Gleichung teilt, teilt es auch die linke Seite, d.h. $a \mid c$.

Satz 5.4 (Kongruenz und GGT):
Für alle ganzen Zahlen a, b, c und m gilt – mit $d := \mathrm{GGT}(c,m)$:

Aus $a \cdot c \equiv b \cdot c \pmod{m}$ folgt $a \equiv b \pmod{\frac{m}{d}}$.

Beweis: Die Kongruenz $a \cdot c \equiv b \cdot c \pmod{m}$ besagt nach Definition:
$m \mid a \cdot c - b \cdot c$. D.h., $m \mid (a-b) \cdot c$ bzw. $k \cdot m = (a-b) \cdot c$ (*)
für eine geeignete ganze Zahl k. Es sei weiterhin (mit $d = \mathrm{GGT}(c,m)$):
$q := \frac{m}{d}$ und $s := \frac{c}{d}$. Mit anderen Worten: $m = q \cdot d$ und $c = s \cdot d$. Aus (*) folgt durch Einsetzen $k \cdot q \cdot d = (a-b) \cdot s \cdot d$. Da d von Null verschieden ist, kann gekürzt werden. Es gilt also $k \cdot q = (a-b) \cdot s$, d.h. es ist

$$k \cdot \frac{m}{d} = (a-b) \cdot \frac{c}{d}. \qquad (**)$$

Man beachte: $q = \frac{m}{d}$ und $s = \frac{c}{d}$ sind ganze Zahlen. Die ganze Zahl $\frac{m}{d}$ ist wegen (**) ein Teiler von $(a-b) \cdot \frac{c}{d}$. Wegen $d = \mathrm{GGT}(c,m)$ sind $q = \frac{m}{d}$ und $s = \frac{c}{d}$ teilerfremd (vgl. Regel GGT-9). Also ist $\frac{m}{d}$ nach dem vorigen Hilfssatz ein Teiler von $(a-b)$; es ist also $a \equiv b \pmod{\frac{m}{d}}$.

Folgerung 1: Für alle ganzen Zahlen a, b, c und m mit $c \mid m$ gilt:

Aus $a \cdot c \equiv b \cdot c \pmod{m}$ folgt $a \equiv b \pmod{\frac{m}{c}}$.

Beweis: Aus $c \mid m$ folgt $GGT(c,m) = c$.

Folgerung 2 („Kürzungsregel“): Für alle ganzen Zahlen a, b, c und m gilt:
Ist $\mathrm{GGT}(c,m) = 1$ (d.h. sind c und m teilerfremd), dann gilt:
Aus $a \cdot c \equiv b \cdot c \pmod{m}$ folgt $a \equiv b \pmod{m}$.

Bemerkung: Die letzte Aussage lässt sich auch folgendermaßen formulieren: Eine Kongruenz modulo m lässt sich mit c *kürzen* (bzw. mit c „durchdividieren"), wenn c teilerfremd zu m ist.

Beispiel: Es ist $18 \equiv 102 \pmod 7$. Da $18 = 6 \cdot 3$, $102 = 34 \cdot 3$ und

$$GGT(3,\ 7) = 1 \text{ ist, gilt auch } \frac{18}{3} \equiv \frac{102}{3} \pmod 7, \text{ d.h. } 6 \equiv 34 \pmod 7.$$

Ohne die Voraussetzung der Teilerfremdheit gilt die entsprechende Aussage nicht; so ist z.B. $26 \equiv 38 \pmod{12}$; aber im Falle von $c = 2$ gilt *nicht* $13 \equiv 19 \pmod{12}$.

Man beachte in diesem Zusammenhang auch die Folgerung aus dem Euklidischen Algorithmus (Vielfachsummendarstellung bzw. *Lemma von Bachet*):

> Sind die natürlichen Zahlen a und b teilerfremd (d.h.: $GGT(a,b) = 1$), dann gilt: Es gibt ganze Zahlen x und y mit: $x \cdot a + y \cdot b = 1$.

Anders ausgedrückt, heißt das: $b \mid x \cdot a - 1$, bzw. $x \cdot a \equiv 1 \pmod b$ bzw. $\bar{x} \cdot \bar{a} = \bar{1}$ in R_b $(= \mathbb{Z}/b\mathbb{Z})$. Die Restklasse $\bar{x}$ ist also „multiplikativ invers" zur Restklasse $\bar{a}$.

Im „Rechenbereich" R_b gibt es also genau dann ein *Inverses* $\bar{x}$ zur Restklasse $\bar{a}$, wenn a und b teilerfremd sind. Man findet dieses inverse Element mit Hilfe der aus dem erweiterten Euklidischen Algorithmus (Berlekamp-Algorithmus) folgenden Vielfachsummendarstellung.

5.2 Restklassenarithmetik

Die Verträglichkeit der Kongruenzrelation mit den arithmetischen Grundoperationen der Addition und der Multiplikation ermöglicht die Übertragung dieser Operationen auf das Restklassensystem $R_m = \mathbb{Z}/m\mathbb{Z}$ wie folgt:

Definition der *Restklassenaddition*: $\bar{a} \oplus \bar{b} := \overline{a+b}$

Definition der Restklassenmultiplikation: $\bar{a} \otimes \bar{b} := \overline{a \cdot b}$

Diese Definitionen unterliegen dem folgenden im Zusammenhang mit Äquivalenzrelationen oft verwendeten *universellen Prinzip*:

Das Ergebnis der neuen Operation, angewandt auf die jeweiligen Restklassen, wird definiert als die Restklasse der alten (ursprünglichen) Operation, angewandt auf die Repräsentanten der Restklassen.

Dies führt zum immer wieder auftretenden Problem der *Wohldefiniertheit* der neuen Operationen: Ist diese Definition unabhängig von der Wahl der Repräsentanten für die jeweiligen Restklassen? Nur dann ist ja die neu definierte Operation wohldefiniert – d.h. sinnvoll.

Konkret heißt das (nach dem Prinzip „Gleiches zu Gleichem ergibt Gleiches“):

Sind a_1, a_2, b_1, b_2 und m ganze Zahlen derart, dass in
$\mathbb{Z}/_{m\cdot\mathbb{Z}}$ $\overline{a_1} = \overline{a_2}$ und $\overline{b_1} = \overline{b_2}$ ist, dann ist stets
$\overline{a_1} \oplus \overline{b_1} = \overline{a_2} \oplus \overline{b_2}$ und $\overline{a_1} \otimes \overline{b_1} = \overline{a_2} \otimes \overline{b_2}$.

Beispiel zur Erläuterung des Problems der Wohldefiniertheit: Als Modul betrachten wir im Folgenden $m = 6$.

1. Addition von Restklassen modulo 6: $\overline{3} \oplus \overline{5} = \overline{3+5} = \overline{8} = \overline{2}$
   Nun ist aber z.B. $\overline{3} = \overline{27}$ und $\overline{5} = \overline{41}$. Wir hätten die Summe $\overline{3} \oplus \overline{5}$ also genauso gut als $\overline{27} \oplus \overline{41}$ schreiben können. Aber dann wäre die Summe bei ganz direkter Anwendung der Additionsregel folgendermaßen zu berechnen gewesen: $\overline{27} \oplus \overline{41} = \overline{27+41} = \overline{68}$.
   Es wäre nun nicht akzeptabel, wenn das Ergebnis der Restklassenaddition von der Wahl der Repräsentanten abhinge, wenn also z.B. der Ausdruck $\overline{2} \oplus \overline{5}$ ein anderes Ergebnis liefern würde als der Ausdruck $\overline{27} \oplus \overline{41}$. Im konkreten Fall ist auch alles in Ordnung, denn 68 ist kongruent zu 2 modulo 6, d.h. $\overline{68} = \overline{2}$ in R_6. Im betrachteten Beispiel war das Ergebnis also tatsächlich unabhängig von der Wahl der Repräsentanten.

2. Multiplikation von Restklassen modulo 6:
   Führen Sie diese Überlegung zur Übung parallel zum soeben diskutierten Beispiel durch.

Aufgabe 5.2: Zeigen Sie allgemein, dass die oben eingeführten Operationen der Restklassenaddition und Restklassenmultiplikation wohldefiniert sind.

Wegen der engen („kanonischen“) Verbindung zwischen der alten und der neuen Operation übernimmt man (da Verwechslungen und Zweideutigkeiten praktisch ausgeschlossen sind) oft die Schreibweise der alten Operation für die

neue Operation, also in diesem Fall $\bar{a}+\bar{b}$ an Stelle von $\bar{a}\oplus\bar{b}$ und $\bar{a}\cdot\bar{b}$ an Stelle von $\bar{a}\otimes\bar{b}$. Man beugt so der Verbreitung einer Vielzahl neuer, exotischer Operations- und Funktionssymbole vor. (Gelegentlich wird in der Literatur sogar auch noch das die Restklassen symbolisierende Überstreichungszeichen weggelassen).

Da R_m im Falle $m \geq 2$ nur aus den endlich vielen Elementen $\{\bar{0},\bar{1},\bar{2},...,\overline{m-1}\}$ besteht, kann man die Restklassenaddition und -multiplikation in diesem Falle in der Form einer kompletten Verknüpfungstabelle darstellen.

Beispiel: $m=6$: $R_6 = \mathbb{Z}/6\mathbb{Z} = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}\}$.

+	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{4}$	$\bar{4}$	$\bar{5}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{5}$	$\bar{5}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$

•	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{4}$	$\bar{0}$	$\bar{2}$	$\bar{4}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{0}$	$\bar{3}$
$\bar{4}$	$\bar{0}$	$\bar{4}$	$\bar{2}$	$\bar{0}$	$\bar{4}$	$\bar{2}$
$\bar{5}$	$\bar{0}$	$\bar{5}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

Das Beispiel macht einige bemerkenswerte Eigenschaften der Restklassenaddition und Restklassenmultiplikation deutlich. Zum einen zeigt es die enge Verwandtschaft der Restklassenoperationen mit den entsprechenden Operationen in den ganzen Zahlen. Viele Eigenschaften der Ganzzahladdition und Ganzzahlmultiplikation (wie z.B. das assoziative und kommutative Gesetz oder das Distributivgesetz) übertragen sich durch die Art der Definition unmittelbar auf die Restklassen. Man sagt auch, die Restklassenaddition und -multiplikation „erben“ diese Eigenschaften von der gewöhnlichen Addition und Multiplikation im Bereiche der ganzen Zahlen. Dies sei exemplarisch am Beispiel der Kommutativität der Restklassenaddition gezeigt.

Zu zeigen ist, dass für alle $\bar{a}$ und $\bar{b}$ aus R_m stets gilt: $\bar{a}+\bar{b}=\bar{b}+\bar{a}$.

Nach Definition ist $\bar{a} + \bar{b} = \overline{a+b}$, wobei auf der rechten Seite die gewöhnliche Addition der ganzen Zahlen steht. Für diese gilt aber $a + b = b + a$ und somit auch $\overline{a+b} = \overline{b+a}$. Das heißt, es ist $\bar{a} + \bar{b} = \bar{b} + \bar{a}$.

Ganz entsprechend wird der Beweis für die anderen oben genannten Operationseigenschaften durchgeführt. Durch die „kanonische" Art der Definition der Restklassenoperationen werden wesentliche allgemeine Eigenschaften „vererbt".

Sowohl die Tabellendarstellung wie auch die allgemeine Definition machen weitere Gemeinsamkeiten deutlich. So ist z.B. $\bar{0}$ das neutrale Element der Addition und $\bar{1}$ das neutrale Element der Multiplikation in R_m. (In den Tabellen kommt dies dadurch zum Ausdruck, dass $\bar{0}$ in der Additionstabelle die Eingangsspalte und Eingangszeile „reproduziert"; entsprechendes gilt für $\bar{1}$ in Bezug auf die Multiplikationstabelle.) In Bezug auf die Restklassenmultiplikation ist $\bar{0}$ das „Nullelement"; Multiplikation mit diesem Element macht jedes Produkt zu Null. In der Sprache der modernen Algebra gesprochen ist R_m (wie auch $\mathbb{Z}$) ein *kommutativer Ring* (mit Einselement $\bar{1}$).

Andererseits treten, wie das Beispiel R_6 zeigt, bei den Restklassen auch neuartige Phänomene auf, die in $\mathbb{Z}$ nicht bekannt sind. Wenn man die Restklasse $\bar{1}$ hinreichen oft „aufaddiert", erhält man als Ergebnis die Null: $\bar{1}+\bar{1}+\bar{1}+\bar{1}+\bar{1}+\bar{1} = \bar{0}$ (m.a.W.: R_m ist eine *endliche zyklische* Gruppe).

In der Multiplikationstabelle von R_6 tritt die folgende neuartige Gleichung auf: $\bar{2} \cdot \bar{3} = \bar{0}$.

Ein Produkt von zwei Zahlen, die beide von Null verschieden sind, wird also zu Null! Man kann die letzte Gleichung auch durch die Sprechweise ausdrücken (vgl. Definition der Teilbarkeitsrelation):

$\bar{2}$ und $\bar{3}$ sind Teiler von $\bar{0}$.

Elemente mit dieser Eigenschaft, die selbst von Null verschieden sind, werden dementsprechend auch als *Nullteiler* bezeichnet.

Allgemein werden in Ringen von Null verschiedene Elemente a und b, deren Produkt gleich Null ist $(a \cdot b = 0)$, als *Nullteiler* bezeichnet. In Restklassenringen können also Nullteiler auftreten.

Aufgabe 5.3: Zeigen Sie: Wenn der Modul m eine Primzahl ist, so ist der Restklassenring *nullteilerfrei*.

Eine weitere interessante Gleichung in R_6 ist $\bar{4} \cdot \bar{4} = \bar{4}$. Das heißt $\bar{4}^2 = \bar{4}$ und daraus folgt sofort $\bar{4}^3 = \bar{4}^4 = \bar{4}^5 = \ldots = \bar{4}^n = \bar{4}$. Alle Potenzen von $\bar{4}$ sind gleich $\bar{4}$. Solche Elemente nennt man *idempotent*[24]. Auch im Bereiche der ganzen Zahlen gibt es idempotente Elemente, nämlich die Zahlen 0 und 1. Dies sind die trivialen idempotenten Elemente. In $\mathbb{Z}$ gibt es keine weitere (also keine nichttriviale) idempotente Elemente; in Restklassenringen treten jedoch, wie das obige Beispiel zeigt, solche nichttriviale idempotente Elemente auf.

Aufgabe 5.4: Deuten Sie die Kongruenz modulo 12, den Prozess des Zählens und die Restklassenaddition modulo 12 am Ziffernblatt einer Uhr.

Eine typische Aufgabe, die leicht mit Hilfe der Kongruenzrechnung gelöst werden kann, lautet z.B. folgendermaßen: Was ist im Dezimalsystem die letzte Ziffer der Zahl 7^{1999}?

Lösungsskizze: Die gesuchte Zahl stimmt offenbar mit dem kanonischen Repräsentanten von 7^{1999} modulo 10 überein.

Nun gilt: $7^2 \equiv 49 \equiv 9 \pmod{10}$. Daraus folgt:

$7^4 \equiv 9^2 \equiv 81 \equiv 1 \pmod{10}$ und somit $7^{4 \cdot k} \equiv (7^4)^k \equiv 1^k \equiv 1 \pmod{10}$.

Also ist z.B. $7^{1996} \equiv 7^{4 \cdot 499} \equiv 1 \pmod{10}$ und schließlich

$7^{1999} \equiv 7^{1996+3} \equiv 7^{1996} \cdot 7^3 \equiv 1 \cdot 343 \equiv 3 \pmod{10}$.

Aufgabe 5.5: Zeigen Sie

1. Jede Quadratzahl ist kongruent 1 oder kongruent 0 modulo 4.
2. Die Summe zweier Quadratzahlen ist nie kongruent 3 modulo 4.
3. Eine Primzahl p der Form $p = 4 \cdot k + 3$ ist nie als Summe zweier Quadratzahlen darstellbar.

[24] *idem* (lateinisch): derselbe, dasselbe

5.3 Systeme linearer Kongruenzen und der Chinesische Restsatz

Der Name des Satzes geht auf die folgende Aufgabe im *Handbuch der Arithmetik* des Chinesischen Mathematikers Sun-Tse (etwa 3. Jahrhundert n. Chr.) zurück:

> *Es soll eine Anzahl von Dingen gezählt werden. Zählt man sie zu je drei, dann bleiben zwei übrig. Zählt man sie zu je fünf, dann bleiben drei übrig. Zählt man sie zu je sieben, dann bleiben zwei übrig. Wie viele sind es?*

In der Terminologie der Kongruenzen kann man dies folgendermaßen ausdrücken: Gesucht ist eine ganze Zahl x mit der Eigenschaft:

$x \equiv 2 \quad (3)$, $x \equiv 3 \quad (5)$ und $x \equiv 2 \quad (7)$.

Man bezeichnet ein solches System von Kongruenzen auch als ein *System (simultaner) linearer Kongruenzen*. Die Lösungen derartiger Systeme werden durch den folgenden Satz beschrieben.

Satz 5.5 (Chinesischer Restsatz):

Es seien $m_1, m_2, ..., m_k$ paarweise teilerfremde natürliche Zahlen. Weiterhin seien $b_1, b_2, ..., b_k$ beliebige ganze Zahlen. Dann besitzt das System linearer Kongruenzen

$x \equiv b_1 \quad (m_1)$
$x \equiv b_2 \quad (m_2)$
...
$x \equiv b_k \quad (m_k)$

eine ganzzahlige Lösung x.

Diese erhält man wie folgt: Man setze $m := m_1 \cdot m_2 \cdot \ldots \cdot m_k$ und $a_i := \frac{m}{m_i}$. Dann ist a_i teilerfremd zu m_i und die Kongruenz $a_i \cdot x_i \equiv b_i \quad (m_i)$ besitzt eine Lösung x_i (vgl. Bemerkungen zum Euklidischen Algorithmus bzw. zur Vielfachsummendarstellung). Man setze nun

$x := a_1 x_1 + a_2 x_2 + \ldots + a_k x_k$

und erhält damit eine Lösung des oben angegebenen Systems linearer Kongruenzen.

Alle Lösungen des Gleichungssystems sind „*modulo m*“ eindeutig; d.h.: Eine ganze Zahl x' ist genau dann eine Lösung des oben angegebenen Systems linearer Kongruenzen, wenn gilt: $x' \equiv x \quad (m)$.

Beweis: Zur *Existenz* der Lösung: Es ist zu zeigen, dass die ganze Zahl

$x := a_1 x_1 + a_2 x_2 + \ldots + a_k x_k$ eine Lösung des Systems linearer Kongruenzen ist.

Für jedes i und jedes von i verschiedene j gilt: $m_i \mid a_j$ – oder mit anderen Worten: $a_j \equiv 0\,(m_i)$. Deshalb gilt für alle i: $x \equiv a_i x_i\,(m_i)$. Da nach Voraussetzung $a_i \cdot x_i \equiv b_i\,(m_i)$ gilt, folgt $x \equiv b_i\,(m_i)$.

Die oben angegebene ganze Zahl x löst also das System der linearen Kongruenzen.

Zur *Eindeutigkeitsaussage*: Es sei x' eine weitere Lösung. Dann folgt für alle i: $x' \equiv x\,(m_i)$; d.h. $m_i \mid (x'-x)$. Da die ganzen Zahlen $m_1, m_2, \ldots, m_k$ paarweise teilerfremd sind, ist dann $(x'-x)$ auch durch m teilbar; d.h. $x' \equiv x \quad (m)$.

