

Herbert Möller

**Elementare Zahlentheorie  
und Problemlösen**

Kompass-Buch

Prof. a. D. Dr. H. Möller

Mathematisches Institut der Universität

Einsteinstr. 62, D-48149 Münster

E-Mail: [mollerh@math.uni-muenster.de](mailto:mollerh@math.uni-muenster.de).

WWW: <http://www.math.uni-muenster.de/u/mollerh> (Die Webseite hat den Namen *Mathkompass*, mit dem sie auch im Folgenden zitiert wird).

Dieses Buch wurde mit dem (L<sup>A</sup>T<sub>E</sub>X-) Satzsystem OzT<sub>E</sub>X4.0 von Andrew Trevor-  
row, dem Texteditor *ALPHA7* von Pete Keleher und für die Pdf-Erzeugung mit  
dem Satzsystem TeXShop 2 (Entwicklung koordiniert von Richard Koch, Dirk  
Olmes und Gerben Wierda) auf Macintosh-Computern hergestellt.

OzT<sub>E</sub>X4.0 ist ein Shareware-Programm (<http://www.trevorrow.com>),

*ALPHA7* ist ein Shareware-Programm

(<http://www.kelehers.org/alpha>),

TeXShop 2 ist ein GNU Public Licence Programm

(<http://www.uoregon.edu/~koch/texshop>).

Macintosh ist ein Warenzeichen der Apple Computer, Inc.

*Copyright* © 2008 Herbert Möller.

*Permission is granted to copy, distribute and/or modify this document under the terms of the GNU Free Documentation License, Version 1.2 or any later version published by the Free Software Foundation; with no Invariant Sections, no Front-Cover Texts, and no Back-Cover Texts. A copy of the license is included in the section entitled “GNU Free Documentation License” (page 239).*

Dieses Buch gehört zu dem Projekt “Vitale Mathematik”. Im *Mathkompass* unter ‘Sonstiges’ gibt es einen Link auf einen Bericht über “Ergebnisse und Ziele”, der auch eine Projektbeschreibung enthält. Der Quelltext des Buches wird zum Beispiel für Übersetzungen vom Autor zur Verfügung gestellt.

*Letzte Korrektur am 29.8.2011*

# Vorwort

Dieses Buch ist aus mehreren Lehrveranstaltungen hervorgegangen, die jeweils von der üblichen Form abwichen. Die Standardvorlesung “Elementare Zahlentheorie” war im Sommersemester 2001 eine “Jubiläumsvorlesung”, weil im Jahre 1801 das Buch “*Disquisitiones arithmeticae*” [9] von C. F. GAUß<sup>1</sup> erschienen ist. Es enthielt zum ersten Mal den größten Teil der Ergebnisse, die noch heute die “elementare Zahlentheorie” bilden. Schon bevor dieses Buch 1889 mit dem Titel “Untersuchungen über höhere Arithmetik” ins Deutsche übersetzt wurde, gehörte es zu den bedeutendsten Werken der Mathematik.

Da GAUß viele Zusammenhänge durch umfangreiche Rechnungen gefunden hat, führte die Vorlesung einerseits zu einer Rückbesinnung auf “konkrete” Mathematik als Ausgleich für die zunehmende Abstraktheit durch “Algebraisierung”, und andererseits wurden an mehreren geeigneten Stellen Ausblicke auf die weitere Entwicklung der Zahlentheorie gegeben. Eine im Sommersemester 1989 durchgeführte Vorlesung mit dem Titel “Höhere Zahlentheorie mit Mikrocomputern” lieferte außerdem das Material für die Berücksichtigung effizienter Berechnungsverfahren und aktueller Anwendungen.

Untersuchungsobjekte der elementaren Zahlentheorie sind die natürlichen, die ganzen und die rationalen Zahlen, deren Kenntnis normalerweise vorausgesetzt wird. Wiederholte Nachfragen ergaben, dass nur wenige Studierende etwas von der Einführung der natürlichen Zahlen mit Hilfe der PEANO-Axiome gehört haben, und keiner von ihnen wusste, wie sich damit die Verknüpfungen definieren lassen. Deshalb wurde eine geeignete Präzisierung der natürlichen Zahlen an den Anfang der Vorlesung gestellt. Hier wird diese Skizze durch einen Ausblick auf die Brüche und die ganzen Zahlen in Form einer “zweiten Textsorte” ergänzt.

Die vielen Besonderheiten der Jubiläumsvorlesung veranlassten den Studenten *Thorsten Wetter*, völlig freiwillig die Vorlesung mit einem Textsystem so aufzuschreiben, dass andere Studierende die Ausarbeitung kopieren konnten. Anschließend hat er im Rahmen seiner Staatsexamensarbeit mit dem Titel “Hochschuldidaktische Aspekte einer Zahlentheorievorlesung” eine L<sup>A</sup>T<sub>E</sub>X-Version angefertigt, die die Herstellung dieses E-Buches motivierte.

---

<sup>1</sup> CARL FRIEDRICH GAUß (1777-1855) wirkte in Göttingen.

Der Problemlöseteil verwendet ebenfalls teilweise den Text einer Staatsexamensarbeit. *Stefan Krämer* hat sie 2001 mit dem Titel “Analyse und Weiterentwicklung eines Seminars über Problemlösen in der Zahlentheorie für Lehramtsstudierende” geschrieben. Dieses Seminar wurde von 1997 bis 2004 elfmal durchgeführt. Alle TeilnehmerInnen gestalteten jeweils eine Sitzung mit zwei Aufgaben: Zuerst musste ein Vortrag über ein Zahlentheorieproblem der *Internationalen Mathematikolympiade* (IMO) mit besonderer Herausarbeitung der Findestrategien gehalten werden; anschließend war eine zahlentheoretische Aufgabe des *Bundeswettbewerbs Mathematik* (BWM) von den übrigen TeilnehmerInnen in der Form einer Unterrichtssimulation mit “suggestionsarmer” Anleitung zu lösen.

Der erfreuliche Effekt, dass die Studierenden auf diese Weise innerhalb eines Semesters gute Problemlösefähigkeiten entwickelten, lässt sich leider nicht ohne Weiteres durch ein Buch erreichen, weil das aktive Handeln fehlt. Dennoch soll hier versucht werden, auch in die “Kunst des Problemlösens” einzuführen, die im Anschluss an einen mehr als 2500 Jahre alten griechischen Begriff “*Heuristik*” heißt.

Deshalb sind in diesem Buch - anders als in der Vorlesung - einige Findestrategien bereits in den Text und vor allem in die Beweise integriert. Im sechsten Kapitel finden sich dann die wesentlichen Methoden systematisch mit geeigneten Beispielen zusammengestellt. Außerdem wird bei einer Reihe von zahlentheoretischen Problemen des BWM und der IMO eine das Problemlösen fördernde Art der Lösungsvermittlung vorgestellt, die Überlegungen aus der Staatsexamensarbeit von *Elisabeth Mahn* mit dem Titel “Erschließung von Zahlentheorieproblemen des Bundeswettbewerbs Mathematik im Hinblick auf fragend-entwickelnden Unterricht” verwendet.

Alle Sätze haben suggestive Namen, mit denen sie zitiert werden. Die Beweise der Sätze beginnen jeweils mit der Angabe des Beweistyps, des “methodischen” Typs und des Schwierigkeitsgrades. Die methodischen Typbezeichnungen sind r (routinemäßiger Beweis), a (anregender Beweis) und h (herausfordernder Beweis). Der Schwierigkeitsgrad wird mit 1 (leichter Beweis), 2 (mittelschwerer Beweis) und 3 (schwerer Beweis) gekennzeichnet.

Als Besonderheiten bietet dieses Buch auch ein Verzeichnis aller Sätze und ein ausgedehntes Referenzsystem, das in der Online-Version Hypertext-Sprünge zu den angegebenen Seiten oder Gleichungen ermöglicht.

Münster, im August 2008

H. Möller

# Inhaltsverzeichnis

|  |           |
|--|-----------|
| <b>Vorwort</b>   | <b>3</b>  |
| <b>Inhaltsverzeichnis</b>  | <b>5</b>  |
| <b>1 Die natürlichen Zahlen</b>  | <b>7</b>  |
| 1.1 Grundlegung . . . . .  | 7         |
| 1.2 Die Beweissätze . . . . .  | 10        |
| 1.3 Verknüpfungen von natürlichen Zahlen . . . . .                     | 12        |
| 1.4 Einführung in die elementare Zahlentheorie . . . . .               | 14        |
| 1.5 Abgrenzungen . . . . .   | 16        |
| <b>2 Teilbarkeit</b>   | <b>17</b> |
| 2.1 Teiler von ganzen Zahlen . . . . .                                 | 17        |
| 2.2 Der größte gemeinsame Teiler von zwei natürlichen Zahlen . . . . . | 19        |
| 2.3 Der Kettenbruchalgorithmus und die lineare diophantische Gleichung | 23        |
| 2.4 Die Gaußsche Erkundungsstrategie . . . . .                         | 30        |
| 2.5 Die Kernbruchstrategie und pythagoreische Tripel . . . . .         | 35        |
| 2.6 Die $g$ -adische Zahlendarstellung . . . . .                       | 40        |
| 2.7 Aufgaben und Probleme zu Kapitel 2 . . . . .                       | 43        |
| <b>3 Elementare Primzahltheorie</b>                                    | <b>47</b> |
| 3.1 Definition und grundlegende Eigenschaften der Primzahlen . . . . . | 47        |
| 3.2 Der Hauptsatz der elementaren Zahlentheorie . . . . .              | 49        |

|          |  |            |
|----------|--|------------|
| 3.3      | Anwendungen des Hauptsatzes . . . . .                              | 53         |
| 3.4      | Vollkommene Zahlen und spezielle Primzahlen . . . . .              | 56         |
| 3.5      | Verteilung der Primzahlen . . . . .                                | 62         |
| 3.6      | Ausblick auf bedeutende Resultate der analytischen Primzahltheorie | 71         |
| 3.7      | Aufgaben und Probleme zu Kapitel 3 . . . . .                       | 76         |
| <b>4</b> | <b>Kongruenzen</b>   | <b>83</b>  |
| 4.1      | Die Kongruenzrelation . . . . .                                    | 83         |
| 4.2      | Restklassen . . . . .  | 84         |
| 4.3      | Kongruenzsätze . . . . .   | 91         |
| 4.4      | Eigenschaften der Restsysteme . . . . .                            | 92         |
| 4.5      | Die Eulersche Phi-Funktion . . . . .                               | 98         |
| 4.6      | Kongruenzen mit einer Unbekannten . . . . .                        | 101        |
| 4.7      | Potenzreste . . . . .  | 106        |
| 4.8      | Ordnungen, Primitivwurzeln und Indizes . . . . .                   | 120        |
| 4.9      | Aufgaben und Probleme zu Kapitel 4 . . . . .                       | 130        |
| <b>5</b> | <b>Ergänzungen</b>   | <b>137</b> |
| 5.1      | Die Faltung zahlentheoretischer Funktionen . . . . .               | 137        |
| 5.2      | Darstellung als Summe von Quadraten . . . . .                      | 141        |
| 5.3      | Binäre quadratische Formen und die Klassengruppe . . . . .         | 151        |
| 5.4      | Quadratische Zahlkörper . . . . .                                  | 163        |
| <b>6</b> | <b>Problemlösestrategien in der Zahlentheorie</b>                  | <b>181</b> |
|          | <b>Satzverzeichnis</b>   | <b>235</b> |
|          | <b>Symbolverzeichnis</b>   | <b>238</b> |
|          | <b>GNU Free Documentation License</b>                              | <b>239</b> |
|          | <b>Literaturverzeichnis</b>  | <b>247</b> |
|          | <b>Index</b>   | <b>249</b> |

# Kapitel 1

## Die natürlichen Zahlen

### 1.1 Grundlegung

Die fünf Axiome, die GIUSEPPE PEANO 1891 formuliert hat und mit denen üblicherweise die natürlichen Zahlen eingeführt werden, entsprechen nicht der Erfahrung der Menschen sondern stellen ein Endprodukt mathematisch-logischer Forschung dar. Grundsätzlich ist ein Axiomensystem nicht geeignet, die natürlichen Zahlen eindeutig festzulegen. Deshalb wird in heutiger Sprechweise eine *Struktur* definiert, von der schon PEANO beweisen konnte, dass alle möglichen Realisierungen (‘‘Modelle’’) zueinander ‘‘isomorph’’ (d. h. mathematisch äquivalent) sind.

#### Definition der Peano-Struktur

Ein Tripel  $(\mathcal{N}, a, \nu)$  bestehend aus einer Menge  $\mathcal{N}$ , einem ausgezeichneten Element  $a \in \mathcal{N}$  und einer injektiven Abbildung  $\nu : \mathcal{N} \rightarrow \mathcal{N} \setminus \{a\}$  (‘‘Nachfolgerabbildung’’) heißt *Peano-Struktur*, wenn das folgende *Induktionsaxiom* erfüllt ist: Stellt  $\mathcal{M}$  eine Teilmenge von  $\mathcal{N}$  mit  $a \in \mathcal{M}$  und  $\nu(n) \in \mathcal{M}$  für alle  $n \in \mathcal{M}$  dar, so gilt  $\mathcal{M} = \mathcal{N}$ .

Vier der ursprünglichen *Peano-Axiome* stecken jetzt in der Charakterisierung der Nachfolgerabbildung. Bei der nicht auszuschließenden Modellvielfalt ist es trotz des Isomorphiebeweises von PEANO problematisch, von **den** natürlichen Zahlen zu sprechen. Der größte Mangel des Axiomensystems von PEANO beziehungsweise der obigen Definition ist jedoch die nachgewiesene Unmöglichkeit, die Widerspruchsfreiheit zu zeigen. Das bedeutet vor allem, dass im Rahmen der Theorie, die durch die Axiome begründet werden soll, gar kein Modell angegeben werden kann.

Bei all diesen Schwierigkeiten überrascht es nicht, dass viele Mathematikstudierende die Peano-Axiome lediglich glauben. Insbesondere ist ihnen nicht klar, was die Nachfolgerabbildung bedeutet und wieso das Induktionsaxiom gültig sein soll, das unendliche Mengen vergleicht, während unser Universum als endlich angenommen wird.

Obwohl zum Verständnis der elementaren Zahlentheorie solche Kenntnisse der Grundlagen der Mathematik nicht unbedingt nötig sind, soll doch zunächst ein alternativer Zugang skizziert werden, der diese Fragen klärt und der insbesondere die beiden wichtigen Beweisverfahren, die meistens “*Minimumprinzip*” und “*Induktionsprinzip*” heißen, als einprägsam hergeleitete Sätze verstehen lässt.

Die zugehörige Basistheorie hat den Titel “*Zahlgenese*”, weil sie im Unterschied zum wissenschaftsorientierten “*Zahlensystem*” die Schwierigkeiten der Lernenden in den entsprechenden Altersstufen berücksichtigt. Unter anderem wird anstelle der didaktisch fragwürdigen “*axiomatischen Methode*” von DAVID HILBERT (1899) die “*Postulat-Methode*” von EUKLID ( $\approx 325$  v. Chr.) verwendet. Das Hypertext-Buch *Zahlgenese* [16] ist im *Mathkompas* [14] erschienen.

Ausgehend von dem durch GEORG CANTOR 1874 eingeführten Mengenbegriff wird zuerst die “*Gleichmächtigkeit*” von zwei Mengen  $\mathcal{M}_1$  und  $\mathcal{M}_2$  dadurch definiert, dass es eine bijektive Abbildung von  $\mathcal{M}_1$  auf  $\mathcal{M}_2$  gibt. Die ersten beiden der folgenden sieben Postulate beruhen einerseits auf Einsichten, die die Menschheit im Laufe von Jahrtausenden gewonnen hat und die in angepasster Form schon Kindern in der Grundschule vermittelt werden. Andererseits definieren sie implizit die “*C-Mengen*”, die für diesen Aufbau grundlegend sind.

### Kardinalzahlpostulate

a) Jede *C-Menge*  $\mathcal{M}$  hat eine Eigenschaft - *Kardinalzahl* von  $\mathcal{M}$  genannt und  $\text{card } \mathcal{M}$  geschrieben -, die sich für alle *C-Mengen*  $\mathcal{A}$  und  $\mathcal{B}$  folgendermaßen vergleichen lässt:

Definitionsgemäß ist  $\text{card } \mathcal{A} = \text{card } \mathcal{B}$ , wenn  $\mathcal{A}$  und  $\mathcal{B}$  gleichmächtig sind.

Definitionsgemäß gilt  $\text{card } \mathcal{A} \leq \text{card } \mathcal{B}$ , wenn  $\mathcal{B}$  eine zu  $\mathcal{A}$  gleichmächtige Teilmenge enthält.

Definitionsgemäß ist  $\text{card } \mathcal{A} < \text{card } \mathcal{B}$ , wenn  $\text{card } \mathcal{A} \leq \text{card } \mathcal{B}$  gilt, aber nicht  $\text{card } \mathcal{A} = \text{card } \mathcal{B}$  erfüllt ist.

b) Für je zwei *C-Mengen*  $\mathcal{A}$ ,  $\mathcal{B}$  gilt genau eine der Beziehungen  $\text{card } \mathcal{A} = \text{card } \mathcal{B}$  oder  $\text{card } \mathcal{A} < \text{card } \mathcal{B}$  oder  $\text{card } \mathcal{B} < \text{card } \mathcal{A}$ .

Wie üblich werden die Zeichen “ $\leq$ ” bzw. “ $<$ ” “kleiner gleich” bzw. “kleiner” gelesen, und anstelle von  $\text{card } \mathcal{A} \leq \text{card } \mathcal{B}$  bzw.  $\text{card } \mathcal{A} < \text{card } \mathcal{B}$  wird auch  $\text{card } \mathcal{B} \geq \text{card } \mathcal{A}$  bzw.  $\text{card } \mathcal{B} > \text{card } \mathcal{A}$  verwendet und entsprechend gelesen.

### Erzeugungspostulate

- a) Die leere Menge  $\emptyset$  ist eine C-Menge mit  $0 := \text{card } \emptyset$ .
- b) Alle Mengenbildungen, die für Mengen im Sinne von CANTOR gebraucht werden (Klammerung, Teilmenge, Durchschnitt, Differenz, Vereinigung, Produkt und Potenz), ergeben zu C-Mengen wieder C-Mengen.

Die “*natürlichen Zahlen*” sind die Kardinalzahlen der “*endlichen Mengen*”, deren korrekte Definition unabhängig voneinander von BERNARD BOLZANO (1851) und R. DEDEKIND<sup>1</sup> (1888) gefunden wurde.

### Definition der endlichen und der unendlichen Menge

Eine Menge heißt *endlich*, wenn sie zu keiner ihrer echten Teilmengen gleichmächtig ist. Andernfalls heißt sie *unendlich*.

### Zugehörigkeitspostulate

- a) Jede endliche Menge ist eine C-Menge.
- b) Die Zusammenfassung  $\mathbb{N}$  (nach DIN 1302) der Kardinalzahlen aller endlichen Mengen ist eine C-Menge.

Die meisten Mengen, die wir im täglichen Leben betrachten, sollen C-Mengen sein. Die Zusammenfassung aller endlichen Mengen bildet **keine** C-Menge. Als ausgezeichnete Vertreter (“*Repräsentanten*”) der endlichen Mengen verwenden wir die “*Anfänge*”

$$\mathcal{A}_n := \{m \in \mathbb{N} ; m < n\} \text{ mit } n \in \mathbb{N}.$$

Die C-Menge  $\mathcal{A}_n$  heißt *n-Anfang von  $\mathbb{N}$* . Das folgende starke Postulat gibt die Erfahrung wieder, dass die Kardinalzahl einer endlichen Menge durch “Auszählen” bestimmt werden kann.

<sup>1</sup> RICHARD DEDEKIND (1831-1916) wirkte in Göttingen und Braunschweig.

### Anfängepostulat

Für jedes  $n \in \mathbb{N}$  gilt  $\text{card } \mathcal{A}_n = n$ .

Der Beweis des nächsten Satzes lässt sich weitgehend mit Hilfe dieses Postulats führen, wobei im Folgenden stets die Abkürzungen

$$\mathbb{N}_k := \mathbb{N} \setminus \mathcal{A}_k \text{ mit } k \in \mathbb{N} \text{ und } k > 0$$

verwendet werden. Außerdem ist zu beachten, dass  $\{\mathcal{M}\} \neq \mathcal{M}$  für beliebige C-Mengen  $\mathcal{M}$  gilt.

### Nachfolgersatz

Die *Nachfolgerabbildung*  $\nu : \mathbb{N} \rightarrow \mathbb{N}_1$ ,  $\text{card } \mathcal{E} \mapsto \text{card } (\mathcal{E} \cup \{\mathcal{E}\})$  ist *wohldefiniert* (d. h. unabhängig von der Auswahl der endlichen Menge  $\mathcal{E}$ ). Sie hat folgende Eigenschaften:

- a) (*Zunahme*) Für jedes  $m \in \mathbb{N}$  ist  $m < \nu(m)$ .
- b) (*Lückenlosigkeit*) Ist  $m \leq n \leq \nu(m)$  für  $m, n \in \mathbb{N}$ , so gilt  $n = m$  oder  $n = \nu(m)$ .
- c) (*Anfängetreue*) Für jedes  $m \in \mathbb{N}$  ist  $\mathcal{A}_{\nu(m)} = \{0\} \cup \nu(\mathcal{A}_m) = \mathcal{A}_m \cup \{m\}$ .
- d) (*Bijektivität*) Die Nachfolgerabbildung ist bijektiv.

Für C-Mengen  $\mathcal{A}$  wird  $1 := \text{card } \{\mathcal{A}\}$  gesetzt, weil es keine Kardinalzahl  $n$  mit  $0 < n < \text{card } \{\mathcal{A}\}$  gibt, da  $\mathcal{A}$  nach CANTOR das einzige Element von  $\{\mathcal{A}\}$  ist. Die spätere Einführung der “Addition” von natürlichen Zahlen (Seite 13) geht dann von der Gleichsetzung  $n + 1 := \nu(n)$  aus.

## 1.2 Die Beweissätze

Nun lassen sich die beiden oben genannten wichtigen Beweisverfahren durch Sätze begründen. Die skizzenhafte Herleitung des “*Minimumsatzes*” beruht auf der expliziten Angabe des Minimums, das vorweg für nicht leere Teilmengen von  $\mathbb{N}$  definiert wird. Der Beweis des grundlegenden “*Induktionssatzes*” erfolgt dann einprägsam mit Hilfe des *Minimumsatzes*.

### Definition des Minimums

Ist  $\mathcal{T}$  eine nicht leere Teilmenge von  $\mathbb{N}$ , so heißt ein Element  $m \in \mathcal{T}$  *Minimum* von  $\mathcal{T}$ , wenn  $m \leq n$  für alle  $n \in \mathcal{T}$  gilt.

Das Minimum einer nicht leeren Teilmenge  $\mathcal{T}$  von  $\mathbb{N}$  ist wegen des zweiten *Kardinalzahlpostulats* (Seite 8) eindeutig bestimmt. Bei dem folgenden *Minimumsatz* wird das Minimum in drei Schritten gewonnen. i) Im Falle  $0 \in \mathcal{T}$  stellt 0 das Minimum von  $\mathcal{T}$  dar. ii) Gehört 0 nicht zu  $\mathcal{T}$  und ist  $b$  ein beliebiges Element von  $\mathcal{T}$ , so wird für die nicht leere, endliche Menge  $\mathcal{U} := \{c \in \mathcal{A}_b ; \mathcal{A}_{\nu(c)} \cap \mathcal{T} = \emptyset\}$  mit der Kardinalzahl  $m$  gezeigt, dass  $\mathcal{U} = \mathcal{A}_m$  gilt. iii) Mit einfachen Schlüssen folgt dann, dass  $m$  das Minimum von  $\mathcal{T}$  ist.

### Minimumsatz

Jede nicht leere Teilmenge von  $\mathbb{N}$  besitzt genau ein Minimum.

Das Minimum von  $\mathcal{T}$  wird mit  $\min \mathcal{T}$  bezeichnet. Mit Hilfe des *Minimumsatzes* lässt sich der *Maximumsatz* herleiten. Dazu benötigen wir zwei Begriffe.

### Definition der Beschränktheit und des Maximums

- a) Eine Teilmenge  $\mathcal{T}$  von  $\mathbb{N}$  heißt *beschränkt*, wenn es ein  $b \in \mathbb{N}_1$  gibt, sodass  $\mathcal{T} \subseteq \mathcal{A}_b$  gilt.
- b)  $M \in \mathcal{T}$  heißt *Maximum* von  $\mathcal{T}$ , wenn  $t \leq M$  für alle  $t \in \mathcal{T}$  erfüllt ist.

### Maximumsatz

Jede nicht leere, beschränkte Teilmenge von  $\mathbb{N}$  besitzt genau ein Maximum.

**Beweis** Es sei  $\mathcal{T} \subseteq \mathcal{A}_b$  mit  $b \in \mathbb{N}_1$ . Dann ist  $b \in \mathcal{V} := \{n \in \mathbb{N} \mid \mathcal{T} \subseteq \mathcal{B}_n\}$ . Aufgrund des *Minimumsatzes* kann also  $M := \min \mathcal{V}$  gesetzt werden. Der Fall  $M = 0$  tritt nur ein, wenn  $\mathcal{T} = \mathcal{B}_0$  ist. Andernfalls gibt es wegen der *Bijektivität* von  $\nu$  (Seite 10) ein  $L \in \mathbb{N}$  mit  $\nu(L) = M$ . Aus der *Anfängerstreue* von  $\nu$  folgt  $\mathcal{T} \subseteq \mathcal{B}_L \cup \{M\}$ . Wegen  $L < M$  ist  $\mathcal{T}$  keine Teilmenge von  $\mathcal{B}_L$ . Also gilt  $M \in \mathcal{T}$ , und wegen  $\mathcal{T} \subseteq \mathcal{B}_M$  ist  $t \leq M$  für alle  $t \in \mathcal{T}$ . Aufgrund des *Kardinalzahlpostulats* b) enthält  $\mathcal{T}$  nur ein Maximum. Dieses wird mit  $\max \mathcal{T}$  bezeichnet.  $\square$

### Induktionssatz

Ist  $\mathcal{M}$  eine Teilmenge von  $\mathbb{N}$  mit  $0 \in \mathcal{M}$  und  $\nu(n) \in \mathcal{M}$  für alle  $n \in \mathcal{M}$ , so gilt  $\mathcal{M} = \mathbb{N}$ .

**Beweis** (durch Widerspruch, a1):

Wir nehmen an, es wäre  $\mathcal{M} \neq \mathbb{N}$ . Dann ist  $\mathcal{M}' := \mathbb{N} \setminus \mathcal{M} \neq \emptyset$ . Aufgrund des *Minimumsatzes* besitzt  $\mathcal{M}'$  ein Minimum  $m$ . Wegen  $0 \in \mathcal{M}$  ist  $m > 0$ . Die Bijektivitätsaussage des *Nachfolgersatzes* (Seite 10) ergibt, dass ein  $k \in \mathbb{N}$  mit  $\nu(k) = m$  existiert. Aus  $k < m$  (Zunahmeaussage im *Nachfolgersatz*) folgt  $k \in \mathcal{M}$  und damit nach Voraussetzung auch  $m = \nu(k) \in \mathcal{M}$  - im Widerspruch zu  $m \in \mathcal{M}'$ .  $\square$

### Beweis durch vollständige Induktion

Bei dem **Beweis durch vollständige Induktion** (kurz: “**Induktionsbeweis**”) wird im **Induktionsschritt** häufig eine Formulierung der folgenden Art gebraucht: “Es sei  $n \in \mathbb{N}$  eine Zahl, für die die zu beweisende Aussage schon gezeigt ist. Nun soll die entsprechende Aussage für  $n + 1$  hergeleitet werden.” (Ab Seite 13 wird  $n + 1$  anstelle von  $\nu(n)$  geschrieben.) Dadurch entsteht zumindest bei Mathematiklernenden Verwirrung, weil hier ohne ausreichende Trennung eine Aussage über Aussagen gemacht wird. Wir führen deshalb Induktionsbeweise stets im Anschluss an den **Induktionssatz** mit Hilfe einer Menge  $\mathcal{M}$ , die die zu beweisende Aussage in den Mengenklammern eingeschlossen enthält. Anstelle von  $\mathbb{N}$  kann auch eine “Induktionsmenge” der Form  $\mathbb{N}_b$  auftreten, sodass der **Induktionsanfang**  $b \in \mathcal{M}$  ist. Der **Induktionsschritt** hat meistens die Form: “Für jedes  $m \in \mathcal{M}$  gilt  $m + 1 \in \mathcal{M}$ .”

## 1.3 Verknüpfungen von natürlichen Zahlen

In engem Zusammenhang mit dem Induktionsbeweis steht die *Definition durch Rekursion*. Als erstes werden wir die Addition und die Multiplikation von natürlichen Zahlen einführen. Zum Beispiel lässt sich die Summe  $i + j$  für  $i, j \in \mathbb{N}_1$  in der Form  $\underbrace{\nu(\cdots \nu(i) \cdots)}_j$  durch wiederholte Anwendung der Nachfolgerabbildung gewinnen. Weitere Beispiele sind die Einführung der *Potenz*  $a^n := \underbrace{a \cdots a}_n$ , der “*Fakultät*”  $n! := 1 \cdots n$  und des Summenzeichens.

In allen diesen Beispielen muss jeweils die Existenz und die Eindeutigkeit einer Abbildung von  $\mathbb{N}$  bzw.  $\mathbb{N}_1$  nach einer C-Menge  $\mathcal{C}$  mit den gewünschten Eigenschaften gezeigt werden. Das leistet mit großer Allgemeinheit der *Rekursionssatz* von DEDEKIND (1888). Dabei wird die gesuchte Abbildung mit Hilfe der Anfänge konstruktiv gewonnen.

### Rekursionssatz

Ist  $\mathcal{C}$  eine C-Menge,  $a \in \mathcal{C}$  und  $g : \mathbb{N} \times \mathcal{C} \rightarrow \mathcal{C}$  eine Abbildung ( “*Rekursionsbedingung*”), so gibt es genau eine Abbildung  $f : \mathbb{N} \rightarrow \mathcal{C}$  mit

- a)  $f(0) = a$  und
- b)  $f(\nu(n)) = g(n, f(n))$  für alle  $n \in \mathbb{N}$ .

Wie bei der obigen Vorüberlegung soll nun die *Addition zu einer festen Zahl*  $i \in \mathbb{N}_1$  und die *Multiplikation mit einer festen Zahl*  $i \in \mathbb{N}_1$  rekursiv definiert werden. Für die gesuchte von  $i$  abhängige Abbildung  $f$  schreiben wir deshalb vorübergehend  $\oplus_i$  bzw.  $\odot_i$  und versuchen, die gewünschten Eigenschaften durch die Objekte des *Rekursionssatzes* auszudrücken. Die “Startgleichung”  $\oplus_i(0) = i$  legt es nahe,  $\mathcal{C} := \mathbb{N}$  und  $a := i$  zu wählen. Da  $\oplus_i(\nu(k)) = \nu(\oplus_i(k))$  gelten soll, stellt dann  $g : \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$ ,  $(n, k) \mapsto \nu(k)$  die Rekursionsabbildung dar.

Nachdem die Existenz und die Eindeutigkeit von  $\oplus_i$  durch den *Rekursionssatz* gesichert sind, schreiben wir für die “*Summe*” wie üblich  $i + j := \oplus_i(j)$ .

Bei der Multiplikation geht man ganz ähnlich vor. Die Startgleichung  $\odot_i(0) = 0$  ergibt  $\mathcal{C} := \mathbb{N}$  und  $a := 0$ . Aus  $\odot_i(\nu(k)) = \odot_i(k) + i$  lässt sich die von  $i$  abhängige Rekursionsabbildung  $g_i : \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$ ,  $(n, k) \mapsto k + i$  erschließen. Für das “*Produkt*”  $\odot_i(j)$ , das durch den *Rekursionssatz* allgemein definiert ist, schreibt man  $i \cdot j$  und lässt den “*Malpunkt*”  $\cdot$  weg, wenn keine Missverständnisse auftreten können.

## Brüche und ganze Zahlen

Wegen ihres engen Zusammenhangs mit den natürlichen Zahlen spielen auch **Brüche** und **ganze Zahlen** eine Rolle in der elementaren Zahlentheorie. Allerdings hängt der Reiz, den sie im Hinblick auf das Problemlösen ausüben können, sehr von der Art ihrer Einführung ab. Werden

Brüche - wie in der Mathematik üblich - als “Bezeichnungen für Äquivalenzklassen von Paaren natürlicher Zahlen” aufgefasst (siehe [4], Seite 21), so können sie kaum zahlentheoretische Neugier wecken. Bei den ganzen Zahlen, die selbst als “Äquivalenzklassen von Paaren natürlicher Zahlen” angesehen werden, ist es ähnlich.

Deshalb sind in der **Zahlgenese** Brüche und **Differenzen** eigenständige mathematische Objekte mit bestimmten Gleichheitsrelationen und mit gut motivierten Verknüpfungen. Die “Repräsentanten” der jeweils unendlich vielen zueinander gleichen Brüche heißen meistens “**Kernbrüche**”. Da sie teilerfremde Zähler und Nenner haben, stellt ihre Bestimmung eine zahlentheoretische Aufgabe und zugleich ein didaktisches Problem dar. In der **Zahlgenese** wird hierfür mit Hilfe einer “spielerischen” Form des “**Kettenbruchalgorithmus**” (siehe Seite 23) eine neue schulgemäße Lösung beschrieben.

Betrachtet man die ganzen Zahlen als Differenzen, die mindestens eine 0 enthalten, so haben sie als Repräsentanten der Differenzen den Vorteil, dass ihre **Ringeigenschaften**, die bei der “Kongruenzrechnung” in Kapitel 4 benötigt werden, sich ohne Fallunterscheidungen herleiten lassen.

## 1.4 Einführung in die elementare Zahlentheorie

Die Präzisierung der natürlichen Zahlen und ihrer Verknüpfungen lässt noch nicht erkennen, wieso das Gebiet der “Zahlentheorie” seit mehr als zweitausend Jahren Mathematiker und auch Laien fasziniert. Wesentlich dazu beigetragen hat der griechische Mathematiker EUKLID, der in seinem berühmten Werk “*Die Elemente*” [6] ( $\approx 325$  v. Chr.) bereits den Begriff der “*Primzahl*” einführte und die Unendlichkeit der Primzahlmenge zeigte, wobei seine Definition der Primzahl in heutiger Sprache folgendermaßen lautet: Eine natürliche Zahl größer als 1 heißt Primzahl, wenn sie nur durch 1 und sich selbst teilbar ist. Sein wichtigstes zahlentheoretisches Ergebnis, nämlich die (nicht ganz vollständig bewiesene) Darstellbarkeit aller natürlichen Zahlen als eindeutiges Produkt von Primzahlen, heißt heute “*Hauptsatz der elementaren Zahlentheorie*”.

Schon vor EUKLID wurde eine Zahl  $n$  als “*vollkommen*” angesehen, wenn die Summe ihrer echten Teiler (also ohne den Teiler  $n$ ) gleich  $n$  ist. EUKLID gab ein hinreichendes Kriterium für gerade vollkommene Zahlen an, und L. EULER<sup>2</sup> konnte in einer posthum veröffentlichten Arbeit zeigen, dass dieses Kriterium auch

<sup>2</sup>LEONHARD EULER (1707-1783) wirkte in St. Petersburg und in Berlin.

notwendig ist. Obwohl es damals nicht üblich war, “Vermutungen” der Nachwelt zu überliefern, können wir doch annehmen, dass schon EUKLID sich die folgenden “naheliegenden” Fragen gestellt hat, die damit die ältesten bis heute ungelösten Probleme sind:

- Gibt es unendlich viele gerade vollkommene Zahlen?
- Gibt es ungerade vollkommene Zahlen?
- Gibt es unendlich viele “Primzahlzwillinge”, d. h. Primzahlpaare  $(p, q)$  mit  $q - p = 2$ ?

Zu den “Merkwürdigkeiten” der elementaren Zahlentheorie gehört die häufig sehr große Diskrepanz zwischen der Einfachheit der Formulierung eines Problems und den enormen Schwierigkeiten, die zu seiner Lösung überwunden werden müssen. Ein typisches Beispiel ist das folgende Problem, das P. DE FERMAT<sup>3</sup> um 1637 gelöst zu haben glaubte:

Gibt es Tripel  $(x, y, z) \in \mathbb{N}_1^3$  mit  $x^n + y^n = z^n$ , wenn  $n \in \mathbb{N}_3$  ist?

Nachdem zahlreiche Mathematiker tiefliegende Teilergebnisse gefunden hatten, schien die vollständige Lösung längere Zeit unerreichbar. Als ANDREW WILES 1995 das Problem mit “neuester” Mathematik abschließend löste, berichteten sogar internationale Zeitungen auf der Titelseite darüber.

Aber nur relativ wenige zahlentheoretische Probleme sind wirklich schwer, denn in keinem anderen Teilgebiet der Mathematik gibt es so viele Ergebnisse wie in der Zahlentheorie. Bereits 1923 umfasste das dreibändige Werk “History of the Theory of Numbers” von LEONARD E. DICKSON [3], das über die elementare Zahlentheorie berichtet, rund 1600 Seiten.

Ein weiterer Aspekt, der sich nur in der elementaren Zahlentheorie findet, ist zumindest erwähnenswert. GAUß, dessen grundlegendes Werk *Disquisitiones arithmeticae* [9] schon im Vorwort genannt wurde, bezeichnete die “höhere Arithmetik” in der Vorrede zu jenem Buch (Seite VI) als “göttliche Wissenschaft”. Etwa 80 Jahre später konstatierte L. KRONECKER<sup>4</sup>: “Die ganzen Zahlen hat der liebe Gott gemacht, alles übrige ist Menschenwerk.”

---

<sup>3</sup> PIERRE DE FERMAT (1601-1665) wirkte als Jurist, Mathematiker und Parlamentsrat in Toulouse.

<sup>4</sup> LEOPOLD KRONECKER (1823-1891) war Mathematikprofessor in Berlin.

## 1.5 Abgrenzungen

Die Zahlentheorie lässt sich grob in drei Teilgebiete einteilen, die auf diejenigen Bereiche der Mathematik bezogen sind, aus denen ihre wichtigsten Hilfsmittel stammen:

- Elementare Zahlentheorie (Arithmetik);
- Algebraische Zahlentheorie (Algebra);
- Analytische Zahlentheorie (Analysis).

Es gibt aber noch weitere Teilgebiete, die eine geringere Rolle spielen, wie “geometrische Zahlentheorie” (Geometrie), “probabilistische Zahlentheorie” (Wahrscheinlichkeitstheorie) und “computergestützte Zahlentheorie” (Informatik).

Die elementare Zahlentheorie beginnt mit dem Begriff des “*Teilers*”. Als spezielle Teiler werden die *Primzahlen* und die mit ihnen mögliche Produktdarstellung der natürlichen Zahlen untersucht. Zu den zahlreichen Anwendungen des damit gewonnenen “*Hauptsatzes (der elementaren Zahlentheorie)*” gehört die Analyse einiger “*zahlentheoretischer Funktionen*” und die Betrachtung von “*diophantischen Gleichungen*”, d. h. von Gleichungen, bei denen nur die ganzzahligen Lösungen interessieren. Zum Beispiel ist einerseits die “*Irrationalität*” von  $\sqrt{2}$  äquivalent mit der Nichtexistenz von Paaren  $(x, y) \in \mathbb{N}_1^2$ , die  $x^2 = 2y^2$  erfüllen, und andererseits lassen sich mit Hilfe des *Hauptsatzes* alle “*pythagoreischen Tripel*”  $(x, y, z) \in \mathbb{N}_1^3$  angeben, die als Lösungen der Gleichung  $x^2 + y^2 = z^2$  definiert sind. Wir werden für die Parameterdarstellung dieser Tripel schon im zweiten Kapitel durch Anwenden einer “*Problemlösestrategie*” einen expliziten Zusammenhang zwischen den Parametern und den Lösungskomponenten herleiten.

Der zweite Hauptteil der elementaren Zahlentheorie beruht auf einer einfachen Umformulierung der Teilbarkeit, die zum Begriff der “*Kongruenz*” führt. Die damit vorliegende Äquivalenzrelation ergibt Äquivalenzklassen, die zusammen mit den entsprechenden Verknüpfungen “*Addition*” und “*Multiplikation*” Ringe bilden und die mit dem “ $\equiv$ -Zeichen” anstelle des Gleichheitszeichens die bisherigen Gleichungen “bündeln”.

Der letzte Hauptteil ist nach dem Vorbild von GAUß der “*quadratischen Zahlentheorie*” gewidmet. Dazu gehören “*quadratische Reste*”, “*quadratische Formen*” und als Ausblick “*quadratische Zahlkörper*”.

# Kapitel 2

## Teilbarkeit

### 2.1 Teiler von ganzen Zahlen

#### Definition des Teilers

Bezeichnet  $\mathbb{Z}$  die Menge der ganzen Zahlen und sind  $a, d \in \mathbb{Z}$ , so heißt  $d$  *Teiler von  $a$* , wenn es ein  $f \in \mathbb{Z}$  gibt, sodass  $a = df$  gilt.

Man schreibt  $d \mid a$  und liest “ $d$  teilt  $a$ ” oder “ $d$  ist Teiler von  $a$ ”. Ist  $d$  kein Teiler von  $a$ , so schreibt man  $d \nmid a$ .

#### Beispiele:

$2 \mid 6$ : Eine Zahl  $a \in \mathbb{Z}$  heißt *gerade*, wenn  $2 \mid a$  gilt;

$2 \nmid 5$ : Eine Zahl  $a \in \mathbb{Z}$  heißt *ungerade*, wenn  $2 \nmid a$  ist;

Wegen  $0 = 0d$  gilt  $d \mid 0$  für alle  $d \in \mathbb{Z}$ ; aber es ist  $0 \nmid a$  für alle  $a \neq 0$ .

Stellt  $d$  einen Teiler von  $a \neq 0$  dar, so ist der Faktor  $f$  in der Gleichung  $a = df$  eindeutig bestimmt (Kürzungsregel);

$3 \mid 12$  und  $(-3) \mid 12$ ,  $4 \mid (-16)$  und  $(-4) \mid (-16)$  :

Wegen  $a = df = (-d)(-f)$  gilt  $(-d) \mid a$  genau dann, wenn  $d \mid a$  erfüllt ist. Bei Teilbarkeitsproblemen genügt es also, die natürlichen Zahlen zu betrachten.

### Satz über Teilbarkeitsregeln

Sind  $a, b, c, d \in \mathbb{Z}$ , so gilt:

- i)  $a \mid a$  (“Reflexivität”);
- ii) Aus  $a \mid b$  und  $b \mid c$  folgt  $a \mid c$  (“Transitivität”);
- iii) Aus  $a \mid b$  und  $c \mid d$  folgt  $(ac) \mid (bd)$  (“Multiplikativität”);
- iv) Aus  $a \mid b$  und  $a \mid c$  folgt  $a \mid (ub + vc)$  für alle  $u, v \in \mathbb{Z}$  (“Linearität”).

**Beweis** (direkt, r1):

- i) Es gilt  $a = a \cdot 1$ ;
- ii) Aus  $b = a f_1$  und  $c = b f_2$  folgt  $c = (a f_1) f_2 = a (f_1 f_2)$ ;
- iii) Aus  $b = a f_1$  und  $d = c f_2$  folgt  $bd = a f_1 c f_2 = (ac) (f_1 f_2)$ ;
- iv) Aus  $b = a f_1$  und  $c = a f_2$  folgt  $ub + vc = a (u f_1 + v f_2)$ . □

### Satz über die Teileranzahl

Jedes  $a \in \mathbb{N}_1$  hat höchstens  $a$  Teiler.

**Beweis** (direkt, r1):

Ist  $d \mid a$ , so gibt es ein  $f \in \mathbb{N}_1$  mit  $a = d f$ . Wegen  $d \in \mathbb{N}_1$  gilt  $1 \leq d \leq d f = a$ . □

### Bezeichnung der Teileranzahlfunktion

Die Abbildung  $d : \mathbb{N}_1 \rightarrow \mathbb{N}_1$ ,  $n \mapsto d(n)$  mit  $d(n) := \text{card} \{t \in \mathbb{N}_1; t \mid n\}$  für alle  $n \in \mathbb{N}_1$  heißt *Teileranzahlfunktion*.

Der Buchstabe  $d$  steht für “*Divisor*”. In Deutschland schreibt man auch  $\tau(n)$ . Hier steht das  $\tau$  für “*Teiler*”.

Diese Funktion ist das erste Beispiel einer *zahlentheoretischen Funktion*.

Der größte gemeinsame Teiler von zwei natürlichen Zahlen wird im nächsten Abschnitt behandelt, um den Beweis von EUKLID für den *Hauptsatz der elementaren Zahlentheorie* bringen zu können. Soll in einer Vorlesung nur der “moderne” Beweis geführt werden, der hier ebenfalls zu finden ist, so lässt sich der Inhalt der folgenden fünf Abschnitte, die beim Problemlösen in der Zahlentheorie eine wichtige Rolle spielen, in das dritte Kapitel hinter 3.5 verschieben.

## 2.2 Der größte gemeinsame Teiler von zwei natürlichen Zahlen

Schon in der vierten Klasse der Grundschule erfahren SchülerInnen die “Division mit Rest” als “so oft wie möglich zu wiederholende Subtraktion”.

### Satz über Division mit Rest

Ist  $(a, b) \in \mathbb{Z} \times \mathbb{N}_1$ , so gibt es genau ein Paar  $(q, r) \in \mathbb{Z} \times \mathcal{A}_b$ , sodass gilt:

$$(2.1) \quad a = qb + r.$$

**Beweis** (zwei Teile, direkt, r1):

**i) Existenz:** Wir setzen  $q := \max \{u \in \mathbb{Z} ; a - ub \geq 0\}$  und  $r := a - qb$ , wobei der *Maximumsatz* durch Fallunterscheidung auf  $\mathbb{Z}$  übertragen wird. Dann ist definitionsgemäß  $r \geq 0$  und  $r - b = a - (q + 1)b < 0$ . Also gilt (2.1).

**ii) Eindeutigkeit:** Sind  $(q, r)$  und  $(q', r')$  aus  $\mathbb{Z} \times \mathcal{A}_b$  mit  $a = qb + r$  und  $a = q'b + r'$ , so folgt  $(q - q')b = r' - r$ . Damit erhalten wir  $|q - q'|b = |r' - r| \leq \max \{r, r'\} < b$ . Division durch  $b$  ergibt  $|q - q'| < 1$ , sodass  $q = q'$  und damit auch  $r = r'$  gelten muss.  $\square$

Mit Hilfe der “Gauß-Klammer”  $[x] := \max \{u \in \mathbb{Z} ; u \leq x\}$  können  $q$  und  $r$  explizit angegeben werden:

$$(2.2) \quad q = \left[ \frac{a}{b} \right] \quad \text{und} \quad r = a - \left[ \frac{a}{b} \right] b =: \text{mod}(a, b).^1$$

### Bezeichnung des größten gemeinsamen Teilers

Der *größte gemeinsame Teiler* von  $n$  Zahlen  $a_1, \dots, a_n \in \mathbb{Z}$  mit  $n \in \mathbb{N}_2$  und mit  $(a_1, \dots, a_n) \neq (0, \dots, 0)$  wird mit  $\text{ggT}(a_1, \dots, a_n)$  bezeichnet.

### Satz über die ggT-Rekursion

Ist  $(a, b) \in \mathbb{Z} \times \mathbb{N}_1$  und  $r := \text{mod}(a, b)$ , so gilt  $\text{ggT}(a, b) = \text{ggT}(b, r)$ .

<sup>1</sup>In vielen Computeralgebrasystemen wird  $\text{div}(a, b)$  für  $q$  und  $\text{mod}(a, b)$  für  $r$  gebraucht.

**Beweis** (direkt, r1):

Es sei  $d := \text{ggT}(a, b)$  und  $t := \text{ggT}(b, r)$ . Aus  $d | a$ ,  $d | b$  und  $r = a - \left[ \frac{a}{b} \right] b$  folgt aufgrund der *Linearitätsaussage* des *Satzes über Teilbarkeitsregeln* (Seite 18), dass  $d | r$  gilt. Damit folgt  $d | t$ . Also ist  $d \leq t$ . Analog ergibt  $t | b$  und  $t | r$ , dass  $t | a$  und damit  $t | d$  bzw.  $t \leq d$  gilt. Also ist  $t = d$ .  $\square$

Wegen  $\text{mod}(a, b) = \text{mod}(a + gb, b)$  folgt

$$(2.3) \quad \text{ggT}(a, b) = \text{ggT}(a + gb, b) \quad \text{für alle } (a, b) \in \mathbb{Z} \times \mathbb{N}_1 \quad \text{und für jedes } g \in \mathbb{Z}.$$

Die Bedingung  $r \in \mathcal{A}_b$  wurde bei dem obigen Beweis nicht benötigt. Sie bietet aber jetzt die Möglichkeit, die ggT-Rekursion fortzusetzen bis wegen der echten Verkleinerung des Restes in jedem Schritt nach endlich vielen Wiederholungen Teilbarkeit ohne Rest eintritt, sodass der größte gemeinsame Teiler direkt entnommen werden kann. Das eindeutig bestimmte Tupel der nacheinander auftretenden Divisoren und Reste bezeichnen wir nach EUKLID, von dem dieses Verfahren zur Berechnung des größten gemeinsamen Teilers stammt (*“Euklidischer Algorithmus”*).

### Bezeichnung des Euklidischen Tupels

Ist  $(r_0, r_1) \in \mathbb{N}_1^2$ , so heißt  $(r_1, \dots, r_n) \in \mathbb{N}_1^n$  mit  $r_{i+1} = \text{mod}(r_{i-1}, r_i)$  für  $i = 1, \dots, n-1$  und mit  $r_n | r_{n-1}$  *“Euklidisches Tupel”* von  $(r_0, r_1)$ .

**Beispiel:** (525, 231)

$$525 = 2 \cdot 231 + 63,$$

$$231 = 3 \cdot 63 + 42,$$

$$63 = 1 \cdot 42 + 21,$$

$$42 = 2 \cdot 21.$$

(231, 63, 42, 21) ist also das Euklidische Tupel von (525, 231).

### Satz über den Euklidischen Algorithmus

Gehört zu  $(r_0, r_1) \in \mathbb{N}_1^2$  das Euklidische Tupel  $(r_1, \dots, r_n)$ , so gilt

$$(2.4) \quad \text{ggT}(cr_0, cr_1) = cr_n \quad \text{für alle } c \in \mathbb{N}_1.$$

**Beweis** (Fallunterscheidung und “finite Induktion”, a1):

Wir beweisen zunächst (2.4) für  $c = 1$  und führen die allgemeine Aussage darauf zurück (“Zurückführungsstrategie”).

i) Der Fall  $n = 1$  mit dem Euklidischen Tupel  $(r_1)$  tritt auf, wenn  $r_1 \mid r_0$  ist. Dann gilt  $\text{ggT}(r_0, r_1) = r_1$ .

ii) Im Falle  $n \in \mathbb{N}_2$  wollen wir zeigen, dass  $\text{ggT}(r_0, r_1) = \text{ggT}(r_{k+1}, r_{k+2})$  für  $k = 0, \dots, n - 2$  erfüllt ist, indem wir für den Übergang von  $k = m$  zu  $k = m + 1$  für  $m \leq n - 3$  den *Satz über die ggT-Rekursion* (Seite 19) in der Form

$$(2.5) \quad \text{ggT}(r_{m+1}, r_{m+2}) = \text{ggT}(r_{m+2}, r_{m+3})$$

verwenden. Obwohl bei festem  $n$  nur endlich viele Gleichungen zu beweisen sind, haben wir als Nachweismethode nur die *vollständige Induktion* zur Verfügung. Deshalb werden in der “Induktionsmenge”  $\mathcal{M}_n$  die zu beweisenden Gleichungen durch die von selbst erfüllten Ungleichungen  $k \geq n - 1$  ergänzt:

$$\mathcal{M}_n :=$$

$$\{k \in \mathbb{N}; (k \leq n - 2 \text{ und } \text{ggT}(r_0, r_1) = \text{ggT}(r_{k+1}, r_{k+2})) \text{ oder } (k \geq n - 1)\}.$$

Wegen  $n \geq 2$  und aufgrund des *Satzes über die ggT-Rekursion* gilt  $0 \in \mathcal{M}_n$ . Ist  $m \in \mathcal{M}_n$  und  $m \leq n - 3$ , so folgt mit Hilfe von (2.5), dass  $m + 1 \in \mathcal{M}_n$  gilt. Für  $m \geq n - 2$  ist  $m + 1 \geq n - 1$ , sodass auch hier  $m + 1 \in \mathcal{M}_n$  gilt. Der *Induktionssatz* (Seite 12) ergibt also  $\mathcal{M}_n = \mathbb{N}$ .

Damit gilt  $\text{ggT}(r_0, r_1) = \text{ggT}(r_{n-1}, r_n)$ , und wegen  $r_n \mid r_{n-1}$  ist  $\text{ggT}(r_{n-1}, r_n) = r_n$ .

Diese etwas umständliche Durchführung der “*fniten Induktion*” kürzt man üblicherweise wie folgt ab:

$$\text{ggT}(r_0, r_1) = \text{ggT}(r_1, r_2) = \dots = \text{ggT}(r_{n-1}, r_n) = r_n.$$

Die Aussage für  $c > 1$  ergibt sich, indem man alle Gleichungen für die Division mit Rest, die bei der Bestimmung des Euklidischen Tupels  $(r_1, \dots, r_n)$  von  $(r_0, r_1)$  auftreten, mit  $c$  multipliziert und die Eindeutigkeit des jeweiligen Restes in (2.1) beachtet. Als Euklidisches Tupel zu  $(cr_0, cr_1)$  erhält man also  $(cr_1, \dots, cr_n)$ . Mit Hilfe des oben bewiesenen Spezialfalls folgt schließlich

$$\text{ggT}(cr_0, cr_1) = cr_n = c \text{ggT}(r_0, r_1). \quad \square$$

Da jetzt der Zusammenhang der *finiten Induktion* mit der *vollständigen Induktion* ausführlich gezeigt ist, werden wir im Folgenden bei Beweisen mit *finiten Induktion* meistens eine geeignete Kurzschreibweise verwenden.

**Beispiel:** Das obige Euklidische Tupel ergibt  $\text{ggT}(525, 231) = 21$ .

Weitere Beispiele vor allem mit großen Zahlen führen zu der Vermutung, dass der *Euklidische Algorithmus* ungewöhnlich “schnell” ist. Diese zunächst überraschende Tatsache wird in dem folgenden Satz präzisiert.

### Effizienzsatz

Gehört zu  $(r_0, r_1) \in \mathbb{N}_1^2$  mit  $r_1 < r_0$  das Euklidische Tupel  $(r_1, \dots, r_n)$ , so gilt

$$n < 3 \ln r_1 + 1.$$

**Beweis** (Fallunterscheidung, finite Induktion und Widerspruch, a2):

Von dem Euklidischen Tupel  $(r_1, \dots, r_n)$  wissen wir bisher nur, dass  $r_{i+1} < r_i$  für  $i = 1, \dots, n-1$  gilt. Zahlenbeispiele lassen vermuten, dass  $r_{i+2} < \frac{1}{2} r_i$  für  $i = 1, \dots, n-2$  erfüllt ist.

Es sei also  $r_i = r_{i+1}q + r_{i+2}$  mit  $q \in \mathbb{N}_1$  und  $0 < r_{i+2} < r_{i+1}$  für  $i \in \{1, \dots, n-2\}$ . Im Falle  $r_{i+1} \leq \frac{1}{2} r_i$  folgt sofort  $r_{i+2} < r_{i+1} \leq \frac{1}{2} r_i$ . Ist  $r_{i+1} > \frac{1}{2} r_i$ , so erhält man  $r_{i+1}q \geq r_{i+1} > \frac{1}{2} r_i$  und damit  $r_{i+2} = r_i - r_{i+1}q < \frac{1}{2} r_i$ .

*Finite Induktion* ergibt nun  $r_{2k-1} < \frac{1}{2^{k-1}} r_1$  für  $k = 2, \dots, \left\lceil \frac{n+1}{2} \right\rceil$ . Ist  $m := \min \{k \in \mathbb{N}_1 ; 2^k > r_1\}$ , also  $2^{m-1} \leq r_1 < 2^m$ , so folgt  $1 \leq \frac{1}{2^{m-1}} r_1 < 2$ . Wäre  $n > 2m-1$ , so würde sich  $r_{2m-1} < 2$ , also  $r_{2m-1} = 1$  und damit  $n \leq 2m-1$  im Widerspruch zur Annahme ergeben. Deshalb gilt

$$n \leq 2m-1 = 2 \max \{k \in \mathbb{N}_1 ; 2^{k-1} \leq r_1\} - 1$$

$$= 2 \left\lceil \frac{\ln r_1}{\ln 2} \right\rceil + 1 \leq \frac{2}{\ln 2} \ln r_1 + 1 < 3 \ln r_1 + 1. \quad \square$$

Der *Euklidische Algorithmus* ist auch ein Hilfsmittel für die Herleitung des folgenden Satzes, der schon in diesem Kapitel mehrere Anwendungen besitzt und der vor allem bei dem ersten Beweis für den *Hauptsatz* benötigt wird.

**Produktteilersatz**

Sind  $a, n, b_0, \dots, b_n \in \mathbb{N}_1$  mit  $a \mid b_0 \cdots b_n$  und  $\text{ggT}(a, b_i) = 1$  für  $i = 1, \dots, n$ , so gilt  $a \mid b_0$ .

**Beweis** (vollständige Induktion, a1):

Es sei  $\mathcal{M} :=$

$\{k \in \mathbb{N}_1 ; \text{Aus } a \mid b_0 \cdots b_k \text{ und } \text{ggT}(a, b_i) = 1 \text{ für } i = 1, \dots, k \text{ folgt } a \mid b_0\}$ .

Für den Induktionsanfang  $1 \in \mathcal{M}$  ist zu zeigen, dass sich  $a \mid b_0$  aus  $a \mid b_0 b_1$  und  $\text{ggT}(a, b_1) = 1$  ergibt. Wegen der Voraussetzung  $a \mid b_0 b_1$  existiert ein  $f \in \mathbb{N}_1$ , sodass  $b_0 b_1 = a f$  erfüllt ist. Mit zweimaliger Anwendung von (2.4) erhalten wir dann

$$b_0 = b_0 \text{ggT}(a, b_1) = \text{ggT}(a b_0, b_0 b_1) = a \text{ggT}(b_0, f),$$

d. h. es gilt  $a \mid b_0$ .

Für  $m \in \mathcal{M}$  und  $a \mid (b_0 \cdots b_m) b_{m+1}$  mit  $\text{ggT}(a, b_{m+1}) = 1$  folgt wie bei dem Induktionsanfang, dass  $a$  Teiler von  $b_0 \cdots b_m$  ist. Wegen  $m \in \mathcal{M}$  ergibt sich  $a \mid b_0$  und damit  $m + 1 \in \mathcal{M}$ , also  $\mathcal{M} = \mathbb{N}_1$ . □

Die Eigenschaft von zwei natürlichen Zahlen, nur 1 als gemeinsamen Teiler zu haben, tritt in der Zahlentheorie oft auf. Sie hat deshalb eine eigene Bezeichnung, bei der nur die Teiler berücksichtigt werden, die größer als 1 sind.

**Definition der Teilerfremdheit**

Zwei Zahlen  $a, b \in \mathbb{N}_1$  heißen *teilerfremd*, wenn  $\text{ggT}(a, b) = 1$  gilt.

## 2.3 Der Kettenbruchalgorithmus und die lineare diophantische Gleichung

Bei der Berechnung des größten gemeinsamen Teilers mit Hilfe des Euklidischen Algorithmus treten Quotienten auf, die bisher nicht weiter genutzt wurden. Der folgende Begriff, der einen weiten Bereich der Zahlentheorie begründet, wird erkennen lassen, dass diese Quotienten zu einem Algorithmus gehören, der mit dem Euklidischen Algorithmus zusammenhängt wie die "beiden Seiten einer Medaille".

### Bezeichnung der Kettenbruchentwicklung

Es sei  $\alpha_1 \in \mathbb{R} \setminus \mathbb{Z}$ ,<sup>2</sup>  $\alpha_{i+1} := \frac{1}{\alpha_i - [\alpha_i]}$  für  $i \in \mathbb{N}_1$ , solange  $\alpha_i \notin \mathbb{Z}$  ist, und es werde  $q_i := [\alpha_i]$  gesetzt. Dann heißt im Falle  $\alpha_n \in \mathbb{Z}$  das  $n$ -Tupel  $[q_1, q_2, \dots, q_n]$  und im Falle  $\alpha_i \notin \mathbb{Z}$  für alle  $i \in \mathbb{N}_2$  die in der Form  $[q_1, q_2, \dots]$  geschriebene Folge  $(q_n)_{n \in \mathbb{N}_1}$  *Entwicklung von  $\alpha_1$  in einen (einfachen) Kettenbruch*.

Bricht die Entwicklung ab, so heißt der Kettenbruch *endlich*. Die natürlichen Zahlen  $q_2, q_3, \dots$  heißen *Teilnenner* des Kettenbruchs. Die (reellen) Zahlen  $\alpha_2, \alpha_3, \dots$  bezeichnet man als *vollständige Quotienten*. Der Bruch  $[q_1, \dots, q_s]$  für  $s \in \{2, \dots, n\}$  bzw. für  $s \in \mathbb{N}_2$  wird *s-ter Näherungsbruch von  $\alpha_1$*  genannt.

Für  $u_1 \in \mathbb{R}$  und  $u_i \in \mathbb{R}^+$ ,  $i = 2, \dots, n$ , wird durch

$$(2.6) \quad [u_1, u_2, \dots, u_n] := u_1 + \frac{1}{u_2 + \frac{1}{u_3 + \dots \frac{1}{u_n}}}$$

ein (*einfacher*) *Kettenbruch* definiert.

### Satz über die Kettenbruchentwicklung

Ist  $(r_1, \dots, r_n) \in \mathbb{N}_1^n$  das Euklidische Tupel von  $(r_0, r_1) \in \mathbb{Z} \times \mathbb{N}_1$  und wird  $q_i := \left[ \frac{r_{i-1}}{r_i} \right]$  für  $i = 1, \dots, n$  gesetzt, so stellt  $[q_1, \dots, q_n]$  die Kettenbruchentwicklung von  $\frac{r_0}{r_1}$  dar.

**Beweis** (finite Induktion, r1):

| Euklidischer Algorithmus                   | Kettenbruchalgorithmus   |
|--|--|
| $r_0 = q_1 r_1 + r_2, \quad 0 < r_2 < r_1$ | $\frac{r_0}{r_1} = q_1 + \frac{r_2}{r_1}, \quad 0 < \frac{r_2}{r_1} < 1$ |
| $r_1 = q_2 r_2 + r_3, \quad 0 < r_3 < r_2$ | $\frac{r_1}{r_2} = q_2 + \frac{r_3}{r_2}, \quad 0 < \frac{r_3}{r_2} < 1$ |
| $\vdots$                                   | $\vdots$   |
| $r_{n-1} = q_n r_n + 0$                    | $\frac{r_{n-1}}{r_n} = q_n$  |

<sup>2</sup>  $\mathbb{R}$  bezeichnet die Menge der reellen Zahlen. [16] enthält eine elementare Einführung.  $\mathbb{R}^+$  ist die Menge der positiven reellen Zahlen.  $\mathbb{Q}$  stellt die Menge der rationalen Zahlen dar und  $\mathbb{Q}^+$  steht für  $\{q \in \mathbb{Q}; q > 0\}$ .

Aus dieser Tabelle entnehmen wir die Vermutung, dass im Falle einer rationalen Ausgangszahl  $\alpha_1 = \frac{r_0}{r_1}$  die Entwicklung von  $\alpha_1$  in einen Kettenbruch mit Hilfe der Zahlen  $q_i$  und  $r_i$  aus dem Euklidischen Algorithmus gewonnen werden kann. Da  $q_i := [\alpha_i]$  ist, wenden wir den *Induktionssatz* (Seite 12) auf  $\mathcal{M}_n := \{k \in \mathbb{N}_1 ; (k \leq n \text{ und } \alpha_k = \frac{r_{k-1}}{r_k}) \text{ oder } (k > n)\}$  an. Aufgrund der Voraussetzung ist  $1 \in \mathcal{M}_n$ . Für den Induktionsschritt sei  $m \in \mathcal{M}_n$  mit  $m \leq n$ . Im Falle  $m < n$  folgt aus der Gleichung  $r_{m-1} = q_m r_m + r_{m+1}$  des Euklidischen Algorithmus die Darstellung  $\alpha_m = \frac{r_{m-1}}{r_m} = q_m + \frac{r_{m+1}}{r_m}$  mit  $0 < \frac{r_{m+1}}{r_m} < 1$ . Also ist  $\alpha_{m+1} = \frac{1}{\alpha_m - q_m} = \frac{r_m}{r_{m+1}}$ . Für  $m = n$  sind  $r_{n-1} = q_n r_n$  und  $\alpha_n = \frac{r_{n-1}}{r_n} = q_n$  äquivalent. Da  $m \in \mathcal{M}_n$  für alle  $m > n$  gilt, ist  $\mathcal{M}_n = \mathbb{N}_1$ . □

Der folgende Satz enthält drei Kettenbruceigenschaften, die in einer Reihe von Anwendungen genutzt werden und die zu der Bezeichnung *Kettenbruchalgorithmus* führen.

**Satz über vollständige Quotienten und Näherungsbrüche**

Zu dem Näherungsbruch  $[q_1, \dots, q_s]$  von  $\alpha_1 \in \mathbb{R} \setminus \mathbb{Z}$  seien  $P_k$  und  $Q_k$  rekursiv durch  $P_0 := 1, P_1 := q_1, P_k := q_k P_{k-1} + P_{k-2}$  und  $Q_0 := 0, Q_1 := 1, Q_k := q_k Q_{k-1} + Q_{k-2}$  für  $k = 2, \dots, s$  definiert. Dann gilt

$$(2.7) \quad \alpha_1 = \frac{\alpha_s P_{s-1} + P_{s-2}}{\alpha_s Q_{s-1} + Q_{s-2}},$$

$$(2.8) \quad [q_1, \dots, q_s] = \frac{P_s}{Q_s} \text{ und}$$

$$(2.9) \quad P_s Q_{s-1} - Q_s P_{s-1} = (-1)^s.$$

*Hinweis:* Die Werte  $P_0 := 1, P_1 := q_1, Q_0 := 0, Q_1 := 1$  lassen sich mit

$$\alpha_1 = q_1 + \frac{1}{\alpha_2} = \frac{\alpha_2 \boxed{q_1} + \boxed{1}}{\alpha_2 \boxed{1} + \boxed{0}} = \frac{\alpha_2 \boxed{P_1} + \boxed{P_0}}{\alpha_2 \boxed{Q_1} + \boxed{Q_0}}$$

in Erinnerung rufen.

**Beweis** (zwei Teile):

**i) Bruchdarstellungen** (finite Induktion, a1):

Schreiben wir (2.8) in der Form

$$[q_1, \dots, q_{s-1}, q_s] = \frac{q_s P_{s-1} + P_{s-2}}{q_s Q_{s-1} + Q_{s-2}},$$

so lässt der Vergleich mit (2.7) vermuten, dass

$$(2.10) \quad \alpha_1 = [q_1, \dots, q_{s-1}, \alpha_s]$$

gilt. Bei dem Beweis mit finiter Induktion ist  $2 \in \mathcal{M}_s := \{n \in \mathbb{N}_2; (n \leq s \text{ und } \alpha_1 = [q_1, \dots, q_{n-1}, \alpha_n]) \text{ oder } (n > s)\}$ , weil (2.6) die Darstellung  $\alpha_1 = q_1 + \frac{1}{\alpha_2} = [q_1, \alpha_2]$  erlaubt. Entsprechend folgt für  $m \in \mathcal{M}_s$  mit  $m < s$ , dass  $\alpha_1 = [q_1, \dots, q_{m-1}, \alpha_m] = \left[ q_1, \dots, q_{m-1}, q_m + \frac{1}{\alpha_{m+1}} \right] = [q_1, \dots, q_m, \alpha_{m+1}]$  erfüllt ist, so dass sich wegen  $m+1 \in \mathcal{M}_s$  und mit dem *Induktionssatz* (Seite 12)  $\mathcal{M}_s = \mathbb{N}_2$  ergibt.

Nun bietet es sich an, mit der *Verallgemeinerungsstrategie* (2.7) und (2.8) gleichzeitig zu beweisen, indem wir  $q_s$  beziehungsweise  $\alpha_s$  durch eine reelle Variable  $x_s$  ersetzen und für die finite Induktion die Menge  $\mathcal{M}'_s := \left\{ n \in \mathbb{N}_2; (n \leq s \text{ und } [q_1, \dots, q_{n-1}, x_n] = \frac{x_n P_{n-1} + P_{n-2}}{x_n Q_{n-1} + Q_{n-2}} \text{ für jedes } x_n \in \mathbb{R}^+) \text{ oder } (n > s) \right\}$  verwenden. Der Induktionsanfang  $2 \in \mathcal{M}'_s$  entspricht der Merkregel im obigen Hinweis, wenn  $\alpha_2$  durch  $x_2$  ersetzt wird. Für  $m \in \mathcal{M}'_s$  mit  $m < s$  folgt

$$\begin{aligned} [q_1, \dots, q_{m-1}, q_m, x_{m+1}] &= \left[ q_1, \dots, q_{m-1}, q_m + \frac{1}{x_{m+1}} \right] \\ &= \frac{(q_m x_{m+1} + 1) P_{m-1} + x_{m+1} P_{m-2}}{(q_m x_{m+1} + 1) Q_{m-1} + x_{m+1} Q_{m-2}} = \frac{x_{m+1} P_m + P_{m-1}}{x_{m+1} Q_m + Q_{m-1}}. \end{aligned}$$

Damit ist auch  $m+1 \in \mathcal{M}'_s$  und der *Induktionssatz* ergibt  $\mathcal{M}'_s = \mathbb{N}_2$ .

Ersetzen wir  $x_s$  durch  $\alpha_s$  beziehungsweise  $q_s$  und berücksichtigen wir (2.10), so erhalten wir (2.7) und mit den Rekursionsgleichungen für  $P_s$  und  $Q_s$  auch (2.8). Eine Anwendung von (2.7) mit nicht rationalen  $\alpha_i$  findet sich in Abschnitt 5.4 auf Seite 172.

**ii) Produktdifferenz** (finite Induktion, r1):

Wegen  $P_1 Q_0 - Q_1 P_0 = q_1 \cdot 0 - 1 \cdot 1 = (-1)^1$  ist  $1 \in \mathcal{M}''_n := \left\{ s \in \mathbb{N}_1; (s \leq n \text{ und } P_s Q_{s-1} - Q_s P_{s-1} = (-1)^s) \text{ oder } (s > n) \right\}$ . Für  $m \in \mathcal{M}''_n$  mit  $m < n$  folgt

$$\begin{aligned} P_{m+1} Q_m - Q_{m+1} P_m &= (q_{m+1} P_m + P_{m-1}) Q_m - (q_{m+1} Q_m + Q_{m-1}) P_m \\ &= P_{m-1} Q_m - Q_{m-1} P_m = -(P_m Q_{m-1} - Q_m P_{m-1}) = -(-1)^m = (-1)^{m+1}, \end{aligned}$$

d. h. es ist  $m + 1 \in \mathcal{M}''_n$ . Also gilt  $\mathcal{M}''_n = \mathbb{N}_1$ . □

Aus (2.9) folgt mit dem *Satz über Teilbarkeitsregeln* (Seite 18), dass  $\text{ggT}(P_s, Q_s) = 1$  für alle Näherungsbrüche  $\frac{P_s}{Q_s}$  gilt. Geht man umgekehrt von einem Bruch  $\frac{a}{b}$  mit  $a, b \in \mathbb{N}_2$  und  $\text{ggT}(a, b) = 1$  aus, so ergibt (2.8) die Gleichung  $\frac{a}{b} = \frac{P_n}{Q_n}$ , wenn  $[q_1, \dots, q_n]$  die Kettenbruchentwicklung von  $\frac{a}{b}$  ist. Wendet man auf  $a Q_n = b P_n$  viermal den *Produktteilersatz* (Seite 23) an, so erhält man  $a|P_n, P_n|a, b|Q_n, Q_n|b$  und damit  $P_n = a$  und  $Q_n = b$ . Ersetzt man nun in (2.9) (mit  $s = n$ )  $P_n$  durch  $a$  sowie  $Q_n$  durch  $b$ , multipliziert beide Seiten mit  $(-1)^n$  und führt die Abkürzungen  $x := (-1)^n Q_{n-1}, y := -(-1)^n P_{n-1}$  ein, so stellt  $(x, y)$  eine ganzzahlige Lösung der Gleichung

$$ax + by = 1$$

dar. Dieses ist das einfachste Beispiel eines Typs von Gleichungen, die in der Zahlentheorie eine wichtige Rolle spielen und die nach dem griechischen Mathematiker DIOPHANT (zwischen 150 und 350 n. Chr.) benannt werden, der als Erster Methoden zur Bestimmung rationaler Lösungen von Gleichungen untersuchte.

### Bezeichnung der diophantischen Gleichung

Eine Gleichung  $f(x_1, \dots, x_n) = g(x_1, \dots, x_n)$  mit  $f(x_1, \dots, x_n) \in \mathbb{Z}$  und  $g(x_1, \dots, x_n) \in \mathbb{Z}$  für alle  $(x_1, \dots, x_n) \in \mathbb{Z}^n$  heißt *diophantische Gleichung*. Ein  $n$ -tupel  $(y_1, \dots, y_n) \in \mathbb{Z}^n$  heißt *Lösung* der diophantischen Gleichung, wenn  $f(y_1, \dots, y_n) = g(y_1, \dots, y_n)$  gilt.