Dass schließlich (umgekehrt) jede ganze Zahl x' mit der Eigenschaft $x' \equiv x\ (m)$ eine Lösung des Systems linearer Kongruenzen ist, ergibt sich durch direktes Nachrechnen.

Beispiel: Wir betrachten das von Sun-Tse angegebene System linearer Kongruenzen

$x \equiv 2 \quad (3) \qquad$ für $\qquad x \equiv b_1 \quad (m_1)$
$x \equiv 3 \quad (5) \qquad$ für $\qquad x \equiv b_2 \quad (m_2)$
$x \equiv 2 \quad (7) \qquad$ für $\qquad x \equiv b_3 \quad (m_3)$.

Mit den Bezeichnungen des Chinesischen Restsatzes gilt:

$m := m_1 \cdot m_2 \cdot m_3 = 3 \cdot 5 \cdot 7 = 105$; sowie

$$a_1 := \frac{m}{m_1} = \frac{3 \cdot 5 \cdot 7}{3} = 5 \cdot 7 = 35$$

$$a_2 := \frac{m}{m_2} = \frac{3 \cdot 5 \cdot 7}{5} = 3 \cdot 7 = 21$$

$$a_3 := \frac{m}{m_3} = \frac{3 \cdot 5 \cdot 7}{7} = 3 \cdot 5 = 15 .$$

Die Kongruenzen $a_i \cdot x_i \equiv b_i \quad (m_i)$ stellen sich nun wie folgt dar:

$i = 1$: $a_1 \cdot x_1 \equiv b_1 \quad (m_1)$ $35 \cdot x_1 \equiv 2 \quad (3)$

„Reduktion der Koeffizienten“ modulo 3 ergibt: $2 \cdot x_1 \equiv 2 \quad (3)$

„Durchmultiplizieren“ mit 2 ergibt (modulo 3): $x_1 \equiv 1 \quad (3)$

$i = 2$: $a_2 \cdot x_2 \equiv b_2 \quad (m_2)$ $21 \cdot x_2 \equiv 3 \quad (5)$ $x_2 \equiv 3 \quad (5)$

$i = 3$: $a_3 \cdot x_3 \equiv b_3 \quad (m_3)$ $15 \cdot x_3 \equiv 2 \quad (7)$ $x_3 \equiv 2 \quad (7)$

Mit den so ermittelten Werten $a_1, a_2, a_3, x_1, x_2, x_3$ erhält man nun

$$x := a_1 x_1 + a_2 x_2 + a_3 x_3 = 35 \cdot 1 + 21 \cdot 3 + 15 \cdot 2 = 128 .$$

Modulo $m \quad (= 105)$ lautet die kleinste nichtnegative Lösung: $x' = 128 - 105 = 23$.

Probe: $23 \equiv 2 \quad (3)$ ist richtig
$23 \equiv 3 \quad (5)$ ist richtig
$23 \equiv 2 \quad (7)$ ist richtig

Aufgabe 5.6: Lösen Sie die in Kapitel 1 beschriebene Aufgabe des „Chinesischen Reiters“ mit Hilfe der im Chinesischen Restsatz entwickelten Methode.

Aufgabe 5.7: Innerhalb desselben Kalendermonats sind die Tagesdaten der Sonntage (Montage, Dienstage,...) jeweils kongruent modulo 7. Finden Sie für 2014 einen Monat mit 5 Sonntagen und überprüfen Sie die Aussage an dem Beispiel.

Aufgabe 5.8: Zeigen Sie: Jede ungerade Quadratzahl ist kongruent zu 1 modulo 8.

Aufgabe 5.9: Ausdrücke der Form $\binom{n}{k} = \frac{n!}{k!(n-k)!}$ heißen *Binomialkoeffizienten*. Zeigen Sie: Ist p eine Primzahl und $k \in \{1, 2, 3, \ldots, p-1\}$, dann ist $\binom{p}{k}$ durch p teilbar (d.h. $\binom{p}{k} \equiv 0 \pmod{p}$.

Aufgabe 5.10: Zeigen Sie: Für beliebige ganze Zahlen x und y und jede Primzahl p gilt: $(x+y)^p = x^p + y^p \pmod{p}$.

Aufgabe 5.11: Für jede reelle Zahl x ist $\lfloor x \rfloor$ („Gaußsche Klammer“) definiert als die größte ganze Zahl, die kleiner oder gleich x ist.
Zeichnen Sie den Funktionsgraphen der Funktion $x \to \lfloor x \rfloor$ im Bereich von -5 bis 10.

Aufgabe 5.12 (Berechnung des Wochentags): Sie behaupten, dass Sie als Sonntagskind geboren sind, aber Ihre Freunde glauben Ihnen nicht und einen Kalender aus Ihrem Geburtsjahr haben Sie nicht zur Verfügung. In Form der Gleichung (* W *), weiter unten, finden Sie eine Formel, nach der Sie den Wochentag (auf der Basis des Gregorianischen Kalenders, also für jedes Datum nach Freitag, dem 15. Oktober 1582) berechnen können. Die Datumsangabe erfolgt (man vergleiche die Beispiele unten) nach dem Schema: Jahrhundert (H), Jahr (J), Monat (M), Tag (T).

Codierung der Wochentage: So=0, Mo=1, Di=2, Mi=3, Do=4, Fr=5, Sa=6.
Codierung der Monate: März=1, April=2, Mai=3,..., Dez=10, Jan=11, Feb=12

Die Monate Januar und Februar werden zum Vorjahr gerechnet; der 8. Februar 2006 ist also wie folgt zu codieren: H=20, J=5, M=12, T=8.

Mit diesen Bezeichnungen berechnet sich der Wochentag W wie folgt:

$$W \equiv T + \lfloor (13 \cdot M - 1)/5 \rfloor + J + \lfloor J/4 \rfloor + \lfloor H/4 \rfloor - 2 \cdot H \pmod 7 . \qquad (* \text{ W } *)$$

1. Berechnen Sie weitere Beispiele; z.B. Ihr Geburtsdatum.
2. Analysieren Sie die Formel für den Wochentag. (*Hinweis*: Ore 1967)

Beispiele:
Tag des Mauerfalls: 9. Nov. 1989; H=19, J=89, M=9, T=9
==> W=4 (Donnerstag)
19. September 1971: T=19, M=7, J=71, H=19 ==> W=0 (Sonntag)
3. Oktober 1990: T=3, M=8, J=90, H=19 ==> W=3 (Mittwoch)
1. Januar 2000: T=1, M=11, J=99, H=19 ==> W=6 (Samstag)
29. Februar 2016: T=29, M=12, J=15, H=20 ==> W=1 (Montag)

6 Stellenwertsysteme, Teilbarkeitsregeln und Rechenproben

Smog-Alarm in Paris – nur Autos mit ungerader Endziffer dürfen fahren, die Autos mit gerader Endziffer nicht. Es gab Unklarheiten: Ist die Endziffer 0 eine gerade Zahl? Fahrer mit der Endziffer 0 gingen straffrei aus, denn die Polizei wusste auch keine Antwort.

ZDF Nachrichtensendung „heute“ 1. Oktober 1997, 19 Uhr

6.1 Stellenwertsysteme

In der heute üblichen Darstellung im Zehnersystem bedeutet die Schreibweise 7285 dasselbe wie

$7 \cdot 1000 + 2 \cdot 100 + 8 \cdot 10 + 5 \cdot 1$ bzw.

$7 \cdot 10^3 + 2 \cdot 10^2 + 8 \cdot 10^1 + 5 \cdot 10^0$.

Diese Darstellungsform ist eine *Stellenwertschreibweise* zur *Basis* 10.

Mit Hilfe einer Stellenwerttafel kann man dies folgendermaßen anschaulich darstellen:

Tausender	Hunderter	Zehner	Einer
T	H	Z	E
7	2	8	5

Man kann ebenso andere *Stellenwertsysteme* (d.h. Stellenwertschreibweisen mit anderen Basen) betrachten. Voraussetzung für jede Form der Stellenwertdarstellung ist die „Erfindung“ der Null durch die Inder etwa im 6. Jahrhundert n. Chr. Die Null macht es möglich, Positionen in der Stellenwerttafel, die nicht besetzt sind, zu kennzeichnen und so z.B. die Zahldarstellungen 345, 3045, 3405, 30405, 30045, 34005, 304005, ... zu unterscheiden. Sie ist darüber hinaus die Voraussetzung für die Realisierung unserer heute gebräuchlichen Grundrechenarten, so wie sie z.B. in der Grundschule gelehrt und erlernt werden.

J. Ziegenbalg, *Elementare Zahlentheorie*, DOI 10.1007/978-3-658-07171-4_6

Satz 6.1 (Existenz und Eindeutigkeit der Zahldarstellung in Stellenwertsystemen):
Es sei b eine natürliche Zahl $(b > 1)$. Dann besitzt jede beliebige natürliche Zahl n eine Stellenwertdarstellung im Stellenwertsystem zur Basis b, d.h., es gibt eindeutig bestimmte Zahlen r sowie ganze Zahlen m_r, m_{r-1}, $m_{r-2}, \ldots, m_2, m_1, m_0$ (mit $0 \le m_i < b$ für $i = 0,\ldots,r$ und $m_r \neq 0$) mit der Eigenschaft:

$$n = m_r \cdot b^r + m_{r-1} \cdot b^{r-1} + m_{r-2} \cdot b^{r-2} + \ldots + m_2 \cdot b^2 + m_1 \cdot b^1 + m_0 \cdot b^0.$$

Die Zahlen m_i heißen auch die *Ziffern* von n bei der Darstellung im System zur Basis b – kurz im b-System. Die Eindeutigkeitsaussage besagt in dieser Terminologie, dass die Ziffernfolge m_r, m_{r-1}, $m_{r-2}, \ldots, m_2, m_1, m_0$ eindeutig ist.

Beweis: Die *Existenz* der Stellenwertdarstellung wird als Widerspruchsbeweis mit „kleinstem Verbrecher“ k durchgeführt. Die Division mit Rest von k durch b ergibt $k = q \cdot b + r$ mit $0 \le r < b$.

1. *Fall*: Wäre in der vorangehenden Gleichung $q = 0$, so folgte daraus $k = r$. Dann wäre aber $k = r \cdot b^0$ eine Darstellung von k im b-System. Dies stünde im Widerspruch zu der Annahme, dass k keine solche Darstellung besitzt. Also kann q nicht gleich Null sein.

2. *Fall*: Zu untersuchen bleibt also der Fall $q \ge 1$. Wegen $b > 1$ ist $q < k$. Der Quotient q kann also kein „Verbrecher“ sein, q besitzt also eine eindeutige Stellenwertdarstellung im b-System:

$$q = z_s \cdot b^s + z_{s-1} \cdot b^{s-1} + z_{s-2} \cdot b^{s-2} + \ldots + z_2 \cdot b^2 + z_1 \cdot b^1 + z_0 \cdot b^0.$$

Dann ist aber im Widerspruch zur Annahme, k sei ein Verbrecher,

$$\begin{aligned} k &= q \cdot b + r \\ &= z_s \cdot b^{s+1} + z_{s-1} \cdot b^s + z_{s-2} \cdot b^{s-1} + \ldots + z_2 \cdot b^3 + z_1 \cdot b^2 + z_0 \cdot b^1 + r \cdot b^0 \end{aligned}$$

eine Darstellung von k im b-System.

Beweisskizze für die *Eindeutigkeit* der Darstellung (Widerspruchsbeweis): Angenommen, es gäbe eine natürliche Zahl k mit zwei verschiedenen Stellenwertdarstellungen; etwa

$$k = z_s \cdot b^s + z_{s-1} \cdot b^{s-1} + z_{s-2} \cdot b^{s-2} + \ldots + z_2 \cdot b^2 + z_1 \cdot b^1 + z_0 \cdot b^0 \quad \text{und}$$

$$k = c_t \cdot b^t + c_{t-1} \cdot b^{t-1} + c_{t-2} \cdot b^{t-2} + \ldots + c_2 \cdot b^2 + c_1 \cdot b^1 + c_0 \cdot b^0 .$$

Es sei j der größte Index, wo sich die Koeffizienten c_i und z_i unterscheiden und es sei etwa (ohne Beschränkung der Allgemeinheit) $c_j < z_j$. Dann beträgt der Unterschied *an dieser Stelle* $(z_j - c_j) \cdot b^j$. Diese Differenz ist größer oder gleich b^j und der „Fehlbetrag" kann durch die Ziffernfolgen an den „niedrigeren" Stellen nicht mehr wett gemacht werden, denn die maximale Zahl an den niedrigen Stellen wäre

$$(b-1) \cdot b^{j-1} + (b-1) \cdot b^{j-2} + \ldots + (b-1) \cdot b^2 + (b-1) \cdot b^1 + (b-1) \cdot b^0$$

und dies ist immer noch kleiner als b^j („Kilometerzähler"-Argument).

Ein *Beispiel* zur Verdeutlichung: Im Zehnersystem $(b = 10)$ gilt – etwa an der Stelle $j = 3$: $1 \cdot b^3 = 1000 > 999 = (b-1) \cdot b^2 + (b-1) \cdot b^1 + (b-1) \cdot b^0$.

Spezielle Stellenwertsysteme

***b* = 2:** Das *Zweiersystem* (*Binärsystem*, *Dualsystem*) wird heute besonders in der Datenverarbeitung angewandt. Es wurde erstmals im Jahre 1705 von *G. W. Leibniz* unter dem Titel *„Explication de l'Arithmétique Binaire"* (Erläuterung der binären Arithmetik) in der Zeitschrift der Académie Royale des Sciences (Paris) beschrieben (vgl. Abb. 6.1).

Die Bedeutung des Zweiersystems für die Datenverarbeitung rührt daher, dass Computer physikalisch aus Speicherelementen aufgebaut sind, die genau zwei unterscheidbare Zustände besitzen. Der eine dieser Zustände wird meist mit 0, der andere mit 1 bezeichnet (in der Elektrotechnik werden oft auch die Symbole O und L verwendet). Jedes solche Speicherelement wird als *Bit* (*binary digit*) bezeichnet. Das „Bit" ist in der Informationstheorie zugleich auch die Grundeinheit des von C. Shannon[25] eingeführten Informationsmaßes.

***b* = 8:** Auch das *Achtersystem* (*Oktalsystem*) kommt gelegentlich in der Datenverarbeitung zur Anwendung

[25] Claude E. Shannon (1916–2001), amerikanischer Mathematiker, Elektrotechniker und Kryptologe, „Vater der Informationstheorie"

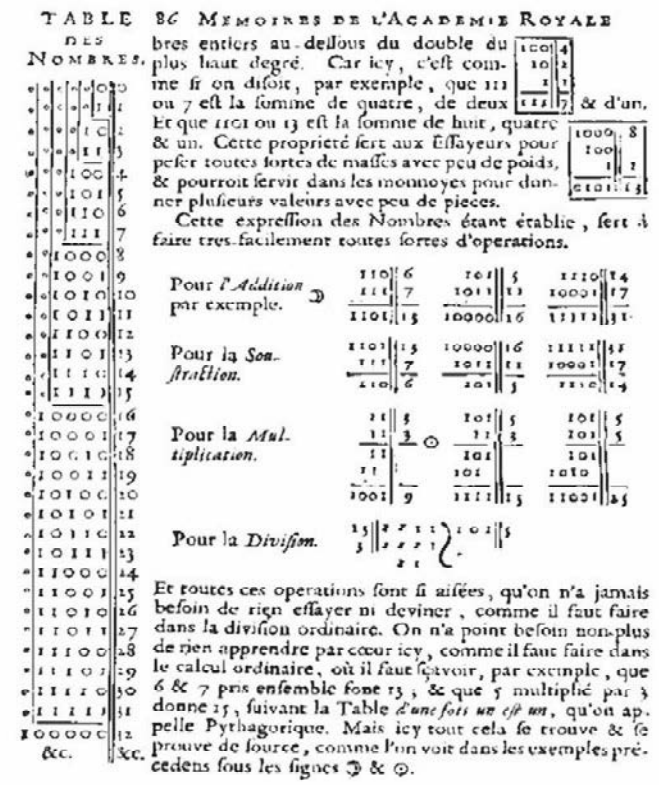


TABLE DES NOMBRES.

86 MEMOIRES DE L'ACADEMIE ROYALE

bres entiers au-deſſous du double du plus haut degré. Car icy, c'eſt comme ſi on diſoit, par exemple, que 111 ou 7 eſt la ſomme de quatre, de deux & d'un. Et que 1101 ou 13 eſt la ſomme de huit, quatre & un. Cette proprieté ſert aux Eſſayeurs pour peſer toutes ſortes de maſſes avec peu de poids, & pourroit ſervir dans les monnoyes pour donner pluſieurs valeurs avec peu de pieces.

Cette expreſſion des Nombres étant établie, ſert à faire tres-facilement toutes ſortes d'operations.

Pour l'*Addition* par exemple.

Pour la *Souſtraction.*

Pour la *Multiplication.*

Pour la *Diviſion.*

Et toutes ces operations ſont ſi aiſées, qu'on n'a jamais beſoin de rien eſſayer ni deviner, comme il faut faire dans la diviſion ordinaire. On n'a point beſoin non-plus de rien apprendre par cœur icy, comme il faut faire dans le calcul ordinaire, où il faut ſçavoir, par exemple, que 6 & 7 pris enſemble ſont 13, & que 5 multiplié par 3 donne 15, ſuivant la Table *d'une fois un eſt un*, qu'on appelle Pythagorique. Mais icy tout cela ſe trouve & ſe prouve de ſource, comme l'on voit dans les exemples précedens ſous les ſignes ☽ & ☉.

Abb. 6.1: G.W. Leibniz zum Zweiersystem

***b* = 10:** Das Zehnersystem ist unser heutiges, auf die Inder zurückgehendes System (vgl. Abschnitt 1.2)

***b* = 16:** Das *Sechzehnersystem* (*Hexadezimalsystem*) wird heute häufig zur Beschreibung der Byte-Struktur von Computern verwendet. Dabei werden jeweils 4 Bit zu einem Halbbyte zusammengeschaltet, das jeweils einen von 16 Zuständen („Werten“) annehmen kann. Als „Ziffern“ benutzt man im Hexadezimalsystem meist die 16 Symbole 0, 1, 2, ..., 9, A, B, C, D, E, F.

Schaltet man zwei Halbbytes, also 8 Bits, zu einer Einheit zusammen, so erhält man die als *Byte* bezeichnete Speichereinheit, die über viele Jahrzehnte hin-

weg weltweit fast durchgängig die Basis für den Computerbetrieb abgab. Jedes Byte kann also einen der 256 (= 16•16) Werte 00 bis FF annehmen.

Die Bedeutung der einzelnen Byte-Belegungen wurde im Rahmen des sogenannten ASCII-Code (American Standard Code for Information Interchange) festgelegt. Dabei verwendete man ursprünglich nur die 7 „niedrigst-wertigen" Bits eines Bytes zur Zeichen-Codierung (7-Bit-ASCII). Dies macht es möglich, 128 verschiedene Zeichen darzustellen. Bald erkannte man, dass dies nicht ausreichte, um die in nicht-englischen Sprachen mit lateinischem Grundalphabet vorkommenden speziellen Zeichen (wie z.B. Umlaute, „accents" und ähnliche Zeichen) darzustellen. Dies lies sich relativ leicht reparieren, indem man alle 8 Bits eines Bytes zur Codierung heranzog. Man konnte so 256 Zeichen darstellen. Als sich die Computer immer stärker verbreiteten, sah man sich gezwungen, vom 8-Bit-Codierungs-Prinzip abzurücken. Man entwarf einen neuen Standard, den *Unicode* Standard, mit dem neben mathematischen und technischen Zeichen auch die Zeichen aller anderer „lebenden" Sprachen (arabisch, asiatisch ...) darstellbar sein sollten. Die 2-Byte-Unicode-Codierung ermöglichte die Darstellung von 256 • 256 = 65536 Zeichen. Als man auch historische Schriften (wie z.B. die ägyptischen Hieroglyphen oder die babylonischen Keilschriftzeichen) in das Unicode-System integrieren wollte, musste man die 2-Byte-Codierung zu einer 4-Byte-Codierung erweitern. Damit ist die Darstellung von 4.294.967.296 Zeichen möglich und man hofft, dass dies ausreicht, um jedes jemals geschriebene Zeichen darstellen zu können[26]. In Abb. 1.2 sind beispielsweise die Ägyptischen Zahlzeichen für 1, 10, 100, 1000, 10000, 100000 und 1000000 mit ihren Unicode Werten dargestellt.

b = 20: Das System der *Maya* – siehe Abschnitt 1.2.

b = 60: Das *babylonische* System (ein noch nicht voll entwickeltes Stellenwertsystem) – siehe Abschnitt 1.2.

---

[26] Damit, dass man eine "Code-Nummer" für jedes mögliche Zeichen festlegt, ist das Gesamtproblem jedoch noch nicht gelöst. Zur Darstellung der Schriftzeichen benötigt man noch die graphische Fassung der Zeichen (in Form von Zeichentabellen), die es derzeit noch nicht für alle Unicode-Zeichen gibt.

Aufgabe 6.1: Informieren Sie sich (z.B. in Ziegenbalg 2010, Abschnitt 5.4) über Algorithmen zur Umwandlung von Stellenwertdarstellungen eines Stellenwertsystems in ein anderes System, und realisieren Sie die Algorithmen in einer geeigneten Programmiersprache.

6.2 Stellenwertdarstellung und Kongruenzen

Auch im Zusammenhang mit der Stellenwertdarstellung erweist sich das Rechnen mit Kongruenzen als sehr nützlich.

Hilfssatz: Es ist $b \equiv 1 \pmod{b-1}$ und $b \equiv -1 \pmod{b+1}$.

Beweis: Übung

Also gilt speziell: $10 \equiv 1 \pmod{9}$ und $10 \equiv -1 \pmod{11}$.

Folgerungen:

(1) $b^2 \equiv 1 (\text{mod } b-1),\ \ldots\ , b^n \equiv 1 (\text{mod } b-1)$

(2) $b^2 \equiv 1 (\text{mod } b+1),\ b^3 \equiv -1 (\text{mod } b+1),\ b^4 \equiv 1 (\text{mod } b+1),\ \ldots$
$b^n \equiv (-1)^n \pmod{b+1}$

Speziell im *Zehnersystem* gilt

(3) $10^2 \equiv 1 \pmod{9},\ \ldots,\ 10^n \equiv 1 \pmod{9}$

(4) $10^2 \equiv 1 (\text{mod } 11),\ 10^3 \equiv -1 (\text{mod } 11),\ 10^4 \equiv 1 (\text{mod } 11),\ \ldots$
$10^n \equiv (-1)^n \pmod{11}$

Definition 6.1: Die Stellenwertdarstellung der natürlichen Zahl n im b-System sei
$n = m_r \cdot b^r + m_{r-1} \cdot b^{r-1} + m_{r-2} \cdot b^{r-2} + \ldots + m_2 \cdot b^2 + m_1 \cdot b^1 + m_0 \cdot b^0$.
Als *b-Quersumme* von n wird die Summe der Ziffern von n bezeichnet:

$$Q_b(n) = m_r + m_{r-1} + m_{r-2} + \ldots + m_2 + m_1 + m_0 .$$

Die *alternierende b-Quersumme* von n ist folgendermaßen definiert:

$$Q'_b(n) = m_0 - m_1 + m_2 - m_3 + m_4 - \ldots + m_{2i} - m_{2i+1} + \ldots + (-1)^r m_r .$$

Im Zehnersystem schreibt man kürzer $Q(n)$ an Stelle von $Q_{10}(n)$ und

$Q'(n)$ an Stelle von $Q'_{10}(n)$ und spricht kurz von der Quersumme statt von der 10-Quersumme.

Satz 6.2 (Quersummenregel):
Mit den obigen Bezeichnungen gilt:
$n \equiv Q_b(n) \pmod{b-1}$ und
$n \equiv Q'_b(n) \pmod{b+1}$.

Beweis:
$$n = m_r \cdot b^r + m_{r-1} \cdot b^{r-1} + m_{r-2} \cdot b^{r-2} + \ldots + m_2 \cdot b^2 + m_1 \cdot b^1 + m_0 \cdot b^0$$
Der Beweis beruht fast gänzlich auf der Verträglichkeit der Kongruenzrelation mit den arithmetischen Operationen.

Erinnerung: Aus $b \equiv 1 \pmod{b-1}$ folgt $b^k \equiv 1 \pmod{b-1}$ für beliebiges $k \in \mathbb{N}$.

Daraus folgt: $m_k \cdot b^k \equiv m_k \pmod{b-1}$ und schließlich (formal mit vollständiger Induktion):
$$n = \sum_{k=0}^{r} m_k \cdot b^k \equiv \sum_{k=0}^{r} m_k = Q_b(n) \pmod{b-1}.$$

Folgerung: Im Zehnersystem gilt $n \equiv Q(n) \pmod 9$ und entsprechend $n \equiv Q'(n) \pmod{11}$.

Folgerungen (Teilbarkeitsregeln):

(1) Eine Zahl ist durch 9 teilbar, wenn ihre Quersumme durch 9 teilbar ist.

(2) Eine Zahl ist durch 11 teilbar, wenn ihre alternierende Quersumme durch 11 teilbar ist.

6.3 Rechenproben – eine Anwendung mit historischer Bedeutung

Diese Folgerungen ermöglichen im Zehnersystem die historisch und vom Schulunterricht her wohlbekannte „*Neunerprobe*“.

Es seien x und y natürliche Zahlen, deren Produkt $x \cdot y$ zu berechnen ist.

Es gilt: $x \equiv Q(x)\,(\text{mod}9)$, $y \equiv Q(y)\,(\text{mod}9)$ und $x \cdot y \equiv Q(x \cdot y)\,(\text{mod}9)$.
Weiterhin gilt wegen der Verträglichkeit der Kongruenzrelation mit der Multiplikation: $x \cdot y \equiv Q(x) \cdot Q(y) \pmod 9$.

Daraus folgt: $Q(x) \cdot Q(y) \equiv Q(x \cdot y) \pmod 9$.

Dies ermöglicht die folgende Rechenprobe: Gegeben x und y.

(1.) Berechne das Produkt $x \cdot y$.
(2.) Berechne die Quersummen $Q(x), Q(y)$ und $Q(x \cdot y)$.
(3.) Berechne das Produkt der Quersummen: $Q(x) \cdot Q(y)$.
(4.) Prüfe: $Q(x) \cdot Q(y) \equiv Q(x \cdot y) \pmod 9$.

Ist die Gleichung in (4.) verletzt, so ist die Rechnung fehlerhaft. Ist die Gleichung nicht verletzt, so erhöht dies die Plausibilität, dass die Rechnung richtig war (es ist aber kein definitiver Beweis für die Richtigkeit der Rechnung).

Beispiel: Stimmt die Rechnung $523 \cdot 9874 = 5164102$?

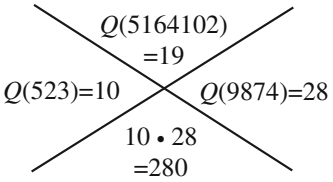
$Q(523) = 10$, $Q(9874) = 28$ und $Q(5164102) = 19$

$Q(523) \cdot Q(9874) = 10 \cdot 28 = 280$

$280 \equiv 19 \pmod 9$, denn $280 - 19 = 261$ und 261 wird von 9 geteilt.

Die Rechnung ist also nicht falsifiziert; der Grad der Plausibilität, dass die Rechnung richtig ist, hat sich durch die Probe erhöht.

Schematisch wird die Rechenprobe oft wie in der nebenstehenden Graphik dargestellt:



Historische Darstellung nach *Adam Ries* (1492–1559)

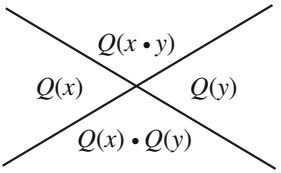


Abb. 6.2: Rechenprobe
Deutsche Bundespost 1959

Bemerkung: Die Vorgehensweise im Zusammenhang mit der Rechenprobe war in mehrfacher Hinsicht exemplarisch:

1. Analog zur Multiplikation funktioniert die Probe auch mit der Addition bzw. Subtraktion (die Methode erweist sich aber bei der Multiplikation am nützlichsten).
2. Analog zur Neunerprobe (mit Hilfe der Quersumme) kann man auch die Elferprobe (mit der alternierenden Quersumme) durchführen.
3. Analog zur Basis 10 funktionieren die Rechenproben auch im b-System mit $b-1$ an Stelle von 9 und $b+1$ an Stelle von 11.
4. Man kann von der Quersumme $Q(n)$ wieder die Quersumme $Q(Q(n))$ bilden, u.s.w. Man nennt dies die *iterierte Quersumme* von n. Es gilt dann aus denselben Gründen wie im Falle der einfachen Quersumme $n \equiv Q(n) \equiv Q(Q(n)) \equiv Q(Q(Q(n))) \equiv ... \equiv Q^k(n)$. Die Rechenproben lassen sich auch mit der iterierten Quersumme durchführen.
5. Falsche Rechnungen werden durch die Neunerprobe nicht aufgedeckt, wenn sich das (falsche) Ergebnis um ein Vielfaches von 9 vom richtigen Ergebnis unterscheidet.

   Ein *Beispiel*: $23 \cdot 76 = 1784$?

   Neunerprobe: $Q(23) \cdot Q(76) = 5 \cdot 13 = 65$; $Q(1784) = 20$;

   $65 \equiv 20 \pmod 9$, aber das Ergebnis war falsch; korrekt ist: $23 \cdot 76 = 1748$.

Aufgabe 6.2: Erläutern Sie, ob und ggf. zu welcher Rechnung Abb. 6.3 als Rechenprobe zu verstehen ist.

Abb. 6.3: Rechenprobe
Deutsche Bundespost 1992

Bemerkung: Die Quersumme von 10, 100, 1000, 10000 ist jeweils 1. Man kann sich also vorstellen, dass man jedes (additiv) in einer Zahl steckende Zehner-, Hunderter-, Tausender-, Zehntausender-Paket durch 1 ersetzt, um zur Quersumme dieser Zahl zu gelangen. An Stelle von 10, 100, 1000, 10000 nimmt man jeweils nur die 1. Man „wirft" also jeweils 9, 99, 999, 9999 „weg", wenn man zur Quersumme einer Zahl übergeht. Dies ist offenbar der Grund dafür, warum man die Quersummenbildung (bzw. die damit verbundenen Rechenproben) im englischen Sprachraum auch als „casting out nines" bezeichnet.

Weitere Rechenproben

Satz 6.3 (Endstellen-Regeln):

Die Darstellung der Zahl n im Zehnersystem sei

$$n = m_r \cdot 10^r + m_{r-1} \cdot 10^{r-1} + m_{r-2} \cdot 10^{r-2} + \ldots + m_2 \cdot 10^2 + m_1 \cdot 10 + m_0 .$$

Dann gilt:

- Die Zahl n ist genau dann durch 2 teilbar, wenn ihre letzte Ziffer m_0 durch 2 teilbar ist.
- Die Zahl n ist genau dann durch 5 teilbar, wenn ihre letzte Ziffer m_0 durch 5 teilbar ist.
- Die Zahl n ist genau dann durch 4 teilbar, wenn ihr „Zweier-Ende" $m_1 \cdot 10 + m_0$ durch 4 teilbar ist.
- Die Zahl n ist genau dann durch 25 teilbar, wenn ihr „Zweier-Ende" $m_1 \cdot 10 + m_0$ durch 25 teilbar ist.

Beweis: Die Endstellen-Regeln folgen unmittelbar aus den Grundeigenschaften der Teilbarkeitsrelation. An dieser Stelle sei exemplarisch der Beweis für die dritte Regel ausgeführt.

Wir betrachten dazu die Zahl

$$n' = m_r \cdot 10^r + m_{r-1} \cdot 10^{r-1} + m_{r-2} \cdot 10^{r-2} + \ldots + m_2 \cdot 10^2 .$$

Sie ist unabhängig von den Ziffern n_i stets durch 4 teilbar, denn man kann den Faktor 100 aus der Summe ausklammern. Also ist n genau dann durch 4 teilbar, wenn $n - n'$ $(= m_1 \cdot 10 + m_0)$ durch 4 teilbar ist.

Aufgabe 6.3: Formulieren und beweisen Sie allgemeine Quersummengesetze und Rechenproben für Zahlen und Rechnungen im *b*-System.

7 Die Sätze von Euler, Fermat und Wilson

7.1 Die Eulersche φ-Funktion („Eulersche Totientenfunktion“)

Definition 7.1:

1. Unter einer *zahlentheoretischen Funktion* versteht man eine Funktion
$$f\colon \mathbb{N} \to \mathbb{R} \quad \text{oder} \quad f\colon \mathbb{N} \to \mathbb{C}\,.$$
2. Gilt für eine zahlentheoretische Funktion f für alle teilerfremden natürlichen Zahlen m und n
$$f(m \cdot n) = f(m) \cdot f(n)\,,$$
so nennt man die Funktion f *multiplikativ*.
3. Es sei n eine natürliche Zahl. Mit $\varphi(n)$ wird die Anzahl der zu n teilerfremden Zahlen zwischen 1 und n bezeichnet. Die Funktion φ heißt *Eulersche* φ*-Funktion* (gelegentlich auch Eulersche *Totientenfunktion*).

   Beispiel: Für $n = 12$ sind die entsprechenden teilerfremden Zahlen: 1, 5, 7, 11; also ist $\varphi(12) = 4$.

Bemerkung: Weitere multiplikative zahlentheoretische Funktionen sind (vgl. Abschnitt 2.4):

$\tau(n)$ = Anzahl der Teiler von n (Teilerzahl)

$\sigma(n)$ = Summe der Teiler von n (Teilersumme)

Satz 7.1 (Multiplikativität der Eulerschen φ-Funktion):
Die Eulersche φ-Funktion ist multiplikativ.

(In Anhang 8.4 ist ein ausführliches Zahlenbeispiel zur Multiplikativität der φ-Funktion gegeben.)

Beweis: Seien m und n teilerfremde natürliche Zahlen. Es ist zu zeigen: $\varphi(m \cdot n) = \varphi(m) \cdot \varphi(n)$. Wir ordnen die Zahlen 1 bis $m \cdot n$ entsprechend dem folgenden rechteckigen Schema an:

J. Ziegenbalg, *Elementare Zahlentheorie*, DOI 10.1007/978-3-658-07171-4_7

1	2	3	...	n
n+1	n+2	n+3	...	2n
2n+1	2n+2	2n+3	...	3n
...	...	...	...	...
(m-1)·n +1	(m-1)·n +2	(m-1)·n +3	...	m·n

Jede dieser Zahlen lässt sich eindeutig in der Form $q \cdot n + r$ mit $1 \le r \le n$ und $0 \le q \le m - 1$ schreiben.

Jede Spalte ist durch ihren „Anfangswert“ r $(1 \le r \le n)$ charakterisiert. Ist r teilerfremd zu n, so auch jede weitere Zahl in dieser Spalte. Denn diese Zahlen sind von der Form $q \cdot n + r$ mit $0 \le q \le m - 1$ und es ist

$$GGT(q \cdot n + r, n) = GGT((q-1) \cdot n + r, n) = \ldots = GGT(r, n).$$

In der ersten Zeile sind nach Definition der Eulerschen Funktion genau $\varphi(n)$ der Zahlen teilerfremd zu n. Folglich sind auch alle Zahlen der zugehörigen $\varphi(n)$ Spalten teilerfremd zu n.

Zwischenbehauptung: Jede dieser $\varphi(n)$ Spalten enthält $\varphi(m)$ zu m teilerfremde Zahlen.

Beweis der Zwischenbehauptung: Wir betrachten die durch das „Anfangselement“ r gekennzeichnete Spalte. Sie besteht aus den Elementen:

$$r,\ n + r,\ 2n + r,\ 3n + r,\ \ldots,\ (m-1) \cdot n + r. \qquad (*)$$

Keine zwei dieser Zahlen sind kongruent modulo m. Denn wäre etwa $q_1 \cdot n + r \equiv q_2 \cdot n + r \pmod{m}$, so würde daraus $q_1 \cdot n \equiv q_2 \cdot n \pmod{m}$ folgen, und somit wäre wegen der Teilerfremdheit von m und n: $q_1 \equiv q_2 \pmod{m}$. Da q_1 und q_2 jeweils zwischen 0 und $m-1$ liegen, würde daraus $q_1 = q_2$ folgen – im Widerspruch zur Voraussetzung, dass die beiden Zahlen verschieden sein sollten.

Modulo m gibt es genau die m verschiedenen Reste 0, 1, 2, ..., $m-1$. Die m Zahlen in (*) sind also modulo m ein vollständiges Restesystem; sie sind insgesamt modulo m kongruent zu den Zahlen 0, 1, 2, ... , $m-1$. Das heißt insbesondere, dass es unter den Zahlen in (*) genau $\varphi(m)$ gibt, die zu m teilerfremd sind.

In dem rechteckigen Zahlenschema gibt es also insgesamt $\varphi(n)$ Spalten mit jeweils $\varphi(m)$ Zahlen, (also insgesamt $\varphi(n)\cdot\varphi(m)$ Zahlen), von denen jede sowohl zu n als auch zu m teilerfremd ist. Dies sind also genau die zu $n\cdot m$ teilerfremden Zahlen und somit ist $\varphi(m\cdot n)=\varphi(m)\cdot\varphi(n)$.

Satz 7.2 (Die Eulersche φ-Funktion und Primzahlen):
Für jede Primzahl p ist $\varphi(p)=p-1$.

Beweis: Dies folgt unmittelbar aus dem Begriff der Primzahl.

Satz 7.3 (Die Eulersche φ-Funktion und Primzahlpotenzen):
Für jede Primzahl p und jede natürliche Zahl n gilt:
$\varphi(p^n)=p^n\cdot(1-\frac{1}{p})$.

Beweis: Von den Zahlen m mit $1\le m\le p^n$ besitzen genau die folgenden Zahlen einen von 1 verschiedenen Teiler mit p^n:

$p,\ 2p,\ 3p,\ 4p,\ \ldots,\ p^{n-1}\cdot p=p^n$.

Dies sind p^{n-1} Zahlen. Die anderen Zahlen zwischen 1 und p^n sind teilerfremd zu p^n. Ihre Anzahl ist: $p^n-p^{n-1}=p^n(1-\frac{1}{p})$.

Satz 7.4 (Produktformel für die Eulersche φ -Funktion):
Die natürliche Zahl n $(n>1)$ habe die Primfaktorzerlegung
$n=p_1^{m_1}\cdot p_2^{m_2}\cdot\ldots\cdot p_r^{m_r}$.
Dann ist $\varphi(n)=n\cdot(1-\frac{1}{p_1})\cdot(1-\frac{1}{p_2})\cdot\ldots\cdot(1-\frac{1}{p_r})$.