### Beispiele

- i)  $ax + by = c$  mit  $a, b \in \mathbb{Z} \setminus \{0\}$  und  $c \in \mathbb{Z}$  (“*Lineare diophantische Gleichung*”);
- ii)  $x^2 = 2y^2$  (Irrationalität von  $\sqrt{2}$ , siehe Seite 30);
- iii)  $x^2 + y^2 = z^2$  (“*Pythagoreische Tripel*”, siehe Seite 35);
- iv)  $x^2 - my^2 = 1$  mit  $m \in \mathbb{N}_2$  und  $\sqrt{m} \notin \mathbb{N}_2$  (“*Fermat-Pell-Gleichungen*” oder “*Pellsche Gleichungen*”, siehe Seite 168).

Mit Hilfe der obigen Überlegungen können wir nun die lineare diophantische Gleichung abschließend behandeln.

### Satz über die lineare diophantische Gleichung

Es seien  $a, b \in \mathbb{Z} \setminus \{0\}$ ,  $c \in \mathbb{Z}$  und  $d := \text{ggT}(a, b)$ .

Die lineare diophantische Gleichung

$$(2.11) \quad ax + by = c$$

hat keine Lösung, wenn  $d$  nicht  $c$  teilt.

Gilt  $d \mid c$ , so besitzt (2.11) unendlich viele Lösungen und mit den Abkürzungen  $x_0 := (-1)^n Q_{n-1} \frac{c}{d}$  und  $y_0 := -(-1)^n P_{n-1} \frac{c}{d}$ , wobei  $\frac{P_{n-1}}{Q_{n-1}} = [q_1, \dots, q_{n-1}]$  der  $(n-1)$ -te Näherungsbruch der Kettenbruchentwicklung  $[q_1, \dots, q_n]$  von  $\frac{a}{b}$  ist, stellt  $\left\{ \left( x_0 + t \frac{b}{d}, y_0 - t \frac{a}{d} \right) ; t \in \mathbb{Z} \right\}$  die Lösungsmenge von (2.11) dar.

**Beweis** (zwei Teile):

**i) Unlösbarkeit** (direkt, r1):

Aufgrund des *Satzes über Teilbarkeitsregeln* (Seite 18) gilt  $d \mid (ax + by)$  für alle  $(x, y) \in \mathbb{Z}^2$ . Damit kann keine Zahl  $c \in \mathbb{Z}$  mit  $d \nmid c$  als ganzzahlige Linearkombination von  $a$  und  $b$  dargestellt werden.

**ii) Lösungsmenge** (direkt, a1):

Es gelte  $d \mid c$ . Um mit Hilfe des *Kettenbruchalgorithmus* eine Lösung finden zu können, teilen wir zunächst die drei Zahlen  $a, b, c$  durch  $d$ . Wird die Lösungsmenge von (2.11) mit  $\mathcal{L}(a, b, c)$  bezeichnet und  $a' := \frac{a}{d}$ ,  $b' := \frac{b}{d}$ ,  $c' := \frac{c}{d}$  gesetzt, so ist  $\mathcal{L}(a, b, c) = \mathcal{L}(a', b', c')$ , weil die Lösungsbedingung bei der Division beider Seiten von (2.11) erhalten bleibt. Wegen  $\frac{a}{b} = \frac{a'}{b'}$  ergeben die obigen Vorüberlegungen mit  $x_1 := (-1)^n Q_{n-1}$  und  $y_1 := -(-1)^n P_{n-1}$ , dass  $(x_1, y_1)$  in  $\mathcal{L}(a', b', 1)$  liegt.

Aus  $a'x_1 + b'y_1 = 1$  folgt außerdem  $a'(x_1 c') + b'(y_1 c') = c'$ . Mit  $x_0 := x_1 c'$  und  $y_0 := y_1 c'$  ist also  $(x_0, y_0)$  eine "spezielle Lösung" von

$$(2.12) \quad a'x + b'y = c'$$

und damit auch von (2.11).

Stellt  $(\bar{x}, \bar{y}) \in \mathcal{L}(a', b', c')$  eine beliebige Lösung dar, so ergibt sich - wie in der linearen Algebra - durch Differenzbildung, dass  $(\bar{x} - x_0, \bar{y} - y_0) \in \mathcal{L}(a', b', 0)$  gilt. Aus der dazu äquivalenten Gleichung

$$a'(\bar{x} - x_0) = b'(y_0 - \bar{y})$$

erhalten wir die Bedingungen  $a' \mid b'(y_0 - \bar{y})$  und  $b' \mid a'(\bar{x} - x_0)$ . Da  $\text{ggT}(a', b') = 1$  ist, folgt mit dem *Produktteilersatz* (Seite 23), dass  $a' \mid (y_0 - \bar{y})$  und  $b' \mid (\bar{x} - x_0)$  erfüllt sein muss, d. h. es gibt  $s, t \in \mathbb{Z}$  mit  $y_0 - \bar{y} = sa'$  und  $\bar{x} - x_0 = tb'$ . Auflösen nach  $\bar{x}$  und  $\bar{y}$  sowie Einsetzen in (2.12) ergibt schließlich  $s = t$ . □

### Beispiel

Um die Lösungsmenge der diophantischen Gleichung  $321x + 111y = 6$  zu finden, bestimmen wir in der folgenden Abbildung zunächst mit Hilfe der Kettenbruchentwicklung von  $\frac{321}{111}$  die Teilnenner  $q_1, q_2, q_3$  (umrahmt) und  $\text{ggT}(321, 111)$  (doppelt umrahmt). Wie bei der "schriftlichen Division" ist jeweils der mit dem Ergebnis multiplizierte Divisor von dem Dividenden zu subtrahieren. Anders als bei der schriftlichen Division wird dann vor den neuen Rest der vorige Divisor als nächster Dividend geschrieben.

Anschließend wird eine Tabelle für die Zähler und Nenner der Näherungsbrüche erstellt. Nachdem die Werte von  $q_1, \dots, q_{n-1}$  und von  $P_0, P_1, Q_0, Q_1$  eingetragen sind, lassen sich die weiteren Zähler und Nenner einheitlich berechnen, indem jeweils zuerst das Produkt der beiden zu der "schrägen \*-Linie" gehörenden Zahlen gebildet wird, wozu dann die vor der entsprechenden + -Linie stehende Zahl zu addieren ist.

$$[321 / 111] = \boxed{2} =: q_1$$

$$\begin{array}{r} -222 \\ 111 / 99 = \boxed{1} =: q_2 \end{array}$$

$$\begin{array}{r} -99 \\ 99 / 12 = \boxed{8} =: q_3 \end{array}$$

$$12 / \boxed{\boxed{3}} = 4$$

| $s$   | 0 | 1 | 2 | 3  |
|-------|---|---|---|--|
| $q_s$ | - | 2 | 1 | 8  |
| $P_s$ | 1 | 2 | 3 | <span style="border: 1px solid black; padding: 2px;">26</span> |
| $Q_s$ | 0 | 1 | 1 | <span style="border: 1px solid black; padding: 2px;">9</span>  |

Abbildung 2.1: Lösung der linearen diophantischen Gleichung  $321x + 111y = 6$

Mit  $n = 4, d = 3, P_3 = 26$  und  $Q_3 = 9$  erhalten wir die Lösungsmenge  $\mathcal{L}(321, 111, 6) = \{(18 + 37t, -52 - 107t) ; t \in \mathbb{Z}\}$ .

## Irrationalität von $\sqrt{2}$

Wir schließen diesen Abschnitt mit der in 1.5 erwähnten diophantischen Gleichung

$$(2.13) \quad x^2 = 2y^2.$$

Ihre gleich zu zeigende Unlösbarkeit für positive ganze Zahlen  $x, y$  hängt mit der Irrationalität von  $\sqrt{2}$  zusammen, die schon im letzten Abschnitt mit derselben Beweismethode hätte behandelt werden können. Da bei zahlentheoretischen Problemen häufiger diophantische Gleichungen mit endlich vielen Lösungen auftreten, soll hier die Gelegenheit genutzt werden, dieses Beispiel dafür zu bringen.

Wir nehmen an, dass es ein Paar  $(x, y) \in \mathbb{N}_1^2$  gibt, das (2.13) erfüllt, und setzen

$$t := \text{ggT}(x, y), \quad a := \frac{x}{t}, \quad b := \frac{y}{t}.$$

Dann gilt

$$(2.14) \quad a^2 = 2b^2 \quad \text{mit} \quad \text{ggT}(a, b) = 1.$$

Wegen  $(2k)^2 = 2(2k^2)$  und  $(2k-1)^2 = 2(2k^2 - 2k) + 1$  für jedes  $k \in \mathbb{N}_1$  ergibt sich, dass eine Quadratzahl  $m^2$  genau dann eine gerade Zahl darstellt, wenn  $m$  gerade ist. Nach (2.14) gilt  $2 \mid a^2$ . Also muss  $a$  gerade sein. Damit ist  $a^2$  durch 4 teilbar, woraus folgt, dass auch  $2 \mid b$  gilt - im Widerspruch zur Teilerfremdheit von  $a$  und  $b$ .

Da mit jeder Lösung  $(x, y)$  von (2.13) auch  $(-x, y)$ ,  $(x, -y)$  und  $(-x, -y)$  Lösungen sind, stellt  $(0, 0)$  das einzige Paar aus  $\mathbb{Z} \times \mathbb{Z}$  dar, das (2.13) erfüllt.

Bei dem indirekten Nachweis der Irrationalität von  $\sqrt{2}$  ergibt sich aus der Annahme, dass ein Paar  $(a, b) \in \mathbb{N}_1^2$  mit  $\text{ggT}(a, b) = 1$  und  $\sqrt{2} = \frac{a}{b}$  existiert, durch Quadrieren direkt die nicht erfüllbare Gleichung (2.14).

## 2.4 Die Gaußsche Erkundungsstrategie

Mit der bisher bereitgestellten Theorie könnten schon eine Reihe von Aufgabentypen behandelt werden. Das Beispiel im letzten Abschnitt zeigt etwa, wie sich die folgenden beiden Aufgaben effizient lösen lassen:

i) Berechnen Sie den größten gemeinsamen Teiler von 187 und 391.

ii) Bestimmen Sie alle  $(x, y) \in \mathbb{Z}^2$  mit  $11x + 53y = 236$ .

Im Hinblick auf unser anspruchsvolleres Ziel, Problemlösefähigkeiten zu entwickeln, soll in diesem Buch auf solche “Rechenaufgaben” verzichtet werden. Eine endgültige Unterscheidung von Aufgaben und Problemen ist aber auf diese Weise nicht möglich, weil unter anderem individuelle Vorkenntnisse eine Rolle beim Problemlösen spielen. Zum Beispiel stellt die Aufforderung, die Irrationalität der reellen Zahl  $s := \sqrt{2} + \sqrt{3}$  zu beweisen, kein Problem dar, wenn der obige Beweis von EUKLID für die Irrationalität von  $\sqrt{2}$  (Seite 30) bekannt ist, weil es wegen  $s^2 - 5 = \sqrt{6}$  genügt, mit derselben Methode zu zeigen, dass  $\sqrt{6}$  irrational ist.

Aufgaben werden gestellt, um bestimmte kurz vorher entwickelte Zusammenhänge und Methoden zu üben. Ein Problem enthält dagegen immer mindestens eine noch nicht bekannte oder nicht direkt sichtbare Komponente. Das Ziel des Problemlösens ist meistens die Herstellung eines Zusammenhangs mit gesicherten Aussagen, die Angabe einer Lösungsmenge oder die Konstruktion eines Gegenbeispiels.

Das Phänomen, dass gute mathematische Schulkenntnisse und eine Vorlesung beziehungsweise ein Lehrbuch der Zahlentheorie nicht ausreichen, um selbst relativ einfache zahlentheoretische Probleme zu lösen, kann verglichen werden mit der Situation eines Menschen, der reichlich Material - z. B. Holz - hat, dem aber Werkzeuge und Fähigkeiten fehlen, um daraus etwas zielgerichtet Gewünschtes herzustellen. Im zweiten Strang dieses Buches sollen deshalb Werkzeuge, Fähigkeiten und Einstellungen zum Problemlösen in der Zahlentheorie entwickelt beziehungsweise aufgedeckt werden.

Wir beginnen mit einem Beispiel, das eine geringfügige Abwandlung von Aufgabe 1 der zweiten Runde 1970/71 des BWM ist.

### **Problem 1**

Beweisen Sie, dass für alle  $a, b, c, d \in \mathbb{N}_1$  mit  $ad = bc$  die Zahl  $a^2 + b^2 + c^2 + d^2$  mehr als zwei Teiler hat.

Es soll dazu dienen, die allgemeinste Vorgehensweise bewusst zu machen, die häufig anzuwenden ist, wenn sich zunächst keine Suchrichtung anbietet. Wir nennen dieses “Arbeitsprogramm” *Gaußsche Erkundungsstrategie*, weil bekannt ist, dass GAUß einen großen Teil seiner neuen Ergebnisse in der Zahlentheorie durch

eigene Berechnungen gefunden hat. Typische Merkmale dieser Strategie sind die Behandlung von Spezialfällen, wozu auch Zahlenbeispiele gehören, und das Stellen von Fragen (an sich selbst!), wie sie in der folgenden “Checkliste” von G. PÓLYA<sup>3</sup> enthalten sind.

### Pólyas Heuristik-Checkliste

(aus: G. Pólya, Schule des Denkens [17])

#### Wie sucht man die Lösung?

##### Erstens

Du mußt die Aufgabe *verstehen*.

##### Zweitens

Suche den Zusammenhang zwischen den Daten und der Unbekannten. Du mußt vielleicht Hilfsaufgaben betrachten, wenn ein unmittelbarer Zusammenhang nicht gefunden werden kann.

Du mußt schließlich den *Plan* der Lösung erhalten.

##### Drittens

*Führe* Deinen Plan *aus*.

##### Viertens

*Prüfe* die erhaltene Lösung.

#### (1) Verstehen der Aufgabe

- *Was ist unbekannt? Was ist gegeben? Wie lautet die Bedingung?*
- Ist es möglich, die Bedingung zu befriedigen? Ist die Bedingung ausreichend, um die Unbekannte zu bestimmen? Oder ist sie unzureichend? Oder überbestimmt? Oder kontradiktorisch?
- Zeichne eine Figur! Führe eine passende Bezeichnung ein!
- Trenne die verschiedenen Teile der Bedingung! Kannst Du sie hinschreiben?

#### (2) Ausdenken eines Planes

- Hast Du die Aufgabe schon früher gesehen? Oder hast Du dieselbe Aufgabe in einer wenig verschiedenen Form gesehen?
- *Kennst Du eine verwandte Aufgabe?* Kennst Du einen Lehrsatz, der förderlich sein könnte?
- *Betrachte die Unbekannte!* Und versuche, Dich auf eine Dir bekannte Aufgabe zu besinnen, die dieselbe oder eine ähnliche Unbekannte hat.

<sup>3</sup> GEORG PÓLYA (1887-1985) wirkte in Zürich und Stanford.

- *Hier ist eine Aufgabe, die der Deinen verwandt und schon gelöst ist. Kannst Du sie gebrauchen?* Kannst Du ihr Resultat verwenden? Kannst Du ihre Methode verwenden? Würdest Du irgend ein Hilfselement einführen, damit Du sie verwenden kannst?
- Kannst Du die Aufgabe anders ausdrücken? Kannst Du sie auf noch verschiedene Weise ausdrücken? Geh auf die Definition zurück!
- Wenn Du die vorliegende Aufgabe nicht lösen kannst, so versuche, zuerst eine verwandte Aufgabe zu lösen. Kannst Du Dir eine zugänglichere verwandte Aufgabe denken? Eine allgemeinere Aufgabe? Eine speziellere Aufgabe? Eine analoge Aufgabe? Kannst Du einen Teil der Aufgabe lösen? Behalte nur einen Teil der Bedingung bei und lasse den anderen fort; wie weit ist die Unbekannte dann bestimmt, wie kann ich sie verändern? Kannst Du etwas Förderliches aus den Daten ableiten? Kannst Du Dir andere Daten denken, die geeignet sind, die Unbekannte zu bestimmen? Kannst Du die Unbekannte ändern oder die Daten oder, wenn nötig, beide, so daß die neue Unbekannte und die neuen Daten einander näher sind?
- Hast Du alle Daten benutzt? Hast Du die ganze Bedingung benutzt? Hast Du alle wesentlichen Begriffe in Rechnung gezogen, die in der Aufgabe enthalten sind?

### **(3) Ausführen des Planes**

- Wenn Du Deinen Plan der Lösung durchführst, so *kontrolliere jeden Schritt*. Kannst Du deutlich sehen, daß der Schritt richtig ist? Kannst Du beweisen, daß er richtig ist?

### **(4) Rückschau**

- Kannst Du das *Resultat kontrollieren*? Kannst Du den Beweis kontrollieren?
- Kannst Du das Resultat auf verschiedene Weise ableiten? Kannst Du es auf den ersten Blick sehen?
- Kannst Du das Resultat oder die Methode für irgend eine andere Aufgabe gebrauchen?

Mit der Frage nach der unteren Grenze der Teileranzahl von  $e^2 - f^2$  für  $e \geq f + 2$  haben wir zwar eine verwandte Aufgabe, und das Ersetzen etwa von  $d$  durch

$\frac{bc}{a}$  ermöglicht es, unsere Aufgabe anders auszudrücken. Aber beides ergibt keine bessere Einsicht. Deshalb probieren wir Spezialfälle.

- Ist  $a = b$ , so folgt  $c = d$  durch Kürzen, und für  $m := a^2 + b^2 + c^2 + d^2$  ergibt sich die Zerlegung  $m = 2(a^2 + b^2)$ , sodass 2 einen von 1 und  $m$  verschiedenen Teiler darstellt.
- Im Falle  $a = 1$  muss  $d = bc$  sein, und es gilt  $m = 1^2 + b^2 + c^2 + b^2c^2 = (1^2 + b^2)(1^2 + c^2)$ .
- Als ein Beispiel mit verschiedenen Zahlen, die größer als 1 sind, erhalten wir für  $a = 2 \cdot 3$ ,  $b = 2 \cdot 4$ ,  $c = 3 \cdot 5$ ,  $d = 4 \cdot 5$  das Produkt  $m = 2^23^2 + 2^24^2 + 3^25^2 + 4^25^2 = (2^2 + 5^2)(3^2 + 4^2)$ .

Da auch der Faktor 2 im ersten Fall die Form  $2 = 1^2 + 1^2$  hat, **vermuten** wir nun, dass eine Zerlegung

$$m = (s^2 + t^2)(u^2 + v^2) \quad \text{mit } s, t, u, v \in \mathbb{N}_1$$

als Grund für den zusätzlichen Teiler in Frage kommt. Durch Ausmultiplizieren erhalten wir die Quadratsumme

$$m = (su)^2 + (sv)^2 + (tu)^2 + (tv)^2.$$

Wegen  $(su)(tv) = (sv)(tu)$  und  $1 < s^2 + t^2 < m$  wäre also unser Problem gelöst, wenn wir zu  $a, b, c, d \in \mathbb{N}_1$  mit  $ad = bc$  stets Zahlen  $s, t, u, v \in \mathbb{N}_1$  finden könnten, für die

$$(2.15) \quad a = su, \quad b = sv, \quad c = tu, \quad d = tv,$$

erfüllt ist.

Offenbar arbeiten wir jetzt rückwärts. Damit wenden wir eine der ältesten Problemlösemethoden an. Sie wird dem griechischen Philosophen PLATON (429?-348? v. Chr.) zugeschrieben. Ein ausführlicher Bericht des griechischen Mathematikers PAPPUS (PAPPOS von Alexandria, um 320 n. Chr.) ist in dem siebenten Buch seines Werks “Collectiones” zu finden. Er behandelt dort den Studienzweig “Heuristik” als “Kunst des Aufgabenlösen” und stellt dem fortschreitenden Schließen, welches er “Synthese” nennt, das als “Analyse” bezeichnete rückläufige Schließen gegenüber. Wir wollen das “Rückwärtsarbeiten” von PLATON und die “Analyse” von PAPPUS in Zukunft *Rückwärtsstrategie* nennen.

Gehen wir noch einen weiteren Schritt zurück und bilden wegen der gemeinsamen Teiler von  $a$  und  $b$  sowie von  $c$  und  $d$  die Brüche  $\frac{a}{b}$  und  $\frac{c}{d}$ , so gewinnen wir mit

$$\frac{a}{b} = \frac{c}{d} = \frac{u}{v}$$

die überraschende Einsicht, dass die in der sechsten Klasse eingeführten *Kernbrüche* die gesuchte Lösung liefern; denn ist  $\frac{u}{v}$  ein Kernbruch, so stellen  $\frac{a}{b}$  und  $\frac{c}{d}$  Erweiterungen von  $\frac{u}{v}$  dar, d. h. es gibt Zahlen  $s, t \in \mathbb{N}_1$ , mit denen (2.15) gilt.

Dieser Zusammenhang ist die Grundlage einer Problemlösestrategie, die zwar nicht oft, dafür aber recht wirkungsvoll eingesetzt werden kann. Wir bezeichnen sie als *Kernbruchstrategie*. Die dazu gehörenden Begriffe sind in der Literatur nicht einheitlich und oft auch ungünstig erklärt. Im nächsten Abschnitt wird deshalb zunächst der entsprechende Teil der *Zahlgenese* skizziert, bevor wir mit der *Kernbruchstrategie* einen kaum bekannten Zugang zu einem rund 4000 Jahre alten Fragenkreis aufdecken.

## 2.5 Die Kernbruchstrategie und pythagoreische Tripel

Auf Seite 14 wurde schon erwähnt, dass Kernbrüche als Brüche mit teilerfremdem Zähler und Nenner Repräsentanten von unendlich vielen zueinander gleichen Brüchen sind. Will man im Mathematikunterricht am Anfang der Mittelstufe das als schwierig geltende “Kürzen” vermeiden, so lassen sich zwei Brüche als *gleich* definieren, wenn sie eine gemeinsame Erweiterung besitzen. Diese umständlich zu prüfende Bedingung wird in dem folgenden Satz durch ein einfaches Kriterium ersetzt.

### Gleichheitssatz

Sind  $a, b, c, d \in \mathbb{N}_1$ , so gilt  $\frac{a}{b} = \frac{c}{d}$  genau dann, wenn  $ad = bc$  erfüllt ist.

**Beweis** (direkt, zwei Teile, r1):

i) Stellt  $\frac{u}{v}$  die gemeinsame Erweiterung dar, so gibt es  $s, t \in \mathbb{N}_1$  mit  $u = sa$ ,  $v = sb$ ,  $u = tc$ ,  $v = td$ . Damit erhält man  $satd = uv = sbtc$ , und die *Kürzungsregel* (der *Zahlgenese*) ergibt  $ad = bc$ .

ii) Aus  $ad = bc$  folgt die Gleichheit der gleichnamigen Brüche  $\frac{ad}{bd}$  und  $\frac{bc}{bd}$ , die damit eine gemeinsame Erweiterung von  $\frac{a}{b}$  und  $\frac{c}{d}$  sind.  $\square$

Mit Hilfe des *Satzes über den Euklidischen Algorithmus* (Seite 20) können wir zeigen, dass für jeden Bruch  $\frac{a}{b}$  durch Kürzen mit  $d := \text{ggT}(a, b)$  tatsächlich ein Kernbruch entsteht. Mit  $a = a'd$  und  $b = b'd$  folgt nämlich  $d = \text{ggT}(a, b) = \text{ggT}(a'd, b'd) = d \text{ggT}(a', b')$ , woraus sich  $1 = \text{ggT}(a', b')$  ergibt.

Der folgende Satz, der für die *Kernbruchstrategie* entscheidend ist, besagt auch, dass unter den unendlich vielen zueinander gleichen Brüchen genau ein Kernbruch vorkommt.

### Erweiterungssatz

Alle zueinander gleichen Brüche sind Erweiterungen desselben Kernbruchs.

**Beweis** (direkt, a1):

Sind  $\frac{a}{b}$ ,  $\frac{c}{d}$ ,  $\frac{u}{v}$  und  $\frac{x}{y}$  Brüche mit  $\frac{a}{b} = \frac{c}{d}$ ,  $\frac{a}{b} = \frac{u}{v}$ ,  $\text{ggT}(u, v) = 1$ ,  $\frac{c}{d} = \frac{x}{y}$  und  $\text{ggT}(x, y) = 1$ , so ist zu zeigen, dass  $u = x$  und  $v = y$  gilt. Durch Einsetzen der aus dem *Gleichheitssatz* (Seite 35) folgenden Gleichungen  $ad = bc$ ,  $av = bu$  und  $cy = dx$  erhalten wir zunächst  $(ad)(vx) = advx = (av)(dx) = (bu)(cy) = bcuy = (ad)(uy)$ , also  $vx = uy$ . Viermalige Anwendung des *Produktteilersatzes* (Seite 23) ergibt dann  $x | u$ ,  $u | x$ ,  $v | y$ ,  $y | v$ , also  $u = x$  und  $v = y$ .  $\square$

Im Rückblick erkennen wir, dass die Bedingung von *Problem 1* gerade das Kriterium des *Gleichheitssatzes* ist. Typisch für den Einsatz der *Kernbruchstrategie* ist tatsächlich das Vorliegen einer *Gleichung zwischen zwei Produkten*, die dann in eine äquivalente Bruchgleichung umgeformt und durch den zugehörigen Kernbruch ergänzt wird.

Beim Problemlösen kommt es oft darauf an, solche “Muster” zu sehen. Man spricht sogar von der “Kunst des Sehens”. So heißt etwa ein Buch über Problemlösen von B. DE FINETTI “Die Kunst des Sehens in der Mathematik” [7]. Mit den folgenden beiden Beispielen, die üblicherweise mit Hilfe des *Hauptsatzes der elementaren Zahlentheorie* (Seite 49) behandelt werden, soll diese Kunst ein wenig geübt werden.

### Rationalitätskriterium für $\sqrt{m}$ mit $m \in \mathbb{N}_1$

Die reelle Zahl  $\sqrt{m}$  mit  $m \in \mathbb{N}_1$  ist genau dann rational, wenn es Zahlen  $a, b \in \mathbb{N}_1$  mit  $\text{ggT}(a, b) = 1$  gibt, sodass  $\sqrt{m} = \frac{a}{b}$  gilt. Wie bei dem Nachweis der Irrationalität von  $\sqrt{2}$  (Seite 30) erhalten wir durch Quadrieren die zur Definition äquivalente Gleichung

$$(2.16) \quad a^2 = mb^2 \quad \text{mit } a, b \in \mathbb{N}_1 \quad \text{und} \quad \text{ggT}(a, b) = 1.$$

Die Beweismethode von Seite 30 mit Fallunterscheidung könnte hier einen “psychologischen Block” bilden, der uns daran hindert, die *Kernbruchstrategie* anzuwenden. In der zu (2.16) äquivalenten Bruchgleichung

$$\frac{a}{b} = \frac{mb}{a}$$

stellt  $\frac{a}{b}$  schon einen Kernbruch dar. Aufgrund des *Erweiterungssatzes* (Seite 36) gibt es also ein  $t \in \mathbb{N}_1$ , sodass  $mb = ta$  und  $a = tb$  gilt. Einsetzen der zweiten Gleichung in die erste und Kürzen ergibt die notwendige Bedingung  $m = t^2$ , die offensichtlich auch hinreichend dafür ist, dass  $\sqrt{m}$  eine rationale Zahl darstellt.

Die übliche Herleitungsmethode mit Hilfe des *Hauptsatzes der elementaren Zahlentheorie* (Seite 49) werden wir auf Seite 56 verwenden, um ein Rationalitätskriterium für  $\sqrt[k]{q}$  mit  $k \in \mathbb{N}_2$  und  $q \in \mathbb{Q}^+$  zu erhalten.

### Pythagoreische Tripel

Bei dem zweiten Beispiel geht es um die Bestimmung aller Tripel  $(x, y, z) \in \mathbb{N}_1^3$ , die die Gleichung

$$(2.17) \quad x^2 + y^2 = z^2$$

erfüllen. Diese Lösungen heißen üblicherweise *pythagoreische Tripel*, weil PYTHAGORAS (ca. 550 v. Chr.) sowohl den nach ihm benannten geometrischen Satz über die Seitenquadrate von rechtwinkligen Dreiecken bewies als auch Beispiele für rechtwinklige Dreiecke mit ganzzahligen Seitenlängen suchte und fand. Seit etwa sechzig Jahren weiß man aber, dass mehr als tausend Jahre früher Babylonier bereits alle solche Tripel kannten (siehe [21]).

Mit einer Methode, die wohl schon PYTHAGORAS verwendet hat, konnte EUKLID [6] zeigen, dass (2.17) unendlich viele Lösungen  $(x, y, z) \in \mathbb{N}_1^3$  besitzt: In der Gleichung  $(n+1)^2 - n^2 = 2n+1$  wird  $n$  so gewählt, dass  $2n+1 = m^2$

gilt. Dann ergibt sich für jedes  $m \in \mathbb{N}_2$  mit  $2 \nmid m$  ein pythagoreisches Tripel  $(m, \frac{1}{2}(m^2 - 1), \frac{1}{2}(m^2 + 1))$ .

DIOPHANT gab am Anfang eines Buches, das nur Aufgaben zu pythagoreischen Tripeln enthielt, eine Parameterdarstellung für die Lösungsgesamtheit von (2.17) an (siehe [21]). Ähnlich wie schon bei früheren Quellen kann man schließen, dass zur Herleitung der Lösungen anstelle von (2.17) die Produktdarstellung

$$(2.18) \quad x^2 = (z - y)(z + y)$$

benutzt wurde. Diese Methode, bei der eine Gleichung mit mindestens einer Summe durch Klammerung so umgeformt wird, dass sich auf beiden Seiten Produkte ergeben, nennen wir *Klammerungsstrategie*, weil sie bei Zahlentheorieproblemen relativ oft verwendet werden kann.

Bevor wir damit und mit der *Kernbruchstrategie* alle Lösungen von (2.17) bestimmen, vereinfachen wir die Aufgabe mit Hilfe der *Zurückführungsstrategie*. Durch Multiplikation von (2.17) mit  $d^2$  folgt, dass mit einer Lösung  $(x, y, z)$  auch  $(dx, dy, dz)$  für jedes  $d \in \mathbb{N}_1$  die Gleichung erfüllt. Umgekehrt läßt sich im Falle  $\text{ggT}(x, y, z) > 1$  der gemeinsame Teiler herausdividieren, sodass jede Lösung durch "Erweitern" aus einem Lösungstripel entsteht, bei dem die drei Komponenten keinen gemeinsamen Teiler haben.

Der *Satz über Teilbarkeitsregeln* (Seite 18) ergibt außerdem, dass aus  $d \mid x$  und  $d \mid y$  auch  $d \mid z$  folgt. Damit hat eine Lösung  $(x, y, z)$  genau dann teilerfremde Komponenten, wenn  $\text{ggT}(x, y) = 1$  gilt. Insbesondere kann höchstens eine Komponente gerade sein. Wegen  $(2m)^2 = 4(m^2)$  und  $(2m + 1)^2 = 4(m^2 + m) + 1$  für alle  $m \in \mathbb{N}$  gilt  $\text{mod}(w^2, 4) = \text{mod}(w, 2)$  für alle  $w \in \mathbb{N}$ . Aus  $2 \nmid x$  und  $2 \nmid y$  würde also  $\text{mod}(x^2, 4) = \text{mod}(y^2, 4) = 1$  und damit  $\text{mod}(x^2 + y^2, 4) = 2$  folgen - im Widerspruch zu  $\text{mod}(z^2, 4) \in \mathcal{A}_2$ . Da  $x$  und  $y$  vertauschbar sind, können wir in dem folgenden Satz  $2 \mid x$  und damit  $2 \nmid yz$  annehmen.

### Satz über pythagoreische Tripel

Es sei  $\mathcal{P} := \{(x, y, z) \in \mathbb{N}_1^3; x^2 + y^2 = z^2, \text{ggT}(x, y) = 1 \text{ und } 2 \mid x\}$  und  $\mathcal{Q} := \{(u, v) \in \mathbb{N}_1^2; \text{ggT}(u, v) = 1, u > v \text{ und } 2 \nmid (u + v)\}$ . Ist  $(x, y, z) \in \mathcal{P}$  und stellt  $\frac{u}{v}$  den Kernbruch von  $\frac{y+z}{x}$  dar, so ergibt die Zuordnung  $(u, v) \mapsto (x, y, z)$  eine bijektive Abbildung  $\psi : \mathcal{Q} \rightarrow \mathcal{P}$  mit  $\psi(u, v) = (2uv, u^2 - v^2, u^2 + v^2)$  ("eindeutige Parameterdarstellung").

**Beweis** (zwei Teile):

**i) Herleitung der Parameterdarstellung** (direkt, a1):

Die aus (2.18) und der Voraussetzung folgende Kernbruchgleichung

$$\frac{y+z}{x} = \frac{x}{z-y} = \frac{u}{v}$$

ergibt für die Quotienten  $\frac{y}{x}$  und  $\frac{z}{x}$  die beiden Gleichungen  $\frac{y}{x} + \frac{z}{x} = \frac{u}{v}$  und

$\frac{z}{x} - \frac{y}{x} = \frac{v}{u}$ . Durch Subtraktion der zweiten Gleichung von der ersten erhalten wir

$\frac{2y}{x} = \frac{u^2 - v^2}{uv}$ . Da  $x$  gerade ist, setzen wir  $x' := \frac{x}{2}$ . Schreiben wir außerdem  $u^2 - v^2$

als Produkt, so haben wir

$$(2.19) \quad \frac{y}{x'} = \frac{(u-v)(u+v)}{uv} \quad \text{mit} \quad \text{ggT}(x', y) = 1.$$

Nun zeigen wir, dass auch auf der rechten Seite der Bruchgleichung ein Kernbruch steht. Aus  $\text{ggT}(u, v) = 1$  und mit (2.3) folgt

$$1 = \text{ggT}(u+v, u) = \text{ggT}(u-v, u) = \text{ggT}(u+v, v) = \text{ggT}(u-v, v)$$

Um  $\text{ggT}(u^2 - v^2, uv) = 1$  zu erhalten, brauchen wir also nur zu beweisen, dass

$$(2.20) \quad \text{ggT}(a, bc) = 1 \quad \text{für alle } a, b, c \in \mathbb{N}_1 \quad \text{mit} \quad \text{ggT}(a, b) = \text{ggT}(a, c) = 1$$

gilt, weil sich damit nacheinander  $\text{ggT}(u+v, uv) = 1$ ,  $\text{ggT}(u-v, uv) = 1$  und  $\text{ggT}((u-v)(u+v), uv) = 1$  ergibt. Setzen wir  $r := \text{ggT}(a, bc)$ , so folgt  $r \mid a$  und  $r \mid bc$ . Wegen  $\text{ggT}(a, b) = 1$  ist auch  $\text{ggT}(r, b) = 1$ . Mit dem *Produktteilersatz* (Seite 23) erhalten wir  $r \mid c$ , sodass  $r \mid \text{ggT}(a, c)$  gilt. Wegen  $\text{ggT}(a, c) = 1$  muss also  $r = 1$  sein.

Da zwei zueinander gleiche Kernbrüche aufgrund des *Erweiterungssatzes* (Seite 36) durch Erweiterung auseinander hervorgehen, müssen die Zähler und die Nenner jeweils gleich sein. Aus (2.19) mit  $\text{ggT}(u^2 - v^2, uv) = 1$  und aus  $z = \frac{u}{v}x - y$  folgt also

$$x = 2uv, \quad y = u^2 - v^2, \quad z = u^2 + v^2.$$

**ii) Abbildungseigenschaften** (direkt, r1):

$\alpha)$   $\psi$  ist eine Abbildung von  $\mathcal{Q}$  nach  $\mathcal{P}$ : Wegen  $u > v > 0$  ist  $\psi(u, v) \in \mathbb{N}_1^3$ . Für alle  $(u, v) \in \mathbb{N}_1^2$  gilt  $(2uv)^2 + (u^2 - v^2)^2 = 4u^2v^2 + u^4 - 2u^2v^2 + v^4 = (u^2 + v^2)^2$

und  $2 \mid (2uv)$ . Mit  $2 \nmid (u+v)$  ist auch  $2 \nmid (u-v)$  und  $2 \nmid (u^2 - v^2)$ . Damit gilt  $\text{ggT}(2uv, u^2 - v^2) = \text{ggT}(uv, u^2 - v^2)$ , und wie oben folgt  $\text{ggT}(uv, u^2 - v^2) = 1$ .

$\beta$ ) *Surjektivität*: Hier ist nur zu zeigen, dass das Paar  $(u, v)$ , das in i) einer beliebigen Lösung  $(x, y, z) \in \mathcal{P}$  zugeordnet wurde, in  $\mathcal{Q}$  liegt. Die Bedingungen  $(u, v) \in \mathbb{N}_1^2$ ,  $\text{ggT}(u, v) = 1$  und  $u > v$  sind wegen des Kernbruchansatzes erfüllt, und aus  $2 \nmid y$  ergibt sich wegen  $y = u^2 - v^2$  wie oben  $2 \nmid (u+v)$ .

$\gamma$ ) *Injektivität*: Aus den Gleichungen  $z+y = 2u^2$  und  $z-y = 2v^2$ , die unabhängig von der Art der Herleitung sind, und bei unserem Ansatz durch die Zuordnung  $u = \frac{y+z}{g}$ ,  $v = \frac{x}{g}$  mit  $g := \text{ggT}(y+z, x)$  folgt die Eindeutigkeit von  $(u, v) \in \mathcal{Q}$  bei gegebenem  $(x, y, z) \in \mathcal{P}$ .  $\square$

## 2.6 Die $g$ -adische Zahlendarstellung

Wir schließen dieses Kapitel mit einem Satz, der einerseits Grundlage der auch in der Praxis wichtigen *Stellenwertsysteme* ist und der andererseits beim Lösen zahlentheoretischer Probleme relativ oft eine Rolle spielt. Wie schon der letzte Satz unterscheidet sich auch der folgende von den entsprechenden in den üblichen Lehrbüchern durch seine "Konkretheit": An die Stelle einer unbestimmten Existenzaussage tritt die explizite Angabe aller wesentlichen Größen, weil auch damit das Problemlösen unterstützt wird.

### Satz über die $g$ -adische Zahlendarstellung

Für  $g \in \mathbb{N}_2$  und  $m \in \mathbb{N}_1$  gilt

$$m = \sum_{k=0}^s a_k g^k \text{ mit } s \in \mathbb{N}, (a_0, \dots, a_s) \in \mathcal{A}_g^{s+1} \text{ und } a_s > 0$$

genau dann, wenn

$$s = \left\lfloor \frac{\ln m}{\ln g} \right\rfloor \text{ und } a_k = \text{mod} \left( \left[ \frac{m}{g^k} \right], g \right) \text{ für } k = 0, \dots, s$$

erfüllt ist.

**Beweis** (zwei Teile):

i) Die zweite Aussage folgt aus der ersten (direkt, finite Induktion, a1):

Es gilt  $g^s \leq a_s g^s \leq m \leq \sum_{k=0}^s (g-1)g^k = (g-1) \frac{g^{s+1}-1}{g-1} = g^{s+1} - 1$ . Also ist  $g^s \leq m < g^{s+1}$ . Aufgrund des streng monotonen Steigens der natürlichen Logarithmus-Funktion ist diese Ungleichungskette äquivalent zu  $s \leq \frac{\ln m}{\ln g} < s+1$  und damit zu  $s = \left\lfloor \frac{\ln m}{\ln g} \right\rfloor$ .

Analog erhalten wir für jedes  $k \in \mathcal{A}_{s+1}$  die Abschätzung  $0 \leq a_k g^k + \dots + a_0 \leq g^{k+1} - 1$ . Daraus folgt  $\text{mod}(m, g^{k+1}) = a_k g^k + \dots + a_0$  für  $k = 0, \dots, s$ . Dann ist  $a_k g^k = \text{mod}(m, g^{k+1}) - \text{mod}(m, g^k) = m - \left\lfloor \frac{m}{g^{k+1}} \right\rfloor g^{k+1} - m + \left\lfloor \frac{m}{g^k} \right\rfloor g^k = \left\lfloor \frac{m}{g^k} \right\rfloor g^k - \left\lfloor \frac{m}{g^{k+1}} \right\rfloor g^{k+1}$ . Division durch  $g^k$  ergibt

$$(2.21) \quad a_k = \left\lfloor \frac{m}{g^k} \right\rfloor - \left\lfloor \frac{m}{g^{k+1}} \right\rfloor g.$$

Für den Übergang zu  $a_k = \text{mod}\left(\left\lfloor \frac{m}{g^k} \right\rfloor, g\right)$  fehlt uns also nur die Gleichung

$$(2.22) \quad \left\lfloor \frac{m}{g^{k+1}} \right\rfloor = \left\lfloor \left\lfloor \frac{m}{g^k} \right\rfloor \frac{1}{g} \right\rfloor,$$

die der Spezialfall  $\alpha = \frac{m}{g^k}$  der folgenden nützlichen Beziehung zwischen Gauß-Klammern ist: Es gilt

$$(2.23) \quad \left\lfloor \frac{\alpha}{g} \right\rfloor = \left\lfloor \frac{[\alpha]}{g} \right\rfloor \quad \text{für alle } \alpha \in \mathbb{R} \text{ und jedes } g \in \mathbb{N}_2.$$

Setzen wir für den Nachweis  $q := \left\lfloor \frac{[\alpha]}{g} \right\rfloor$  und  $r := \text{mod}([\alpha], g)$ , so ist einerseits  $\alpha = [\alpha] + (\alpha - [\alpha]) = qg + r + \alpha - [\alpha]$ , und andererseits folgt aus  $0 \leq \alpha - [\alpha] < 1$  und  $0 \leq r \leq g-1$ , dass  $0 \leq r + \alpha - [\alpha] < g$  gilt. Damit ergibt sich  $\left\lfloor \frac{\alpha}{g} \right\rfloor = \left\lfloor \frac{qg+r+\alpha-[\alpha]}{g} \right\rfloor = q + \left\lfloor \frac{r+\alpha-[\alpha]}{g} \right\rfloor = q$ .

**ii) Die erste Aussage folgt aus der zweiten** (direkt, finite Induktion, r1):

Wegen  $\frac{\ln m}{\ln g} > 0$  ist  $s \in \mathbb{N}$ . Die oben festgestellte Äquivalenz von  $s = \left\lfloor \frac{\ln m}{\ln g} \right\rfloor$  und  $g^s \leq m < g^{s+1}$  ergibt jetzt  $\left\lfloor \frac{m}{g^{s+1}} \right\rfloor = 0$  und  $1 \leq \left\lfloor \frac{m}{g^s} \right\rfloor < g$ , sodass  $a_s = \text{mod}\left(\left\lfloor \frac{m}{g^s} \right\rfloor, g\right) = \left\lfloor \frac{m}{g^s} \right\rfloor > 0$  gilt.

Unmittelbar aus der Darstellung der Koeffizienten  $a_k$  folgt  $(a_0, \dots, a_s) \in \mathcal{A}_g^{s+1}$ . Schließlich erhalten wir aus (2.21) mit finiter Induktion durch "Aufsummieren"

$$\sum_{k=0}^r a_k g^k = m - \left[ \frac{m}{g^{r+1}} \right] g^{r+1} \text{ für jedes } r \in \mathcal{A}_{s+1}.$$

Für  $r = s$  ergibt sich daraus wegen der oben gewonnenen Gleichung  $\left[ \frac{m}{g^{s+1}} \right] = 0$  die  $g$ -adische Summendarstellung von  $m$ .  $\square$

Die Berechnung der Koeffizienten  $a_k$  lässt sich mit Hilfe von (2.22) vereinfachen.

Setzen wir nämlich  $q_k := \left[ \frac{m}{g^k} \right]$ , so ist  $q_{k+1} = \left[ \frac{q_k}{g} \right]$ . Die Zahlen  $q_{k+1}$  und  $a_k$

ergeben sich also durch sukzessive Division mit Rest aus den Gleichungen

$$q_0 = m, \quad q_k = q_{k+1} g + a_k \text{ mit } a_k \in \mathcal{A}_g \text{ für } k = 0, \dots, s,$$

wobei  $s$  erreicht ist, wenn  $q_{s+1} = 0$  gilt.

Die Zahlensysteme, die zu  $g = 2, 8$  und  $16$  gehören und die eine besondere Rolle in der Informatik spielen, haben eigene Namen: *Binär-* oder *Dualsystem* (früher auch *dyadisches System*), *Oktalsystem* und *Hexadezimal-* oder *Sedezimalsystem*.

In dem letzten System werden anstelle der Zahlen  $10, 11, 12, 13, 14, 15$  die Buchstaben A, B, C, D, E, F verwendet, um einstellige "Ziffern" zu erhalten.

## Beispiele

$$m = 111, \quad \boxed{g = 2} :$$

| Quotient | Rest | Exponent |
|----------|------|----------|
| 55       | 1    | 0        |
| 27       | 1    | 1        |
| 13       | 1    | 2        |
| 6        | 1    | 3        |
| 3        | 0    | 4        |
| 1        | 1    | 5        |
| 0        | 1    | 6        |

Damit ist  $111 = (1101111)_2$ .

$$m = 111, \quad \boxed{g = 16} :$$

| Quotient | Rest | Exponent |
|----------|------|----------|
| 6        | 15   | 0        |
| 0        | 6    | 1        |

Damit ist  $111 = (6F)_{16}$ .

$$m = 111, \quad \boxed{g = 3} :$$

| Quotient | Rest | Exponent |
|----------|------|----------|
| 37       | 0    | 0        |
| 12       | 1    | 1        |
| 4        | 0    | 2        |
| 1        | 1    | 3        |
| 0        | 1    | 4        |

Damit ist  $111 = (11010)_3$ .

$$m = 111, \quad \boxed{g = 8} :$$

| Quotient | Rest | Exponent |
|----------|------|----------|
| 13       | 7    | 0        |
| 1        | 5    | 1        |
| 0        | 1    | 2        |

Damit ist  $111 = (157)_8$ .

## 2.7 Aufgaben und Probleme zu Kapitel 2

### Aufgabe 2.1:

Suchen und beweisen Sie (mindestens) vier nichttriviale zahlentheoretische Eigenschaften der *Fibonacci-Folge*  $(f_n)_n$ , die rekursiv durch  $f_1 := 1$ ,  $f_2 := 1$  und  $f_{n+2} := f_{n+1} + f_n$  für alle  $n \in \mathbb{N}_1$  definiert wird.

[Hinweis: “Trivial” wäre, dass  $(f_n)_n$  eine monoton wachsende Folge natürlicher Zahlen ist. Es folgen einige Suchvorschläge: Partialsummen der Folgenglieder und ihrer Quadrate, Darstellung der Quadrate der Folgenglieder, ggT benachbarter Glieder, Teilbarkeit durch Primzahlen, Reste bei Division durch feste natürliche Zahlen.]

### Aufgabe 2.2:

Drücken Sie für ungerades  $n \in \mathbb{N}_1$  die Anzahl

$$A(n) := \text{card} \{ (x, y) \in \mathbb{N}_1^2; n = x^2 - y^2 \}$$

mit Hilfe einer zahlentheoretischen Funktion aus.

### Aufgabe 2.3:

Es sei  $F_m := 2^{2^m} + 1$  für  $m \in \mathbb{N}$ . Beweisen Sie, dass  $\text{ggT}(F_m, F_n) = 1$  für alle  $m, n \in \mathbb{N}$  mit  $m < n$  gilt.

[Hinweis: Zeigen Sie zunächst, dass  $F_m$  Teiler von  $F_n - 2$  ist.]

### Aufgabe 2.4:

Berechnen Sie  $d := \text{ggT}(323, 391)$  und stellen Sie  $d$  als Linearkombination von 323 und 391 dar.

### Aufgabe 2.5:

Berechnen Sie für  $m, n \in \mathbb{N}_1$  den größten gemeinsamen Teiler von  $\sum_{k=0}^{m-1} 9 \cdot 10^k$  und  $\sum_{k=0}^{n-1} 9 \cdot 10^k$ .

### Aufgabe 2.6:

a) Ein “Schnellrechner” fordert jemand auf, sich eine dreistellige Zahl zu merken, sie mit 143 zu multiplizieren und die letzten drei Ziffern des Ergebnisses zu

nennen. Der Schnellrechner sagt dann ohne Mühe die dreistellige Zahl. Wieso? [Hinweis: Er multipliziert mit 7.]

b) Zeigen Sie, dass jeder Mensch, dessen Geburtstag zwischen 1901 und 2071 liegt, seinen achtundzwanzigsten Geburtstag am selben Wochentag feiert, an dem er geboren wurde. [Hinweis: Das Jahr 2000 war ein Schaltjahr.]

### Aufgabe 2.7:

Für jedes  $a \in \mathbb{N}_1$  sei  $z(a) := \left\lceil \frac{\ln a}{\ln 2} \right\rceil$  und  $a = \sum_{k=0}^{z(a)} b_k(a) 2^k$  mit  $b_k(a) \in \{0, 1\}$  für  $k = 0, \dots, z(a)$  sei die Darstellung von  $a$  im 2-adischen Zahlensystem. Außerdem sei  $b_k(a) := 0$  für  $k > z(a)$  sowie  $z(0) := 0$  und  $b_0(0) := 0$  gesetzt. Für alle  $m, n \in \mathbb{N}$  wird die Verknüpfung  $++$  (*binäre Addition*, gelesen “biplus”) durch  $m ++ n := \sum_{k=0}^{z(m+n)} |b_k(m) - b_k(n)| 2^k$  definiert.

i) Zeigen Sie, dass  $\mathbb{N}$  mit dem neutralen Element 0 und mit der Verknüpfung  $++$  eine abelsche Gruppe darstellt, in der jedes Element zu sich selbst invers ist.

ii) Leiten Sie mit Hilfe der für jedes  $a \in \mathbb{N}_1$  erklärten Abkürzung  $\hat{a} := 2^{z(a)}$  Rekursionsformeln zur Berechnung von  $m ++ n$  her, indem Sie die Fälle  $\hat{m} = \hat{n}$ ,  $\hat{m} > \hat{n}$  und  $\hat{m} < \hat{n}$  unterscheiden.

### Aufgabe 2.8:

Es sei  $S = (s_1, \dots, s_n) \in \mathbb{N}^n$  eine “*Stellung des Nimspiels*”.  $S' = (s'_1, \dots, s'_n) \in \mathbb{N}^n$  heißt “*Folgestellung von S*”, wenn es ein  $k \in \{1, \dots, n\}$  gibt, sodass  $s'_k < s_k$  und  $s'_i = s_i$  für  $i \neq k$  gilt.  $\mathcal{F}(S)$  sei die Menge aller Folgestellungen von  $S$  und  $B(S) := s_1 ++ \dots ++ s_n$ , wobei  $m ++ n$  die in Aufgabe 2.7 definierte binäre Addition bezeichnet. Beweisen Sie, dass  $B(S) = 0$  genau dann erfüllt ist, wenn  $B(S') > 0$  für alle  $S' \in \mathcal{F}(S)$  gilt.

### Aufgabe 2.9:

Bestimmen Sie alle Tripel  $(x, y, z) \in \mathbb{N}_1^3$ , die  $323x + 391y + 437z = 10473$  erfüllen.

Die folgenden zwölf Probleme stammen aus dem Bundeswettbewerb Mathematik.

**Problem 2:**

Für jede natürliche Zahl  $n$  werde die Quersumme ihrer Darstellung im Zehnersystem mit  $Q(n)$  bezeichnet. Man beweise, dass für unendlich viele natürliche Zahlen  $k$  die Ungleichung  $Q(3^k) \geq Q(3^{k+1})$  gilt.

**Problem 3:**

Man bestimme (mit Beweis) alle Primzahlen  $p$ , für die das Gleichungssystem

$$\begin{aligned} p + 1 &= 2x^2 \\ p^2 + 1 &= 2y^2 \end{aligned}$$

Lösungen mit ganzen Zahlen  $x, y$  besitzt.

**Problem 4:**

Es gibt Paare von Quadratzahlen mit folgenden beiden Eigenschaften:

- (1) Ihre Dezimaldarstellungen haben die gleiche Ziffernzahl, wobei die erste Ziffer jeweils von 0 verschieden ist.
- (2) Hängt man an die Dezimaldarstellung der ersten die der zweiten an, so entsteht die Dezimaldarstellung einer weiteren Quadratzahl.

Beispiel: 16 und 81;  $1681 = 41^2$ . Man beweise, dass es unendlich viele Paare von Quadratzahlen mit diesen Eigenschaften gibt.

**Problem 5:**

Von der Zahlenfolge  $a_0, a_1, a_2, \dots$  ist bekannt:  $a_0 = 0, a_1 = 1, a_2 = 1$  und  $a_{n+2} + a_{n-1} = 2(a_{n+1} + a_n)$  für alle  $n \in \mathbb{N}$ . Es ist zu beweisen, dass alle Glieder dieser Folge Quadratzahlen sind.

**Problem 6:**

Gesucht werden drei natürliche Zahlen  $a, b, c$ , bei denen das Produkt von je zweien bei Division durch die dritte den Rest 1 lässt. Man bestimme alle Lösungen.

**Problem 7:**

Welche Zahlen durchläuft die Folge  $\left(n + \left\lfloor \sqrt{n} + \frac{1}{2} \right\rfloor\right)_{n \in \mathbb{N}}$ , wenn  $[x]$  die größte ganze Zahl  $\leq x$  bedeutet?

**Problem 8:**

Das arithmetische Mittel zweier verschiedener natürlicher Zahlen  $x$  und  $y$  ist eine zweistellige Zahl. Sie geht in das geometrische Mittel von  $x$  und  $y$  über, wenn man ihre Ziffern vertauscht.

a) Bestimme  $x$  und  $y$ .

b) Weise nach, dass die Aufgabe a) bis auf die Reihenfolge von  $x$  und  $y$  genau ein Lösungspaar hat, wenn die Basis  $g$  des benützten Stellungszahlensystems 10 ist, dass es dagegen für  $g = 12$  keine Lösung gibt.

**Problem 9:**

Eine natürliche Zahl besitzt eine tausendstellige Darstellung im Dezimalsystem, bei der höchstens eine Ziffer von 5 verschieden ist. Man zeige, dass sie keine Quadratzahl ist.

**Problem 10:**

Gegeben sind  $n$  Ziffern  $a_1$  bis  $a_n$  in fester Reihenfolge. Gibt es eine natürliche Zahl, bei der die Dezimaldarstellung ihrer Quadratwurzel hinter dem Komma gerade mit diesen Ziffern in der vorgeschriebenen Reihenfolge beginnt? Das Ergebnis ist zu begründen.

**Problem 11:**

Man beweise: Für jede natürliche Zahl  $n$  gibt es eine im Dezimalsystem  $n$ -stellige Zahl aus den Ziffern 1 und 2, die durch  $2^n$  teilbar ist.

Gilt dieser Satz auch in einem Stellenwertsystem der Basis 4 bzw. 6?

**Problem 12:**

Man bestimme die Menge aller natürlichen Zahlen  $n$ , für die  $n2^{n-1} + 1$  eine Quadratzahl ist.

**Problem 13:**

An einer Tafel stehen die Zahlen 1, 2, 3,  $\dots$ , 2002. Man darf irgend zwei Zahlen wegwischen und dafür ihre Differenz anschreiben. Wiederholt man diesen Vorgang genügend oft, so bleibt an der Tafel schließlich nur noch eine Zahl stehen. Es ist nachzuweisen, dass diese Zahl ungerade ist.

# Kapitel 3

## Elementare Primzahltheorie

### 3.1 Definition und grundlegende Eigenschaften der Primzahlen

EUKLIDS Beschreibung der Primzahlen (Seite 14) lässt sich mit Hilfe der Teileranzahlfunktion etwas zweckmäßiger formulieren.

#### Definition der Primzahl

Eine natürliche Zahl  $n$  heißt *Primzahl*, wenn  $d(n) = 2$  ist.

Die Menge aller Primzahlen wird mit  $\mathbb{P}$  bezeichnet.

Nach der Größe geordnet bezeichnet  $p_i$  für  $i \in \mathbb{N}_1$  die  $i$ -te Primzahl. Also ist  $p_1 = 2$ ,  $p_2 = 3$ ,  $p_3 = 5$ ,  $\dots$ . Häufig verwenden wir den Buchstaben  $q$  (mit Index) für Primzahlen. Analog zur Bezeichnung der “gekappten” Mengen natürlicher Zahlen (Seite 10) ist auch die folgende Abkürzung sehr zweckmäßig:

#### Bezeichnung von “gekappten” Primzahlmengen

$\mathbb{P}_a := \{p \in \mathbb{P} ; p \geq a\}$  für jedes  $a \in \mathbb{N}_3$ .

Der nächste Satz gibt den Anlass für eine weitere nützliche Abkürzung.

#### Satz über den kleinsten Primteiler

Jedes  $n \in \mathbb{N}_2$  hat einen kleinsten Teiler  $d \in \mathbb{N}_2$ . Dieser Teiler  $d$  ist eine Primzahl, die mit  $kP(n)$  bezeichnet wird.

**Beweis** (zwei Teile, zweite Aussage indirekt, r1):

a) Die Menge der Teiler ist endlich und besitzt wegen  $n > 1$  mindestens zwei Elemente. Aufgrund des *Minimumsatzes* (Seite 11) gilt die erste Aussage.

b) Aus  $d \notin \mathbb{P}$  würde folgen, dass es ein  $f \in \mathbb{N}_2$  gibt mit  $f < d$  und  $f \mid d$ . Mit dem *Satz über Teilbarkeitsregeln* (Seite 18) ergäbe sich  $f \mid n$  im Widerspruch dazu, dass  $d$  kleinster Teiler von  $n$  in  $\mathbb{N}_2$  ist.  $\square$

### Satz über die Primzahlmenge

Die Menge  $\mathbb{P}$  ist unendlich.

**Beweis** (Idee von EUKLID, ca. 300 v. Chr., vollständige Induktion, a1):

Es sei  $\mathcal{M} := \{k \in \mathbb{N}_1; \text{card } \mathbb{P} \geq k\}$ . Mit  $2 \in \mathbb{P}$  gilt  $1 \in \mathcal{M}$ . Ist  $m \in \mathcal{M}$  und sind  $q_1, \dots, q_m$  paarweise verschiedene Primzahlen, so folgt, dass  $q_{m+1} := kP(s_m)$  mit  $s_m := q_1 \cdots q_m + 1$  eine von  $q_1, \dots, q_m$  verschiedene Primzahl darstellt, weil  $s_m$  beim Teilen durch  $q_1, \dots, q_m$  jeweils den Rest 1 lässt. Damit ist  $\text{card } \mathbb{P} \geq m + 1$ , d. h.  $m + 1 \in \mathcal{M}$ . Also gilt  $\mathcal{M} = \mathbb{N}_1$ , und wegen  $\mathbb{P} \subset \mathbb{N}_1$  ergibt sich  $\text{card } \mathbb{P} = \text{card } \mathbb{N}_1$ .  $\square$

## Vorteile der vollständigen Induktion

In den meisten Lehrbüchern wird der **Satz über die Primzahlmenge** indirekt bewiesen. Obwohl EUKLID weder das Beweisprinzip der vollständigen Induktion noch den Begriff “unendlich” kannte, formulierte er den Satz (“Die Anzahl der Primzahlen ist größer als jede natürliche Zahl”) und seine Begründung ganz im Sinne des obigen Beweises.

Auf Seite 40 wurde im Hinblick auf das Problemlösen der Vorteil konkreter Satzformulierungen gegenüber reinen Existenzaussagen erwähnt. Bei den Herleitungen liegt eine ähnliche Situation vor. Falls für einen zahlentheoretischen Satz sowohl ein indirekter Beweis als auch ein Beweis mit vollständiger Induktion möglich ist, liefert meistens der letztere die tiefere Einsicht oder sogar weiterführende Aspekte. Im obigen Fall bietet es sich zum Beispiel an, die durch  $q_1 := 2$  und  $q_{n+1} := kP(q_1 \cdots q_n + 1)$  für  $n \in \mathbb{N}_1$  rekursiv definierte Folge  $(q_n)_n$ <sup>1</sup>, die wir “**Euklid-Folge**” nennen wollen, zu betrachten:  $q_1 = 2, q_2 = 3, q_3 = 7, q_4 = 43, q_5 = 13, q_6 = 53, q_7 = 5, \dots, q_{12} = 11, q_{13} = 17, \dots$

<sup>1</sup> Ist der Indexbereich einer Folge  $\mathbb{N}_1$ , so lassen wir in dem Folgensymbol diese Angabe weg.

Der Beweis des **Satzes über die Primzahlmenge** liefert die Aussage, dass die Folge aus paarweise verschiedenen Primzahlen besteht. Beachtet man, dass die lineare diophantische Gleichung  $q_1 \cdots q_n s + q_{n+1} t = 1$ , die das Erscheinen der jeweils kleinsten noch nicht aufgetretenen Primzahl  $q_{n+1}$  wiedergibt, aufgrund des **Satzes über die lineare diophantische Gleichung** (Seite 28) unendlich viele Lösungen besitzt, so ist es nicht allzu gewagt, die Beobachtung, die sich auf die ersten sieben Primzahlen stützt, zu verallgemeinern:

### Vermutung über die Euklid-Folge

Alle Primzahlen kommen in der Euklid-Folge vor.

Diese Vermutung ist in zweifacher Hinsicht “sehr stark”:

- i) Bisher ist außer  $(p_n)_n$  und einfachen Umordnungen von  $(p_n)_n$  keine arithmetisch definierte Folge bekannt, die jede Primzahl genau einmal und sonst keine Zahlen enthält.
- ii) Da die Produkte der sukzessiv auftretenden Primzahlen rasch wachsen, ist die Aussage nur für kleine Indizes nachprüfbar.

Schon für die Berechnung der obigen Werte wurde ein Computeralgebrasystem (CAS) benötigt. Empfehlenswert für die Zahlentheorie ist das Computeralgebrasystem PARI (<http://pari.math.u-bordeaux.fr/>). Wer reichlich Speicherplatz (mehr als 1 Gb) zur Verfügung hat, kann das kostenlose Ausführungsprogramm SAGE (<http://www.sagemath.org>) benutzen, das neben PARI mehr als 60 Mathematikprogramme bereitstellt.

## 3.2 Der Hauptsatz der elementaren Zahlentheorie

### Hauptsatz (der elementaren Zahlentheorie)

Zu jedem  $n \in \mathbb{N}_2$  gibt es genau ein  $t \in \mathbb{N}_1$  und eindeutig bestimmte Primzahlen  $q_1, \dots, q_t$  mit  $q_1 \leq \dots \leq q_t$ , sodass

$$(3.1) \quad n = q_1 \cdots q_t$$

gilt.

**Beweis** (zwei Teile: Existenz und Eindeutigkeit):

Vorübergehend wird für  $n \in \mathbb{N}_2$  eine Darstellung

$$n = q_1 \cdots q_t \text{ mit } q_i \in \mathbb{P} \text{ für } i = 1, \dots, t \text{ und } q_1 \leq \dots \leq q_t$$

als *Primärzerlegung* von  $n$  bezeichnet.

**i) Existenz** (erweiterte Induktion, Fallunterscheidung, a1)

Jede Primzahl hat sich selbst als Primärzerlegung. Für Zahlen  $n \in \mathbb{N}_2 \setminus \mathbb{P}$  hilft der kleinste Primteiler von  $n$ , eine Primärzerlegung anzugeben, wenn für alle kleineren Zahlen aus  $\mathbb{N}_2$  schon eine solche bekannt ist. Deshalb setzen wir

$$\mathcal{M} := \{k \in \mathbb{N}_2 ; \text{ Jedes } j \in \mathbb{N}_2 \text{ mit } j \leq k \text{ besitzt eine Primärzerlegung} \}.$$

Wegen  $2 \in \mathbb{P}$  ist  $2 \in \mathcal{M}$ . Für  $m \in \mathcal{M}$  sei

$$q := kP(m+1).$$

Dann gibt es ein  $h \in \mathbb{N}_1$ , sodass  $m+1 = qh$  gilt.

Im Falle  $h = 1$  ist  $m+1 = q$  eine Primärzerlegung, die zu den Primärzerlegungen aller Zahlen  $j \in \mathbb{N}_2$  mit  $j \leq m$  hinzukommt. Also ist  $m+1 \in \mathcal{M}$ .

Für  $h \in \mathbb{N}_2$  gilt  $h = \frac{m+1}{q} \leq \frac{m+1}{2} < m$ . Damit besitzt  $h$  nach Induktionsvoraussetzung eine Primärzerlegung  $h = q'_1 \cdots q'_r$ . Es folgt  $m+1 = q q'_1 \cdots q'_r$ . Dabei ist  $q \leq q'_1$  aufgrund der Definition von  $q$ . Also gilt auch in diesem Fall  $m+1 \in \mathcal{M}$ , und der *Induktionssatz* (Seite 12) ergibt  $\mathcal{M} = \mathbb{N}_2$ .

**ii) Eindeutigkeit**

Von den bisher bekannten beiden Beweistypen bringen wir wegen der Bedeutung des *Hauptsatzes* und aus didaktischen Gründen zwei Vertreter, deren Verschmelzung zu einem “schulgeeigneten” Beweis in der *Zahlgenese* zu finden ist.

**Erster Beweis** (Idee von EUKLID, ca. 300 v. Chr., vollständige Induktion, a2):

Die Induktionsmenge

$$\mathcal{M} := \{k \in \mathbb{N}_1 ; \text{ Bei allen } n \in \mathbb{N}_2, \text{ die eine Primärzerlegung mit } k \text{ Primfaktoren besitzen, ist diese Zerlegung eindeutig} \}$$

enthält 1, weil die Primzahlen definitionsgemäß nur sich selbst als Primärzerlegung haben. Ist  $m \in \mathcal{M}$  und stellt  $n \in \mathbb{N}_2$  eine Zahl dar, die eine Primärzerlegung  $q_1 \cdots q_{m+1}$  besitzt, so sei  $q'_1 \cdots q'_s$  irgendeine Primärzerlegung von  $n$ . Da  $q_1$  und  $q'_1$  Teiler von  $n$  sind, gilt  $q_1 \mid q'_1 \cdots q'_s$  und  $q'_1 \mid q_1 \cdots q_{m+1}$ . Der *Produkteilersatz* (Seite 23) mit  $a = q_1$  und  $b_0 \cdots b_n = q'_1 \cdots q'_s$  ergibt, dass ein  $i \in \{1, \dots, s\}$  existiert, für

das  $q_1 = q'_i$  gilt, weil für Primzahlen  $a, b_0, \dots, b_n$  die Bedingungen  $\text{ggT}(a, b_i) = 1$  mit  $a \nmid b_i$  äquivalent sind und die Aussage  $a \mid b_0$  mit  $a = b_0$  gleichwertig ist.

Entsprechend gibt es ein  $j \in \{1, \dots, m+1\}$  mit  $q'_1 = q_j$ . Wegen  $q_1 = q'_i \geq q'_1$  und  $q'_1 = q_j \geq q_1$  folgt  $q_1 = q'_1$ . Damit ist  $\frac{n}{q_1} = q_2 \cdots q_{m+1}$  nach Induktionsvoraussetzung die einzige Primärzerlegung von  $\frac{n}{q_1}$ . Da auch  $\frac{n}{q_1} = q'_2 \cdots q'_s$  mit  $q'_2 \leq \dots \leq q'_s$  gilt, muss  $m+1 = s$  und  $q_i = q'_i$  für  $i = 2, \dots, m+1$  sein. Also ist  $m+1 \in \mathcal{M}$ , und der *Induktionssatz* (Seite 12) ergibt  $\mathcal{M} = \mathbb{N}_1$ .

**Zweiter Beweis** (erweiterte Induktion, Fallunterscheidung, Widerspruchsschluss, a3):

Die Induktionsmenge sei

$\mathcal{M} := \{k \in \mathbb{N}_2 ; \text{Jedes } j \in \mathbb{N}_2 \text{ mit } j \leq k \text{ besitzt genau eine Primärzerlegung}\}$ .

Als kleinste Primzahl liegt 2 in  $\mathcal{M}$ . Für den Induktionsschritt sei  $m \in \mathcal{M}$  und  $q := kP(m+1)$ .

a) Im Falle  $m+1 = q$  hat  $m+1$  als Primzahl nur diese Primärzerlegung. Mit  $m \in \mathcal{M}$  gehört also auch  $m+1$  zu  $\mathcal{M}$ .

b) Für  $m+1 \neq q$  wird zunächst mit Hilfe eines indirekten Schlusses von E. ZERMELO (1934) **ohne Verwendung des Produktteilersatzes** gezeigt, dass  $q$  als Faktor in *jeder* Primärzerlegung von  $m+1$  vorkommt. Anschließend lässt sich auf  $\frac{m+1}{q}$  die Induktionsaussage anwenden.

Ist  $q'_1 \cdots q'_s$  mit  $s \geq 2$  irgendeine Primärzerlegung von  $m+1 \in \mathbb{N}_2 \setminus \mathbb{P}$ , so gilt  $q \leq q'_1$  aufgrund der Definition von  $q$ . Unter der **Annahme, dass  $q < q'_1$  ist**, setzen wir

$$a := q'_2 \cdots q'_s \quad \text{und} \quad b := (q'_1 - q) a.$$

Wegen  $a \geq q'_2 \geq 2$  und  $a = \frac{m+1}{q'_1} \leq \frac{m+1}{2} < m$  besitzt  $a$  nach Induktionsvoraussetzung die eindeutige Primärzerlegung  $q'_2 \cdots q'_s$ , und aus  $q < q'_2 \leq \dots \leq q'_s$  folgt  $q \neq q'_i$  für  $i = 2, \dots, s$ .

Auch  $b$  hat eine eindeutige Primärzerlegung, weil einerseits mit  $q'_1 - q \geq 1$  und  $a \geq 2$  die untere Schranke  $b \geq 2$  und andererseits wegen  $b = q'_1 a - qa = m+1 - qa$  die obere Abschätzung  $b \leq m$  für die Induktionsvoraussetzung vorliegt. Außerdem ergibt der *Satz über Teilbarkeitsregeln* (Seite 18), dass mit  $q \mid (m+1)$  und  $q \mid (qa)$  auch  $q \mid b$  gilt. Wegen  $b \geq a \geq q'_2 > q$  besitzt  $\frac{b}{q}$  nach Induktionsvoraus-

setzung eine eindeutige Primärzerlegung. Deshalb gehört  $q$  zu den Primfaktoren der eindeutigen Primärzerlegung von  $b = (q'_1 - q) a$ . Da  $q$  aber unter den Primfaktoren von  $a$  nicht vorkommt, muss  $q$  Teiler von  $q'_1 - q$  sein. Dann folgt mit dem *Satz über Teilbarkeitsregeln*, dass  $q$  die Primzahl  $q'_1$  teilt. Das ist **wegen der Annahme  $q < q'_1$  ein Widerspruch** zur Primzahleigenschaft von  $q'_1$ . Also muss  $q = q'_1$  gelten.

Da  $\frac{m+1}{q}$  nach Induktionsvoraussetzung nur die Primärzerlegung  $q'_2 \cdots q'_s$  hat, ist  $m+1 = q q'_2 \cdots q'_s$  die eindeutige Primärzerlegung von  $m+1$ , sodass  $m+1$  in  $\mathcal{M}$  liegt. Der *Induktionssatz* ergibt schließlich  $\mathcal{M} = \mathbb{N}_2$ .  $\square$

Anstelle der *Primärzerlegung* (3.1) werden im Folgenden zwei zweckmäßigere Darstellungen verwendet. Durch Zusammenfassen gleicher Primfaktoren zu Potenzen erhalten wir die erste Darstellung:

### Bezeichnung der Primpotenzdarstellung

Hat  $n \in \mathbb{N}_2$  die *Primärzerlegung*  $n = q'_1 \cdots q'_t$  und wird rekursiv

$$e_1 := \max \{j \in \mathbb{N}_1; q'_j = q'_1\},$$

$$e_2 := \max \{j \in \mathbb{N}_1; j > e_1 \text{ und } q'_j = q'_{e_1+1}\},$$

...

$$e_r := \max \{j \in \mathbb{N}_1; j > e_1 + \cdots + e_{r-1} \text{ und } q'_j = q'_{e_1+\cdots+e_{r-1}+1}\}$$

definiert, so heißt

$$(3.2) \quad n = \prod_{k=1}^r q_k^{e_k} \text{ mit } q_1 := q'_1 \text{ und } q_k := q'_{e_1+\cdots+e_{k-1}+1}, \quad k = 2, \dots, r,$$

*Primpotenzdarstellung* von  $n$ .

Falls die Primzahlexponenten mehrerer Zahlen verglichen werden sollen, ist eine Darstellung günstiger, bei der die *Primpotenzdarstellung* (3.2) von  $n \in \mathbb{N}_2$  für alle Primzahlen, die  $n$  nicht teilen, "formal" durch entsprechende Potenzfaktoren mit dem Exponenten 0 ergänzt wird:

### Bezeichnung der formalen Darstellung

Hat  $n \in \mathbb{N}_2$  die *Primpotenzdarstellung*  $n = \prod_{k=1}^r q_k^{e_k}$ , so heißt

$$(3.3) \quad n = \prod_{p \in \mathbb{P}} p^{\nu_p(n)} \text{ mit } \nu_p(n) := \begin{cases} e_k, & \text{wenn } p = q_k, \quad k \in \{1, \dots, r\}, \\ 0 & \text{sonst,} \end{cases}$$

*formale Darstellung von  $n$ .* Zu der Zahl 1 wird die *formale Darstellung* durch  $\nu_p(1) := 0$  für alle  $p \in \mathbb{P}$  erklärt.

### 3.3 Anwendungen des Hauptsatzes

Die Zahlen  $r$  und  $t$  aus der *Primpotenzdarstellung* beziehungsweise aus der *Primärzerlegung* ergeben zwei nützliche zahlentheoretische Funktionen:

**Bezeichnung der Primteileranzahl und der Primpotenzteileranzahl**

Die Abbildung  $\omega : \mathbb{N}_1 \rightarrow \mathbb{N}$  mit

$$(3.4) \quad \omega(n) := \begin{cases} \text{card} \{ p \in \mathbb{P} ; p \mid n \}, & \text{wenn } n \in \mathbb{N}_2, \\ 0, & \text{wenn } n = 1, \end{cases}$$

heißt *Anzahlfunktion der Primteiler*.