Beweis: Wegen der Multiplikativität der Eulerschen Funktion gilt:

$$\varphi(n)=\varphi(p_1^{m_1}\cdot p_2^{m_2}\cdot\ldots\cdot p_r^{m_r})=\varphi(p_1^{m_1})\cdot\varphi(p_2^{m_2})\cdot\ldots\cdot\varphi(p_r^{m_r})$$
$$=p_1^{m_1}\cdot(1-\frac{1}{p_1})\cdot p_2^{m_2}\cdot(1-\frac{1}{p_2})\cdot\ldots\cdot p_r^{m_r}\cdot(1-\frac{1}{p_r})$$
$$=n\cdot(1-\frac{1}{p_1})\cdot(1-\frac{1}{p_2})\cdot\ldots\cdot(1-\frac{1}{p_r}).$$

Satz 7.5 (Summenformel für die Eulersche φ -Funktion):
Für jede natürliche Zahl n gilt $\sum_{d \mid n} \varphi(d) = n$.

Ein *Beispiel*: $n = 12$

Teiler von 12: $d =$	1	2	3	4	6	12
$\varphi(d) =$	1	1	2	2	2	4

Beweis der Summenformel: Zunächst sei an das folgende Ergebnis aus Kapitel 3 erinnert (vgl. GGT-10): Ist $d = GGT(a,b)$, so ist $GGT(\frac{a}{d}, \frac{b}{d}) = 1$.

Wir zerlegen die Zahlen $1,2,3,\ldots,n$ in disjunkte (d.h. elementfremde) Klassen. Die Klassen sind so definiert, dass zu jedem Teiler t von n diejenigen Elemente $x \in \{1,2,3,\ldots,n\}$ in einer Klasse A_t zusammengefasst werden, für die $GGT(x,n) = t$ ist.

Dies sei zunächst am Beispiel $n = 20$ und $t = 4$ erläutert: $GGT(x,20) = 4$ ist erfüllt für die Zahlen 4, 8, 12 und 16; man erhält so die Klasse $A_4 = \{4,8,12,16\}$.

Führt man Entsprechendes mit jedem Teiler von n durch, so erhält man eine Klasseneinteilung, die im Falle $n = 20$ folgendermaßen tabellarisch dargestellt werden kann:

t	$A_t = \{x \in \{1,\ldots,n\} : GGT(x,n) = t\}$	$\frac{n}{t}$	zu $\frac{n}{t}$ teilerfremde Zahlen	$\varphi(\frac{n}{t})$	$\lvert A_t \rvert$
1	A_1 = {1, 3, 7, 9, 11, 13, 17, 19}	20	$= A_1$	8	8
2	A_2 = {2, 6, 14, 18}	10	{1, 3, 7, 9}	4	4
4	A_4 = {4, 8, 12, 16}	5	{1, 2, 3, 4}	4	4
5	A_5 = {5, 15}	4	{1, 3}	2	2
10	A_{10} = {10}	2	{1}	1	1
20	A_{20} = {20}	1	{1}	1	1
			Summen:	20	20

Wie das Beispiel zeigt, stellen die Mengen A_1, A_2, A_4, A_5, A_{10}, A_{20} eine Zerlegung der Menge $\{1,2,3,\ldots,20\}$ dar. Da im Beispiel stets

$|A_t| = \varphi(\frac{n}{t})$ gilt, lässt sich die Zahl $n = 20$ wie folgt zerlegen:

$$20 = \sum_{t \mid n} |A_t| = \sum_{t \mid n} \varphi(\frac{n}{t}) .$$

Nun zum allgemeinen Fall:

Für jeden Teiler t von n sei also $A_t = \{x \in \{1,\ldots,n\}: GGT(x,n) = t\}$. Für verschiedene Teiler t und s von n ist dann offenbar stets $A_t \cap A_s = \varnothing$. Jedes x mit $x \in \{1,...,n\}$ liegt in der Menge A_r, wo $r = GGT(x,n)$ ist. Also bilden die Mengen A_t eine Zerlegung der Menge $\{1,...,n\}$, d.h.

$$n = \sum_{t \mid n} |A_t| .$$

Nach (GGT-10) gilt: $GGT(x,n) = t \quad \Leftrightarrow \quad GGT(\frac{x}{t}, \frac{n}{t}) = 1$.

Also ist $|A_t| = \left| \left\{ x \in \{1,\ldots,n\}: \; GGT(\frac{x}{t}, \frac{n}{t}) = 1 \right\} \right| = \varphi\left(\frac{n}{t}\right)$.

Mit t durchläuft auch $\frac{n}{t}$ alle Teiler von n. Also ist $\sum_{d \mid n} \varphi(d) = \sum_{t \mid n} \varphi(\frac{n}{t})$.

Und daraus folgt schließlich $n = \sum_{t \mid n} |A_t| = \sum_{t \mid n} \varphi(\frac{n}{t}) = \sum_{d \mid n} \varphi(d)$.

7.2 Die Sätze von Euler und Fermat

Satz 7.6 (Satz von Euler):

Es sei n eine beliebige und a eine zu n teilerfremde natürliche Zahl. Dann gilt $a^{\varphi(n)} \equiv 1 \; (n)$.

Beweis: Nach Definition der Eulerschen Funktion gibt es $\varphi(n)$ verschiedene zu n teilerfremde Zahlen zwischen 1 und n; sie seien mit

$$r_1, r_2, \ldots, r_{\varphi(n)}$$

bezeichnet. Wir betrachten im Folgenden die Produkte $a \cdot r_1, a \cdot r_2, \ldots, a \cdot r_{\varphi(n)}$

Zwischenbehauptung 1: Für jedes $i \in \{1,\ldots,\varphi(n)\}$ gilt: $a \cdot r_i$ ist teilerfremd zu n.

Beweis: Besäßen $a \cdot r_i$ und n einen gemeinsamen Teiler t $(t > 1)$, so besäßen sie insbesondere einen gemeinsamen Primteiler p (aus der Primfaktorzerlegung von t). Da die Primzahl p das Produkt $a \cdot r_i$ teilt, müsste sie einen der Faktoren (a oder r_i) teilen. Dann wäre dieser Faktor aber, im Widerspruch zur Voraussetzung, nicht teilerfremd zu n.

Zwischenbehauptung 2: Für verschiedene Indizes $i, j \in \{1,\ldots,\varphi(n)\}$ ist stets $a \cdot r_i \neq a \cdot r_j \ (n)$.

Beweis: Aus $a \cdot r_i \equiv a \cdot r_j \ (n)$ folgt $a \cdot r_i - a \cdot r_j \equiv 0 \ (n)$; d.h. $a \cdot (r_i - r_j) \equiv 0 \ (n)$. Mit der Teilerfremdheit von a und n folgt hieraus (nach Kürzung mit a) $r_i - r_j \equiv 0 \ (n)$.

Die Zahl n ist also ein Teiler von $r_i - r_j$. Die (positiven) Zahlen r_i und r_j sind nach Definition beide kleiner als n. Ihre Differenz muss deshalb (betragsmäßig) auch kleiner als n sein. Da n diese Differenz teilt, muss die Differenz gleich Null sein. Mit anderen Worten: $r_i = r_j$.

Aus $a \cdot r_i \equiv a \cdot r_j \ (n)$ folgt also $r_i = r_j$, d.h., $i = j$.

Fortsetzung des Hauptbeweises: Aus den beiden Zwischenbehauptungen folgt, dass die Mengen $\{r_1, r_2, \ldots, r_{\varphi(n)}\}$ und $\{a \cdot r_1, a \cdot r_2, \ldots, a \cdot r_{\varphi(n)}\}$ modulo n übereinstimmen. Die jeweiligen Produkte der in diesen Mengen enthaltenen Elemente sind also kongruent modulo n:

$$r_1 \cdot r_2 \cdot \ldots \cdot r_{\varphi(n)} \equiv a \cdot r_1 \cdot a \cdot r_2 \cdot \ldots \cdot a \cdot r_{\varphi(n)} \ (n).$$

Daraus folgt:

$$r_1 \cdot r_2 \cdot \ldots \cdot r_{\varphi(n)} \equiv a^{\varphi(n)} \cdot r_1 \cdot r_2 \cdot \ldots \cdot r_{\varphi(n)} \ (n).$$

Da alle r_i (nach Definition) teilerfremd zu n sind, kann man mit diesen Faktoren kürzen; d.h., es folgt $1 \equiv a^{\varphi(n)} \ (n)$.

Folgerung („*Kleiner Fermatscher Satz*"): Es sei p eine Primzahl und a eine natürliche Zahl, die kein Vielfaches von p ist. Dann gilt $a^{p-1} \equiv 1 \quad (p)$.

Bemerkung: Der Eulersche Satz nimmt im Kontext der modernen Algebra (genauer: der Gruppentheorie) eine besonders klare und durchsichtige Form an. Er ist in diesem Zusammenhang als *Satz von Lagrange*[27] bekannt und lautet:

> *Die Ordnung jeder Untergruppe einer beliebigen (endlichen) Gruppe teilt stets die Ordnung der Gruppe.*

Aufgabe 7.1 (für Leser, die mit den Grundbegriffen der Gruppentheorie vertraut sind): Zeigen Sie

1. Im Restklassenring $\mathbb{Z}/n\mathbb{Z}$ bilden die zu n teilerfremden Restklassen mit der üblichen Restklassenmultiplikation (vgl. Kapitel 5) eine Gruppe. Sie wird auch als die Gruppe der *primen Restklassen* modulo n bezeichnet.
2. Sei G eine endliche Gruppe, $a \in G$ und $\langle a \rangle := \{a, a^2, a^3, \ldots, a^n, \ldots\}$. Zeigen Sie $\langle a \rangle$ ist eine Untergruppe von G.

Die von a $(a \neq 1)$ erzeugte Untergruppe der Gruppe der primen Restklassen habe die Ordnung k. Nach dem Satz von Lagrange ist dann k ein Teiler von $\varphi(n)$. Es sei $\varphi(n) = k \cdot s$. Dann gilt: $a^{\varphi(n)} = a^{k \cdot s} = (a^k)^s \equiv 1^s \equiv 1 \,(\text{mod } n)$.

Ein erster Primzahltest

Der kleine Fermatsche Satz kann bei der Suche nach Primzahlen auch als Test verwendet werden, um auszuschließen, dass eine natürliche Zahl n eine Primzahl ist. Man wähle eine natürliche Zahl a mit $1 < a < n$ und berechne $a^{n-1} \,(\text{mod } n)$. Ist letzteres von 1 verschieden (modulo n), dann kann n keine Primzahl sein.

---

[27] Joseph-Louis Lagrange: geb. 1736 in Turin, gest. 1813 in Paris; Mathematiker, Physiker, Astronom. Lagrange setzte sich u.a. auch stark für die Verbreitung des in Mitteleuropa heute weit verbreiteten metrischen Maß- und Gewichtssystems ein.

Wenn allerdings $a^{n-1} \equiv 1 \pmod{n}$ ist, so ist dies keine Garantie dafür, dass n eine Primzahl ist. So ist z.B. $3^{91-1} \equiv 1 \pmod{91}$, aber 91 (=7*13) ist keine Primzahl. Man bezeichnet 91 auch als *Pseudoprimzahl* zur Basis 3.

7.3 Der Satz von Wilson – ein Primzahlkriterium

Satz 7.7 (Satz von Wilson[28]):

Für jede Primzahl p gilt: $p \mid 1+(p-1)!$

Bzw. in gleichwertiger Formulierung: $(p-1)! \equiv -1 \ (p)$.

Bemerkung: Der Satz wurde (allerdings in der Form einer unbewiesenen Hypothese) bereits von dem arabischen Mathematiker *Ibn al-Haitam* (vgl. Kapitel 1) angewandt. Vollständig wurde der Satz (und seine Umkehrung – s.u.) erstmals 1773 von J.-L. Lagrange bewiesen.

Beweis: Nach Definition ist $(p-1)! = 1 \cdot 2 \cdot 3 \cdot \ldots \cdot (p-3) \cdot (p-2) \cdot (p-1)$.

Wir betrachten die Menge $M := \{2,3,\ldots,(p-3),(p-2)\}$ der von 1 und $p-1$ verschiedenen Faktoren im obigen Produkt.

Zwischenbehauptung: Modulo p besitzt jeder der Faktoren $a \in M$ ein multiplikativ Inverses b mit der Eigenschaft: $a \neq b$. Für das Zahlenpaar $\{a, b\}$ gilt also: $a \cdot b = b \cdot a \equiv 1 \ (p)$.

Die Gültigkeit der Zwischenbehauptung folgt aus dem Euklidischen Algorithmus und seinen Folgerungen (insbesondere der Vielfachsummendarstellung). Da p eine Primzahl ist, sind a und p teilerfremd; es gibt also ganze Zahlen x und y mit der Eigenschaft

$GGT(a,p) = 1 = x \cdot a + y \cdot p$.

Setzen wir $b := x$, und betrachten wir die daraus resultierende Gleichung modulo p, so folgt daraus: $1 \equiv b \cdot a \ (p)$; a und b sind also „modulo p zueinander invers".

Es bleibt zu zeigen: $a \neq b$. Wäre $a = b$, so hieße das $a^2 \equiv 1 \ (p)$. Daraus würde aber folgen $a^2 - 1 = (a-1) \cdot (a+1) \equiv 0 \ (p)$, also

[28] John Wilson (1741–1793) englischer Mathematiker

$p \mid (a-1)\cdot(a+1)$ und somit $p \mid (a-1)$ oder $p \mid (a+1)$. Wegen $2 \le a \le p-2$ liegen aber die beiden Faktoren $(a-1)$ und $(a+1)$ zwischen 1 und $(p-1)$ und es ist unmöglich, dass sie von p geteilt werden.

Damit ist die Zwischenbehauptung bewiesen.

Zurück zum Hauptbeweis des Wilsonschen Satzes: Modulo p betrachtet, lassen sich in dem Produkt $1\cdot 2\cdot 3\cdot\ldots\cdot(p-3)\cdot(p-2)\cdot(p-1)$ alle Faktoren, mit Ausnahme der Faktoren 1 und $(p-1)$, zu „inversen Paaren“ zusammenfassen; d.h.,

$$(p-1)! = 1\cdot 2\cdot 3\cdot\ldots\cdot(p-3)\cdot(p-2)\cdot(p-1) \equiv p-1 \equiv -1\,(p).$$

Beispiel: Für $p = 13$ gilt

$2\cdot 7 = 14 = 1\cdot 13+1 \equiv 1\ (13)$,
$3\cdot 9 = 27 = 2\cdot 13+1 \equiv 1\ (13)$,
$4\cdot 10 = 40 = 3\cdot 13+1 \equiv 1\ (13)$,
$5\cdot 8 = 40 \equiv 1\ (13)$,
$6\cdot 11 = 66 = 5\cdot 13+1 \equiv 1\ (13)$.

Also ist $(13-1)! = 12! = 1\cdot 2\cdot 3\cdot 4\cdot 5\cdot 6\cdot 7\cdot 8\cdot 9\cdot 10\cdot 11\cdot 12$

$= 1\cdot(2\cdot 7)\cdot(3\cdot 9)\cdot(4\cdot 10)\cdot(5\cdot 8)\cdot(6\cdot 11)\cdot 12 \equiv 1\cdot 12 \equiv -1 \quad (13)$.

Probe: $12! = 479001600 = 36846277\cdot 13 - 1 \equiv -1 \quad (13)$

Bemerkung: Es gilt auch die Umkehrung des Wilsonschen Satzes; d.h., es gilt insgesamt der

Satz 7.8 (Ein Primzahlkriterium):

Für jede natürliche Zahl n $(n>1)$ gilt:

n ist eine Primzahl $\Leftrightarrow$ $(n-1)! \equiv -1\ (n)$.

Bemerkung: In dieser Form ist der Satz von Wilson eines der ältesten *Primzahlkriterien*.

Beweis: Der Aussageteil „$\Rightarrow$“ stellt genau den soeben bewiesenen Wilsonschen Satz dar.

Zum Aussageteil „$\Leftarrow$“: Sei also n eine natürliche Zahl $(n>1)$ mit der Eigenschaft $(n-1)! \equiv -1\ (n)$. Es ist zu zeigen, dass n dann eine Primzahl ist. Wäre n zusammengesetzt, etwa $n = a\cdot b$, so würden in dem Produkt $(n-1)! = 1\cdot 2\cdot 3\cdot\ldots\cdot(n-2)\cdot(n-1)$ die Faktoren a und b auftreten; das Produkt wäre damit ein Vielfaches von n, also kongruent zu 0 modulo n und

nicht, wie vorausgesetzt, kongruent zu -1 modulo n. Also kann n nicht zusammengesetzt sein, d.h. n ist eine Primzahl.

Beispiele zur Anwendung des Wilsonschen Satzes als Primzahlkriterium:

Beispiel 1: (Als Hilfsmittel wird ein Computeralgebra System verwendet)

Ist 133 eine Primzahl? Es ist:

(133-1)! = 111824865119600430744996307607616902997562475571842633838412167568361169672820118454045730260688510087990927196104962685462595837360336094267205134948250389032461924909766607715924086489297715200000000000000000000000000000000000

Direktes Nachrechnen ergibt: $(133-1)! \equiv 0 \pmod{133}$; 133 ist also keine Primzahl.

Bemerkung: Der Wert der Fakultätsfunktion $f(n) = n!$ wird durch wiederholtes Multiplizieren ermittelt. Reduziert man die Zwischenergebnisse nach jedem Rechenschritt sofort modulo n, so erhält man das Ergebnis $(133-1)! \equiv 0 \pmod{133}$ mit sehr viel geringerem Rechenaufwand.

Konkret erkennt man bei diesem Beispiel sehr schnell, dass 133 das Produkt der Zahlen 7 und 19 ist. Beim fortlaufenden Ausmultiplizieren von 132! erhält man also im Falle der sofortigen Reduktion modulo 133 beim Faktor 19 (nachdem der Faktor 7 schon „dran" war) das Ergebnis Null (modulo 133). Es ist klar, dass damit auch das Gesamtprodukt 132! gleich Null (modulo 133) sein muss – und man braucht nicht weiterzurechnen.

Beispiel 2: Ist 97 eine Primzahl? Es ist:

96! = 99167793487094968920957140154189380115818364865126779544437605483849222280909149998768947603700074898207509473896575430563987456000000000000000000000000

Auch in diesem Fall erhält man durch sofortige Reduktion der Zwischenergebnisse modulo 97 das Ergebnis $96! \equiv 96 \pmod{97} \equiv -1 \pmod{97}$; 97 ist also eine Primzahl.

Diese (sehr kleinen) Beispiele zeigen aber bereits, dass der Rechenaufwand für die Anwendung des Wilsonschen Satzes erheblich ist; dies schmälert die Nützlichkeit dieses Primzahlkriteriums deutlich.

8 Anhänge

8.1 Allgemeine Beweisprinzipien und Beweisverfahren

Das Prinzip des „tertium non datur“

Jede Aussage A ist entweder *wahr* oder *falsch*; es gibt kein „drittes“ (lateinisch: *tertium non datur*).

Dies gilt unabhängig davon, ob die Wahrheit oder Falschheit der Aussage zu einem bestimmten Zeitpunkt bekannt ist. So ist z.B. bis heute der Status (ob wahr oder falsch) der „Goldbachschen Vermutung“ nicht bekannt; dennoch geht man davon aus, dass *eines* davon zutrifft, dass sie also entweder wahr oder falsch ist.

Die *Goldbachsche Vermutung* besagt (vgl. Abschnitt 4.9): Jede gerade Zahl (die größer ist als 2) lässt sich als Summe zweier Primzahlen schreiben.