Die Abbildung  $\Omega : \mathbb{N}_1 \rightarrow \mathbb{N}$  mit

$$(3.5) \quad \Omega(n) := \begin{cases} \text{card} \{ (p, k) \in \mathbb{P} \times \mathbb{N}_1 ; p^k \mid n \}, & \text{wenn } n \in \mathbb{N}_2, \\ 0, & \text{wenn } n = 1, \end{cases}$$

heißt *Anzahlfunktion der Primpotenzteiler*.

Der Vorteil der *formalen Darstellung* zeigt sich schon, wenn eine Darstellung für das Produkt von zwei Zahlen  $a, b \in \mathbb{N}_2$  mit  $a = \prod_{p \in \mathbb{P}} p^{\nu_p(a)}$  und  $b = \prod_{p \in \mathbb{P}} p^{\nu_p(b)}$  benötigt wird. Für jeden Primteiler, der in beiden *Primpotenzdarstellungen* vorkommt, lässt sich die *Potenzproduktregel der Zahlgenese* anwenden. Fallunterscheidung ergibt dann

$$(3.6) \quad \nu_p(ab) = \nu_p(a) + \nu_p(b) \text{ für alle } p \in \mathbb{P}.$$

Mit Hilfe der *formalen Darstellung* erhalten wir ein sehr häufig anwendbares Teilbarkeitskriterium:

**Teilbarkeitssatz**

Haben  $a, b \in \mathbb{N}_1$  die *formalen Darstellungen*  $a = \prod_{p \in \mathbb{P}} p^{\nu_p(a)}$  und  $b = \prod_{p \in \mathbb{P}} p^{\nu_p(b)}$ , so gilt  $a \mid b$  genau dann, wenn

$$(3.7) \quad \nu_p(a) \leq \nu_p(b) \text{ für alle } p \in \mathbb{P}$$

erfüllt ist.

**Beweis** (zwei Teile, direkt, r1):

a) Ist  $a \mid b$ , so gibt es ein  $c \in \mathbb{N}_1$  mit  $b = ac$  und  $c = \prod_{p \in \mathbb{P}} p^{\nu_p(c)}$ . Mit (3.6) folgt  $\nu_p(b) = \nu_p(a) + \nu_p(c)$  für alle  $p \in \mathbb{P}$ . Wegen  $\nu_p(c) \geq 0$  gilt  $\nu_p(a) \leq \nu_p(b)$ .

b) Da (3.7) für alle  $p \in \mathbb{P}$  mit  $\nu_p(b) - \nu_p(a) \in \mathbb{N}$  äquivalent ist, gilt  $d := \prod_{p \in \mathbb{P}} p^{\nu_p(b) - \nu_p(a)} \in \mathbb{N}_1$ . Damit folgt  $b = ad$ , also  $a \mid b$ .  $\square$

Erst jetzt kann die Methode streng begründet werden, mit der meistens im Mathematikunterricht der fünften Klasse die Berechnung des *größten gemeinsamen Teilers* (ggT) und des *kleinsten gemeinsamen Vielfachen* (kgV) erfolgt. Während der größte gemeinsame Teiler auf Seite 19 erklärt wurde, findet sich die formelmäßige Definition des kleinsten gemeinsamen Vielfachen in dem nächsten Satz. Für die im Folgenden häufig auftretenden *Indexmengen* wird zur Vereinfachung die Abkürzung

$$\mathcal{I}_n := \{1, \dots, n\}$$

eingeführt.

### Satz über die ggT- und kgV-Darstellung

Für  $n \in \mathbb{N}_2$  seien  $a_1, \dots, a_n \in \mathbb{N}_1$  mit den formalen Darstellungen  $a_i = \prod_{p \in \mathbb{P}} p^{\nu_p(a_i)}$  für  $i \in \mathcal{I}_n$ . Ist  $t := \text{ggT}(a_1, \dots, a_n)$  und  $v := \text{kgV}(a_1, \dots, a_n) := \min \{e \in \mathbb{N}_1; a_i \mid e \text{ für jedes } i \in \mathcal{I}_n\}$ , so gilt

$$(3.8) \quad t = \prod_{p \in \mathbb{P}} p^{\delta_p} \text{ mit } \delta_p := \min \{\nu \in \mathbb{N}; \text{Es gibt ein } j \in \mathcal{I}_n \text{ mit } \nu = \nu_p(a_j)\}$$

und

$$(3.9) \quad v = \prod_{p \in \mathbb{P}} p^{\gamma_p} \text{ mit } \gamma_p := \max \{\nu \in \mathbb{N}; \text{Es gibt ein } k \in \mathcal{I}_n \text{ mit } \nu = \nu_p(a_k)\}.$$

**Beweis** (zwei Teile, direkt, r1):

a) Aus  $t \mid a_i$  für jedes  $i \in \mathcal{I}_n$  folgt aufgrund des *Teilbarkeitssatzes* (Seite 53), dass

$$(3.10) \quad \nu_p(t) \leq \nu_p(a_i) \text{ für jedes } i \in \mathcal{I}_n \text{ und alle } p \in \mathbb{P}$$

gilt. Die Minimalität von  $\delta_p$  ergibt

$$(3.11) \quad \delta_p \leq \nu_p(a_i) \text{ für jedes } i \in \mathcal{I}_n \text{ und alle } p \in \mathbb{P},$$

und es existiert ein  $j \in \mathcal{I}_n$  mit  $\delta_p = \nu_p(a_j)$ . Aus (3.10) folgt also  $\nu_p(t) \leq \delta_p$ .

Wegen der Maximalität von  $t$  gibt es zu jedem  $p \in \mathbb{P}$  ein  $l \in \mathcal{I}_n$ , sodass  $\nu_p(t) = \nu_p(a_l)$  erfüllt ist. Mit (3.11) erhält man dann  $\delta_p \leq \nu_p(t)$  und zusammengefasst  $\delta_p = \nu_p(t)$ .

b) Entsprechend folgt  $\nu_p(a_i) \leq \nu_p(v)$  aus  $a_i | v$  für jedes  $i \in \mathcal{I}_n$ , und die Maximalität von  $\gamma_p$  ergibt  $\nu_p(a_i) \leq \gamma_p$ . Als Brücke für  $\gamma_p \leq \nu_p(v)$  dient ein  $k \in \mathcal{I}_n$  mit  $\nu_p(a_k) = \gamma_p$ . Die Minimalität von  $v$  sichert dann die Existenz eines  $m \in \mathcal{I}_n$  mit  $\nu_p(v) = \nu_p(a_m)$ , sodass schließlich  $\nu_p(v) \leq \gamma_p$  und mit der vorhergehenden Ungleichung  $\nu_p(v) = \gamma_p$  folgt. □

Der nächste Satz bringt eine typische Anwendung der *Primpotenzdarstellung*:

### Satz über die Teileranzahlfunktion

Hat  $a \in \mathbb{N}_2$  die Primpotenzdarstellung  $a = \prod_{k=1}^r q_k^{e_k}$ , so gilt

$$(3.12) \quad d(a) = \prod_{k=1}^r (e_k + 1).$$

**Beweis** (vollständige Induktion, r1):

Die Induktionsmenge sei

$$\mathcal{M} := \left\{ s \in \mathbb{N}_1 ; \text{Für } a = \prod_{k=1}^s q_k^{e_k} \text{ gilt } d(a) = \prod_{k=1}^s (e_k + 1) \right\}.$$

Der *Teilbarkeitssatz* (Seite 53) ergibt, dass eine Primzahlpotenz  $q^e$  genau die  $e + 1$  Teiler  $1, q, \dots, q^e$  besitzt. Für  $q = q_1$  und  $e = e_1$  erhalten wir damit den Induktionsanfang  $1 \in \mathcal{M}$ .

Für  $m \in \mathcal{M}$  setzen wir  $b := \prod_{k=1}^m q_k^{e_k}$  und  $c := q_{m+1}^{e_{m+1}}$ . Die Induktionsannahme

liefert  $d(b) = \prod_{k=1}^m (e_k + 1)$ . Aufgrund des vorweg behandelten Falles mit  $q = q_{m+1}$

und  $e = e_{m+1} + 1$  ist  $d(c) = e_{m+1}$ . Aus der Darstellung aller Teiler von  $b, c$  und  $bc$  mit Hilfe des *Teilbarkeitssatzes* folgt, dass die Menge der Teiler von  $bc$  genau aus den Produkten aller Teiler von  $b$  mit den Teilern von  $c$  besteht. Also gilt

$$d(a) = d(bc) = d(b)d(c).$$

Damit ist  $m + 1 \in \mathcal{M}$ , und der *Induktionssatz* ergibt  $\mathcal{M} = \mathbb{N}_1$ . □

Der folgende Satz, der diesen Abschnitt beschließt, enthält das auf Seite 37 angekündigte Rationalitätskriterium für  $k$ -te Wurzeln. Wichtiger ist jedoch wieder

der Beweis, der die *Exponentenvergleichsstrategie* einführt, die bei einigen zahlentheoretischen Problemen wirksam eingesetzt werden kann.

### Satz über rationale $k$ -teWurzeln

Ist  $k \in \mathbb{N}_2$  und  $w \in \mathbb{Q}^+$ , so stellt  $\sqrt[k]{w}$  genau dann eine rationale Zahl dar, wenn es ein  $v \in \mathbb{Q}^+$  mit  $w = v^k$  gibt.

**Beweis** (zwei Teile, direkt, Fallunterscheidung, r1):

a) Aus  $w = v^k$  folgt definitionsgemäß  $\sqrt[k]{w} = v \in \mathbb{Q}^+$ .

b) Sind  $a, b, c, d \in \mathbb{N}_1$  mit  $\text{ggT}(a, b) = 1$ ,  $\text{ggT}(c, d) = 1$ ,  $w = \frac{a}{b}$  und  $\sqrt[k]{w} = \frac{c}{d}$ , so ist  $\sqrt[k]{\frac{a}{b}} = \frac{c}{d}$  äquivalent mit

$$(3.13) \quad a d^k = b c^k.$$

Werden für  $a, b, c, d$  die *formalen Darstellungen* eingesetzt, so ergeben (3.6) und die *Eindeutigkeitsaussage* des *Hauptsatzes* (Seite 49), dass (3.13) genau dann gilt, wenn

$$(3.14) \quad \nu_p(a) + k \nu_p(d) = \nu_p(b) + k \nu_p(c) \text{ für alle } p \in \mathbb{P}$$

erfüllt ist. Aus der Teilerfremdheit von  $a$  und  $b$  folgt, dass für jedes  $p \in \mathbb{P}$  höchstens eine der beiden Zahlen  $\nu_p(a)$  und  $\nu_p(b)$  nicht verschwindet. Im Falle  $\nu_p(a) > 0$  beziehungsweise  $\nu_p(b) > 0$  ergibt dann (3.14), dass  $\frac{1}{k} \nu_p(a) = \nu_p(c) - \nu_p(d)$  beziehungsweise  $\frac{1}{k} \nu_p(b) = \nu_p(d) - \nu_p(c)$  in  $\mathbb{N}_1$  liegt. Mit den *formalen Darstellungen*

$e := \prod_{p \in \mathbb{P}} p^{\frac{1}{k} \nu_p(a)}$  und  $f := \prod_{p \in \mathbb{P}} p^{\frac{1}{k} \nu_p(b)}$  ist also  $v := \frac{e}{f}$  eine positive rationale Zahl,

für die  $v^k = w$  gilt. □

## 3.4 Vollkommene Zahlen und spezielle Primzahlen

### Bezeichnung der Teilersummenfunktion

Die Abbildung  $\sigma : \mathbb{N}_1 \rightarrow \mathbb{N}_1$ ,  $n \mapsto \sigma(n)$  mit  $\sigma(n) := \sum_{d|n} d$  für alle  $n \in \mathbb{N}_1$  heißt

*Teilersummenfunktion*.

**Satz über die Teilersummenfunktion**

Hat  $n \in \mathbb{N}_2$  die Primpotenzdarstellung  $n = \prod_{k=1}^r q_k^{e_k}$ , so gilt

$$(3.15) \quad \sigma(n) = \prod_{k=1}^r \frac{q_k^{e_k+1} - 1}{q_k - 1}.$$

**Beweis** (Vollständige Induktion, r1):

Wegen  $\sigma(q^e) = 1 + q + \dots + q^e = \frac{q^{e+1} - 1}{q - 1}$  für alle  $q \in \mathbb{P}$  und jedes  $e \in \mathbb{N}_1$  liegt 1 in der Induktionsmenge  $\mathcal{M} := \{r \in \mathbb{N}_1; (3.15) \text{ ist richtig für alle } n \text{ mit } \omega(n) = r\}$ . Ist  $m \in \mathcal{M}$ ,  $n \in \mathbb{N}_2$  mit  $\omega(n) = m$  und  $q_{m+1} \nmid n$ , so erhält man alle Teiler von  $n q_{m+1}^{e_{m+1}}$ , indem man alle Teiler von  $n$  mit jedem Teiler von  $q_{m+1}^{e_{m+1}}$  multipliziert. Also ist

$$\sigma(n q_{m+1}^{e_{m+1}}) = \sigma(n) \sum_{k=0}^{e_{m+1}} q_{m+1}^k = \sigma(n) \frac{q_{m+1}^{e_{m+1}+1} - 1}{q_{m+1} - 1},$$

d. h. es gilt  $m + 1 \in \mathcal{M}$ , und der *Induktionssatz* (Seite 12) ergibt  $\mathcal{M} = \mathbb{N}_1$ .  $\square$

Dieser Satz ermöglicht einen Beweis der auf Seite 15 erwähnten Ergebnisse von EUKLID und EULER über vollkommene Zahlen, die heute mit Hilfe der Teilersummenfunktion definiert werden.

**Definition der vollkommenen Zahlen**

Eine Zahl  $n \in \mathbb{N}_1$  heißt *vollkommen*, wenn  $\sigma(n) = 2n$  ist.

**Beispiele**

Wegen  $\sigma(6) = 12$ ,  $\sigma(28) = 56$  und  $\sigma(496) = 992$  sind 6, 28 und 496 vollkommene Zahlen. Unterhalb von 8127 gibt es keine weiteren.

**Satz über gerade vollkommene Zahlen**

Ist  $n \in \mathbb{N}_2$  mit  $2|n$ , so stellt  $n$  genau dann eine vollkommene Zahl dar, wenn es ein  $m \in \mathbb{N}_2$  mit  $2^m - 1 \in \mathbb{P}$  gibt, sodass

$$(3.16) \quad n = 2^{m-1} (2^m - 1)$$

gilt.

**Beweis** (zwei Teile, direkt):

i) (r1, EUKLID):

Mit  $q := 2^m - 1 \in \mathbb{P}$  ergibt (3.15), dass

$$\sigma(n) = \frac{2^m - 1}{2 - 1} \frac{q^2 - 1}{q - 1} = (2^m - 1)(q + 1) = (2^m - 1)2^m = 2n$$

gilt.

ii) (a1, EULER):

Da  $n$  eine gerade vollkommene Zahl sein soll und da  $\sigma(2^{m-1}) = 2^m - 1 < 2^m$  für  $m \in \mathbb{N}_2$  gilt, gibt es  $(m, b) \in \mathbb{N}_2 \times \mathbb{N}_3$  mit  $2 \nmid b$ , sodass  $2n = 2^m b = \sigma(2^{m-1}b)$  erfüllt ist. Aus (3.15) folgt  $\sigma(2^{m-1}b) = \sigma(2^{m-1})\sigma(b) = (2^m - 1)\sigma(b)$ . Damit erhält man

$$\frac{\sigma(b)}{b} = \frac{2^m}{2^m - 1},$$

wobei die rechte Seite einen Kernbruch darstellt, sodass die *Kernbruchstrategie* angewendet werden kann. Aufgrund des *Erweiterungssatzes* (Seite 36) existiert also ein  $c \in \mathbb{N}_1$ , mit dem

$$(3.17) \quad \sigma(b) = 2^m c \quad \text{und} \quad b = (2^m - 1)c$$

gilt. EULER zeigte nun mit Hilfe eines etwas längeren indirekten Schlusses, dass  $c = 1$  und damit  $\sigma(b) = b + 1$  - also  $b \in \mathbb{P}$  - folgt.

Wir wollen hier die Gelegenheit nutzen, eine weitere wichtige Methode einzuführen, indem wir mit Hilfe der *Rückwärtsstrategie* herauszufinden versuchen, wie sich die Primzahleigenschaft von  $b$  direkt gewinnen lässt. Offenbar ist der von EULER verwendete Schluss, dass  $b \in \mathbb{P}$  aus  $\sigma(b) = b + 1$  folgt, ein mit  $d(b) = 2$  äquivalentes  $\sigma$ -Primzahlkriterium. Wir steuern also als nächsten Vorwärtsschritt die Herleitung der Gleichung  $\sigma(b) = b + 1$  an. Wegen (3.17) und mit  $2^m - 1 \in \mathbb{N}_3$  gilt

$$(3.18) \quad \sigma(b) = b + c, \quad c \mid b \quad \text{und} \quad c < b,$$

d. h. es muss  $c = 1$  sein, weil  $\sigma(b)$  die Summe aller Teiler von  $b$  ist. Aus (3.17) folgt damit  $b = 2^m - 1$ , und das  $\sigma$ -Primzahlkriterium ergibt, dass  $b \in \mathbb{P}$  ist.  $\square$

Die gleichzeitige oder abwechselnde Verwendung des Vorwärtsschließens und der Rückwärtsstrategie erinnert an den Bau einer Brücke von zwei gegenüberliegenden Ufern aus. Deshalb nennen wir diese Methode im Anschluss an G. PÓLYA [19]

*Brückenstrategie.* Auf Seite 16 des zweiten Bandes schreibt PÓLYA: «Die Lösung einer Aufgabe entdecken heißt, eine Verbindung zwischen vorher getrennten Dingen oder Ideen finden (zwischen den Dingen, die wir haben, und den Dingen, die wir suchen, den Daten und der Unbekannten, der Voraussetzung und der Behauptung). Je weiter die in Verbindung gebrachten Dinge ursprünglich auseinander lagen, um so größer ist das Verdienst, eine solche Verbindung zu entdecken. Wir sehen diese Verbindung manchmal in Gestalt einer *Brücke*: Eine große Entdeckung erscheint uns wie das Überbrücken einer tiefen Kluft zwischen zwei weit auseinander liegenden Ideen.»

Bevor wir auf die Primzahlen der Form  $2^m - 1$  näher eingehen, geben wir den aktuellen Stand des auf Seite 15 erwähnten Problems der Existenz ungerader vollkommener Zahlen wieder. Gibt es eine solche Zahl  $n$ , so hat sie mindestens 300 Dezimalziffern, und es gilt  $\Omega(n) \geq 37$  sowie  $\omega(n) \geq 8$ , wobei mindestens ein Primteiler größer als  $10^{20}$  ist.

### Satz über Primzahlen der Form $2^m - 1$

Ist  $2^m - 1 \in \mathbb{P}$ , so gilt  $m \in \mathbb{P}$ .

**Beweis** (Kontraposition<sup>2</sup>, r1):

Aus  $m = uv$  mit  $u, v \in \mathbb{N}_2$  folgt  $2^{uv} - 1 = (2^u)^v - 1^v = (2^u - 1) \sum_{k=0}^{v-1} (2^u)^k$  mit  $2^u - 1 \in \mathbb{N}_2$  und  $1 + 2^u + \dots \in \mathbb{N}_2$ , d. h.  $2^m - 1$  ist zerlegbar.  $\square$

### Bezeichnung der Mersenne-Primzahlen<sup>3</sup>

Die Zahlen  $M_p := 2^p - 1 \in \mathbb{P}$  heißen *Mersenne-Primzahlen*.

### Beispiele

$M_2 = 3$ ,  $M_3 = 7$ ,  $M_5 = 31$ ,  $M_7 = 127$ , ( $M_{11} = 2047 = 23 \cdot 89 \notin \mathbb{P}$ ).

<sup>2</sup> Der *Beweis durch Kontraposition* gehört zu den *indirekten Beweisen*. Sind A und B Aussagen, so beweist man anstelle der Aussage “Aus A folgt B” die dazu aussagenlogisch äquivalente Aussage “Aus  $\neg B$  folgt  $\neg A$ ”, wobei  $\neg A$  und  $\neg B$  die Negationen der Aussagen A und B sind.

<sup>3</sup> MARIN MERSENNE (1588-1648) war ein französischer Mönch, der sich auch mit Mathematik, Physik und Musiktheorie beschäftigte.

**Theorem über Mersenne-Primzahlen**<sup>4</sup> (von E. LUCAS 1876 entdeckt und von D. H. LEHMER 1936 allgemein bewiesen)

Die Folge  $(u_n)_n$  sei durch  $u_1 := 4$  und  $u_{n+1} := u_n^2 - 2$  für  $n \in \mathbb{N}_1$  rekursiv definiert. Ist  $p \in \mathbb{P}_3$ , so stellt  $M_p = 2^p - 1$  genau dann eine Primzahl dar, wenn  $M_p \mid u_{p-1}$  gilt.

## Primzahlrekorde

Das **Theorem über Mersenne-Primzahlen** stellt die Grundlage für den **Lucas-Lehmer-Test** für Mersenne-Primzahlen dar, der ungewöhnlich schnell ist, weil einerseits nur die Reste von  $u_k$  beim Teilen durch  $M_p$  für  $k = 1, \dots, p-1$  zu berechnen sind und weil andererseits auf Computern mit Dualzahlarithmetik die Division durch  $2^p - 1$  besonders einfach programmiert werden kann. Seit LUCAS 1876 zeigte, dass  $M_{127}$  (mit 39 Ziffern) eine Primzahl ist, waren immer Zahlen vom Mersenneschen Typ die jeweils größten bekannten Primzahlen. Bis heute (Juni 2005) wurden die folgenden 42 Exponenten von Mersenne-Primzahlen bestimmt: 1: 2, 2: 3, 3: 5, 4: 7, 5: 13, 6: 17, 7: 19, 8: 31, 9: 61, 10: 89, 11: 107, 12: 127, 13: 521, 14: 607, 15: 1279, 16: 2203, 17: 2281, 18: 3217, 19: 4253, 20: 4423, 21: 9689, 22: 9941, 23: 11213, 24: 19937, 25: 21701, 26: 23209, 27: 44497, 28: 86243, 29: 110503, 30: 132049, 31: 216091, 32: 756839, 33: 859433, 34: 1257787, 35: 1398269, 36: 2976221, 37: 3021377, 38: 6972593, 39: 13466917, 40: 20996011, 41: 24036583, 42: 25964951.

Die letzten acht dieser Exponenten von Mersenne-Primzahlen wurden im Rahmen des **GIMPS-Projekts** (**G**reat **I**nternet **M**ersenne **P**ri $\text{m}$  **S**earch) gefunden. Dabei handelt es sich um einen Internet-Zusammenschluss von mehr als 100000 privaten Computern (siehe [www.mersenne.org](http://www.mersenne.org)). In diesem Projekt werden nach und nach auch die Zahlen  $2^p - 1$  systematisch getestet, für die die Primzahl  $p$  zwischen den obigen Exponenten liegt. Auf diese Weise wurde festgestellt, dass es bis zur 38. Mersenne-Primzahl keine weiteren als die schon gefundenen gibt.

Die neueste Mersenne-Primzahl hat im Februar 2005 ein deutscher Augenarzt entdeckt, der insgesamt 24 Computer einsetzte und mehr als 50 Tage Rechenzeit für die 7816230-stellige Zahl benötigte.

## Vermutungen über vollkommene Zahlen

Es gibt unendlich viele gerade vollkommene Zahlen aber keine ungeraden.

<sup>4</sup> Als *Theoreme* bezeichnen wir in diesem Buch Sätze, deren Beweise wegen ihres Umfangs und Schwierigkeitsgrades hier nicht wiedergegeben werden können.

Durch das folgende Theorem wird eine Primzahlmenge ausgezeichnet, deren Elemente den Mersenne-Primzahlen ähneln, über die aber noch weniger bekannt ist.

**Theorem über regelmäßige Vielecke** (GAUß, 1796)

Für  $n \in \mathbb{N}_3$  kann das regelmäßige  $n$ -Eck genau dann mit Zirkel und Lineal konstruiert werden, wenn  $2^{-\nu_2(n)}n$  entweder 1, eine Primzahl der Form  $2^t + 1$  mit  $t \in \mathbb{N}_1$  oder das Produkt von verschiedenen Primzahlen dieses Typs ist.

**Satz über Primzahlen der Form  $2^t + 1$**

Ist  $2^t + 1 \in \mathbb{P}$ , so gibt es ein  $k \in \mathbb{N}$  mit  $t = 2^k$ .

**Beweis** (Kontraposition, r1):

Aus  $t = 2^k d$  mit  $d \in \mathbb{N}_3$  und  $2 \nmid d$  folgt mit  $x := 2^{2^k}$  die Gleichungskette

$$\begin{aligned} 2^t + 1 &= 2^{2^k d} + 1 = \left(2^{2^k}\right)^d + 1 \\ &= x^d + 1 = x^d - (-1)^d \\ &= (x - (-1)) \left(x^{d-1} (-1)^0 + x^{d-2} (-1)^1 + \dots + x^0 (-1)^{d-1}\right). \end{aligned}$$

Einerseits gilt  $x + 1 \geq 3$ , und andererseits ergibt sich aus  $x + 1 < x^d + 1$ , dass  $x^{d-1} (-1)^0 + \dots + x^0 (-1)^{d-1} \in \mathbb{N}_2$  ist. Damit kann  $2^t + 1$  keine Primzahl sein.  $\square$

**Bezeichnung der Fermat-Primzahlen**

Die Zahlen  $F_n := 2^{2^n} + 1 \in \mathbb{P}$  heißen *Fermat-Primzahlen*.

Die bisher bekannten Fermat-Primzahlen sind

$$F_0 = 3, F_1 = 5, F_2 = 17, F_3 = 257, F_4 = 65537.$$

EULER fand den Faktor 641 von  $F_5$ .  $F_9$  wurde 1990 “faktorisiert”, d. h. es wurden alle Primfaktoren berechnet.  $F_{20}$  mit ungefähr 380000 Stellen war bis 1995 ungeklärt. Inzwischen ist bekannt, dass  $F_{20}$  keine Primzahl darstellt. Fermat-Primzahlen können mit Hilfe des folgenden Tests gefunden werden, der allerdings wegen des raschen Wachsens der Exponenten in absehbarer Zeit keine neuen Ergebnisse mehr liefern kann.

### Theorem über Fermat-Primzahlen

Für  $n \in \mathbb{N}_1$  stellt  $F_n$  genau dann eine Primzahl dar, wenn  $F_n$  Teiler von  $3^{\frac{F_n-1}{2}} + 1$  ist.

### Vermutung über Fermat-Primzahlen

Es gibt nur die obigen fünf Fermat-Primzahlen.

## 3.5 Verteilung der Primzahlen

Die Folge der Primzahlen hat beliebig lange Lücken, weil für jedes  $m \in \mathbb{N}_2$  alle Zahlen der Menge  $\{n \in \mathbb{N}_3 ; \text{Es gibt ein } i \in \mathcal{I}_{m-1} \text{ mit } n = m! + i + 1\}$  keine Primzahlen sind. Bei einigen zahlentheoretischen Problemen haben die Zahlen aus  $\mathbb{N}_2$ , die nicht zu den Primzahlen gehören, einen eigenen Namen, der aber erst bei Verallgemeinerungen in der Algebra eine größere Bedeutung gewinnt.

### Bezeichnung der zerlegbaren Zahlen

Die Zahlen aus  $\mathbb{N}_2 \setminus \mathbb{P}$  heißen *zerlegbar*.

In der entgegengesetzten Richtung sprechen numerische Befunde dafür, dass die Frage von Seite 15 bezüglich der Unendlichkeit der Menge  $\{p \in \mathbb{P} ; p + 2 \in \mathbb{P}\}$  positiv zu beantworten ist.

Auf der Suche nach Regelmäßigkeiten der Primzahlfolge stellte GAUß 1792 als 16-Jähriger die unveröffentlichte Vermutung auf, dass die Anzahl der Primzahlen unterhalb einer positiven Schranke  $x$  "asymptotisch" so groß ist wie  $\frac{x}{\ln x}$ . Wegen ihrer Bedeutung hat diese Anzahlfunktion ein eigenes Symbol:

### Bezeichnung der Primzahlfunktion

Die Abbildung  $\pi : \mathbb{R}^+ \rightarrow \mathbb{N}$ ,  $x \mapsto \text{card} \{p \in \mathbb{P} ; p \leq x\}$  heißt *Primzahlfunktion*.

Unabhängig von GAUß wurde diese Vermutung von A. M. LEGENDRE gefunden und 1798 publiziert. In der Schreibweise der Analysis hat die Vermutung die Form

$$(3.19) \quad \lim_{x \rightarrow \infty} \frac{\pi(x) \ln x}{x} = 1.$$

### Beispiele

$$\pi(10^2) = 25, \quad \pi(10^4) = 1229, \quad \pi(10^6) = 78498, \quad \pi(10^8) = 5761455, \quad \pi(10^{10}) = 455052512.$$

Es dauerte fast einhundert Jahre, bis die Aussage (3.19) 1896 bewiesen wurde. Wir können hier nur einige elementare Sätze herleiten. Im nächsten Abschnitt geben wir einen Ausblick auf die zur analytischen Zahlentheorie gehörende Entwicklung der Primzahltheorie.

### Satz über ein Primzahlkriterium

Eine Zahl  $n \in \mathbb{N}_2$  ist genau dann eine Primzahl, wenn  $kP(n) > \sqrt{n}$  gilt.

**Beweis** (zwei Teile: erster Teil direkt, zweiter mit Kontraposition, r1):

- i) Stellt  $n$  eine Primzahl dar, so gilt  $kP(n) = n$ , und aus  $n > 1$  folgt  $n > \sqrt{n}$ .
- ii) Ist  $n \in \mathbb{N}_2 \setminus \mathbb{P}$  und  $q := kP(n)$ , so gibt es ein  $f \in \mathbb{N}_2$  mit  $n = fq$  und  $q \leq kP(f) \leq f$ . Damit gilt  $q^2 \leq n$ , also  $q \leq \sqrt{n}$ . □

Mit Hilfe dieses Primzahlkriteriums lassen sich Primzahlen “aussieben” und abzählen. Sind nämlich die Primzahlen  $p$  mit  $p \leq \sqrt{n}$  für  $n \in \mathbb{N}_4$  bekannt und werden alle Vielfachen dieser Primzahlen in  $\mathcal{I}_n$  gestrichen, so bleiben genau die Primzahlen  $q$  mit  $\sqrt{n} < q \leq n$  und die Zahl 1 übrig. Dieses Verfahren stammt von dem griechischen Mathematiker ERATOSTHENES (276? - 194? v. Chr.). Es wird deshalb *Sieb des Eratosthenes* genannt. Das nächste Beispiel bereitet den zugehörigen Satz über die Anzahl

$$(3.20) \quad A(n) := 1 + \text{card} \{m \in \mathbb{N}_2 ; m \leq n \text{ und } kP(m) > \sqrt{n}\}$$

der verbleibenden Zahlen für  $n \in \mathbb{N}_4$  vor.

### Beispiel

Für  $n = 40$  ist  $[\sqrt{n}] = 6$  und  $\mathbb{P} \cap \mathcal{I}_6 = \{2, 3, 5\}$ . Die folgende Abbildung 3.1 gibt den Siebvorgang durch verschieden geneigte Striche wieder.

|               |                 |                 |               |                 |               |               |               |               |               |
|---------------|-----------------|-----------------|---------------|-----------------|---------------|---------------|---------------|---------------|---------------|
| $\diamond 1$  | $\circledast 2$ | $\circledast 3$ | <del>4</del>  | $\circledast 5$ | <del>6</del>  | $\square 7$   | <del>8</del>  | <del>9</del>  | <del>10</del> |
| $\square 11$  | <del>12</del>   | $\square 13$    | <del>14</del> | <del>15</del>   | <del>16</del> | $\square 17$  | <del>18</del> | $\square 19$  | <del>20</del> |
| <del>21</del> | <del>22</del>   | $\square 23$    | <del>24</del> | <del>25</del>   | <del>26</del> | <del>27</del> | <del>28</del> | $\square 29$  | <del>30</del> |
| $\square 31$  | <del>32</del>   | <del>33</del>   | <del>34</del> | <del>35</del>   | <del>36</del> | $\square 37$  | <del>38</del> | <del>39</del> | <del>40</del> |

$\swarrow$  : Teiler 2,       $\searrow$  : Teiler 3,       $-$  : Teiler 5

Abbildung 3.1: Sieb des Eratosthenes

Aus dem Siebschema entnehmen wir  $\pi(40) - \pi(\sqrt{40}) = 9$ , sodass  $A(40) = 1 + 9 = 10$  ist.

Zählen wir die Vielfachen der Primzahlen 2, 3, 5 und beachten die Mehrfachstreichungen, so erhalten wir eine zweite Darstellung für  $A(40)$ , in der die Primzahlfunktion nicht vorkommt.

Von 40 werden zuerst  $\left[\frac{40}{2}\right]$  Vielfache von 2 gestrichen, dann  $\left[\frac{40}{3}\right]$  Vielfache von 3 und  $\left[\frac{40}{5}\right]$  Vielfache von 5. Dabei sind alle Vielfachen von  $2 \cdot 3$ ,  $2 \cdot 5$  und  $3 \cdot 5$  doppelt weggestrichen. Ihre Anzahlen werden also wieder addiert. Die Anzahl der Vielfachen von  $2 \cdot 3 \cdot 5$  ist schließlich einmal zuviel gerechnet und wird deshalb wieder subtrahiert.

Damit ergibt sich

$$\begin{aligned}
 A(40) &= 40 - \left[\frac{40}{2}\right] - \left[\frac{40}{3}\right] - \left[\frac{40}{5}\right] + \left[\frac{40}{2 \cdot 3}\right] + \left[\frac{40}{2 \cdot 5}\right] + \left[\frac{40}{3 \cdot 5}\right] - \left[\frac{40}{2 \cdot 3 \cdot 5}\right] \\
 &= 40 - 20 - 13 - 8 + 6 + 4 + 2 - 1 = 10.
 \end{aligned}$$

Die Vorzeichen der Gauß-Klammern hängen offenbar von der Anzahl der Primfaktoren in den Nennerprodukten ab. In der allgemeinen Aussage wird dieser Zusammenhang durch die folgende zahlentheoretische Funktion erfasst.

### Bezeichnung der Möbius-Funktion<sup>5</sup>

Die zahlentheoretische Funktion  $\mu : \mathbb{N}_1 \rightarrow \{-1, 0, 1\}$  mit

$$(3.21) \quad \mu(n) := \begin{cases} (-1)^{\omega(n)}, & \text{wenn } \omega(n) = \Omega(n) \text{ ist,} \\ 0 & \text{sonst,} \end{cases}$$

heißt *Möbius-Funktion* oder  $\mu$ -*Funktion*.

<sup>5</sup> AUGUST FERDINAND MÖBIUS (1790-1868) war Mathematiker und Physiker in Leipzig.

Die ersten Werte der Möbius-Funktion sind

$$\mu(1) = 1, \mu(2) = -1, \mu(3) = -1, \mu(4) = 0, \mu(5) = -1, \mu(6) = 1, \mu(7) = -1, \\ \mu(8) = 0, \mu(9) = 0, \mu(10) = 1, \mu(11) = -1, \mu(12) = 0.$$

Die Zahlen, für die die Möbius-Funktion von 0 verschieden ist, spielen in vielen Teilen der Zahlentheorie eine Rolle. Sie haben deshalb ein eigenes Adjektiv. Die Übereinstimmung der Bedingung in der folgenden Definition mit derjenigen des ersten Falles der Möbius-Funktion lässt sich als einfache Übungsaufgabe zeigen.

### Definition der quadratfreien Zahlen

Eine Zahl  $n \in \mathbb{N}_1$  heißt *quadratfrei*, wenn  $\nu_p(n) \leq 1$  für alle  $p \in \mathbb{P}$  erfüllt ist.

### Satz über die Möbius-Summe

Ist  $n \in \mathbb{N}_1$ , so gilt

$$(3.22) \quad \sum_{d|n} \mu(d) = \begin{cases} 1 & \text{für } n = 1, \\ 0 & \text{sonst.} \end{cases}$$

**Beweis** (direkt, r2):

Für  $n = 1$  ist definitionsgemäß  $\mu(1) = 1$ . Im Falle  $n \in \mathbb{N}_2$  eliminieren wir alle Nullsummanden, indem wir  $n$  durch  $n' := \prod_{p|n} p$  ersetzen. Dann gilt

$$\sum_{d|n} \mu(d) = \sum_{d|n'} \mu(d),$$

weil aufgrund des *Teilbarkeitssatzes* (Seite 53) die quadratfreien Teiler von  $n$  genau die Teiler von  $n'$  sind. Mit  $r := \omega(n')$  liefert der Binomialkoeffizient<sup>6</sup>  $\binom{r}{k}$  für  $k \in \mathcal{A}_{r+1}$  die Anzahl der Teiler  $d$  mit  $k$  Primfaktoren. Die *Binomialformel*

$$(3.23) \quad (1+x)^r = \sum_{k=0}^r \binom{r}{k} x^k \text{ für alle } x \in \mathbb{R}$$

ergibt also

$$\sum_{d|n'} \mu(d) = \sum_{k=0}^r \binom{r}{k} (-1)^k = (1-1)^r = 0. \quad \square$$

<sup>6</sup> Für  $r \in \mathbb{R}$  und  $k \in \mathbb{N}_1$  werden die *Binomialkoeffizienten* durch  $\binom{r}{k} := \frac{1}{k!} \prod_{i=0}^{k-1} (r-i)$  definiert, und es wird  $\binom{r}{0} := 1$  gesetzt.

### Satz über das Eratosthenes-Sieb

Es seien  $x, y \in \mathbb{R}^+$  mit  $x \geq 4$  und  $2 \leq y \leq \sqrt{x}$ . Wird  $w := \prod_{\substack{p \in \mathbb{P} \\ p \leq y}} p$ , und

$B(x, y) := 1 + \text{card} \{m \in \mathbb{N}_2 ; m \leq x \text{ und } kP(m) > y\}$  gesetzt, so gilt

$$(3.24) \quad B(x, y) = \sum_{d|w} \mu(d) \left[ \frac{x}{d} \right].$$

Für die durch (3.20) definierte Anzahlfunktion  $A(n)$  ergibt sich mit  $n \in \mathbb{N}_4$  insbesondere

$$(3.25) \quad A(n) = B(n, \sqrt{n}) = \pi(n) - \pi(\sqrt{n}) + 1.$$

**Beweis** (zwei Teile, direkt, a2/r1)

i) Würden wir versuchen, (3.24) ausgehend von der Definition von  $B(x, y)$  zu beweisen, so wäre gleich am Anfang eine Umformung nötig, die als Trick erschiene. Wenden wir dagegen die *Rückwärtsstrategie* an, so ergibt sich der Übergang fast von selbst. Zunächst beachten wir, dass

$$\left[ \frac{x}{d} \right] = \text{card} \{m \in \mathbb{N}_1 ; m \leq x \text{ und } d|m\} = \sum_{\substack{m=1 \\ d|m}}^{[x]} 1$$

gilt. Die durch Einsetzen entstehende Doppelsumme lässt sich so umformen, dass der *Satz über die Möbius-Summe* (Seite 65) angewendet werden kann:

$$\begin{aligned} \sum_{d|w} \mu(d) \left[ \frac{x}{d} \right] &= \sum_{d|w} \mu(d) \sum_{\substack{m=1 \\ d|m}}^{[x]} 1 = \sum_{d|w} \sum_{\substack{m=1 \\ d|m}}^{[x]} \mu(d) = \sum_{m=1}^{[x]} \sum_{\substack{d|m \\ d|w}} \mu(d) \\ &= \sum_{m=1}^{[x]} \left( \sum_{d|\text{ggT}(m, w)} \mu(d) \right) = \sum_{\substack{m=1 \\ \text{ggT}(m, w)=1}}^{[x]} 1. \end{aligned}$$

Da  $w$  das Produkt der Primzahlen bis  $y$  ist, gilt die Bedingung  $\text{ggT}(m, w) = 1$  für  $m \in \mathbb{N}_2$  genau dann, wenn  $kP(m) > y$  erfüllt ist. Damit hat die letzte Summe den Wert  $B(x, y)$ .

ii) Definitionsgemäß gilt  $A(n) = B(n, \sqrt{n})$ . Aufgrund des *Satzes über ein Primzahlkriterium* (Seite 63) ist  $\pi(n) - \pi(\sqrt{n}) + 1$  die Anzahl  $A(n)$  der nicht “gestrichenen” Zahlen.  $\square$

Die Darstellung von  $A(n)$  als Spezialfall von (3.24) wird auch *Wechselwegnahmestrategie* oder *Ein- und Ausschaltformel* genannt. Mit Hilfe einer wesentlichen Verbesserung von (3.24) und (3.25) hat ein amerikanisches Team 1985  $\pi(4 \cdot 10^{16})$  exakt berechnet. Bei dem folgenden letzten Satz dieses Kapitels wird (3.24) für die obere Abschätzung verwendet.

### Satz über $\pi(x)$ -Abschätzungen

Für alle  $x \in \mathbb{R}$  mit  $x \geq 21$  gilt

$$\ln x - 1 < \pi(x) < \frac{2x}{\ln(\ln x)}.$$

**Beweis** (zwei Teile, direkt, h2):

#### i) Untere Abschätzung von $\pi(x)$ :

a) EULER (1737) verwendete den Produktansatz

$$(3.26) \quad P(x) := \prod_{\substack{p \in \mathbb{P} \\ p \leq x}} \frac{1}{1 - \frac{1}{p}},$$

um einen weiteren Beweis für die Unendlichkeit der Primzahlmenge zu führen. Wir zeigen zunächst, dass  $P(x)$  eine untere Schranke für  $\pi(x) + 1$  darstellt und schätzen anschließend  $P(x)$  nach unten durch  $\ln x$  ab.

Ist  $p_k$  für  $k \in \mathbb{N}_1$  die  $k$ -te Primzahl, so gilt  $p_1 = 2$  und  $p_{k+1} \geq p_k + 1$  für alle  $k \in \mathbb{N}_1$ . Vollständige Induktion ergibt also  $p_i \geq i + 1$  für jedes  $i \in \mathbb{N}_1$ .

Damit folgt

$$\begin{aligned} P(x) &= \prod_{i=1}^{\pi(x)} \frac{1}{1 - \frac{1}{p_i}} \\ &\leq \prod_{i=1}^{\pi(x)} \frac{1}{1 - \frac{1}{i+1}} = \prod_{i=1}^{\pi(x)} \frac{i+1}{i} \\ &= \frac{2 \cdot 3 \cdots (\pi(x) + 1)}{1 \cdot 2 \cdots \pi(x)} = \pi(x) + 1. \end{aligned}$$

#### b) Untere Abschätzung von $P(x)$ für $x \geq 2$ :

Jeder der Faktoren in (3.26) lässt sich als geometrische Reihe schreiben:

$$\frac{1}{1 - \frac{1}{p}} = \sum_{k=0}^{\infty} \frac{1}{p^k}.$$

Diese endlich vielen Reihen sind absolut konvergent. Sie können deshalb gliedweise ausmultipliziert und umgeordnet werden. Mit

$$N_x := \{m \in \mathbb{N}_1 ; \text{Für alle Primteiler } p \text{ von } m \text{ gilt } p \leq x\}$$

ergibt sich also

$$P(x) = \prod_{\substack{p \in \mathbb{P} \\ p \leq x}} \sum_{k=0}^{\infty} \frac{1}{p^k} = \sum_{n \in N_x} \frac{1}{n}.$$

Da alle  $m \in N_x$  mit  $m \leq x$  zu  $N_x$  gehören, lässt sich  $P(x)$  nach unten durch eine Summe abschätzen, für die ein Integral mit bekannter Stammfunktion als untere Schranke angegeben werden kann (siehe Abbildung 3.2):

$$\begin{aligned} P(x) &= \sum_{n \in N_x} \frac{1}{n} \geq \sum_{n=1}^{[x]} \frac{1}{n} \\ &= \sum_{n=1}^{[x]} \frac{1}{n} \int_n^{n+1} dv = \sum_{n=1}^{[x]} \int_n^{n+1} \frac{1}{n} dv \\ &\geq \sum_{n=1}^{[x]} \int_n^{n+1} \frac{1}{v} dv = \int_1^{[x]+1} \frac{1}{v} dv \\ &= \ln([x] + 1) > \ln x, \text{ also} \end{aligned}$$

$$(3.27) \quad \ln x < P(x).$$

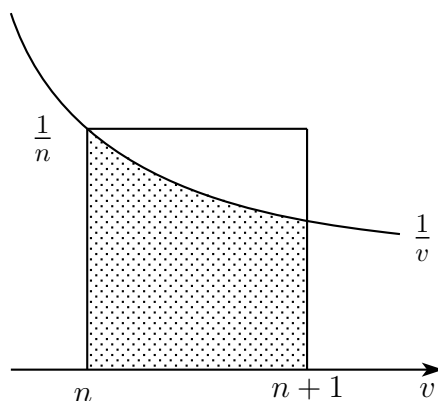


Abbildung 3.2: Untere Abschätzung von  $P(x)$

<sup>7</sup> EULER schließt hier, dass die Annahme endlich vieler Primzahlen im Widerspruch zur Divergenz der harmonischen Reihe stünde.

Durch Zusammenfassen der beiden  $P(x)$  enthaltenden Ungleichungen ergibt sich für  $\pi(x)$  die untere Abschätzung

$$\ln x - 1 < \pi(x).$$

## ii) Obere Abschätzung von $\pi(x)$

- a) Ähnlich wie  $P(x)$  bei der unteren Abschätzung spielt jetzt  $B(x, y)$  aus dem *Satz über das Eratosthenes-Sieb* (Seite 66) die Rolle eines Mittelgliedes. Dazu sei  $x \geq 4$  und  $2 \leq y \leq \sqrt{x}$ . Da natürlich alle  $p \in \mathbb{P}$  mit  $y < p \leq x$  zu  $B(x, y)$  gehören, gilt zunächst  $\pi(x) - \pi(y) \leq B(x, y)$ . In der dazu äquivalenten Ungleichung

$$\pi(x) \leq B(x, y) + \pi(y)$$

wird nun die rechte Seite nach oben abgeschätzt und dann  $y$  in Abhängigkeit von  $x$  geeignet gewählt.

In der Summe von (3.24) ersetzen wir  $\left[\frac{x}{d}\right]$  durch  $\frac{x}{d} + \Theta_{x,d}$  mit  $-1 < \Theta_{x,d} \leq 0$ . Damit folgt

$$\begin{aligned} B(x, y) &= \sum_{d|w} \mu(d) \left( \frac{x}{d} + \Theta_{x,d} \right) \\ &= x \sum_{d|w} \mu(d) \frac{1}{d} + \sum_{d|w} \mu(d) \Theta_{x,d} \\ &\leq x \sum_{d|w} \mu(d) \frac{1}{d} + \sum_{d|w} 1 \\ &= x \sum_{d|w} \mu(d) \frac{1}{d} + d(w). \end{aligned}$$

- b) Wird  $w = \prod_{\substack{p \in \mathbb{P} \\ p \leq y}} p$  in der Form  $w = \prod_{j=1}^r p_j$  mit  $r := \pi(y)$  geschrieben, so kann

schon für  $r \leq 3$  vermutet werden, dass

$$(3.28) \quad \sum_{d|w} \mu(d) \frac{1}{d} = \prod_{j=1}^r \left( 1 - \frac{1}{p_j} \right) \quad \text{für jedes } r \in \mathbb{N}_1$$

gilt. Der Beweis mit vollständiger Induktion erfolgt ähnlich wie bei dem *Satz über die Teileranzahlfunktion* (Seite 55). Besteht die Induktionsmenge  $\mathcal{M}$  aus denjenigen  $k \in \mathbb{N}_1$ , für die (3.28) erfüllt ist, so gehört 1 zu  $\mathcal{M}$ , weil

$\sum_{d|p_1} \mu(d) \frac{1}{d} = 1 - \frac{1}{p_1}$  gilt. Für  $k \in \mathcal{M}$  beruht der Induktionsschritt mit Hilfe

des *Teilbarkeitssatzes* (Seite 53) auf der expliziten Kenntnis aller Teiler:

$$\begin{aligned} \prod_{j=1}^{k+1} \left(1 - \frac{1}{p_j}\right) &= \left(\sum_{d|p_1 \cdots p_k} \mu(d) \frac{1}{d}\right) \left(1 - \frac{1}{p_{k+1}}\right) \\ &= \sum_{d|p_1 \cdots p_k} \mu(d) \frac{1}{d} + \sum_{d|p_1 \cdots p_k} (-\mu(d)) \frac{1}{d p_{k+1}} \\ &= \sum_{d|p_1 \cdots p_{k+1}} \mu(d) \frac{1}{d}. \end{aligned}$$

c) Mit (3.28) und (3.27) folgt

$$\sum_{d|w} \mu(d) \frac{1}{d} = \prod_{\substack{p \in \mathbb{P} \\ p \leq y}} \left(1 - \frac{1}{p}\right) = \frac{1}{P(y)} \leq \frac{1}{\ln y}.$$

Zusammenfassend haben wir damit

$$\pi(x) \leq \frac{x}{\ln y} + d(w) + \pi(y).$$

Aufgrund des *Satzes über die Teileranzahlfunktion* (Seite 55) ist  $d(w) = 2^{\pi(y)} \leq 2^y$ , und grob abgeschätzt gilt auch  $\pi(y) \leq y \leq 2^y$ . Wegen  $2^{\ln x} = e^{(\ln 2)(\ln x)} = x^{\ln 2}$  ist  $2 \cdot 2^y$  kleiner als  $\frac{x}{\ln y}$ , wenn  $y := \ln x$  für hinreichend großes  $x$  gewählt wird. Wir zeigen abschließend, dass dieses für  $x \geq e^3$  der Fall ist. Dazu setzen wir

$$h(x) := \frac{1}{x} 2^{\ln x} \ln(\ln x) = \frac{\ln(\ln x)}{x^{1-\ln 2}}.$$

Dann gilt  $h(e^3) = \frac{\ln 3}{e^{3(1-\ln 2)}} = 0,43\dots < \frac{1}{2}$  und

$$h'(x) = \left(\frac{1}{\ln x} - (1 - \ln 2) \ln(\ln x)\right) \frac{1}{x^{2-\ln 2}} < 0 \quad \text{für } x \geq e^3,$$

weil  $x \mapsto \frac{1}{\ln x}$  monoton fallend,  $x \mapsto (1 - \ln 2) \ln(\ln x)$  monoton steigend und  $\frac{1}{3} - (1 - \ln 2) \ln 3 = -0,003\dots$  negativ ist. Also stellt  $x \mapsto h(x)$  für  $x \geq e^3$  eine monoton fallende Funktion dar. Damit gilt  $\pi(x) < \frac{2x}{\ln(\ln x)}$  für  $x \geq 21 > e^3$ .  $\square$

## 3.6 Ausblick auf bedeutende Resultate der analytischen Primzahltheorie

### i) Primzahlen in arithmetischen Folgen

Neben den beiden Folgen  $(2^n - 1)_n$  und  $(2^n + 1)_n$  aus Abschnitt 3.4 haben vor allem die “arithmetischen Folgen”  $(kn + l)_n$  mit  $(k, l) \in \mathbb{N}_3 \times \mathbb{Z}$  und  $\text{ggT}(k, l) = 1$  das Interesse der Zahlentheoretiker geweckt. Während  $kn + l$  im Falle  $\text{ggT}(k, l) > 1$  aufgrund des *Satzes über Teilbarkeitsregeln* (Seite 18) für alle  $n \in \mathbb{N}_2$  zerlegbar ist, konnte G. DIRICHLET<sup>8</sup> in einer bedeutenden Arbeit die folgende Aussage beweisen:

**Theorem über Primzahlen in arithmetischen Folgen** (G. DIRICHLET, 1837)

Sind  $(k, l) \in \mathbb{N}_3 \times \mathbb{Z}$  mit  $\text{ggT}(k, l) = 1$ , so enthält die Folge  $(kn + l)_n$  unendlich viele Primzahlen.

Zum Beweis führte DIRICHLET zwei neue Begriffe ein, die später nach ihm benannt wurden, nämlich Dirichlet-Reihen und Dirichlet-Charaktere. Ist  $(a_n)_n$  eine Folge von reellen oder komplexen Zahlen, so heißt die Funktionenreihe  $\sum_{n=1}^{\infty} \frac{a_n}{n^s}$  mit der reellen (und später auch komplexen) Variablen  $s$  *Dirichlet-Reihe* mit der Koeffizientenfolge  $(a_n)_n$ . Die wichtigste Dirichlet-Reihe ist  $\sum_{n=1}^{\infty} \frac{1}{n^s}$ . Ihre Bedeutung beruht auf der Produktdarstellung

$$(3.29) \quad \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_{p \in \mathbb{P}} \left(1 - \frac{1}{p^s}\right)^{-1},$$

die von EULER für alle  $s \in \mathbb{R}$  mit  $s > 1$  bewiesen wurde. Einen Spezialfall seiner Methode haben wir bei dem Beweis der unteren Abschätzung von  $\pi(x)$  auf Seite 68 verwendet. Mit der dort definierten Menge  $N_x$  gilt

$$\prod_{\substack{p \in \mathbb{P} \\ p \leq x}} \left(1 - \frac{1}{p^s}\right)^{-1} = \sum_{n \in N_x} \frac{1}{n^s} \quad \text{für jedes } x \in \mathbb{R}^+.$$

Durch den Übergang  $x \rightarrow \infty$  und mit dem *Hauptsatz* (Seite 49) ergibt sich (3.29).

<sup>8</sup> PETER GUSTAV (LEJEUNE-) DIRICHLET (1805-1859) wirkte in Breslau, Berlin und Göttingen.

*Dirichlet-Charaktere* sind Abbildungen  $\chi : \mathbb{N}_1 \rightarrow \mathbb{C}$ . Sie haben in Abhängigkeit von der festen Zahl  $k \in \mathbb{N}_3$  die folgenden Eigenschaften:

$$\chi(1) := 1, \quad \chi(n) := 0, \quad \text{wenn } \text{ggT}(k, n) > 1 \text{ ist,}$$

$$\chi(ab) = \chi(a)\chi(b) \quad \text{für alle } a, b \in \mathbb{N}_1 \text{ und}$$

$$\chi(a) = \chi(b), \quad \text{wenn } k|(a-b) \text{ gilt.}$$

Sie werden gebraucht, um in  $\mathbb{N}_1$  die Zahlen der Form  $kn + l$  auszusieben.

Jedem Dirichlet-Charakter wird eine Dirichlet-Reihe  $L(s, \chi) := \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}$  zugeordnet. Diese sogenannten *L-Reihen* konvergieren für alle  $s \in \mathbb{R}^+$ , wenn es ein  $n \in \mathbb{N}_1$  mit  $\chi(n) \notin \{0, 1\}$  gibt. Als entscheidenden Zwischenschritt für den Beweis des obigen Theorems konnte DIRICHLET zeigen, dass  $L(1, \chi) \neq 0$  für alle Dirichlet-Charaktere gilt.

## ii) Approximation von $\pi(x)$

Über die auf Seite 62 erwähnte Hypothese hinausgehend stellte GAUß 1793 die Vermutung auf, dass der für  $x > 1$  definierte *Integrallogarithmus*

$$\text{li}(x) := \lim_{\varepsilon \rightarrow 0} \left( \int_0^{1-\varepsilon} \frac{1}{\ln t} dt + \int_{1+\varepsilon}^x \frac{1}{\ln t} dt \right) = \int_2^x \frac{1}{\ln t} dt + 1,04\dots$$

die Primzahlfunktion  $\pi(x)$  “mit einem viel kleineren Rest” approximiert als  $\frac{x}{\ln x}$ . Eine erste Bestätigung lieferte P. L. TSCHEBYSCHEFF<sup>9</sup>:

**Theorem über  $\pi(x)$ -Approximation durch  $\text{li}(x)$**  (P. L. TSCHEBYSCHEFF, 1851)

Für jedes  $A > 0$  gilt

$$\limsup_{x \rightarrow \infty} (\pi(x) - \text{li}(x)) \frac{(\ln x)^A}{x} \geq 0 \quad \text{und} \quad \liminf_{x \rightarrow \infty} (\pi(x) - \text{li}(x)) \frac{(\ln x)^A}{x} \leq 0.$$

Insbesondere ist  $\lim_{x \rightarrow \infty} \frac{\pi(x)}{\text{li}(x)} = 1$ , wenn der Limes existiert.

Da mit partieller Integration  $\lim_{x \rightarrow \infty} \frac{\text{li}(x) \ln x}{x} = 1$  gezeigt werden kann, folgt auch

$$\lim_{x \rightarrow \infty} \frac{\pi(x) \ln x}{x} = 1, \quad \text{wenn der Grenzwert vorhanden ist.}$$

<sup>9</sup> PAFNUTI LWOWITSCH TSCHEBYSCHEFF (1821-1894) wirkte in Moskau und St. Petersburg.

Das für längere Zeit beste Ergebnis in Richtung auf die Limesexistenz erzielte TSCHEBYSCHJEFF durch sorgfältige Analyse von zahlentheoretischen Eigenschaften der Binomialkoeffizienten:

**Theorem über die Quotientenschachtelung** (P. L. TSCHEBYSCHJEFF, 1852)

Es gibt ein  $x_0 \in \mathbb{R}^+$ , sodass

$$0,92129\dots < \frac{\pi(x) \ln x}{x} < 1,0555\dots \quad \text{für alle } x \in \mathbb{R} \text{ mit } x \geq x_0$$

erfüllt ist.

### iii) Die Wende zur Funktionentheorie

Im Unterschied zu seinen Vorgängern untersuchte B. RIEMANN<sup>10</sup> die Reihe in der von EULER entdeckten Beziehung (3.29) als Funktion auf den *komplexen Zahlen*

$$\zeta : \mathbb{C} \rightarrow \mathbb{C}, \quad s \mapsto \sum_{n=1}^{\infty} \frac{1}{n^s}.$$

Sie wurde deshalb später *Riemannsche Zetafunktion* genannt. Zunächst ist  $\zeta(s)$  für  $\operatorname{Re} s > 1$  definiert, weil die Reihe dort konvergiert. Mit Methoden der “analytischen Fortsetzung” aus der Funktionentheorie konnte RIEMANN  $\zeta(s)$  für alle  $s \in \mathbb{C} \setminus \{1\}$  konsistent erklären. Er zeigte dann, dass die Funktionen  $s \mapsto (s-1)\zeta(s)$  und  $s \mapsto \zeta(s) - \frac{1}{1-s}$  auf  $\mathbb{C}$  komplex differenzierbar sind und bewies die folgende merkwürdige Symmetrieaussage, wobei die  $\Gamma$ -Funktion durch

$$\Gamma(s) := \int_0^{\infty} t^{s-1} e^{-t} dt \quad \text{für alle } s \in \mathbb{C} \text{ mit } \operatorname{Re} s > 0$$

definiert und auf  $\mathbb{C} \setminus \{-n; n \in \mathbb{N}\}$  analytisch fortgesetzt wird:

**Theorem über die Riemannsche Funktionalgleichung** (B. RIEMANN, 1859)

Die Funktion

$$\xi : \mathbb{C} \rightarrow \mathbb{C}, \quad s \mapsto \frac{1}{2}s(s-1)\pi^{-\frac{1}{2}s}\Gamma\left(\frac{1}{2}s\right)\zeta(s)$$

ist überall komplex differenzierbar, und es gilt

$$\xi(1-s) = \xi(s) \quad \text{für alle } s \in \mathbb{C}.$$

<sup>10</sup> BERNHARD RIEMANN (1826-1866) wirkte in Göttingen.

In der wegweisenden Arbeit von RIEMANN standen außerdem sechs Vermutungen, von denen eine bis heute unbewiesen ist. Da  $\Gamma(s)$  an den Stellen  $s = -n$  mit  $n \in \mathbb{N}$  Pole hat, kann aus der komplexen Differenzierbarkeit von  $\xi(s)$  entnommen werden, dass  $\zeta(s)$  für jedes  $s \in \{-2n; n \in \mathbb{N}_1\}$  eine Nullstelle besitzt. Diese reellen Nullstellen heißen “triviale Nullstellen” der Riemannschen Zetafunktion, die übrigen Nullstellen werden “nicht trivial” genannt.

### Riemannsche Vermutung

Für alle nicht trivialen Nullstellen  $s$  der Riemannschen Zetafunktion gilt  $\operatorname{Re} s = \frac{1}{2}$ .

Es ist bekannt, dass  $0 < \operatorname{Re} s < 1$  für alle nicht trivialen Nullstellen  $s$  gilt, dass es unendlich viele Nullstellen auf der “kritischen Geraden”  $\left\{s \in \mathbb{C}; \operatorname{Re} s = \frac{1}{2}\right\}$  gibt und dass alle Nullstellen  $s$  mit  $0 < |\operatorname{Im} s| < 5 \cdot 10^8$  auf der kritischen Geraden liegen (siehe Abbildung 3.3).

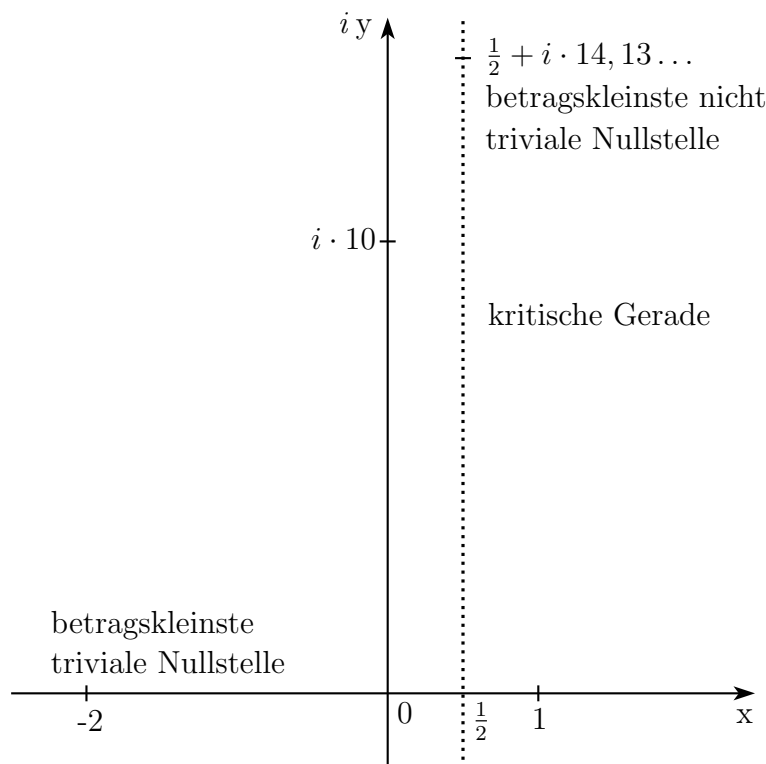


Abbildung 3.3: Nullstellen der Riemannschen Zetafunktion

Die Gültigkeit der Riemannschen Vermutung hätte weitreichende Konsequenzen für die Zahlentheorie. Unter anderem folgt unter Annahme der Richtigkeit der Riemannschen Vermutung (meistens “uARV” abgekürzt) die Existenz von  $c, x_1 \in \mathbb{R}^+$ , sodass  $|\pi(x) - \text{li}(x)| \leq c\sqrt{x} \ln x$  für alle  $x \in \mathbb{R}$  mit  $x \geq x_1$  gilt.

**iv) Das asymptotische Wachstum von  $\pi(x)$**

Erst nachdem J. HADAMARD<sup>11</sup> die Theorie der auf  $\mathbb{C}$  komplex differenzierbaren Funktionen mit “endlicher (Wachstums-) Ordnung” entwickelt hatte, konnten er und CH. DE LA VALLÉE-POUSSIN<sup>12</sup> unabhängig voneinander die Vermutungen von GAUß und LEGENDRE (siehe Seite 63 und Seite 72) beweisen:

**Theorem über das Wachstum von  $\pi(x)$**  (J. HADAMARD und CH. DE LA VALLÉE-POUSSIN, 1896)

Es gilt  $\lim_{x \rightarrow \infty} \frac{\pi(x)}{\text{li}(x)} = \lim_{x \rightarrow \infty} \frac{\pi(x) \ln x}{x} = 1$ .

Beim Beweis werden Summen verwendet, die mit  $\vartheta(x) := \sum_{p \in \mathbb{P}, p \leq x} \ln p$  zusammenhängen und für die Integraldarstellungen mit Hilfe des Residuensatzes der Funktionentheorie möglich sind. Damit lässt sich  $\lim_{x \rightarrow \infty} \vartheta(x) x^{-1} = 1$  zeigen, woraus die obigen Limesaussagen folgen.

Später konnte der Beweis sehr vereinfacht werden, aber erst 1948 gelang es, ihn ohne Funktionentheorie zu führen.

**v) Fastprimzahlzwillinge und Siebverfahren**

Durch starke Verallgemeinerungen des *Siebverfahrens* von ERATOSTHENES in verschiedenen Richtungen wurden “angenäherte” Lösungen für einige klassische Probleme gefunden. Das interessanteste Beispiel soll diesen Ausblick abschließen, wobei Paare  $(p, p + 2) \in \mathbb{P} \times \mathbb{N}_4$  mit  $\Omega(p + 2) \leq 2$  als “Fastprimzahlzwillinge” bezeichnet werden.

**Theorem über Fastprimzahlzwillinge** (CHEN JING RUN, 1973)

Es gibt unendlich viele  $p \in \mathbb{P}$  mit  $\Omega(p + 2) \leq 2$ .

<sup>11</sup> JACQUES HADAMARD (1865-1963) wirkte in Paris.  
<sup>12</sup> CHARLES DE LA VALLÉE-POUSSIN (1866-1962) wirkte in Löwen (Belgien).

## 3.7 Aufgaben und Probleme zu Kapitel 3

### Aufgabe 3.1:

Zeigen Sie, dass  $S_n := \sum_{k=1}^n \frac{1}{k}$  für alle  $n \in \mathbb{N}_2$  keine ganze Zahl darstellt.

[Hinweis: Betrachten Sie die Summe  $S_n$  zunächst für einige kleine Werte von  $n$ , bringen Sie die Summanden auf den Hauptnenner  $N_n$ , ohne die Summe bzw. das Produkt auszurechnen, und stellen Sie dann eine Vermutung über Teilereigenschaften auf. Beachten Sie beim Beweis die Primfaktorzerlegung des kgV.]

Achtung: Fundgrube! [Mit einem Computeralgebrasystem (CAS): Primteiler des Zählers  $Z_n$  von  $S_n$ .]

### Aufgabe 3.2:

Zeigen Sie, dass die Menge  $\{p \in \mathbb{P}; \text{Es gibt } k \in \mathbb{N} \text{ mit } p = 4k + 3\}$  unendlich ist.

[Hinweis: Betrachten Sie zu den ersten  $n$  Primzahlen  $q_1, \dots, q_n$  aus der Menge den Ausdruck  $4q_1 \cdots q_n - 1$ .]

### Aufgabe 3.3:

Bestimmen Sie alle  $n \in \mathbb{N}_1$  mit  $\prod_{d|n} d = n^2$ .

[Hinweis: Suchen Sie zunächst eine allgemeingültige Formel für  $\prod_{d|n} d$ .]

### Aufgabe 3.4:

Beweisen Sie die folgenden beiden Aussagen:

- Sind  $p$  und  $q$  aufeinanderfolgende ungerade Primzahlen, so ist  $\Omega(p+q) \geq 3$ .
- Es sei  $k \in \mathbb{N}_2$ . Ist  $n$  eine natürliche Zahl, die  $p \nmid n$  für alle  $p \in \mathbb{P}$  mit  $p^k \leq n$  erfüllt, so gilt  $\Omega(n) \leq k - 1$ .

### Aufgabe 3.5:

Es sei  $f(x) := \sum_{k=0}^n a_k x^k$  ein Polynom mit  $n \in \mathbb{N}_1$ ,  $a_n \in \mathbb{N}_1$  und  $a_k \in \mathbb{Z}$  für  $k = 0, \dots, n-1$ . Beweisen Sie, dass die Menge  $\{p \in \mathbb{P}; \text{Es gibt } m \in \mathbb{N}_1 \text{ mit } p | f(m)\}$  unendlich ist.

[Hinweis: Beachten Sie, dass  $f(a_0 m) = a_0 (1 + m \sum_{k=1}^n a_k a_0^{k-1} m^{k-1})$  gilt.]

### Aufgabe 3.6:

Für  $n \in \mathbb{N}_1$  sei  $n = \prod_{p \in \mathbb{P}} p^{\nu_p(n)}$  die formale Darstellung von  $n$ .

a) Zeigen Sie, dass

$$\nu_p(m!) = \sum_{k=1}^{\lfloor \frac{\ln m}{\ln p} \rfloor} \left\lfloor \frac{m}{p^k} \right\rfloor \quad \text{für alle } m \in \mathbb{N}_2 \text{ und jedes } p \in \mathbb{P} \text{ mit } p \leq m \text{ gilt.}$$

b) Bestimmen Sie die Anzahl der Nullen, mit denen  $(2004!)$  im Dezimalsystem endet.

### Aufgabe 3.7:

a) Beweisen Sie, dass  $n^5 + 4n$  für alle  $n \in \mathbb{N}_1$  durch 5 teilbar ist.

b) Berechnen Sie  $1 + \text{card} \{m \in \mathbb{N}_2 ; m \leq 2004 \text{ und } kP(m) > 7\}$ .

### Aufgabe 3.8:

Bestimmen Sie  $\sum_{d|n} \mu^2(d)$  für jedes  $n \in \mathbb{N}_1$ .

### Aufgabe 3.9:

Beweisen Sie, dass  $\sigma(n) < 2n$  für alle  $n \in \mathbb{N}_1$  mit  $2 \nmid n$  und  $\omega(n) = 2$  gilt.

### Aufgabe 3.10:

Begründen Sie, wieso  $\sigma(n^2)$  für jedes  $n \in \mathbb{N}_1$  ein Teiler von  $\sum_{d|n^2} d^2$  ist.

### Aufgabe 3.11:

Für  $m \in \mathbb{N}_1$  und  $p \in \mathbb{P}$  sei  $m = : \sum_{k=0}^s a_k p^k$  mit  $s := \lfloor \frac{\ln m}{\ln p} \rfloor$  und mit  $a_k \in \mathcal{A}_p$  für  $k = 0, \dots, s$  die eindeutig bestimmte Darstellung von  $m$  im  $p$ -adischen Zahlensystem und  $q_p(m) := \sum_{k=0}^s a_k$  sei die "Quersumme" dieser Darstellung. Zeigen Sie im Anschluss an Aufgabe 3.6, dass  $\nu_p(m!) = \frac{m - q_p(m)}{p-1}$  gilt.

### Aufgabe 3.12:

Es sei  $\mathcal{I} \subset \mathbb{N}_1$  mit  $\text{card} \mathcal{I} \in \mathbb{N}_2$ ,  $t := \text{ggT}(\mathcal{I}) := \max \{d \in \mathbb{N}_1 ; d \mid n \text{ für alle}$

$n \in \mathcal{I}$ },  $v := \text{kgV}(\mathcal{I}) := \min \{d \in \mathbb{N}_1; n \mid d \text{ für alle } n \in \mathcal{I}\}$  und  $\mu$  die Möbius-Funktion. Beweisen Sie die folgenden Identitäten:

$$\text{i) } \text{kgV} \left( \left\{ \frac{v}{k}; k \in \mathcal{I} \right\} \right) = \text{kgV} \left( \left\{ \frac{k}{t}; k \in \mathcal{I} \right\} \right) = \frac{v}{t},$$

$$\text{ii) } \prod_{k \in \mathcal{I}} \mu^2 \left( \frac{v}{k} \right) = \prod_{k \in \mathcal{I}} \mu^2 \left( \frac{k}{t} \right) = \mu^2 \left( \frac{v}{t} \right).$$

[Hinweis: Verwenden Sie die formalen Darstellungen aller beteiligten Zahlen.]

### Aufgabe 3.13:

Es seien  $m, n \in \mathbb{N}_1$  mit  $n < m$  und  $p \in \mathbb{P}$ . Mit  $\beta_p(m, n)$  werde die Anzahl der “Borgestellen” (bzw. der “Überträge”) bei der Subtraktion von  $m$  und  $n$  im  $p$ -adischen Zahlensystem bezeichnet. Zeigen Sie im Anschluss an Aufgabe 3.11, dass

$$\nu_p \left( \binom{m}{n} \right) = \beta_p(m, n) \text{ gilt, wobei } \binom{m}{n} = \frac{m!}{n!(m-n)!} \text{ die Binomialkoeffizienten sind.}$$

[Hinweis: Stellen Sie einen Zusammenhang zwischen  $q_p(m-n)$ ,  $q_p(m)$ ,  $q_p(n)$  und  $\beta_p(m, n)$  her.]

### Aufgabe 3.14:

$$\text{a) Bestimmen Sie alle } m \in \mathbb{N}_1 \text{ mit } 2 \nmid \prod_{k=0}^m \binom{m}{k}.$$

$$\text{b) Beweisen Sie, dass } \binom{2n}{n} \text{ für jedes } n \in \mathbb{N}_1 \text{ gerade ist.}$$

[Hinweis: Bei a) können Sie das Ergebnis von Aufgabe 3.13 verwenden.]

### Aufgabe 3.15:

Zeigen Sie, dass  $p_{2m+2} < p_1 p_2 \cdots p_m$  für alle  $m \in \mathbb{N}_3$  gilt.

[Hinweis: Betrachten Sie für  $m \in \mathbb{N}_4$  die  $p_m$  Zahlen  $k p_1 p_2 \cdots p_{m-1} - 1$ ,  $k = 1, \dots, p_m$ , und schließen Sie ähnlich wie bei dem Beweis von EUKLID für die Unendlichkeit von  $\mathbb{P}$ , dass  $\pi(p_1 \cdots p_m) > 2m + 1$  ist.]

### Aufgabe 3.16:

Beweisen Sie, dass es zu jedem  $n \in \mathbb{N}_{31}$  ein  $m \in \mathbb{N}_2 \setminus \mathbb{P}$  mit  $m < n$  und  $\text{ggT}(m, n) = 1$  gibt.