Nach dem Prinzip des *tertium non datur* gilt: Ist die Aussage A wahr, so ist die Aussage (nicht A) falsch – und umgekehrt. Dies führt zum folgenden Beweisverfahren des *indirekten Beweises* bzw. *Widerspruchsbeweises*.

Indirekter Beweis / Widerspruchsbeweis

Die Gültigkeit (Wahrheit) einer Aussage A ist zu zeigen.

Man nimmt an, dass die Aussage A falsch (und somit die Aussage „nicht A“ wahr) ist – und leitet aus dieser Annahme einen Widerspruch her. Wenn die gesamte Schlusskette korrekt ist, dann kann der Widerspruch nur daher kommen, dass die gemachte Annahme (A ist falsch) selbst falsch ist; und damit muss nach dem Prinzip vom *tertium non datur* die Aussage A wahr sein.

Ein klassisches Beispiel für den Widerspruchsbeweis ist der folgende

Satz 8.1 (Irrationalität von $\sqrt{2}$):
Ist a eine reelle Zahl mit der Eigenschaft $a \cdot a = 2$, dann ist a irrational.
(Mit anderen Worten: $\sqrt{2}$ ist irrational.)

Beweis: Wir nehmen im Widerspruch zur Aussage des Satzes an, die Zahl a sei nicht irrational, d.h. sie sei rational. Dann lässt sie sich schreiben als

J. Ziegenbalg, *Elementare Zahlentheorie*, DOI 10.1007/978-3-658-07171-4_8

$a = \frac{p}{q}$ mit ganzen Zahlen p und q. Wir können annehmen, dass die Zahlen p und q teilerfremd sind, d.h., dass also der Bruch $\frac{p}{q}$ in „gekürzter Form" geschrieben ist (denn wäre dies nicht der Fall, dann könnte man den Bruch ja kürzen und dann mit dem gekürzten Bruch weiterarbeiten). Nun ist $a^2 = 2 = \frac{p^2}{q^2}$, also $p^2 = 2q^2$. Da p^2 eine gerade Zahl ist, muss auch p gerade sein, denn wäre p ungerade, so wäre auch p^2 ungerade – das Produkt zweier ungerader Zahlen ist stets ungerade (Übung!). Da p also gerade ist, lässt es sich schreiben als $p = 2r$ mit einer geeigneten natürlichen Zahl *r*. Aus $p^2 = 2q^2$ folgt dann $4r^2 = 2q^2$, d.h. $2r^2 = q^2$. Das heißt, q^2 ist eine gerade Zahl und somit ist (wie oben im Falle von p^2) auch q gerade. Somit sind p und q beides gerade Zahlen. Dies steht aber im Widerspruch zu der Annahme, dass der Bruch $\frac{p}{q}$ eine Darstellung des Bruches a in gekürzter Form sei.

Der Widerspruch resultiert aus der Annahme, dass a eine rationale Zahl sei. Diese Annahme ist also zu verwerfen, d.h. die Zahl a muss eine irrationale Zahl sein.

Beweis mit Hilfe von Fallunterscheidungen

Die Gültigkeit (Wahrheit) eines Schlusses „aus A folgt B" (symbolisch $A \Rightarrow B$) ist zu zeigen. Zerfällt die Aussage A in die Teilaussagen A_1, A_2, …, A_n, genauer: ist A gleichwertig zur Aussage „A_1 oder A_2 oder A_3 oder ... oder A_n" (symbolisch: $A \Leftrightarrow A_1 \vee A_2 \vee \ldots \vee A_n$) und gilt $A_i \Rightarrow B$ für alle $i = 1,\ldots n$ dann gilt auch $A \Rightarrow B$.

*Bemerkung*en: In den meisten konkreten Anwendungen hat man es mit einem (exklusiven) „oder" im Sinne von „entweder-oder" zu tun; für die Anwendbarkeit des Prinzips der Fallunterscheidung ist dies aber irrelevant.

Satz 8.2 (Endziffern von Quadratzahlen):
Keine Quadratzahl hat im Zehnersystem die Endziffer 8.

Beweis: Die Quadratzahl sei a^2. Wir betrachten die möglichen Endziffern von a.

Fall 1: Die Endziffer von a ist ungerade. Dann ist auch die Endziffer von a^2 ungerade.

Fall 2: Die Endziffer von a ist 0. Dann ist auch die Endziffer von a^2 gleich 0.

Fall 3: Die Endziffer von a ist 2 oder 8. Dann ist die Endziffer von a^2 gleich 4.

Fall 4: Die Endziffer von a ist 4 oder 6. Dann ist die Endziffer von a^2 gleich 6.

Beweis der Gleichwertigkeit zweier Aussagen

Es seien A und B zwei beliebige Aussagen. Man sagt: A ist *gleichwertig* zu B oder A ist *äquivalent* zu B (symbolisch $A \Leftrightarrow B$), wenn folgendes gilt:

(1.) Aus A folgt B (symbolisch $A \Rightarrow B$) und

(2.) aus B folgt A (symbolisch $B \Rightarrow A$).

Beweis der Gleichheit zweier Mengen

Der Beweis für die Gleichheit zweier Mengen A und B (symbolisch $A = B$) wird oft dadurch geführt, dass man zeigt:

(1.) Die Menge A ist eine Teilmenge von B (symbolisch $A \subseteq B$) und

(2.) die Menge B ist eine Teilmenge von A (symbolisch $B \subseteq A$).

8.2 Axiomatische Beschreibung der natürlichen Zahlen und das Prinzip der vollständigen Induktion

Eines der wichtigsten Objekte der Mathematik (und insbesondere auch der „Rohstoff“ für die Zahlentheorie) sind die **natürlichen Zahlen**. Sie sind konstruktiv beschrieben durch die Axiome von *G. Peano*[29]. Im Folgenden ist der Aufbau der natürlichen Zahlen in der Formulierung von *E. Landau*[30], aus dem Jahre 1929 wiedergegeben:

Axiom 1: 1 ist eine natürliche Zahl.
(Die Menge der natürlichen Zahlen ist also insbesondere nicht leer. Sie enthält ein Ding, das 1 heißt.)

Axiom 2: Zu jeder natürlichen Zahl x gibt es genau eine natürliche Zahl, die der Nachfolger von x heißt und mit x’ bezeichnet werden möge.

Axiom 3: Stets ist $x' \neq 1$.
(Es gibt also keine natürliche Zahl, deren Nachfolger 1 ist.)

Axiom 4: Aus $x' = y'$ folgt $x = y$.
(Mit anderen Worten: unterschiedliche natürliche Zahlen haben unterschiedliche Nachfolger.)

Axiom 5 (Induktionsaxiom): Es sei $\mathcal{M}$ eine Menge natürlicher Zahlen mit den Eigenschaften:

(1) 1 gehört zu $\mathcal{M}$.

(2) Wenn x zu $\mathcal{M}$ gehört, so gehört x’ zu $\mathcal{M}$.

Dann umfasst $\mathcal{M}$ alle natürlichen Zahlen.

Vollständige Induktion

Eine besondere Rolle in der Definition der natürlichen Zahlen spielt Axiom 5, das *Induktionsaxiom*. Diejenige mathematische Beweistechnik, die auf der Verwendung des Induktionsaxioms beruht, nennt man die *vollständige Induktion* (im Kontrast zu der aus den empirischen Wissenschaften bekannten sogenannten „unvollständigen“ Induktion). Praktisch jeder Beweis über natürliche Zahlen (und darüber hinaus noch viele andere) beruht direkt oder indirekt auf dem Prinzip der vollständigen Induktion. Jeder Beweis, der auf dem In-

[29] Giuseppe Peano (1858–1932), italienischer Mathematiker
[30] Edmund Landau (1877–1938), deutscher Mathematiker

duktionsaxiom aufbaut, muss strukturell aus den folgenden Teilen bestehen.

Kontext: Eine Aussage $\mathcal{A} = \mathcal{A}(n)$ über natürliche Zahlen ist zu beweisen. Zunächst wird $\mathcal{M}$ als die Menge derjenigen natürlichen Zahlen definiert, welche die Aussage $\mathcal{A}$ erfüllen.

1. Es ist zu zeigen, dass die Zahl 1 zu $\mathcal{M}$ gehört. Dieser Schritt wird im Folgenden als *Induktionsverankerung* (IV) bezeichnet.
2. Es ist zu zeigen: Wenn eine natürliche Zahl x zu $\mathcal{M}$ gehört, so gehört auch stets deren Nachfolger *x'* zu $\mathcal{M}$. Dieser Schritt wird im Folgenden als *Induktionsschritt* (IS) bezeichnet. Im Induktionsschritt ist unter Verwendung von Axiom 5 zu zeigen, dass für jede beliebige natürliche Zahl x gilt:

   Aus der *Induktionsannahme* „x gehört zu $\mathcal{M}$“ folgt der
   Induktionsschluss „der Nachfolger *x'* von x gehört ebenfalls zu $\mathcal{M}$“

Bemerkungen:

1. Die axiomatische Beschreibung der natürlichen Zahlen formalisiert den Zählprozess:

   1 (ist vorgegeben), 2 := 1', 3 := 2', 4 := 3', u.s.w.
2. Wenn später die Addition der durch die Peano-Axiome definierten natürlichen Zahlen eingeführt worden ist, schreibt man dann meist $x+1$ an Stelle von *x'*.

Einige Beispiele zur vollständigen Induktion

Die Zahlenbeispiele

$$\begin{aligned} 1^3+2^3 &= 9 = 3^2 \\ 1^3+2^3+3^3 &= 36 = 6^2 \\ 1^3+2^3+3^3+4^3 &= 100 = 10^2 \\ 1^3+2^3+3^3+4^3+5^3 &= 225 = 15^2 \\ 1^3+2^3+3^3+4^3+5^3+6^3 &= 441 = 21^2 \end{aligned}$$

legen die Vermutung nahe, dass für alle natürlichen Zahlen n die Gleichung

$$1^3+2^3+\ldots+n^3=(1+2+\ldots+n)^2 \qquad (*)$$

gilt.

Wir beweisen dies mit Hilfe der vollständigen Induktion: Es sei $\mathcal{M}$ die Menge der natürlichen Zahlen, für welche die Gleichung (*) gilt.

Induktionsverankerung: Die Zahl 1 gehört zu $\mathcal{M}$, denn es ist $1^3 = 1^2$.

Induktionsschritt: Zu zeigen ist: Aus der

Induktionsannahme: Die natürliche Zahl k gehört zu $\mathcal{M}$.

folgt der

Induktionsschluss: Die natürliche Zahl $k+1$ gehört ebenfalls zu $\mathcal{M}$.

Es gelte also $1^3 + 2^3 + \ldots + k^3 = (1 + 2 + \ldots + k)^2$. Dann ist

$$\begin{aligned}
1^3 + 2^3 + \ldots + k^3 + (k+1)^3 &= (1 + 2 + \ldots + k)^2 + (k+1)^3 \\
&= \left(\frac{k \cdot (k+1)}{2}\right)^2 + (k+1)^3 \\
&= \frac{k^2 \cdot (k+1)^2 + 4 \cdot (k+1)^3}{4} \\
&= \frac{(k^2 + 4k + 4) \cdot (k+1)^2}{4} \\
&= \frac{(k+2)^2 \cdot (k+1)^2}{4} \\
&= \left(\frac{(k+2) \cdot (k+1)}{2}\right)^2 \\
&= (1 + 2 + \ldots + (k+1))^2 .
\end{aligned}$$

Aus der Tatsache, dass die behauptete Aussage (*) für die beliebige natürliche Zahl k gilt, folgt also, dass sie auch für $k+1$ gilt. Damit gilt die Aussage nach dem Induktionsaxiom für alle natürlichen Zahlen.

Aufgabe 8.1: Beweisen Sie mit vollständiger Induktion die Aussage:

Für jede natürliche Zahl n gilt: $2^n = (2^0 + 2^1 + 2^2 + \ldots + 2^{n-1}) + 1$.

Bemerkung: Die Induktionsverankerung erfolgt meist bei der Zahl 1; gelegentlich aber auch bei der Zahl 0. Sie kann aber im Prinzip bei jeder natürlichen (oder ganzen) Zahl b beginnen. Die Aussage gilt dann eben für alle natürlichen (bzw. ganzen) Zahlen größer oder gleich *b*.

Aufgabe 8.2: Die Gleichung $2^n > n^2$ gilt für alle natürlichen Zahlen ober-

halb einer bestimmten Grenze b. Bestimmen Sie diese Grenze und beweisen Sie die Aussage mit vollständiger Induktion.

Beweise mit vollständiger Induktion kommen auch in Situationen vor, die nicht so offensichtlich mit den natürlichen Zahlen zusammenhängen.

Aufgabe 8.3: Zeigen Sie (vgl. Skizze): Eine Landkarte, deren Ländergrenzen aus (endlich vielen) Geraden besteht, die von Rand zu Rand verlaufen, lässt sich mit zwei Farben so färben, dass benachbarte Länder stets verschieden gefärbt sind.

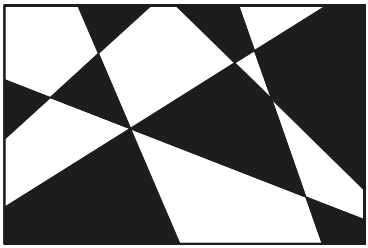


Abb. 8.01: zweifarbige Landkarte

Wie jedes Beweisprinzip, so ist auch das Prinzip der vollständigen Induktion nicht frei von der Gefahr, in Scheinbeweisen verwendet zu werden. Ein Beispiel:

„Satz 8.3“: Alle Knöpfe haben dieselbe Farbe.

„Beweis“: Wir betrachten n-elementige Mengen von Knöpfen und zeigen, dass alle Knöpfe in einer beliebigen solchen n-elementigen Menge dieselbe Farbe haben.

Induktionsverankerung: In jeder ein-elementigen Menge haben alle Knöpfe trivialerweise dieselbe Farbe.

Induktionsschluss: Wir nehmen an, die Aussage gelte für beliebige k-elementige Mengen und zeigen, dass sie auch für beliebige $(k+1)$-elementige Mengen gilt. Sei also eine beliebige $(k+1)$-elementige Menge von Knöpfen gegeben. Wir stellen uns die Knöpfe entlang einer Geraden angeordnet vor.

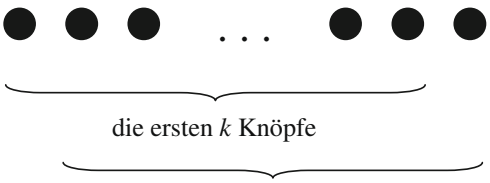


Abb. 8.02: gleichfarbige Knöpfe

Wir fassen nun, wie in der Abbildung angedeutet, die ersten k Knöpfe und die letzten k Knöpfe zusammen. Nach Induktionsvoraussetzung haben die ersten k Knöpfe dieselbe Farbe; entsprechendes gilt für die letzten k Knöpfe. Der zweite Knopf gehört zu beiden Mengen. Also haben alle Knöpfe in der ersten Menge dieselbe Farbe wie der zweite Knopf – und ebenso alle Knöpfe in der zweiten Menge – und somit haben alle Knöpfe in der $(k+1)$-elementigen Menge dieselbe Farbe.

Aufgabe 8.4: Decken Sie den Fehler im „Knopf"-Beweis auf.

Auch in humoristischen Beweisvarianten kommt die vollständige Induktion vor:

„Satz 8.4": Jeder Koffer fasst unendlich viele Taschentücher.

„Beweis": Dass jeder Koffer ein Taschentuch fasst, ist klar. Und wenn schon eine bestimmte Menge von Taschentüchern im Koffer ist, so geht ein Taschentuch immer noch hinein.

Aufgabe 8.5: Betrachten Sie die folgenden Summen:

$$\begin{aligned} Q_1 &= 1^2 \\ Q_2 &= 1^2 - 2^2 \\ Q_3 &= 1^2 - 2^2 + 3^2 \\ Q_4 &= 1^2 - 2^2 + 3^2 - 4^2 \\ Q_5 &= 1^2 - 2^2 + 3^2 - 4^2 + 5^2 \end{aligned}$$

Berechnen Sie konkrete Zahlenwerte und stellen Sie eine „allgemeine Formel" für Q_n auf.

Aufgabe 8.6: Betrachten Sie die folgenden Summen:

$$\begin{aligned} S_1 &= 1\cdot 2 \\ S_2 &= 1\cdot 2+2\cdot 3 \\ S_3 &= 1\cdot 2+2\cdot 3+3\cdot 4 \\ S_4 &= 1\cdot 2+2\cdot 3+3\cdot 4+4\cdot 5 \\ S_5 &= 1\cdot 2+2\cdot 3+3\cdot 4+4\cdot 5+5\cdot 6 \end{aligned}$$

Berechnen Sie konkrete Zahlenwerte und stellen Sie eine „allgemeine Formel" für S_n auf.

Aufgabe 8.7: Zeigen Sie mit Hilfe von vollständiger Induktion:

$$\frac{1}{1\cdot 2}+\frac{1}{2\cdot 3}+\frac{1}{3\cdot 4}+\ldots+\frac{1}{n\cdot(n+1)}=\frac{n}{n+1}$$

Weitere Beweisprinzipien für Aussagen über natürliche Zahlen

Das Prinzip der vollständigen Induktion kommt in verschiedenen Spielarten vor; eine davon wird als das *Prinzip vom kleinsten El*ement, oder noch griffiger, als das *Prinzip vom kleinsten Verbrecher* bezeichnet. Es beruht auf dem folgenden

Satz 8.5 (Satz vom kleinsten Element):
Jede nichtleere Menge natürlicher Zahlen besitzt ein kleinstes Element.

Aufgabe 8.8: Beweisen Sie den Satz vom kleinsten Element mit vollständiger Induktion.

Dieses Prinzip wird meist nach dem folgenden Muster im Zusammenhang mit Widerspruchsbeweisen verwendet: Man möchte eine mathematische Aussage über natürliche Zahlen beweisen (z.B. den Fundamentalsatz der Zahlentheorie). Im Sinne des Widerspruchsbeweises nimmt man an, die zu beweisende Aussage sei falsch; es gebe also natürliche Zahlen, welche die Gültigkeit der Aussage „verderben" – dies sind dann offenbar „Verbrecher". Da die Verbrecher natürliche Zahlen sind, gibt es einen kleinsten unter ihnen, den *kleinsten Verbrecher*. Im weiteren Verlauf ist nun jeweils situationsspezifisch zu zeigen, dass die Annahme der Existenz eines solchen Verbrechers zu einem

Widerspruch führt. Damit kann es keinen kleinsten – und somit überhaupt keinen Verbrecher geben; der Satz ist also allgemeingültig.

Satz 8.6 (Das Schubfachprinzip[31]):

Sind n Dinge auf s Schubfächer zu verteilen, und ist $n > s$, so wird mindestens ein Schubfach mehrfach belegt.

Aufgabe 8.9: Beweisen Sie das Schubfachprinzip mit vollständiger Induktion. Hinweis: Beweisen Sie den Sachverhalt zunächst für $n = s + 1$ Dinge.

Beispiel: Wir betrachten die gewöhnliche schriftliche Division natürlicher Zahlen, wie sie standardmäßig im Schulunterricht gelehrt wird. Zur Illustration wird dieses Verfahren am Beispiel der Division $53 : 14$ im Folgenden ausführlich dargestellt (vgl. auch: das Divisionsschema auf der nächsten Seite). Als Reste kommen bei der Division durch 14 nur die Zahlen 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13 in Frage. Da das Divisionsverfahren nicht stoppt, muss sich nach dem Schubfachprinzip im Laufe des Verfahrens nach hinreichend vielen (in diesem Fall nach höchstens 14) Schritten einer der Reste wiederholen. Im Beispiel ist das der 2. Rest (=12), der bereits nach 6 Schritten wieder auftritt. Sobald sich einer der Reste wiederholt, wird das Verfahren „zyklisch", d.h. die gesamte Kette der folgenden Rechnungen wiederholt sich. Man erhält so eine periodische Dezimalbruchdarstellung. Im obigen Beispiel besteht die Periode aus den 6 Ziffern 857142.