[Hinweis: Ist  $n$  durch  $p_1 \cdots p_k$  teilbar, so gilt  $p_1 \cdots p_\kappa p_{\kappa+1} \cdots p_k \leq n$  mit  $\kappa := \left\lfloor \frac{k}{2} \right\rfloor$ .

Folgern Sie daraus unter Verwendung von Aufgabe 3.15, dass ein  $p \in \mathbb{P}$  mit  $p \nmid n$  und  $p^2 < n$  existiert.]

Die nächsten dreizehn Probleme stammen aus dem Bundeswettbewerb Mathematik, die übrigen sieben aus der Internationalen Mathematikolympiade.

**Problem 14:**

Für die natürlichen Zahlen  $x$  und  $y$  gelte  $2x^2 + x = 3y^2 + y$ . Man beweise, dass dann  $x - y$ ,  $2x + 2y + 1$  und  $3x + 3y + 1$  Quadratzahlen sind.

**Problem 15:**

Man bestimme alle positiven ganzen Zahlen  $n$  mit der folgenden Eigenschaft: Jede natürliche Zahl, deren Dezimaldarstellung aus  $n$  Ziffern besteht, und zwar genau einer Sieben und  $n - 1$  Einsen, ist eine Primzahl.

**Problem 16:**

Unter der *Standarddarstellung* einer positiven ganzen Zahl  $n$  wird nachfolgend die Darstellung von  $n$  im Dezimalsystem verstanden, bei der die erste Ziffer verschieden von 0 ist. Jeder positiven ganzen Zahl  $n$  wird nun eine Zahl  $f(n)$  zugeordnet, indem in der Standarddarstellung von  $n$  die letzte Ziffer vor die erste gestellt wird; Beispiele:  $f(1992) = 2199$ ,  $f(2000) = 200$ .

Man bestimme die kleinste positive ganze Zahl  $n$ , für die  $f(n) = 2n$  gilt.

**Problem 17:**

Es sei  $f(x) = x^n$ , wobei  $n$  eine natürliche Zahl ist. Kann dann die Dezimalzahl  $0, f(1)f(2)f(3) \dots$  periodisch sein? Die Antwort ist zu begründen. (Beispiel: Für  $n = 2$  geht es um  $0,1\ 4\ 9\ 16\ 25 \dots$ , für  $n = 3$  ist die betrachtete Zahl  $0,1\ 8\ 27\ 64\ 125 \dots$ )

**Problem 18:**

Man bestimme alle Tripel  $(x, y, z)$  ganzer Zahlen, für die gilt:  $2^x + 3^y = z^2$ .

**Problem 19:**

Man gebe eine Zahl  $k \in \mathbb{N}$  und ein Polynom  $f(x) = a_0 + a_1x + a_2x^2 + \dots + a_kx^k$ ,  $a_k \neq 0$ , mit folgenden Eigenschaften an:

- (1) Die Koeffizienten  $a_0, a_1, a_2, \dots, a_k$  sind Elemente von  $\{-1, 0, 1\}$ .
- (2) Für jedes  $n \in \mathbb{N}$  ist  $f(n)$  durch 30 teilbar.
- (3) Kein Polynom kleineren Grades hat ebenfalls beide Eigenschaften (1) und (2).

**Problem 20:**

Es sei  $d_n$  die letzte von 0 verschiedene Ziffer der Dezimaldarstellung von  $n!$ . Man zeige, dass die Folge  $d_1, d_2, d_3, \dots$  nicht periodisch ist.

Erläuterung: Eine Folge  $a_1, a_2, a_3, \dots$  heißt genau dann periodisch, wenn es natürliche Zahlen  $T$  und  $n_0$  mit der folgenden Eigenschaft gibt: Für alle natürlichen Zahlen  $n$  mit  $n > n_0$  gilt  $a_n = a_{n+T}$ .

**Problem 21:**

Auf jedem Feld eines Schachbrettes von  $n$  mal  $n$  Feldern steht eine Zahl. Die Summe der Zahlen in einem "Kreuz" ist  $\geq a$ ; ein Kreuz ist die Vereinigung einer beliebigen Zeile mit einer beliebigen Spalte. Bestimme die bestmögliche untere Schranke für die Summe aller Zahlen auf dem Schachbrett. Das Ergebnis ist zu begründen.

**Problem 22:**

Mit einer im Zehnersystem geschriebenen natürlichen Zahl darf man folgende Operationen vornehmen:

- a) am Ende der Zahl 4 anhängen,
- b) am Ende der Zahl 0 anhängen,
- c) die Zahl durch 2 teilen, wenn sie gerade ist.

Man zeige, dass man ausgehend von 4 durch eine Folge der Operationen  $a, b, c$  jede natürliche Zahl erreichen kann.

**Problem 23:**

Peter und Paul spielen um Geld. Sie bestimmen der Reihe nach bei jeder natürlichen Zahl deren größten ungeraden Teiler. Liegt dieser um 1 über einem ganzzahligen Vielfachen von 4, dann zahlt Peter an Paul einen EURO, andernfalls Paul an Peter einen EURO. Nach einiger Zeit brechen sie ab und machen Bilanz. Es ist nachzuweisen, dass Paul gewonnen hat.

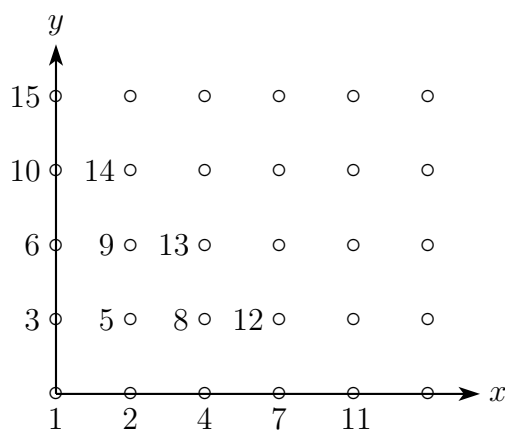
**Problem 24:**

Man bestimme eine Folge von Quadratzahlen mit folgenden Eigenschaften:

- Das arithmetische Mittel je zweier benachbarter Folgenglieder ist eine Quadratzahl.
- Die Folge wächst streng monoton.
- Je zwei benachbarte Folgenglieder sind teilerfremd.

**Problem 25:**

In einem ebenen Koordinatensystem werden die Punkte mit nichtnegativen ganzzahligen Koordinaten gemäß der nachfolgenden Figur nummeriert. Z.B. hat der Punkt  $(3, 1)$  die Nummer 12. Welche Nummer hat der Punkt  $(u, v)$ ?

**Problem 26:**

Man zeige, dass keine der Zahlen der Folge

$$10001, 100010001, 1000100010001, \dots$$

eine Primzahl ist.

**Problem 27:**

Man finde alle Paare  $(a, b)$  positiver ganzer Zahlen, sodass  $a^2b + a + b$  durch  $ab^2 + b + 7$  teilbar ist.

**Problem 28:**

Bestimme alle dreiziffrigen Zahlen, die durch 11 geteilt eine Zahl ergeben, die gleich ist der Summe der Quadrate der Ziffern der ursprünglichen Zahl.

**Problem 29:**

Für jede positive ganze Zahl  $n$  bezeichne  $d(n)$  die Anzahl der positiven Teiler von  $n$  (einschließlich 1 und  $n$ ). Man bestimme alle positiven ganzen Zahlen  $k$ , für die es ein  $n$  gibt, sodass gilt:  $\frac{d(n^2)}{d(n)} = k$ .

**Problem 30:**

Man bestimme alle Paare  $(a, b)$  ganzer Zahlen mit  $a, b \geq 1$ , die folgende Gleichung erfüllen:  $a^{b^2} = b^a$ .

**Problem 31:**

Es sei  $p$  eine ungerade Primzahl. Man bestimme die Anzahl aller Teilmengen  $A$  der Menge  $\{1, 2, \dots, 2p\}$ , für die gilt:

- i)  $A$  hat genau  $p$  Elemente.
- ii) Die Summe aller Elemente von  $A$  ist durch  $p$  teilbar.

**Problem 32:**

Man zeige: Für jede natürliche Zahl  $n$  gibt es  $n$  aufeinanderfolgende natürliche Zahlen, von denen keine eine Primzahlpotenz mit ganzzahligem Exponenten ist.

**Problem 33:**

Sei  $n$  eine ganze Zahl  $\geq 2$ . Man beweise:

Wenn  $k^2 + k + n$  für alle ganzen Zahlen  $k$  mit  $0 \leq k \leq \sqrt{\frac{n}{3}}$  eine Primzahl ist, dann ist auch  $k^2 + k + n$  für alle ganzen Zahlen  $k$  mit  $0 \leq k \leq n - 2$  eine Primzahl.

# Kapitel 4

## Kongruenzen

### 4.1 Die Kongruenzrelation

Der auf Seite 16 erwähnte Begriff der *Kongruenz* wurde von GAUß am Anfang des ersten Abschnitts von [9] eingeführt. Mit der folgenden Fortsetzung der Teilbarkeitsuntersuchungen von Kapitel 2 erscheinen bei uns Kongruenzen je nach Blickwinkel als Verfeinerung oder als Verallgemeinerung des Teilbarkeitsbegriffs.

#### Definition der Kongruenz

Ist  $m \in \mathbb{N}_1$  und  $(a, b) \in \mathbb{Z}^2$ , so heißt  $a$  *kongruent zu  $b$  modulo  $m$* , wenn  $m \mid (a - b)$  gilt.

Es wird  $a \equiv b \pmod{m}$  oder  $a \equiv b (m)$  geschrieben. Wenn klar ist, um welchen *Modul*  $m$  es sich handelt, kann auch  $a \equiv b$  abgekürzt werden.

Die Negation wird  $a \not\equiv b \pmod{m}$  geschrieben und “ $a$  ist inkongruent zu  $b$  modulo  $m$ ” gesprochen.

Bezeichnet  $m$  einen Modul, so sei im Folgenden stets  $m \in \mathbb{N}_1$ .

#### Satz über die Kongruenzrelation

Die Kongruenz  $\equiv$  ist eine Äquivalenzrelation auf  $\mathbb{Z}$ .

**Beweis** (direkt, r1):

**Reflexivität:** Aus  $m \mid 0$  folgt  $m \mid (a - a)$ , also  $a \equiv a \pmod{m}$ .

**Symmetrie:** Ist  $m \mid (a - b)$ , so gilt auch  $m \mid (b - a)$ . Damit folgt  $b \equiv a$  aus  $a \equiv b$ .

**Transitivität:** Ist  $a \equiv b$  und  $b \equiv c$  ( $c \in \mathbb{Z}$ ), so gilt  $m \mid (b - c)$ . Aufgrund des *Satzes über Teilbarkeitsregeln* (Seite 18) folgt  $m \mid ((a - b) + (b - c))$ , d.h.  $m \mid (a - c)$ , bzw.  $a \equiv c$ .  $\square$

### Bezeichnung des kleinsten nichtnegativen Restes

Ist  $m \in \mathbb{N}_1$  und  $c \in \mathbb{Z}$ , so heißt die Zahl  $\text{mod}(c, m) \in \mathcal{A}_m$  *kleinster nichtnegativer Rest von  $c$  modulo  $m$* .

### Satz über ein Kongruenzkriterium

Zwei Zahlen  $a, b \in \mathbb{Z}$  sind genau dann kongruent modulo  $m$ , wenn sie denselben kleinsten nichtnegativen Rest besitzen.

**Beweis** (direkt, zwei Teile, r1):

a) Wegen  $\text{mod}(a, m) = a - m \left[ \frac{a}{m} \right]$  und aus  $a - m \left[ \frac{a}{m} \right] = b - m \left[ \frac{b}{m} \right]$  folgt  $a - b = m \left( \left[ \frac{a}{m} \right] - \left[ \frac{b}{m} \right] \right)$ , d.h.  $m \mid (a - b)$  und damit  $a \equiv b$ .

b) Aufgrund des *Satzes über Division mit Rest* (Seite 19) gibt es genau ein Paar  $(q, r) \in \mathbb{Z} \times \mathcal{A}_m$  mit  $a = mq + r$ . Aus  $a \equiv b \pmod{m}$  folgt also  $b = a + q_1 m = (q + q_1)m + r$  mit  $q_1 \in \mathbb{Z}$ , d.h.  $b$  hat denselben kleinsten nichtnegativen Rest wie  $a$ .  $\square$

## 4.2 Restklassen

### Bezeichnung der Restklassen

Die durch die Kongruenzrelation modulo  $m$  bestimmten Äquivalenzklassen aller ganzen Zahlen, die jeweils zueinander kongruent sind, heißen *Restklassen modulo  $m$* .

### Bezeichnung der Repräsentanten und Reste

Jede Zahl einer Restklasse heißt *Repräsentant* (oder *Vertreter*) der Restklasse. Die Elemente jeder Restklasse heißen *Reste modulo  $m$* . Die durch  $a \in \mathbb{Z}$  bestimmte Restklasse  $\{b \in \mathbb{Z}; b \equiv a \pmod{m}\}$  wird bei vorgegebenem  $m$  mit  $\bar{a}$  bezeichnet.

### Bezeichnung des vollständigen Restsystems

Eine Teilmenge  $\mathcal{R}$  von  $\mathbb{Z}$ , die aus jeder Restklasse modulo  $m$  genau eine Zahl enthält, heißt *vollständiges Restsystem modulo  $m$* .

### Beispiele für $m = 7$ :

$\mathcal{A}_7 = \{0, 1, 2, 3, 4, 5, 6\}$  (kleinste nichtnegative Reste),

$\mathcal{R}_7 = \{-3, -2, -1, 0, 1, 2, 3\}$  (“*absolut kleinste Reste*”),

$\mathcal{R}'_7 = \left\{ 0, \underbrace{3}_{\equiv 3}, \underbrace{3^2}_{\equiv 2}, \underbrace{3^3}_{\equiv 6}, \underbrace{3^4}_{\equiv 4}, \underbrace{3^5}_{\equiv 5}, \underbrace{3^6}_{\equiv 1} \right\}$  (siehe Seite 122).

Der folgende Satz spielt eine besondere Rolle beim Problemlösen in der Zahlentheorie. Er wird aber auch in anderen Teilen der Mathematik benutzt. Dennoch findet man ihn als “*Schubfachprinzip*” üblicherweise nur in einer umgangssprachlichen Form und ohne Beweis.

### Schubfachsatz

Für  $n \in \mathbb{N}_1$  sei  $\mathcal{E}_n$  eine Menge mit  $\text{card } \mathcal{E}_n = n$ .

a) Keine Abbildung  $f : \mathcal{A}_{n+1} \rightarrow \mathcal{E}_n$  ist injektiv.

[“*Erster Dirichletscher Schubfachschluss*”: Sind  $n + 1$  Dinge in  $n$  Schubfächern, so liegt in mindestens einem Schubfach mehr als ein Ding.]

b) Stellt  $g : \mathcal{A}_n \rightarrow \mathcal{E}_n$  eine surjektive oder eine injektive Abbildung dar, so ist  $g$  bijektiv.

[“*Zweiter Dirichletscher Schubfachschluss*”: Sind  $n$  Dinge in  $n$  Schubfächern und befindet sich in allen Fächern mindestens ein Ding oder befindet sich in allen Fächern höchstens ein Ding, so liegt in jedem Fach genau ein Ding.]

**Beweis** (drei Teile: Nichtinjektivität, Surjektivität impliziert Injektivität und Injektivität impliziert Surjektivität):

**i) Nichtinjektivität** (vollständige Induktion, Fallunterscheidung, r2):

Die Induktionsmenge sei

$\mathcal{M} := \{n \in \mathbb{N}_1 ; \text{Für jede Menge } \mathcal{E}_n \text{ mit } \text{card } \mathcal{E}_n = n \text{ sind alle Abbildungen } f : \mathcal{A}_{n+1} \rightarrow \mathcal{E}_n \text{ nicht injektiv}\},$

Es gilt  $1 \in \mathcal{M}$ , weil  $f : \mathcal{A}_2 \rightarrow \mathcal{E}_1$  mit  $\mathcal{E}_1 =: \{a\}$  wegen  $f(0) = a = f(1)$  nicht injektiv ist.

Es sei  $m \in \mathcal{M}$ ,  $f_1 : \mathcal{A}_{m+2} \rightarrow \mathcal{E}_{m+1}$  und  $b := f_1(m+1)$ . Gibt es ein  $j \in \mathcal{A}_{m+1}$  mit  $f_1(j) = b$ , so ist  $f_1$  nicht injektiv. Andernfalls stellt  $f_1|_{\mathcal{A}_{m+1}} : \mathcal{A}_{m+1} \rightarrow \mathcal{E}'_m$  mit  $\mathcal{E}'_m := \mathcal{E}_{m+1} \setminus \{b\}$  nach Induktionsvoraussetzung eine nicht injektive Abbildung dar, wobei  $f_1|_{\mathcal{A}_{m+1}}$  die "Einschränkung von  $f_1$  auf  $\mathcal{A}_{m+1}$ " bezeichnet. Damit ist  $m+1 \in \mathcal{M}$  und es folgt  $\mathcal{M} = \mathbb{N}_1$ .

**ii) Surjektivität impliziert Injektivität** (vollständige Induktion, r1):

Es sei

$$\mathcal{M} := \{n \in \mathbb{N}_1 ; \text{Für jede Menge } \mathcal{E}_n \text{ mit } \text{card } \mathcal{E}_n = n \text{ sind alle surjektiven Abbildungen } g : \mathcal{A}_n \rightarrow \mathcal{E}_n \text{ injektiv} \}.$$

Wegen  $\text{card } \mathcal{A}_1 = 1$  gilt  $1 \in \mathcal{M}$ . Ist  $m \in \mathcal{M}$  und stellt  $g_1 : \mathcal{A}_{m+1} \rightarrow \mathcal{E}_{m+1}$  eine surjektive Abbildung dar, so werde  $c := g_1(m)$  und  $\mathcal{E}''_m := \mathcal{E}_{m+1} \setminus \{c\}$  gesetzt. Dann ist auch  $g_1|_{\mathcal{A}_m} : \mathcal{A}_m \rightarrow \mathcal{E}''_m$  surjektiv. Da  $\text{card } \mathcal{E}''_m = m$  gilt, ergibt die Induktionsvoraussetzung, dass  $g_1|_{\mathcal{A}_m}$  injektiv ist. Wegen  $g_1(j) \neq c$  für alle  $j \in \mathcal{A}_m$  ergibt sich die Injektivität von  $g_1$ . Damit ist  $m+1 \in \mathcal{M}$ , sodass  $\mathcal{M} = \mathbb{N}_1$  folgt.

**iii) Injektivität impliziert Surjektivität** (Kontraposition, a1):

An Stelle der Aussage, dass alle injektiven Abbildungen  $g : \mathcal{A}_n \rightarrow \mathcal{E}_n$  surjektiv sind, beweisen wir die dazu äquivalente Implikation, dass alle nicht surjektiven Abbildungen  $g : \mathcal{A}_n \rightarrow \mathcal{E}_n$  nicht injektiv sind. Ist  $g$  nicht surjektiv, so gibt es ein  $d \in \mathcal{E}_n$  mit  $d \notin g(\mathcal{A}_n)$ . Nach i) ist dann  $g : \mathcal{A}_n \rightarrow \mathcal{E}_n \setminus \{d\}$  wegen  $\text{card } \mathcal{E}_n \setminus \{d\} = n - 1$  nicht injektiv.  $\square$

### Satz über vollständige Restsysteme

Ist  $\mathcal{R}$  eine Teilmenge von  $\mathbb{Z}$ , so ergibt sich jede der folgenden drei Aussagen aus den beiden anderen, wobei die ersten beiden der Definition des vollständigen Restsystems modulo  $m$  entsprechen:

- Je zwei Zahlen aus  $\mathcal{R}$  sind modulo  $m$  zueinander inkongruent.
- Jede ganze Zahl ist modulo  $m$  kongruent zu einer Zahl aus  $\mathcal{R}$ .
- $\mathcal{R}$  enthält genau  $m$  Elemente.

**Beweis** (drei Teile, i) indirekt, ii) und iii) direkt, r1):

Bei allen drei Implikationen wird der *Schubfachsatz* mit der Abbildung  $f : \mathcal{R} \rightarrow \mathcal{A}_m, r \mapsto \text{mod}(r, m)$ , verwendet. Außerdem nutzen wir die zu i) äquivalente Aussage des *Satzes über ein Kongruenzkriterium* (Seite 84).

i) Aus a) und b) folgt c): Ist  $n := \text{card } \mathcal{R}$ , so zeigen wir, dass die Annahmen  $n < m$  oder  $n > m$  jeweils zu einem Widerspruch führen. Im ersten Falle gäbe es ein  $a \in \mathcal{A}_m$  mit  $\text{mod}(r, m) \neq a$  für alle  $r \in \mathcal{R}$  - im Widerspruch zu b). Der zweite Fall würde wegen  $n \geq m + 1 > m$  mit Hilfe des ersten Teils des *Schubfachsatzes* ergeben, dass  $f$  nicht injektiv wäre - im Widerspruch zu a).

ii) Aus a) und c) ergibt sich b): Jetzt ist  $f$  wegen a) injektiv. Der zweite Teil des *Schubfachsatzes* ergibt die Bijektivität von  $f$  und damit auch b).

iii) Aus b) und c) folgt a): Nun stellt  $f$  wegen b) eine surjektive Abbildung dar. Deshalb liefert der zweite Teil des *Schubfachsatzes* die Injektivität, also a).  $\square$

Der folgende Satz bringt Eigenschaften, die der Gleichheitsrelation entsprechen, wobei  $a \equiv b$  mit  $\bar{a} = \bar{b}$  äquivalent ist.

### Satz über Kongruenzregeln

Die folgenden sieben Aussagen sind für jeden festen Modul  $m$  erfüllt:

i) Ist  $a \equiv b$  und  $c \equiv d$ , so gilt  $a \pm c \equiv b \pm d$ .

ii) Aus  $a_k \equiv b_k, k = 1, \dots, n$ , folgt  $\sum_{k=1}^n a_k \equiv \sum_{k=1}^n b_k$ .

iii) Mit  $a \equiv b$  und  $c \in \mathbb{Z}$  gilt  $ac \equiv bc$ .

iv) Für  $a \equiv b$  und  $c \equiv d$  ergibt sich  $ac \equiv bd$ .

v) Entsprechend gilt  $\prod_{k=1}^n a_k \equiv \prod_{k=1}^n b_k$ , wenn  $a_k \equiv b_k$  für  $k = 1, \dots, n$  vorausgesetzt wird.

vi) Mit  $a_k = a$  und  $b_k = b$  für  $k = 1, \dots, n$  folgt speziell  $a^n \equiv b^n$ .

vii) Ist  $f(x) := \sum_{k=0}^n c_k x^k$  ein Polynom mit  $c_k \in \mathbb{Z}$  für  $k = 0, \dots, n$ , so ergibt sich  $f(a) \equiv f(b)$  aus  $a \equiv b$ .

**Beweis** (direkt, r1):

i) Aus  $m \mid (a - b)$  und  $m \mid (c - d)$  folgt mit Hilfe des *Satzes über Teilbarkeitsregeln* (Seite 18), dass  $m \mid ((a - b) \pm (c - d))$  und damit  $m \mid ((a \pm c) - (b \pm d))$  gilt.

- ii) i) ergibt mit vollständiger Induktion die allgemeine Summenkongruenz.
- iii)  $m \mid (a - b)$  hat mit der Teilerdefinition  $m \mid (a - b)c$  und damit  $m \mid (ac - bc)$  zur Folge.
- iv) Mit der Teilereigenschaft und mit i) erhalten wir  $m \mid (ac - bd)$  aus  $m \mid (a - b)c$  und  $m \mid (c - d)b$ .
- v) Mit vollständiger Induktion ergibt iv) die allgemeine Produktkongruenz.
- vi) Die Potenzkongruenz ist ein Spezialfall von v).
- vii) Nacheinander ergeben vi), iii) und ii) die allgemeine Polynomkongruenz.  $\square$
- Nach i) und iv) sind die durch

$$\bar{a} + \bar{b} := \overline{a + b} \quad \text{und} \quad \bar{a} \cdot \bar{b} := \overline{a \cdot b}$$

definierten Verknüpfungen unabhängig von der Auswahl der Repräsentanten aus den jeweiligen Restklassen.

Um zu jedem  $m \in \mathbb{N}_1$  die Menge der Restklassen modulo  $m$  mit einer Ringstruktur zu versehen, die mit der von  $\mathbb{Z}$  "verträglich" ist, stellen wir die Eigenschaften von  $(\mathbb{Z}, +, \cdot, 0, 1, -)$  als *kommutativer Ring mit Einselement*<sup>1</sup> zusammen, wobei  $a, b, c \in \mathbb{Z}$  seien:

- |       |   |  |
|-------|---|--|
| i)    | $(a + b) + c = a + (b + c)$                   | (Assoziativgesetz der Addition),       |
| ii)   | $a + b = b + a$                               | (Kommutativgesetz der Addition),       |
| iii)  | $0 + a = a$                                   | (Neutralität der Null),                |
| iv)   | $(-a) + a = 0$                                | (Eigenschaft der Inversen)             |
| v)    | $(a \cdot b) \cdot c = a \cdot (b \cdot c)$   | (Assoziativgesetz der Multiplikation), |
| vi)   | $a \cdot b = b \cdot a$                       | (Kommutativgesetz der Multiplikation), |
| vii)  | $(a + b) \cdot c = (a \cdot c) + (b \cdot c)$ | (Distributivgesetz),                   |
| viii) | $1 \cdot a = a$                               | (Neutralität der Eins).                |

Aus den gewünschten Ringeigenschaften für die Restklassen lassen sich nun die neutralen Elemente und die Inversen erschließen:

$$\begin{aligned} \bar{0} &:= \{a \in \mathbb{Z} ; m \mid a\}, \\ \bar{1} &:= \{b \in \mathbb{Z} ; b \equiv 1 \pmod{m}\}, \\ -\bar{a} &:= \overline{-a}, \end{aligned}$$

---

<sup>1</sup> In diesem Buch sind Ringe stets bezüglich der "Multiplikation" kommutative Ringe mit Einselement. In der Algebra werden auch Ringe betrachtet, die bezüglich der Multiplikation nicht kommutativ sind und/oder die kein Einselement besitzen.

wobei die letzte Definition wieder unabhängig von der Auswahl des Repräsentanten  $a$  ist.

### Satz über Restklassenringe

Die Menge der Restklassen modulo  $m$  zusammen mit den Verknüpfungen  $+$  :  $(\bar{a}, \bar{b}) \mapsto \bar{a} + \bar{b}$  und  $\cdot$  :  $(\bar{a}, \bar{b}) \mapsto \bar{a} \cdot \bar{b}$ , den neutralen Elementen  $\bar{0}$  und  $\bar{1}$  und der Inversenabbildung  $-$  :  $\bar{a} \mapsto -\bar{a}$  stellt einen kommutativen Ring mit Einselement dar, der mit  $\mathbb{Z}/_m\mathbb{Z}$  (gelesen:  $\mathbb{Z}$  modulo  $m\mathbb{Z}$ ) bezeichnet wird und der *Restklassenring modulo  $m$*  heißt.

**Beweis** (direkt, r1):

Aufgrund der Definitionen der Verknüpfungen, der neutralen Elemente und der Inversenabbildung übertragen sich alle Grundeigenschaften des Ringes  $\mathbb{Z}$  auf den Restklassenring  $\mathbb{Z}/_m\mathbb{Z}$ . □

Im Mathematikunterricht werden manchmal zu diesen Restklassenringen *isomorphe* (d. h. “strukturgleiche”) Ringe in der Form  $\mathbb{Z}_m := (\mathcal{A}_m, \boxplus, \boxminus, 0, 1, \boxminus)$  mit

$$a \boxplus b := \text{mod}(a + b, m),$$

$$a \boxminus b := \text{mod}(ab, m) \text{ und}$$

$$\boxminus a := \begin{cases} 0, & \text{wenn } a = 0, \\ m - a, & \text{wenn } a \in \mathcal{A}_m \setminus \{0\}, \end{cases}$$

eingeführt.

Aus algebraischer Sicht gibt es zwei verschiedene Typen von Restklassenringen. Zum Beispiel für  $m = 6$  gilt  $\bar{2} \cdot \bar{3} = \bar{0}$ , d. h. in  $\mathbb{Z}/_6\mathbb{Z}$  ist  $\bar{0}$  Produkt von zwei Elementen, die von  $\bar{0}$  verschieden sind. Das Gleiche gilt offenbar für alle  $m \in \mathbb{N}_2 \setminus \mathbb{P}$ , weil es zu diesen zerlegbaren Moduln Zahlen  $k, l \in \mathbb{N}_2$  mit  $m = kl$  gibt, so dass also  $\bar{k} \cdot \bar{l} = \bar{0}$  erfüllt ist.

Im Falle eines Primzahlmoduls  $p$  liegt eine ganz andere Situation vor. Die Voraussetzungen  $\bar{a} \cdot \bar{b} = \bar{0}$  und  $\bar{a} \neq \bar{0}$  sind definitionsgemäß gleichbedeutend mit  $p \mid ab$  und  $p \nmid a$ . Wegen  $\text{ggT}(p, a) = 1$  ergibt der *Produktteilersatz* (Seite 23), dass  $p$  Teiler von  $b$  sein muss, womit  $\bar{b} = \bar{0}$  folgt.

Diese “bessere” Eigenschaft der Ringe  $\mathbb{Z}$  und  $\mathbb{Z}/_p\mathbb{Z}$  für  $p \in \mathbb{P}$  wird durch die folgenden beiden Definitionen erfasst:

### Definition des nullteilerfreien Ringes beziehungsweise des Integritätsringes

Ein Ring  $(\mathcal{R}, +, \cdot, 0, 1, -)$  heißt *nullteilerfreier Ring* oder *Integritätsring*, wenn  $a \cdot b \neq 0$  für alle  $a, b \in \mathcal{R} \setminus \{0\}$  gilt.

Also stellt  $\mathbb{Z}/_p\mathbb{Z}$  für jedes  $p \in \mathbb{P}$  einen Integritätsring dar, und  $\mathbb{Z}/_m\mathbb{Z}$  ist für alle  $m \in \mathbb{N}_2 \setminus \mathbb{P}$  kein Integritätsring. Im Unterschied zu  $\mathbb{Z} \setminus \{0\}$  lässt sich auf  $\mathbb{Z}/_p\mathbb{Z} \setminus \{\bar{0}\}$  für  $p \in \mathbb{P}$  eine “*Reziprokenabbildung*” einführen. Damit erhält  $\mathbb{Z}/_p\mathbb{Z}$  eine Struktur, die bei den Zahlringen erst für  $\mathbb{Q}$  vorliegt.

### Definition des Körpers

Ein Integritätsring  $(\mathcal{R}, +, \cdot, 0, 1, -)$  heißt *Körper*, wenn es eine Abbildung  $/ : \mathcal{R} \setminus \{0\} \rightarrow \mathcal{R} \setminus \{0\}$ ,  $a \mapsto /a$ , gibt, sodass  $a \cdot (/a) = 1$  für alle  $a \in \mathcal{R} \setminus \{0\}$  gilt.

### Satz über Restklassenkörper

Jeder Restklassenring  $\mathbb{Z}/_p\mathbb{Z}$  mit  $p \in \mathbb{P}$  ist ein Körper.

**Beweis** (direkt, r1):

Bei dem üblichen abstrakten Beweis ist dieser Satz ein Spezialfall der allgemeinen Aussage, dass jeder endliche Integritätsring  $(\mathcal{R}, +, \cdot, 0, 1, -)$  einen Körper darstellt. Für jedes  $a \in \mathcal{R}^* := \mathcal{R} \setminus \{0\}$  zeigt sich nämlich durch Anwenden des *Schubfachsatzes* (Seite 85) auf die Abbildung  $\alpha : \mathcal{R}^* \rightarrow \mathcal{R}^*$ ,  $x \mapsto a \cdot x$ , die Bijektivität von  $\alpha$ . Aus  $a \cdot x_1 = a \cdot x_2$  folgt  $a \cdot (x_1 - x_2) = 0$ , und die Nullteilerfreiheit von  $\mathcal{R}$  ergibt  $x_1 = x_2$ , sodass  $\alpha$  injektiv ist. Wegen der Endlichkeit von  $\mathcal{R}$  liefert der *Schubfachsatz* die Surjektivität von  $\alpha$ , sodass ein  $x \in \mathcal{R}^*$  mit  $a \cdot x = 1$  existiert.

In unserem Falle muss für jedes  $\bar{a} \in \mathbb{Z}/_p\mathbb{Z} \setminus \{\bar{0}\}$  die Gleichung  $\bar{a} \cdot \bar{x} = \bar{1}$ , die mit  $ax \equiv 1 \pmod{p}$  äquivalent ist, gelöst werden. Das können wir konkret mit Hilfe des *Satzes über die lineare diophantische Gleichung* (Seite 28), der auf die Gleichung  $ax - py = 1$  anzuwenden ist. Da  $\text{ggT}(a, p) = 1$  gilt, gibt es mindestens eine Lösung, die wir in dem nächsten Satz explizit angeben.  $\square$

## 4.3 Kongruenzsätze

### Satz über die lineare Kongruenz

Sind  $a \in \mathbb{N}_1$  und  $m \in \mathbb{N}_2$  mit  $\text{ggT}(a, m) = 1$ , so stellt  $x = (-1)^n Q_{n-1} b$  für jedes  $b \in \mathbb{Z}$  eine Lösung der *linearen Kongruenz*  $ax \equiv b \pmod{m}$  dar. Dabei ist  $Q_{n-1}$  der Nenner des vorletzten Näherungsbruches der Kettenbruchentwicklung von  $\frac{a}{m}$ .

**Beweis** (direkt, r1):

Ist  $\frac{P_{n-1}}{Q_{n-1}}$  der vorletzte Näherungsbruch der Kettenbruchentwicklung von  $\frac{a}{m}$ , so wird im *Satz über die lineare diophantische Gleichung* (Seite 28) gezeigt, dass  $(x, y) := ((-1)^n Q_{n-1} b, (-1)^n P_{n-1} b)$  eine Lösung der linearen diophantischen Gleichung  $ax - my = b$  darstellt. Wegen  $\frac{ax-b}{m} = y \in \mathbb{Z}$  ist damit  $x = (-1)^n Q_{n-1} b$  eine Lösung der linearen Kongruenz  $ax \equiv b \pmod{m}$ .  $\square$

### Satz über Kongruenzkürzung

Sind  $k, m \in \mathbb{Z}^2$  mit  $k \neq 0$ ,  $m \geq 1$  und  $d := \text{ggT}(k, m)$ , so gilt  $ka \equiv kb \pmod{m}$  genau dann, wenn  $a \equiv b \pmod{\frac{m}{d}}$  ist.

**Beweis** (zwei Teile, direkt, r1):

i) Ist  $k = k_1 d$  und  $m = m_1 d$  mit  $\text{ggT}(k_1, m_1) = 1$ , so gilt

$$\frac{ka - kb}{m} = \frac{k_1 da - k_1 db}{m_1 d} = \frac{k_1(a - b)}{m_1}.$$

Aufgrund des *Produktteilersatzes* (Seite 23) folgt  $m_1 \mid (a - b)$ , d.h.  $a \equiv b \pmod{m_1}$ .

ii) Ist  $m_1 \mid (a - b)$ , so zeigt die Gleichungskette, dass auch  $m \mid (ka - kb)$  gilt.  $\square$

### Satz über Kongruenzvergrößerung

Sind  $m, n \in \mathbb{N}_1$  mit  $n \mid m$ , so folgt  $a \equiv b \pmod{n}$  aus  $a \equiv b \pmod{m}$ .

**Beweis** (direkt, r1):

Mit  $m = kn$  und  $a - b = lm$  gilt  $a - b = (kl)n$ . □

### Satz über Kongruenzzusammenfassung

Es seien  $m_1, \dots, m_n$  verschiedene Zahlen aus  $\mathbb{N}_1$  und es werde  $m := \text{kgV}(m_1, \dots, m_n)$  gesetzt. Aus  $a \equiv b \pmod{m_k}$  für  $k = 1, \dots, n$  folgt  $a \equiv b \pmod{m}$ .

**Beweis** (direkt, r2):

Ist  $m_k = \prod_{p \in \mathbb{P}} p^{\nu_p(m_k)}$  für  $k = 1, \dots, n$  und  $m = \prod_{p \in \mathbb{P}} p^{\nu_p(m)}$ , so ergibt der Satz über die ggT- und kgV-Darstellung (Seite 54), dass  $\nu_p(m) = \max \{\nu \in \mathbb{N}; \text{Es gibt ein } k \in \mathcal{I}_n \text{ mit } \nu = \nu_p(m_k)\}$  gilt.

Aufgrund der Maximumsdefinition gibt es zu jedem  $p \mid m$  ein  $k \in \mathcal{I}_n$  mit  $\nu_p(m_k) = \nu_p(m)$ , d.h. es gilt  $p^{\nu_p(m)} \mid m_k$ . Daraus folgt  $p^{\nu_p(m)} \mid (a - b)$ .

Wegen  $\text{ggT}(p^{\nu_p(m)}, q^{\nu_q(m)}) = 1$  für alle  $p, q \in \mathbb{P}$  mit  $p \mid m$ ,  $q \mid m$  und  $p \neq q$  ergibt schließlich der Produktteilersatz (Seite 23), dass  $\prod_{p \in \mathbb{P}} p^{\nu_p(m)} \mid (a - b)$  und damit  $m \mid (a - b)$  erfüllt ist. □

## 4.4 Eigenschaften der Restsysteme

### Satz über modifizierte Restsysteme

a) Ist  $\mathcal{R}_m$  ein vollständiges Restsystem modulo  $m$  und  $(k, l) \in \mathbb{Z}^2$  mit  $k \neq 0$  und  $\text{ggT}(k, m) = 1$ , so stellt auch  $\{c \in \mathbb{Z}; \text{Es gibt } a \in \mathcal{R}_m, \text{ sodass } c = ka + l \text{ gilt}\}$  ein vollständiges Restsystem modulo  $m$  dar.

b) Es sei  $m' \in \mathbb{N}_1$  mit  $\text{ggT}(m, m') = 1$ , und  $\mathcal{R}_{m'}$  sei ein vollständiges Restsystem modulo  $m'$ . Dann ist  $\{c \in \mathbb{Z}; \text{Es gibt } a \in \mathcal{R}_m \text{ und } a' \in \mathcal{R}_{m'}, \text{ so dass } c = a'm + am' \text{ gilt}\}$  ein vollständiges Restsystem modulo  $mm'$ .

**Beweis** (direkt und Kontraposition, r1):

a) Ist  $\mathcal{R}_m = \{a_1, \dots, a_m\}$ , so zeigen wir zunächst durch Kontraposition, dass die Zahlen  $ka_r + l$  für  $r = 1, \dots, m$  inkongruent sind. Aus  $ka_r + l \equiv ka_s + l \pmod{m}$ ,

$r, s \in \mathcal{I}_m$ , folgt mit Hilfe des *Satzes über Kongruenzkürzung* (Seite 91), dass  $a_r \equiv a_s \pmod{m}$  ist. Definitionsgemäß gilt dann  $a_r = a_s$ , und der *Satz über vollständige Restsysteme* (Seite 86) ergibt die Aussage.

b) Es gibt  $mm'$  Zahlen der Form  $a'm + am'$  mit  $a \in \mathcal{R}_m$  und  $a' \in \mathcal{R}_{m'}$ . Um wieder den *Satz über vollständige Restsysteme* anwenden zu können, beweisen wir durch Kontraposition, dass je zwei dieser Zahlen modulo  $mm'$  inkongruent sind.

Aus  $a'_1m + a_1m' \equiv a'_2m + a_2m' \pmod{mm'}$  mit  $a_1, a_2 \in \mathcal{R}_m, a'_1, a'_2 \in \mathcal{R}_{m'}$  folgt  $mm' \mid ((a'_1 - a'_2)m + (a_1 - a_2)m')$ , d.h.  $m \mid (a_1 - a_2)m'$  und  $m' \mid (a'_1 - a'_2)m$ . Da  $\text{ggT}(m, m') = 1$  vorausgesetzt ist, ergibt der *Produkteilersatz* (Seite 23)  $a_1 \equiv a_2 \pmod{m}$  und  $a'_1 \equiv a'_2 \pmod{m'}$ . Definitionsgemäß gilt damit  $a_1 = a_2$  und  $a'_1 = a'_2$ . Wie bei a) folgt die Behauptung. □

### Satz über den ggT in Restklassen

Sind  $a, b \in \mathbb{Z}$  mit  $a \equiv b \pmod{m}$ , so gilt  $\text{ggT}(a, m) = \text{ggT}(b, m)$ .

**Beweis** (direkt, r1):

Da aufgrund des *Satzes über ein Kongruenzkriterium* (Seite 84) die Voraussetzung mit  $\text{mod}(a, m) = \text{mod}(b, m)$  äquivalent ist und weil  $b$  in der Form  $a + gm$  mit  $g \in \mathbb{Z}$  geschrieben werden kann, ergibt (2.3), dass  $\text{ggT}(a, m) = \text{ggT}(b, m)$  gilt. □

### Definition der primen Restklasse und Bezeichnung des reduzierten Restsystems

Eine Restklasse heißt *prim modulo m*, wenn alle ihre Elemente zu  $m$  teilerfremd sind.

Eine Menge  $\mathcal{R}_m^* \subset \mathbb{Z}$ , die aus jeder primen Restklasse genau eine Zahl enthält, heißt *reduziertes Restsystem modulo m*.<sup>2</sup>

Aufgrund des *Satzes über den ggT in Restklassen* ist  $\bar{a}$  genau dann eine prime Restklasse modulo  $m$ , wenn  $\text{ggT}(a, m) = 1$  gilt.

Für jedes  $m \in \mathbb{N}_1$  ist die Menge

---

<sup>2</sup> Reduzierte Restsysteme werden auch *prime Restsysteme* genannt. Um Verwechslungen zu vermeiden, gebrauchen wir diese Bezeichnung nicht.

$$\mathcal{A}_m^* := \{n \in \mathcal{A}_m ; \text{ggT}(n, m) = 1\}$$

als Teilmenge von  $\mathcal{A}_m$  ein reduziertes Restsystem, weil sie aus jeder primen Restklasse modulo  $m$  den kleinsten nichtnegativen Rest modulo  $m$  enthält. Wir werden diese Mengen als “reduzierte Standardrestsysteme” verwenden, so wie die Anfänge  $\mathcal{A}_m$  unter den vollständigen Restsystemen ausgezeichnet sind. Stellt  $\mathcal{R}_m^*$  ein beliebiges reduziertes Restsystem dar, so ist die Abbildung

$$(4.1) \quad \beta : \mathcal{R}_m^* \rightarrow \mathcal{A}_m^*, \quad r \mapsto \text{mod}(r, m),$$

bijektiv; denn einerseits ist  $\beta$  surjektiv, weil  $\mathcal{R}_m^*$  zu jedem  $a \in \mathcal{A}_m^*$  ein  $b$  mit  $a \equiv b \pmod{m}$  enthält, und andererseits ergibt der *Satz über ein Kongruenzkriterium* (Seite 84) die Injektivität von  $\beta$ .

Insbesondere gilt  $\text{card } \mathcal{R}_m^* = \text{card } \mathcal{A}_m^*$  für jedes reduzierte Restsystem  $\mathcal{R}_m^*$  modulo  $m$ . Da diese “invarianten Anzahlen” an vielen Stellen der Zahlentheorie eine Rolle spielen, hat die entsprechende Abbildung einen eigenen Namen:

### Bezeichnung der Eulerschen $\varphi$ -Funktion

Die Abbildung  $\varphi : \mathbb{N}_1 \rightarrow \mathbb{N}_1$ ,  $m \mapsto \text{card } \mathcal{A}_m^*$ , heißt *Eulersche  $\varphi$ -Funktion*.

Jedes reduzierte Restsystem modulo  $m$  enthält also  $\varphi(m)$  Elemente. Der folgende Satz ermöglicht unter anderem im nächsten Abschnitt die einfache Herleitung von zwei grundlegenden Eigenschaften der Eulerschen  $\varphi$ -Funktion.

### Satz über modifizierte reduzierte Restsysteme

- a) Ist  $\mathcal{R}_m^*$  ein reduziertes Restsystem modulo  $m$  und  $k \in \mathbb{Z}$  mit  $k \neq 0$  und  $\text{ggT}(k, m) = 1$ , so stellt  $\{c \in \mathbb{Z} ; \text{Es gibt } a \in \mathcal{R}_m^*, \text{ sodass } c = k a \text{ gilt}\}$  ein reduziertes Restsystem modulo  $m$  dar.
- b) Es sei  $m' \in \mathbb{N}_1$  mit  $\text{ggT}(m, m') = 1$ , und  $\mathcal{R}_{m'}^*$  sei ein reduziertes Restsystem modulo  $m'$ . Dann ist  $\{c \in \mathbb{Z} ; \text{Es gibt } a \in \mathcal{R}_m^* \text{ und } a' \in \mathcal{R}_{m'}^*, \text{ so dass } c = a' m + a m' \text{ gilt}\}$  ein reduziertes Restsystem modulo  $m m'$ .

**Beweis** (zwei Teile, direkt, i) r1, ii) r2):

Um möglichst viel von dem *Satz über modifizierte Restsysteme* (Seite 92) übernehmen zu können, erweitern wir die gegebenen reduzierten Restsysteme zu vollständigen Restsystemen; z. B. ist  $\mathcal{R} := \mathcal{R}_m^* \cup (\mathcal{A}_m \setminus \mathcal{A}_m^*)$  wegen der Bijektivität von  $\beta$  in (4.1) ein  $\mathcal{R}_m^*$  umfassendes vollständiges Restsystem modulo  $m$ .

Die beiden modifizierten reduzierten Restsysteme sind in den jeweiligen modifizierten vollständigen Restsystemen enthalten. Damit überträgt sich die paarweise Inkongruenz aller Elemente. Außerdem gibt es in den vollständigen Systemen jeweils genau ein reduziertes Restsystem. Deshalb ist nur noch zu zeigen, dass die Elemente der modifizierten reduzierten Restsysteme die Teilerfremdheitsbedingung erfüllen, die übrigen dagegen nicht.

**a)** Wie für (2.20) wird mit den entsprechenden Elementbezeichnungen gezeigt, dass mit  $a$  und  $k$  auch  $ka$  zu  $m$  teilerfremd ist. Aus  $\text{ggT}(a, m) > 1$  folgt, dass  $\text{ggT}(ka, m) > 1$  gilt.

**b)** Wird  $d := \text{ggT}(a'm + am', mm')$  gesetzt, so gilt  $d \mid (a'm + am')$  und  $d \mid mm'$ . Wegen  $\text{ggT}(m, m') = 1$  ist  $d$  Teiler von  $m$  oder von  $m'$ ; sei etwa  $d \mid m$ . Wegen  $d \mid (a'm + am')$  folgt  $d \mid am'$ , und der *Produktteilersatz* (Seite 23) ergibt  $d \mid m'$ , also  $d = 1$ . Analog verläuft der Beweis im Falle  $d \mid m'$ .

Ist  $\text{ggT}(a, m) > 1$  oder  $\text{ggT}(a', m') > 1$ , so gilt aufgrund des *Satzes über Teilbarkeitsregeln* (Seite 18) auch  $d > 1$ . □

Als Beispiel für die zweite Modifikation betrachten wir die reduzierten Standardsysteme  $\mathcal{A}_4^* = \{1, 3\}$  und  $\mathcal{A}_9^* = \{1, 2, 4, 5, 7, 8\}$ . Die Menge der Linearkombinationen ist dann  $\{1 \cdot 9 + 1 \cdot 4, \dots, 1 \cdot 9 + 8 \cdot 4, 3 \cdot 9 + 1 \cdot 4, \dots, 3 \cdot 9 + 8 \cdot 4\} = \{13, 17, 25, 29, 1, 5, 31, 35, 7, 11, 19, 23\}$ , und die zweite Menge stellt  $\mathcal{A}_{36}^*$  dar, weil es bei Mengen nicht auf die Reihenfolge der Elemente ankommt.

## Prime Restklassengruppen

Wenden wir im Falle  $\mathcal{R}_m^* = \mathcal{A}_m^*$  die erste Modifikation mit  $k = b \in \mathcal{A}_m^*$  an, so können wir die Abbildung

$$\boxtimes : \mathcal{A}_m^* \times \mathcal{A}_m^* \rightarrow \mathcal{A}_m^*, (a, b) \mapsto \text{mod}(ab, m),$$

als “multiplikative Verknüpfung” in  $\mathcal{A}_m^*$  ansehen.

Für  $m \in \mathbb{N}_2$  ist  $1 \in \mathcal{A}_m^*$ , und der **Satz über die lineare Kongruenz** (Seite 91) liefert für jedes  $a \in \mathcal{A}_m^*$  eine explizite Lösung  $x = (-1)^n Q_{n-1}$  der linearen Kongruenz  $ax \equiv 1 \pmod{m}$ . Da auch alle zu  $x$  modulo  $m$  kongruenten Zahlen die Kongruenz erfüllen, stellt  $\text{mod}(x, m)$  ebenfalls eine Lösung dar. Außerdem ist  $x$  und damit auch  $\text{mod}(x, m)$  teilerfremd zu  $m$ , weil andernfalls  $\text{ggT}(ax, m) > 1$  wäre. Also ist  $\text{mod}(x, m) \in \mathcal{A}_m^*$ , sodass in  $\mathcal{A}_m^*$  eine Reziprokenabbildung

$$\boxdot : \mathcal{A}_m^* \rightarrow \mathcal{A}_m^*, a \mapsto \text{mod}((-1)^n Q_{n-1}, m),$$

erklärt werden kann, mit der  $a(\boxplus a) \equiv 1 \pmod{m}$  für jedes  $a \in \mathcal{A}_m^*$  gilt. Damit ist

$$\mathbb{Z}_m^* := (\mathcal{A}_m^*, \boxplus, 1, \boxminus) \text{ für jedes } m \in \mathbb{N}_2$$

eine **abelsche Gruppe**.

Obwohl Gruppen in der elementaren Zahlentheorie eine untergeordnete Rolle spielen, sei hier die Definition in einer passenden Form wiedergegeben.

### Definition der (abelschen) Gruppe

Ein Viertupel  $(\mathcal{G}, \circ, n, ^{-})$  bestehend aus einer nichtleeren Menge  $\mathcal{G}$ , einer Verknüpfung  $\circ : \mathcal{G} \times \mathcal{G} \rightarrow \mathcal{G}$ ,  $(a, b) \mapsto a \circ b$ , einem ausgezeichneten (“neutralen”) Element  $n \in \mathcal{G}$  und einer (“Inversen-”) Abbildung  $^- : \mathcal{G} \rightarrow \mathcal{G}$ ,  $a \mapsto \bar{a}$ , heißt *Gruppe*, wenn für alle  $a, b, c \in \mathcal{G}$  gilt:

- i)  $(a \circ b) \circ c = a \circ (b \circ c)$  (Assoziativgesetz),
- ii)  $n \circ a = a$  (Eigenschaft des neutralen Elements),
- iii)  $\bar{a} \circ a = n$  (Eigenschaft der inversen Elemente).

Eine Gruppe heißt *abelsch*<sup>3</sup> (oder *kommutativ*), wenn außerdem

- iv)  $a \circ b = b \circ a$  (Kommutativgesetz)

für alle  $a, b \in \mathcal{G}$  erfüllt ist.

Betrachtet man anstelle der Elemente  $a$  von  $\mathcal{A}_m^*$  die zugehörigen Restklassen  $\bar{a}$  und definiert entsprechend unter Beachtung der Unabhängigkeit von der Auswahl der Repräsentanten die Verknüpfung  $\cdot$  sowie die Inversenabbildung  $/$ , so erhält man für jedes  $m \in \mathbb{N}_2$  die zu  $\mathbb{Z}_m^*$  isomorphe Gruppe  $(\mathbb{Z}/m\mathbb{Z})^*$ , die **prime Restklassengruppe modulo  $m$**  heißt.

Einige der folgenden Ergebnisse lassen sich gruppentheoretisch deuten oder als Spezialfälle gruppentheoretischer Sätze gewinnen. Wir werden nur dann darauf eingehen, wenn die gruppentheoretische Aussage eine eigenständige Bedeutung für die Zahlentheorie hat, wie z. B. bei den “Klassengruppen” in Kapitel 5 (Seite 159).

Die primen Restklassengruppen geben uns die Gelegenheit, in einem kurzen Ausblick die Ergebnisse zu skizzieren, durch die GAUß als 19-Jähriger berühmt wurde, nämlich die Konstruierbarkeit der regelmäßigen Vielecke und insbesondere die Konstruktion des regelmäßigen 17-Ecks, die dann in den fünf Jahre später erschienenen “Disquisitiones” [9] auf mehr als fünfzig Seiten im siebenten Abschnitt dargestellt wurden.

Die Konstruktion eines regelmäßigen  $m$ -Ecks für  $m \in \mathbb{N}_3$  kann in der komplexen Zahlenebene auf die Konstruktion der  **$m$ -ten Einheitswurzeln**

<sup>3</sup> Die Bezeichnung “abelsch” erfolgt zu Ehren des norwegischen Mathematikers NIELS HENRIK ABEL (1802-1829).

$\zeta^k$  mit  $\zeta := \cos\left(\frac{2\pi}{m}\right) + i \sin\left(\frac{2\pi}{m}\right)$  und  $k \in \mathcal{I}_{m-1}$  zurückgeführt werden, die “Eckpunkte” eines regelmäßigen  $m$ -Ecks sind.

Wesentlich sind dabei die **primitiven  $m$ -ten Einheitswurzeln**  $\zeta^k$  mit  $k \in \mathcal{A}_m^*$ . Sie bilden die Nullstellen des  **$m$ -ten Kreisteilungspolynoms**  $\Phi_m(x)$ , das ganzzahlige Koeffizienten hat und das irreduzibel ist (d. h. es lässt sich nicht als Produkt von nicht konstanten Polynomen mit rationalen Koeffizienten darstellen). Deshalb hat der  **$m$ -te Kreisteilungskörper**  $\mathbb{Q}(\zeta)$  (d. h. der kleinste Körper in  $\mathbb{C}$ , der  $\mathbb{Q}$  und  $\zeta$  enthält) über  $\mathbb{Q}$  den **Körpergrad**  $\varphi(m)$ .

Die Beschränkung auf die Zeichenwerkzeuge Lineal und Zirkel bedeutet, dass nur Punkte konstruiert werden können, die Schnittpunkte von ebenso konstruierbaren Geraden und Kreisen sind. Eine komplexe Zahl ist deshalb “konstruierbar”, wenn sie Lösung einer linearen oder quadratischen Gleichung ist, deren Koeffizienten Lösungen solcher Gleichungen sind.

Im Falle  $m = q \in \mathbb{P}_3$  mit  $\varphi(q) = 2^k$ ,  $k \in \mathbb{N}_1$ , gab GAUß die Kette der quadratischen Gleichungen für  $\zeta$  explizit an, indem er die Lösungen als Summen von  $\zeta$ -Potenzen darstellte. Diese Summen, die er “Perioden” nannte, gehen ineinander über, wenn  $\zeta$  durch eine andere primitive Einheitswurzel ersetzt wird. Solche “Substitutionen” von primitiven Einheitswurzeln bestimmen in eindeutiger Weise die **Automorphismen** (d. h. die strukturtreuen bijektiven Abbildungen) des Körpers  $\mathbb{Q}(\zeta)$ , die  $\mathbb{Q}$  elementweise festlassen. Diese Automorphismen bilden in heutiger Sprechweise die **Galois-Gruppe**<sup>4</sup> des entsprechenden Kreisteilungskörpers  $\mathbb{Q}(\zeta)$  über  $\mathbb{Q}$ .

Da GAUß einerseits das Konstruktionsproblem auf die Fälle zurückführen konnte, in denen  $m$  eine Primzahlpotenz ist, und da er andererseits zeigte, dass zu jedem ungeraden Primteiler  $p$  von  $\varphi(m)$  eine Gleichung vom Grad  $p$  in der Gleichungskette für  $\zeta$  auftritt, gewann er als notwendige und hinreichende Bedingung für die Konstruierbarkeit des regelmäßigen  $m$ -Ecks, dass  $\varphi(m)$  eine Potenz von 2 ist, was sich mit dem nächsten Satz als äquivalent zum **Theorem über regelmäßige Vielecke** (Seite 61) erweist.

Obwohl die Begriffe Gruppe und Körper erst später eingeführt wurden, schaffte GAUß mit seiner Methode die Grundlage für den Beweis des folgenden Theorems, das heute für die Herleitung des **Theorems über regelmäßige Vielecke** entscheidend ist.

### Theorem über Kreisteilungskörper

Die Galois-Gruppe des  $m$ -ten Kreisteilungskörpers über  $\mathbb{Q}$  ist isomorph zu  $(\mathbb{Z}/m\mathbb{Z})^*$ .

<sup>4</sup> Die Benennung erfolgt zu Ehren des französischen Mathematikers EVARISTE GALOIS (1811-1832).

## 4.5 Die Eulersche $\varphi$ -Funktion

### Satz über die Eulersche $\varphi$ -Funktion

- a) Für alle  $m, m' \in \mathbb{N}_1$  mit  $\text{ggT}(m, m') = 1$  ist  $\varphi(mm') = \varphi(m)\varphi(m')$ .
- b) Es gilt  $\varphi(m) = m \prod_{\substack{p \in \mathbb{P} \\ p|m}} \left(1 - \frac{1}{p}\right) = \sum_{d|m} \mu(d) \frac{m}{d}$  für alle  $m \in \mathbb{N}_2$ .

**Beweis** (direkt, r1):

a) Aufgrund des *Satzes über modifizierte reduzierte Restsysteme* (Seite 94) mit  $\mathcal{R}_m^* = \mathcal{A}_m^*$  und  $\mathcal{R}_{m'}^* = \mathcal{A}_{m'}^*$  ist  $\varphi(mm') = \text{card} \{c \in \mathbb{Z}; \text{Es gibt } a \in \mathcal{A}_m^* \text{ und } a' \in \mathcal{A}_{m'}^*, \text{ sodass } c = a'm + am' \text{ gilt}\} = \varphi(m)\varphi(m')$ .

b) Es sei  $m =: \prod_{\substack{p \in \mathbb{P} \\ p|m}} p^{e_p}$  mit  $e_p \in \mathbb{N}_1$ . Aus a) folgt mit finiter Induktion  $\varphi(m) =$

$\prod_{\substack{p \in \mathbb{P} \\ p|m}} \varphi(p^{e_p})$ . In dem Spezialfall  $m'' := p^{e_p}$  sind genau die  $\frac{m''}{p}$  Zahlen  $0, p, \dots, \frac{m''}{p} p - p$  aus  $\mathcal{A}_{m''}^*$  nicht zu  $m''$  teilerfremd.  $\mathcal{A}_{m''}^*$  enthält also  $p^{e_p} - p^{e_p-1} = \varphi(p^{e_p})$  Elemente.

Damit ergibt sich  $\varphi(m) = \prod_{\substack{p \in \mathbb{P} \\ p|m}} (p^{e_p} - p^{e_p-1}) = \prod_{\substack{p \in \mathbb{P} \\ p|m}} p^{e_p} \left(1 - \frac{1}{p}\right) = m \prod_{\substack{p \in \mathbb{P} \\ p|m}} \left(1 - \frac{1}{p}\right)$ .

Die Summendarstellung  $\prod_{\substack{p \in \mathbb{P} \\ p|m}} \left(1 - \frac{1}{p}\right) = \sum_{d|m} \frac{\mu(d)}{d}$  wurde für quadratfreies  $m \in \mathbb{N}_2$

mit vollständiger Induktion bereits im Beweis des zweiten Teils des *Satzes über  $\pi(x)$ -Abschätzungen* (Seite 67) hergeleitet. Wegen  $\mu(d) = 0$  für nicht quadratfreies  $d$  gilt diese Darstellung für alle  $m \in \mathbb{N}_2$ .  $\square$

Die folgenden beiden Sätze werden auch bei einigen zahlentheoretischen Problemen gebraucht. In vielen Lehrbüchern treten sie in umgekehrter Reihenfolge auf, weil der ältere Satz ein Spezialfall der 120 Jahre jüngeren Aussage ist. Im Hinblick auf das Problemlösen interessiert in diesem Falle auch die Beweisentwicklung. FERMAT fand keinen korrekten Beweis für den von ihm entdeckten Satz. Der heutige Beweis, der auch für den Mathematikunterricht geeignet wäre, stammt von EULER, der wiederum seine Verallgemeinerung nur recht mühsam mit Fallunterscheidung beweisen konnte. Die hier wiedergegebene Beweismethode wurde erst 1806 von dem englischen Mathematiker JAMES IVORY veröffentlicht.

Unabhängig von ihm wendete DIRICHLET 1828 die Beweisstrategie an, die wir im Anschluss an [13] bei dem Problemlösen *Invarianzstrategie* nennen wollen.

### Fermatscher Kongruenzsatz (1640)

Für alle  $(a, p) \in \mathbb{Z} \times \mathbb{P}$  ist  $a^p \equiv a \pmod{p}$ .

**Beweis** (Fallunterscheidung, vollständige Induktion, a1):

i) Für  $a \in \mathbb{N}_1$  wird die Aussage mit vollständiger Induktion gezeigt. Dazu sei  $\mathcal{M} := \{b \in \mathbb{N}_1 ; b^p \equiv b \pmod{p}\}$ . Wegen  $1^p \equiv 1 \pmod{p}$  gilt  $1 \in \mathcal{M}$ . Für beliebiges  $m \in \mathbb{R}$  ergibt die *Binomialformel* (3.23) zunächst  $(1+m)^p = \sum_{k=0}^p \binom{p}{k} m^k$ . Wegen  $\binom{p}{k} = \frac{p!}{k!(p-k)!}$  gilt  $k \binom{p}{k} = p \binom{p-1}{k-1}$  für jedes  $k \in \mathcal{I}_{p-1}$ . Mit dem *Produktteilersatz* (Seite 23) folgt  $p \mid \binom{p}{k}$ . Für  $m \in \mathcal{M}$  gilt nun  $(1+m)^p \equiv m^0 + m^p \equiv 1+m \pmod{p}$ , sodass auch  $m+1$  in  $\mathcal{M}$  liegt. Der *Induktionssatz* (Seite 12) ergibt damit  $\mathcal{M} = \mathbb{N}_1$ .

ii) Es sei  $a \in \mathbb{Z} \setminus \mathbb{N}$ , also  $-a \in \mathbb{N}_1$ . Im Falle  $p = 2$  ist  $-1 \equiv 1 \pmod{2}$ , sodass  $a^2 = (-a)^2 \equiv -a \equiv a \pmod{2}$  wegen i) gilt. Für  $p \in \mathbb{P}_3$  ergibt i) mit  $(-1)^p \equiv -1 \pmod{p}$  die Kongruenzkette  $a^p \equiv -(-a)^p \equiv -(-a) \equiv a \pmod{p}$ . Wegen  $0^p \equiv 0 \pmod{p}$  gilt der Satz auch für  $a = 0$ .  $\square$

### Kongruenzsatz von Euler (1760)

Für alle  $(a, m) \in \mathbb{Z} \times \mathbb{N}_1$  mit  $\text{ggT}(a, m) = 1$  gilt

$$(4.2) \quad a^{\varphi(m)} \equiv 1 \pmod{m}.$$

**Beweis** (direkt, a1):

Es sei  $n := \varphi(m)$  und  $\mathcal{A}_m^* := \{a_1, \dots, a_n\}$ . Aufgrund des *Satzes über modifizierte reduzierte Restsysteme* (Seite 94) ist auch  $\{aa_1, \dots, aa_n\}$  ein reduziertes Restsystem. Zu jedem  $i \in \mathcal{I}_n$  gibt es also genau ein  $j \in \mathcal{I}_n$  mit  $aa_j \equiv a_i \pmod{m}$ . Damit folgt  $\prod_{i=1}^n a_i \equiv \prod_{j=1}^n aa_j \equiv a^n \prod_{j=1}^n a_j \pmod{m}$ . Die Beweismethode von (2.20) ergibt mit vollständiger Induktion, dass  $\text{ggT}\left(\prod_{i=1}^n a_i, m\right) = 1$  ist. Der *Satz über Kongruenzkürzung* (Seite 91) liefert schließlich (4.2).  $\square$

## Anwendungen in der Kryptographie

Eine der wichtigsten Anwendungen der elementaren Zahlentheorie in der gegenwärtigen Informationsgesellschaft bildet die Verschlüsselung von Daten mit einem öffentlichen Schlüssel und einem geheimen - aber flexibel variierbaren - Code (“public-key secret code”). Die verbreitetste Methode stammt von den amerikanischen Mathematikern R. L. RIVEST, A. SHAMIR und L. ADLEMAN. Sie heißt deshalb **RSA-Verfahren**. Der mathematische Hintergrund wird mit dem letzten der folgenden drei Schritte klar.

i) Der “Entschlüsseler” (Empfänger, z. B. eine Bankzentrale) gibt zwei (Schlüssel-) Zahlen  $m, s \in \mathbb{N}_2$  bekannt, wobei  $m$  das Produkt von zwei sehr großen (mindestens 100-stelligen) Primzahlen und  $s \in \mathcal{A}_{\varphi(m)}^*$  ist.

ii) Der “Verschlüsseler” (Sender) stellt seine Nachricht in der Form von natürlichen Zahlen  $a \in \mathbb{N}_2$  etwa mit  $a < 10^{100}$  dar. Dann berechnet er  $r := a^s \pmod{m}$  und sendet die Zahl  $r$ .

iii) Der Empfänger hat eine geheime Zahl  $t \in \mathbb{N}_2$ , die  $st \equiv 1 \pmod{\varphi(m)}$  erfüllt. Damit gewinnt er  $a$  in der Form  $a \equiv r^t \pmod{m}$ , weil mit  $n := \frac{st-1}{\varphi(m)}$  und mit dem **Kongruenzsatz von Euler** die Kongruenzkette  $r^t \equiv (a^s)^t \equiv a^{st} \equiv a^1 (a^{\varphi(m)})^n \equiv a \cdot 1^n \equiv a \pmod{m}$  gilt.

Die Sicherheit des RSA-Verfahrens beruht darauf, dass es effiziente Verfahren gibt, mit denen festgestellt werden kann, ob eine gegebene Zahl mit mehreren hundert Stellen eine Primzahl ist. Dagegen würde es mit den heute bekannten oder in den nächsten Jahrzehnten zu erwartenden Methoden “astronomische” Zeiten dauern, die Primfaktoren von  $m$  zu bestimmen. Diese Primzahlen werden aber benötigt, um zuerst  $\varphi(m)$  und dann  $t$  zu berechnen.

Die Potenzen  $a^s$  und  $r^t$  werden zweckmäßig mit Hilfe der 2-adischen Darstellung der Exponenten bestimmt. Zum Beispiel für  $s = 23 = (10111)_2$  ergibt sich durch Klammerung  $2^4 + 2^2 + 2 + 1 = (((2+0)2+1)2+1)2+1$ , sodass  $a^{23} = \left( \left( (a^2 a^0)^2 a^1 \right)^2 a^1 \right)^2 a^1$  von innen nach außen durch die Potenzen  $a^2, a^4, a^5, a^{10}, a^{11}, a^{22}, a^{23}$  gewonnen wird. Im Falle der obigen Kongruenzen modulo  $m$  brauchen aufgrund des **Satzes über Kongruenzregeln** (Seite 87) auch alle Zwischenpotenzen nur modulo  $m$  berechnet zu werden.

Eine weitere Anwendung der elementaren Zahlentheorie in der Kryptographie verwendet “Quadratwurzeln modulo  $m$ ”, wobei  $b \in \mathcal{A}_m^*$  **Quadratwurzel modulo  $m$**  von  $a \in \mathcal{A}_m^*$  heißt, wenn  $a \equiv b^2 \pmod{m}$  gilt. Im Fall von Moduln  $m$  mit zwei großen Primfaktoren kann  $b$  nur dann effizient berechnet werden, wenn die Primteiler von  $m$  bekannt sind. Der darauf beruhende **Fiat-Shamir-Algorithmus** wird z. B. bei der Identifikation von Personen mit Hilfe von Chip-Karten genutzt.

## 4.6 Kongruenzen mit einer Unbekannten

### Bezeichnung des Grades eines Polynoms, der Wurzel einer Kongruenz und der Anzahl der Lösungen modulo $m$

Es sei  $f(x) = \sum_{k=0}^n c_k x^k$  mit  $n \in \mathbb{N}_1$  und  $c_k \in \mathbb{Z}$  für  $k = 0, \dots, n$ .

a) Falls es ein  $k \in \mathcal{A}_{n+1}$  mit  $m \nmid c_k$  gibt, wird  $g := \max \{k \in \mathcal{A}_{n+1} ; m \nmid c_k\}$  Grad des Polynoms  $f(x)$  modulo  $m$  genannt.

b) Eine Zahl  $a \in \mathbb{Z}$  heißt Lösung oder Wurzel der Kongruenz  $f(x) \equiv 0 \pmod{m}$ , wenn  $f(a) \equiv 0 \pmod{m}$  gilt. (Aufgrund des Satzes über Kongruenzregeln (Seite 87) sind dann auch alle  $b \in \bar{a}$  Lösungen der Kongruenz.)

c) Ist  $\mathcal{R}_m$  ein vollständiges Restsystem modulo  $m$ , so wird die von  $\mathcal{R}_m$  unabhängige Zahl  $\text{card} \{a \in \mathcal{R}_m ; f(a) \equiv 0 \pmod{m}\}$  als Anzahl der Lösungen der Kongruenz  $f(x) \equiv 0 \pmod{m}$  bezeichnet.

Zum Beispiel hat  $x^2 \equiv 1 \pmod{8}$  vier Lösungen, weil die Zahlen 1, 3, 5, 7 aus  $\mathcal{A}_8$  der Kongruenz genügen, die übrigen Zahlen 0, 2, 4, 6 aber nicht.

Der folgende Satz, der eine Fortsetzung des Satzes über die lineare Kongruenz (Seite 91) darstellt, enthält eine der wenigen genauen Lösungsanzahlen von Polynomkongruenzen.

### Satz über die Lösungsanzahl der linearen Kongruenz

Sind  $a, m \in \mathbb{N}_1$ ,  $b \in \mathbb{Z}$  und  $d := \text{ggT}(a, m)$ , so besitzt die Kongruenz  $ax \equiv b \pmod{m}$  keine Lösung, wenn  $d \nmid b$  gilt. Ist  $d$  Teiler von  $b$ , so hat die Kongruenz genau  $d$  Lösungen, die alle zu einer bestimmten Restklasse modulo  $\frac{m}{d}$  gehören.

**Beweis** (Fallunterscheidung, direkter und indirekter Schluss, r1):

i) Zunächst sei  $d = 1$ . Ist  $\mathcal{R}_m$  ein beliebiges vollständiges Restsystem modulo  $m$ , so stellt  $\{ax - b ; x \in \mathcal{R}_m\}$  aufgrund des Satzes über modifizierte Restsysteme (Seite 92) ein vollständiges Restsystem dar. Also gibt es genau ein  $x_0 \in \mathcal{R}_m$  mit  $ax_0 \equiv b \pmod{m}$ . Damit hat die Kongruenz genau eine Lösung.

ii) Es sei  $d > 1$ . Ist die Kongruenz lösbar, so folgt  $d \mid b$  aus  $d \mid a$  und  $d \mid m$ . Im Falle  $d \nmid b$  hat also die Kongruenz keine Lösung.

Nun sei  $d$  ein Teiler von  $b$  und es werde  $a =: a_1 d$ ,  $m =: m_1 d$ ,  $b =: b_1 d$  gesetzt. Dann ist  $\text{ggT}(a_1, m_1) = 1$ , und der *Satz über Kongruenzkürzung* (Seite 91) ergibt, dass aus  $a x \equiv b \pmod{m}$  die Kongruenz  $a_1 x \equiv b_1 \pmod{m_1}$  folgt, die nach i) genau eine Lösung  $x_1$  modulo  $m_1$  besitzt. Alle Zahlen, die Lösungen von  $a x \equiv b \pmod{m}$  sind, genügen also der Kongruenz  $x \equiv x_1 \pmod{m_1}$ . Modulo  $m$  ergeben sich damit die  $d$  inkongruenten Lösungen  $x_1, x_1 + m_1, \dots, x_1 + (d-1)m_1$ .  $\square$

Im Zusammenhang mit dem letzten Satz spielen die folgenden beiden Begriffe bei einigen Herleitungen von Sätzen und bei Lösungen von Problemen eine wichtige methodische Rolle, wenn alle Elemente von  $\mathcal{A}_m^*$  für  $m \in \mathbb{P}_3$  "gleichberechtigt" verknüpft sind - wie z. B. im ersten Teil des nächsten Satzes.

### Definition des reziproken Restes und der Assoziiiertheit

Es sei  $(a, m) \in \mathbb{Z} \times \mathbb{N}_2$  mit  $\text{ggT}(a, m) = 1$ . Eine Zahl  $a' \in \mathbb{Z}$  heißt zu  $a$  *reziproker Rest modulo  $m$* , wenn  $a a' \equiv 1 \pmod{m}$  gilt. Ist ein reduziertes Restsystem  $\mathcal{R}_m$  vorgegeben, so wird anstelle des eindeutig bestimmten  $a' \in \mathcal{R}_m$  auch  $a^{-1}$  oder  $\frac{1}{a}$  geschrieben.

Zwei Zahlen  $a, a' \in \mathbb{Z}$  mit  $\text{ggT}(a a', m) = 1$  heißen *assoziiert modulo  $m$* , wenn sie  $a a' \equiv 1 \pmod{m}$  erfüllen.

Obwohl der folgende Satz nur für Primzahlen gilt, stellt er doch wegen des starken Wachsens der linken Seiten kein sinnvolles Primzahlkriterium dar. Den zweiten Teil werden wir zum Beweis des *Zweiquadratesatzes* von EULER (Seite 141) verwenden.

### Wilsonscher Fakultätensatz <sup>5</sup>

Für ungerade Primzahlen  $p$  und nur für Primzahlen  $p$  gilt

- a)  $(p-1)! \equiv -1 \pmod{p}$  und
- b)  $\left(\left(\frac{p-1}{2}\right)!\right)^2 \equiv (-1)^{\frac{p+1}{2}} \pmod{p}$ .

<sup>5</sup> Der nach SIR JOHN WILSON (1741-1793) benannte *Wilsonsche Satz* wurde zuerst 1770 von dem in Cambridge wirkenden Mathematiker EDWARD WARING (1734-1798) veröffentlicht.

**Beweis** (Fallunterscheidung und indirekte Schlüsse, a1):

i) Es sei  $p \in \mathbb{P}$ . Für  $p = 2$  ist  $1 \equiv -1 \pmod{2}$  bei i). Ist  $p = 3$ , so gilt  $2 \equiv -1 \pmod{3}$  bei i) und  $1 \equiv 1 \pmod{3}$  bei ii).

a) Für  $p \in \mathbb{P}_5$  setzen wir  $\mathcal{C} := \{2, \dots, p-2\}$ . Zu jedem  $x \in \mathcal{C}$  gibt es aufgrund des *Satzes über die Lösungsanzahl der linearen Kongruenz* (Seite 101) genau ein  $x' \in \mathcal{A}_p = \mathcal{C} \cup \{0, 1, p-1\}$  mit  $xx' \equiv 1 \pmod{p}$ .

Die Zahlen 0, 1 und  $p-1$  können nicht als  $x'$  auftreten, weil  $x \cdot 0 = 0 \not\equiv 1 \pmod{p}$ ,  $x \cdot 1 = x \not\equiv 1 \pmod{p}$  und  $x(p-1) \equiv -x \not\equiv 1 \pmod{p}$ . Also ist  $x' \in \mathcal{C}$ . Außerdem kann nicht  $x = x'$  sein, weil sonst  $x^2 \equiv 1 \pmod{p}$  die Teilbarkeit von  $x^2 - 1 = (x-1)(x+1)$  durch  $p$  zur Folge hätte. Aufgrund des *Produktteilersatzes* (Seite 23) wäre dann  $x \equiv 1 \pmod{p}$  oder  $x \equiv -1 \pmod{p}$  im Widerspruch zu  $1 \notin \mathcal{C}$  und  $p-1 \notin \mathcal{C}$ . Zu jedem  $x \in \mathcal{C}$  gibt es also genau ein  $x' \in \mathcal{C} \setminus \{x\}$  mit  $xx' \equiv 1 \pmod{p}$ , d. h. die Zahlen aus  $\mathcal{C}$  zerfallen in  $\frac{p-3}{2}$  Paare von assoziierten Zahlen. Damit gilt die Kongruenzkette  $(p-1)! \equiv 1 \cdot \left(\prod_{x \in \mathcal{C}} x\right) (p-1) \equiv 1 \cdot \frac{p-1}{2} \cdot (-1) \equiv -1 \pmod{p}$ .

b) Für  $p \in \mathbb{P}_5$  setzen wir  $k := \frac{p-1}{2}$ . Dann ist die Menge der modulo  $p$  absolut kleinsten Reste  $\{-k, \dots, -1, 0, 1, \dots, k\}$  ein vollständiges Restsystem modulo  $p$ . Aus a) i) folgt  $-1 \equiv (p-1)! \equiv (-k) \cdots (-1) \cdot 1 \cdots k \equiv (-1)^k (k!)^2 \pmod{p}$ , also  $(k!)^2 \equiv (-1)^{k+1} \pmod{p}$ .

ii) Ist  $m \in \mathbb{N}_2 \setminus \mathbb{P}$ , so gibt es aufgrund des *Satzes über ein Primzahlkriterium* (Seite 63) ein  $d \in \mathbb{N}_2$  mit  $d \mid m$  und  $d \leq \sqrt{m} \leq \frac{m}{2}$ . Damit gilt  $d \mid \left[\frac{m}{2}\right]!$  und erst recht  $d \mid (m-1)!$ . Also folgt für ungerades  $m$ , dass  $d$  und damit auch  $m$  bei

ii) nicht Teiler von  $\left(\left(\left(\frac{m-1}{2}\right)!\right)^2 \pm 1\right)$  ist. Entsprechend ergibt sich bei a), dass  $m \nmid ((m-1)! + 1)$  gilt. □

Der folgende Satz ermöglicht Koeffizientenvergleich bei Polynomen modulo  $p$ .

### Polynomkongruenzsatz von Lagrange <sup>6</sup>

a) Ist  $g$  der Grad modulo  $p$  des Polynoms  $f(x) = \sum_{i=0}^n c_i x^i$ ,  $c_i \in \mathbb{Z}$ , so besitzt die Kongruenz

<sup>6</sup> JOSEPH LOUIS LAGRANGE (1736-1813) wirkte in Turin, Berlin und Paris.

$$(4.3) \quad f(x) \equiv 0 \pmod{p}$$

höchstens  $g$  Lösungen.

b) Hat die Kongruenz (4.3) mehr als  $n$  Lösungen, so sind alle Koeffizienten von  $f(x)$  durch  $p$  teilbar.

**Beweis** (Vollständige Induktion und indirekter Schluss, r2):

Es genügt den Fall  $g = n$  zu betrachten, weil  $p \mid c_i$  für  $i > g$  gilt. Dann sind die Aussagen a) und b) äquivalent.

Es sei  $\mathcal{M} := \{n \in \mathbb{N}_1; \text{Für alle Polynome mit dem Grad } n \text{ modulo } p \text{ gilt i)}\}$ . Aufgrund des *Satzes über die Lösungsanzahl der linearen Kongruenz* (Seite 101) ist  $1 \in \mathcal{M}$ .

Für  $m \in \mathcal{M}$  sei  $f(x)$  ein Polynom mit dem Grad  $m + 1$  modulo  $p$ . Wir nehmen an, dass die Kongruenz (4.3)  $m + 1$  modulo  $p$  inkongruente Lösungen  $x_0, \dots, x_{m+1}$

besitzt. Es gilt  $f(x) - f(x_0) = \sum_{i=1}^{m+1} c_i (x^i - x_0^i) = (x - x_0) \sum_{i=1}^{m+1} c_i \sum_{j=0}^{i-1} x^j x_0^{i-1-j}$  für

alle  $x \in \mathbb{Z} \setminus \{x_0\}$ . Setzen wir  $h(x) := \sum_{i=1}^{m+1} c_i \sum_{j=0}^{i-1} x^j x_0^{i-1-j} =: \sum_{j=0}^m b_j x^j$ , so ist

$f(x) - f(x_0) = (x - x_0) h(x)$  für jedes  $x \in \mathbb{Z}$  erfüllt. Wegen  $b_m = c_{m+1}$  teilt  $p$  nicht  $b_m$ , d. h.  $h(x)$  hat modulo  $p$  den Grad  $m$ .

Für  $k = 1, \dots, m + 1$  gilt aber  $(x_k - x_0) h(x_k) \equiv f(x_k) - f(x_0) \equiv 0 - 0 \equiv 0 \pmod{p}$ . Aufgrund des *Produktteilersatzes* (Seite 23) folgt dann, dass  $h(x)$  modulo  $p$  die  $m + 1$  Lösungen  $x_1, \dots, x_{m+1}$  besitzt - im Widerspruch zur Induktionsvoraussetzung. Also ist auch  $m + 1 \in \mathcal{M}$ . Damit gilt  $\mathcal{M} = \mathbb{N}_1$ .  $\square$

Neben den Polynomkongruenzen spielen Systeme von Kongruenzen ersten Grades sowohl theoretisch als auch praktisch eine Rolle. Die Problemstellung des folgenden Satzes trat vermutlich schon vor mehr als zweitausend Jahren bei astronomischen Berechnungen auf. Die erste bekannte Quelle, die auch die heutige Lösungsmethode an Beispielen aufzeigte, ist ein wahrscheinlich zwischen 280 und 473 n. Chr. entstandenes Werk des chinesischen Mathematikers SUN-TSU. Daher hat der Satz seinen Namen.

### Chinesischer Restsatz

Für  $k \in \mathbb{N}_2$  seien  $m_1, \dots, m_k \in \mathbb{N}_2$  paarweise teilerfremd, und

$$(4.4) \quad x \equiv b_i \pmod{m_i} \text{ mit } b_i \in \mathbb{Z}, i = 1, \dots, k,$$

sei ein Kongruenzsystem. Werden  $m, M_i, M'_i$  und  $x_0$  durch  $m := \prod_{i=1}^k m_i$ ,  $M_i := \frac{m}{m_i}$ ,  $M_i M'_i \equiv 1 \pmod{m_i}$  und  $x_0 := \sum_{i=1}^k M_i M'_i b_i$  definiert, so ist  $x \in \mathbb{Z}$  genau dann Lösung von (4.4), wenn  $x \equiv x_0 \pmod{m}$  gilt.

**Beweis** (direkt, r1):

Da  $\text{ggT}(M_i, m_i) = 1$  gilt, ist  $M'_i$  modulo  $m_i$  eindeutig bestimmt. Wegen  $m_i \mid M_j$  für jedes  $j \in \mathcal{I}_k \setminus \{i\}$  folgt  $x_0 \equiv M_i M'_i b_i + \sum_{\substack{j=1 \\ j \neq i}}^k M_j M'_j b_j \equiv b_i \pmod{m_i}$ .

Stellt  $y$  eine beliebige Lösung von (4.4) dar, so gilt  $y \equiv b_i \equiv x_0 \pmod{m_i}$  für  $i = 1, \dots, k$ . Da die Zahlen  $m_i$  paarweise teilerfremd sind, ergibt der *Satz über Kongruenzzusammenfassung* (Seite 92)  $y \equiv x_0 \pmod{m}$ , d. h. die Lösung  $x_0$  ist modulo  $m$  eindeutig. □

Als Beispiel betrachten wir das Kongruenzsystem

$$5x \equiv -1 \pmod{8}, \quad x \equiv 1 \pmod{15}, \quad 3x \equiv 13 \pmod{20},$$

das in zweifacher Hinsicht nicht die Voraussetzungen des *chinesischen Restsatzes* erfüllt: Einerseits sind nicht alle Koeffizienten von  $x$  gleich 1, und andererseits haben zwei Modulpaare gemeinsame Teiler größer als 1. Der erste Mangel lässt sich stets beheben, indem beide Seiten der jeweiligen Kongruenz - eventuell nach Anwendung des *Satzes über Kongruenzkürzung* (Seite 91) - mit dem reziproken Rest des betreffenden Koeffizienten multipliziert werden.

Da die erste Kongruenz zu  $5x \equiv 15 \pmod{8}$  äquivalent ist, liefert der *Satz über Kongruenzkürzung* die gleichwertige Kongruenz  $x \equiv 3 \pmod{8}$ . Zu der dritten Kongruenz ergibt Multiplikation mit dem reziproken Rest 7 modulo 20 die äquivalente Kongruenz  $x \equiv 11 \pmod{20}$ .

Aufgrund des *Satzes über Kongruenzvergrößerung* (Seite 91) und des *Satzes über Kongruenzzusammenfassung* (Seite 92) haben die drei resultierenden Kongruenzen dieselben Lösungen wie das Kongruenzsystem

$$x \equiv 3 \pmod{8}, \quad x \equiv 11 \equiv 1 \pmod{5}, \quad x \equiv 1 \pmod{3}, \quad x \equiv 11 \equiv 3 \pmod{4}.$$

Wenn  $x \equiv 3 \pmod{8}$  erfüllt ist, gilt auch  $x \equiv 3 \pmod{4}$ . Damit ist  $m_1 = 8$ ,  $m_2 = 5$ ,  $m_3 = 3$ ,  $m = 120$ ,  $M_1 = 15$ ,  $M'_1 \equiv 7 \pmod{8}$ ,  $M_2 = 24$ ,  $M'_2 \equiv 4 \pmod{5}$ ,  $M_3 = 40$ ,  $M'_3 \equiv 1 \pmod{3}$  und  $x_0 = 15 \cdot 7 \cdot 3 + 24 \cdot 4 \cdot 1 + 40 \cdot 1 \cdot 1 = 451$ . Also ist  $x \in \mathbb{Z}$  genau dann eine Lösung des Ausgangssystems, wenn  $x \equiv 451 \equiv 91 \pmod{120}$  gilt.

## 4.7 Potenzreste

Ein großer Teil der grundlegenden Ergebnisse über die speziellen Polynomkongruenzen  $x^n - a \equiv 0 \pmod{p}$  wurde zum ersten Mal von GAUß in [9] im dritten Abschnitt mit dem Titel “Von den Potenzresten” und im vierten Abschnitt über Kongruenzen zweiten Grades dargestellt. Wir behandeln zunächst die “quadratische” Theorie, weil sie weitgehend abgeschlossen ist. Außerdem spielen einige ihrer Resultate und Methoden auch beim Problemlösen eine Rolle.

### Definition des Potenzrestes und des Potenznichtrestes

Es seien  $m, n \in \mathbb{N}_2$ . Eine Zahl  $a \in \mathbb{Z}$  mit  $\text{ggT}(a, m) = 1$  heißt *n-ter Potenzrest modulo m*, wenn es ein  $x \in \mathbb{Z}$  gibt, sodass  $x^n \equiv a \pmod{m}$  gilt. Andernfalls heißt  $a$  *n-ter Potenznichtrest modulo m*.

Insbesondere spricht man für  $n = 2$  von quadratischen, für  $n = 3$  von kubischen und für  $n = 4$  von biquadratischen Resten bzw. Nichtresten.

Hat  $m$  die *Primpotenzdarstellung*  $m = \prod_{k=1}^r q_k^{e_k}$ , so ergeben der *Satz über Kongruenzvergrößerung* (Seite 91) und der *Satz über Kongruenzzusammenfassung* (Seite 92), dass  $f(x) \equiv 0 \pmod{m}$  genau dann gilt, wenn  $f(x) \equiv 0 \pmod{q_k^{e_k}}$  für  $k = 1, \dots, r$  erfüllt ist.

Bei Potenzresten kann der Exponent  $e_k$  für  $q_k = 2$  mindestens auf 3 und für  $q_k \in \mathbb{P}_3$  auf 1 erniedrigt werden. Die Beweismethode des folgenden Satzes über quadratische Reste lässt sich auch bei den übrigen Potenzresten und sogar bei  $f(x)$  mit Fallunterscheidung bezüglich  $f'(x)$  anwenden. Weitere Ergebnisse über Potenzreste höheren als zweiten Grades erhalten wir mit Hilfe von “Indizes” im nächsten Abschnitt.

### Satz über Modulareduktion

Es sei  $k \in \mathbb{N}_1$  und  $p \in \mathbb{P}_3$ . Die Zahl  $a \in \mathbb{Z}$  ist genau dann quadratischer Rest modulo  $2^k$ , wenn  $a \equiv 1 \pmod{2^{\min\{3, k\}}}$  gilt.

Genau dann stellt  $a$  einen quadratischen Rest modulo  $p^k$  dar, wenn  $a$  quadratischer Rest modulo  $p$  ist.

**Beweis** (direkt und vollständige Induktion, r1):

Es ist  $1^2 \equiv 3^2 \equiv 5^2 \equiv 7^2 \equiv 1 \pmod{8}$ . Also sind die Zahlen  $a \in \mathbb{Z}$  mit  $a \equiv 1 \pmod{8}$  die einzigen quadratischen Reste modulo 8. Aufgrund des *Satzes über Kongruenzvergrößerung* (Seite 91) gelten die entsprechenden Kongruenzbedingungen auch modulo 2 und 4. Derselbe Satz liefert außerdem alle Schlüsse von Potenzmoduln mit größeren Exponenten auf solche mit kleineren.

Für den Nachweis der entgegengesetzten Schlussrichtung mit vollständiger Induktion sei  $q \in \mathbb{P}$ ,  $b := 3$  für  $q = 2$ ,  $b := 1$  für  $q \in \mathbb{P}_3$  und  $\mathcal{M}_{q,a} := \{k \in \mathbb{N}_b; a \text{ ist quadratischer Rest modulo } q^k\}$ , wobei  $a$  einen quadratischen Rest modulo  $q^b$  darstellt, womit sich zugleich der Induktionsanfang  $b \in \mathcal{M}_{q,a}$  ergibt. Ist  $m \in \mathcal{M}_{q,a}$ , so existiert ein  $x \in \mathbb{Z}$  mit  $q \nmid x$  und  $x^2 \equiv a \pmod{q^m}$ . Wir bestimmen ein  $s \in \mathbb{Q}$  derart, dass  $y := x + s q^m \in \mathbb{Z}$  die Kongruenz  $y^2 \equiv a \pmod{q^{m+1}}$  erfüllt.

Mit  $u := \frac{x^2 - a}{q^m}$  gilt zunächst

$$\begin{aligned} y^2 &= (x + s q^m)^2 = x^2 + 2 x s q^m + s^2 q^{2m} \\ &= a + u q^m + 2 x s q^m + s^2 q^{2m} = a + (u + 2 x s) q^m + s^2 q^{2m}. \end{aligned}$$

Im Falle  $q \in \mathbb{P}_3$  ergibt der *Satz über die lineare diophantische Gleichung* (Seite 28) mindestens ein Paar  $(s, t) \in \mathbb{Z}^2$  mit  $q t - 2 x s = u$ . Wegen  $m \in \mathbb{N}_1$  ist  $2 m \geq m + 1$ , und es folgt  $y^2 = a + t q^{m+1} + s^2 q^{2m} \equiv a \pmod{q^{m+1}}$ .

Für  $q = 2$  setzen wir  $s := \frac{u}{2}$  und  $t := u \frac{x+1}{2}$ . Dann ist  $t \in \mathbb{Z}$ ,  $u + 2 x s = 2 t$  und  $s^2 2^{2m} = u^2 2^{2m-2}$ . Wegen  $m \in \mathbb{N}_3$  gilt  $2 m - 2 \geq m + 1$ , sodass sich hier  $y^2 = a + t 2^{m+1} + u^2 2^{2m-2} \equiv a \pmod{2^{m+1}}$  ergibt. Damit ist in beiden Fällen  $m + 1 \in \mathcal{M}_{q,a}$ , und es folgt  $\mathcal{M}_{q,a} = \mathbb{N}_b$ .  $\square$

Das folgende Symbol, das 1798 eingeführt wurde, ermöglicht gegenüber [9] eine erheblich einfachere Darstellung der Ergebnisse über quadratische Reste und Nichtreste. Wegen der obigen Reduktion sei im Rest dieses Abschnitts  $p \in \mathbb{P}_3$ .

### Bezeichnung des Legendre-Symbols <sup>7</sup>

Für  $(a, p) \in \mathbb{Z} \times \mathbb{P}_3$  mit  $p \nmid a$  wird

$$\left(\frac{a}{p}\right) := \begin{cases} 1, & \text{wenn } a \text{ einen quadratischen Rest modulo } p \text{ darstellt, und} \\ -1, & \text{wenn } a \text{ quadratischer Nichtrest modulo } p \text{ ist,} \end{cases}$$

gesetzt. (Das Symbol liest man “ $a$  nach  $p$ ”.)

Im Falle  $p \mid a$  wird  $\left(\frac{a}{p}\right) := 0$  definiert.

Mit Hilfe einer Reihe von Regeln, die wir im Folgenden herleiten, lässt sich das Legendre-Symbol effizient berechnen, ohne dass nach einer Lösung der entsprechenden quadratischen Kongruenz gesucht werden muss. Wie auf Seite 100 schon erwähnt wurde, ist es viel schwieriger, für quadratische Reste  $a$  eine Lösung  $x$  der Kongruenz  $x^2 \equiv a \pmod{m}$  zu bestimmen.

Die erste Regel ergibt sich unmittelbar aus der Definition des Legendre-Symbols und aus der *Transitivität der Kongruenzrelation* (Seite 83). Sind  $a, b \in \mathbb{Z}$  mit  $a \equiv b \pmod{p}$ , so gilt  $p \mid a$  genau dann, wenn  $p \mid b$  erfüllt ist, und zu  $a$  gibt es genau dann ein  $x \in \mathbb{Z}$  mit  $x^2 \equiv a \pmod{p}$ , wenn dieses für  $b$  der Fall ist. Also gilt

$$(4.5) \quad \left(\frac{a}{p}\right) = \left(\frac{b}{p}\right) \text{ für alle } a, b \in \mathbb{Z} \text{ mit } a \equiv b \pmod{p}.$$

Am Anfang des Beweises für den *Satz über Modulreduktion* (Seite 107) haben wir gesehen, dass es modulo 8 nur einen quadratischen Rest aber 3 Nichtreste gibt. Der folgende Satz zeigt, dass diese Anzahlen bei ungeraden Primzahlmoduln gleich sind.

### Satz über die Anzahl quadratischer Reste

Ist  $\mathcal{R}_p^*$  ein reduziertes Restsystem modulo  $p$ , so gilt

$$\text{card} \left\{ a \in \mathcal{R}_p^*; \left(\frac{a}{p}\right) = 1 \right\} = \text{card} \left\{ b \in \mathcal{R}_p^*; \left(\frac{b}{p}\right) = -1 \right\} = \frac{p-1}{2}.$$

Die  $\frac{p-1}{2}$  Klassen der quadratischen Reste werden durch die Zahlen  $1^2, \dots, \left(\frac{p-1}{2}\right)^2$  repräsentiert.

<sup>7</sup> ADRIEN MARIE LEGENDRE (1752-1833) wirkte in Paris.

**Beweis** (direkt, r1):

Wenn  $x^2 \equiv a \pmod{p}$  lösbar ist, so gibt es wegen  $p \nmid a$  auch mindestens eine Lösung  $x \in \mathcal{A}_p^*$ , aufgrund des *Polynomkongruenzsatzes von Lagrange* (Seite 103) aber höchstens zwei solche. Wegen  $(p-x)^2 \equiv (-x)^2 \equiv x^2 \pmod{p}$  gibt es also jeweils eine Lösung  $x \in \left\{1, \dots, \frac{p-1}{2}\right\}$ , zu der eine zweite Lösung  $p-x$  aus  $\mathcal{A}_p^* \setminus \left\{1, \dots, \frac{p-1}{2}\right\}$  gehört. Damit gibt es modulo  $p$  keine weiteren quadratischen Reste, und je zwei der Zahlen  $1^2, \dots, \left(\frac{p-1}{2}\right)^2$  sind modulo  $p$  inkongruent.  $\square$

In vielen Zahlentheorielehrbüchern wird das Legendre-Symbol durch die in dem folgenden Satz wiedergegebene Resteigenschaft von  $a^{\frac{p-1}{2}}$  modulo  $p$  eingeführt. Dann ist dieses “*Euler-Kriterium*” grundlegend für die Theorie der quadratischen Reste. Aber auch bei dem hier gewählten Aufbau hat das Kriterium etliche Anwendungen - besonders in Aufgaben und Problemen.

### Satz über das Euler-Kriterium

Für alle  $(a, p) \in \mathbb{Z} \times \mathbb{P}_3$  mit  $p \nmid a$  gilt  $a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \pmod{p}$ .

**Beweis** (Fallunterscheidung, direkt und indirekt, a1):

Der *Fermatsche Kongruenzsatz* (Seite 99) ergibt  $p \mid \left(a^{\frac{p-1}{2}} - 1\right)\left(a^{\frac{p-1}{2}} + 1\right)$ . Aufgrund des *Produktteilersatzes* (Seite 23) teilt  $p$  mindestens einen der Faktoren. Da die Differenz der beiden Zahlen in den Klammern 2 ist und  $p > 2$  gilt, ist  $p$  entweder Teiler von  $a^{\frac{p-1}{2}} - 1$  oder von  $a^{\frac{p-1}{2}} + 1$ .

i) Ist  $\left(\frac{a}{p}\right) = 1$ , so gibt es ein  $x \in \mathbb{Z}$  mit  $p \nmid x$  und mit  $x^2 \equiv a \pmod{p}$ . Der *Satz über Kongruenzregeln* (Seite 87) und der *Fermatsche Kongruenzsatz* ergeben  $a^{\frac{p-1}{2}} \equiv (x^2)^{\frac{p-1}{2}} \equiv x^{p-1} \equiv 1 \equiv \left(\frac{a}{p}\right) \pmod{p}$ .

ii) Im Falle  $\left(\frac{a}{p}\right) = -1$  wird indirekt geschlossen: Die Kongruenz  $y^{\frac{p-1}{2}} - 1 \equiv 0 \pmod{p}$  hat aufgrund des *Polynomkongruenzsatzes von Lagrange* (Seite 103) höchstens  $\frac{p-1}{2}$  Lösungen. Nach i) und wegen des *Satzes über die Anzahl quadratischer Reste* (Seite 108) gibt es die in dem Satz angegebenen  $\frac{p-1}{2}$  Lösungen. Also hat die Kongruenz keine weiteren Lösungen, und  $a$  muß der zweiten Beziehung  $a^{\frac{p-1}{2}} + 1 \equiv 0 \pmod{p}$  genügen.  $\square$

Zur Berechnung des Legendre-Symbols werden üblicherweise die folgenden weiteren vier Regeln hergeleitet, wobei  $p, q \in \mathbb{P}_3$  und  $a, b \in \mathbb{Z}$  mit  $\text{ggT}(ab, p) = 1$  sind:

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right) \left(\frac{b}{p}\right), \quad \left(\frac{p}{q}\right) \left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2} \frac{q-1}{2}} \quad (\text{“Quadratisches Reziprozitätsgesetz”}),$$

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} \quad \text{und} \quad \left(\frac{2}{p}\right) = (-1)^{\left[\frac{p+1}{4}\right]}.$$

Das Ziel ist die sukzessive Zurückführung auf Legendre-Symbole mit verkleinerten oberen und unteren Teilen. Wird  $\left(\frac{q}{p}\right)$  für  $p < q$  mit Hilfe des quadratischen Reziprozitätsgesetzes gewonnen, so ergibt die Anwendung von (4.5) häufig im oberen Teil eine zerlegbare Zahl. Um fortfahren zu können, ist die Zahl in Primfaktoren zu zerlegen und dann die erste der obigen Regeln zu benutzen. Dadurch kann die Berechnung bei großen Ausgangszahlen sehr mühsam werden.

Die folgende Vorgehensweise, die ein schönes Beispiel für die *Verallgemeinerungsstrategie* darstellt, hat aber nicht nur das Vereinfachungsziel: Durch ständige Erweiterungen wurden im Laufe der Zeit immer leistungsfähigere Symbole eingeführt.

### Definition der Halbsysteme

Es sei  $m$  aus  $\mathbb{U} := \{n \in \mathbb{N}_3; 2 \nmid n\}$  und  $m_- := \frac{m-1}{2}$  (gelesen: m durch). Eine Teilmenge  $\{h_1, \dots, h_{m_-}\} \subset \mathbb{Z}$  heißt *Halbsystem modulo m*, wenn  $\{h_1, \dots, h_{m_-}\} \cup \{0, (-1)h_1, \dots, (-1)h_{m_-}\}$  ein vollständiges Restsystem modulo  $m$  ist.

Beispiele sind  $\mathcal{I}_{m_-}$ ,  $\{m_- + 1, \dots, m - 1\}$  und  $\{-1, \dots, -m_-\}$ .

### Satz über Halbsysteme

Es sei  $(a, m) \in \mathbb{Z} \times \mathbb{U}$  mit  $\text{ggT}(a, m) = 1$  und  $\{h_1, \dots, h_{m_-}\}$  sei ein Halbsystem modulo  $m$ . Dann gibt es Zahlen  $e_k \in \{-1, 1\}$ ,  $k = 1, \dots, m_-$ , und eine Permutation  $\pi : \mathcal{I}_{m_-} \rightarrow \mathcal{I}_{m_-}$ , sodass  $ah_k \equiv h_{\pi(k)} e_k \pmod{m}$  für  $k = 1, \dots, m_-$  gilt.

Das Produkt  $\prod_{k=1}^{m_-} e_k$  ist von der Auswahl des Halbsystems unabhängig.

**Beweis** (direkt, a1):

Aufgrund des *Satzes über modifizierte Restsysteme* (Seite 92) gibt es zu jedem  $k \in \mathcal{I}_{m_-}$  ein  $j \in \mathcal{I}_{m_-}$  und ein  $e_k \in \{-1, 1\}$ , sodass  $a h_k \equiv h_j e_k \pmod{m}$  gilt. Da  $j$  und  $e_k$  eindeutig durch  $k$  bestimmt sind, stellt  $\pi : \mathcal{I}_{m_-} \rightarrow \mathcal{I}_{m_-}$ ,  $k \mapsto j$ , eine Abbildung dar. Wir zeigen, dass  $\pi$  injektiv ist. Sind  $i, j \in \mathcal{I}_{m_-}$  mit  $\pi(i) = \pi(j)$ , so folgt  $a h_i e_i \equiv h_{\pi(i)} \equiv h_{\pi(j)} \equiv a h_j e_j \pmod{m}$ . Der *Satz über Kongruenzkürzung* (Seite 91) ergibt  $h_i e_i e_j \equiv h_j \pmod{m}$ , sodass wegen der Halbsystemeigenschaft  $i = j$  und  $e_i = e_j$  sein muss. Mit Hilfe des *Schubfachsatzes* (Seite 85) folgt, dass  $\pi$  eine bijektive Abbildung und damit eine Permutation darstellt.

Es sei  $\{h'_1, \dots, h'_{m_-}\}$  ein beliebiges Halbsystem modulo  $m$ , und es seien  $c_1, \dots, c_{m_-}$  aus  $\mathbb{N}$  so gewählt, dass  $h'_k \equiv h_k (-1)^{c_k} \pmod{m}$  für  $k = 1, \dots, m_-$  gilt. Dann ist  $a h'_k \equiv a h_k (-1)^{c_k} \equiv h_{\pi(k)} e_k (-1)^{c_k} \equiv h'_{\pi(k)} e_k (-1)^{c_k + c_{\pi(k)}} \pmod{m}$ . Bildet man hier entsprechend das Produkt  $\prod_{k=1}^{m_-} (-1)^{c_k + c_{\pi(k)}} e_k$ , so ergibt sich  $\prod_{k=1}^{m_-} e_k$ , weil die Zahlen  $c_1, \dots, c_{m_-}$  in den Exponenten doppelt vorkommen.  $\square$

### Bezeichnung des Jacobi-Symbols <sup>8</sup>

Ist  $(a, m) \in \mathbb{Z} \times \mathbb{U}$  mit  $\text{ggT}(a, m) = 1$  und stellt  $\prod_{k=1}^{m_-} e_k$  das invariante Produkt aus dem *Satz über Halbsysteme* dar, so wird das Symbol  $\left(\frac{a}{m}\right) := \prod_{k=1}^{m_-} e_k$  *Jacobi-Symbol* genannt.

### Übereinstimmungssatz <sup>9</sup>

Ist  $(a, m) \in \mathbb{Z} \times \mathbb{P}_3$  mit  $\text{ggT}(a, m) = 1$ , so stimmt das Jacobi-Symbol  $\left(\frac{a}{m}\right)$  mit dem Legendre-Symbol überein, und es gilt

$$\left(\frac{a}{m}\right) = (-1)^\alpha \text{ mit } \alpha := \text{card} \{u \in \mathcal{I}_{m_-} ; m_- < \text{mod}(au, m)\}.$$

**Beweis** (direkt, r1):

Durch Multiplikation der Kongruenzen des *Satzes über Halbsysteme* erhält man

<sup>8</sup> CARL GUSTAV JACOB JACOBI (1804-1851) wirkte in Berlin und Königsberg.

<sup>9</sup> Die Aussage über die Potenzdarstellung des Legendre-Symbols heißt üblicherweise *Lemma von Gauß*.

$a^{m_-} \prod_{k=1}^{m_-} h_k \equiv \prod_{k=1}^{m_-} e_k \prod_{k=1}^{m_-} h_{\pi(k)} \pmod{m}$ . Wegen  $\text{ggT}\left(\prod_{k=1}^{m_-} h_k, m\right) = 1$  ergibt der

*Satz über Kongruenzkürzung* (Seite 91)  $a^{m_-} \equiv \prod_{k=1}^{m_-} e_k \pmod{m}$ . Aufgrund des

*Satzes über das Euler-Kriterium* (Seite 109) ist  $a^{m_-} \equiv \left(\frac{a}{m}\right) \pmod{m}$ . Also gilt

$\prod_{k=1}^{m_-} e_k \equiv \left(\frac{a}{m}\right) \pmod{m}$ , und wegen  $m > 2$  müssen beide Zahlen gleich sein.

Für das ‘‘Standardhalbsystem’’  $\mathcal{I}_{m_-}$  gilt  $\prod_{k=1}^{m_-} e_k = (-1)^\alpha$ , weil  $\text{mod}(au, m) > m_-$

mit  $-m_- \leq \text{mod}(au, m) - m < 0$  äquivalent ist.  $\square$

**Achtung:** Ist  $m \in \mathbb{N}_2 \setminus \mathbb{P}$ , so folgt aus  $\left(\frac{a}{m}\right) = 1$  nicht notwendig, dass  $a$  einen quadratischen Rest modulo  $m$  darstellt. Zum Beispiel für  $\left(\frac{2}{15}\right)$  ergibt das Standardhalbsystem  $\mathcal{I}_7$  mit  $\alpha = 4$  den Wert  $\left(\frac{2}{15}\right) = (-1)^4 = 1$ , aber für alle  $x \in \mathcal{I}_7$  ist  $x^2 \not\equiv 2 \pmod{15}$ .

Auf Seite 114 werden wir erkennen, dass im Falle  $\left(\frac{a}{m}\right) = -1$  notwendig  $a$  quadratischer Nichtrest modulo  $m$  ist.

Im Folgenden sei  $m \in \mathbb{U}$ , und  $\{h_1, \dots, h_{m_-}\}$  sei ein Halbsystem modulo  $m$ .

### Satz über obere Kongruenzinvarianz

Für alle  $a, b \in \mathbb{Z}$  mit  $\text{ggT}(ab, m) = 1$  und  $a \equiv b \pmod{m}$  gilt

$$(4.6) \quad \left(\frac{a}{m}\right) = \left(\frac{b}{m}\right).$$

**Beweis** (direkt, r1):

Aufgrund des *Satzes über Halbsysteme* (Seite 110) ist  $b h_k \equiv a h_k \equiv h_{\pi(k)} e_k \pmod{m}$  für  $k = 1, \dots, m_-$ . Zu  $a$  und  $b$  gehören also dieselben Zahlen  $e_k$ .  $\square$

### Satz über obere Multiplikativität

Für alle  $a, b \in \mathbb{Z}$  mit  $\text{ggT}(ab, m) = 1$  gilt

$$(4.7) \quad \left(\frac{ab}{m}\right) = \left(\frac{a}{m}\right) \left(\frac{b}{m}\right).$$

**Beweis** (direkt, r1):

Es sei  $a h_k \equiv h_{\pi(k)} e_k \pmod{m}$ ,  $k = 1, \dots, m_-$ , wie im *Satz über Halbsysteme* (Seite 110) und entsprechend

$$(4.8) \quad b h_k \equiv h_{\pi'(k)} e'_k \pmod{m} \text{ mit } e'_k \in \{-1, 1\}.$$

Multiplikation von (4.8) mit  $a$  und Anwendung des *Satzes über Halbsysteme*

ergibt  $a b h_k \equiv (a h_{\pi'(k)}) e'_k \equiv h_{\pi(\pi'(k))} e_{\pi'(k)} e_k \pmod{m}$ . Damit gilt  $\left(\frac{ab}{m}\right) =$

$$\prod_{k=1}^{m_-} e_{\pi'(k)} e'_k = \prod_{k=1}^{m_-} e_{\pi'(k)} \prod_{k=1}^{m_-} e'_k = \left(\frac{a}{m}\right) \left(\frac{b}{m}\right). \quad \square$$

### Satz über untere Multiplikativität

Für alle  $m, n \in \mathbb{U}$  und  $a \in \mathbb{Z}$  mit  $\text{ggT}(a, mn) = 1$  gilt

$$(4.9) \quad \left(\frac{a}{mn}\right) = \left(\frac{a}{m}\right) \left(\frac{a}{n}\right).$$

**Beweis** (direkt, a1):

Neben dem oben vereinbarten Halbsystem modulo  $m$  sei  $(h'_1, \dots, h'_{n_-})$  ein Halbsystem modulo  $n$ , und es gelte

$$a h'_j \equiv h'_{\tau(j)} e'_j \pmod{n} \text{ mit } e'_j \in \{-1, 1\}, \quad j = 1, \dots, n_-,$$

wobei  $\tau$  eine Permutation auf  $\{1, \dots, n_-\}$  darstellt. Wir zeigen, dass die Menge

$$\mathcal{H} := \{h_k + m s; k = 1, \dots, m_- \text{ und } s = 0, \dots, n - 1\} \cup \{m h'_j; j = 1, \dots, n_-\}$$

ein Halbsystem modulo  $mn$  ist. Die Elemente von

$$\mathcal{H}_1 := \mathcal{H} \cup \{0\} \cup \{-n; n \in \mathcal{H}\}$$

haben alle die Form  $r + m s$ , wobei  $r$  ein vollständiges Restsystem modulo  $m$

und  $s$  ein vollständiges Restsystem modulo  $n$  durchläuft. Aufgrund des *Satzes*

*über vollständige Restsysteme* (Seite 86) stellt  $\mathcal{H}_1$  ein vollständiges Restsystem

dar, weil  $\text{card } \mathcal{H}_1 = 2(m_- n + n_-) + 1 = mn$  ist und weil die Elemente von  $\mathcal{H}_1$

modulo  $mn$  zueinander inkongruent sind, denn aus  $r + m s \equiv r' + m s' \pmod{mn}$

folgt  $m \mid (r - r')$ , also  $r = r'$ , und aufgrund des *Satzes über Kongruenzkürzung*

(Seite 91) ergibt sich  $s \equiv s' \pmod{n}$ , also  $s = s'$ .

Wir multiplizieren nun die Elemente des Halbsystems  $\mathcal{H}$  mit  $a$  und wenden den

*Satz über Halbsysteme* (Seite 110) an. Wegen  $a h_k = h_{\pi(k)} e_k + t m$  mit  $t \in \mathbb{Z}$  gilt

$a(h_k + m s) = h_{\pi(k)} e_k + (a s + t) m$ . Setzen wir  $u := \text{mod}(e_k (a s + t), n)$ , so folgt

$a(h_k + ms) \equiv (h_{\pi(k)} + mu) e_k \pmod{mn}$  und

$$a(mh'_j) \equiv (mh'_{\tau(j)}) e'_j \pmod{mn}.$$

Damit erhält man  $\left(\frac{a}{mn}\right) = \prod_{k=1}^{m-} e_k^n \prod_{j=1}^{n-} e'_j \stackrel{2 \nmid n}{=} \prod_{k=1}^{m-} e_k \prod_{j=1}^{n-} e'_j = \left(\frac{a}{m}\right) \left(\frac{a}{n}\right)$ .  $\square$

Hat  $m$  die *Primpotenzdarstellung*  $m = \prod_{k=1}^r q_k^{e_k}$  und ist  $\text{ggT}(a, m) = 1$ , so wird das Jacobi-Symbol meistens mit Hilfe der Legendre-Symbole  $\left(\frac{a}{q_k}\right)$ ,  $k = 1, \dots, r$ , durch  $\left(\frac{a}{m}\right) := \prod_{k=1}^r \left(\frac{a}{q_k}\right)^{e_k}$  eingeführt. Der *Satz über untere Multiplikativität* und vollständige Induktion bezüglich der Primfaktorenzahl im unteren Teil liefern den Zusammenhang.

Jetzt können wir auch den auf Seite 112 angekündigten Nachweis führen, dass im Falle  $\left(\frac{a}{m}\right) = -1$  notwendig  $a$  quadratischer Nichtrest modulo  $m$  ist. Wegen der obigen Produktdarstellung muss mindestens eines der Legendre-Symbole  $\left(\frac{a}{q_k}\right)$  negativ sein. Damit ist  $a$  quadratischer Nichtrest modulo  $q_k$ . Aufgrund des *Satzes über Kongruenzvergrößerung* (Seite 91) besitzt dann auch die Kongruenz  $x^2 \equiv a \pmod{m}$  keine Lösung.

Für das Legendre-Symbol wurde der folgende Satz 1796 zum ersten Mal von GAUß bewiesen. Er hielt dieses Ergebnis, das er als “*theorema fundamentale*” bezeichnete, für eines seiner bedeutendsten Beiträge zur Zahlentheorie und gab dafür sechs verschiedene Beweise. Der hier wiedergegebene Beweis ist dadurch entstanden, dass eine Reihe von Mathematikern den dritten Beweis von GAUß immer weiter vereinfacht und später auf das Jacobi-Symbol übertragen haben.

### Quadratisches Reziprozitätsgesetz

Für alle  $(m, n) \in \mathbb{U}^2$  mit  $\text{ggT}(m, n) = 1$  gilt

$$(4.10) \quad \left(\frac{n}{m}\right) \left(\frac{m}{n}\right) = (-1)^{\frac{m-1}{2} \frac{n-1}{2}}.$$

**Beweis** (direkt, a2):

Am Schluss des Beweises für den *Übereinstimmungssatz* (Seite 111) haben wir unter Verwendung des Standardhalbsystems und mit  $a$  anstelle von  $n$  durch Um-

formulierung die Darstellung

$$\left(\frac{n}{m}\right) = (-1)^\alpha \text{ mit } \alpha = \text{card} \left\{ u \in \mathcal{I}_{m_-}; -m_- \leq nu - m \left( \left[ \frac{nu}{m} \right] + 1 \right) < 0 \right\}$$

gewonnen. Hier setzen wir  $v := \left[ \frac{nu}{m} \right] + 1$  und zeigen, dass  $v \in \mathcal{I}_{n_-}$  gilt, um mit einer Strategie, die Symmetrie ausnutzt und die wir deshalb *Symmetriestrategie* nennen, fortfahren zu können. Einerseits ist wegen  $m, n, u \in \mathbb{N}_1$  auch  $v \in \mathbb{N}_1$ , und andererseits gilt  $mv \leq nu + m_- < n \frac{m}{2} + \frac{m}{2} = m \frac{n+1}{2}$ , also  $v < n_- + 1$ . Außerdem folgt für jedes  $v'$  mit  $-m_- \leq nu - mv' < 0$ , dass  $\frac{n}{m}u < v' < \frac{n}{m}u + \frac{1}{2}$  und damit  $v' = \left[ \frac{nu}{m} \right] + 1 = v$  erfüllt ist. Wegen der eindeutigen Bestimmtheit von  $v$  durch  $u$  können wir in  $\alpha$  statt der Zahlen  $u$  die Paare  $(u, v)$  zählen:

$$\alpha = \text{card} \left\{ (u, v) \in \mathcal{I}_{m_-} \times \mathcal{I}_{n_-}; -m_- \leq nu - mv < 0 \right\}.$$

Durch Vertauschen von  $m$  und  $n$  erhalten wir dann

$$\left(\frac{m}{n}\right) = (-1)^\beta \text{ mit } \beta = \text{card} \left\{ (u, v) \in \mathcal{I}_{n_-} \times \mathcal{I}_{m_-}; -n_- \leq mu - nv < 0 \right\}.$$

Wir ersetzen  $u$  durch  $v''$  und  $v$  durch  $u''$ , vertauschen die Paarkomponenten und multiplizieren die Ungleichungskette mit  $-1$ . Damit ergibt sich

$$\beta = \text{card} \left\{ (u'', v'') \in \mathcal{I}_{m_-} \times \mathcal{I}_{n_-}; 0 < nu'' - mv'' \leq n_- \right\},$$

wobei die Striche im Folgenden wieder weggelassen werden. Da die Gleichung  $nu - mv = 0$  wegen  $\text{ggT}(m, n) = 1$  aufgrund des *Produktteilersatzes* (Seite 23) keine Lösung  $(u, v) \in \mathcal{I}_{m_-} \times \mathcal{I}_{n_-}$  besitzt, können wir  $\alpha + \beta$  als Kardinalzahl der ‘‘Gitterpunktmenge’’

$$\mathcal{G} = \left\{ (x, y) \in \mathcal{I}_{m_-} \times \mathcal{I}_{n_-}; -m_- \leq nx - my \leq n_- \right\}$$

schreiben und erhalten

$$\left(\frac{n}{m}\right) \left(\frac{m}{n}\right) = (-1)^{\text{card } \mathcal{G}}.$$

Da  $m_- n_-$  die Kardinalzahl des ‘‘Gitterpunktrechtecks’’  $\mathcal{R} := \mathcal{I}_{m_-} \times \mathcal{I}_{n_-}$  ist, das definitionsgemäß  $\mathcal{G}$  enthält, bietet es sich an,  $\mathcal{R}$  und  $\mathcal{G}$  zu ‘‘visualisieren’’, um einen Grund für die noch zu beweisende Beziehung  $\text{card } \mathcal{R} \equiv \text{card } \mathcal{G} \pmod{2}$  zu finden (siehe Abbildung 4.1).

Obwohl beim Problemlösen in der elementaren Zahlentheorie nur selten Figuren verwendet werden, geben wir dieser Vorgehensweise den Namen *Visualisierungsstrategie*, weil sie in dem großen Problembereich der Elementargeometrie grundlegend ist.

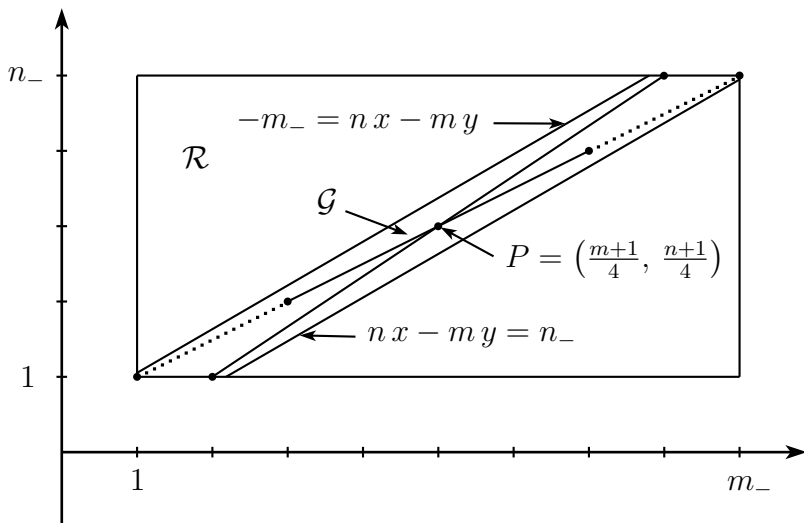


Abbildung 4.1: Die Gitterpunktmenge  $\mathcal{G}$  und  $\mathcal{R}$  (für  $m = 19$  und  $n = 11$ )

Tatsächlich drängt sich nun die Vermutung auf, dass  $\mathcal{G}$  als Durchschnitt von  $\mathcal{R}$  mit dem Parallelstreifen  $\mathcal{S} := \{(x, y) \in \mathbb{Q}^2; -m_- \leq nx - my \leq n_-\}$  punktsymmetrisch zu dem Punkt  $P := \left(\frac{m+1}{4}, \frac{n+1}{4}\right)$  ist, der den Mittelpunkt des Rechtecks mit den Ecken  $(1, 1)$ ,  $(m_-, 1)$ ,  $(m_-, n_-)$ ,  $(1, n_-)$  in  $\mathbb{Q}^2$  darstellt. Da mit  $D_k(u) := \frac{k+1}{2} - u = k_- + 1 - u$  für  $k = m, n$  offensichtlich  $(D_m(x), D_n(y)) \in \mathcal{R}$  genau dann erfüllt ist, wenn  $(x, y) \in \mathcal{R}$  gilt, brauchen wir nur noch zu zeigen, dass auch  $(D_m(x), D_n(y)) \in \mathcal{S}$  und  $(x, y) \in \mathcal{S}$  äquivalent sind.

Umformung des mittleren Teils der zu  $(D_m(x), D_n(y)) \in \mathcal{S}$  gehörenden Ungleichungskette ergibt  $n D_m(x) - m D_n(y) = n \frac{m+1}{2} - m \frac{n+1}{2} - nx + my = \frac{n-m}{2} - nx + my = n_- - m_- - (nx - my)$ . Damit sind die Ungleichungsketten  $-m_- \leq n D_m(x) - m D_n(y) \leq n_-$  und  $-m_- \leq n_- - m_- - (nx - my) \leq n_-$  gleichbedeutend. Subtrahieren wir nun bei beiden Ungleichungen der letzten Kette  $n_- - m_-$  und multiplizieren mit  $-1$ , wobei sich die Ungleichungsrichtungen ändern, so erhalten wir die Ungleichungskette  $-m_- \leq nx - my \leq n_-$ , die zu  $(x, y) \in \mathcal{S}$  gehört. Da alle verwendeten Operationen umkehrbar sind, folgt die Äquivalenz, die für die Punktsymmetrie von  $\mathcal{S}$  und auch von  $\mathcal{G}$  nachzuweisen war.

Setzen wir  $\sigma : \mathbb{Q}^2 \rightarrow \mathbb{Q}^2$ ,  $(x, y) \mapsto (D_m(x), D_n(y))$ , so ergibt eine einfache Rechnung, dass  $\sigma = \sigma^{-1}$  gilt und dass die Einschränkung  $\sigma|_{\mathcal{R} \setminus \mathcal{G}}$  bi-

ektiv ist. Der einzige Fixpunkt  $P$  von  $\sigma$  liegt in  $\mathcal{S}$  und gehört damit niemals zu  $\mathcal{R} \setminus \mathcal{G}$ . Deshalb lässt sich  $\mathcal{R} \setminus \mathcal{G}$  als Vereinigung von disjunkten zweielementigen Mengen der Form  $\{X, \sigma(X)\}$  schreiben. Insbesondere gilt  $2 \mid \text{card } \mathcal{R} \setminus \mathcal{G}$ , sodass  $\text{card } \mathcal{R} = \text{card } \mathcal{G} + \text{card } \mathcal{R} \setminus \mathcal{G} \equiv \text{card } \mathcal{G} \pmod{2}$  folgt. Damit ist  $\binom{n}{m} \binom{m}{n} = (-1)^{\text{card } \mathcal{R}} = (-1)^{m_- - n_-}$ . □

### Erster Ergänzungssatz

Für jedes  $m \in \mathbb{U}$  gilt

$$(4.11) \quad \left(\frac{-1}{m}\right) = (-1)^{\frac{m-1}{2}}.$$

**Beweis** (direkt, r1):

Wegen  $(-1)h_k \equiv h_k(-1) \pmod{m}$  für  $k = 1, \dots, m_-$  ist  $\left(\frac{-1}{m}\right) = \prod_{k=1}^{m_-} (-1) = (-1)^{m_-}$ . □

### Zweiter Ergänzungssatz

Für jedes  $m \in \mathbb{U}$  gilt

$$(4.12) \quad \left(\frac{2}{m}\right) = (-1)^{\left[\frac{m+1}{4}\right]} = (-1)^{\frac{1}{8}(m^2 - 1)}.$$

**Beweis** (direkt, r1):

Die Vielfachen  $2k$  der Zahlen  $k \in \mathcal{I}_{m_-}$  liegen genau dann in der oberen Resthälfte  $\{m_- + 1, \dots, m - 1\}$  und ergeben damit bei dem Standardhalbsystem aufgrund des *Satzes über Halbsysteme* (Seite 110) ein negatives Vorzeichen, wenn  $\frac{m+1}{4} \leq k \leq \frac{m-1}{2}$  ist.

Im Fall  $m \equiv 1 \pmod{4}$  sind das die  $\frac{m-1}{4}$  Zahlen  $\frac{m-1}{4} + 1, \dots, \frac{m-1}{4} + \frac{m-1}{4}$ . Also gilt hier  $\left(\frac{2}{m}\right) = (-1)^{\frac{m-1}{4}}$ .

Für  $m \equiv 3 \pmod{4}$  sind es die  $\frac{m+1}{4}$  Zahlen  $\frac{m+1}{4}, \dots, \frac{m+1}{4} + \frac{m-3}{4}$ . Nun folgt  $\left(\frac{2}{m}\right) = (-1)^{\frac{m+1}{4}}$ .

Diese beiden Fälle lassen sich offensichtlich zu  $\left(\frac{2}{m}\right) = (-1)^{\left[\frac{m+1}{4}\right]}$  zusammenfassen. Wegen  $\frac{1}{8}(m^2 - 1) = \frac{(m+1)(m-1)}{2 \cdot 4}$  ist

$$\frac{1}{8}(m^2 - 1) = \begin{cases} \frac{m-1}{4} \left(1 + 2 \frac{m-1}{4}\right) & \text{für } m \equiv 1 \pmod{4}, \\ \frac{m+1}{4} \left(1 + 2 \frac{m-3}{4}\right) & \text{für } m \equiv 3 \pmod{4}. \end{cases}$$

Da beide Klammerfaktoren ungerade natürliche Zahlen sind, gilt  $\frac{1}{8}(m^2 - 1) \equiv \left[\frac{m+1}{4}\right] \pmod{2}$ .  $\square$

Das folgende Beispiel für die Berechnung eines Legendre-Symbols mit Hilfe von Jacobi-Symbolen stammt aus [1]. Dort tritt auf Seite 452 nach dem zweiten Gleichheitszeichen ein Fehler auf, der den Endwert falsch werden lässt. Wir geben hier und bei dem Beweis des nächsten Satzes über den Gleichheitszeichen die letzte Ziffer der jeweils verwendeten Formel an, nämlich 6 für die *obere Kongruenzinvarianz*, 7 für *obere Multiplikativität*, 0 für das *quadratische Reziprozitätsgesetz*, 1 für den *ersten Ergänzungssatz* und 2 für den *zweiten Ergänzungssatz*.

$$\begin{aligned} & \left(\frac{20002}{134353}\right) \stackrel{7}{=} \left(\frac{2}{134353}\right) \left(\frac{10001}{134353}\right) \stackrel{20}{=} (+1) \left(\frac{134353}{10001}\right) \stackrel{(+1)}{=} \stackrel{6}{=} \left(\frac{4340}{10001}\right) \stackrel{7}{=} \\ & \left(\frac{4}{10001}\right) \left(\frac{1085}{10001}\right) \stackrel{70}{=} \stackrel{(+1)}{=} \left(\frac{10001}{1085}\right) \stackrel{(+1)}{=} \stackrel{6}{=} \left(\frac{236}{1085}\right) \stackrel{7}{=} \left(\frac{4}{1085}\right) \left(\frac{59}{1085}\right) \stackrel{70}{=} \\ & \stackrel{(+1)}{=} \left(\frac{1085}{59}\right) \stackrel{(+1)}{=} \stackrel{6}{=} \left(\frac{23}{59}\right) \stackrel{0}{=} \left(\frac{59}{23}\right) \stackrel{(-1)}{=} \stackrel{6}{=} -\left(\frac{13}{23}\right) \stackrel{0}{=} -\left(\frac{23}{13}\right) \stackrel{(+1)}{=} \stackrel{6}{=} \\ & -\left(\frac{-3}{13}\right) \stackrel{7}{=} -\left(\frac{-1}{13}\right) \left(\frac{3}{13}\right) \stackrel{10}{=} -\stackrel{(+1)}{=} \left(\frac{13}{3}\right) \stackrel{(+1)}{=} \stackrel{6}{=} -\left(\frac{1}{3}\right) = -1. \end{aligned}$$

Da  $134353 \in \mathbb{P}$  gilt, ist 20002 quadratischer Nichtrest modulo 134353.

Aus den beiden *Ergänzungssätzen* kann man entnehmen, dass  $-1$  beziehungsweise 2 genau für die Primzahlen  $p$  mit  $p \equiv 1 \pmod{4}$  beziehungsweise mit  $p \equiv \pm 1 \pmod{8}$  quadratischer Rest ist. Der folgende Satz über das Jacobi-Symbol ermöglicht es, diese Feststellung über die Restklassen der Primzahlen, für die eine gegebene ganze Zahl quadratischer Rest ist, zu verallgemeinern.

### Satz über untere Kongruenzinvarianz

Ist  $a \in \mathbb{Z}$  und sind  $m, n \in \mathbb{U}$  mit  $\text{ggT}(a, mn) = 1$  und  $m \equiv n \pmod{4|a|}$ , so gilt

$$(4.13) \quad \left(\frac{a}{m}\right) = \left(\frac{a}{n}\right).$$

**Beweis** (direkt mit Fallunterscheidung, r1):

Wir behandeln zunächst vier spezielle Fälle für Teiler  $c$  von  $a$  und fügen sie abschließend im allgemeinen fünften Fall zusammen.

i)  $c = 1$ : Definitionsgemäß ist  $1 = \left(\frac{1}{m}\right) = \left(\frac{1}{n}\right)$ .

Für die folgenden Fälle sei  $t := \frac{n-m}{4|a|}$ . Wegen  $n_- = m_- + 2|a|t$  ist dann  $n_- \equiv m_- \pmod{2}$ . Neben den Formelkennzeichnungen aus dem vorigen Beispiel verwenden wir im Folgenden die Ziffer 3 für die letzte Kongruenz.

ii)  $c = -1$ : Hier gilt  $\left(\frac{-1}{m}\right) \stackrel{1}{=} (-1)^{m_-} \stackrel{3}{=} (-1)^{n_-} \stackrel{1}{=} \left(\frac{-1}{n}\right)$ .

iii)  $c = 2$ : Nun ist  $\left[\frac{n+1}{4}\right] = \left[\frac{m+1}{4}\right] + |a|t$  mit  $2 \mid a$ . Aus  $\left[\frac{n+1}{4}\right] \equiv \left[\frac{m+1}{4}\right] \pmod{2}$  ergibt sich dann  $\left(\frac{2}{m}\right) \stackrel{2}{=} (-1)^{\left[\frac{m+1}{4}\right]} = (-1)^{\left[\frac{n+1}{4}\right]} \stackrel{2}{=} \left(\frac{2}{n}\right)$ .

iv)  $c \in \mathbb{U}$ : Es gilt  $\left(\frac{c}{m}\right) \stackrel{0}{=} \left(\frac{m}{c}\right) (-1)^{c_- m_-} \stackrel{63}{=} \left(\frac{n}{c}\right) (-1)^{c_- n_-} \stackrel{0}{=} \left(\frac{c}{n}\right)$ .

v)  $a = (-1)^h 2^k b$  mit  $h \in \{0, 1\}$ ,  $k \in \mathbb{N}$  und  $b \in \{1\} \cup \mathbb{U}$ : Zusammenfassung ergibt  $\left(\frac{a}{m}\right) \stackrel{7}{=} \left(\frac{-1}{m}\right)^h \left(\frac{2}{m}\right)^k \left(\frac{b}{m}\right) \stackrel{i-iv)}{=} \left(\frac{-1}{n}\right)^h \left(\frac{2}{n}\right)^k \left(\frac{b}{n}\right) \stackrel{7}{=} \left(\frac{a}{n}\right)$ . □

Wir schließen die Theorie der quadratischen Kongruenzen mit der Zurückführung der allgemeinen quadratischen Kongruenz auf quadratische Reste und Quadratwurzeln modulo  $m$ .

### Satz über die allgemeine quadratische Kongruenz

Es seien  $a, b, c \in \mathbb{Z}$ ,  $\alpha := \frac{2}{\text{ggT}(2,b)}$  und  $b_1 := \frac{b}{\text{ggT}(2,b)}$ . Für jedes  $m \in \mathbb{N}_2$  mit  $\text{ggT}(\alpha a, m) = 1$  existiert genau dann ein  $x \in \mathbb{Z}$  mit

$$(4.14) \quad ax^2 + bx + c \equiv 0 \pmod{m},$$

wenn es ein  $y \in \mathbb{Z}$  gibt, sodass

$$(4.15) \quad y^2 \equiv b_1^2 - \alpha^2 ac \pmod{m}$$

gilt. Zu jeder solchen Zahl  $y$  lässt sich aus  $\alpha ax \equiv y - b_1 \pmod{m}$  eine Lösung  $x$  von (4.14) berechnen.

**Beweis** (direkt, r1):

Aufgrund des *Satzes über Kongruenzkürzung* (Seite 91) lässt sich die Kongruenz (4.14) mit  $\alpha^2 a$  multiplizieren, ohne dass die Lösungsmenge geändert wird. Wegen  $\alpha^2 a^2 x^2 + \alpha^2 a b x + \alpha^2 a c = \alpha^2 a^2 x^2 + 2 \alpha a b_1 x + \alpha^2 a c = (\alpha a x + b_1)^2 - b_1^2 + \alpha^2 a c$  ist dann (4.14) äquivalent mit  $(\alpha a x + b_1)^2 \equiv b_1^2 - \alpha^2 a c \pmod{m}$ .

Hat (4.14) eine Lösung  $x$ , so stellt  $y := \alpha a x + b_1$  eine Lösung von (4.15) dar. Ist  $y$  eine Lösung von (4.15), so besitzt  $\alpha a x \equiv y - b_1 \pmod{m}$  aufgrund des *Satzes über die lineare Kongruenz* (Seite 91) eine Lösung  $x$ , die auch (4.14) erfüllt.  $\square$

## 4.8 Ordnungen, Primitivwurzeln und Indizes

Zum Abschluss dieses Kapitels über Kongruenzen behandeln wir die am Anfang von 4.7 erwähnten Ergebnisse aus dem dritten Abschnitt von [9].

Im Folgenden seien  $a \in \mathbb{Z}$  und  $m \in \mathbb{N}_2$  mit  $\text{ggT}(a, m) = 1$ . Die Menge  $\{\gamma \in \mathbb{N}_1 ; a^\gamma \equiv 1 \pmod{m}\}$  ist aufgrund des *Kongruenzsatzes von Euler* (Seite 99) nicht leer. Der *Minimumsatz* (Seite 11) sichert damit die Existenz eines eindeutigen Minimums.

### Bezeichnung der Ordnung

Die Zahl  $\min\{\gamma \in \mathbb{N}_1 ; a^\gamma \equiv 1 \pmod{m}\}$  heißt *Ordnung von  $a$  modulo  $m$* . Sie wird mit  $\text{ord}_m(a)$  abgekürzt.<sup>10</sup>

### Satz über die Ordnung

- Ist  $\delta := \text{ord}_m(a)$ , so sind die Zahlen  $1, a^1, \dots, a^{\delta-1}$  modulo  $m$  inkongruent.
- Es gilt  $a^\gamma \equiv a^{\gamma'} \pmod{m}$  genau dann, wenn  $\gamma \equiv \gamma' \pmod{\delta}$  ist. Insbesondere folgt, dass  $a^\gamma \equiv 1 \pmod{m}$  und  $\delta \mid \gamma$  äquivalent sind.
- Stets ist  $\text{ord}_m(a)$  ein Teiler von  $\varphi(m)$ .

<sup>10</sup> Ist  $\delta := \text{ord}_m(a)$ , so sagte man früher “ $a$  gehört modulo  $m$  zu dem Exponenten  $\delta$ ”.

**Beweis** (Teil a) indirekt, sonst direkt, r1):

a) Aus  $a^l \equiv a^k \pmod{m}$  mit  $0 \leq k < l < \delta$  würde aufgrund des *Satzes über Kongruenzkürzung* (Seite 91)  $a^{l-k} \equiv 1 \pmod{m}$  mit  $0 < l - k < \delta$  im Widerspruch zur Definition von  $\delta$  folgen.

b) Aufgrund des *Satzes über Division mit Rest* (Seite 19) gibt es jeweils genau ein Paar  $(q, r) \in \mathbb{Z} \times \mathcal{A}_\delta$  beziehungsweise  $(q', r') \in \mathbb{Z} \times \mathcal{A}_\delta$  mit  $\gamma = \delta q + r$  beziehungsweise  $\gamma' = \delta q' + r'$ . Damit folgt  $a^\gamma \equiv (a^\delta)^q a^r \equiv a^r \pmod{m}$  und  $a^{\gamma'} \equiv (a^\delta)^{q'} a^{r'} \equiv a^{r'} \pmod{m}$ . Also gilt  $a^\gamma \equiv a^{\gamma'} \pmod{m}$  genau dann, wenn  $a^r \equiv a^{r'} \pmod{m}$  erfüllt ist, d.h. nach a), wenn  $r$  und  $r'$  gleich sind.

c) Aus  $a^{\varphi(m)} \equiv 1 \pmod{m}$  und b) mit  $\gamma = \varphi(m)$ ,  $\gamma' = 0$  folgt  $\delta \mid \varphi(m)$ .  $\square$

### Satz über Ordnungsbeziehungen

a) Für jedes  $n \in \mathbb{N}_1$  gilt

$$(4.16) \quad \text{ord}_m(a^n) = \frac{\text{ord}_m(a)}{\text{ggT}(n, \text{ord}_m(a))}.$$

b) Ist außerdem  $b \in \mathbb{Z}$  mit  $\text{ggT}(b, m) = 1$  und  $\text{ggT}(\text{ord}_m(a), \text{ord}_m(b)) = 1$ , so folgt

$$(4.17) \quad \text{ord}_m(ab) = \text{ord}_m(a) \text{ord}_m(b).$$

**Beweis** (direkt, a1):

a) Es seien  $s := \text{ord}_m(a^n)$ ,  $t := \text{ord}_m(a)$ ,  $d := \text{ggT}(n, t)$ ,  $n' := \frac{n}{d}$  und  $t' := \frac{t}{d}$ .

Es gilt  $(a^n)^s \equiv a^{ns} \equiv 1 \pmod{m}$ . Der *Satz über die Ordnung* (mit  $\gamma' = 0$ ) liefert  $t \mid (ns)$ , also  $t' \mid (n's)$ . Aufgrund des *Produktteilersatzes* (Seite 23) und wegen  $\text{ggT}(n', t') = 1$  folgt  $t' \mid s$ .

Analog erhält man  $(a^n)^{t'} \equiv a^{dn't'} \equiv a^{t'n'} \equiv (a^t)^{n'} \equiv 1 \pmod{m}$ , also  $s \mid t'$  und zusammengefasst  $s = t' = \frac{t}{d}$ .

b) Es seien  $u := \text{ord}_m(a)$ ,  $v := \text{ord}_m(b)$  und  $w := \text{ord}_m(ab)$ . Aus  $1 \equiv (ab)^{wv} \equiv a^{vw} b^{vw} \equiv a^{vw} (b^v)^w \equiv a^{vw} \pmod{m}$  folgt  $u \mid (vw)$ , und wegen  $\text{ggT}(u, v) = 1$  gilt  $u \mid w$ . Mit  $1 \equiv (ab)^{wu}$  ergibt sich analog  $v \mid w$  und damit  $(uv) \mid w$ .

Außerdem ist  $(ab)^{uv} \equiv (a^u)^v (b^v)^u \equiv 1 \pmod{m}$ . Also folgt  $w \mid (uv)$  und zusammengefasst  $w = uv$ .  $\square$

### Definition der Primitivwurzel

Sind  $a \in \mathbb{Z}$  und  $m \in \mathbb{N}_2$  mit  $\text{ggT}(a, m) = 1$ , so heißt  $a$  *Primitivwurzel* (oder *primitive Wurzel*) modulo  $m$ , wenn  $\text{ord}_m(a) = \varphi(m)$  gilt.

Als Beispiel betrachten wir das auf Seite 85 angegebene vollständige Restsystem  $\mathcal{R}'_7 = \{0, 3, 3^2, 3^3, 3^4, 3^5, 3^6\}$ . Wegen  $3^1 \equiv 3 \pmod{7}$ ,  $3^2 \equiv 2 \pmod{7}$ ,  $3^3 \equiv 6 \pmod{7}$ ,  $3^4 \equiv 4 \pmod{7}$ ,  $3^5 \equiv 5 \pmod{7}$  und  $3^6 \equiv 1 \pmod{7}$  ist 3 Primitivwurzel modulo 7.

### Satz über Primitivwurzeln

a) Für jedes  $m \in \{2, 4\} \cup \{cp^k; c \in \mathcal{I}_2, p \in \mathbb{P}_3 \text{ und } k \in \mathbb{N}_1\}$  gibt es Primitivwurzeln modulo  $m$ .

b) Ist  $g$  eine Primitivwurzel modulo  $p$  für  $p \in \mathbb{P}_3$ , so sei

$$t := \begin{cases} 0 & \text{im Falle } g^{p-1} \not\equiv 1 \pmod{p^2}, \\ 1, & \text{wenn } g^{p-1} \equiv 1 \pmod{p^2} \text{ gilt.} \end{cases}$$

Dann ist  $g + pt$  Primitivwurzel modulo  $p^k$  für jedes  $k \in \mathbb{N}_2$ . Stellt  $h$  eine Primitivwurzel modulo  $p^k$  dar, so ist die ungerade der Zahlen  $h$  und  $h + p^k$  eine Primitivwurzel modulo  $2p^k$ .

**Beweis** (direkt, finite und vollständige Induktion, a2):

a) Für  $m \in \{2, 4\}$  ist  $m - 1$  eine Primitivwurzel modulo  $m$ . Es wird nun zuerst gezeigt, dass zu jedem  $p \in \mathbb{P}_3$  Primitivwurzeln existieren.

Es sei  $\mathcal{D}_p := \{\delta \in \mathcal{I}_p; \text{Es gibt } a \in \mathcal{A}_p^* \text{ mit } \delta = \text{ord}_p(a)\}$ , und für  $\tau := \text{kgV}(\mathcal{D}_p)$

sei  $\tau =: \prod_{k=1}^r q_k^{e_k}$  die *Primpotenzdarstellung*. Dann existiert zu jedem  $s \in \mathcal{I}_r$  ein

$\delta_s \in \mathcal{D}_p$  mit  $q_s^{e_s} \mid \delta_s$ . Es gibt also Zahlen  $c_s \in \mathbb{N}_1$  und  $a_s \in \mathcal{A}_p^*$  mit  $c_s q_s^{e_s} = \delta_s = \text{ord}_p(a_s)$ . Die Formeln (4.16) und (4.17) des *Satzes über Ordnungsbeziehungen*

(Seite 121) ergeben nacheinander  $\text{ord}_p(a_s^{c_s}) = \frac{\delta_s}{\text{ggT}(c_s, \delta_s)} = q_s^{e_s}$  und mit finiter

Induktion  $\text{ord}_p(a_1^{c_1} \cdots a_r^{c_r}) = \tau$ . Wegen  $\delta \mid \tau$  für jedes  $\delta \in \mathcal{D}_p$  gilt  $x^\tau \equiv 1 \pmod{p}$

für alle  $x \in \mathcal{A}_p^*$ . Aufgrund des *Polynomkongruenzsatzes von Lagrange* (Seite 103)

ist dann  $p - 1 \leq \tau$ . Der *Satz über die Ordnung* (Seite 120) ergibt  $\tau \mid (p - 1)$  und

damit  $\tau = p - 1$ , d.h.  $a_1^{c_1} \cdots a_r^{c_r}$  stellt eine Primitivwurzel modulo  $p$  dar.

b) Da  $g$  Primitivwurzel modulo  $p$  ist, gilt  $g^{p-1} \equiv 1 \pmod{p}$ . Für  $t = 0$  ist dann  $g^{p-1} = 1 + p u_1$  mit  $p \nmid u_1$ . Im Fall  $t = 1$  gilt  $(g+p)^{p-1} = g^{p-1} + (p-1)p g^{p-2} + p^2 v = 1 + p((p-1)g^{p-2} + p v_1) = 1 + p u'_1$  mit  $v, v_1 \in \mathbb{Z}$  und  $p \nmid u'_1$ .

Mit vollständiger Induktion erhalten wir nun

$$(4.18) \quad (g + pt)^{p^{\alpha-1}(p-1)} \equiv 1 + p^\alpha u_\alpha \pmod{p^{\alpha+1}}$$
 mit  $p \nmid u_\alpha$  für alle  $\alpha \in \mathbb{N}_1$ .

Ist  $\delta := \text{ord}_{p^k}(g + pt)$ , so ergibt sich  $(g + pt)^\delta \equiv 1 \pmod{p^k}$  und damit auch  $(g + pt)^\delta \equiv 1 \pmod{p}$ . Da  $g + pt$  Primitivwurzel modulo  $p$  ist, folgt aufgrund des *Satzes über die Ordnung* (Seite 120), dass  $(p-1) \mid \delta$  gilt. Außerdem ist  $\delta$  ein Teiler von  $\varphi(p^k) = p^{k-1}(p-1)$ . Damit gibt es ein  $r \in \mathbb{I}_k$  mit  $\delta = p^{r-1}(p-1)$ .

Gleichung (4.18) mit  $\alpha = r$  liefert

$$1 \equiv (g + pt)^{p^{r-1}(p-1)} \equiv 1 + p^r u_r \pmod{p^{r+1}}.$$

Da  $p \nmid u_r$  gilt, ergibt sich  $p^r \equiv 0 \pmod{p^{r+1}}$ . Also folgt  $r = k$  und  $\delta = \varphi(p^k)$ .

Wegen  $\varphi(p^k) = \varphi(2p^k)$  für  $p \in \mathbb{P}_3$  ist jede ungerade Primitivwurzel modulo  $p^k$  auch Primitivwurzel modulo  $2p^k$ . Ist  $h$  eine gerade Primitivwurzel modulo  $p^k$ , so stellt  $h + p^k$  eine ungerade Primitivwurzel modulo  $p^k$  und damit auch modulo  $2p^k$  dar. □

### Satz über ein Primitivwurzelkriterium

Ist  $m \in \{c p^k; c \in \mathbb{I}_2, p \in \mathbb{P}_3 \text{ und } k \in \mathbb{N}_1\}$  und sind  $q_1, \dots, q_r$  die verschiedenen Primteiler von  $\varphi(m)$ , so ist eine Zahl  $g \in \mathbb{Z}$  mit  $\text{ggT}(g, m) = 1$  genau dann eine Primitivwurzel modulo  $m$ , wenn

$$(4.19) \quad g^{\frac{\varphi(m)}{q_i}} \not\equiv 1 \pmod{m} \text{ für jedes } i \in \mathbb{I}_r$$

gilt.