In der Zahlentheorie werden im Hinblick auf die Dezimaldarstellung von u.a. die folgenden Fragen untersucht:

- Unter welchen Bedingungen bricht die Dezimalbruchdarstellung eines Bruches ab (wie z.B. im Fall $7 : 4 = 1{,}75$) und wann wird sie periodisch (wie z.B. im Fall $53 : 14$)?
- Wie hängt die Periodenlänge vom Zähler und Nenner des Ausgangsbruches ab?
- Ab welcher Stelle nach dem Komma beginnt die Periode?
- Gibt es Zahlen, deren Dezimalbruchdarstellung weder abbricht noch periodisch wird? Was kann man über solche Zahlen sagen?
- Wie lauten die Antworten auf diese Fragen in nichtdekadischen Stellenwertsystemen?

[31] nach Johann P. G. Lejeune Dirichlet (1805–1859), deutscher Mathematiker

Ein Beispiel: *schulisches Divisionsverfahren*

```
                        53 : 14 = 3,785714285 ...
es geht   3*14:         42
                        11                  1. Rest
Rest mal 10:            110
es geht   7*14:          98
                         12                 2. Rest
Rest mal 10:             120
es geht   8*14:          112
                           8                3. Rest
Rest mal 10:               80
es geht   5*14:            70
                           10               4. Rest
Rest mal 10:               100
es geht   7*14:             98
                             2              5. Rest
Rest mal 10:                 20
es geht   1*14:              14
                              6             6. Rest
Rest mal 10:                  60
es geht   4*14:               56
                               4            7. Rest
Rest mal 10:                   40
es geht   2*14:                28
                               12           8. Rest
Rest mal 10:                   120
es geht   8*14:                112
                                 8          9. Rest
Rest mal 10:                     80
es geht   5*14:                  70
                                 10      10. Rest
                                 ...
```

8.3 Mengentheoretische Grundbegriffe

Die zweite Hälfte des 19. Jahrhunderts war durch eine rasche Entwicklung in vielen mathematischen Themenbereichen geprägt. Die verwendeten mathematischen Begriffe erreichten eine bis dahin ungeahnte Komplexität und Vielfalt. *Georg Cantor* (1845–1918) unternahm mit seiner „Mengenlehre“ den Versuch, das gesamte Gebäude der Mathematik auf wenige zentrale Grundbegriffe, allen voran den Begriff der Menge, zu begründen. Er formulierte:

> *Unter einer* **Menge** *verstehen wir jede Zusammenfassung M von bestimmten, wohlunterschiedenen Objekten unserer Anschauung oder unseres Denkens zu einem Ganzen.*

Wir verwenden heute die folgenden Darstellungsformen (Schreibweisen) für Mengen:

- *aufzählend*: Die Menge aller ungeraden Zahlen zwischen 0 und 10: $\{1, 3, 5, 7, 9\}$
- *prädikativ*: zum Beispiel: $\{x: x \in \mathbb{N} \text{ und } x \text{ hat genau zwei Teiler}\}$

  in Worten: Menge aller x mit der Eigenschaft: $x \in \mathbb{N}$ und
  x hat genau zwei Teiler

  alternative Schreibweisen („Grundmengen“-orientiert):
  $\{x \in \mathbb{N}: x \text{ hat genau zwei Teiler}\}$ oder:
  $\{x \in \mathbb{N} \ / \ x \text{ hat genau zwei Teiler}\}$

Einige *Standardmengen* in der Mathematik:

$\mathbb{N}$ = Menge der natürlichen Zahlen = $\{1, 2, 3, ...\}$

$\mathbb{N}_0 = \{0, 1, 2, 3, ...\} = \mathbb{N} \cup \{0\} = \mathbb{N}$ vereinigt mit der Menge $\{0\}$

(Sprechweise: $\mathbb{N}_0$ = Menge der *nichtnegativen* ganzen Zahlen)

$\mathbb{Z}$ = Menge der ganzen Zahlen, d.h. $\mathbb{Z} = \{0, 1, -1, 2, -2, 3, -3, \ldots\}$

bzw. (nur zur Veranschaulichung):
$\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$

$\mathbb{Q}$ = Menge der rationalen Zahlen

$\mathbb{R}$ = Menge der reellen Zahlen

$\mathbb{C}$ = Menge der komplexen Zahlen

Das *kartesische Produkt* (auch genannt die *Paarmenge*) zweier Mengen A und B ist gegeben durch: $A \times B = \{(x, y) \ / \ x \in A \text{ und } y \in B\}$

Eine *Relation* $\mathcal{R}$ zwischen den Elementen einer Menge A und den Elementen einer Menge B ist eine Teilmenge des kartesischen Produkts $A \times B$; im Zeichen: $\mathcal{R} \subseteq A \times B$.

Schreib- und *Sprechweisen*:

$(x, y) \in \mathcal{R}$ bedeute: die Elemente x und y stehen in der Relation $\mathcal{R}$.
An Stelle von $(x, y) \in \mathcal{R}$ schreibt man auch kürzer $x \mathcal{R} y$ (z.B.: $x \mid y$).

Häufiger *Spezialfall*: $A = B$. Man spricht dann von einer *Relation in* A oder einer *Relation auf* A. (So ist z.B. die Teilbarkeitsrelation eine Relation auf $\mathbb{N}$ oder auch eine Relation auf $\mathbb{Z}_\infty$)

Wichtige *Relationseigenschaften*:

- Eine Relation $\mathcal{R}$ auf A heißt *reflexiv*, wenn für alle $x \in A$ gilt $x \mathcal{R} x$
- Eine Relation $\mathcal{R}$ auf A heißt *symmetrisch*, wenn für alle $x \in A$ und für alle $y \in A$ gilt: Aus $x \mathcal{R} y$ folgt stets $y \mathcal{R} x$.
- Eine Relation $\mathcal{R}$ auf A heißt *transitiv*, wenn für alle $x \in A$, für alle $y \in A$ und für alle $z \in A$ gilt:
  Aus $x \mathcal{R} y$ und $y \mathcal{R} z$ folgt stets $x \mathcal{R} z$.
- Eine Relation $\mathcal{R}$ auf A heißt *antisymmetrisch* (oder *identitiv*), wenn für alle $x \in A$ und für alle $y \in A$ gilt:
  Aus $x \mathcal{R} y$ und $y \mathcal{R} x$ folgt stets $x = y$.
- Eine Relation auf A heißt *Äquivalenzrelation* auf A, wenn sie reflexiv, symmetrisch und transitiv ist.
- Eine Relation auf A heißt *Ordnungsrelation* auf A, wenn sie reflexiv, antisymmetrisch und transitiv ist.

Bemerkung: Ist A eine endliche Menge, so lässt sich eine Relation $\mathcal{R}$ auf A wie im folgenden Beispiel in einem Tabellenschema darstellen.

Beispiel (Veranschaulichung der Teilbarkeitsrelation im Tabellenschema):
$A = \{1, 2, 3, \ldots, 20\}$; $\mathcal{R}$ sei die Teilbarkeitsrelation auf A, d.h.
$x \mathcal{R} y \Leftrightarrow x$ ist ein Teiler von y.

Im Tabellenschema ist die Relation folgendermaßen dargestellt; ein „Kreuz“ in Zeile x und Spalte y bedeute dabei, dass x ein Teiler von y ist.

Die *Reflexivität* stellt sich im Tabellenschema dadurch da, dass alle Zellen entlang der *Hauptdiagonalen* angekreuzt sind.

Die *Symmetrie* einer Relation (die in diesem Beispiel nicht erfüllt ist) erkennt man im Tabellenschema daran, dass die angekreuzten Zellen *spiegelbildlich* zur Hauptdiagonalen angeordnet sind.

Die *Transitivität* stellt sich in der durch Pfeile angedeuteten Art als „*Rechtecks-Ergänzung*“ dar: Aus $3 \mid 6$ und $6 \mid 18$ folgt $3 \mid 18$.

	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**	**17**	**18**	**19**	**20**
1	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
2		X		X		X		X		X		X		X		X		X		X
3			X			X			X			X			X			X		
4				X				X				X				X				X
5					X					X					X					X
6						X						X						X		
7							X							X						
8								X								X				
9									X									X		
10										X										X
11											X									
12												X								
13													X							
14														X						
15															X					
16																X				
17																	X			
18																		X		
19																			X	
20																				X

Die Teilbarkeitsrelation ist auf der Menge der natürlichen Zahlen reflexiv, antisymmetrisch und transitiv (vgl. Kapitel 2); d.h. die Teilbarkeitsrelation ist eine Ordnungsrelation auf der Menge der natürlichen Zahlen.

Da die Teilbarkeitsrelation auf der Menge der ganzen Zahlen nicht antisymmetrisch ist ($3 \mid -3$ und $-3 \mid 3$, aber $3 \neq -3$), ist sie auf der Menge der *ganzen* Zahlen keine Ordnungsrelation.

Äquivalenzrelationen und Äquivalenzklassen

Jede Äquivalenzrelation $\mathcal{R}$ auf einer Menge A zerlegt diese Menge wie folgt in *Äquivalenzklassen*: Zu jedem Element $x \in A$ sei die Menge K_x die Menge aller zu x äquivalenten Elemente von A: $K_x := \{y \in A : y \mathcal{R} x\}$.

Die Menge K_x heißt die zum Element x gehörende *Äquivalenzklasse*. Es gilt der folgende

Satz 8.7 (Eigenschaften von Äquivalenzklassen):

1. Je zwei solcher Äquivalenzklassen sind entweder gleich oder elementfremd (disjunkt); als Formel: $K_x = K_y$ oder $K_x \cap K_y = \varnothing$.

2. Die Vereinigung aller zur Relation $\mathcal{R}$ gehörenden Äquivalenzklassen ist gleich der Menge A; als Formel: $\bigcup_{x \in A} K_x = A$.

Aufgabe 8.10: Beweisen Sie diesen Satz.

Aufgabe 8.11: Es sei $f : A \to B$ eine Abbildung (Funktion) der Menge A in die Menge B. Zeigen Sie: Die durch $x \mathcal{R} y :\Leftrightarrow f(x) = f(y)$ gegebene Relation ist eine Äquivalenzrelation auf A.

Bemerkung: Äquivalenzrelationen spielen in der Zahlentheorie im Zusammenhang mit *Kongruenzen* eine herausragende Rolle. Die Äquivalenzklassen werden in diesem Zusammenhang als *Restklassen* bezeichnet (vgl. Kapitel 5).

8.4 Zur Multiplikativität der Eulerschen φ-Funktion – ein ausführliches Beispiel

Die folgenden Tabellen dienen der Veranschaulichung des Satzes in Abschnitt 7.1: Die Eulersch φ-Funktion ist multiplikativ.

Zahlenbeispiel: Wir wählen

$m = 5 * 11 = 55$ (= Zeilenzahl in den folgenden Tabellen)

$n = 2 * 7 = 14$ (= Spaltenzahl in den folgenden Tabellen)

Es ist:

$\varphi(m) = 40 \quad \varphi(n) = 6 \quad \varphi(m) * \varphi(n) = 240 \quad \varphi(m*n) = 240$

Bei dem im Beweis auftretenden kompletten Tabellenschema in der Form

$q \cdot n + r$ mit $0 \le q \le m-1$ und $1 \le r \le n$

ist q der Zeilen-Index und r der Spalten-Index

In **Tabelle 1** ist (als Ausgangspunkt) das komplette Schema wiedergegeben.

In **Tabelle 2** sind die zu n (= 14) teilerfremden Zahlen dargestellt.

In **Tabelle 3** sind die zu m (= 55) teilerfremden Zahlen dargestellt.

In **Tabelle 4** sind die zu m (= 55) teilerfremden Zahlen dargestellt in der Form *modulo m*. D.h., ihre Reste bei der Division durch m sind dargestellt. Man beachte: *Jede Spalte enthält dieselbe Menge von Zahlen* (wenn auch in unterschiedlicher Reihenfolge).

In **Tabelle 5** sind die sowohl zu m (= 55) als auch zu n (=14) teilerfremden Zahlen dargestellt. Die beiden Bedingungen werden in dieser Tabelle *einzeln* und *unabhängig* voneinander überprüft.
Spalten- und zeilenweises Überprüfen der Tabelle ergibt:

1. Es gibt 6 Spalten mit zu m (= 14) teilerfremden Zahlen.
2. In jeder dieser 6 Spalten gibt es 40 Zahlen, die zu n (= 55) teilerfremden sind.

Also enthält Tabelle 5 insgesamt 240 Zahlen, von denen jede sowohl zu m also auch zu n teilerfremd ist.

In **Tabelle 6** sind die zu 770 (= $m * n$) teilerfremden Zahlen dargestellt.
Die Tatsache, dass Tabelle 6 exakt mit Tabelle 5 übereinstimmt, ist eine Veranschaulichung (bzw. ein empirischer Beleg) für die Multiplikativität der Eulerschen φ-Funktion.

Tabelle 1: Das komplette Schema

1	2	3	4	5	6	7	8	9	10	11	12	13	14
15	16	17	18	19	20	21	22	23	24	25	26	27	28
29	30	31	32	33	34	35	36	37	38	39	40	41	42
43	44	45	46	47	48	49	50	51	52	53	54	55	56
57	58	59	60	61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80	81	82	83	84
85	86	87	88	89	90	91	92	93	94	95	96	97	98
99	100	101	102	103	104	105	106	107	108	109	110	111	112
113	114	115	116	117	118	119	120	121	122	123	124	125	126
127	128	129	130	131	132	133	134	135	136	137	138	139	140
141	142	143	144	145	146	147	148	149	150	151	152	153	154
155	156	157	158	159	160	161	162	163	164	165	166	167	168
169	170	171	172	173	174	175	176	177	178	179	180	181	182
183	184	185	186	187	188	189	190	191	192	193	194	195	196
197	198	199	200	201	202	203	204	205	206	207	208	209	210
211	212	213	214	215	216	217	218	219	220	221	222	223	224
225	226	227	228	229	230	231	232	233	234	235	236	237	238
239	240	241	242	243	244	245	246	247	248	249	250	251	252
253	254	255	256	257	258	259	260	261	262	263	264	265	266
267	268	269	270	271	272	273	274	275	276	277	278	279	280
281	282	283	284	285	286	287	288	289	290	291	292	293	294
295	296	297	298	299	300	301	302	303	304	305	306	307	308
309	310	311	312	313	314	315	316	317	318	319	320	321	322
323	324	325	326	327	328	329	330	331	332	333	334	335	336
337	338	339	340	341	342	343	344	345	346	347	348	349	350
351	352	353	354	355	356	357	358	359	360	361	362	363	364
365	366	367	368	369	370	371	372	373	374	375	376	377	378
379	380	381	382	383	384	385	386	387	388	389	390	391	392
393	394	395	396	397	398	399	400	401	402	403	404	405	406
407	408	409	410	411	412	413	414	415	416	417	418	419	420
421	422	423	424	425	426	427	428	429	430	431	432	433	434
435	436	437	438	439	440	441	442	443	444	445	446	447	448
449	450	451	452	453	454	455	456	457	458	459	460	461	462
463	464	465	466	467	468	469	470	471	472	473	474	475	476
477	478	479	480	481	482	483	484	485	486	487	488	489	490
491	492	493	494	495	496	497	498	499	500	501	502	503	504
505	506	507	508	509	510	511	512	513	514	515	516	517	518
519	520	521	522	523	524	525	526	527	528	529	530	531	532
533	534	535	536	537	538	539	540	541	542	543	544	545	546
547	548	549	550	551	552	553	554	555	556	557	558	559	560
561	562	563	564	565	566	567	568	569	570	571	572	573	574
575	576	577	578	579	580	581	582	583	584	585	586	587	588
589	590	591	592	593	594	595	596	597	598	599	600	601	602
603	604	605	606	607	608	609	610	611	612	613	614	615	616
617	618	619	620	621	622	623	624	625	626	627	628	629	630
631	632	633	634	635	636	637	638	639	640	641	642	643	644
645	646	647	648	649	650	651	652	653	654	655	656	657	658
659	660	661	662	663	664	665	666	667	668	669	670	671	672
673	674	675	676	677	678	679	680	681	682	683	684	685	686
687	688	689	690	691	692	693	694	695	696	697	698	699	700
701	702	703	704	705	706	707	708	709	710	711	712	713	714
715	716	717	718	719	720	721	722	723	724	725	726	727	728
729	730	731	732	733	734	735	736	737	738	739	740	741	742
743	744	745	746	747	748	749	750	751	752	753	754	755	756
757	758	759	760	761	762	763	764	765	766	767	768	769	770

Tabelle 2: Die zu n (= 14) teilerfremden Zahlen

1	–	3	–	5	–	–	–	9	–	11	–	13	–
15	–	17	–	19	–	–	–	23	–	25	–	27	–
29	–	31	–	33	–	–	–	37	–	39	–	41	–
43	–	45	–	47	–	–	–	51	–	53	–	55	–
57	–	59	–	61	–	–	–	65	–	67	–	69	–
71	–	73	–	75	–	–	–	79	–	81	–	83	–
85	–	87	–	89	–	–	–	93	–	95	–	97	–
99	–	101	–	103	–	–	–	107	–	109	–	111	–
113	–	115	–	117	–	–	–	121	–	123	–	125	–
127	–	129	–	131	–	–	–	135	–	137	–	139	–
141	–	143	–	145	–	–	–	149	–	151	–	153	–
155	–	157	–	159	–	–	–	163	–	165	–	167	–
169	–	171	–	173	–	–	–	177	–	179	–	181	–
183	–	185	–	187	–	–	–	191	–	193	–	195	–
197	–	199	–	201	–	–	–	205	–	207	–	209	–
211	–	213	–	215	–	–	–	219	–	221	–	223	–
225	–	227	–	229	–	–	–	233	–	235	–	237	–
239	–	241	–	243	–	–	–	247	–	249	–	251	–
253	–	255	–	257	–	–	–	261	–	263	–	265	–
267	–	269	–	271	–	–	–	275	–	277	–	279	–
281	–	283	–	285	–	–	–	289	–	291	–	293	–
295	–	297	–	299	–	–	–	303	–	305	–	307	–
309	–	311	–	313	–	–	–	317	–	319	–	321	–
323	–	325	–	327	–	–	–	331	–	333	–	335	–
337	–	339	–	341	–	–	–	345	–	347	–	349	–
351	–	353	–	355	–	–	–	359	–	361	–	363	–
365	–	367	–	369	–	–	–	373	–	375	–	377	–
379	–	381	–	383	–	–	–	387	–	389	–	391	–
393	–	395	–	397	–	–	–	401	–	403	–	405	–
407	–	409	–	411	–	–	–	415	–	417	–	419	–
421	–	423	–	425	–	–	–	429	–	431	–	433	–
435	–	437	–	439	–	–	–	443	–	445	–	447	–
449	–	451	–	453	–	–	–	457	–	459	–	461	–
463	–	465	–	467	–	–	–	471	–	473	–	475	–
477	–	479	–	481	–	–	–	485	–	487	–	489	–
491	–	493	–	495	–	–	–	499	–	501	–	503	–
505	–	507	–	509	–	–	–	513	–	515	–	517	–
519	–	521	–	523	–	–	–	527	–	529	–	531	–
533	–	535	–	537	–	–	–	541	–	543	–	545	–
547	–	549	–	551	–	–	–	555	–	557	–	559	–
561	–	563	–	565	–	–	–	569	–	571	–	573	–
575	–	577	–	579	–	–	–	583	–	585	–	587	–
589	–	591	–	593	–	–	–	597	–	599	–	601	–
603	–	605	–	607	–	–	–	611	–	613	–	615	–
617	–	619	–	621	–	–	–	625	–	627	–	629	–
631	–	633	–	635	–	–	–	639	–	641	–	643	–
645	–	647	–	649	–	–	–	653	–	655	–	657	–
659	–	661	–	663	–	–	–	667	–	669	–	671	–
673	–	675	–	677	–	–	–	681	–	683	–	685	–
687	–	689	–	691	–	–	–	695	–	697	–	699	–
701	–	703	–	705	–	–	–	709	–	711	–	713	–
715	–	717	–	719	–	–	–	723	–	725	–	727	–
729	–	731	–	733	–	–	–	737	–	739	–	741	–
743	–	745	–	747	–	–	–	751	–	753	–	755	–
757	–	759	–	761	–	–	–	765	–	767	–	769	–