**Beweis** (Zwei Teile, i) direkt, ii) indirekt, r1):

i) Es sei  $g$  eine Primitivwurzel modulo  $m$ . Dann ist  $\text{ord}_m(g) = \varphi(m)$ , d.h.  $g$  genügt (4.19).

ii) Die Zahl  $g$  erfülle (4.19). Wäre  $\delta := \text{ord}_m(g) < \varphi(m)$ , also  $\frac{\varphi(m)}{\delta} \in \mathbb{N}_2$ , so existierte zu  $q := kP\left(\frac{\varphi(m)}{\delta}\right)$  ein  $n \in \mathbb{N}_1$  mit  $\frac{\varphi(m)}{\delta} = qn$ . Damit ergäbe sich

$\frac{\varphi(m)}{q} = \delta n$ , also  $g^{\frac{\varphi(m)}{q}} \equiv g^{\delta n} \equiv (g^\delta)^n \equiv 1 \pmod{m}$  - im Widerspruch zur Voraussetzung. □

Als Beispiele bringen wir die direkt nachzuprüfenden Primitivwurzelmengen

$$\mathcal{P}_p := \{g \in \mathcal{A}_p^*; \text{ord}_p(g) = p - 1\}$$

für  $p = 3, 5, 7, 11$ :  $\mathcal{P}_3 = \{2\}$ ,  $\mathcal{P}_5 = \{2, 3\}$ ,  $\mathcal{P}_7 = \{3, 5\}$  und  $\mathcal{P}_{11} = \{2, 6, 7, 8\}$ .

Es gibt bisher kein effizientes Verfahren zur Bestimmung von Primitivwurzeln. Deshalb muss jeweils eine Primitivwurzel durch Probieren gefunden werden. Der *Satz über Indizes* (Seite 128) enthält auch eine Methode, mit der sich zu einer Primitivwurzel aus  $\mathcal{P}_p$  alle übrigen aus  $\mathcal{P}_p$  systematisch berechnen lassen.

Der *Satz über ein Primitivwurzelkriterium* liefert nur eine Testmöglichkeit, weil weitgehend unzusammenhängende Potenzen zu berechnen sind und weil im Falle eines Misserfolgs keine weiteren Zahlen ohne zusätzliche Rechnung ausgeschlossen werden können.

Zum Beispiel für  $p = 11$  mit  $\varphi(11) = 10$  und  $q_1 = 2$ ,  $q_2 = 5$  ist  $g$  genau dann Primitivwurzel, wenn  $g^2 \not\equiv 1 \pmod{11}$  und  $g^5 \not\equiv 1 \pmod{11}$  gilt. Der erste Versuch mit  $g = 2$  ergibt  $2^1 \equiv 2$ ,  $2^2 \equiv 4$ ,  $2^4 \equiv 5$  und  $2^5 \equiv 10$ . Also ist 2 Primitivwurzel modulo 11.

Für den allgemeinen Fall der Berechnung einer Primitivwurzel modulo  $p$  mit  $p \in \mathbb{P}_3$  skizzieren wir die von GAUß in Artikel 73 von [9] angegebene Methode, weil bis heute keine wesentlich bessere gefunden wurde. Sie beruht darauf, dass zu jedem  $a \in \mathcal{A}_p^*$  mit  $\text{ord}_p(a) < p - 1$  eine Zahl  $c \in \mathcal{A}_p^*$  mit  $\text{ord}_p(a) \mid \text{ord}_p(c)$  und  $\text{ord}_p(a) < \text{ord}_p(c)$  angegeben werden kann.

Es sei  $t := \text{ord}_p(a)$  und  $\mathcal{C}_{p,a} := \{h \in \mathcal{A}_p^*; \text{Es gibt } k \in \mathcal{I}_t \text{ mit } h \equiv a^k \pmod{p}\}$ . Aufgrund des *Satzes über die Ordnung* (Seite 120) ist  $\text{card } \mathcal{C}_{p,a} = t$ , und für jedes  $h \in \mathcal{C}_{p,a}$  gilt  $h^t \equiv (a^k)^t \equiv (a^t)^k \equiv 1 \pmod{p}$ , sodass  $\text{ord}_p(h)$  ein Teiler von  $t$  ist. Alle Zahlen  $h \in \mathcal{C}_{p,a}$  sind inkongruente Lösungen der Kongruenz  $x^t \equiv 1 \pmod{p}$ , und der *Polynomkongruenzsatz von Lagrange* (Seite 103) ergibt, dass  $\mathcal{A}_p^*$  keine weiteren Lösungen enthält. Für jedes  $b \in \mathcal{A}_p^* \setminus \mathcal{C}_{p,a}$  gilt also  $\text{ord}_p(b) \nmid t$ .

Es werde  $u := \text{ord}_p(b)$  gesetzt. Ist das obige  $t$  ein Teiler von  $u$ , so kann  $c := b$  gewählt werden. Andernfalls sei  $v := \text{kgV}(t, u)$ ,

$$m := \prod_{p \in \mathbb{P}} p^{\gamma'_p} \quad \text{mit} \quad \gamma'_p := \begin{cases} \nu_p(t), & \text{wenn } \nu_p(t) \geq \nu_p(u), \\ 0 & \text{sonst und} \end{cases}$$

$$n := \prod_{p \in \mathbb{P}} p^{\gamma''_p} \quad \text{mit} \quad \gamma''_p := \begin{cases} \nu_p(u), & \text{wenn } \nu_p(t) < \nu_p(u), \\ 0 & \text{sonst.} \end{cases}$$

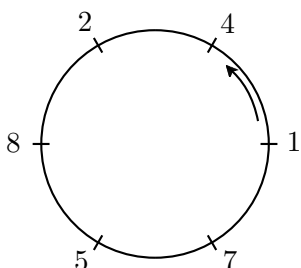
Aufgrund des *Satzes über die ggT- und kgV-Darstellung* (Seite 54) sowie des *Teilbarkeitssatzes* (Seite 53) gilt dann  $v = mn$ ,  $\text{ggT}(m, n) = 1$ ,  $m \mid t$  und  $n \mid u$ . Mit (4.16) folgt, dass  $\text{ord}_p(a^{\frac{t}{m}}) = m$  und  $\text{ord}_p(b^{\frac{u}{n}}) = n$  erfüllt ist, und (4.17) liefert  $\text{ord}_p(a^{\frac{t}{m}} b^{\frac{u}{n}}) = mn = v$ . Wegen  $t \mid v$  und  $t < v$  kann also  $c := \text{mod}(a^{\frac{t}{m}} b^{\frac{u}{n}}, p)$  gesetzt werden.

Man beginnt die Suche nach einer Primitivwurzel in  $\mathcal{A}_p^*$  mit  $a = 2$ , wählt im Falle  $\text{ord}_p(a) < p - 1$  die Zahl  $b$  möglichst klein, bestimmt  $c$ , wenn  $\text{ord}_p(b) < p - 1$  gilt, und fährt mit  $a := c$  fort, solange  $\text{ord}_p(c) < p - 1$  ist.

GAUß wählte als Beispiel  $p = 73$ , weil dieses die kleinste Primzahl ist, bei der drei Durchläufe benötigt werden. Die Mengen  $\mathcal{C}_{73, a}$  der sukzessiven Potenzreste sind  $\mathcal{C}_{73, 2} = \{2, 4, 8, 16, 32, 64, 55, 37, 1\}$ ,  $\mathcal{C}_{73, 3} = \{3, 9, 27, 8, 24, 72, 70, 64, 46, 65, 49, 1\}$  und  $\mathcal{C}_{73, 54} = \{54, 69, 3, 16, 61, 9, 48, 37, 27, 71, 38, 8, 67, 41, 24, 55, 50, 72, 19, 4, 70, 57, 12, 64, 25, 36, 46, 2, 35, 65, 6, 32, 49, 18, 23, 1\}$ , wobei sich 54 wegen  $\text{ord}_{73}(2) = 9$ ,  $\text{ord}_{73}(3) = 12$ ,  $\text{kgV}(9, 12) = 36 = 9 \cdot 4$  als  $2^{\frac{9}{3}} 3^{\frac{12}{4}}$  ergibt. Die kleinste Zahl aus  $\mathcal{A}_{73}^* \setminus \mathcal{C}_{73, 54}$  ist 5. Da in  $\mathcal{C}_{73, 54}$  genau die zu  $\mathcal{A}_{73}^*$  gehörenden Lösungen von  $x^{36} \equiv 1 \pmod{73}$  liegen, ist  $5^{36} \not\equiv 1 \pmod{73}$ . Deshalb muss aufgrund des *Satzes über ein Primitivwurzelkriterium* nur noch  $\text{mod}(5^{24}, 73)$  bestimmt werden. Dazu berechnet man  $\mathcal{C}_{73, 5}$  bis zum 24. Glied und findet  $\text{mod}(5^{24}, 73) = 8$ . Damit (und weil 2 und 3 in  $\mathcal{C}_{73, 54}$  liegen) ist 5 die kleinste Primitivwurzel in  $\mathcal{A}_{73}^*$ .

## Periodenlängen von g-adischen Brüchen

Die Dezimalbruchentwicklungen  $\frac{1}{7} = 0, \overline{142857}$ ,  $\frac{2}{7} = 0, \overline{285714}$ ,  $\frac{3}{7} = 0, \overline{428571}$ ,  $\frac{4}{7} = 0, \overline{571428}$ ,  $\frac{5}{7} = 0, \overline{714285}$  und  $\frac{6}{7} = 0, \overline{857142}$  zeigen ein Phänomen, das nur bei wenigen g-adischen Bruchentwicklungen auftritt:



Die Ziffern der Perioden gehen durch “zyklische Vertauschung” auseinander hervor, d. h. bei Anordnung auf einem Kreis ist die Reihenfolge der Ziffern stets dieselbe (siehe nebenstehende Abbildung).

Um die wesentlichen Zusammenhänge kurz darstellen zu können, beschrän-

ken wir uns auf die **g-adische Entwicklung von Brüchen**  $\frac{a}{b}$  mit  $a \in \mathbb{N}_1$ ,  $b \in \mathbb{N}_2$ ,  $a < b$ ,  $\text{ggT}(a, b) = 1$ ,  $g \in \mathbb{N}_2$  und  $\text{ggT}(b, g) = 1$ . In [20] werden g-adische Bruchentwicklungen ausführlich behandelt.

Die schon zum Lehrplan der Sekundarstufe I gehörende Methode der Umwandlung eines Bruches  $\frac{a}{b}$  in einen Dezimalbruch führt zum **g-adischen Divisionsalgorithmus**, bei dem man zunächst  $a$  durch  $b$  mit Rest dividiert und anschließend wiederholt den jeweils mit  $g$  multiplizierten Rest durch  $b$  mit Rest teilt. Die bei den Divisionen entstehenden g-adischen Ziffern bezeichnen wir für  $n \in \mathbb{N}_1$  mit  $z_n$  und die Reste mit  $r_n$ . Wegen der obigen Voraussetzung  $a < b$  ist die ganze Zahl "vor dem Komma" gleich 0, und für den zugehörigen "nullten" Rest gilt  $r_0 = a$ .

Mit der Eindeutigkeitsaussage des **Satzes über Division mit Rest** (Seite 19) und mit den anschließenden Bezeichnungen erhalten wir die Rekursionsgleichungen

$$(4.20) \quad r_0 = a, \quad r_{n+1} = \text{mod}(g r_n, b) \quad \text{und} \quad z_{n+1} = \left\lfloor \frac{g r_n}{b} \right\rfloor \quad \text{für } n \in \mathbb{N}.$$

Da bei festem  $g$  und  $b$  jeder Rest nur von dem vorhergehenden abhängt und da alle Reste in  $\mathcal{A}_b$  liegen, ergibt der **Schubfachsatz** (Seite 85), dass zwei Zahlen  $j, k$  mit  $0 \leq j < k \leq b$  und  $r_j = r_k$  existieren. Mit vollständiger Induktion folgt, dass  $r_{j+n} = r_{k+n}$  für alle  $n \in \mathbb{N}$  gilt. Damit sind  $(r_n)_{n \in \mathbb{N}}$  und  $(z_{n+1})_{n \in \mathbb{N}}$  **periodische Folgen**.

Unter der Voraussetzung  $\text{ggT}(b, g) = 1$  zeigen wir, dass  $j = 0$  gilt, womit  $(r_n)_{n \in \mathbb{N}}$  und  $(z_{n+1})_{n \in \mathbb{N}}$  **reinperiodische Folgen** darstellen. Dazu verwenden wir die aus (4.20) folgenden Gleichungen  $g r_{j-1} = z_j b + r_j$  und  $g r_{k-1} = z_k b + r_k$ . Mit  $r_j = r_k$  erhalten wir  $g(r_{j-1} - r_{k-1}) = b(z_j - z_k)$ , sodass  $b \mid g(r_{j-1} - r_{k-1})$  gilt. Aufgrund der Voraussetzung  $\text{ggT}(b, g) = 1$  ergibt der **Produktteilersatz** (Seite 23), dass  $b$  Teiler von  $r_{j-1} - r_{k-1}$  ist. Wegen  $|r_{j-1} - r_{k-1}| < b$  muss also  $r_{j-1} = r_{k-1}$  sein. Mit finiter Induktion folgt  $r_0 = r_{k-j}$ , sodass die Periodizitätsaussage mit  $j = 0$  und mit  $k - j$  anstelle von  $k$  erfüllt ist.

Die Zahl

$$\gamma := \min \{k \in \mathbb{N}_1; z_{k+m} = z_k \text{ für alle } m \in \mathbb{N}_1\}$$

wird als **Grundperiodenlänge** der g-adischen Bruchentwicklung von  $\frac{a}{b}$  bezeichnet. Die obigen Schlüsse für den Periodizitätsnachweis von  $(r_n)_{n \in \mathbb{N}}$  und (4.20) zeigen, dass  $\gamma = \min \{k \in \mathbb{N}_1; r_k = r_0\}$  gilt. Mit vollständiger Induktion leiten wir nun eine Darstellung für  $r_k$  her, die es erlaubt, die Bedingung  $r_k = r_0$  nur mit Hilfe von  $b, g$  und  $k$  auszudrücken. Ist

$\mathcal{M} := \left\{ k \in \mathbb{N}; r_k = a g^k - b \sum_{i=1}^k z_i g^{k-i} \right\}$  die Induktionsmenge, so gilt  $0 \in$

$\mathcal{M}$  wegen  $r_0 = a$ , und für jedes  $m \in \mathcal{M}$  ergibt sich  $m + 1 \in \mathcal{M}$  mit Hilfe

der aus (4.20) folgenden Gleichung  $r_{m+1} = g r_m - b z_{m+1}$ . Also ist  $\mathcal{M} = \mathbb{N}$ .  
Damit gilt  $r_k = r_0$  genau dann, wenn  $a(g^k - 1) = b \sum_{i=1}^k z_i g^{k-i}$  erfüllt ist.

Wegen der Voraussetzung  $\text{ggT}(a, b) = 1$  muss aufgrund des **Produktteilersatzes**  $b \mid (g^k - 1)$  gelten, und es folgt

$$(4.21) \quad \gamma = \min \left\{ k \in \mathbb{N}_1 ; g^k \equiv 1 \pmod{b} \right\} = \text{ord}_b(g).$$

Unser Ausgangsproblem der zyklisch vertauschten Ziffern können wir nun klären, wenn wir beachten, dass  $r_0 = a$  gilt. Gehört zu der  $g$ -adischen Bruchentwicklung von  $\frac{a}{b}$  die Restfolge  $(r_n)_{n \in \mathbb{N}}$ , so hat  $\frac{r_s}{b}$  für jedes  $s \in \mathbb{N}_1$  die Restfolge  $(r_{n+s})_{n \in \mathbb{N}}$ . Die Bruchentwicklung von  $\frac{r_{t+1}}{b}$  geht also für jedes  $t \in \mathbb{N}_1$  aus derjenigen von  $\frac{r_t}{b}$  durch Verschiebung der Ziffern um eine Stelle nach links hervor, was für die Periode eine zyklische Vertauschung bedeutet.

Sollen die Grundperioden der Entwicklungen aller Brüche  $\frac{c}{b}$  mit  $c \in \mathcal{I}_{b-1}$  durch zyklische Vertauschung entstehen, so muss jede der Zahlen aus  $\mathcal{I}_{b-1}$  als Rest vorkommen. Wegen (4.21) gilt dann  $\text{ord}_b(g) = b - 1$ . Der **Satz über die Ordnung** (Seite 120) und der **Satz über die Eulersche  $\varphi$ -Funktion** (Seite 98) ergeben  $b - 1 = \text{ord}_b(g) \leq \varphi(b) \leq b - 1$ . Also muss einerseits  $\varphi(b) = b - 1$  und andererseits  $\text{ord}_b(g) = \varphi(b)$  sein.

Für alle  $b \in \mathbb{N}_2 \setminus \mathbb{P}$  gilt

$$\varphi(b) = b \prod_{\substack{p \in \mathbb{P} \\ p \mid b}} \left( 1 - \frac{1}{p} \right) \leq b \left( 1 - \frac{1}{kP(b)} \right) = b - \frac{b}{kP(b)} < b - 1.$$

Deshalb ist  $\varphi(b) = b - 1$  nur für  $b \in \mathbb{P}$  erfüllt. Die Gleichung  $\text{ord}_b(g) = \varphi(b)$  bedeutet definitionsgemäß, dass  $g$  eine Primitivwurzel modulo  $b$  ist.

Zusammenfassend haben wir also unter den anfangs genannten Bedingungen für  $a$ ,  $b$  und  $g$ , dass die  $g$ -adische Bruchentwicklung von  $\frac{a}{b}$  genau dann die maximale Grundperiodenlänge  $\gamma = b - 1$  besitzt, wenn  $b \in \mathbb{P}$  ist und  $g$  eine Primitivwurzel modulo  $b$  darstellt. Nur in diesem Falle gehen die Grundperioden der  $g$ -adischen Entwicklungen aller Brüche  $\frac{c}{b}$  mit  $c \in \mathcal{I}_{b-1}$  durch zyklische Vertauschung auseinander hervor.

Für  $g = 10$  tritt diese Situation ein, wenn  $b \in \{7, 17, 19, 23, 29, 47, \dots\}$  ist. Vermutlich gibt es zu jedem  $g \in \mathbb{N}_2$  mit  $\sqrt{g} \notin \mathbb{N}$  unendlich viele Primzahlen  $b$ , sodass  $g$  Primitivwurzel modulo  $b$  ist ("Artinsche Vermutung").

Wir schließen dieses Kapitel mit einem Begriff, dessen Bedeutung GAUß in Artikel 57 von [9] durch Vergleich mit den Logarithmen hervorhebt.

### Bezeichnung der Indizes

Es sei  $m \in \{cp^k; c \in \mathcal{I}_2, p \in \mathbb{P}_3 \text{ und } k \in \mathbb{N}_1\}$  und  $g$  sei eine Primitivwurzel modulo  $m$ . Ist  $a \in \mathbb{Z}$  mit  $\text{ggT}(a, m) = 1$ , so heißt die eindeutig bestimmte Zahl  $\gamma \in \mathcal{A}_{\varphi(m)}$  mit  $a \equiv g^\gamma \pmod{m}$  *Index von  $a$  modulo  $m$  (zur Basis  $g$ )*. Sie wird mit  $\text{ind}_g a$  oder kurz mit  $\text{ind } a$  bezeichnet.

### Satz über Indizes

Es sei  $m \in \{cp^k; c \in \mathcal{I}_2, p \in \mathbb{P}_3 \text{ und } k \in \mathbb{N}_1\}$  und  $a \in \mathbb{Z}$  mit  $\text{ggT}(a, m) = 1$ . Ist  $n \in \mathbb{N}_2$  und  $d := \text{ggT}(n, \varphi(m))$ , so gilt:

a) Die Kongruenz  $x^n \equiv a \pmod{m}$  ist genau dann lösbar (und  $a$  ist dann  $n$ -ter Potenzrest modulo  $m$ ), wenn  $\text{ind}_g a$  durch  $d$  teilbar ist. Im Falle der Lösbarkeit hat die Kongruenz  $d$  Lösungen.

b) Die Zahl  $a$  ist genau dann  $n$ -ter Potenzrest modulo  $m$ , wenn  $a^{\frac{\varphi(m)}{d}} \equiv 1 \pmod{m}$  gilt. Die Anzahl der  $n$ -ten Potenzreste in einem reduzierten Restsystem modulo  $m$  ist  $\frac{\varphi(m)}{d}$ .

c) Zwischen dem Index  $\text{ind}_g a$  und der Ordnung  $\text{ord}_m(a)$  modulo  $m$  besteht die Beziehung  $\text{ord}_m(a) = \frac{\varphi(m)}{\text{ggT}(\text{ind}_g a, \varphi(m))}$ . Insbesondere ist  $\text{ggT}(\text{ind}_g a, \varphi(m))$  unabhängig von der Primitivwurzel  $g$ , und  $a$  ist Primitivwurzel modulo  $m$  genau dann, wenn  $\text{ggT}(\text{ind}_g a, \varphi(m)) = 1$  gilt.

d) Stellt  $\mathcal{R}_m^*$  ein reduziertes Restsystem modulo  $m$  dar und ist  $\vartheta$  ein Teiler von  $\varphi(m)$ , so gilt  $\text{card}\{a \in \mathcal{R}_m^*; \text{ord}_m(a) = \vartheta\} = \varphi(\vartheta)$ . Insbesondere ist  $\varphi(\varphi(m))$  die Anzahl der Primitivwurzeln in  $\mathcal{R}_m^*$ .

**Beweis** (direkt, a1):

a) Aufgrund des *Satzes über die Ordnung* (Seite 120) ist  $x^n \equiv a \pmod{m}$  wegen  $x^n \equiv (g^{\text{ind } x})^n \pmod{m}$  und  $a \equiv g^{\text{ind } a} \pmod{m}$  äquivalent zu  $n \text{ ind } x \equiv \text{ind } a \pmod{\varphi(m)}$ . Ersetzt man  $\text{ind } x$  durch  $y$ , so ergibt der *Satz über die Lösungsanzahl der linearen Kongruenz* (Seite 101), dass  $ny \equiv \text{ind } a \pmod{\varphi(m)}$  genau dann lösbar ist, wenn  $d \mid \text{ind } a$  gilt. Falls  $ny \equiv \text{ind } a \pmod{\varphi(m)}$  lösbar ist, gibt es  $d$  modulo  $\varphi(m)$  inkongruente Werte für  $y$ . Ihnen entsprechen  $d$  modulo  $m$  inkongruente Werte für  $x$ , weil es zu jeder Lösung  $y$  ein  $x \in \mathcal{A}_m^*$  gibt, sodass  $\text{ind } x$  eine zu  $y$  modulo  $\varphi(m)$  kongruente Lösung darstellt.

**b)** Die Bedingung  $d \mid \text{ind } a$  aus i) ist äquivalent zu  $\frac{\varphi(m)}{d} \text{ind } a \equiv 0 \pmod{\varphi(m)}$  und damit zu  $a^{\frac{\varphi(m)}{d}} \equiv 1 \pmod{m}$ .

In  $\mathcal{A}_{\varphi(m)}$  ist die Anzahl der durch  $d$  teilbaren Elemente gleich  $\frac{\varphi(m)}{d}$ . Wegen a) ist dieses auch die Anzahl der  $n$ -ten Potenzreste in jedem reduzierten Restsystem modulo  $m$ .

**c)** Wird  $\delta := \text{ord}_m(a)$  gesetzt, so ist  $\delta$  der kleinste Teiler von  $\varphi(m)$  mit  $a^\delta \equiv 1 \pmod{m}$ . Die Kongruenz ist äquivalent mit  $\delta \text{ind } a \equiv 0 \pmod{\varphi(m)}$ , also mit  $\frac{\varphi(m)}{\delta} \mid \text{ind } a$ . Damit ist  $\frac{\varphi(m)}{\delta}$  der größte Teiler von  $\varphi(m)$ , der auch  $\text{ind } a$  teilt, d. h. es gilt  $\frac{\varphi(m)}{\delta} = \text{ggT}(\text{ind } a, \varphi(m))$ .

**d)** In der Indexmenge  $\mathcal{A}_{\varphi(m)}$  haben die durch  $\frac{\varphi(m)}{\vartheta}$  teilbaren Zahlen die Form  $\frac{\varphi(m)}{\vartheta} y$  mit  $y \in \mathcal{A}_{\vartheta}$ . Die aus c) folgende Bedingung  $\text{ggT}\left(\frac{\varphi(m)}{\vartheta} y, \varphi(m)\right) = \frac{\varphi(m)}{\vartheta}$  ist äquivalent mit  $\text{ggT}(y, \vartheta) = 1$ . Dieser Forderung genügen genau die  $\varphi(\vartheta)$  Werte  $y \in \mathcal{A}_{\vartheta}^*$ . □

Wegen des großen Nutzens der Indizes für zahlentheoretische Untersuchungen wurde 1839 von C. G. J. JACOBI eine Sammlung von Indextafeln für alle Moduln  $m$  unterhalb 1000, zu denen Primitivwurzeln existieren, herausgegeben. Da dieses schon lange vergriffene Werk mit dem Titel “*Canon Arithmeticus*” zahlreiche Fehler enthielt, erschien 1956 eine vollständig neu berechnete und erweiterte Ausgabe. Die Indizes werden dabei mit Hilfe der ebenfalls abgedruckten “*Numerustafeln*” bestimmt, die zu den Argumenten  $I \in \mathcal{I}_{\varphi(m)}$  die Werte  $N := \text{mod}(g^I, m)$  enthalten, wobei  $g$  die kleinste positive Primitivwurzel modulo  $m$  ist.

Als Beispiel folgen die Numerustafel und die Indextafel für  $p = 11$  mit  $g = 2$ .

|   |   |   |   |   |    |   |   |   |   |    |
|---|---|---|---|---|----|---|---|---|---|----|
| I | 1 | 2 | 3 | 4 | 5  | 6 | 7 | 8 | 9 | 10 |
| N | 2 | 4 | 8 | 5 | 10 | 9 | 7 | 3 | 6 | 1  |

|   |    |   |   |   |   |   |   |   |   |    |
|---|----|---|---|---|---|---|---|---|---|----|
| N | 1  | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
| I | 10 | 1 | 8 | 2 | 4 | 9 | 7 | 3 | 6 | 5  |

Die Indizes sind modulo  $\varphi(m)$  “multiplikativ”: Aus  $a \equiv g^{\text{ind } a} \pmod{m}$  und  $b \equiv g^{\text{ind } b} \pmod{m}$  folgt nämlich  $ab \equiv g^{\text{ind } a + \text{ind } b} \pmod{m}$ , also  $\text{ind}(ab) \equiv \text{ind } a + \text{ind } b \pmod{\varphi(m)}$ . Deshalb heißen die Indizes auch *diskrete Logarithmen*.

## 4.9 Aufgaben und Probleme zu Kapitel 4

### Aufgabe 4.1:

Es sei  $n \in \mathbb{N}_1$  und  $\mathcal{M}$  sei eine Teilmenge von  $\{1, 2, \dots, 2n\}$  mit  $\text{card } \mathcal{M} = n + 1$ .  
Beweisen Sie, dass es zwei Zahlen  $a, b \in \mathcal{M}$  mit  $a \neq b$  und  $a \mid b$  gibt.

[Hinweis: Schreiben Sie die Zahlen aus  $\mathcal{M}$  in der Form  $2^k u$  mit  $2 \nmid u$ , und wenden Sie den *Schubfachsatz* an.]

### Aufgabe 4.2:

a) Es sei  $p \in \mathbb{P}$  und  $a \in \mathbb{N}_1$  mit  $a < p$ . Zeigen Sie, dass  $ax \equiv b \pmod{p}$  die Lösung  $x \equiv (-1)^{a-1} bc \pmod{p}$  mit  $c := \frac{1}{a} \binom{p-1}{a-1} \in \mathbb{N}_1$  besitzt.

[Hinweis: Beachten Sie, dass  $\binom{p}{a} = \frac{p}{a} \binom{p-1}{a-1}$  gilt.]

b) Lösen Sie die Kongruenz  $256x \equiv 179 \pmod{337}$  mit Hilfe des Kettenbruchalgorithmus.

### Aufgabe 4.3:

Beweisen Sie die folgenden Aussagen:

i)  $m^7 \equiv m \pmod{42}$  für alle  $m \in \mathbb{Z}$ ,

ii)  $3m^5 + 5m^3 \equiv 8m \pmod{15}$  für alle  $m \in \mathbb{Z}$ ,

iii)  $3 \cdot 5^{2n+1} + 2^{3n+1} \equiv 0 \pmod{17}$  für alle  $n \in \mathbb{N}$ .

### Aufgabe 4.4:

Lösen Sie das folgende Kongruenzsystem:

$x \equiv 1 \pmod{3}$ ,  $x \equiv 4 \pmod{5}$ ,  $x \equiv 2 \pmod{7}$ ,  $x \equiv 9 \pmod{11}$ ,  $x \equiv 3 \pmod{13}$ .

### Aufgabe 4.5:

Es sei  $p \in \mathbb{P}_3$  und  $i^{-1}$  sei zu  $i$  modulo  $p$  assoziiert. Beweisen Sie die Kongruenz

$$\sum_{i=1}^{p-1} (-1)^{i+1} i^{-1} \equiv \frac{2^p - 2}{p} \pmod{p}.$$

[Hinweis: Drücken Sie die rechte Seite mit Hilfe von Binomialkoeffizienten aus und beachten Sie Aufgabe 4.2.]

**Aufgabe 4.6:**

Es sei  $n \in \mathbb{N}_2$ . Zeigen Sie, dass  $\omega(n^2 + 2n) = 2$  genau dann gilt, wenn  $4(n-1)! + n + 4 \equiv 0 \pmod{(n^2 + 2n)}$  erfüllt ist.

**Aufgabe 4.7:**

Es seien  $m, n \in \mathbb{N}_2$  mit  $\text{ggT}(m, n^2 - n) = 1$ . Weisen Sie nach, dass es ein  $k \in \{1, \dots, m-2\}$  gibt, für das  $m \mid \left(\sum_{i=0}^k n^i\right)$  gilt.

**Aufgabe 4.8:**

Es sei  $p \in \mathbb{P}_5$  und  $\sum_{k=0}^{p-2} c_k x^k := \prod_{j=1}^{p-1} (x-j) - x^{p-1} + 1$ . Beweisen Sie, dass  $p \mid c_k$  für  $k = 2, \dots, p-2$  und  $p^2 \mid c_1$  gilt.

[Hinweis: Sie können  $x = p$  setzen, nachdem Sie den *Polynomkongruenzsatz von Lagrange* und den *Fermatschen Kongruenzsatz* angewendet haben.]

**Aufgabe 4.9:**

Berechnen Sie die Zahlen  $a \in \mathcal{A}_5$ ,  $b \in \mathcal{A}_7$  und  $c \in \mathcal{A}_{11}$ , für die  $\{x \in \mathbb{Z} ; x \equiv 348 \pmod{385}\}$  die Lösungsmenge des Kongruenzsystems

$$ax \equiv -1 \pmod{5}, \quad bx \equiv 2 \pmod{7}, \quad cx \equiv -3 \pmod{11}$$

darstellt.

**Aufgabe 4.10:**

Lösen Sie die Kongruenzen i)  $x^2 \equiv 5 \pmod{19}$  und ii)  $x^2 \equiv 5 \pmod{29}$ .

**Aufgabe 4.11:**

Bestimmen Sie unter Verwendung des Jacobi-Symbols die Anzahl der Lösungen der Kongruenzen i)  $x^2 \equiv 3766 \pmod{5987}$  und ii)  $x^2 \equiv 3149 \pmod{5987}$ .

**Aufgabe 4.12:**

i) Zeigen Sie, dass  $\left(\frac{d}{p}\right) = 1$  für alle  $(d, p) \in \mathbb{Z} \times \mathbb{P}$  mit  $p \equiv 1 \pmod{4}$  und

$d \mid \frac{p-1}{4}$  gilt.

ii) Bestimmen Sie alle Primzahlen  $p$ , für die  $\left(\frac{6}{p}\right) = -1$  ist.

**Aufgabe 4.13:**

Zeigen Sie, dass  $\left(\frac{-5}{p}\right) = (-1)^{\left[\frac{p}{10}\right]}$  für alle  $p \in \mathbb{P} \setminus \{2, 5\}$  gilt.

**Aufgabe 4.14:**

Beweisen Sie, dass  $\sum_{j=1}^{p-1} \left( \frac{j(j+k)}{p} \right) = -1$  für alle  $(k, p) \in \mathbb{Z} \times \mathbb{P}_3$  mit  $p \nmid k$  gilt.

[Hinweis: Nehmen Sie die reziproken Reste von  $j$  modulo  $p$  zu Hilfe.]

**Aufgabe 4.15:**

Beweisen Sie, dass  $p \mid \sum_{k=1}^{p-1} \left( 1 + \left( \frac{k}{p} \right) \right) k^n$  für alle  $(p, n) \in \mathbb{P}_3 \times \mathbb{N}_1$  mit  $\frac{p-1}{2} \nmid n$  gilt.

[Hinweis: Zeigen Sie zunächst, dass es ein  $g \in \mathbb{Z}$  mit  $\left( \frac{g}{p} \right) = 1$  und  $g^n \not\equiv 1 \pmod{p}$  gibt.]

**Aufgabe 4.16:**

Zeigen Sie, dass  $\left( \frac{a}{m+2a} \right) = (-1)^{\left[ \frac{a}{2} \right]} \left( \frac{a}{m} \right)$  für alle  $(a, m) \in \mathbb{N}_1 \times \mathbb{N}_3$  mit  $2 \nmid m$  und  $\text{ggT}(a, m) = 1$  gilt.

Die nächsten vier Probleme stammen aus dem Bundeswettbewerb Mathematik, die übrigen wurden bei der Internationalen Mathematikolympiade gestellt.

**Problem 34:**

Man beweise, dass jede natürliche Zahl  $k$  ( $k > 1$ ) ein Vielfaches besitzt, das kleiner als  $k^4$  ist und im Zehnersystem mit höchstens vier verschiedenen Ziffern geschrieben wird.

**Problem 35:**

Die Folge  $z_0, z_1, z_2, \dots$  wird rekursiv definiert durch  $z_0 := 0$ ,

$$z_n := z_{n-1} + \frac{1}{2} (3^r - 1), \text{ wenn } n = 3^{r-1}(3k + 1) \text{ ist, und}$$

$$z_n := z_{n-1} - \frac{1}{2} (3^r + 1), \text{ wenn } n = 3^{r-1}(3k + 2)$$

jeweils für geeignete ganze Zahlen  $r, k$  ist.

Man beweise: In dieser Folge tritt jede ganze Zahl genau einmal auf.

**Problem 36:**

Kann man aus 100 beliebig gegebenen ganzen Zahlen stets 15 Zahlen derart auswählen, dass die Differenz zweier beliebiger dieser 15 Zahlen durch 7 teilbar ist? Wie lautet die Antwort, wenn 15 durch 16 ersetzt wird? (Beweis!)

**Problem 37:**

Beweise: Unter 79 aufeinanderfolgenden natürlichen Zahlen gibt es stets mindestens eine, deren Quersumme durch 13 teilbar ist. Zeige durch ein Gegenbeispiel, dass sich hierbei die Zahl 79 nicht durch die Zahl 78 ersetzen lässt.

**Problem 38:**

Die positiven ganzen Zahlen  $a$  und  $b$  sind derart, dass die Zahlen  $15a + 16b$  und  $16a - 15b$  beide Quadrate von positiven ganzen Zahlen sind. Man bestimme den kleinsten möglichen Wert, den das Minimum dieser beiden Quadrate annehmen kann.

**Problem 39:**

Es sei  $n$  eine natürliche Zahl größer als 6 und es seien  $a_1, a_2, \dots, a_k$  alle diejenigen natürlichen Zahlen, die kleiner als  $n$  und teilerfremd zu  $n$  sind. Man beweise: Falls  $a_2 - a_1 = a_3 - a_2 = \dots = a_k - a_{k-1} > 0$ , dann ist  $n$  entweder eine Primzahl oder eine Potenz von 2 mit natürlichem Exponenten.

**Problem 40:**

Sei  $d$  eine positive ganze Zahl ungleich 2, 5, 13. Man zeige, dass es in der Menge  $\{2, 5, 13, d\}$  zwei verschiedene Elemente  $a, b$  gibt, für die  $ab - 1$  keine Quadratzahl ist.

**Problem 41:**

Es sei  $M$  eine Menge aus 1985 verschiedenen positiven ganzen Zahlen. Keine dieser Zahlen hat einen Primteiler größer als 26. Man beweise: In  $M$  gibt es vier paarweise verschiedene Elemente, für die ihr Produkt die vierte Potenz einer ganzen Zahl ist.

**Problem 42:**

Man finde ein Paar  $a, b$  positiver ganzer Zahlen, die folgenden Bedingungen genügen:

(1) Die Zahl  $ab(a + b)$  ist nicht durch 7 teilbar,

(2)  $(a + b)^7 - a^7 - b^7$  ist durch  $7^7$  teilbar.

Begründe die Antwort!

**Problem 43:**

Gibt es 1983 verschiedene positive ganze Zahlen kleiner oder gleich  $10^5$ , unter denen keine drei die aufeinanderfolgenden Glieder einer arithmetischen Folge sind? (Die Antwort ist zu begründen.)

**Problem 44:**

Es seien  $m$  und  $n$  natürliche Zahlen mit  $1 \leq m, n \leq 1981$ .

Es gelte  $(n^2 - mn - m^2)^2 = 1$ . Man bestimme den maximalen Wert von  $m^2 + n^2$ .

**Problem 45:**

a) Für welche Werte von  $n > 2$  gibt es  $n$  aufeinanderfolgende positive ganze Zahlen so, dass die größte dieser Zahlen ein Teiler des kleinsten gemeinsamen Vielfachen der übrigen  $n - 1$  Zahlen ist?

b) Für welche Werte von  $n > 2$  gibt es genau eine Folge mit dieser Eigenschaft?

**Problem 46:**

Seien  $p$  und  $q$  natürliche Zahlen, sodass  $\frac{p}{q} = 1 - \frac{1}{2} + \frac{1}{3} - \frac{1}{4} + \dots - \frac{1}{1318} + \frac{1}{1319}$  gilt. Man beweise, dass  $p$  durch 1979 teilbar ist.

**Problem 47:**

Bei einem Sportwettkampf wurden  $m$  Medaillen im Laufe von  $n$  Tagen ( $n > 1$ ) verliehen.

Am 1. Tage wurden eine Medaille und  $\frac{1}{7}$  der übrigen  $m - 1$ , am 2. Tage 2 Medaillen und  $\frac{1}{7}$  des nun verbliebenen Restes verliehen usw. Schließlich wurden am  $n$ -ten Tage gerade  $n$  Medaillen vergeben, ohne dass noch welche übrig blieben. Wieviel Tage dauerte der Wettkampf, und wieviel Medaillen wurden insgesamt verliehen?

**Problem 48:**

Man beweise, dass die Folge  $(2^{n+2} - 3)_{n \in \mathbb{N}}$  mindestens eine unendliche Teilfolge mit paarweise teilerfremden Elementen enthält.

**Problem 49:**

Es seien  $m$  und  $n$  beliebige nichtnegative ganze Zahlen. Es ist zu zeigen, dass  $\frac{(2m)!(2n)!}{m!n!(m+n)!}$  mit  $0! = 1$  eine ganze Zahl ist.

**Problem 50:**

Es sei  $A$  die Summe der Ziffern der im dekadischen Zahlensystem dargestellten Zahl  $4444^{4444}$ . Es sei  $B$  die Summe der Ziffern von  $A$ . Man berechne die Summe der Ziffern von  $B$ . (Alle Zahlen sind im dekadischen Zahlensystem dargestellt.)

**Problem 51:**

Man bestimme den größten Wert des Produktes positiver ganzer Zahlen, deren Summe 1976 ist.

**Problem 52:**

Eine Zahlenfolge  $u_0, u_1, u_2, \dots$  sei wie folgt definiert:

$$u_0 = 2, \quad u_1 = \frac{5}{2}, \quad u_{n+1} = u_n (u_{n-1}^2 - 2) - u_1, \quad n = 1, 2, \dots$$

Man zeige, dass  $[u_n] = 2^{\frac{1}{3}(2^n - (-1)^n)}$  gilt,  $n = 1, 2, \dots$

$[x]$  bezeichnet die größte ganze Zahl, die nicht größer als  $x$  ist.

**Problem 53:**

Es seien  $a$  und  $b$  natürliche Zahlen, für die  $ab + 1$  ein Teiler von  $a^2 + b^2$  ist. Man zeige, dass dann  $\frac{a^2+b^2}{ab+1}$  das Quadrat einer ganzen Zahl darstellt.

**Problem 54:**

Man bestimme alle natürlichen Zahlen  $n > 1$ , für die  $(2^n + 1)n^{-2}$  eine ganze Zahl ist.

**Problem 55:**

Es sei  $S = \{1, 2, \dots, 280\}$ . Man bestimme die kleinste natürliche Zahl  $n$  mit folgender Eigenschaft: In jeder  $n$ -elementigen Teilmenge von  $S$  gibt es 5 Elemente, die paarweise teilerfremd sind.

**Problem 56:**

Man bestimme alle geordneten Paare  $(m, n)$  von natürlichen Zahlen, sodass  $\frac{n^3+1}{mn-1}$  eine natürliche Zahl ist.

**Problem 57:**

Man bestimme alle ganzen Zahlen  $a, b, c$  mit  $1 < a < b < c$ , so dass  $(a-1)(b-1)(c-1)$  ein Teiler von  $abc-1$  ist.

**Problem 58:**

Für eine beliebige natürliche Zahl  $k$  sei  $f(k)$  die Anzahl jener Elemente in der Menge  $\{k+1, k+2, \dots, 2k\}$ , deren Binärdarstellung genau drei Einsen enthält.

a) Man zeige: Zu jeder natürlichen Zahl  $m$  gibt es wenigstens eine natürliche Zahl  $k$ , sodass  $f(k) = m$  ist.

b) Man bestimme alle natürlichen Zahlen  $m$ , für die es genau ein  $k$  mit  $f(k) = m$  gibt.

**Problem 59:**

Man zeige, dass für keine natürliche Zahl  $n$  die Zahl  $\sum_{k=0}^n \binom{2n+1}{2k+1} 2^{3k}$  durch 5 teilbar ist.

**Problem 60:**

Für jede natürliche Zahl  $n$  bezeichne  $s(n)$  die größte natürliche Zahl, für die gilt: Für jede natürliche Zahl  $k$  mit  $k \leq s(n)$  lässt sich die Zahl  $n^2$  als Summe von genau  $k$  Quadraten natürlicher Zahlen schreiben.

a) Man beweise  $s(n) \leq n^2 - 14$  für jedes  $n \geq 4$ .

b) Man gebe eine ganze Zahl  $n$  mit  $s(n) = n^2 - 14$  an.

c) Man beweise, dass es unendlich viele ganze Zahlen  $n$  mit  $s(n) = n^2 - 14$  gibt.

**Problem 61:**

Zu Beginn ist eine natürliche Zahl  $n_0 > 1$  gegeben. Zwei Spieler  $A$  und  $B$  wählen abwechselnd natürliche Zahlen  $n_1, n_2, n_3, \dots$  nach den folgenden Regeln: Nach der  $k$ -ten Runde kennt  $A$  die Zahl  $n_{2k}$  und wählt  $n_{2k+1}$  derart, dass  $n_{2k} \leq n_{2k+1} \leq n_{2k}^2$  ist,  $k = 0, 1, \dots$ .

Kennt nun  $B$  die natürliche Zahl  $n_{2k+1}$ , dann wählt er die natürliche Zahl  $n_{2k+2}$  derart, dass  $\frac{n_{2k+1}}{n_{2k+2}} = p^r$ , wobei  $p$  eine Primzahl und  $r \geq 1$  eine natürliche Zahl ist.

Der Spieler  $A$  gewinnt das Spiel, sobald er die Zahl 1990,  $B$  gewinnt, sobald er die Zahl 1 wählt. Für welche  $n_0$  kann

a)  $A$  einen Gewinn erzwingen,

b)  $B$  einen Gewinn erzwingen und

c) keiner der Spieler einen Gewinn erzwingen?

# Kapitel 5

## Ergänzungen

### 5.1 Die Faltung zahlentheoretischer Funktionen

Die folgenden speziellen Abbildungen von  $\mathbb{N}_1$  in eine Zahlenmenge wurden bisher als *zahlentheoretische Funktionen* eingeführt: die *Teileranzahlfunktion*  $d$  (Seite 18), die *Anzahlfunktion der Primteiler*  $\omega$  (Seite 53), die *Anzahlfunktion der Primpotenzteiler*  $\Omega$  (Seite 53), die *Teilersummenfunktion*  $\sigma$  (Seite 56), die *Möbiussche  $\mu$ -Funktion*  $\mu$  (Seite 64) und die *Eulersche  $\varphi$ -Funktion*  $\varphi$  (Seite 94). Hier sollen einige allgemeine Zusammenhänge zwischen diesen und weiteren zahlentheoretischen Funktionen dargestellt werden, wobei im ersten Teil der folgenden Definition der Begriff der “zahlentheoretischen Eigenschaft” vage bleibt.

#### Definition der (multiplikativen) zahlentheoretischen Funktion

Eine Funktion  $f : \mathbb{N}_1 \rightarrow \mathbb{C}$  heißt *zahlentheoretische Funktion*, wenn das Bildungsgesetz von  $f$  auf zahlentheoretischen Eigenschaften beruht und wenn es ein  $m \in \mathbb{N}_1$  mit  $f(m) \neq 0$  gibt.

Eine zahlentheoretische Funktion  $f$  heißt *multiplikativ*, wenn  $f(ab) = f(a)f(b)$  für alle  $a, b \in \mathbb{N}_1$  mit  $\text{ggT}(a, b) = 1$  gilt.<sup>1</sup>

Für alle multiplikativen Funktionen gilt  $f(1) = 1$ , denn für jede Zahl  $m$  mit  $f(m) \neq 0$  folgt  $f(m) = f(1 \cdot m) = f(1)f(m)$ , also  $f(m)(f(1) - 1) = 0$ , woraus man durch Kürzen die Behauptung erhält.

<sup>1</sup> Im Folgenden sind mit multiplikativen Funktionen stets multiplikative zahlentheoretische Funktionen gemeint.

Die Multiplikativität von  $d$ ,  $\sigma$  und  $\varphi$  ergibt sich jeweils aus der Produktdarstellung im Satz über die Teileranzahlfunktion (Seite 55), im Satz über die Teilersummenfunktion (Seite 57) und im Satz über die Eulersche  $\varphi$ -Funktion (Seite 98). Bei der Möbiusschen  $\mu$ -Funktion liefert schon die Definition mit Fallunterscheidung die Multiplikativität. Dagegen zeigen die Werte  $\omega(1) = \Omega(1) = 0$ , dass  $\omega$  und  $\Omega$  nicht multiplikativ sind.

### Bezeichnung der Faltung und der Summatorfunktion

Sind  $f$  und  $g$  zahlentheoretische Funktionen, so heißt die zahlentheoretische Funktion  $f \star g : \mathbb{N}_1 \rightarrow \mathbb{C}$ ,  $n \mapsto \sum_{d|n} f(d) g\left(\frac{n}{d}\right)$  *Faltung*<sup>2</sup> von  $f$  und  $g$ .

Die zahlentheoretische Funktion  $F := f \star e$  mit  $e : \mathbb{N}_1 \rightarrow \mathbb{C}$ ,  $n \mapsto 1$  heißt *Summatorfunktion* von  $f$ .

### Satz über die Faltung multiplikativer Funktionen

Sind  $f$  und  $g$  multiplikative Funktionen, so ist auch  $f \star g$  multiplikativ.

**Beweis** (direkt, r1):

Es seien  $n_1, n_2 \in \mathbb{N}_1$  mit  $\text{ggT}(n_1, n_2) = 1$ . Wir zeigen zunächst einen Zusammenhang zwischen  $\mathcal{D}_1 := \{d \in \mathbb{N}_1 ; d \mid n_1 n_2\}$  und  $\mathcal{D}_2 := \{d \in \mathbb{N}_1 ; \text{Es gibt genau ein Paar } (d_1, d_2) \in \mathbb{N}_1^2 \text{ mit } d = d_1 d_2 \text{ und } d_1 \mid n_1 \text{ und } d_2 \mid n_2\}$ .

Ist  $d \in \mathcal{D}_1$ , so gibt es wegen des *Hauptsatzes* (Seite 49) genau ein Paar  $(d_1, d_2) \in \mathbb{N}_1^2$  mit  $d = d_1 d_2$  und  $d_1 \mid n_1$  und  $d_2 \mid n_2$ . Also gilt  $d \in \mathcal{D}_2$ , d. h.  $\mathcal{D}_1 \subseteq \mathcal{D}_2$ .

Umgekehrt folgt aus  $d \in \mathcal{D}_2$  unmittelbar  $d \mid (n_1 n_2)$ , also  $d \in \mathcal{D}_1$ , d. h.  $\mathcal{D}_1 = \mathcal{D}_2$ .

Damit gilt

$$\begin{aligned} (f \star g)(n_1 n_2) &= \sum_{d|(n_1 n_2)} f(d) g\left(\frac{n_1 n_2}{d}\right) \\ &= \sum_{\substack{(d_1, d_2) \in \mathbb{N}_1^2 \\ d_1 | n_1, d_2 | n_2}} f(d_1 d_2) g\left(\frac{n_1 n_2}{d_1 d_2}\right) \end{aligned}$$

<sup>2</sup> Die Faltung zahlentheoretischer Funktionen heißt auch *Dirichlet-Faltung*.

$$\begin{aligned}
 &= \sum_{d_1|n_1} \sum_{d_2|n_2} f(d_1) f(d_2) g\left(\frac{n_1}{d_1}\right) g\left(\frac{n_2}{d_2}\right) \\
 &= \left( \sum_{d_1|n_1} f(d_1) g\left(\frac{n_1}{d_1}\right) \right) \left( \sum_{d_2|n_2} f(d_2) g\left(\frac{n_2}{d_2}\right) \right) \\
 &= (f \star g)(n_1) (f \star g)(n_2). \quad \square
 \end{aligned}$$

Oben haben wir die Multiplikativität von  $d$ ,  $\sigma$ ,  $\varphi$  und  $\mu$  mit Hilfe der jeweiligen Produktdarstellung bewiesen. In dem folgenden Satz wird gezeigt, dass die Summatorfunktion jeder multiplikativen Funktion eine Produktdarstellung besitzt.

**Satz über die Summatorfunktion**

Ist  $f$  eine multiplikative Funktion und  $F := f \star e$ , so gilt  $F(n) = \prod_{k=1}^r \left( \sum_{j=0}^{e_k} f(q_k^j) \right)$  für alle  $n \in \mathbb{N}_2$ , wobei  $n = \prod_{k=1}^r q_k^{e_k}$  die *Primpotenzdarstellung* von  $n$  ist.

**Beweis** (direkt, r1):

Da auch  $e$  multiplikativ ist, folgt die Multiplikativität von  $F$  aus dem *Satz über die Faltung multiplikativer Funktionen*. Wegen  $\text{ggT}(q_k^{e_k}, n q_k^{-e_k}) = 1$  ergibt finite Induktion, dass  $F(n) = \prod_{k=1}^r \left( \sum_{d|q_k^{e_k}} f(d) \right)$  gilt. □

Bei den folgenden Beispielen ist stets  $n = \prod_{k=1}^r q_k^{e_k}$  die *Primpotenzdarstellung* von  $n \in \mathbb{N}_2$ .

i) Mit  $f = e$  ergibt sich  $d(n) = \sum_{d|n} 1 = \prod_{k=1}^r \left( \sum_{j=0}^{e_k} 1 \right) = \prod_{k=1}^r (e_k + 1)$ , also (3.12).

ii) Durch  $f(d) = d^s$  für alle  $d \in \mathbb{N}_1$  und mit  $s \in \mathbb{N}_1$  wird (3.15) verallgemeinert:

$$\sigma_s(n) := \sum_{d|n} d^s = \prod_{k=1}^r \left( \sum_{j=0}^{e_k} q_k^{s \cdot j} \right) = \prod_{k=1}^r \frac{q_k^{s(e_k+1)} - 1}{q_k^s - 1}.$$

iii) Ist  $f_1$  multiplikativ und wird  $f(d) = \mu(d) f_1(d)$  gesetzt, so erhalten wir

$$F(n) = \sum_{d|n} \mu(d) f_1(d) = \prod_{k=1}^r (1 - f_1(q_k)) \text{ für jedes } n \in \mathbb{N}_2.$$

Hiervon sind uns zwei Spezialfälle schon bekannt:

a) Mit  $f_1 = e$  folgt  $o(n) := \sum_{d|n} \mu(d) = 0$  für alle  $n \in \mathbb{N}_2$ , sodass wir wegen  $o(1) = 1$  das Ergebnis des *Satzes über die Möbius-Summe* (Seite 65) gewinnen. Die multiplikative Funktion  $o : \mathbb{N}_1 \rightarrow \mathbb{N}$ ,  $n \mapsto \left[\frac{1}{n}\right]$  stellt bezüglich der Verknüpfung  $\star$  das “neutrale Element” dar.

b) Für  $f_1(d) = \frac{1}{d}$ ,  $d \in \mathbb{N}_1$ , ergibt sich

$$F(n) = \sum_{d|n} \frac{\mu(d)}{d} = \prod_{k=1}^r \left(1 - \frac{1}{q_k}\right) = \frac{\varphi(n)}{n} \text{ für alle } n \in \mathbb{N}_2,$$

was dem zweiten Teil des *Satzes über die Eulersche  $\varphi$ -Funktion* (Seite 98) entspricht.

iv) Im Falle  $f = \varphi$  erhalten wir ein Ergebnis, das GAUß in Artikel 39 von [9] mit einer anderen Methode zum ersten Mal bewiesen hat:

$$\sum_{d|n} \varphi(d) = \prod_{k=1}^r \left( \sum_{j=0}^{e_k} \varphi(q_k^j) \right) = \prod_{k=1}^r \left( 1 + \sum_{j=1}^{e_k} (q_k^j - q_k^{j-1}) \right) = \prod_{k=1}^r q_k^{e_k} = n.$$

Der Zusammenhang zwischen iii) b) und iv) wird durch den folgenden Satz verallgemeinert.

### Umkehrsatz von Möbius

Sind  $f$  und  $F$  zahlentheoretische Funktionen, so gilt  $F = f \star e$  genau dann, wenn  $f = F \star \mu$  erfüllt ist. Insbesondere stellt jede zahlentheoretische Funktion  $F$  die Summatorfunktion genau einer zahlentheoretischen Funktion  $f$  dar.

**Beweis** (direkt, zwei Teile, r1):

$$\text{i) } (F \star \mu)(n) = (\mu \star F)(n) = \sum_{d|n} \mu(d) F\left(\frac{n}{d}\right) = \sum_{d|n} \mu(d) \sum_{c|\frac{n}{d}} f(c) = \sum_{\substack{(c,d) \in \mathbb{N}_1^2 \\ (cd)|n}} \mu(d) f(c) =$$

$$\sum_{c|n} f(c) \sum_{d|\frac{n}{c}} \mu(d) = f(n) \text{ aufgrund des } \textit{Satzes über die Möbius-Summe} \text{ (Seite 65).}$$

$$\text{ii) } (f \star e)(n) = (e \star f)(n) = \sum_{d|n} f\left(\frac{n}{d}\right) = \sum_{d|n} \sum_{c|\frac{n}{d}} \mu\left(\frac{n}{cd}\right) F(c) = \sum_{\substack{(c,d) \in \mathbb{N}_1^2 \\ (cd)|n}} \mu\left(\frac{n}{cd}\right) F(c) =$$

$$\sum_{c|n} F(c) \sum_{d|\frac{n}{c}} \mu\left(\frac{n}{cd}\right) = \sum_{c|n} F(c) \sum_{d|\frac{n}{c}} \mu(d) = F(n). \quad \square$$

## 5.2 Darstellung als Summe von Quadraten

Für  $k \in \mathbb{N}_2$  sei  $\mathcal{Q}_k := \left\{ n \in \mathbb{N}_1 ; \text{Es gibt } (x_1, \dots, x_k) \in \mathbb{Z}^k \text{ mit } n = \sum_{i=1}^k x_i^2 \right\}$ .

Die drei Sätze dieses Abschnitts sind Beispiele für “kollektives Problemlösen”, weil der jeweilige Beweis erst einige Zeit nach der Formulierung des Satzes von einem anderen Mathematiker gefunden wurde. Den folgenden Satz hat FERMAT verbreitet; einen vollständigen Beweis konnte aber erst EULER veröffentlichen.

### Zweiquadratesatz (EULER, 1749)

Es gilt  $\mathcal{Q}_2 = \{n \in \mathbb{N}_1 ; 2 \mid \nu_p(n) \text{ für alle } p \in \mathbb{P} \text{ mit } p \equiv 3 \pmod{4}\}$ .

**Beweis** (fünf Teile: i), ii) direkt, iii) indirekt, iv) vollständige Induktion, v) indirekt, h1):

i) Die für alle  $x_1, x_2, y_1, y_2 \in \mathbb{Z}$  gültige **Identität**

$$(x_1^2 + x_2^2)(y_1^2 + y_2^2) = (x_1 y_1 + x_2 y_2)^2 + (x_1 y_2 - x_2 y_1)^2,$$

die schon DIOPHANT bekannt war, erlaubt es uns, den allgemeinen Fall auf die Darstellbarkeit von Primzahlen  $p$  mit  $p = 2$  oder  $p \equiv 1 \pmod{4}$  zurückzuführen. Nach dem Ausmultiplizieren der Klammern stehen auf beiden Seiten der Gleichung dieselben Quadratprodukte, während sich die beiden gemischten Glieder der rechten Seite wegheben.

ii) In einem **vorbereitenden Schritt** zeigen wir, dass es zu jedem  $p \in \mathbb{P}$  mit  $p \equiv 1 \pmod{4}$  ein  $\mu \in \mathcal{I}_{p-1}$  und ein  $x \in \mathbb{Z}$  gibt, sodass  $\mu p = x^2 + 1^2$  gilt. Der zweite Teil des *Wilsonschen Fakultätensatzes* (Seite 102) lässt sich im Falle  $p \equiv 1 \pmod{4}$  in der Form  $p \mid \left( \left( \left( \frac{p-1}{2} \right)! \right)^2 + 1^2 \right)$  schreiben. Ist  $x$  der absolut kleinste Rest von  $\left( \frac{p-1}{2} \right)! \pmod{p}$ , so gilt  $p \mid (x^2 + 1^2)$  und  $|x| < \frac{p}{2}$ . Damit gibt es ein  $\mu \in \mathbb{N}_1$  mit  $x^2 + 1^2 = \mu p$  und  $\mu p < \left( \frac{p}{2} \right)^2 + 1 < p^2$ , woraus  $\mu < p$  folgt.

Wegen  $2 = 1^2 + 1^2$  liegt für  $p = 2$  schon eine Darstellung mit  $\mu = 1$  vor.

iii) Für **Primzahlen**  $p$  mit  $p \equiv 1 \pmod{4}$  sei  $\mathcal{V}_p := \{ \mu \in \mathbb{N}_1 ; \text{Es gibt } x_1, x_2 \in \mathbb{N} \text{ mit } \mu p = x_1^2 + x_2^2 \}$ . Wir setzen  $m = m(p) := \min \mathcal{V}_p$  und zeigen, dass die Annahme  $m > 1$  zu einem Widerspruch führt. Damit wenden wir eine Variante

der *Methode des unendlichen Abstiegs* von FERMAT an, mit der hier bewiesen würde, dass zu jedem  $\mu \in \mathcal{V}_p$  mit  $\mu > 1$  ein  $\mu' \in \mathcal{V}_p$  mit  $\mu' < \mu$  existiert.

Es sei also  $m > 1$ . Wegen der Minimalität von  $m$  folgt aus  $\mu < p$  auch  $m < p$ . Sind  $x_1, x_2$  ganze Zahlen mit  $mp = x_1^2 + x_2^2$ , so gilt  $m \nmid x_1$  oder  $m \nmid x_2$ , denn andernfalls wäre  $m^2 \mid (x_1^2 + x_2^2)$ , also  $m \mid p$  im Widerspruch zu  $1 < m < p$  und  $p \in \mathbb{P}$ . Wählen wir  $y_i$  für  $i \in \mathcal{I}_2$  als absolut kleinsten Rest von  $x_i$  modulo  $m$ , so erhalten wir einerseits  $y_1^2 + y_2^2 > 0$ , und andererseits folgt aus  $-\frac{m}{2} < y_i \leq \frac{m}{2}$ , dass  $y_1^2 + y_2^2 \leq 2\left(\frac{m}{2}\right)^2 = \frac{1}{2}m^2 < m^2$  gilt, was wir in

$$(5.1) \quad 0 < y_1^2 + y_2^2 < m^2$$

zusammenfassen. Wegen  $y_1^2 + y_2^2 \equiv x_1^2 + x_2^2 \equiv 0 \pmod{m}$  ist  $n := \frac{1}{m}(y_1^2 + y_2^2)$  eine ganze Zahl, und (5.1) ergibt  $0 < n < m$ .

Mit Hilfe der Identität aus i) folgt nun

$$\begin{aligned} m^2 np &= (x_1^2 + x_2^2)(y_1^2 + y_2^2) = s_1^2 + s_2^2 \text{ mit} \\ s_1 &:= x_1 y_1 + x_2 y_2 \equiv x_1^2 + x_2^2 \equiv 0 \pmod{m} \text{ und} \\ s_2 &:= x_1 y_2 - x_2 y_1 \equiv x_1 x_2 - x_2 x_1 \equiv 0 \pmod{m}. \end{aligned}$$

Division durch  $m^2$  liefert

$$np = \left(\frac{s_1}{m}\right)^2 + \left(\frac{s_2}{m}\right)^2 \text{ mit } 0 < n < m \text{ und } \frac{s_i}{m} \in \mathbb{Z} \text{ für } i \in \mathcal{I}_2.$$

Damit erhalten wir einen Widerspruch zur Minimalität von  $m$ . Also muss  $m = 1$  gelten.

**iv)** Für den **Darstellungsnachweis** seien  $\mathcal{H}_0 := \{n \in \mathbb{N}_1; \nu_p(n) = 0 \text{ für alle } p \in \mathbb{P} \text{ mit } p \equiv 3 \pmod{4}\}$  und  $\mathcal{H} := \{n \in \mathbb{N}_1; 2 \mid \nu_p(n) \text{ für alle } p \in \mathbb{P} \text{ mit } p \equiv 3 \pmod{4}\}$ . Wir zeigen zunächst mit vollständiger Induktion, dass  $\mathcal{H}_0 \subset \mathcal{Q}_2$  gilt. Anschließend ergibt sich durch einfache Erweiterung, dass auch  $\mathcal{H} \setminus \mathcal{H}_0$  in  $\mathcal{Q}_2$  liegt. Wegen  $1 = 1^2 + 0^2$  ist  $0 \in \mathcal{M} := \{k \in \mathbb{N}; \text{Für jedes } n \in \mathcal{H}_0 \text{ mit } \Omega(n) = k \text{ gibt es } x_1, x_2 \in \mathbb{Z} \text{ mit } n = x_1^2 + x_2^2\}$ . Ist  $k \in \mathcal{M}$ , so folgt mit i) und ii), dass auch  $k+1$  zu  $\mathcal{M}$  gehört. Aufgrund des *Induktionssatzes* (Seite 12) ist also  $\mathcal{M} = \mathbb{N}$  und damit  $\mathcal{H}_0 \subset \mathcal{Q}_2$ .

Ist  $n \in \mathcal{H} \setminus \mathcal{H}_0$ , so werde  $n_0 := \max \{d \in \mathcal{H}_0; d \mid n\}$  gesetzt. Wegen  $2 \mid \nu_p(n)$  für alle Primteiler  $p$  von  $n$  mit  $p \equiv 3 \pmod{4}$  gibt es ein  $f \in \mathbb{N}_2$ , so dass  $\frac{n}{n_0} = f^2$  gilt. Aus  $n_0 = x_1^2 + x_2^2$  folgt dann  $n = f^2 n_0 = (fx_1)^2 + (fx_2)^2$ . Also ist auch  $n \in \mathcal{Q}_2$ , und zusammengenommen gilt  $\mathcal{H} \subset \mathcal{Q}_2$ .

v) Nun ist noch die **Komplementäraussage** zu beweisen, dass  $n \notin \mathcal{Q}_2$  für alle  $n \in \mathbb{N}_1 \setminus \mathcal{H}$  gilt. Zu jedem solchen  $n$  existiert definitionsgemäß ein  $p \in \mathbb{P}$  mit  $p \equiv 3 \pmod{4}$  und  $2 \nmid \nu_p(n)$ . Wir nehmen an, es gäbe  $x_1, x_2 \in \mathbb{Z}$  mit  $n = x_1^2 + x_2^2$ . Wird  $d := \text{ggT}(x_1, x_2)$ ,  $y_1 := \frac{x_1}{d}$  und  $y_2 := \frac{x_2}{d}$  gesetzt, so gilt  $\text{ggT}(y_1, y_2) = 1$  und  $n = d^2(y_1^2 + y_2^2)$ . Mit  $n_1 := \frac{n}{d^2} = y_1^2 + y_2^2$  folgt  $\nu_p(n_1) = \nu_p(n) - 2\nu_p(d) > 0$ , weil  $\nu_p(n)$  ungerade ist. Also gilt  $p \mid n_1$ . Wegen  $\text{ggT}(y_1, y_2) = 1$  gibt es aufgrund des *Satzes über die lineare Kongruenz* (Seite 91) ein  $u \in \mathbb{Z}$  mit  $y_2 \equiv u y_1 \pmod{p}$ . Einsetzen ergibt  $0 \equiv n_1 \equiv y_1^2(1 + u^2) \pmod{p}$ . Wegen  $p \mid (y_1^2 + y_2^2)$  und  $\text{ggT}(y_1, y_2) = 1$  kann  $p$  nicht Teiler von  $y_1^2$  sein. Also folgt mit Hilfe des *Produktteilersatzes* (Seite 23), dass  $u^2 \equiv -1 \pmod{p}$  gilt. Damit wäre  $\left(\frac{-1}{p}\right) = 1$  für  $p \equiv 3 \pmod{4}$  - im Widerspruch zum *Ersten Ergänzungssatz* (Seite 117). Zusammenfassend erhalten wir schließlich  $\mathcal{Q}_2 = \mathcal{H}$ .  $\square$

Wir behandeln nun zuerst den Fall  $k = 4$ , weil einerseits die Beweisstruktur des zugehörigen Satzes weitgehend mit der des *Zweiquadratesatzes* übereinstimmt und weil andererseits die Beweismethode, die wir für  $\mathcal{Q}_3$  skizzieren werden, zu dem nächsten Abschnitt überleitet.

Die Aussage des folgenden *Vierquadratesatzes* wird DIOPHANT zugeschrieben. FERMAT, DESCARTES, EULER und andere haben vergeblich versucht, den Satz zu beweisen, bevor dieses LAGRANGE gelang. Der hier wiedergegebene Beweis stammt aber von EULER, von dem LAGRANGE ausdrücklich schreibt, dass er ihm wesentliche Ideen aus einer früheren Arbeit verdankt.

### Vierquadratesatz (LAGRANGE, 1772)

Es gilt  $\mathcal{Q}_4 = \mathbb{N}_1$ .

**Beweis** (vier Teile: i), ii) direkt, iii) indirekt, iv) vollständige Induktion, h1):

i) Die folgende **Eulersche Identität** ermöglicht die Anwendung der *Zurückführungsstrategie*:

Für alle  $x_1, x_2, x_3, x_4, y_1, y_2, y_3, y_4 \in \mathbb{Z}$  gilt  $\left(\sum_{i=1}^4 x_i^2\right) \left(\sum_{i=1}^4 y_i^2\right) = \sum_{i=1}^4 s_i^2$  mit  $s_1 := \sum_{i=1}^4 x_i y_i$  und  $s_j := x_1 y_j - x_j y_1 + x_k y_l - x_l y_k$  für  $(j, k, l) \in \{(2, 3, 4), (3, 4, 2)\}$ ,

$(4, 2, 3)$ } (“zyklische Vertauschung”). Durch einfaches Ausmultiplizieren oder mit Hilfe eines CAS erhält man auf beiden Seiten  $x_1^2 y_1^2 + x_1^2 y_2^2 + x_1^2 y_3^2 + x_1^2 y_4^2 + x_2^2 y_1^2 + x_2^2 y_2^2 + x_2^2 y_3^2 + x_2^2 y_4^2 + x_3^2 y_1^2 + x_3^2 y_2^2 + x_3^2 y_3^2 + x_3^2 y_4^2 + x_4^2 y_1^2 + x_4^2 y_2^2 + x_4^2 y_3^2 + x_4^2 y_4^2$ . Damit kann der Beweis des Satzes auf den Nachweis der Darstellbarkeit von Primzahlen zurückgeführt werden.

ii) Als **Vorstufe** wird gezeigt, dass es zu jedem  $p \in \mathbb{P}_3$  ein  $\mu \in \mathcal{I}_{p-1}$  und  $(x_1, \dots, x_4) \in \mathbb{N}^4$  gibt, sodass  $\mu p = \sum_{i=1}^4 x_i^2$  gilt. Aufgrund des *Satzes über die Anzahl quadratischer Reste* (Seite 108) bestehen die Mengen  $\left\{x^2; x = 0, \dots, \frac{p-1}{2}\right\}$  und  $\left\{-1 - y^2; y = 0, \dots, \frac{p-1}{2}\right\}$  aus jeweils  $\frac{p+1}{2}$  modulo  $p$  inkongruenten Elementen. Das sind zusammen  $p + 1$  Zahlen, während modulo  $p$  nur höchstens  $p$  Werte inkongruent sein können. Also folgt mit Hilfe des *Schubfachsatzes* (Seite 85), dass es  $x, y \in \mathbb{N}$  mit  $x < \frac{p}{2}$ ,  $y < \frac{p}{2}$  und  $x^2 \equiv -1 - y^2 \pmod{p}$  gibt. Damit existiert ein  $\mu \in \mathbb{N}_1$  mit  $x^2 + y^2 + 1^2 + 0^2 = \mu p$  und  $\mu p < \frac{p^2}{4} + \frac{p^2}{4} + 1 = \frac{p^2}{2} + 1 < p^2$ , sodass außerdem  $\mu < p$  gilt.

Für  $p = 2$  ist  $2 = 1^2 + 1^2 + 0^2 + 0^2$  eine geeignete Summe mit  $\mu = 1$ .

iii) Im Falle **ungerader Primzahlen**  $p$  setzen wir  $m = m(p) := \min \left\{ \mu \in \mathbb{N}_1; \mu p = \sum_{i=1}^4 x_i^2 \text{ ist lösbar} \right\}$ . Im Folgenden sei  $m p = x_1^2 + x_2^2 + x_3^2 + x_4^2$ . Ist  $m = 1$ , so liegt eine gewünschte Darstellung vor. Für gerade  $m$  und für ungerade  $m \in \mathbb{N}_3$  leiten wir jeweils einen Widerspruch her.

**1. Fall:** Wir nehmen an, dass  $m$  **gerade** ist. Dann gilt  $0 \equiv m p \equiv x_1^2 + \dots + x_4^2 \pmod{2}$ . Um zu erreichen, dass  $x_1 + x_2$  und  $x_3 + x_4$  beide gerade sind, werden die  $x_i$  umgeordnet, falls jeweils genau ein Element aus  $\{x_1, x_2\}$  und aus  $\{x_3, x_4\}$  ungerade ist. Für alle anderen Viertupel sind  $x_1 + x_2$  und  $x_3 + x_4$  schon gerade. Dann besitzt  $\frac{m}{2} p$  die ganzzahlige Quadratsummendarstellung

$$\frac{m}{2} p = \left(\frac{x_1+x_2}{2}\right)^2 + \left(\frac{x_1-x_2}{2}\right)^2 + \left(\frac{x_3+x_4}{2}\right)^2 + \left(\frac{x_3-x_4}{2}\right)^2$$

- im Widerspruch zur Minimalität von  $m$ .

**2. Fall:** Unter der Annahme, dass  $m$  **ungerade** und  $m \geq 3$  ist, sei  $y_i$  für jedes  $i \in \mathcal{I}_4$  der absolut kleinste Rest von  $x_i$  modulo  $m$ , d. h. es sei

$$(5.2) \quad x_i \equiv y_i \pmod{m} \text{ und } |y_i| < \frac{m}{2}.$$

Daraus folgt  $0 \equiv mp \equiv \sum_{i=1}^4 x_i^2 \equiv \sum_{i=1}^4 y_i^2 \pmod{m}$ . Also gibt es ein  $n \in \mathbb{N}$ , sodass  $\sum_{i=1}^4 y_i^2 = mn$  ist. Es kann nicht  $n = 0$  sein, weil sonst  $y_i = 0$ , also  $m \mid x_i$  für  $i = 1, \dots, 4$  wäre. Wegen  $m^2 \mid x_i^2$  würde dann  $m^2 \mid mp$ , also  $m \mid p$  folgen - im Widerspruch dazu, dass  $p \in \mathbb{P}$  und  $1 < m < p$  gilt.

Außerdem ergibt  $mn = \sum_{i=1}^4 y_i^2 < 4 \frac{m^2}{4} = m^2$ , dass  $n < m$  ist. Aus  $mp = \sum_{i=1}^4 x_i^2$  und  $mn = \sum_{i=1}^4 y_i^2$  folgt nach i)  $m^2 np = \sum_{i=1}^4 s_i^2$ . Hier gilt  $m \mid s_i$  für  $i = 1, \dots, 4$ , weil wegen (5.2)  $s_1 \equiv \sum_{i=1}^4 x_i^2 \equiv 0 \pmod{m}$  und  $x_k y_l - x_l y_k \equiv x_k x_l - x_l x_k \equiv 0 \pmod{m}$  gilt. Schließlich folgt  $np = \sum_{i=1}^4 \left(\frac{s_i}{m}\right)^2$  mit  $\frac{s_i}{m} \in \mathbb{Z}$  - im Widerspruch zur Minimalität von  $m$ .

iv) Der Satz wird nun durch vollständige Induktion mit  $\mathcal{M} := \left\{ k \in \mathbb{N}; \text{Für jedes } n \in \mathbb{N}_1 \text{ mit } \Omega(n) = k \text{ gibt es } x_1, \dots, x_4 \in \mathbb{Z} \text{ mit } n = \sum_{i=1}^4 x_i^2 \right\}$  bewiesen. Wegen  $1 = 1^2 + 0^2 + 0^2 + 0^2$  ist  $0 \in \mathcal{M}$ . Aus  $k \in \mathcal{M}$  folgt mit i) und iii), dass auch  $k + 1$  zu  $\mathcal{M}$  gehört. Der *Induktionssatz* (Seite 12) ergibt damit, dass  $\mathcal{M} = \mathbb{N}$ , also  $\mathcal{Q}_4 = \mathbb{N}_1$  gilt.  $\square$

Für die Darstellbarkeit von natürlichen Zahlen  $n$  als Summe von drei Quadraten lieferte DESCARTES 1638 einen Beweis der 1636 von FERMAT formulierten notwendigen Bedingung  $n \neq 4^a(8b + 7)$  für alle  $a, b \in \mathbb{N}$ . EULER bemühte sich zwischen 1730 und 1780 um den Nachweis, dass diese Bedingung auch hinreichend ist. Den ersten Beweis erbrachte LEGENDRE 1798 in einem Lehrbuch über Zahlentheorie. Er verwendete dabei spezielle Sätze über "reziproke quadratische Teiler" von  $t^2 + cu^2$ . Völlig anders ist die von GAUß entwickelte Beweismethode, die drei Jahre später in [9] erschien. Die von ihm nur zum Teil für diesen Zweck eingeführte Äquivalenztheorie von "quadratischen Formen" wurde später einer der Ausgangspunkte für das große Gebiet der algebraischen Zahlentheorie. Mit Hilfe von "binären" und "ternären" quadratischen Formen bestimmte GAUß sogar für jede natürliche Zahl die Anzahl der Darstellungen als Summe von drei Quadraten.