Tabelle 3: Die zu m (= 55) teilerfremden Zahlen

1	2	3	4	–	6	7	8	9	–	–	12	13	14
–	16	17	18	19	–	21	–	23	24	–	26	27	28
29	–	31	32	–	34	–	36	37	38	39	–	41	42
43	–	–	46	47	48	49	–	51	52	53	54	–	56
57	58	59	–	61	62	63	64	–	–	67	68	69	–
71	72	73	74	–	76	–	78	79	–	81	82	83	84
–	86	87	–	89	–	91	92	93	94	–	96	97	98
–	–	101	102	103	104	–	106	107	108	109	–	111	112
113	114	–	116	117	118	119	–	–	122	123	124	–	126
127	128	129	–	131	–	133	134	–	136	137	138	139	–
141	142	–	144	–	146	147	148	149	–	151	152	153	–
–	156	157	158	159	–	161	162	163	164	–	166	167	168
169	–	171	172	173	174	–	–	177	178	179	–	181	182
183	184	–	186	–	188	189	–	191	192	193	194	–	196
197	–	199	–	201	202	203	204	–	206	207	208	–	–
211	212	213	214	–	216	217	218	219	–	221	222	223	224
–	226	227	228	229	–	–	232	233	234	–	236	237	238
239	–	241	–	243	244	–	246	247	248	249	–	251	252
–	254	–	256	257	258	259	–	261	262	263	–	–	266
267	268	269	–	271	272	273	274	–	276	277	278	279	–
281	282	283	284	–	–	287	288	289	–	291	292	293	294
–	296	–	298	299	–	301	302	303	304	–	306	307	–
309	–	311	312	313	314	–	316	317	318	–	–	321	322
323	324	–	326	327	328	329	–	331	332	333	334	–	336
337	338	339	–	–	342	343	344	–	346	347	348	349	–
351	–	353	354	–	356	357	358	359	–	361	362	–	364
–	366	367	368	369	–	371	372	373	–	–	376	377	378
379	–	381	382	383	384	–	386	387	388	389	–	391	392
393	394	–	–	397	398	399	–	401	402	403	404	–	406
–	408	409	–	411	412	413	414	–	416	417	–	419	–
421	422	423	424	–	426	427	428	–	–	431	432	433	434
–	436	437	438	439	–	441	442	443	444	–	446	447	448
449	–	–	452	453	454	–	456	457	458	459	–	461	–
463	464	–	466	467	468	469	–	471	472	–	474	–	476
477	478	479	–	481	482	483	–	–	486	487	488	489	–
491	492	493	494	–	496	497	498	499	–	501	502	503	504
–	–	507	508	509	–	511	512	513	514	–	516	–	518
519	–	521	522	523	524	–	526	527	–	529	–	531	532
533	534	–	536	537	538	–	–	541	542	543	544	–	546
547	548	549	–	551	552	553	554	–	556	557	558	559	–
–	562	563	564	–	566	567	568	569	–	571	–	573	574
–	576	577	578	579	–	581	582	–	584	–	586	587	588
589	–	591	592	593	–	–	596	597	598	599	–	601	602
603	604	–	606	607	608	609	–	611	612	613	614	–	–
617	618	619	–	621	622	623	624	–	626	–	628	629	–
631	632	633	634	–	636	637	–	639	–	641	642	643	644
–	646	647	648	–	–	651	652	653	654	–	656	657	658
659	–	661	662	663	664	–	666	667	668	669	–	–	672
673	674	–	676	677	678	679	–	681	–	683	684	–	686
687	688	689	–	691	692	–	694	–	696	697	698	699	–
701	702	703	–	–	706	707	708	709	–	711	712	713	714
–	716	717	718	719	–	721	722	723	724	–	–	727	728
729	–	731	732	733	734	–	736	–	738	739	–	741	742
743	744	–	746	747	–	749	–	751	752	753	754	–	756
757	758	–	–	761	762	763	764	–	766	767	768	769	–

Tabelle 4: Die zu m (= 55) teilerfremden Zahlen **modulo m**

1	2	3	4	–	6	7	8	9	–	–	12	13	14
–	16	17	18	19	–	21	–	23	24	–	26	27	28
29	–	31	32	–	34	–	36	37	38	39	–	41	42
43	–	–	46	47	48	49	–	51	52	53	54	–	1
2	3	4	–	6	7	8	9	–	–	12	13	14	–
16	17	18	19	–	21	–	23	24	–	26	27	28	29
–	31	32	–	34	–	36	37	38	39	–	41	42	43
–	–	46	47	48	49	–	51	52	53	54	–	1	2
3	4	–	6	7	8	9	–	–	12	13	14	–	16
17	18	19	–	21	–	23	24	–	26	27	28	29	–
31	32	–	34	–	36	37	38	39	–	41	42	43	–
–	46	47	48	49	–	51	52	53	54	–	1	2	3
4	–	6	7	8	9	–	–	12	13	14	–	16	17
18	19	–	21	–	23	24	–	26	27	28	29	–	31
32	–	34	–	36	37	38	39	–	41	42	43	–	–
46	47	48	49	–	51	52	53	54	–	1	2	3	4
–	6	7	8	9	–	–	12	13	14	–	16	17	18
19	–	21	–	23	24	–	26	27	28	29	–	31	32
–	34	–	36	37	38	39	–	41	42	43	–	–	46
47	48	49	–	51	52	53	54	–	1	2	3	4	–
6	7	8	9	–	–	12	13	14	–	16	17	18	19
–	21	–	23	24	–	26	27	28	29	–	31	32	–
34	–	36	37	38	39	–	41	42	43	–	–	46	47
48	49	–	51	52	53	54	–	1	2	3	4	–	6
7	8	9	–	–	12	13	14	–	16	17	18	19	–
21	–	23	24	–	26	27	28	29	–	31	32	–	34
–	36	37	38	39	–	41	42	43	–	–	46	47	48
49	–	51	52	53	54	–	1	2	3	4	–	6	7
8	9	–	–	12	13	14	–	16	17	18	19	–	21
–	23	24	–	26	27	28	29	–	31	32	–	34	–
36	37	38	39	–	41	42	43	–	–	46	47	48	49
–	51	52	53	54	–	1	2	3	4	–	6	7	8
9	–	–	12	13	14	–	16	17	18	19	–	21	–
23	24	–	26	27	28	29	–	31	32	–	34	–	36
37	38	39	–	41	42	43	–	–	46	47	48	49	–
51	52	53	54	–	1	2	3	4	–	6	7	8	9
–	–	12	13	14	–	16	17	18	19	–	21	–	23
24	–	26	27	28	29	–	31	32	–	34	–	36	37
38	39	–	41	42	43	–	–	46	47	48	49	–	51
52	53	54	–	1	2	3	4	–	6	7	8	9	–
–	12	13	14	–	16	17	18	19	–	21	–	23	24
–	26	27	28	29	–	31	32	–	34	–	36	37	38
39	–	41	42	43	–	–	46	47	48	49	–	51	52
53	54	–	1	2	3	4	–	6	7	8	9	–	–
12	13	14	–	16	17	18	19	–	21	–	23	24	–
26	27	28	29	–	31	32	–	34	–	36	37	38	39
–	41	42	43	–	–	46	47	48	49	–	51	52	53
54	–	1	2	3	4	–	6	7	8	9	–	–	12
13	14	–	16	17	18	19	–	21	–	23	24	–	26
27	28	29	–	31	32	–	34	–	36	37	38	39	–
41	42	43	–	–	46	47	48	49	–	51	52	53	54
–	1	2	3	4	–	6	7	8	9	–	–	12	13
14	–	16	17	18	19	–	21	–	23	24	–	26	27
28	29	–	31	32	–	34	–	36	37	38	39	–	41
42	43	–	–	46	47	48	49	–	51	52	53	54	–

Tabelle 5: Die sowohl zu m als auch zu n teilerfremden Zahlen

1	–	3	–	–	–	–	–	9	–	–	–	13	–
–	–	17	–	19	–	–	–	23	–	–	–	27	–
29	–	31	–	–	–	–	–	37	–	39	–	41	–
43	–	–	–	47	–	–	–	51	–	53	–	–	–
57	–	59	–	61	–	–	–	–	–	67	–	69	–
71	–	73	–	–	–	–	–	79	–	81	–	83	–
–	–	87	–	89	–	–	–	93	–	–	–	97	–
–	–	101	–	103	–	–	–	107	–	109	–	111	–
113	–	–	–	117	–	–	–	–	–	123	–	–	–
127	–	129	–	131	–	–	–	–	–	137	–	139	–
141	–	–	–	–	–	–	–	149	–	151	–	153	–
–	–	157	–	159	–	–	–	163	–	–	–	167	–
169	–	171	–	173	–	–	–	177	–	179	–	181	–
183	–	–	–	–	–	–	–	191	–	193	–	–	–
197	–	199	–	201	–	–	–	–	–	207	–	–	–
211	–	213	–	–	–	–	–	219	–	221	–	223	–
–	–	227	–	229	–	–	–	233	–	–	–	237	–
239	–	241	–	243	–	–	–	247	–	249	–	251	–
–	–	–	–	257	–	–	–	261	–	263	–	–	–
267	–	269	–	271	–	–	–	–	–	277	–	279	–
281	–	283	–	–	–	–	–	289	–	291	–	293	–
–	–	–	–	299	–	–	–	303	–	–	–	307	–
309	–	311	–	313	–	–	–	317	–	–	–	321	–
323	–	–	–	327	–	–	–	331	–	333	–	–	–
337	–	339	–	–	–	–	–	–	–	347	–	349	–
351	–	353	–	–	–	–	–	359	–	361	–	–	–
–	–	367	–	369	–	–	–	373	–	–	–	377	–
379	–	381	–	383	–	–	–	387	–	389	–	391	–
393	–	–	–	397	–	–	–	401	–	403	–	–	–
–	–	409	–	411	–	–	–	–	–	417	–	419	–
421	–	423	–	–	–	–	–	–	–	431	–	433	–
–	–	437	–	439	–	–	–	443	–	–	–	447	–
449	–	–	–	453	–	–	–	457	–	459	–	461	–
463	–	–	–	467	–	–	–	471	–	–	–	–	–
477	–	479	–	481	–	–	–	–	–	487	–	489	–
491	–	493	–	–	–	–	–	499	–	501	–	503	–
–	–	507	–	509	–	–	–	513	–	–	–	–	–
519	–	521	–	523	–	–	–	527	–	529	–	531	–
533	–	–	–	537	–	–	–	541	–	543	–	–	–
547	–	549	–	551	–	–	–	–	–	557	–	559	–
–	–	563	–	–	–	–	–	569	–	571	–	573	–
–	–	577	–	579	–	–	–	–	–	–	–	587	–
589	–	591	–	593	–	–	–	597	–	599	–	601	–
603	–	–	–	607	–	–	–	611	–	613	–	–	–
617	–	619	–	621	–	–	–	–	–	–	–	629	–
631	–	633	–	–	–	–	–	639	–	641	–	643	–
–	–	647	–	–	–	–	–	653	–	–	–	657	–
659	–	661	–	663	–	–	–	667	–	669	–	–	–
673	–	–	–	677	–	–	–	681	–	683	–	–	–
687	–	689	–	691	–	–	–	–	–	697	–	699	–
701	–	703	–	–	–	–	–	709	–	711	–	713	–
–	–	717	–	719	–	–	–	723	–	–	–	727	–
729	–	731	–	733	–	–	–	–	–	739	–	741	–
743	–	–	–	747	–	–	–	751	–	753	–	–	–
757	–	–	–	761	–	–	–	–	–	767	–	769	–

Tabelle 6: Die zu n*m (= 770) teilerfremden Zahlen

1	–	3	–	–	–	–	–	9	–	–	–	13	–
–	–	17	–	19	–	–	–	23	–	–	–	27	–
29	–	31	–	–	–	–	–	37	–	39	–	41	–
43	–	–	–	47	–	–	–	51	–	53	–	–	–
57	–	59	–	61	–	–	–	–	–	67	–	69	–
71	–	73	–	–	–	–	–	79	–	81	–	83	–
–	–	87	–	89	–	–	–	93	–	–	–	97	–
–	–	101	–	103	–	–	–	107	–	109	–	111	–
113	–	–	–	117	–	–	–	–	–	123	–	–	–
127	–	129	–	131	–	–	–	–	–	137	–	139	–
141	–	–	–	–	–	–	–	149	–	151	–	153	–
–	–	157	–	159	–	–	–	163	–	–	–	167	–
169	–	171	–	173	–	–	–	177	–	179	–	181	–
183	–	–	–	–	–	–	–	191	–	193	–	–	–
197	–	199	–	201	–	–	–	–	–	207	–	–	–
211	–	213	–	–	–	–	–	219	–	221	–	223	–
–	–	227	–	229	–	–	–	233	–	–	–	237	–
239	–	241	–	243	–	–	–	247	–	249	–	251	–
–	–	–	–	257	–	–	–	261	–	263	–	–	–
267	–	269	–	271	–	–	–	–	–	277	–	279	–
281	–	283	–	–	–	–	–	289	–	291	–	293	–
–	–	–	–	299	–	–	–	303	–	–	–	307	–
309	–	311	–	313	–	–	–	317	–	–	–	321	–
323	–	–	–	327	–	–	–	331	–	333	–	–	–
337	–	339	–	–	–	–	–	–	–	347	–	349	–
351	–	353	–	–	–	–	–	359	–	361	–	–	–
–	–	367	–	369	–	–	–	373	–	–	–	377	–
379	–	381	–	383	–	–	–	387	–	389	–	391	–
393	–	–	–	397	–	–	–	401	–	403	–	–	–
–	–	409	–	411	–	–	–	–	–	417	–	419	–
421	–	423	–	–	–	–	–	–	–	431	–	433	–
–	–	437	–	439	–	–	–	443	–	–	–	447	–
449	–	–	–	453	–	–	–	457	–	459	–	461	–
463	–	–	–	467	–	–	–	471	–	–	–	–	–
477	–	479	–	481	–	–	–	–	–	487	–	489	–
491	–	493	–	–	–	–	–	499	–	501	–	503	–
–	–	507	–	509	–	–	–	513	–	–	–	–	–
519	–	521	–	523	–	–	–	527	–	529	–	531	–
533	–	–	–	537	–	–	–	541	–	543	–	–	–
547	–	549	–	551	–	–	–	–	–	557	–	559	–
–	–	563	–	–	–	–	–	569	–	571	–	573	–
–	–	577	–	579	–	–	–	–	–	–	–	587	–
589	–	591	–	593	–	–	–	597	–	599	–	601	–
603	–	–	–	607	–	–	–	611	–	613	–	–	–
617	–	619	–	621	–	–	–	–	–	–	–	629	–
631	–	633	–	–	–	–	–	639	–	641	–	643	–
–	–	647	–	–	–	–	–	653	–	–	–	657	–
659	–	661	–	663	–	–	–	667	–	669	–	–	–
673	–	–	–	677	–	–	–	681	–	683	–	–	–
687	–	689	–	691	–	–	–	–	–	697	–	699	–
701	–	703	–	–	–	–	–	709	–	711	–	713	–
–	–	717	–	719	–	–	–	723	–	–	–	727	–
729	–	731	–	733	–	–	–	–	–	739	–	741	–
743	–	–	–	747	–	–	–	751	–	753	–	–	–
757	–	–	–	761	–	–	–	–	–	767	–	769	–

Abbildungsverzeichnis

Hier finden sich die Quellen- und Lizenzangaben zu den Abbildungen, die nicht vom Autor selbst hergestellt worden sind.

Abb. 1.1: Wolfsknochen mit Einkerbungen
Beckmann P.: A History of π; The Golem Press, New York 1971

Abb. 1.2: Ägyptische Zahlzeichen
Für Unicode support und ägyptische Zeichensätze bin ich George Douros zu Dank verpflichtet (vgl.: http://users.teilar.gr/~g1951d/)

Abb. 1.4: Babylonische Keilschrift-Zahlzeichen
Wikimedia Commons, CreativeCommons-Lizenz by-sa-2.0-de
Quelle: http://commons.wikimedia.org/wiki/File:Babylonian_numerals.svg
Urheber: Josell7

Abb. 1.5: Chinesisches Rechengerät Suan-pan
Wikimedia Commons, Creative Commons Attribution-Share Alike 3.0 Unported license.
Quelle: http://commons.wikimedia.org/wiki/File:Suanpan.jpg
Photo: Biswajoysaha

Abb. 1.6: Zahlzeichen der Maya
Wikimedia Commons, Creative Commons Attribution-Share Alike 3.0 Unported license,
GNU Free Documentation License, Version 1.2
Quelle: http://commons.wikimedia.org/wiki/File:Maya_numerals.png

Abb. 1.9: Statue von Al-Khwarizmi in Khiva (Usbekistan)
Wikimedia Commons, Creative Commons Attribution-Share Alike 3.0 Unported license
Quelle: http://commons.wikimedia.org/wiki/File:Al-Khwarizmi,_Khiva.jpg
Photo: Hunter Johnson

J. Ziegenbalg, *Elementare Zahlentheorie*, DOI 10.1007/978-3-658-07171-4

Abb. 1.10: Leonardo von Pisa ("Fibonacci")
Wikimedia Commons, public domain
Quelle:
http://commons.wikimedia.org/wiki/Category:Fibonacci#mediaviewer/File:Fibonacci_plastika.jpg
Photo: Jan Hamsik

Abb. 1.11: Adam Ries Denkmal in Erfurt
Wikimedia Commons, CC BY-SA 3.0
Quelle:
http://commons.wikimedia.org/wiki/Category:Busts_in_Erfurt#mediaviewer/File:Adam-Ries-Erfurt-JMUnger.jpg
Photo: Jörg M. Unger

Abb. 1.12: Gregor Reisch, Margarita Philosophica
Wikimedia Commons, public domain
Quelle:
http://commons.wikimedia.org/wiki/File:Gregor_Reisch,_Margarita_Philosophica,_1508_%281230x1615%29.png

Abb. 1.13: Pierre de Fermat
Wikimedia Commons, CC-PD-Mark public domain
Quelle:
http://commons.wikimedia.org/wiki/Pierre_de_Fermat#mediaviewer/File:Pierre_de_Fermat.png

Abb. 1.14: G. W. Leibniz
Wikimedia Commons, public domain
Quelle:
http://commons.wikimedia.org/wiki/File:Gottfried_Wilhelm_von_Leibniz.jpg
Künstler: Christoph Bernhard Francke (um 1700)
Standort des Originals: Herzog Anton Ulrich–Museum, Braunschweig

Abb. 1.15: Leonhard Euler, Sowjetische Briefmarke 1957

Abb. 1.16: Carl Friedrich Gauß, Briefmarke DDR 1977

Abb. 1.17: Gauß auf 10 DM Schein, Ausschnitt, Bundesrepublik Deutschland

Abb. 1.18: David Hilbert
Wikimedia Commons, public domain
Quelle:
http://commons.wikimedia.org/wiki/David_Hilbert#mediaviewer/File:Hilbert.jpg

Abb. 1.19: Srinivasa Ramanujan
Wikimedia Commons, CC BY-SA-2.0-de
Quelle:
http://en.wikipedia.org/wiki/Srinivasa_Ramanujan#mediaviewer/File:Srinivasa_Ramanujan_-_OPC_-_1.jpg
Konrad Jacobs - Oberwolfach Photo Collection

Abb. 1.20: G. H. Hardy
Wikipedia, public domain
Quelle:
http://commons.wikimedia.org/wiki/G._H._Hardy#mediaviewer/File:Ghhardy@72.jpg

Abb. 4.3: M. Mersenne
Wikimedia Commons, public domain
Quelle: http://commons.wikimedia.org/wiki/File:Marin_mersenne.jpg

Abb. 6.1: G. W. Leibniz zum Zweiersystem
Wikimedia Commons, public domain
Quelle:
http://commons.wikimedia.org/wiki/File:Leibniz_binary_system_1703.png

Abb. 6.2: Briefmarke Rechenprobe, Deutsche Bundespost 1959

Abb. 6.3: Briefmarke Rechenprobe, Deutsche Bundespost 1992

Verzeichnis internetbasierter Materialien des Autors

Sowohl zum Basistext als auch zu den weiterführenden Themen stehen im Internet neben themenbezogenen Computeralgebra-Quelltexten die folgenden zum Experimentieren gedachten interaktiven Seiten zur Verfügung.

Interaktive Materialien

Zum *Sieb des Eratosthenes*:

http://www.ziegenbalg.ph-karlsruhe.de/materialien-homepage-jzbg/Sieb-des-Eratosthenes/Sieb-des-Eratosthenes.htm

http://www.ziegenbalg.ph-karlsruhe.de/materialien-homepage-jzbg/Sieb-des-Eratosthenes/Sieb-des-Eratosthenes-Simulation.htm

Zum Thema *Codierung und Kryptographie*:

http://www.ziegenbalg.ph-karlsruhe.de/materialien-homepage-jzbg/cc-interaktiv/index.htm

Zum Thema *Würfelverdopplung*:

http://www.ziegenbalg.ph-karlsruhe.de/materialien-homepage-jzbg/Wuerfelverdopplung/erat-mp.htm

Computeralgebra Texte und Materialien

http://www.ziegenbalg.ph-karlsruhe.de/#Computeralgebra-notebooks

http://www.ziegenbalg.ph-karlsruhe.de/materialien-homepage-jzbg/materials-in-english/index.html

Dort stehen Computeralgebra notebooks (CAS Mathematica) bzw. worksheets (CAS Maxima) in deutscher und englischer Sprache insbesondere zu den folgenden Themen zur Verfügung:

Der Euklidische Algorithmus / Das Sieb des Eratosthenes / Systembrüche / Das Heron-Verfahren / Wachstumsprozesse / Folgen, Induktion, Fibonacci Zahlen, Goldener Schnitt, Phyllotaxis / Public Key Cryptography: Das RSA-Verfahren

Phi, Tau, Sigma in Elementary Number Theory / Figurate Numbers / The Egyptian multiplication algorithm / Fibonacci numbers - case studies in recursion and iteration

Literaturverzeichnis

1. Bücher zur Zahlentheorie im engeren Sinne

Bartholomé A. / Rung J. / Kern H.: Zahlentheorie für Einsteiger; Vieweg+Teubner, Wiesbaden, 7. Aufl. 2010

Bundschuh P.: Einführung in die Zahlentheorie; Springer Verlag, Heidelberg Berlin, 6. Aufl. 2008

Deutsches Institut für Fernstudien (DIFF): Elemente der Zahlentheorie; Reihe „Grundkurs Mathematik“, Heft I,4, Tübingen 1971

Dickson L. E.: History of the theory of numbers I,II, III; Chelsea Publ. Comp. New York 1971 (Nachdruck der ersten Auflage von 1919)

Ebbinghaus H.-D. / Hermes H. / Hirzebruch F. / Koecher M. / Mainzer K. / Prestel A. / Remmert R.: Zahlen; Springer Verlag, Berlin 1983

Euklid: Die Elemente (Nach Heibergs Text aus dem griechischen übersetzt und herausgegeben von Clemens Thaer); Bücher I-XIII; Reihe Ostwalds Klassiker, Bd. 235; Nachdruck durch Wissenschaftliche Buchgesellschaft Darmstadt 1973

Frey G.: Elementare Zahlentheorie; Vieweg Verlag, Braunschweig 1984

Goldman J. R.: The Queen of Mathematics – A Historically Motivated Guide to Number Theory; A. K. Peters, Wellesley (Massachusetts) 1998

Hardy G. H. / Wright E. M.: Einführung in die Zahlentheorie; Verlag R. Oldenbourg, München 1958

Hasse H.: Vorlesungen über Zahlentheorie (zweite Auflage); Springer Verlag, Berlin, 2. Aufl. 1964

Ifrah G.: Universalgeschichte der Zahlen; Campus Verlag, Frankfurt / New York 1989

Ischebeck F.: Einladung zur Zahlentheorie; BI-Wissenschaftsverlag, Mannheim 1992

Leonardo Pisano Fibonacci: The Book of Squares, An Annotated Translation into Modern English by L. E. Sigler; Academic Press, Boston 1987

Lüneburg H.: Vorlesungen über Zahlentheorie; Birkhäuser Verlag, Basel 1978

Lüneburg H.: Kleine Fibel der Arithmetik; BI Wissenschaftsverlag, Mannheim / Wien / Zürich 1987

McLeish J.: The Story of Numbers; Ballantine Books, New York 1992

Menninger K.: Zahlwort und Ziffer; Vandenhoeck & Ruprecht, Göttingen 1958

Mönkemeyer R.: Einführung in die Zahlentheorie; Verlage Schroedel und Schöningh, Hannover und Paderborn 1971

Müller G.N. / Steinbring H. / Wittmann E.Ch.: Arithmetik als Prozess, Kallmeyersche Verlagsbuchhandlung, Hannover 2004

Ore O.: Invitation to Number Theory; Mathematical Association of America, 1967 Yale University

Ore O.: Number Theory and Its History; Dover Publications Inc., New York 1948

Padberg F.: Elementare Zahlentheorie; Spektrum Verlag, Heidelberg, 3. Auflage 2008

Padberg F.: Zahlentheorie und Arithmetik; Spektrum Verlag, Heidelberg 1999

Pracht E. / Heidenreich K.: Elementare Zahlentheorie; Ferd. Schöningh Verlag, Paderborn 1978

Remmert R. / Ullrich P.: Elementare Zahlentheorie, Birkhäuser Verlag, Basel 1987

Ribenboim P.: The Book of Prime Number Records; New York-Berlin, 1989

Ribenboim P.: The New Book of Prime Number Records, New York-Berlin, 1997

Scheid H.: Einführung in die Zahlentheorie, Klett Verlag (Studienbücher), Stuttgart 1972

Scheid H.: Zahlentheorie; B.I. Verlag, Mannheim 1994

Scheid H. / Schwarz W.: Elemente der Arithmetik und Algebra, Spektrum Verlag, Heidelberg, 5. Aufl. 2008

Scholz A. / Schoeneberg B.: Einführung in die Zahlentheorie; W. de Gruyter Verlag (Sammlung Göschen), Berlin 1972

Schwarz F.: Einführung in die Elementare Zahlentheorie; Verlag B.G.Teubner, Stuttgart 1998

Weil A.: Number Theory - An approach through history - From Hammurapi to Legendre; Birkhäuser Verlag, Boston 1984

Winogradow I. M.: Elemente der Zahlentheorie; Verlag R. Oldenbourg, München 1956

Wolfart J.: Einführung in die Zahlentheorie und Algebra; Vieweg+Teubner, Wiesbaden, 2. Aufl. 2011

2. Bücher aus verwandten Gebieten insbesondere zu den Themen: Aufbau des Zahlensystems, Historisches, Populärwissenschaftliches

Aczel A.D.: Fermat's Last Theorem; Delta Book, New York 1996

Alten H.-W., Djafari Naini A., Folkerts M., Schlosser H., Schlote K.-H., Wußing H.: 4000 Jahre Algebra; Geschichte, Kulturen, Menschen, Springer Spektrum, Berlin Heidelberg, 2. Aufl. 2014

Artmann B.: Zahlen und Algebra in der Schule; Vorlesungsmanuskript, TH Darmstadt WS 1995/96

Baptist P.: Pythagoras – und kein Ende?; Ernst Klett Schulbuchverlag, Leipzig 1997

Beckmann P.: A History of π; The Golem Press, New York 1971

Bedürftig T. Murawski R.: Zählen – Grundlage der elementaren Arithmetik, Verlag Franzbecker, Hildesheim 2001

Beutelspacher A. / Petri B.: Der Goldene Schnitt; BI Verlag, Mannheim 1995

Cofman J.: Numbers and shapes revisited; Clarendon Press, Oxford 1995

Conway J. H. et al.: On Games and Numbers; London 1976

deutsche Übersetzung: Über Zahlen und Spiele, Braunschweig 1983

Conway J. H. / Guy R. K.: The Book of Numbers; Springer Verlag (Copernicus Imprint), New York 1996

Courant R. / Robbins H.: Was ist Mathematik? Springer-Verlag, Berlin 1962

Datta, B.; Singh, A.N. : History of Hindu mathematics: A source book; Asia Publishing House, Bombay 1935

Dedekind R.: Was sind und was sollen die Zahlen? (1887); 10. Auflage: Vieweg Verlag, Braunschweig, 1969

Dürr R. / Ziegenbalg J.: Dynamische Prozesse und ihre Mathematisierung durch Differenzengleichungen; Ferdinand Schöningh Verlag, Paderborn 1984
2. Auflage: Mathematik für Computeranwendungen; Ferdinand Schöningh Verlag, Paderborn 1989

Dunham W.: Journey Through Genius - The great theorems of mathematics; John Wiley & Sons 1990 and Penguin Books 1991, Harmondsworth, Middlesex, England

Dunham W.: The Mathematical Universe – An Alphabetical Journey Through the Great Proofs, Problems, and Personalities; John Wiley & Sons, New York 1994

Engel A.: Problem Solving Strategies; Springer Verlag, New York 1998

Enzensberger H. M.: Der Zahlenteufel; Carl Hanser Verlag, München 1997

Felscher W.: Naive Mengen und abstrakte Zahlen I, II, III; Bibliographisches Institut, Mannheim 1978

Ganzhorn K. / Walter W.: Die geschichtliche Entwicklung der Datenverarbeitung; IBM Deutschland, München 1975

Hankel H.: Vorlesungen über die Complexen Zahlen und ihre Functionen; Leopold Voss Verlag, Leipzig 1867

Hermes H.: Aufzählbarkeit, Entscheidbarkeit, Berechenbarkeit; SpringerVerlag, Berlin 1961

Herstein I. N. / Kaplansky I.: Matters Mathematical; Harper & Row Publishers, New York 1974

Huntley H. E.: The Divine Proportion; Dover Publications, New York 1970

Jacobs K.: Resultate: Ideen und Entwicklungen in der Mathematik, Vieweg Verlag, Braunschweig 1987 und 1990
Band 1: Proben mathematischen Denkens
Band 2: Der Aufbau der Mathematik

Kaiser H. / Nöbauer W.: Geschichte der Mathematik (2-te erw. Auflage); Oldenbourg Verlag, Wien 1998 (besonders: Die Entwicklung des Zahlbegriffs, S102-141)

Kamke E.: Mengenlehre; W. de Gruyter Verlag (Sammlung Göschen); Berlin 1965

Karlson P.: Zauber der Zahlen; Ullstein Verlag, Frankfurt a. M. 1965

Kempermann T.: Zahlentheoretische Kostproben; Verlag Harri Deutsch, Thun 1995

Kirsch A.: Elementare Zahlen- und Größenbereiche; Verlag Vandenhoeck und Ruprecht, Göttingen 1970

Kirsch A.: Aspekte des Vereinfachens im Mathematikunterricht; Didaktik der Mathematik, 2, 1977 (87-101)

Kirsch A.: Beispiele für „prämathematische“ Beweise; Schriftenreihe Didaktik der Mathematik, Universität für Bildungswissenschaften, Klagenfurt, Band 2: Beweisen im Mathematikunterricht, Verlag Hölder-Pichler-Tempsky, Wien 1979, (S. 261-274)

Kirsch A.: Mathematik wirklich verstehen; Aulis Verlag Deubner, Köln 1987

Kleine Enzyklopädie Mathematik; Leipzig 1977, Lizenzausgabe für den Verlag Harri Deutsch (komprimierte Ausgabe: Mathematik Ratgeber; Harri Deutsch)

Kramer J.: Zahlen für Einsteiger, Friedr. Vieweg Verlag, Wiesbaden 2008

Landau E.: Grundlagen der Analysis; Wiss. Buchgesellschaft, Darmstadt 1963

Lehmann J.: So rechneten Ägypter und Babylonier; Urania Verlag / Reinhardt Becker Verlag, Leipzig 1994

Lehmann J.: So rechneten Griechen und Römer; Urania Verlag / Reinhardt Becker Verlag, Leipzig 1994

Leuders T.: Erlebnis Arithmetik, Spektrum Akademischer Verlag, Heidelberg 2010

Lietzmann W.: Anschauliche Arithmetik und Algebra; Physica-Verlag, Würzburg 1956

Lietzmann W.: Riesen und Zwerge im Zahlenreich; Teubner Verlagsgesellschaft, Leipzig 1969

Lüneburg H.: Leonardi Pisani Liber Abaci oder Lesevergnügen eines Mathematikers; BI Wissenschaftsverlag, Mannheim 1992

Mäder P.: Mathematik hat Geschichte; Metzler Verlag, Hannover 1992

Maor Eli: e – The Story of a Number; Princeton University Press, Princeton 1994

Oberschelp A.: Aufbau des Zahlensystems; Vandenhoeck & Ruprecht, Göttingen, 1968

Ogilvy C. S. / Anderson J. T.: Excursions in Number Theory; Dover Publications, New York 1988 (Oxford University Press 1966)

Olds C. D.: Continued Fractions; Mathematical Association of America, 1963 Yale University

Padberg F.: Didaktik der Arithmetik; B.I. Verlag, Mannheim 1991

Padberg F.: Didaktik der Bruchrechnung; Spektrum Verlag, Heidelberg 1995

Padberg F. / Danckwerts R. / Stein M.: Zahlbereiche – eine elementare Einführung; Springer Spektrum, Berlin Heidelberg, 4. Aufl. 2009

Posamentier A.S. / Lehmann I.: The Fabulous Fibonacci Numbers, Prometheus Books, Amherst (New York) 2007

Posamentier A.S. / Lehmann I.: The Glorious Golden Ration, Prometheus Books, Amherst (New York) 2012

Rademacher H. / Toeplitz O.: Von Zahlen und Figuren; Springer-Verlag, Berlin 1968

Rautenberg W.: Reelle Zahlen in elementarer Darstellung; Klett Verlag, Stuttgart 1979

Ries Adam: Rechnung auff der Linihen und Federn Auff allerley hanthirung gemacht durch Adam Risen; 1522 (114. Auflage herausgegeben vom Magistrat der Stadt Erfurt 1991)

Schreiber Peter: Euklid, BSB B.G. Teubner Verlagsgesellschaft, Leipzig 1987

Schroeder M. R.: Number Theory in Science and Communication; Springer-Verlag, Berlin Heidelberg 5th ed. 2009

Singh S.: Fermat's Last Theorem / (in the U.S.A.) Fermat's Enigma; Anchor Books, Doubleday, New York 1998

Specht R. (Hrsg.): Geschichte der Philosophie in Text und Darstellung, Band 5: Rationalismus, Reclam Verlag, Stuttgart 1979

Staffelsteiner Schriften: Adam Rieß von Staffelstein – Rechenmeister und Cossist, Staffelstein 1992

Strehl R.: Zahlbereiche; Herder Verlag, Freiburg 1972

Tarski A.: Einführung in die mathematische Logik; Vandenhoeck & Ruprecht, Göttingen 1966

Taschner R.: Der Zahlen gigantische Schatten; Friedr. Vieweg & Sohn Verlag, Wiesbaden 2005

van der Waerden B.L.: Erwachende Wissenschaft; Birkhäuser Verlag, Basel 1966

Wells D.: The Penguin Dictionary of Curious and Interesting Numbers; Penguin Books, London 1986

Wußing H.: Adam Ries; BSB B.G. Teubner Verlagsgesellschaft, Leipzig 2. Aufl. 1992

Wußing H. u.a.: Vom Zählstein zum Computer – Mathematik in der Geschichte, Band 1; diverlag franzbecker, Hildesheim 1997

Wußing H.: 6000 Jahre Mathematik;
Band 1: Eine kulturgeschichtliche Zeitreise – von den Anfängen bis Leibniz und Newton, Springer Spektrum, Heidelberg Berlin 2008

3. Bücher zum Themenbereich: Algorithmen in der Zahlentheorie

Allenby R. B. J. T. / Redfern E. J.: Introduction to number theory with computing; E. Arnold, London 1989

Deutsches Institut für Fernstudien (DIFF): Algorithmen in der elementaren Zahlentheorie (CM 1); Tübingen 1988

Engel A.: Elementarmathematik vom algorithmischen Standpunkt; Klett Verlag, Stuttgart 1977

Engel A.: Mathematisches Experimentieren mit dem PC; Klett Verlag, Stuttgart 1991

Jeger Max: Computer-Streifzüge - Eine Einführung in Zahlentheorie und Kombinatorik aus algorithmischer Sicht; Birkhäuser Verlag, Basel 1986

Sloane N. J. A. / Plouffe S.: The Encyclopedia of Integer Sequences; Academic Press, 1995

Wagon S.: Mathematica in Action; W.H Freeman and Company, New York 1991

Ziegenbalg J.: Algorithmen – von Hammurapi bis Gödel; Verlag Harri Deutsch, Frankfurt am Main, 3. Auflage 2010

4. Bücher zum Thema: Zahlentheorie und Kryptologie

Bauer F. L.: Kryptologie – Methoden und Maximen; Springer-Verlag, Berlin Heidelberg, 2. Aufl. 1994

Beutelspacher A.: Kryptologie; Vieweg+Teubner, Wiesbaden, 9. Aufl. 2009

Beutelspacher A. / Schwenk J. / Wolfenstetter K.-D.: Moderne Verfahren der Kryptographie; Vieweg+Teubner, Wiesbaden, 7. Aufl. 2010

Grams T.: Codierungsverfahren, Bibliographisches Institut (B.I.), Mannheim 1986

Horster P.: Kryptologie; BI Verlag, Zürich 1985

Koblitz N.: A Course in Number Theory and Cryptography; Springer Verlag, New York 2nd ed. 1994

Schulz R.-H.: Codierungstheorie – Eine Einführung; Vieweg Verlag, Wiesbaden, 2. Aufl. 2003

Sinkov A.: Elementary Cryptanalysis; Mathematical Association of America, 1966 Yale University

Index