Die von GAUß sehr breit entwickelte Theorie der quadratischen Formen kann in diesem Buch nur andeutungsweise in zwei Teilen wiedergegeben werden. Für

den *Dreiquadratesatz* skizzieren wir eine Beweisidee von DIRICHLET, der ternäre quadratische Formen und die von ihm stammende Aussage des *Theorems über Primzahlen in arithmetischen Folgen* (Seite 71) verwendet. Die hier zugrunde gelegte vereinfachte Version wurde 1909 von E. LANDAU<sup>3</sup> in dem Lehrbuch [12] veröffentlicht. Die Ergebnisse von GAUß über binäre quadratische Formen behandeln wir dann im nächsten Abschnitt.

**Dreiquadratesatz** (LEGENDRE, 1798)

$$\mathcal{Q}_3 = \{n \in \mathbb{N}_1; \text{Es gibt kein Paar } (a, b) \in \mathbb{N}^2 \text{ mit } n = 4^a(8b + 7)\}.$$

*Beweisskizze* (7 Schritte):

### i) Bezeichnung der ternären quadratischen Formen und ihrer Determinanten

Sind  $a_{ik} \in \mathbb{Z}$  für  $i, k \in \mathcal{I}_3$  und ist  $a_{ik} = a_{ki}$  für  $1 \leq i < k \leq 3$ , so wird

$$F : \mathbb{Z}^3 \rightarrow \mathbb{Z}, (x_1, x_2, x_3) \mapsto \sum_{i=1}^3 \sum_{k=1}^3 a_{ik} x_i x_k$$

*ternäre quadratische Form* (im Folgenden kurz *Form*) genannt.

Mit  $\det(a_{ik}) := a_{11} a_{22} a_{33} + a_{12} a_{23} a_{31} + a_{13} a_{21} a_{32} - a_{11} a_{23} a_{32} - a_{12} a_{21} a_{33} - a_{13} a_{22} a_{31}$  werde die *Determinante der Form*  $F$  bezeichnet.

### ii) Definition der Äquivalenz von Formen und Feststellung einer Äquivalenzrelation

Sind  $F$  und  $G$  Formen, so heißt  $F$  zu  $G$  *äquivalent*, wenn es Zahlen  $c_{ik} \in \mathbb{Z}$ ,  $i, k \in \mathcal{I}_3$ , mit  $\det(c_{ik}) = 1$  gibt, sodass mit der Abbildung

$$\gamma : \mathbb{Z}^3 \rightarrow \mathbb{Z}^3, (y_1, y_2, y_3) \mapsto \left( \sum_{l=1}^3 c_{1l} y_l, \sum_{l=1}^3 c_{2l} y_l, \sum_{l=1}^3 c_{3l} y_l \right)$$

die Abbildungsgleichheit  $G = F \circ \gamma$  gilt, wobei  $\circ$  die Hintereinanderausführung von Abbildungen bezeichnet.

Die Äquivalenz von Formen stellt eine *Äquivalenzrelation* auf der Menge aller Formen dar, d. h. es gilt die *Reflexivität* (Jede Form  $F$  ist zu sich selbst äquivalent),

<sup>3</sup> EDMUND LANDAU (1877-1938) wirkte in Göttingen.

die *Symmetrie* (Ist  $F$  zu  $G$  äquivalent, so auch  $G$  zu  $F$ ) und die *Transitivität* (Stellt  $H$  eine Form dar und ist  $F$  zu  $G$  und  $G$  zu  $H$  äquivalent, so folgt die Äquivalenz von  $F$  zu  $H$ ).

Die Reflexivität ergibt sich aus  $F = F \circ \varepsilon$  mit  $\varepsilon : \mathbb{Z}^3 \rightarrow \mathbb{Z}^3$ ,  $(y_1, y_2, y_3) \mapsto (y_1, y_2, y_3)$ .

Ist  $G = F \circ \gamma$ , so zeigt man für den Nachweis der Symmetrie durch Auflösen des entsprechenden linearen Gleichungssystems, dass  $\gamma$  wegen  $\det(c_{ik}) = 1$  eine Umkehrabbildung  $\gamma^{-1}$  mit ganzen Koeffizienten, die die Symmetriebedingung erfüllen, und mit der Determinante 1 besitzt. Damit und wegen  $F = G \circ \gamma^{-1}$  ist  $G$  zu  $F$  äquivalent.

Aus  $G = F \circ \gamma$  und  $H = G \circ \beta$  mit einer geeigneten Abbildung  $\beta$  folgt  $H = F \circ (\gamma \circ \beta)$ , wobei die Koeffizienten von  $\gamma \circ \beta$  ganz sind und die Determinante aufgrund des *Determinantenproduktsatzes* der linearen Algebra den Wert 1 hat. Damit ist auch  $H$  zu  $F$  äquivalent.

Die durch die Äquivalenzrelation bestimmten Äquivalenzklassen von ternären quadratischen Formen heißen *Formenklassen*.

### iii) Invarianz der Determinanten und der Mengen aller darstellbaren Zahlen

Ist  $G = F \circ \gamma$  und haben  $F, G$  bzw.  $\gamma$  die Koeffizienten  $a_{ik}, b_{ik}, c_{ik}$ , so gilt

$$\begin{aligned} & \sum_{k=1}^3 \sum_{l=1}^3 a_{kl} \left( \sum_{m=1}^3 c_{km} y_m \right) \left( \sum_{n=1}^3 c_{ln} y_n \right) \\ &= \sum_{m=1}^3 \sum_{n=1}^3 \left( \sum_{k=1}^3 \sum_{l=1}^3 c_{km} a_{kl} c_{ln} \right) y_m y_n \\ &= \sum_{m=1}^3 \sum_{n=1}^3 b_{mn} y_m y_n. \end{aligned}$$

Durch Koeffizientenvergleich erhält man

$$b_{mn} = \sum_{k=1}^3 \sum_{l=1}^3 c_{km} a_{kl} c_{ln} \text{ für } m, n \in \mathcal{I}_3.$$

Der *Determinantenproduktsatz* der linearen Algebra ergibt damit

$$\det(b_{ik}) = \det(c_{ik}) \det(a_{ik}) \det(c_{ik}) = \det(a_{ik}).$$

Also haben alle Formen einer Formenklasse dieselbe Determinante, und umgekehrt lässt sich die Menge aller Formen mit einer festen Determinante als Vereinigung von disjunkten Formenklassen darstellen.

Bezeichnet  $\mathcal{W}_F := \{n \in \mathbb{Z}; \text{Es gibt } (x_1, x_2, x_3) \in \mathbb{Z}^3 \text{ mit } n = F(x_1, x_2, x_3)\}$  die Wertemenge der Form  $F$ , so ist es für den Beweis des *Dreiquadratesatzes* entscheidend, dass alle Formen einer Formenklasse dieselbe Wertemenge haben. Sind  $F$  und  $G$  zueinander äquivalent, so folgt nämlich  $\mathcal{W}_G \subseteq \mathcal{W}_F$  aus  $G = F \circ \gamma$ , und die mit der Symmetrieeigenschaft der Äquivalenzrelation gewonnene Beziehung  $F = G \circ \gamma^{-1}$  ergibt  $\mathcal{W}_F \subseteq \mathcal{W}_G$ . Also ist  $\mathcal{W}_G = \mathcal{W}_F$ .

#### iv) Definition der Positiv-Definitheit und ein Definitheitskriterium

Für die “Reduktion” im nächsten Schritt ist es sinnvoll, nur Formen  $F$  mit  $F(x_1, x_2, x_3) > 0$  für alle  $(x_1, x_2, x_3) \in \mathbb{Z}^3 \setminus \{(0, 0, 0)\}$  zu betrachten. Diese und nur diese Formen heißen *positiv-definit*. Wir zeigen, dass eine Form  $F$  mit den Koeffizienten  $a_{ik}$  genau dann positiv-definit ist, wenn die drei Bedingungen

$$(5.3) \quad a_{11} > 0, \quad b := a_{11}a_{22} - a_{12}^2 > 0 \quad \text{und} \quad \Delta := \det(a_{ik}) > 0$$

erfüllt sind. Durch einfache Rechnungen erhalten wir

$$(5.4) \quad a_{11}F(x_1, x_2, x_3) = (a_{11}x_1 + a_{12}x_2 + a_{13}x_3)^2 + bx_2^2 + 2cx_2x_3 + dx_3^2$$

mit  $c := a_{11}a_{23} - a_{12}a_{13}$  und  $d := a_{11}a_{33} - a_{13}^2$  sowie

$$(5.5) \quad b(bx_2^2 + 2cx_2x_3 + dx_3^2) = (bx_2 + cx_3)^2 + a_{11}\Delta x_3^2.$$

Es sei zunächst  $F$  als positiv-definit vorausgesetzt. Wegen  $F(1, 0, 0) = a_{11}$  ist dann notwendig  $a_{11} > 0$ . Aus (5.4) folgt  $F(-a_{11}a_{12}, a_{11}^2, 0) = a_{11}b$ , sodass  $b > 0$  gelten muss, weil  $a_{11} > 0$  und  $x_2 = a_{11}^2 \neq 0$  ist. Mit (5.4) und (5.5) erhalten wir  $F(a_{11}a_{12}c - a_{11}a_{13}b, -a_{11}c, a_{11}b) = a_{11}^2b\Delta$ . Wegen  $a_{11}^2b > 0$  und  $x_3 = a_{11}b \neq 0$  ergibt sich daraus  $\Delta > 0$ .

Ist (5.3) erfüllt, so können wir (5.4) und (5.5) zu

$$F(x_1, x_2, x_3) = \frac{1}{a_{11}}(a_{11}x_1 + a_{12}x_2 + a_{13}x_3)^2 + \frac{1}{a_{11}b}(bx_2 + cx_3)^2 + \frac{\Delta}{b}x_3^2$$

zusammenfassen. Damit folgt  $\mathcal{W}_F \subseteq \mathbb{N}$ , und es kann nur dann  $F(x_1, x_2, x_3) = 0$  sein, wenn  $x_3 = 0$ ,  $bx_2 + cx_3 = 0$  und  $a_{11}x_1 + a_{12}x_2 + a_{13}x_3 = 0$  gilt, d. h. wenn  $x_3 = x_2 = x_1 = 0$  ist.

Die Positiv-Definitheit gehört zu den invarianten Eigenschaften der Formenklassen; denn sind  $F$  und  $G$  zueinander äquivalente Formen und ist  $F$  positiv-definit, so folgt wegen iii) zunächst  $\mathcal{W}_G = \mathcal{W}_F \subseteq \mathbb{N}$ . Mit  $G = F \circ \gamma$  gilt  $0 = G(x_1, x_2, x_3) = F(\gamma(x_1, x_2, x_3))$  genau dann, wenn  $x_1 = x_2 = x_3 = 0$  ist, weil das durch  $\gamma(x_1, x_2, x_3) = (0, 0, 0)$  gegebene lineare Gleichungssystem wegen  $\det(c_{ik}) = 1$  nur diese eine Lösung besitzt.

### v) Äquivalenz zur Einheitsform $E$ mit $E(x_1, x_2, x_3) := x_1^2 + x_2^2 + x_3^2$

Die Einheitsform  $E$  ist offensichtlich positiv-definit, sie hat die Determinante 1 und definitionsgemäß gilt  $\mathcal{W}_E = \mathcal{Q}_3$ . Als Anwendung der *Invarianzstrategie* wird gezeigt, dass alle positiv-definiten Formen, deren Determinante 1 ist, zu der Einheitsform äquivalent sind. Dann genügt es nämlich, zu den im *Dreiquadratesatz* genannten Zahlen  $n$  irgendeine positiv-definite Form  $G$  mit der Determinante 1 und mit  $n \in \mathcal{W}_G$  anzugeben, weil  $\mathcal{W}_G = \mathcal{W}_E$  ist.

Im umfangreichsten Teil der Beweisversion von LANDAU wird nachgewiesen, dass jede Klasse positiv-definiten Formen mit der Determinante  $\Delta$  mindestens eine Form mit

$$(5.6) \quad 2 \max\{|a_{12}|, |a_{13}|\} \leq a_{11} \leq \frac{4}{3} \sqrt[3]{\Delta}$$

enthält, wobei  $a_{11} = \min(\mathcal{W}_F \setminus \{0\})$  für irgendeine und damit nach iii) für jede Form  $F$  aus der Klasse gilt. Durch Darstellung von  $a_{11}$ ,  $a_{12}$ ,  $a_{13}$  und  $a_{22}$  mit Hilfe geeigneter Formen ergibt sich zuerst die linke und dann die rechte Ungleichung von (5.6).

Für  $\Delta = 1$  liefert (5.6) die Werte  $a_{11} = 1$  und  $a_{12} = a_{13} = 0$ , sodass jede positiv-definite Form mit der Determinante 1 zu der Form  $G$  mit  $G(x_1, x_2, x_3) = x_1^2 + a_{22}x_2^2 + 2a_{23}x_2x_3 + a_{33}x_3^2$  äquivalent ist. Hier hat der erste Summand schon die gewünschte Gestalt, während der Rest eine quadratische Form mit zwei Variablen darstellt. Mit gering geänderter Bezeichnungsweise werden im nächsten Abschnitt für solche “binären” quadratischen Formen die “Diskriminante” (anstelle der Determinante) und die Positiv-Definitheit definiert. Eine ähnliche Existenzaussage wie in (5.6) (*Satz über die Klassenanzahl*, Seite 155) ergibt dann, dass  $G$  zu  $E$  äquivalent ist, womit auch  $F$  und  $E$  in derselben Formenklasse liegen.

### vi) Bestimmung geeigneter Koeffizienten

Um die Darstellbarkeit für alle  $n \in \mathbb{N}_1$  mit  $\text{mod}(n, 8) \in \{1, 2, 3, 5, 6\}$  zu zeigen,

wird nun mit Fallunterscheidung jeweils eine positiv-definite Form  $F$ , deren Determinante den Wert 1 hat, angegeben. Die übrigen Fälle des Satzes können hierauf zurückgeführt werden; denn wenn  $n$  die Form  $4^k m$  mit  $\text{mod}(m, 8) \in \{1, 2, 3, 5, 6\}$  hat und  $m$  die Darstellung  $m = F(x_1, x_2, x_3)$  besitzt, so lässt sich  $n$  als  $n = F(2^k x_1, 2^k x_2, 2^k x_3)$  schreiben.

Die zu erfüllenden Bedingungen lauten

$$n = F(x_1, x_2, x_3), \quad a_{11} > 0, \quad a_{11} a_{22} - a_{12}^2 > 0 \quad \text{und} \quad \det(a_{ik}) = 1.$$

Von den 9 Unbekannten können 6 vorweg festgelegt werden:

$$a_{13} = 1, \quad a_{23} = 0, \quad a_{33} = n, \quad x_1 = 0, \quad x_2 = 0, \quad x_3 = 1.$$

Die  $n$ -Darstellung folgt dann durch  $n = a_{33} = F(0, 0, 1)$ . Mit  $b := a_{11} a_{22} - a_{12}^2$  ergibt die vierte Bedingung  $1 = \det(a_{ik}) = (a_{11} a_{22} - a_{12}^2) n - a_{22} = b n - a_{22}$  und damit  $a_{22} = b n - 1$ . Setzen wir wegen  $1 = 1^2 + 0^2 + 0^2$  im Folgenden  $n \in \mathbb{N}_2$  voraus, so ergibt  $a_{22} > b - 1 \geq 0$  und  $a_{11} a_{22} = a_{12}^2 + b > 0$ , dass schon  $a_{11} > 0$  gilt. Es bleiben also nur noch die Bedingungen

$$(5.7) \quad b = a_{11} a_{22} - a_{12}^2 > 0 \quad \text{und} \quad a_{22} = b n - 1.$$

Die Suche nach geeigneten Koeffizienten lässt sich weiter dadurch vereinfachen, dass (5.7) als quadratische Kongruenz

$$(5.8) \quad x^2 \equiv -b \pmod{b n - 1} \quad \text{mit} \quad b \in \mathbb{N}_1 \quad \text{und} \quad x = a_{12}$$

angesehen wird. Durch Unterscheidung von zwei Fällen ergibt sich nun jeweils die Existenz einer nur von  $n$  abhängigen Primzahl  $p$ , so dass (5.8) mit  $b n - 1 = p \text{ ggT}(n + 1, 2)$  lösbar ist.

*1. Fall:* Für  $n \equiv 2 \pmod{4}$  ist  $\text{ggT}(n - 1, 4n) = 1$ . Deshalb gibt es für jedes dieser  $n$  aufgrund des *Theorems über Primzahlen in arithmetischen Folgen* (Seite 71) unendlich viele  $p \in \mathbb{P}$  mit  $p \equiv n - 1 \pmod{4n}$ . Es folgt  $p \equiv 1 \pmod{4}$ , und für  $b := \frac{p+1}{n}$  gilt wegen  $b = 4 \frac{p-n+1}{4n} + 1$  auch  $b \equiv 1 \pmod{4}$ . Mit Hilfe der zugehörigen Sätze über das Jacobi-Symbol (Seite 112 bis 117) ergibt sich

$$\left(\frac{-b}{p}\right) = \left(\frac{-1}{p}\right) \left(\frac{b}{p}\right) = (-1)^{p-1} \left(\frac{p}{b}\right) (-1)^{p-b} = \left(\frac{p}{b}\right) = \left(\frac{b n - 1}{b}\right) = \left(\frac{-1}{b}\right) = 1,$$

d. h. die Kongruenz (5.8) ist lösbar und liefert die gesuchten Koeffizienten.

*2. Fall:* Für die übrigen  $n$  mit  $\text{mod}(n, 8) \in \{1, 3, 5\}$  wird  $c := \text{mod}(n + 2, 4)$  gesetzt. Dann ist  $\text{ggT}\left(\frac{c n - 1}{2}, 4n\right) = 1$ , und wegen des *Theorems über Primzahlen*

in arithmetischen Folgen gibt es unendlich viele  $p \in \mathbb{P}$  mit  $p \equiv \frac{cn-1}{2} \pmod{4n}$ . Für  $b := \frac{2p+1}{n}$  ist  $b \in \mathbb{N}_1$  und  $b = 8 \frac{2p-cn+1}{8n} + c \equiv c \pmod{8}$ . Damit erhalten wir  $\left[\frac{b+1}{4}\right] \equiv \left[\frac{c+1}{4}\right] \equiv c_- \equiv b_- \pmod{2}$ , und es folgt

$$(5.9) \quad \left(\frac{-2}{b}\right) = \left(\frac{-1}{b}\right) \left(\frac{2}{b}\right) = (-1)^{b_-} (-1)^{\left[\frac{b+1}{4}\right]} = 1.$$

Außerdem gilt  $2 \mid (b_- + 1)$  für  $c = 3$ , und  $p \equiv \frac{cn-1}{2} \pmod{4}$  liefert  $2 \mid p_-$  für  $c = 1$ . Also ist  $(-1)^{p_- (b_- + 1)} = 1$ , und zusammen mit (5.9) ergeben die jeweiligen Sätze über das Jacobi-Symbol

$$\begin{aligned} \left(\frac{-b}{p}\right) &= \left(\frac{-1}{p}\right) \left(\frac{b}{p}\right) = (-1)^{p_-} \left(\frac{p}{b}\right) (-1)^{p_- b_-} = \left(\frac{p}{b}\right) \\ &= \left(\frac{-2}{b}\right) \left(\frac{p}{b}\right) = \left(\frac{-2p}{b}\right) = \left(\frac{1-bn}{b}\right) = \left(\frac{1}{b}\right) = 1. \end{aligned}$$

Damit ist  $-b$  quadratischer Rest modulo  $p$  und wegen  $1^2 \equiv -b \pmod{2}$  auch modulo  $2p$ . Wegen  $2p = bn - 1$  werden die gesuchten Koeffizienten wieder mit Hilfe der Kongruenz (5.8) gewonnen.

### vii) Nicht darstellbare Zahlen

Durch vollständige Induktion mit  $\mathcal{M} := \{m \in \mathbb{N}; 4^m(8b+7) \notin \mathcal{Q}_3 \text{ für jedes } b \in \mathbb{N}\}$  zeigen wir abschließend, dass die Zahlen  $4^a(8b+7)$  für alle  $a, b \in \mathbb{N}$  nicht in  $\mathcal{Q}_3$  liegen. Wegen  $\text{mod}(t^2, 8) \in \{0, 1, 4\}$  für jedes  $t \in \mathbb{Z}$  gehört kein  $n \in \mathbb{Z}$  mit  $n \equiv 7 \pmod{8}$  zu  $\mathcal{Q}_3$ , sodass  $0 \in \mathcal{M}$  gilt. Ist  $m \in \mathcal{M}$  und gäbe es ein  $b \in \mathbb{N}$  sowie  $x_1, x_2, x_3 \in \mathbb{Z}$  mit  $4^{m+1}(8b+7) = x_1^2 + x_2^2 + x_3^2$ , so würde wegen  $x_1^2 + x_2^2 + x_3^2 \equiv 0 \pmod{4}$  folgen, dass  $2 \mid x_i$  für jedes  $i \in \mathcal{T}_3$  sein müsste. Dann wäre aber  $4^m(8b+7) = \left(\frac{x_1}{2}\right)^2 + \left(\frac{x_2}{2}\right)^2 + \left(\frac{x_3}{2}\right)^2$  - im Widerspruch zu  $m \in \mathcal{M}$ . Also folgt  $m+1 \in \mathcal{M}$ , und der Induktionssatz ergibt  $\mathcal{M} = \mathbb{N}$ .  $\square$

## 5.3 Binäre quadratische Formen und die Klassengruppe

Anders als bei den "gemischten Gliedern" von quadratischen Formen mit drei beziehungsweise mit beliebig vielen Variablen wird bei der eigenständigen Untersuchung der "binären" quadratischen Formen der entsprechende Koeffizient ohne Symmetriebedingung (d. h. ohne einen Faktor 2) angesetzt.

### Bezeichnung der binären quadratischen Formen und ihrer Diskriminanten

Sind  $a, b, c \in \mathbb{Z}$ , so heißt

$$F : \mathbb{Z}^2 \rightarrow \mathbb{Z}, (x, y) \mapsto ax^2 + bxy + cy^2$$

*binäre quadratische Form* (im Folgenden kurz *Form*). Die Abkürzung  $(a, b, c)$  beschreibt die Abhängigkeit der Form  $F$  von den Koeffizienten.

Mit  $\text{dis}(a, b, c) := b^2 - 4ac$  wird die *Diskriminante der Form*  $F$  bezeichnet.

Ist  $D$  eine Diskriminante und setzt man  $\alpha := \text{mod}(D, 4)$ , so gilt  $\alpha \in \mathcal{A}_2$ , und für jedes  $D \in \mathbb{Z}$  mit  $\alpha \in \mathcal{A}_2$  stellt  $\left(1, \alpha, \frac{\alpha-D}{4}\right)$  eine Form mit der Diskriminante  $D$  dar, weil  $\text{dis}\left(1, \alpha, \frac{\alpha-D}{4}\right) = \alpha^2 - 4 \frac{\alpha-D}{4} = \alpha(\alpha - 1) + D = D$  gilt.

Da wir hier nur die wichtigsten Zusammenhänge wiedergeben wollen, nehmen wir mehrere Einschränkungen vor. So betrachten wir im Folgenden nur Formen, deren Diskriminante keine Quadratzahl ist, weil diese Formen eng mit den “quadratischen Ordnungen” zusammenhängen, die im nächsten Abschnitt eine wesentliche Rolle spielen. Bei den Herleitungen in diesem Abschnitt wird es sich außerdem als günstig erweisen, dass für die Formen  $(a, b, c)$  mit nichtquadratischer Diskriminante  $a \neq 0$  und  $c \neq 0$  gilt, weil andernfalls  $D = b^2$  wäre.

Im Übrigen gehören zu den quadratischen Diskriminanten genau diejenigen Formen  $(a, b, c)$ , die *zerlegbar* sind, d. h. für die es Zahlen  $r, s, t, u \in \mathbb{Z}$  gibt, so dass  $ax^2 + bxy + cy^2 = (rx + sy)(tx + uy)$  für alle  $x, y \in \mathbb{Z}$  gilt.

Bevor wir analog zum Vorgehen bei dem *Dreiquadratesatz* die Äquivalenz von Formen definieren, klären wir eine typische Eigenschaft der Wertemengen  $\mathcal{W}_F := \{n \in \mathbb{Z}; \text{Es gibt } (x, y) \in \mathbb{Z}^2 \text{ mit } n = F(x, y)\}$  in Abhängigkeit von  $\text{sign } D$ . Wie in (5.4) mit  $x_3 = 0$  ergibt sich

$$4aF(x, y) = (2ax + by)^2 + (4ac - b^2)y^2 = (2ax + by)^2 - Dy^2,$$

sodass  $aF(x, y)$  für  $D < 0$  stets nichtnegativ ist, und der Fall  $aF(x, y) = 0$  kann nur eintreten, wenn  $y = 0$  und wegen  $2ax + by = 0$  auch  $x = 0$  gilt. Damit erhalten wir

$$(5.10) \quad F(x, y) > 0 \text{ für } D < 0, a > 0 \text{ und für alle } x, y \in \mathbb{Z} \setminus \{(0, 0)\}.$$

Diese Formen werden üblicherweise als *positiv-definit* bezeichnet. Wir verwenden im Folgenden meistens die kürzere Charakterisierung  $D < 0$ ,  $a > 0$ .

Als zweite Einschränkung klammern wir die Untersuchung der Formen mit  $D < 0$  und  $a < 0$  aus, weil sich jede solche Form  $(a, b, c)$  umkehrbar eindeutig der Form  $(-a, -b, -c)$  mit  $\text{dis}(-a, -b, -c) = \text{dis}(a, b, c)$  und  $-a > 0$  zuordnen lässt.

Für alle Formen  $F$  mit  $D > 0$  ist  $F(1, 0)F(b, -2a) = a^2(4ac - b^2) = -a^2D < 0$ , sodass zu  $\mathcal{W}_F$  sowohl positive als auch negative Zahlen gehören.

### Definition der Äquivalenz von binären quadratischen Formen

Sind  $F$  und  $G$  Formen, so heißt  $F$  zu  $G$  *äquivalent*, wenn es Zahlen  $r, s, t, u \in \mathbb{Z}$  mit  $ru - st = 1$  gibt, sodass  $F(rx + sy, tx + uy) = G(x, y)$  für alle  $x, y \in \mathbb{Z}$  gilt.

### Satz über Formenäquivalenz

Die Äquivalenz von Formen ist eine Äquivalenzrelation auf der Menge aller binären quadratischen Formen.

**Beweis** (direkt, r1):

**Reflexivität:** Mit  $(r, s, t, u) = (1, 0, 0, 1)$  gilt  $F(x, y) = F(x + 0, 0 + y)$  und  $1 \cdot 1 - 0 \cdot 0 = 1$ .

**Symmetrie:** Es sei  $F$  zu  $G$  äquivalent mit der Beziehung aus der obigen Definition. Wegen  $ru - st = 1$  lässt sich das Gleichungssystem  $rx + sy = x_1$ ,  $tx + uy = y_1$  für alle  $x_1, y_1 \in \mathbb{Z}$  nach  $x$  und  $y$  auflösen:  $x = ux_1 - sy_1$ ,  $y = -tx_1 + ry_1$ . Die ganzzahligen Koeffizienten  $u, -s, -t, r$  erfüllen die Bedingung  $ur - (-s)(-t) = ru - st = 1$ , und es gilt  $G(ux_1 - sy_1, -tx_1 + ry_1) = F(x_1, y_1)$  für alle  $x_1, y_1 \in \mathbb{Z}$ . Also ist  $G$  zu  $F$  äquivalent.

**Transitivität:** Mit  $r, s, t, u, r_1, s_1, t_1, u_1 \in \mathbb{Z}$ ,  $ru - st = 1$  und  $r_1u_1 - s_1t_1 = 1$  sei  $F(rx + sy, tx + uy) = G(x, y)$  für alle  $x, y \in \mathbb{Z}$  und  $G(r_1x_1 + s_1y_1, t_1x_1 + u_1y_1) = H(x_1, y_1)$  für alle  $x_1, y_1 \in \mathbb{Z}$  erfüllt. Dann gilt  $r(r_1x_1 + s_1y_1) + s(t_1x_1 + u_1y_1) = (rr_1 + st_1)x_1 + (rs_1 + su_1)y_1 =: r_2x_1 + s_2y_1$  und  $t(r_1x_1 + s_1y_1) + u(t_1x_1 + u_1y_1) = (tr_1 + ut_1)x_1 + (ts_1 + uu_1)y_1 =: t_2x_1 + u_2y_1$  mit Koeffizienten  $r_2, s_2, t_2, u_2 \in \mathbb{Z}$  und mit  $r_2u_2 - s_2t_2 = rur_1u_1 + sts_1t_1 - rus_1t_1 - str_1u_1 = (ru - st)(r_1u_1 - s_1t_1) = 1$ .

Wegen  $F(r_2x_1 + s_2y_1, t_2x_1 + u_2y_1) = H(x_1, y_1)$  für alle  $x_1, y_1 \in \mathbb{Z}$  ist damit  $F$  zu  $H$  äquivalent.  $\square$

Um alle wesentlichen Invarianten der Formenklassen, in die die Menge der binären quadratischen Formen aufgrund der Äquivalenzrelation zerfällt, in einem Satz zusammenfassen zu können, führen wir schon hier einen Begriff ein, der erst am Schluss dieses Abschnitts benötigt wird.

### Definition der primitiven Form

Eine Form  $(a, b, c)$  heißt *primitiv*, wenn  $\text{ggT}(a, b, c) = 1$  ist.

### Satz über Invarianten der Formenklassen

Es sei  $F = (a, b, c)$  zu  $G = (a_1, b_1, c_1)$  äquivalent. Dann gilt:

- $\text{dis}(a_1, b_1, c_1) = \text{dis}(a, b, c)$ ;
- Aus  $\text{dis}(a, b, c) < 0$  und  $a > 0$  folgt  $a_1 > 0$ ;
- $\mathcal{W}_G = \mathcal{W}_F$ ;
- Ist  $F$  primitiv, so stellt auch  $G$  eine primitive Form dar.

**Beweis** (direkt, r1):

**a)** Aus  $a(rx + sy)^2 + b(rx + sy)(tx + uy) + c(tx + uy)^2 = a_1x^2 + b_1xy + c_1y^2$  für alle  $x, y \in \mathbb{Z}$  folgt durch Koeffizientenvergleich

$$(5.11) \quad a_1 = ar^2 + brt + ct^2,$$

$$(5.12) \quad b_1 = 2ars + b(ru + st) + 2ctu,$$

$$(5.13) \quad c_1 = as^2 + bsu + cu^2.$$

Damit gilt  $b_1^2 - 4a_1c_1 = (2ars + b(ru + st) + 2ctu)^2 - 4(ar^2 + brt + ct^2)(as^2 + bsu + cu^2) = a^2(4r^2s^2 - 4r^2s^2) + b^2(r^2u^2 + 2rstu + s^2t^2 - 4rstu) + c^2(4t^2u^2 - 4t^2u^2) + 4ab(r^2su + rs^2t - r^2su - rs^2t) + 4ac(2rstu - r^2u^2 - s^2t^2) + 4bc(rt u^2 + st^2u - rtu^2 - st^2u) = (b^2 - 4ac)(ru - st)^2 = b^2 - 4ac$ .

**b)** Nach (5.11) ist  $a_1 = F(r, t)$  und aus  $ru - st = 1$  folgt  $(r, t) \neq (0, 0)$ . Damit ergibt (5.10), dass  $a_1 > 0$  gilt.

- c) Wie bei dem Beweis des *Dreiquadratesatzes* ist zunächst  $\mathcal{W}_G \subseteq \mathcal{W}_F$ . Die Symmetrie der Äquivalenzrelation ergibt dann die Gleichheit.
- d) Mit (5.11), (5.12) und (5.13) folgt  $\text{ggT}(a, b, c) \mid \text{ggT}(a_1, b_1, c_1)$ . Aus dem gleichen Grunde wie bei c) gilt auch  $\text{ggT}(a_1, b_1, c_1) \mid \text{ggT}(a, b, c)$ . Also ist  $\text{ggT}(a_1, b_1, c_1) = \text{ggT}(a, b, c)$ .  $\square$

### Satz über die Klassenanzahl

a) In jeder Formenklasse gibt es mindestens eine Form  $(a, b, c)$  mit

$$(5.14) \quad -|a| < b \leq |a| \leq |c|.$$

b) Aus (5.14) folgt  $|b| \leq |a| \leq \sqrt{\frac{1}{3} |\text{dis}(a, b, c)|}$ , woraus sich für jeden festen Diskriminantenwert  $D$  die Endlichkeit der Anzahl der Klassen aller Formen mit der Diskriminante  $D$  ergibt.

**Beweis** (direkt, Fallunterscheidung bei b), a1):

a) Unter allen Formen der zu betrachtenden Klasse sei  $F = (a, b', c')$  eine Form, für die  $|a|$  minimal ist, und  $G = (a, b, c)$  sei diejenige zu  $F$  äquivalente Form, die mit  $s := (\text{sign } a) \left[ \frac{|a| - b'}{2|a|} \right]$  durch  $F(x + sy, y) = G(x, y)$  für alle  $x, y \in \mathbb{Z}$  definiert ist. Die Übereinstimmung des ersten Koeffizienten ergibt sich aus (5.11). Nach (5.12) ist  $b = 2as + b' = 2|a| \left[ \frac{|a| - b'}{2|a|} \right] + b'$  der zweite Koeffizient. Mit der für alle  $x \in \mathbb{R}$  gültigen Ungleichungskette  $x - 1 < [x] \leq x$  erhalten wir

$$(5.15) \quad -|a| = 2|a| \left( \frac{|a| - b'}{2|a|} - 1 \right) + b' < b \leq 2|a| \left( \frac{|a| - b'}{2|a|} \right) + b' = |a|.$$

Wegen  $G(-y, x) = cx^2 - bxy + ay^2$  und  $0 \cdot 0 - (-1) \cdot 1 = 1$  ist

$$(5.16) \quad (a, b, c) \text{ äquivalent zu } (c, -b, a)$$

Deshalb folgt  $|a| \leq |c|$  aufgrund der Minimaleigenschaft von  $|a|$ .

b) Für  $D < 0$  ist  $4ac = b^2 - D > 0$ , und (5.14) ergibt  $4|a|^2 \leq 4|a||c| = 4ac = -D + b^2 \leq -D + |a|^2$ , also  $|a| \leq \sqrt{\frac{1}{3}|D|}$ .

Im Falle  $D > 0$  folgt aus (5.14) zunächst  $|ac| \geq b^2 = D + 4ac > 4ac$ , also  $ac < 0$  und damit  $4a^2 \leq 4|ac| = -4ac = D - b^2 < D$ , d. h. es gilt  $|a| \leq \frac{1}{2}\sqrt{D}$ .

Beide Fälle lassen sich mit (5.14) zu  $|b| \leq |a| \leq \sqrt{\frac{1}{3}|D|}$  zusammenfassen. Da somit bei festem  $D$  der Wertevorrat von  $a$  und  $b$  endlich ist und  $c$  eindeutig von  $a$ ,  $b$  und  $D$  abhängt, gibt es nur endlich viele Formen  $(a, b, c)$ , die (5.14) erfüllen. Ihre Anzahl ist eine obere Schranke für die Zahl der Klassen zur Diskriminante  $D$ , weil in jeder Klasse mindestens eine solche Form liegt.  $\square$

Der Rest dieses Abschnitts ist den Klassen positiv-definiter Formen gewidmet, weil bei diesen die “Composition” von Formenklassen als letzte noch fehlende Entdeckung von GAUß aus [9] relativ einfach dargestellt werden kann. Zunächst sei daran erinnert, dass eine Form genau dann positiv-definit ist, wenn  $D = b^2 - 4ac < 0$  und  $a > 0$  (Seite 153) gilt. Der folgende Begriff und der anschließende Satz, die beide von LAGRANGE (ca. 1773) stammen, werden es ermöglichen, mit ausgezeichneten Formen als Repräsentanten der Klassen zu rechnen und die Klassenanzahl durch Auszählen ohne Äquivalenzuntersuchungen zu bestimmen.

### Definition der reduzierten Form

Eine positiv-definite Form  $(a, b, c)$  heißt *reduziert*, wenn

$$(5.17) \quad -a < b \leq a \leq c - \delta_b \text{ mit } \delta_b := \begin{cases} 1 & \text{für } b < 0, \\ 0 & \text{sonst,} \end{cases}$$

gilt.

### Satz über eindeutige Repräsentanten

Jede Klasse positiv-definiter Formen enthält genau eine reduzierte Form.

**Beweis** (zwei Teile, i) direkt, r1; ii) Fallunterscheidung, a1):

i) Aufgrund des *Satzes über die Klassenanzahl* gibt es in jeder Klasse positiv-definiter Formen mindestens eine Form mit

$$-a < b \leq a \leq c.$$

Da im Falle  $b < 0$  und  $a = c$  wegen (5.16)  $(a, b, a)$  zu  $(a, -b, a)$  mit  $-b > 0$  äquivalent ist, kann die Bedingung  $a \leq c$  durch  $a \leq c - \delta_b$  ersetzt werden.

ii) Stellt  $F = (a, b, c)$  eine reduzierte Form dar, so zeigen wir zunächst, dass  $a \leq a_1$  für alle zu  $(a, b, c)$  äquivalenten Formen  $(a_1, b_1, c_1)$  gilt. Ist  $a_1x^2 + b_1xy + c_1y^2 = F(rx + sy, tx + uy)$  für alle  $x, y \in \mathbb{Z}$ , so ergeben (5.11) und die ersten beiden Reduziertheitsungleichungen aus (5.17)

$$a_1 \geq ar^2 - a|rt| + ct^2 = a(r^2 - |rt| + t^2) + (c - a)t^2.$$

Wegen  $ru - st = 1$  ist  $(r, t) \neq (0, 0)$ , womit  $r^2 - |rt| + t^2 = (|r| - |t|)^2 + |rt| \geq 1$  folgt. Zusammen mit der dritten Reduziertheitsungleichung erhalten wir also

$$(5.18) \quad a_1 \geq a + (c - a)t^2 \geq a.$$

Setzen wir zusätzlich voraus, dass  $(a_1, b_1, c_1)$  reduziert ist, so ergibt (5.18) mit vertauschten Koeffizienten die Beziehung  $a \geq a_1$ . Damit gilt  $a_1 = a$ . Durch Unterscheidung von zwei Fällen weisen wir nun die Gleichheit der beiden Formen nach.

Ist  $c > a$  **oder**  $c_1 > a_1$ , so genügt es wegen der Gleichartigkeit der Durchführungen, von  $c > a$  auszugehen. Da sich für  $t \neq 0$  aus (5.18) ein Widerspruch zu  $a_1 = a$  ergeben würde, muss  $t = 0$  und wegen  $ru - st = 1$  außerdem  $ru = 1$  sein. Mit (5.12) erhalten wir dann  $b_1 = 2ars + b$ . Wegen der Reduziertheit und mit  $a_1 = a$  gilt  $-a < b \leq a$  und  $-a = a_1 < b_1 \leq a_1 = a$ . Daraus folgt  $2a|rs| = |b_1 - b| < 2a$ , sodass sich  $rs = 0$  und damit  $b_1 = b$  ergibt. Stellt  $D$  die gemeinsame Diskriminante aller Formen der Klasse dar, so ist  $c_1 = \frac{b_1^2 - D}{4a_1} = \frac{b^2 - D}{4a} = c$ . Also gilt  $(a_1, b_1, c_1) = (a, b, c)$ .

Als Negation des ersten Falles sei nun  $c = a$  **und**  $c_1 = a_1$ . Wegen  $a_1 = a$  ist dann  $c_1 = c$ , und die Gleichheit der Diskriminanten liefert  $b_1^2 = D + 4a_1c_1 = D + 4ac = b^2$ . Hier muss  $b_1 = b$  sein, weil  $\delta_{b_1} = \delta_b = 0$  nur für  $b_1 \geq 0$  und  $b \geq 0$  gilt. Damit ist stets  $(a_1, b_1, c_1) = (a, b, c)$ , wenn beide Formen positiv-definit, zueinander äquivalent und reduziert sind.  $\square$

Als **Beispiel** bestimmen wir die reduzierten positiv-definiten Formen  $(a, b, c)$  für  $D = -39$ . In einer äußeren Schleife durchläuft  $b$  alle ganzen Zahlen mit  $0 \leq b \leq \sqrt{\frac{1}{3}|D|}$  und  $b \equiv D \pmod{2}$ , während  $a$  in einer inneren Schleife alle ganzzahligen Werte mit  $b \leq a \leq \sqrt{\frac{1}{3}|D|}$  und  $a \mid \frac{b^2 - D}{4}$  annimmt. Wenn  $b \neq 0$ ,  $a \neq b$  und  $a \neq c$  mit  $c := \frac{b^2 - D}{4a}$  gilt, ist neben  $(a, b, c)$  auch  $(a, -b, c)$  reduziert. Für  $D = -39$  erhält man auf diese Weise die Formen  $(1, 1, 10)$ ,  $(2, 1, 5)$ ,  $(2, -1, 5)$  und  $(3, 3, 4)$ .

Als Höhepunkt des fünften Abschnitts von [9] führt GAUß die "Composition" von Formen beziehungsweise Formenklassen ein. Zu Beginn des entsprechenden Abschnitts schreibt er, dass es sich dabei um einen "anderen sehr wichtigen,

bisher noch von Niemand berührten Gegenstand” handelt. Schon bald wurde die grundlegende Bedeutung der folgenden Definition erkannt, die nur wenig an die heutige Schreibweise angepasst ist.

### Definition der Composition von Formen

Die Form  $F$  heißt *aus den Formen  $f_1$  und  $f_2$  componiert*, wenn es ganze Zahlen  $p, p', p'', p''', q, q', q'', q'''$  mit  $\text{ggT}(pq' - qp', pq'' - qp'', pq''' - qp''', p'q'' - q'p'', p'q''' - q'p''', p''q''' - q''p''') = 1$  gibt, so dass

$$F(pxx' + p'xy' + p''yx' + p'''yy', qxx' + q'xy' + q''yx' + q'''yy') = f_1(x, y)f_2(x', y')$$

für alle  $x, x', y, y' \in \mathbb{Z}$  gilt.

In dieser Definition unterliegen die Formen  $f_1$  und  $f_2$  keiner Einschränkung. Insbesondere können ihre Diskriminanten verschieden sein. In dieser großen Allgemeinheit leitete GAUß zunächst sechs Folgerungen her, zeigte als “Aufgabe”, wie sich  $F$  zu beliebigen Formen  $f_1$  und  $f_2$  berechnen lässt, und bewies in vier Sätzen unter anderem, dass die *Composition als Verknüpfung der Formenklassen* angesehen werden kann, weil einerseits  $F$  nur bis auf Äquivalenz bestimmt ist und weil andererseits das Componieren von Formen, die zu  $f_1$  beziehungsweise  $f_2$  äquivalent sind, eine Form aus der Äquivalenzklasse von  $F$  ergibt. Außerdem gewann er als Nebenergebnis die *Assoziativität* und *Kommutativität* der Composition.

Die weiteren Untersuchungen der Composition führte GAUß für Formen mit gleicher Diskriminante durch. Mit einer einfachen zusätzlichen Einschränkung erreichte er, dass die Ergebnisform  $F$  dieselbe Diskriminante hat wie die componierten Formen  $f_1$  und  $f_2$ . Er war dann in der Lage, die Koeffizienten von  $F =: (a_3, b_3, c_3)$  direkt aus denen von  $f_i =: (a_i, b_i, c_i)$ ,  $i = 1, 2$ , zu berechnen. Damit zeigte er auch, dass es zu jeder Diskriminante eine reduzierte Form - von ihm “Hauptform” genannt - gibt, die mit einer beliebigen Form  $f$  derselben Diskriminante componiert eine zu  $f$  äquivalente Form ergibt und dass die Composition einer primitiven Form  $(a, b, c)$  mit  $(a, -b, c)$  stets eine zur Hauptform äquivalente Form liefert.

Damit hatte GAUß alle Nachweise dafür geführt, dass die Klassen der primitiven Formen mit gegebener Diskriminante  $D$  zusammen mit der Composition, die über beliebige Repräsentanten der Klassen auszuführen ist, im heutigen Sinn eine

endliche abelsche Gruppe bilden, die *Klassengruppe zur Diskriminante  $D$*  genannt wird. Wie auf Seite 97 erwähnt wurde, war zur Zeit von GAUß der Begriff der Gruppe noch nicht bekannt. Das folgende zusammenfassende Theorem bereitet zugleich den Übergang zu der neueren Theorie der “quadratischen Zahlkörper” im nächsten Abschnitt vor, wo auch die Skizze eines “modernem” Beweises des Theorems zu finden ist. Da dieser Teil nur ein Ausblick sein soll, beschränken wir uns auf primitive, positiv-definite Formen.

### Theorem über die Klassengruppe

Es seien  $f_1 =: (a_1, b_1, c_1)$  und  $f_2 =: (a_2, b_2, c_2)$  primitive, positiv-definite Formen mit der Diskriminante  $D$ . Ist  $g := \text{ggT}(a_1, a_2, q)$  mit  $q := \frac{b_1 + b_2}{2}$  und sind  $u, v, w$  ganze Zahlen, die  $a_1 u + a_2 v + q w = g$  erfüllen, so stellt  $F = (a_3, b_3, c_3)$  mit  $a_3 := \frac{a_1}{g} \frac{a_2}{g}$ ,  $b_3 := b_2 + 2 \frac{a_2}{g} \bmod \left( (q - b_2) v - c_2 w, \frac{a_1}{g} \right)$  und  $c_3 := \frac{b_3^2 - D}{4a_3}$  eine aus  $f_1$  und  $f_2$  componierte Form mit der Diskriminante  $D$  dar.

Die Composition von Formen, die zu  $f_1$  beziehungsweise  $f_2$  äquivalent sind, ergibt eine Form aus der Äquivalenzklasse von  $F$ . Die Menge dieser Formenklassen zusammen mit der durch Composition beliebiger Repräsentanten der Klassen erklärten Verknüpfung stellt eine endliche abelsche Gruppe dar, deren neutrales Element diejenige Klasse ist, die die *Einheitsform*  $\left(1, \alpha, \frac{\alpha - D}{4}\right)$  mit  $\alpha \equiv \text{mod}(D, 4)$  enthält, und bei der die Klasse mit der reduzierten Form  $(a, b, c)$  zu der Klasse mit der Form  $(a, -b, c)$  invers ist.

Aufgrund des *Satzes über eindeutige Repräsentanten* (Seite 156) bietet es sich an, die Klassen positiver-definiten Formen jeweils durch die Composition der zugehörigen reduzierten Formen zu verknüpfen. Da die positiv-definite Ergebnisform in der Regel nicht reduziert ist, wird der folgende **Reduktionsalgorithmus** benötigt, der sich direkt aus den Beweisen des *Satzes über die Klassenanzahl* (Seite 155) und des *Satzes über eindeutige Repräsentanten* ergibt.

Es sei  $(a, b, c)$  eine primitive, positiv-definite Form. Solange nicht  $-a < b \leq a \leq c$  gilt, werde  $G = (a_1, b_1, c_1)$  mit  $F(x + sy, y) = G(x, y)$  für alle  $x, y \in \mathbb{Z}$  bestimmt, wobei  $s := \left\lfloor \frac{a-b}{2a} \right\rfloor$  ist. Nach (5.11) bis (5.13) gilt  $a_1 = a$ ,  $b_1 = 2as + b$ ,  $c_1 =$

$as^2+bs+c = c+\frac{1}{2}(b+b_1)s$ , und (5.15) ergibt  $-a_1 < b_1 \leq a_1$ . Im Falle  $a_1 > c_1$  werde gemäß (5.16) als Abschluss des Schleifendurchlaufs  $a := c_1$ ,  $b := -b_1$ ,  $c := a_1$  gesetzt; andernfalls sei  $a := a_1$ ,  $b := b_1$ ,  $c := c_1$ .

Nach endlich vielen Schritten hat man eine Form  $(a, b, c)$  mit  $-a < b \leq a \leq c$ , die nur für  $a = c$  und  $b < 0$  nicht reduziert ist. In diesem Fall ergibt  $(a, -b, a)$  wegen (5.16) die gesuchte reduzierte Form.

Für den *Reduktionsalgorithmus* bringen wir zunächst ein **Beispiel** von GAUß, wobei zu beachten ist, dass er mit  $(a, b, c)$  die Form bezeichnet, die bei uns mit  $(a, 2b, c)$  abgekürzt wird, und dass die Diskriminante dem Vierfachen seiner “Determinante” entspricht.

Für  $D = -124$  ergibt der Algorithmus nacheinander die Formen  $(304, 434, 155)$ ,  $(304, -174, 25)$ ,  $(25, 174, 304)$ ,  $(25, 24, 7)$ ,  $(7, -24, 25)$ ,  $(7, 4, 5)$ ,  $(5, -4, 7)$ , und die letzte davon ist reduziert.

Da die von GAUß behandelten Determinanten umkehrbar eindeutig den geraden Diskriminanten entsprechen, hat der folgende Fall mit  $D = -19$  bei ihm kein Gegenstück:  $(23, 25, 7)$ ,  $(23, -21, 5)$ ,  $(5, 21, 23)$ ,  $(5, 1, 1)$ ,  $(1, -1, 5)$ ,  $(1, 1, 5)$ .

Der *Reduktionsalgorithmus* hat ein ähnlich günstiges Laufzeitverhalten wie der *Euklidische Algorithmus*, dessen Schrittzahl im *Effizienzsatz* (Seite 22) abgeschätzt wurde. Gilt nach dem ersten Schleifenschritt  $a = a_1 > \sqrt{|D|}$ , so folgt  $c_1 = \frac{b_1^2+|D|}{4a_1} < \frac{a_1^2+a_1^2}{4a_1} = \frac{1}{2}a_1$ , und die anschließende Vertauschung von  $a_1$  und  $c_1$  ergibt, dass  $a$  bei jedem Schleifendurchlauf mindestens halbiert wird, solange  $a > \sqrt{|D|}$  ist. Für  $a < \sqrt{|D|}$  lässt sich mit Fallunterscheidung zeigen, dass höchstens ein weiterer Reduktionsschritt benötigt wird. Damit ist die Schrittzahl kleiner als  $\frac{3}{2} \ln \left( \frac{a}{\sqrt{|D|}} \right) + 2$ .

Nun ist es möglich, effizient in der Klassengruppe zu “rechnen”, indem reduzierte Formen mit anschließender Reduktion komponiert werden. Da wir in dem folgenden Abschnitt nur einen Ausblick auf die weitere Entwicklung geben, die mit der Formencomposition zusammenhängt, skizzieren wir hier noch eine Anwendung der Klassengruppe positiv-definiten Formen bei der Faktorisierung natürlicher Zahlen. Eine ausführliche Darstellung von algorithmischen Aspekten der elementaren und algebraischen Zahlentheorie ist in [2] enthalten. Die wichtigsten Algorithmen der Zahlentheorie werden auch in [8] behandelt.

## Faktorisierung mit Hilfe der Klassengruppe

In den Abschnitten 329 bis 334 von [9] beschrieb GAUß zwei Methoden zur **Faktorzerlegung** von natürlichen Zahlen mit Hilfe quadratischer Reste. Auf fast einer ganzen Seite erörterte er zunächst die Bedeutung solcher Verfahren für die Faktorisierung von Zahlen mit “sieben und mehr” Ziffern. Der folgende Begriff, den GAUß im Zusammenhang mit binären quadratischen Formen eingeführt hat, bildet heute die Grundlage eines der effizientesten Faktorisierungsverfahren für Zahlen mit 60 und mehr Ziffern.

### Definition der ambigen Form

Eine primitive, positiv-definite Form  $f$  heißt *ambig*, wenn  $f$  mit sich selbst komponiert eine Form ergibt, die zu der Einheitsform äquivalent ist.

Aufgrund des **Theorems über die Klassengruppe** (Seite 159) ist eine primitive, positiv-definite Form  $(a, b, c)$  genau dann *ambig*, wenn  $(a, -b, c)$  eine zu  $(a, b, c)$  äquivalente Form darstellt. Ist  $(a, b, c)$  außerdem reduziert, so können nur die folgenden drei Fälle auftreten:

i) Ist auch  $(a, -b, c)$  reduziert, so muss wegen des **Satzes über eindeutige Repräsentanten** (Seite 156)  $(a, -b, c) = (a, b, c)$  gelten. Daraus folgt  $b = 0$  und damit  $D = -4ac$ .

ii), iii) Ist  $(a, -b, c)$  nicht reduziert, so folgt  $a = b$  **oder**  $a = c$ , weil andernfalls  $(a, -b, c)$  wegen  $-a < -b$  **und**  $a < c$  reduziert wäre.

Auch hier ergibt sich für  $D$  jeweils eine Zerlegung  $D = b(b - 4c)$  beziehungsweise  $D = (b - 2a)(b + 2a)$ . Entsprechende Produktdarstellungen gewinnen wir für die natürlichen Zahlen  $N := -\frac{D}{4-3\alpha}$  mit  $\alpha = \text{mod}(D, 4)$ .

Wegen  $\alpha = \text{mod}(b, 2)$  können wir  $b' := \frac{b}{2-\alpha} \in \mathbb{N}_1$  setzen und erhalten mit  $\beta := 1 + \alpha$  in den drei obigen Fällen  $N = ac$ ,  $N = b'(2\beta c - b')$  beziehungsweise  $N = (\beta a - b')(\beta a + b')$ .

Diese Zerlegungen sind natürlich nur dann von Nutzen, wenn die entsprechende *ambige Form* von der *Einheitsform* verschieden ist. Die Voraussetzung der Existenz solcher Formen wird durch zwei weitere beeindruckende Ergebnisse aus [9] geklärt. Im Zusammenhang mit der Darstellbarkeit von Zahlen durch Formen führte GAUß den Begriff des **Geschlechts von Formenklassen in einer Ordnung** ein.

Heute weiß man, dass diese “Geschlechter in einer Ordnung” diejenigen Äquivalenzklassen von Formen sind, die entstehen, wenn in der Definition von Seite 153 die Zahlen  $r, s, t, u$  rational sein dürfen (siehe [1]). Bei diesem Zugang spricht man von einem **Geschlecht** ohne den Zusatz “in einer Ordnung”. Verwenden wir diese Bezeichnungsweise, so zeigte GAUß, dass in allen Geschlechtern, die zu derselben Diskriminante  $D$  gehören, gleich viele

Klassen liegen und dass es mindestens  $2^{\Omega(-D)-2}$  Geschlechter gibt, wenn  $D$  gerade und  $\Omega(-D) \geq 2$  ist. Bezeichnet  $h$  die **Klassenzahl**, nämlich die Anzahl der Klassen in der Klassengruppe zur Diskriminante  $D$ , so ist also  $h$  mindestens durch  $2^{\Omega(-D)-2}$  teilbar.

Wird für ungerades  $N \in \mathbb{N}_3$  als Umkehrung der obigen Abkürzung die Diskriminante  $D$  durch  $D := \begin{cases} -N, & \text{wenn } N \equiv 3 \pmod{4} \text{ ist,} \\ -4N & \text{sonst,} \end{cases}$  definiert, so ergeben die Resultate von GAUß zusammen mit späteren Verallgemeinerungen, dass  $2^{\Omega(-D)-1}$  die Klassenzahl  $h$  teilt. Für zerlegbares  $N$  ist also  $h$  gerade.

Wird die Verknüpfung in der Klassengruppe ohne ein Verknüpfungszeichen “multiplikativ” geschrieben, so gibt es aufgrund eines allgemeinen Satzes der Algebra wegen des Teilers 2 von  $h$  eine Klasse  $f$ , die von der neutralen Klasse  $e$  verschieden ist und für die  $f^2 = e$  gilt. Definitionsgemäß existiert dann in  $f$  eine ambige Form. Aufgrund des **Theorems über die Klassengruppe** (Seite 159) sind damit alle Formen von  $f$  ambig, sodass man von einer **ambigen Klasse** spricht.

Solche ambigen Klassen können mit einer Standardmethode der Algebra bestimmt werden: Ist  $t := \nu_2(h)$ ,  $q := 2^{-t}h$  und  $f$  eine Formenklasse, für die  $g := f^q$  nicht die neutrale Klasse darstellt, so existiert ein  $m \in \mathcal{A}_t$ , mit dem  $g^{2^m}$  eine ambige Klasse ergibt. Hier lässt sich  $h$  zunächst mit Hilfe einer analytischen Formel, die wir im nächsten Abschnitt (Seite 180) angeben, in einem relativ kleinen Intervall einschließen und dann durch die Berechnung der als Teiler von  $h$  auftretenden “Ordnungen” einer Sequenz von Formenklassen  $f_i$  exakt bestimmen, wobei die **Ordnung** von  $f_i$  durch  $\min \{ \gamma \in \mathbb{N}_1 ; f_i^\gamma = e \}$  analog zur Ordnung modulo  $m$  (Seite 120) definiert ist. Die obigen Formenklassen  $f$  werden durch zufällige Wahl der zugehörigen reduzierten Form unter sinnvollen Bedingungen gewonnen.

Diese Idee und ihre Ausgestaltung als Algorithmus zur Berechnung von  $h$  und zur Faktorisierung großer ungerader Zahlen  $N$  stammt von D. SHANKS (1969). Drei Jahre später hat SHANKS ein weiteres effizientes Faktorisierungsverfahren veröffentlicht, das die Klassengruppe von positiven Diskriminanten verwendet. Etwa zehn Jahre danach wurde die erste Methode von SHANKS durch zwei Gruppen von Mathematikern unabhängig voneinander wesentlich verbessert. Typisch für alle “modernen” Primzahltests und Faktorisierungsalgorithmen ist die Verwendung einer **Verallgemeinerungsstrategie**, indem “höhere” mathematische Strukturen wie zum Beispiel Klassengruppen, “elliptische Kurven” und “Zahlkörper” benutzt werden. Ein Beispiel für die Letzteren gibt der nächste Abschnitt.

## 5.4 Quadratische Zahlkörper

### Eindeutige Darstellung

Ist  $w \in \mathbb{Q}^+$ , so stellt  $\sqrt{w}$  aufgrund des *Satzes über rationale  $k$ -te Wurzeln* (Seite 56) genau dann eine rationale Zahl dar, wenn es ein  $v \in \mathbb{Q}^+$  mit  $w = v^2$  gibt. Im Falle  $-w \in \mathbb{Q}^+$  gilt stets  $\sqrt{w} \notin \mathbb{Q}$ , weil  $\sqrt{w} = \sqrt{|w|}i$  eine komplexe Zahl mit nicht verschwindendem Imaginärteil ist. Um Eindeutigkeit zu erreichen, werden alle Quadratwurzeln aus positiven rationalen Zahlen positiv gewählt. Da  $\sqrt{w} \in \mathbb{C} \setminus \mathbb{Q}$  für jedes  $w \in \mathbb{Q}$  gilt, das keine rationale Quadratzahl ist, kann der kleinste Unterkörper  $\mathbb{Q}(\sqrt{w})$  von  $\mathbb{C}$  bestimmt werden, der  $\mathbb{Q}$  und  $\sqrt{w}$  enthält. Die Körpereigenschaften von  $\mathbb{Q}$  und  $\mathbb{C}$ , die in der *Zahlgenese* hergeleitet werden, setzen wir hier voraus.

Die Elemente von  $\mathbb{Q}(\sqrt{w})$  entstehen durch endlich oft wiederholte Addition, Multiplikation und Division von rationalen Zahlen und  $\xi := \sqrt{w}$ . Sie haben deshalb zunächst die Form  $\frac{P(\xi)}{Q(\xi)}$ , wobei  $P$  und  $Q$  Polynome mit rationalen Koeffizienten und mit  $Q(\xi) \neq 0$  sind. Wegen  $\xi^{2k} = w^k$ ,  $\xi^{2k+1} = w^k \xi$  für  $k \in \mathbb{N}$  und  $\frac{1}{u+v\xi} = \frac{u-v\xi}{u^2-v^2w}$  für  $u, v \in \mathbb{Q}$  lassen sich alle Elemente in der Form  $x + y\sqrt{w}$  mit  $x, y \in \mathbb{Q}$  darstellen.

Wird  $w$  zerlegt als  $w = v^2d$  mit  $v \in \mathbb{Q}^+$  und mit quadratfreiem  $d \in \mathbb{Z} \setminus \mathcal{A}_2$ , so gilt  $x + y\sqrt{w} = x + yv\sqrt{d}$  für alle  $x, y \in \mathbb{Q}$ . Also ist  $\mathbb{Q}(\sqrt{w}) = \mathbb{Q}(\sqrt{d})$ . Die auf diese Weise gewonnenen *quadratischen Zahlkörper*  $\mathbb{Q}(\sqrt{d})$  mit  $d$  aus

$$\mathcal{S} := \{s \in \mathbb{Z} \setminus \mathcal{A}_2; |s| \text{ ist quadratfrei}\}$$

können nicht weiter zurückgeführt werden. Sind nämlich  $d, d' \in \mathcal{S}$  mit  $d \neq d'$ , so gilt  $\mathbb{Q}(\sqrt{d}) \neq \mathbb{Q}(\sqrt{d'})$ , weil andernfalls etwa aus  $\sqrt{d'} = x + y\sqrt{d}$  mit  $x, y \in \mathbb{Q}$  zunächst  $d' - x^2 - dy^2 = 2xy\sqrt{d}$  und dann  $xy = 0$  wegen  $\sqrt{d} \notin \mathbb{Q}$  folgen würde. Für  $y = 0$  ergäbe sich  $d' = x^2 \notin \mathcal{S}$  und für  $x = 0$  wäre  $d' = dy^2$  im Widerspruch zu  $d' \in \mathcal{S}$  beziehungsweise zu  $d' \neq d$ .

Ein Zahlkörper  $\mathbb{Q}(\sqrt{d})$  heißt für  $d > 0$  *reell-quadratisch* und für  $d < 0$  *imaginär-quadratisch*. Für die Zahlentheorie in  $\mathbb{Q}(\sqrt{d})$  benötigen wir einige Begriffe und Abkürzungen.

### Bezeichnungen der Konjugation, Spur, Norm und Diskriminante

Die Abbildung  $\varsigma : \mathbb{Q}(\sqrt{d}) \rightarrow \mathbb{Q}(\sqrt{d})$ ,<sup>4</sup>  $x+y\sqrt{d} \mapsto x-y\sqrt{d}$  heißt *Konjugation*. Damit lassen sich die Abbildungen  $S : \mathbb{Q}(\sqrt{d}) \rightarrow \mathbb{Q}$ ,  $\eta \mapsto \eta + \varsigma(\eta)$  und  $N : \mathbb{Q}(\sqrt{d}) \rightarrow \mathbb{Q}$ ,  $\eta \mapsto \eta\varsigma(\eta)$  definieren, die *Spur* beziehungsweise *Norm* genannt werden.

Zu der *Diskriminante*  $D := \begin{cases} d, & \text{wenn } d \equiv 1 \pmod{4}, \\ 4d, & \text{wenn } d \equiv 2, 3 \pmod{4}, \end{cases}$  gehört die *Parität*

$\alpha = \text{mod}(D, 4) \in \mathcal{A}_2$  (siehe Seite 152 und Seite 159).

## Ganz-algebraische Zahlen

Der nächste grundlegende Begriff verallgemeinert die ganzen Zahlen aus  $\mathbb{Q}$ . Ähnlich wie die rationalen Zahlen und die ganzen Zahlen Lösungen von Gleichungen  $ax + b = 0$  beziehungsweise  $x + c = 0$  mit  $a, b, c \in \mathbb{Z}$  sind, lassen sich die “ganz-algebraischen” Zahlen in  $\mathbb{Q}(\sqrt{d}) \setminus \mathbb{Z}$  als Lösungen von Gleichungen  $x^2 + ex + f = 0$  mit  $e, f \in \mathbb{Z}$  definieren, während alle übrigen nicht rationalen Elemente jeweils einer quadratischen Gleichung mit teilerfremden ganzen Koeffizienten und mit einem von  $\pm 1$  verschiedenen ganzen Quadratkoeffizienten genügen. Da mit  $\eta \in \mathbb{Q}(\sqrt{d})$  auch  $\varsigma(\eta)$  die Ganzheitseigenschaft haben soll, können  $S(\eta)$  und  $N(\eta)$  anstelle von  $e$  und  $f$  verwendet werden.

### Definition der ganz-algebraischen Zahlen in $\mathbb{Q}(\sqrt{d})$

Eine Zahl  $\eta \in \mathbb{Q}(\sqrt{d})$  heißt *ganz-algebraisch*, wenn  $S(\eta) \in \mathbb{Z}$  und  $N(\eta) \in \mathbb{Z}$  gilt.

Obwohl GAUß in einer 1832 veröffentlichten Arbeit über biquadratische Reste die “ganzen komplexen Zahlen” in  $\mathbb{Q}(\sqrt{-1})$  untersuchte und die Bedeutung dieser “Erweiterung des Feldes der Arithmetik” unterstrich, haben die beiden großen Zahlentheoretiker der nachfolgenden Generation, DIRICHLET (ab 1840) und E. E. KUMMER<sup>5</sup> (1847), die “algebraische Zahlentheorie” nur am Rande weitergeführt. Zu ihrer vollen Blüte wurde sie erst durch KRONECKER (1858/1881) und DEDEKIND (1878) entwickelt.

<sup>4</sup> Der griechische Buchstabe  $\varsigma$  heißt auch “Sigma”.

<sup>5</sup> ERNST EDUARD KUMMER (1810-1893) wirkte in Breslau und Berlin.

Bezeichnet  $R_d$  die Menge der ganz-algebraischen Zahlen in  $\mathbb{Q}(\sqrt{d})$ , so ist es für die weiteren Untersuchungen günstig, dass die Elemente von  $R_d$  explizit angegeben werden können.

### Satz über ganz-algebraische Zahlen

Eine Zahl  $\eta \in \mathbb{Q}(\sqrt{d})$  ist genau dann ganz-algebraisch, wenn es  $u, v \in \mathbb{Z}$  gibt, sodass  $\eta = u + v\rho$  mit  $\rho := \frac{\alpha + \sqrt{D}}{2}$  gilt.

**Beweis** (direkt, zwei Teile, Fallunterscheidung, r1):

i) Ist  $\eta = u + v\rho$  mit  $u, v \in \mathbb{Z}$ , so folgt wegen  $\varsigma(\eta) = u + \frac{\alpha}{2}v - \frac{v}{2}\sqrt{D}$ , dass  $S(\eta) = 2u + \alpha v \in \mathbb{Z}$  und  $N(\eta) = (u + \frac{\alpha}{2}v)^2 - \frac{1}{4}v^2D = u^2 + \alpha uv + \frac{\alpha - D}{4}v^2 \in \mathbb{Z}$  gilt. Also gehört  $\eta$  zu  $R_d$ . Die *Normgleichung*

$$(5.19) \quad N(u + v\rho) = (u + \alpha \frac{v}{2})^2 - \frac{D}{4}v^2 = u^2 + \alpha uv + \delta v^2 \quad \text{mit } \delta := \frac{\alpha - D}{4} \in \mathbb{Z}$$

wird noch für weitere Anwendungen benötigt.

ii) Ist  $\eta = x + y\sqrt{d} \in R_d$ , so ergibt sich aus  $s := S(\eta) = 2x \in \mathbb{Z}$  und  $N(\eta) = x^2 - dy^2 \in \mathbb{Z}$ , dass  $\frac{1}{4}(s^2 - d(2y)^2)$  ganz sein muss. Da  $|d|$  quadratfrei ist, folgt  $v := 2y \in \mathbb{Z}$  und  $s^2 - dv^2 \equiv 0 \pmod{4}$ . Im Falle  $d \equiv 1 \pmod{4}$  ist die Kongruenz äquivalent zu  $s \equiv v \pmod{2}$ , sodass ein  $u \in \mathbb{Z}$  mit  $s = v + 2u$  existiert. Also gilt  $\eta = \frac{s}{2} + \frac{v}{2}\sqrt{d} = u + v\rho$  mit  $u, v \in \mathbb{Z}$ .

Für  $\text{mod}(d, 4) \in \{2, 3\}$  kann  $v$  wegen  $\text{mod}(s^2, 4) \in \mathcal{A}_2$  nicht ungerade sein. Aus  $2 \mid v$  und  $s^2 \equiv 0 \pmod{4}$  ergibt sich  $2 \mid s$ , also  $\eta = \frac{s}{2} + \frac{v}{2}\sqrt{d} = s + v\rho$  mit  $s, v \in \mathbb{Z}$ . □

## Die Maximalordnung und ihre Unterringe

Mit Hilfe des *Satzes über ganz-algebraische Zahlen* und wegen

$$(5.20) \quad \rho^2 = \alpha\rho - \delta \in R_d$$

ergibt sich, dass die Summe und das Produkt von Elementen aus  $R_d$  wieder zu  $R_d$  gehören. Damit stellt  $R_{d,1} := (R_d, +, \cdot, 0, 1, -)$  einen Unterring von  $\mathbb{Q}(\sqrt{d})$  dar, der aus historischen Gründen *Maximalordnung* (oder *Hauptordnung*) von  $\mathbb{Q}(\sqrt{d})$  genannt wird. Ein nicht ganz in  $\mathbb{Q}$  enthaltener Unterring  $R$  der Maximalordnung heißt *Ordnung* von  $\mathbb{Q}(\sqrt{d})$ . Diese zusätzlichen Unterringe werden

für die vollständige Beschreibung des Zusammenhangs zwischen binären quadratischen Formen und noch zu definierenden Strukturen in  $\mathbb{Q}(\sqrt{d})$  benötigt.

Alle Ordnungen  $R$  von  $\mathbb{Q}(\sqrt{d})$  lassen sich in einfacher Weise beschreiben. Wegen  $R \subseteq R_{d,1}$  hat jedes Element  $\xi \in R$  die Form  $\xi = x + y\rho$  mit  $x, y \in \mathbb{Z}$ . Wird

$$f := \min \{y \in \mathbb{N}_1 ; \text{Es gibt } x \in \mathbb{Z} \text{ mit } x + y\rho \in R\}$$

gesetzt und  $g \in \mathbb{Z}$  so gewählt, dass  $g + f\rho \in R$  gilt, so folgt  $f\rho \in R$ , weil  $R$  einen Ring darstellt und  $g \in R$  ist. Wegen der Minimalität von  $f$  ergibt sich  $f \mid y$  für alle  $x + y\rho \in R$ .

Nun ist es zweckmäßig, für  $a \in \mathbb{Z}$  und  $b \in R_d$  die folgende auch später benötigte Abkürzung einzuführen:

$$\{a, b\}_{\mathbb{Z}} := \left\{ \xi \in \mathbb{Q}(\sqrt{d}) ; \text{Es gibt } u, v \in \mathbb{Z} \text{ mit } \xi = au + bv \right\}.$$

Zu jeder Ordnung  $R$  von  $\mathbb{Q}(\sqrt{d})$  gibt es also ein  $f \in \mathbb{N}_1$ , sodass  $\xi \in R$  genau dann gilt, wenn  $\xi$  in  $\{1, f\rho\}_{\mathbb{Z}}$  liegt. Umgekehrt stellt

$$R_{d,f} := (\{1, f\rho\}_{\mathbb{Z}}, +, \cdot, 0, 1, -)$$

für jedes  $f \in \mathbb{N}_1$  mit den entsprechend eingeschränkten Verknüpfungen aus  $R_{d,1}$  einen Ring dar, weil einerseits  $(\{1, f\rho\}_{\mathbb{Z}}, +, 0, -)$  eine abelsche Gruppe ist und weil sich andererseits mit vollständiger Induktion ergibt, dass  $(f\rho)^k \in \{1, f\rho\}_{\mathbb{Z}}$  für jedes  $k \in \mathbb{N}$  gilt. Den Induktionsanfang bilden aufgrund der Definition von  $\{1, f\rho\}_{\mathbb{Z}}$  die Fälle  $k = 0, 1$ , und die im Induktionsschritt durchzuführende Reduktion wird durch die aus (5.20) folgende Beziehung

$$(f\rho)^2 = \alpha f(f\rho) - f^2 \delta \in \{1, f\rho\}_{\mathbb{Z}}$$

ermöglicht.

Im Hinblick auf unser Ziel, eine Verbindung zu den binären quadratischen Formen des vorigen Abschnitts herzustellen, führen wir für jede Ordnung  $R_{d,f}$  die üblicherweise mit linearer Algebra definierte *Diskriminante*  $D_f$  einer Ordnung als Diskriminante der quadratischen Form  $N(x + yf\rho)$  ein. Die *Normgleichung* (5.19) ergibt  $N(x + yf\rho) = x^2 + \alpha fxy + f^2 \delta y^2$ . Also folgt mit der Definition einer Form von Seite 152

$$D_f := \alpha^2 f^2 - 4f^2 \delta = \alpha f^2 - f^2(\alpha - D) = f^2 D.$$

Damit ist einerseits jede Ordnung  $R_{d,f}$  irgendeines quadratischen Zahlkörpers eindeutig durch ihre Diskriminante  $f^2 D$  bestimmt, und andererseits tritt jede

mögliche Formendiskriminante (siehe Seite 152) als Diskriminante  $D_f$  genau einer Ordnung  $R_{d,f}$  mit  $d \in \mathcal{S}$  und  $f \in \mathbb{N}_1$  auf. Für diese Diskriminantenmenge verwenden wir im Folgenden die Abkürzung

$$\mathcal{D} := \left\{ D \in \mathbb{Z} ; \text{mod}(D, 4) \in \mathcal{A}_2 \text{ und } \sqrt{D} \notin \mathbb{N} \right\}.$$

Als Unterring des Körpers  $\mathbb{Q}(\sqrt{d})$  ist jede Ordnung  $R_{d,f}$  nullteilerfrei. Damit kann die Teilbarkeit von Elementen aus  $R_{d,f}$  wie in  $\mathbb{Z}$  (Seite 17) definiert werden. In der Zahlentheorie von  $R_{d,f}$  spielen außerdem die von 1 verschiedenen "Einheiten" eine wichtige Rolle.

## Einheiten

### Definition des Teilers und der Einheit

Sind  $\beta, \gamma \in R_{d,f}$ , so heißt  $\beta$  *Teiler von*  $\gamma$ , wenn es ein  $\zeta \in R_{d,f}$  mit  $\gamma = \beta \zeta$  gibt.

Ein Element  $\eta \in R_{d,f}$  heißt *Einheit von*  $R_{d,f}$ , wenn  $\eta$  ein Teiler von 1 ist. Die Menge der Einheiten von  $R_{d,f}$  wird mit  $R_{d,f}^*$  bezeichnet.

Die Teilbarkeitstheorie in  $R_{d,f}$  ist viel komplizierter als in  $\mathbb{Z}$ . Der allein interessierende Fall  $f = 1$  wird später nur gestreift und das wichtigste Ergebnis in einem Theorem wiedergegeben. Dagegen führt der Versuch, die Einheiten von  $R_{d,f}$  explizit zu bestimmen, auf einen wichtigen Zugang zu den meisten der hier eine Rolle spielenden Ergebnisse über Teilbarkeit und über Einheiten.

Zunächst erkennen wir, dass  $(R_{d,f}^*, \cdot, 1, /)$  eine abelsche Gruppe ist; denn aus  $\eta_i, \vartheta_i \in R_{d,f}$  mit  $\eta_i \vartheta_i = 1$  für  $i = 1, 2$  folgt  $(\eta_1 \eta_2)(\vartheta_1 \vartheta_2) = 1$  mit  $\eta_1 \eta_2, \vartheta_1 \vartheta_2 \in R_{d,f}$ , sodass  $\eta_1 \eta_2$  eine Einheit darstellt. Da in  $\mathbb{Q}(\sqrt{d}) \setminus \{0\}$  die Reziproken  $\frac{1}{\eta_i}$  eindeutig durch  $\eta_i \frac{1}{\eta_i} = 1$  definiert sind, ergibt sich auch  $1/\eta_i := \frac{1}{\eta_i} = \vartheta_i \in R_{d,f}^*$ .

Die Elemente dieser Gruppe, die *Einheitengruppe* von  $R_{d,f}$  heißt, werden wir im nächsten Satz vollständig angeben. Dazu benötigen wir ein Kriterium für die Komponenten  $x, y$  von  $x+yf\rho \in R_{d,f}^*$ . Für alle  $\beta_i =: u_i + v_i\sqrt{d} \in \mathbb{Q}(\sqrt{d})$ ,  $i = 1, 2$ , gilt

$$(5.21) \quad \varsigma(\beta_1)\varsigma(\beta_2) = (u_1u_2 + dv_1v_2) - (u_1v_2 + v_1u_2)\sqrt{d} = \varsigma(\beta_1\beta_2).$$

Insbesondere folgt für  $\eta \in R_{d,f}^*$  und  $\vartheta := \frac{1}{\eta}$ , dass  $\varsigma(\eta)\varsigma(\vartheta) = \varsigma(\eta\vartheta) = 1$  ist. Damit gehören auch  $\varsigma(\eta)$  und  $N(\eta) = \eta\varsigma(\eta)$  zu  $R_{d,f}^*$ . Wegen  $N(\eta) \in \mathbb{Z}$  muss also

$N(\eta) = N(x + yf\rho) = x^2 + \alpha fxy + f^2 \delta y^2 \in \{-1, 1\}$  gelten. Erfüllt umgekehrt  $\eta \in R_{d,f}$  eine Gleichung  $N(\eta) = e$  mit  $e \in \{-1, 1\}$ , so gehört  $\eta$  wegen  $\eta(e\varsigma(\eta)) = eN(\eta) = 1$  zu  $R_{d,f}^*$ . Für  $\eta =: x + yf\rho \in R_{d,f}$  gilt damit genau dann  $\eta \in R_{d,f}^*$ , wenn  $|N(\eta)| = 1$  ist beziehungsweise wenn die Komponenten  $x, y \in \mathbb{Z}$  einer der beiden folgenden Gleichungen genügen:

$$(5.22) \quad x^2 + \alpha fxy + f^2 \delta y^2 = e \text{ mit } e \in \{-1, 1\}.$$

Aus (5.21) und wegen  $N(\beta_1\beta_2) = (\beta_1\beta_2)\varsigma(\beta_1\beta_2) = (\beta_1\varsigma(\beta_1))(\beta_2\varsigma(\beta_2))$  folgt außerdem die oben angekündigte grundlegende Beziehung

$$(5.23) \quad N(\beta_1\beta_2) = N(\beta_1)N(\beta_2) \text{ für alle } \beta_1, \beta_2 \in \mathbb{Q}(\sqrt{d}).$$

Im Falle  $d < 0$  und  $\alpha = 0$  ergibt (5.22)  $N(x + yf\rho) = x^2 + f^2|d|y^2 = 1$ , da  $e = -1$  für  $d < 0$  nicht möglich ist. Für  $f^2d = -1$  wird  $x^2 + y^2 = 1$  nur durch die Ganzzahlpaare  $(\pm 1, 0)$  und  $(0, \pm 1)$  erfüllt. Also ist  $R_{-1,1}^* = \{1, -1, i, -i\}$ . Für  $f^2d < -1$  und  $y \neq 0$  gilt  $N(\eta) > 1$ . Die einzigen Einheiten sind dann 1 und  $-1$ .

Ist  $d < 0$  und  $\alpha = 1$ , so schreiben wir (5.22) mit  $e = 1$  in der Form  $4N(x + yf\rho) = 4x^2 + 4fxy + f^2(1-d)y^2 = (2x + fy)^2 + f^2|d|y^2 = 4$ . Für  $f^2d = -3$  hat  $(2x + y)^2 + 3y^2 = 4$  genau die sechs Lösungspaare  $(\pm 1, \mp 1)$ ,  $(0, \pm 1)$  und  $(\pm 1, 0)$ , die die Einheiten  $\left(\frac{1}{2} + \frac{1}{2}\sqrt{-3}\right)^k$  für  $k \in \mathcal{A}_6$  ergeben. Da kein weiteres  $d \in \mathcal{S}$  mit  $-7 < d < 0$  und  $d \equiv 1 \pmod{4}$  existiert und da für  $f^2d \leq -7$  aus  $y \neq 0$  die Ungleichung  $(2x + fy)^2 + f^2|d|y^2 \geq 7$  folgen würde, bleiben hier nur die beiden trivialen Einheiten  $\eta = \pm 1$ .

In reell-quadratischen Zahlkörpern ist die Situation ganz anders. Zum Beispiel stellt  $\varepsilon_1 := 1 + \sqrt{2}$  eine Einheit aus  $R_{2,1}^*$  dar. Da die Einheiten von  $R_{2,1}^*$  eine Gruppe bilden und da  $\varepsilon_1 > 1$  ist, besteht die streng monoton wachsende Folge  $(\varepsilon_1^n)_{n \in \mathbb{N}}$  aus unendlich vielen verschiedenen Einheiten von  $R_{2,1}^*$ . Außerdem gilt hier  $N(\varepsilon_1) = -1$ . Mit (5.23) folgt daraus  $N(\varepsilon_1^{2k}) = 1$  und  $N(\varepsilon_1^{2k+1}) = -1$  für jedes  $k \in \mathbb{N}_1$ . Insbesondere ergeben die Paare  $(x_k, y_k)$  mit  $x_k + y_k\sqrt{2} := \varepsilon_1^{2k} = (3 + 2\sqrt{2})^k$  unendlich viele Lösungen der auf Seite 27 erwähnten *Fermat-Pell-Gleichungen*  $x^2 - my^2 = 1$  für  $m = 2$ .

Tatsächlich führt jede Lösung  $(x, y) \in \mathbb{Z}^2$  einer Gleichung  $x^2 - my^2 = 1$  zu einer Einheit einer Ordnung  $R_{d,f}$ . Sind  $\nu_p(m)$  die Exponenten der *formalen Darstellung* von  $m$  (Seite 52), so erhalten wir mit  $\alpha_p(m) := \left\lfloor \frac{\nu_p(m)}{2} \right\rfloor$  und  $\beta_p(m) := \text{mod}$

$(\nu_p(m), 2)$  die eindeutig bestimmten Faktoren  $f := \prod_{p \in \mathbb{P}} p^{\alpha_p(m)}$  und  $d := \prod_{p \in \mathbb{P}} p^{\beta_p(m)}$ , für die  $d \in \mathcal{S} \cap \mathbb{N}$ ,  $f \in \mathbb{N}_1$  und  $m = f^2 d$  gilt. Aus  $x^2 - f^2 d y^2 = 1$  und der Normgleichung (5.19) folgt dann

$$(5.24) \quad (x - \alpha f y) + f y \rho \in R_{d,f}^*.$$

Da wir im nächsten Satz zu jeder Ordnung  $R_{d,f}$  alle Einheiten angeben werden, sind damit auch alle Lösungen der *Fermat-Pell-Gleichungen* bestimmt.

Die Hauptschwierigkeit bei der Herleitung der noch fehlenden Einheitendarstellungen besteht in dem Nachweis dafür, dass  $R_{d,f}^* \setminus \{-1, 1\} \neq \emptyset$  für alle  $d \in \mathcal{S} \cap \mathbb{N}$  und  $f \in \mathbb{N}_1$  gilt. Ist  $\eta \in R_{d,f}^* \setminus \{-1, 1\}$ , so stellen  $\eta_1 := \eta$ ,  $\eta_2 := \frac{1}{\eta}$ ,  $\eta_3 := -\eta$  und  $\eta_4 := -\frac{1}{\eta}$  vier verschiedene Einheiten dar, weil die Komponentenpaare  $(x_i, y_i)$  von  $\eta_i := x_i + y_i \sqrt{d}$ ,  $i \in \mathcal{I}_4$ , in je einem der vier Quadranten liegen. Da diese Einheiten außerdem dieselbe Norm  $e$  haben und  $\text{sign}(x_i(1+e) + y_i(1-e)) \eta_i^{\text{sign}(x_i y_i)} > 1$  für jedes  $i \in \mathcal{I}_4$  gilt, ist genau diejenige Einheit  $\eta_i$  größer als 1, deren Komponenten beide positiv sind.

Für den Größenvergleich der Elemente von  $\mathbb{Q}(\sqrt{d})$  mit  $d \in \mathcal{S} \cap \mathbb{N}$  wird die Anordnung von  $\mathbb{R}$  nicht benötigt, weil  $x + y \sqrt{d} > 0$  mit  $x, y \in \mathbb{Q}$  genau dann gilt, wenn  $x \geq 0$ ,  $y \geq 0$  und  $(x, y) \neq (0, 0)$  oder wenn  $(\text{sign } x)(\text{sign } y) = -1$  und  $(\text{sign } x)(x^2 - d y^2) > 0$  erfüllt ist. Im Vorgriff darauf, dass wir  $\{\eta \in R_{d,f}^* ; \eta > 1\} \neq \emptyset$  für jedes  $d \in \mathcal{S} \cap \mathbb{N}$  und alle  $f \in \mathbb{N}_1$  beweisen werden, definieren wir unter Anwendung des *Minimumsatzes* (Seite 11) die *Grundeinheiten*

$$(5.25) \quad \varepsilon_{d,f} := \min \{ \eta \in R_{d,f}^* ; \eta > 1 \},$$

mit deren Hilfe sich alle Einheiten von  $R_{d,f}$  darstellen lassen.

### Einheitensatz

Für  $d \in \mathcal{S}$  und  $f \in \mathbb{N}_1$  gilt

$$R_{d,f}^* = \begin{cases} \left\{ \left( \frac{1}{2} + \frac{1}{2} \sqrt{3} i \right)^k ; k \in \mathcal{A}_6 \right\}, & \text{wenn } D_f = -3, \\ \{ i^k ; k \in \mathcal{A}_4 \}, & \text{wenn } D_f = -4, \\ \{-1, 1\}, & \text{wenn } D_f \in \mathcal{D} \text{ mit } D_f < -4, \\ \{ e \varepsilon_{d,f}^k ; e \in \{-1, 1\} \text{ und } k \in \mathbb{Z} \}, & \text{wenn } D_f \in \mathcal{D} \cap \mathbb{N}, \end{cases}$$

wobei  $\varepsilon_{d,f}$  die in (5.25) definierte Grundeinheit ist.

**Beweis** (des vierten Falles, 1. Teil: Induktion, 2. Teil: Induktion und Widerspruch, 3. Teil: Widerspruch, h2):

### i) Kettenbruchentwicklung von $\sqrt{m}$

Da die ersten drei Teile des Satzes vorweg behandelt wurden, fehlen nur noch die Ordnungen in reell-quadratischen Zahlkörpern. Um geeignete Lösungen der entsprechenden *Fermat-Pell-Gleichungen* zu finden, entwickeln wir  $\alpha_1 := \sqrt{m}$  für  $m := f^2d$  in einen Kettenbruch (siehe Seite 23), wobei wir weitgehend LAGRANGE (1767) folgen. Mit  $q_1 := [\alpha_1]$  ist  $\alpha_2 := \frac{1}{\alpha_1 - q_1} = \frac{1}{\sqrt{m} - q_1}$ , und  $\sqrt{m} - 1 < q_1 < \sqrt{m}$  ergibt  $\alpha_2 > 1$ . Wegen  $\varsigma(\alpha_2) = -\frac{1}{\sqrt{m} + q_1}$  gilt außerdem  $-1 < \varsigma(\alpha_2) < 0$ , und schließlich hat  $\alpha_2$  die Form  $\alpha_2 = \frac{\sqrt{m} + b_2}{a_2}$  mit

$$(5.26) \quad b_2 := q_1 \in \mathbb{N}_1 \text{ und } a_2 := m - q_1^2 \in \mathbb{N}_1.$$

Die *Erkundungsstrategie* mit einigen konkreten Werten für  $m$  lässt uns vermuten, dass die entsprechenden drei Eigenschaften

$$(5.27) \quad \alpha_n > 1, \quad -1 < \varsigma(\alpha_n) < 0 \text{ und } \alpha_n = \frac{\sqrt{m} + b_n}{a_n} \text{ mit } a_n, b_n \in \mathbb{N}_1$$

für alle vollständigen Quotienten  $\alpha_n$  mit  $n \in \mathbb{N}_2$  vorliegen. Der Fall  $n = 2$  und die aus (5.26) folgende Gleichung  $a_2 = m - b_2^2$  sind dann der Induktionsanfang für die vollständige Induktion mit der Induktionsmenge

$$\mathcal{M} := \left\{ k \in \mathbb{N}_2; \alpha_k \text{ erfüllt (5.27), und es gilt } a_k \mid (m - b_k^2) \right\}.$$

Es sei  $n \in \mathcal{M}$ . Mit  $q_n := [\alpha_n] \in \mathbb{N}_1$  gilt wie oben  $\alpha_{n+1} = \frac{1}{\alpha_n - q_n} > 1$ , und  $\frac{1}{\varsigma(\alpha_{n+1})} = \varsigma(\alpha_n) - q_n < -1$  liefert  $-1 < \varsigma(\alpha_{n+1}) < 0$ .

Aus  $\alpha_n = \frac{\sqrt{m} + b_n}{a_n}$  folgt

$$\begin{aligned} \alpha_{n+1} &= \frac{a_n}{\sqrt{m} + b_n - a_n q_n} \\ &= \frac{\sqrt{m} + (a_n q_n - b_n)}{(m - (a_n q_n - b_n)^2) a_n^{-1}}. \end{aligned}$$

Wegen  $a_n \mid (m - b_n^2)$  gilt  $m - (a_n q_n - b_n)^2 = m - a_n^2 q_n^2 + 2a_n b_n q_n - b_n^2 \equiv 0 \pmod{a_n}$ .

Definieren wir also

$$(5.28) \quad b_{n+1} := a_n q_n - b_n \text{ und } a_{n+1} := \frac{m - b_{n+1}^2}{a_n},$$

so ergibt sich zunächst  $b_{n+1} \in \mathbb{Z}$  und  $a_{n+1} \in \mathbb{Z} \setminus \{0\}$ . Mit den ersten beiden Aussagen von (5.27) erhalten wir

$$(5.29) \quad 1 < \alpha_{n+1} - \varsigma(\alpha_{n+1}) = \frac{2\sqrt{m}}{a_{n+1}} \text{ und } 0 < \alpha_{n+1} + \varsigma(\alpha_{n+1}) = \frac{2b_{n+1}}{a_{n+1}}.$$

Daraus folgt  $a_{n+1} > 0$ ,  $b_{n+1} > 0$  und damit  $a_{n+1}, b_{n+1} \in \mathbb{N}_1$ . Wegen der zweiten Aussage von (5.28) ist außerdem  $\frac{m-b_{n+1}^2}{a_{n+1}} = a_n \in \mathbb{N}_1$ . Zusammenfassend gilt also  $n + 1 \in \mathcal{M}$ , und der *Induktionssatz* (Seite 12) ergibt  $\mathcal{M} = \mathbb{N}_2$ . Insbesondere bilden die vollständigen Quotienten  $\alpha_n$  eine (nicht abbrechende) Folge.

### ii) Periodizität der Kettenbruchentwicklung

Der erste Teil von (5.29) ergibt  $a_n < 2\sqrt{m}$ , und wegen  $\varsigma(\alpha_n) < 0$  ist  $b_n < \sqrt{m}$  für jedes  $n \in \mathbb{N}_2$ . Alle Paare  $(a_n, b_n)$  liegen also in  $\mathcal{I}_t^2$  mit  $t := [2\sqrt{m}]$ , sodass es höchstens  $t^2$  solcher Paare gibt. Aufgrund des *Rationalitätskriteriums für  $\sqrt{m}$*  (Seite 37) sind die vollständigen Quotienten  $\alpha_n$  eindeutig durch die Paare  $(a_n, b_n)$  festgelegt. Der *Schubfachsatz* (Seite 85) sichert damit die Existenz von zwei Zahlen  $\kappa, \lambda \in \mathbb{N}_1$ , sodass  $\alpha_\kappa = \alpha_{\kappa+\lambda}$  gilt. Da  $\alpha_{n+1}$  für jedes  $n \in \mathbb{N}_1$  nur von  $\alpha_n$  abhängt, ergibt vollständige Induktion

$$\alpha_n = \alpha_{n+\lambda} \text{ für alle } n \in \mathbb{N}_\kappa.$$

Aufgrund des *Minimumsatzes* (Seite 11) kann also

$$k := \min \{ \kappa \in \mathbb{N}_2 ; \alpha_n = \alpha_{n+\lambda} \text{ für alle } n \in \mathbb{N}_\kappa \}$$

definiert werden. Wir nehmen an, dass  $k > 2$  ist und zeigen, dass sich dann ein Widerspruch ergibt.

Aus  $\alpha_{k-1} = q_{k-1} + \frac{1}{\alpha_k}$  folgt

$$\begin{aligned} \varsigma(\alpha_{k-1}) &= q_{k-1} + \frac{1}{\varsigma(\alpha_k)} = q_{k-1} + \frac{1}{\varsigma(\alpha_{k+\lambda})} \\ &= q_{k-1} - q_{k-1+\lambda} + \varsigma(\alpha_{k-1+\lambda}). \end{aligned}$$

Also gilt einerseits

$$\varsigma(\alpha_{k-1}) - \varsigma(\alpha_{k-1+\lambda}) = q_{k-1} - q_{k-1+\lambda} \in \mathbb{Z},$$

und andererseits ergibt die zweite Aussage von (5.27)

$$-1 < \varsigma(\alpha_{k-1}) - \varsigma(\alpha_{k-1+\lambda}) < 1.$$

Damit muss  $\varsigma(\alpha_{k-1}) = \varsigma(\alpha_{k-1+\lambda})$  sein, woraus unmittelbar  $\alpha_{k-1} = \alpha_{k-1+\lambda}$  folgt. Also erhalten wir nur dann keinen Widerspruch zur Minimalität von  $k$ , wenn  $k = 2$  gilt.

Vollständige Induktion ergibt nun

$$(5.30) \quad a_{2+v\lambda} = a_2 \text{ und } b_{2+v\lambda} = b_2 \text{ für alle } v \in \mathbb{N}_1.$$

### iii) Lösungen der *Fermat-Pell-Gleichungen* und Darstellung aller Einheiten

Mit (5.26), (5.30) und mit der zweiten Aussage von (5.28) erhalten wir

$$(5.31) \quad 1 = \frac{m - b_2^2}{a_2} = \frac{m - b_{2+v\lambda}^2}{a_{2+v\lambda}} = a_{1+v\lambda} \text{ für jedes } v \in \mathbb{N}_1.$$

Indem in (2.7)  $\alpha_1 = \sqrt{m}$  und  $\alpha_s = \frac{\sqrt{m} + b_s}{a_s}$  gesetzt wird, folgt

$$\sqrt{m} = \frac{P_{s-1}(\sqrt{m} + b_s) + P_{s-2} a_s}{Q_{s-1}(\sqrt{m} + b_s) + Q_{s-2} a_s}.$$

Multiplikation mit dem Nenner und Zusammenfassung der rationalen Teile liefert

$$(Q_{s-1} b_s + Q_{s-2} a_s - P_{s-1})\sqrt{m} = (P_{s-1} b_s + P_{s-2} a_s - m Q_{s-1}).$$

Aufgrund des *Rationalitätskriteriums* für  $\sqrt{m}$  (Seite 37) muss

$$Q_{s-1} b_s + Q_{s-2} a_s = P_{s-1} \text{ und } P_{s-1} b_s + P_{s-2} a_s = m Q_{s-1}$$

gelten. Subtrahiert man das  $Q_{s-1}$ -Fache der zweiten Gleichung von dem  $P_{s-1}$ -Fachen der ersten, so erhält man

$$(P_{s-1} Q_{s-2} - P_{s-2} Q_{s-1}) a_s = P_{s-1}^2 - m Q_{s-1}^2,$$

und mit (2.9) folgt

$$P_{s-1}^2 - m Q_{s-1}^2 = (-1)^{s-1} a_s.$$

Wird  $s = 1 + v\lambda$  gewählt, so ergibt (5.31)

$$(5.32) \quad P_{v\lambda}^2 - m Q_{v\lambda}^2 = (-1)^{v\lambda} \text{ für jedes } v \in \mathbb{N}_1.$$

Mindestens für jedes gerade  $v$  erhalten wir also eine Lösung  $(P_{v\lambda}, Q_{v\lambda}) \in \mathbb{N}_1^2$  der *Fermat-Pell-Gleichung*  $x^2 - my^2 = 1$ . Wegen (5.24) haben wir damit sogar unendlich viele  $\eta \in R_{d,f}^*$  mit  $\eta > 1$  und können  $\varepsilon_{d,f}$  durch (5.25) definieren.

Da  $(R_{d,f}^*, \cdot, 1, /)$  eine abelsche Gruppe darstellt (siehe Seite 167), sind mit  $1, -1$  und  $\varepsilon_{d,f}$  auch  $\varepsilon_{d,f}^k$  und  $-\varepsilon_{d,f}^k$  für alle  $k \in \mathbb{Z}$  Elemente von  $R_{d,f}^*$ .

Wir nehmen an, dass es ein  $\vartheta$  in  $\tilde{R}_{d,f}^* := R_{d,f}^* \setminus \{e \varepsilon_{d,f}^k; e \in \{-1, 1\} \text{ und } k \in \mathbb{Z}\}$  gibt. Mit  $\vartheta$  liegen auch  $\frac{1}{\vartheta}$ ,  $-\vartheta$  und  $-\frac{1}{\vartheta}$  in  $\tilde{R}_{d,f}^*$ . Deshalb genügt es, den Fall  $\vartheta > 1$  zu einem Widerspruch zu führen. Da die Folge  $(\varepsilon_{d,f}^n)_{n \in \mathbb{N}}$  streng monoton

wachsend und unbeschränkt ist, existiert ein  $h \in \mathbb{N}$ , sodass  $\varepsilon_{d,f}^h < \vartheta < \varepsilon_{d,f}^{h+1}$  gilt, woraus

$$(5.33) \quad 1 < \vartheta \varepsilon_{d,f}^{-h} < \varepsilon_{d,f}$$

folgt. Wegen der Gruppeneigenschaft von  $R_{d,f}^*$  stellt  $\vartheta \varepsilon_{d,f}^{-h}$  ein Element aus  $R_{d,f}^*$  dar, dessen Größenbeziehungen aus (5.33) aber einen Widerspruch zur Minimalität von  $\varepsilon_{d,f}$  ergeben. Also muss  $\tilde{R}_{d,f}^* = \emptyset$  gelten. □

Da auch die kleinste mit der Kettenbruchentwicklung von  $\sqrt{m}$  gewonnene Einheit eine Potenz von  $\varepsilon_{d,f} =: x_1 + y_1\sqrt{m}$  ist, sind ihre Komponenten obere Schranken von  $x_1$  beziehungsweise  $y_1$ . Verwendet man die ganzzahlige Darstellung von (5.24), so benötigt man also nur endlich viele Versuche, um  $\varepsilon_{d,f}$  als Lösung von (5.22) zu finden. Effiziente Algorithmen zur Bestimmung der Grundeinheit werden in [2] (Seite 269 f.) hergeleitet.

## Produkt Darstellungen und Ideale

Jede Einheit aus  $R_{d,f}^*$  ist Teiler aller Elemente von  $R_{d,f}$ . Bei dem Versuch, die Elemente von  $\widehat{R}_{d,f} := R_{d,f} \setminus (R_{d,f}^* \cup \{0\})$  so weit wie möglich zu zerlegen, sind also die Einheiten als Faktoren auszunehmen. Die “unzerlegbaren Zahlen” werden deshalb durch die folgende Definition erfasst, die auch den Begriff für die “Zusammengehörigkeit” solcher Elemente enthält.

### Definition der irreduziblen und der assoziierten Elemente

Ein Element  $\beta \in \widehat{R}_{d,f}$  heißt *irreduzibel*, wenn  $\beta \neq \gamma \zeta$  für alle  $\gamma, \zeta \in \widehat{R}_{d,f}$  gilt.

Zwei Elemente  $\beta, \vartheta \in \widehat{R}_{d,f}$  heißen *assoziiert*, wenn es ein  $\varepsilon \in R_{d,f}^*$  mit  $\beta = \varepsilon \vartheta$  gibt.

Vollständige Induktion mit der Induktionsmenge  $\mathcal{M} := \{k \in \mathbb{N}_1; \text{ Jedes } \beta \in R_{d,f} \setminus \{0\} \text{ mit } \Omega(|N(\beta)|) \in \mathcal{I}_k \text{ ist Produkt von irreduziblen Elementen}\}$  unter Verwendung von (5.23) ergibt, dass jedes  $\beta \in \widehat{R}_{d,f}$  als Produkt von endlich vielen irreduziblen Elementen geschrieben werden kann.

Ein Beispiel zeigt, dass es Maximalordnungen gibt, in denen die Zerlegung in irreduzible Elemente nicht eindeutig ist: In  $R_{-5,1}$  gilt  $9 = 3 \cdot 3 = (2 + i\sqrt{5})(2 - i\sqrt{5})$ . Mit Hilfe der Normabbildung weist man nach, dass 3,  $2 + \sqrt{5}$  und  $2 - \sqrt{5}$  paarweise nicht assoziierte, irreduzible Elemente von  $R_{-5,1}$  darstellen. Deshalb sind die beiden Zerlegungen von 9 “wesentlich verschieden”.

Hier braucht nicht erklärt zu werden, wann man von einer *Maximalordnung mit eindeutiger Faktorzerlegung* spricht, weil nur ein sehr kleiner Teil aller Maximalordnungen diese Eigenschaft hat. Deshalb war es ein "Meilenstein" der Zahlentheorie, als KUMMER um 1850 einen Weg zur Herstellung einer eindeutigen Zerlegung fand, indem er zunächst bemerkte, dass nicht assoziierte irreduzible Zahlen einer Maximalordnung  $R_{d,1}$  einen größten gemeinsamen Teiler haben können, der nicht zu  $\mathbb{Q}(\sqrt{d})$  gehört. Er nannte diese Teiler "ideale Zahlen" und konnte 1856 zeigen, dass sich mit ihrer Hilfe alle Elemente von  $\widehat{R}_{d,1}$  und allgemeiner alle entsprechenden Elemente aus *algebraischen Zahlkörpern*<sup>6</sup> eindeutig zerlegen lassen.

DEDEKIND gelang es 1871, eine dazu äquivalente Erweiterung mit Hilfe derjenigen Teilmengen von  $R_{d,1}$  zu konstruieren, die aus allen durch eine gegebenen ideale Zahl teilbaren Elementen bestehen. Diese Strukturen, die - wie in der folgenden Definition - unabhängig von idealen Zahlen eingeführt werden können, benötigen wir auch für die Herstellung des Zusammenhangs mit quadratischen Formen.

### Definition des Ideals, des Hauptideals und des Primideals

Ist  $(R, +, \cdot, 0, 1, -)$  ein Ring und  $\mathfrak{a}$  eine nicht leere Teilmenge von  $R$ , so heißt  $\mathfrak{a}$  *Ideal von  $R$* , wenn gilt:

- a)  $a + b \in \mathfrak{a}$  und  $-c \in \mathfrak{a}$  für alle  $a, b, c \in \mathfrak{a}$ ,
- b)  $ra \in \mathfrak{a}$  für alle  $r \in R$  und jedes  $a \in \mathfrak{a}$ .

Ein Ideal  $\mathfrak{a}$  heißt *Hauptideal von  $R$* , wenn es ein  $a \in R$  gibt, sodass  $\mathfrak{a} = \{ar ; r \in R\}$  gilt. Man schreibt dann  $(a)$  anstelle von  $\mathfrak{a}$  und entnimmt den zugehörigen Ring aus dem Kontext.

Ein Ideal  $\mathfrak{p}$  heißt *Primideal von  $R$* , wenn  $\mathfrak{p} \neq R$  ist und wenn  $ab \notin \mathfrak{p}$  für alle  $a, b \in R \setminus \mathfrak{p}$  gilt.

Jeder Ring  $R$  enthält die "trivialen" Ideale  $(0)$  und  $(1) = R$ . Sind  $\mathfrak{a}, \mathfrak{b}$  Ideale von  $R$ , so lässt sich durch

$$\mathfrak{a} \mathfrak{b} := \left\{ x \in R ; \text{Es gibt } n \in \mathbb{N}_1, a_i \in \mathfrak{a}, b_i \in \mathfrak{b}, i = 1, \dots, n, \text{ mit } x = \sum_{i=1}^n a_i b_i \right\}$$

eine *Multiplikation von Idealen* definieren, die wieder ein Ideal ergibt und bei der

<sup>6</sup> Ein  $\mathbb{Q}$  enthaltender Körper  $K$  heißt *algebraischer Zahlkörper*, wenn jedes Element von  $K$  Nullstelle eines nicht identisch verschwindenden Polynoms mit rationalen Koeffizienten ist und wenn  $K$  als Vektorraum über  $\mathbb{Q}$  eine endliche Dimension hat.

(1) das "neutrale Ideal" darstellt. Nennt man ein Ideal  $\mathfrak{c} \neq (0)$  *Teiler des Ideals*  $\mathfrak{a}$ , wenn es ein Ideal  $\mathfrak{b}$  mit  $\mathfrak{a} = \mathfrak{b} \mathfrak{c}$  gibt, so ist ein Ideal  $\mathfrak{p} \neq (1)$  genau dann ein Primideal, wenn  $\mathfrak{p}$  nur die Ideale (1) und  $\mathfrak{p}$  als Teiler hat.

Für die Ringe der ganz-algebraischen Elemente in beliebigen algebraischen Zahlkörpern konnte DEDEKIND 1894 beweisen, dass sich jedes von (1) verschiedene Ideal eindeutig als Produkt von Primidealen darstellen lässt.

Um diese Zerlegung für  $R_{d,1}$  nutzen zu können, wird jedem Element  $a$  von  $R_{d,1}$  das Hauptideal  $(a)$  zugeordnet, wobei zwei Hauptideale  $(b)$  und  $(c)$  genau dann übereinstimmen, wenn  $b$  und  $c$  assoziiert sind.

Ist  $R_{d,f}$  eine beliebige Ordnung von  $\mathbb{Q}(\sqrt{d})$ , so lässt sich jedes Ideal von  $R_{d,f}$  in der Form

$$(5.34) \quad \mathfrak{a} = \left\{ a', \frac{\gamma}{2} (b + \sqrt{D_f}) \right\}_{\mathbb{Z}} \quad \text{mit } a' := \min(\mathfrak{a} \cap \mathbb{N}_1), b \in \mathbb{Z}, \\ b^2 \equiv D_f \pmod{4a'}, \gamma \in \mathbb{N}_1 \text{ und } \gamma \mid a'$$

schreiben. Für Primzahlen  $p \in \mathbb{P} \subset R_{d,1}$  kann dann mit Hilfe des Legendre-Symbols die Zerlegung von  $(p)$  als Produkt von Primidealen explizit angegeben werden.

**Theorem über Darstellungen als Primidealprodukt**

Es sei  $D$  die Diskriminante von  $\mathbb{Q}(\sqrt{d})$  und  $p \in \mathbb{P}$ .

a) Ist  $p \mid D$ , so gilt  $(p) = \mathfrak{p}^2$  mit  $\mathfrak{p} := \{p, 1 + \rho\}_{\mathbb{Z}}$  für  $p = 2, D \equiv 12 \pmod{16}$ , und  $\mathfrak{p} := \{p, \rho\}_{\mathbb{Z}}$  sonst.

b) Im Falle  $\left(\frac{D}{p}\right) = -1$  stellt  $(p)$  ein Primideal dar.

c) Für  $\left(\frac{D}{p}\right) = 1$  ergibt sich  $(p) = \mathfrak{p}_1 \mathfrak{p}_2$  mit  $\mathfrak{p}_1 := \left\{ p, \frac{b + \sqrt{D}}{2} \right\}_{\mathbb{Z}}$  und  $\mathfrak{p}_2 := \left\{ p, \frac{-b + \sqrt{D}}{2} \right\}_{\mathbb{Z}} \neq \mathfrak{p}_1$ , wobei  $b$  eine Lösung der Kongruenz  $b^2 \equiv D \pmod{4p}$  ist.

**Die Idealklassengruppe**

Ist  $A$  eine nicht leere Teilmenge von  $\mathbb{Q}(\sqrt{d})$  und  $c \in \mathbb{Q}(\sqrt{d}) \setminus \{0\}$ , so sei im Folgenden

$$cA := \left\{ x \in \mathbb{Q}(\sqrt{d}) ; \text{Es gibt ein } y \in A \text{ mit } x = cy \right\} \text{ und}$$

$$\varsigma(A) := \left\{ x \in \mathbb{Q}(\sqrt{d}) ; \text{Es gibt ein } y \in A \text{ mit } x = \varsigma(y) \right\}.$$

Die Ideale von  $R_{d,f}$  bilden bezüglich der Multiplikation von Idealen im Allgemeinen keine Gruppe, weil nicht zu jedem von (0) verschiedenen Ideal ein Inverses existiert. Dieses Defizit im Hinblick auf unser Ziel, eine Verbindung zu den Klassengruppen herzustellen, wird in der nächsten Definition mit einer Begriffserweiterung und einer Einschränkung behoben.

### Definition des gebrochenen Ideals und des invertierbaren Ideals

Eine nicht leere Teilmenge  $\mathfrak{c}$  von  $\mathbb{Q}(\sqrt{d})$ , die die Eigenschaften a) und b) der Ideale von  $R_{d,f}$  hat, heißt *gebrochenes Ideal* von  $R_{d,f}$ , wenn es ein  $n \in \mathbb{N}_1$  gibt, sodass  $n\mathfrak{c}$  ein Ideal von  $R_{d,f}$  ist. Zur Unterscheidung werden die ursprünglichen Ideale auch *ganze Ideale* genannt.

Ein gebrochenes Ideal  $\mathfrak{a}$  von  $R_{d,f}$  heißt *invertierbar*, wenn es ein gebrochenes Ideal  $\mathfrak{b}$  von  $R_{d,f}$  gibt, sodass  $\mathfrak{a}\mathfrak{b} = R_{d,f}$  gilt, wobei das Produkt von gebrochenen Ideale wie bei ganzen Idealen definiert wird. Solch ein Ideal  $\mathfrak{b}$ , das eindeutig bestimmt ist, wird *Inverses von  $\mathfrak{a}$*  genannt.

Das Produkt von gebrochenen Idealen ist kommutativ und assoziativ. Außerdem stellt das Produkt von invertierbaren Idealen wegen der Kommutativität ein invertierbares Ideal dar. Damit ist die Menge der von (0) verschiedenen invertierbaren Ideale mit der Multiplikation von gebrochenen Idealen und mit  $(1) = R_{d,f}$  als neutralem Element eine abelsche Gruppe.

Für die Angabe eines *Invertierbarkeitskriteriums*, das auch zu einer expliziten Form des Inversen führt, und für die entscheidende Abbildung von Idealen auf quadratische Formen benötigt man die *Norm  $N(\mathfrak{a})$  von Idealen  $\mathfrak{a}$* . Von den verschiedenen Einführungsmöglichkeiten wählen wir diejenige, die auf der expliziten Form (5.34) der Ideale beruht. Wird  $\gamma$  ausgeklammert und durch einen Faktor  $n$  aus der Definition des gebrochenen Ideals dividiert, so ergibt sich eine Darstellung

$$(5.35) \quad \mathfrak{a} = \beta \left\{ a, \frac{b + \sqrt{D_f}}{2} \right\}_{\mathbb{Z}} \quad \text{mit } a := \frac{a'}{\gamma} \in \mathbb{N}_1 \text{ und } \beta := \frac{\gamma}{n} \in \mathbb{Q}^+.$$

Als Betrag der Determinante der "Übergangsmatrix"  $\begin{pmatrix} \beta a & 0 \\ \frac{1}{2}\beta(b - \alpha f) & \beta \end{pmatrix}$  von  $(1, f\rho)$  zu  $(\beta a, \beta \frac{b + \sqrt{D_f}}{2})$  kann dann

$$(5.36) \quad N(\mathfrak{a}) := \beta^2 a$$

gesetzt werden. Da für alle gebrochenen Ideale  $\mathfrak{a}$  von  $R_{d,f}$  auch  $\varsigma(\mathfrak{a})$  ein gebrochenes Ideal ist und da  $\mathfrak{a} \varsigma(\mathfrak{a}) = (N(\mathfrak{a}))$  genau für die invertierbaren Ideale  $\mathfrak{a}$  von  $R_{d,f}$  gilt, stellt  $\frac{1}{N(\mathfrak{a})} \varsigma(\mathfrak{a})$  das Inverse zu  $\mathfrak{a} \neq (0)$  dar. Insbesondere folgt, dass alle von  $(0)$  verschiedenen gebrochenen Ideale von  $R_{d,1}$  invertierbar sind. Mit der Darstellung (5.35) lässt sich außerdem zeigen, dass  $\mathfrak{a} = \beta \left\{ a, \frac{b + \sqrt{D_f}}{2} \right\}_{\mathbb{Z}}$  genau dann invertierbar ist, wenn  $\text{ggT}(a, b, c) = 1$  gilt, wobei  $c := \frac{1}{4a} (b^2 - D_f) \in \mathbb{Z}$  gesetzt wird.

Wesentlich einfacher als die Äquivalenz von quadratischen Formen lässt sich die Äquivalenz von Idealen beschreiben.

### Definition der Äquivalenz von Idealen

Zwei von  $(0)$  verschiedene gebrochene Ideale  $\mathfrak{a}, \mathfrak{b}$  von  $R_{d,f}$  heißen *äquivalent*, wenn es ein  $\alpha \in \mathbb{Q}(\sqrt{d}) \setminus \{0\}$  mit  $\mathfrak{a} = \alpha \mathfrak{b}$  gibt.

Die beiden Ideale werden *äquivalent im engeren Sinne* genannt, wenn ein  $\alpha \in \mathbb{Q}(\sqrt{d})$  mit  $N(\alpha) > 0$  existiert, sodass  $\mathfrak{a} = \alpha \mathfrak{b}$  gilt.

Im Falle  $D_f < 0$  fallen beide Begriffe stets zusammen, weil aus (5.19) folgt, dass  $N(\alpha)$  für jedes  $\alpha \in \mathbb{Q}(\sqrt{d}) \setminus \{0\}$  positiv ist. Für  $D_f > 0$  ist die Äquivalenz zweier Ideale genau dann mit der Äquivalenz im engeren Sinne gleichbedeutend, wenn  $N(\varepsilon_{d,f}) = -1$  gilt, weil sich dann  $N(\alpha \varepsilon_{d,f}) > 0$  für jedes  $\alpha$  mit  $N(\alpha) < 0$  ergibt, während die Ideale bei der Multiplikation mit  $\varepsilon_{d,f}$  ungeändert bleiben.

Beide Äquivalenzbegriffe erfüllen die drei unter anderem im Beweis des *Satzes über Formenäquivalenz* (Seite 153) auftretenden Bedingungen für eine Äquivalenzrelation. Eine Äquivalenzklasse heißt nun *Idealklasse* beziehungsweise *Idealklasse im engeren Sinne*. Die Multiplikation von invertierbaren Idealen, die zu zwei invertierbaren Idealen  $\mathfrak{a}$  beziehungsweise  $\mathfrak{b}$  (im engeren Sinne) äquivalent sind, ergibt ein invertierbares Ideal aus der Äquivalenzklasse (im engeren Sinne) von  $\mathfrak{a}\mathfrak{b}$ . Die Menge der Idealklassen (im engeren Sinne) zusammen mit der durch Multiplikation beliebiger Repräsentanten der Klassen erklärten Verknüpfung stellt eine abelsche Gruppe dar, deren neutrales Element die aus allen invertierbaren Hauptidealen von  $R_{d,f}$  bestehende Idealklasse ist. Diese Gruppe heißt *Idealklassengruppe (im engeren Sinne) der Ordnung  $R_{d,f}$* .

In jeder Idealklasse liegt wegen (5.35) genau ein ganzes Ideal, bei dem in der Darstellung (5.34)  $\gamma = 1$  ist, das also die Form  $\mathfrak{a} = \left\{ a, \frac{1}{2}(b + \sqrt{D_f}) \right\}_{\mathbb{Z}}$  mit  $a \in \mathbb{N}_1$ ,  $b \in \mathbb{Z}$  und  $b^2 \equiv D_f \pmod{4a}$  hat. Einem solchen Ideal lässt sich direkt die quadratische Form  $(a, b, c)$  mit  $c := \frac{1}{4a}(b^2 - D_f) \in \mathbb{Z}$  zuordnen. Aufgrund des zweiten der obigen *Invertierbarkeitskriterien* (Seite 177) gilt  $\text{ggT}(a, b, c) = 1$ , sodass  $(a, b, c)$  eine primitive quadratische Form darstellt.

Um zeigen zu können, dass bei dieser Zuordnung von Repräsentanten auch die zugehörigen Klassen aufeinander abgebildet werden, geht man von einer etwas allgemeineren Darstellung der gebrochenen Ideale aus.

### Definition der $\mathbb{Z}$ -Basis und der zulässigen $\mathbb{Z}$ -Basis eines Ideals

Es sei  $\mathfrak{a}$  ein gebrochenes Ideal. Ein Paar  $(g, h)$  mit  $g, h \in \mathfrak{a}$  und  $gx + hy \neq 0$  für alle  $(x, y) \in \mathbb{Q}^2 \setminus \{(0, 0)\}$  heißt  *$\mathbb{Z}$ -Basis von  $\mathfrak{a}$* , wenn  $\mathfrak{a} = \{g, h\}_{\mathbb{Z}}$  gilt.

Die  $\mathbb{Z}$ -Basis  $(g, h)$  eines Ideals von  $R_{d,f}$  wird als *zulässig* bezeichnet, wenn  $\frac{1}{\sqrt{d}}(h\varsigma(g) - g\varsigma(h)) > 0$  erfüllt ist.

Ist  $(g, h)$  eine zulässige  $\mathbb{Z}$ -Basis von  $\mathfrak{a}$ , so definiert man die quadratische Form durch

$$F_{g,h}(x, y) := \frac{N(gx - hy)}{N(\mathfrak{a})},$$

wobei  $N(\mathfrak{a})$  wie bei der Begründung von (5.36) der Determinantenbetrag derjenigen Matrix ist, die die  $\mathbb{Q}$ -lineare Abbildung von  $(1, f\rho)$  auf  $(g, h)$  beschreibt.

Bei (5.35) mit  $\beta = 1$  ist wegen (5.36)  $N(\mathfrak{a}) = a$ , und mit  $h := \frac{1}{2}(b + \sqrt{D_f})$  folgt

$$F_{a,h}(x, y) = \frac{1}{a}N\left(ax + \frac{1}{2}(b + \sqrt{D_f})y\right) = \frac{1}{a}\left(ax + \frac{1}{2}by\right)^2 - \frac{1}{4a}D_f y^2 = ax^2 + bxy + cy^2.$$

Wegen  $N(\alpha\mathfrak{a}) = |N(\alpha)|N(\mathfrak{a})$  ist  $F_{\alpha g, \alpha h}(x, y) = \frac{N(\alpha)}{|N(\alpha)|}F_{g,h}(x, y)$ . Für  $N(\alpha) > 0$  ergibt sich also  $F_{\alpha g, \alpha h}(x, y) = F_{g,h}(x, y)$ .

Da die Definition von  $F_{g,h}(x, y)$  von der jeweiligen  $\mathbb{Z}$ -Basis  $(g, h)$  von  $\mathfrak{a}$  abhängt, ist für die Wohldefiniertheit der Abbildung zwischen den entsprechenden Äquivalenzklassen noch zu zeigen, dass alle zulässigen  $\mathbb{Z}$ -Basen von  $\mathfrak{a}$  zu äquivalenten Formen führen und dass umgekehrt äquivalente Formen aus entsprechenden zulässigen  $\mathbb{Z}$ -Basen von im engeren Sinne äquivalenten Idealen entstehen. Die einfachen Beweise mit linearer Algebra, die im Wesentlichen in [2] zu finden sind,

können in diesem Ausblick übergangen werden. In dem folgenden Theorem, das die angekündigte Verbindung zwischen quadratischen Formen und neueren Strukturen enthält, bezeichnen Querstriche die jeweiligen Äquivalenzklassen.

### Theorem über die Idealklassengruppe

Für  $D_f \in \mathcal{D}$  sei  $\mathcal{C}(D_f)$  die Idealklassengruppe im engeren Sinne der Ordnung  $R_{d,f}$  mit der Diskriminante  $D_f$ , und  $\mathcal{F}(D_f)$  sei die Klassengruppe der primitiven quadratischen Formen mit der Diskriminante  $D_f$ , wobei für  $D_f < 0$  nur positiv-definite Formen berücksichtigt werden. Ist  $(g, h)$  eine zulässige  $\mathbb{Z}$ -Basis des invertierbaren Ideals  $\mathfrak{a}$  von  $R_{d,f}$ , so sind

$$\mathcal{C}(D_f) \rightarrow \mathcal{F}(D_f), \quad \overline{\{g, h\}_{\mathbb{Z}}} \mapsto \overline{\left( \frac{N(gx - hy)}{N(\mathfrak{a})} \right)} \quad \text{und}$$

$$\mathcal{F}(D_f) \rightarrow \mathcal{C}(D_f), \quad \overline{(a, b, c)} \mapsto \alpha \left\{ a, \frac{1}{2} (b + \sqrt{D_f}) \right\}_{\mathbb{Z}}$$

mit  $\alpha := \begin{cases} \rho, & \text{wenn } d > 0 \text{ und } a < 0, \\ 1, & \text{sonst,} \end{cases}$

wohldefinierte, bijektive, zueinander inverse Abbildungen, die das Produkt von Idealklassen in die Composition der entsprechenden Formenklassen überführen und umgekehrt.

Im Satz über die Klassenanzahl (Seite 155) wurde nachgewiesen, dass  $\mathcal{F}(D_f)$  für jedes  $D_f \in \mathcal{D}$  endlich ist. Wegen der bijektiven Abbildung von  $\mathcal{F}(D_f)$  auf  $\mathcal{C}(D_f)$  gilt  $\text{card } \mathcal{C}(D_f) = \text{card } \mathcal{F}(D_f)$ . Als *Klassenzahl*  $h(D_f)$  von  $R_{d,f}$  wird in Übereinstimmung mit der Definition auf Seite 162 die Anzahl der Idealklassen (im gewöhnlichen Sinne) bezeichnet. Für  $f = 1$  nennt man  $h = h(D)$  die *Klassenzahl des quadratischen Zahlkörpers*  $\mathbb{Q}(\sqrt{d})$ . Sie ist eine wichtige charakteristische Größe der quadratischen Zahlkörper mit einer Reihe von Anwendungen. Zum Beispiel gilt  $h = 1$  genau dann, wenn alle Ideale von  $\mathbb{Q}(\sqrt{d})$  Hauptideale sind, woraus sich ergibt, dass in  $R_{d,1}$  die Zerlegung in irreduzible Elemente eindeutig ist.

GAUß hat umfangreiche Klassenzahltabellen berechnet, die aber erst in seinem Nachlass veröffentlicht wurden. Außerdem leitete er Mittelwertformeln her und erkannte dabei einen wesentlichen Unterschied zwischen den Klassenzahlen für positive und für negative Diskriminanten. Der Grund dafür wurde klar, als DI-

DIRICHLET 1839 als weiteren Höhepunkt in der Geschichte der Zahlentheorie eine analytische Klassenzahlformel für alle algebraischen Zahlkörper bewies. Der Spezialfall für quadratische Zahlkörper bildet den Abschluss dieses Ausblicks, weil damit einerseits die nachhaltige Wirkung der vielen Ideen von GAUß erkennbar wird und weil andererseits die Arbeitsweisen der großen Zahlentheoretiker des neunzehnten Jahrhunderts auch mächtige Problemlösestrategien eröffnet haben.

Für die Darstellung von  $h(D)$  wird eine der auf Seite 72 eingeführten L-Reihen  $L(s, \chi)$  von DIRICHLET benötigt und zwar diejenige, die für  $k = |D|$  zu dem eindeutig bestimmten Charakter  $\chi : \mathbb{N}_1 \rightarrow \{-1, 0, 1\}$  gehört, der die auf Seite 72 genannten Eigenschaften hat und der die Bedingung erfüllt, dass mindestens ein  $n \in \mathbb{N}_1$  mit  $\chi(n) = -1$  existiert.

Während  $\chi(n) = 0$  für alle  $n \in \mathbb{N}_1$  mit  $\text{ggT}(n, D) > 1$  gilt, lassen sich die übrigen Werte durch Jacobi-Symbole ausdrücken:

$$\chi(n) = \begin{cases} \left(\frac{n}{|d|}\right) & \text{für } d \equiv 1 \pmod{4}, \\ (-1)^{\frac{n-1}{2}} \left(\frac{n}{|d|}\right) & \text{für } d \equiv 3 \pmod{4}, \\ (-1)^{\left[\frac{n+1}{4}\right] + \frac{n-1}{2} \frac{u-1}{2}} \left(\frac{n}{|u|}\right) & \text{für } d = 2u \text{ mit } u \in \mathbb{Z} \text{ und } 2 \nmid u. \end{cases}$$

### Theorem über die Klassenzahlformel (DIRICHLET, 1839)

Für  $D \in \mathcal{D}$  gilt

$$h(D) = \begin{cases} \frac{\sqrt{D}}{2 \ln \varepsilon_{d,1}} L(1, \chi), & \text{wenn } D > 0, \\ (\text{card } R_{d,1}^*) \frac{\sqrt{|D|}}{2\pi} L(1, \chi), & \text{wenn } D < 0, \end{cases}$$

mit

$$L(1, \chi) = \begin{cases} -\frac{1}{\sqrt{D}} \sum_{n=1}^D \chi(n) \ln \sin \frac{n\pi}{D}, & \text{wenn } D > 0, \\ -\frac{\pi}{\sqrt{|D|^3}} \sum_{n=1}^{|D|} n \chi(n), & \text{wenn } D < 0. \end{cases}$$

# Kapitel 6

## Problemlösestrategien in der Zahlentheorie

### 6.1 Beschreibung des Konzepts

Im Vorwort und in Abschnitt 2.4 über die *Gaußsche Erkundungsstrategie* wurde darauf hingewiesen, dass der Problemlöseteil als Strang einerseits in den Lehrbuchtext integriert ist und dass andererseits in diesem letzten Kapitel die wichtigsten Aspekte systematisch dargestellt werden sollen. Damit unterscheidet sich unser Aufbau wesentlich von dem üblichen Vorgehen in Büchern über Problemlösen, die jeweils heuristische Strategien an Beispielen vorführen und anschließend dazu passende Aufgaben oder Probleme zusammenstellen.

Deshalb wird zunächst skizziert, welchen Beitrag die zugehörigen Bücher aus dem Literaturverzeichnis für das Problemlösen in der Zahlentheorie liefern. Danach behandeln wir ausführlich die im Buchtext schon eingeführten Strategien und ergänzen sie durch weitere Methoden und Beispiele aus den zitierten Büchern. Hier wird versucht, den geringeren Umfang unseres Heuristikteils dadurch auszugleichen, dass wir die besonderen Chancen nutzen, die die elementare Zahlentheorie im Vergleich mit allen übrigen in Mathematikwettbewerben berücksichtigten Bereichen bietet. Dabei helfen sowohl die Erfahrungen, die mit den 61 Problemen dieses Buches in den im Vorwort beschriebenen Problemseminaren gesammelt wurden, als auch die sorgfältig entwickelte Darstellung jeder Lösung in jeweils einer eigenen verschlüsselten Pdf-Datei.

Mit der Verschlüsselung wird die Notwendigkeit unterstrichen, zum Erwerben von Problemlösefähigkeiten selber Probleme zu lösen und nicht einfach die Lösungen zu lesen. Die aus den Besprechungen zum Problemseminar bekannte Ratlosigkeit vieler Teilnehmer soll hier durch eine Reihe von Maßnahmen behoben oder gemildert werden. Dazu gehören unter anderem die Zuordnung der Probleme zu drei Schwierigkeitsklassen in einer abschließenden Tabelle (Seite 234) und das Aufdecken von “Signalen”. Die Idee für die letzte Hilfestellung stammt aus der im Vorwort genannten Staatsexamensarbeit von *Stefan Krämer*, die inzwischen vollständig im *Mathkompass* verfügbar ist.

Bei Anleitungen entsteht ein Dilemma, weil einerseits nicht zu viel verraten werden soll und weil andererseits bei den ungeübten ProblemlöserInnen Startschwierigkeiten und psychologische Schwellen zu überwinden sind. Deshalb wird im folgenden Text vor allem durch “Querschnitte” angeleitet, die die Nummern der Probleme den entwickelten Strategien zuordnen. In der Schlusstabelle weisen wir auch auf die verwendbaren Sätzen des Buches hin. Im Unterschied zu Lösungsdarstellungen in Zeitschriften und im Internet wird bei den Lösungsdateien besonderer Wert auf eine *Lösungsgenese* und auf die Anwendung von Suchstrategien gelegt. Das zeigt sich besonders in häufigen Unterbrechungen durch motivierende Fragen, deren Beantwortungen durch Hypertextsprünge zu finden sind.

Die Entschlüsselung jeder Lösungsdatei erfolgt mit einem Passwort, das man auf völlig neue Weise erhält, indem man erfolgreich das als Java-Applet programmierte *Auf-und-ab-Spiel* gegen den Computer spielt. Die Spielregeln und die sonstige Vorgehensweise sind in dem *Safe-Programm* im *Mathkompass* erläutert. Das Finden einer sicheren Spielstrategie gehört zur oberen Schwierigkeitsklasse der Probleme. Mit einer relativ einfach zu entwickelnden “Minimalstrategie” benötigt man im Schnitt sechs Zufallsversuche, um ein Passwort zu erfahren.

## 6.2 Heuristikbücher

Als Vorbereitung und Ergänzung des Hauptteils dieses Kapitels werden hier die Bücher [5], [7], [13], [17], [18] und [19] aus dem Literaturverzeichnis in chronologischer Reihenfolge kurz beschrieben. Die frühesten drei Werke [17] bis [19] stammen von PÓLYA, der schon 1917 kurz nach dem Beginn seiner Lehrtätigkeit in Zürich anfang, sich mit Fragen des Problemlösens zu beschäftigen.

## Schule des Denkens

Die “Schule des Denkens” [17] mit dem Untertitel “Vom Lösen mathematischer Aufgaben” ist zwar nur ein Buch im Oktavformat mit 266 Seiten, aber die Vielfalt der darin behandelten Aspekte war damals (1944 in den USA und 1949 in den deutschsprachigen Ländern) völlig neuartig. Während die letzte deutsche Auflage schon lange vergriffen ist, wurde die überarbeitete englische Originalausgabe mit dem Titel “How to Solve It” vor einigen Jahren wieder herausgebracht. Das Buch “wendet sich in erster Linie an junge Menschen mit ernsthaftem Interesse am mathematischen Denken”. Im Hinblick auf die Wortwahl und den Stil des Textes sind damit vor allem SchülerInnen und Studierende gemeint.

Der erste der drei Teile hat den Titel “Im Klassenzimmer”. Mit zahlreichen Formulierungsvarianten und einigen Beispielen wird darin die auf den vorderen Vorsatzblättern abgedruckte “Tabelle” erläutert, die wir vollständig ab Seite 32 wiedergegeben haben. In dem sehr kurzen zweiten Teil beantwortet in idealisierter Form ein Lehrer die ständig wiederkehrenden knappen Fragen eines Schülers zum Aufgabenlösen. Der dritte und umfangreichste Teil heißt “Kleines Wörterbuch der Heuristik”. Darin werden in alphabetischer Reihenfolge 67 Themen zum Aufgaben- und Problemlösen sowohl inhaltlicher Art mit zahlreichen Beispielen als auch psychologisch oder historisch orientiert behandelt. Später kommen wir unter anderem auf die folgenden Stichwörter zurück: Bestimmungs- und Beweisaufgaben, Aufstellen von Gleichungen, Fortschritt und Leistung, unterbewusste Arbeit sowie auf die Rückwärts-, Symmetrie-, Verallgemeinerungs- und Zurückführungsstrategie.

## Mathematik und plausibles Schließen

Dieses zweibändige Werk [18] bringt auf 720 Seiten eine engagierte “Einführung in einen wichtigen, aber meist vernachlässigten Aspekt der Mathematik”. Im Unterschied zum *demonstrativen Schließen*, mit dem das mathematische Wissen in Form von Beweisen gesichert wird, kommt *plausibles Schließen* innerhalb und vor allem außerhalb der Mathematik zur Anwendung, wenn es um Vermutungen, instinktives Vorausfühlen und Erraten geht.

PÓLYA plädiert nachdrücklich dafür, die gute Gelegenheit zu nutzen, die die Mathematik auch zum Lernen des plausiblen Schließens bietet. Durch zahlreiche Beispiele vor allem im ersten Band ermöglicht er das Erfahren des plausiblen

Schließens, und durch tiefgreifende Darlegungen, die bis zur Philosophie reichen, fördert er die entsprechende Bewusstseinsbildung. Viele sorgfältig ausgewählte Aufgaben mit Lösungen dienen der Anwendung und Vertiefung des Gelernten.

Der größte Teil des ersten Bandes mit dem Untertitel “Induktion und Analogie in der Mathematik” ist dem *induktiven* und dem *analogen Schließen* als Spezialfällen gewidmet, wobei *Induktion* die wissenschaftliche Methode bedeutet, die vom besonderen Einzelfall auf das Allgemeine und Gesetzmäßige schließt. Fünf Kapitel enthalten den Begriff Induktion in ihrem Titel, darunter zwei ausführliche Darstellungen zur Geometrie des Raumes und zur Zahlentheorie sowie eines über vollständige Induktion. Im zweiten Kapitel werden neben der Anwendung von *Analogien* auch *Verallgemeinerung* und *Spezialisierung* behandelt.

Als Meister der Induktion wird immer wieder EULER zitiert. Zum Beispiel enthält das sechste Kapitel den vollständig übersetzten Aufsatz “Entdeckung eines ganz außergewöhnlichen Gesetzes der ganzen Zahlen, betreffend die Summe ihrer Teiler”. Da es sich um eines der merkwürdigsten Ergebnisse der Zahlentheorie handelt, geben wir hier diese *Eulersche  $\sigma$ -Rekursion* in heutiger Schreibweise wieder. Sie gehört aber nicht zur elementaren Zahlentheorie, weil alle bisher bekannten Beweise analytische Hilfsmittel erfordern.

### Theorem über die Eulersche $\sigma$ -Rekursion

Ist  $v_k := \begin{cases} (-1)^{r+1}, & \text{wenn sich } k \text{ in der Form } k = \frac{1}{2} r (3r + e) \text{ mit } r \in \mathbb{N}_1 \\ & \text{und } e \in \{-1, 1\} \text{ darstellen lässt,} \\ 0 & \text{sonst,} \end{cases}$

so gilt

$$\sigma(n) = \sum_{k=1}^{n-1} v_k \sigma(n-k) + v_n n \quad \text{für jedes } n \in \mathbb{N}_1.$$

Ebenso außergewöhnlich wie die Aussage dieses Satzes, den EULER erst viele Jahre später beweisen konnte, “ist die freimütige Darlegung der Leitgedanken, die ihn zu dieser Entdeckung geführt hatten”, schreibt PÓLYA bewundernd. Er folgt EULER, indem er zu vielen der wiedergegebenen mathematischen Aussagen eine Geschichte darüber vorbringt, wie die zugehörige Entdeckung, die in der Regel nicht bekannt ist, hätte zustande kommen können. Für uns ist dieses Vorgehen

Vorbild und Ansporn bei der Entwicklung der “*genetischen Lösungsdarstellungen*” für die Probleme dieses Buches.

Der zweite Band mit dem Untertitel “Typen und Strukturen plausibler Folgerung” enthält überwiegend theoretische Erörterungen. Unter anderem geht es um die Bewertung von Vermutungen. Mit Schemata, die denen des demonstrativen Schließens entsprechen, entwickelt PÓLYA “Regeln” wie zum Beispiel die folgende (in einer für uns geeigneten Form): *Ist A eine Vermutung, B eine Folgerung aus A, und lässt sich B verifizieren, so erscheint A glaubwürdiger.*

In zwei umfangreichen Kapiteln wird der Zufallsbegriff vor allem anhand von Beispielen aus dem Alltag und aus den Naturwissenschaften behandelt und ein Zusammenhang zwischen der Wahrscheinlichkeitsrechnung und der Logik des plausiblen Schließens hergestellt. Das letzte Kapitel enthält Überlegungen zum Suchen von Lösungen beziehungsweise von Beweisen im Unterschied zum Aufstellen von Vermutungen.

## Vom Lösen mathematischer Aufgaben

Das 601-seitige Werk [19], das PÓLYA als Fortsetzung von [18] bezeichnet, besteht aus zwei Teilen. Der erste Teil mit dem Titel “Lösungsschemata” behandelt vier konkrete Schemata zum Lösen von Aufgaben, wobei PÓLYA “Aufgaben” ähnlich gegen “Routine-Aufgaben” abgrenzt, wie wir “Probleme” und “Aufgaben” unterscheiden. Neun der elf Kapitel des zweiten Teils “Auf dem Wege zu einer allgemeinen Methode” sind in einem zweiten Band enthalten. Ziel des Werkes ist es, Verständnis für intelligentes Aufgabenlösen zu wecken, “Mittel und Wege zum Lehren des Aufgabenlösen darzubieten und schließlich dem Leser zur Entwicklung seiner Fähigkeiten auf diesem Gebiet zu verhelfen”.

Jedes der vier Schemata des ersten Teils wird mit zahlreichen Beispielen, Aufgaben und zugehörigen Lösungen vorgestellt. Das “Schema zweier geometrischer Örter”, das sich zunächst bei Konstruktionsaufgaben der Geometrie anwenden lässt, wird in der “umfassenderen Deutung” des zweiten Teils auf Aufgaben übertragen, die so zerlegt werden können, dass ihre Lösung der Durchschnitt der Teillösungen ist.

Das zweite Schema wird von PÓLYA nach DESCARTES<sup>1</sup> benannt, weil dieser in

---

<sup>1</sup> RENÉ DESCARTES (1596-1650) war Mathematiker, Physiker und Philosoph.

zwei Werken versucht hat, eine universelle Methode zum Lösen von Problemen aufzustellen. Die ersten beiden “Regeln” bestehen darin, ein Problem auf eine mathematische Aufgabe zurückzuführen und diese in algebraischer Form darzustellen. Die erste Vorgehensweise bezeichnen wir im nächsten Abschnitt als “*Mathematisieren*”. Die meisten Beispiele und Aufgaben dazu sind “eingekleidet” oder “angewandt”. In der umfassenderen Deutung wird die algebraische Form durch Relationen ersetzt, die die Bedingungen der Aufgabe wiedergeben.

Auch das als drittes Schema behandelte *Rekursionsverfahren* lässt sich weitreichend verallgemeinern, wenn man dabei als wesentlich ansieht, “die bereits erworbenen Kenntnisse als Operationsbasis für die Erwerbung weiterer Kenntnisse zu benützen”. Bei dem vierten Schema, das PÓLYA *Superpositionsverfahren* nennt, ist die Verallgemeinerung schon in der zusammenfassenden Formulierung enthalten: “Von einer führenden speziellen Situation oder von mehreren solchen Situationen ausgehend, gewinnen wir die allgemeine Lösung durch Superposition von Spezialfällen, bei denen diese Situationen bestehen”. Dieses Schema hängt eng mit unserer *Zurückführungsstrategie* und mit der Beweismethode der *Fallunterscheidung* zusammen.

Bevor im zweiten Teil die vier obigen Schemata umfassender gedeutet werden, beschreibt und klassifiziert PÓLYA Aufgabentypen, insbesondere Bestimmungs- und Beweisaufgaben. Der zweite Band beginnt mit der geometrischen Darstellung des Werdegangs einer Lösung und schließt daran in jeweils einem Kapitel die folgenden typischen Aspekte des Aufgabenlösen an: Pläne und Programme, Aufgaben in Aufgaben, die Geburt der Idee, wie wir denken und wie wir denken sollten. Die Beispiele und Erörterungen dieses Teils werden ergänzt durch ein Kapitel “Regeln der Entdeckung?”, das Einstellungen, Arten des Denkens und geistige Gewohnheiten in vielen Situationen des Aufgabenlösen enthält.

Die letzten beiden Kapitel bestehen aus Aufsätzen, die PÓLYA schon früher veröffentlicht hat. In “Lernen, lehren und lehren lernen” geht es vor allem um die Ausbildung von MathematiklehrerInnen. Mit der These, dass den SchülerInnen an erster Stelle das “zielgerichtete Denken” beizubringen ist, verbindet er aus verschiedenen Blickrichtungen die Empfehlung, Unterricht im Aufgabenlösen in Mathematiklehrplänen zu verankern und die LehrerInnen zum Beispiel durch “Seminare im Aufgabenlösen” darauf vorzubereiten. Auch das letzte Kapitel “Er-

raten und wissenschaftliche Methode” geht von einer These aus - nämlich, dass der mathematische Unterricht “die Schüler soweit wie möglich mit allen Aspekten mathematischer Tätigkeit bekannt machen” sollte. An einer Reihe von Beispielen, die “Pionieraufgaben” genannt werden, zeigt PÓLYA, “dass ein guter Lehrer selbst einer Durchschnittsklasse etwas vermitteln kann, was an das Erlebnis selbständiger Forschung grenzt”, wenn er geeignete Aufgaben in angemessener Weise stellt.

## Die Kunst des Sehens in der Mathematik

In diesem 91-seitigen Büchlein von BRUNO DE FINETTI [7], das wie [17] primär für SchülerInnen geschrieben ist, geht es im Wesentlichen um die mathematische Behandlung von “natürlichen” Problemen, und nur am Rande spielen Strategien zum Lösen von (gestellten) Aufgaben eine Rolle. In den ersten acht Kapiteln stehen allgemeine Einstellungen und Verhaltensweisen bei der Verwendung von Mathematik im Mittelpunkt. Die übrigen zehn Kapitel sind jeweils einem Aspekt oder Teilgebiet der Mathematik gewidmet.

Das erste Kapitel mit dem Titel “Nachdenken, um ein Resultat zu erreichen” enthält drei aus verschiedenen Zeitaltern stammende Beispiele, mit denen gezeigt wird, wie sich durch Nachdenken interessante und lohnende Ergebnisse gewinnen lassen, wenn man von konkreten Problemen ausgeht und versucht, “jedes einzelne Problem auf solche Art zu «sehen», dass man mit Verstand jede nützliche Einzelheit auswertet”. In den nächsten beiden Kapiteln wird ausgehend von drei Beispielen erläutert, welche Vorteile sich ergeben, wenn man einerseits Probleme nicht nur löst, sondern aus der Lösung auch Lehren zieht, und andererseits, wenn Plausibilitätsbetrachtungen und “Rechenarbeit” nicht ausgeklammert werden.

Mit einem Hinweis auf die Heuristikbücher von PÓLYA bringt das vierte Kapitel eine vorwortartige Abgrenzung: Nach der Analyse von häufigen Schwierigkeiten soll “ein intelligentes Training in der Kunst, *Probleme zu sehen*” angeleitet werden.

Das anschließende Kapitel heißt zwar “Die Kunst, das Leichte zu erkennen”; es geht aber vor allem um drei Gründe für “scheinbare Schwierigkeiten”. Erstens betrachten viele Anfänger eine Aufgabe als ein *einheitliches Ganzes* und glauben, dass es für die Lösung eine feste Regel geben müsse. Die zweite Schwierigkeit beruht auf der Annahme, “*Mathematik können* bedeute, dass man sofort bis

ins kleinste Detail wisse, wie man die Aufgabe anzupacken habe“. Der dritte Grund zumindest für eine psychologische Barriere ist die Vorstellung, *Mathematik verstehen* heißt, dass man in der Lage ist, “eine Folge von kleinen Übergängen auszuführen, ihre Richtigkeit zu kontrollieren und auf diese Weise die Gültigkeit des Ergebnisses zu bestätigen“. Nach einer Reihe von Beispielen schließt das Kapitel mit dem Rat, schrittweise vorzugehen.

Auch die nächsten beiden Titel beginnen nicht ganz zutreffend mit “Die Kunst, . . .”, nämlich im sechsten Kapitel “die konkreten Dinge” und im siebenten “die ökonomischen Aspekte” zu sehen. Das Erstere entspricht der “physikalischen Mathematik”, die PÓLYA ausführlich im Kapitel IX von [18] behandelt. Bei DE FINETTI geht es nur um *kürzeste Linien* in Form von gespannten Schnüren und von Großkreisen auf der Kugel. Etwas allgemeiner sind mit ökonomischen Aspekten Extremwertaufgaben gemeint, zu denen als Beispiel eine Gewinnmaximierung und zwei Weglängenminimierungen angegeben werden. Da die nächsten drei Kapitel von dem Sinn der “allgemeinen, systematischen, in Formeln niedergelegten Methoden der Mathematik” handeln, stellt die Betrachtung von “Sonderfällen” einen Übergang zum mathematisch dominierten Teil dar. Zwei Beispiele zeigen, dass oft ein Spezialfall genügt, um einen *Beweis durch Widerspruch* zu führen, und mit *Fallunterscheidung* wird bewiesen, dass  $10^k - 1$  für jedes  $k \in \mathbb{N}_2$  keine Quadratzahl ist.

Da die zahlreichen Themen, die in den anschließenden Kapiteln gestreift werden, nur wenig mit Heuristik zu tun haben, geben wir sie in Form einer Aufzählung wieder: Formeln, Algorithmen; vollständige Induktion; dynamische Betrachtungsweise, Prozess, Funktionsbegriff; geometrische Örter; geometrische Transformationen, Halbgruppen, Gruppen, Untergruppen, Kommutativität, komplexe Zahlen; Vektoren, Skalarprodukt, Ringe; Approximation, Fehlerabschätzung; Stetigkeit, Grenzwerte, Lösungsdarstellung; Wahrscheinlichkeitstheorie, Prognosen; elektronische Gehirne, Iterationsmethoden, Logik, Gedächtnisformen.

Das Buch schließt mit 32 Übungsaufgaben und mit einer “didaktischen Bemerkung für Lehrer”, die ein Plädoyer für anregenden Mathematikunterricht darstellt, der auch Anwendungen und konkrete Probleme berücksichtigt.

## **Problem-Solving Through Problems**

Dieses 332-seitige Werk von LOREN C. LARSON [13] lieferte - abgesehen von den

Problemen - die meisten Materialien und Anregungen für unsere Problemseminare, weil es für den oberen “undergraduate”-Bereich in den USA und damit für den Anfang des “Hauptstudiums” bei uns geschrieben wurde und weil es sich zum Ziel gesetzt hatte, die wichtigsten Problemlösemethoden für die Mathematik auf diesem Niveau herauszuarbeiten. Dabei sollte auch gezeigt werden, dass eine kleine Menge von einfachen “Techniken” auf viele Weisen verwendet werden kann, um eine sehr große Anzahl von Problemen zu lösen.

Typisch für die “Heuristiken” des ersten Kapitels ist die Aufforderungsform der zwölf Titel, bei denen wir im Folgenden in Klammern angeben, welchen Strategien sie in diesem Buch entsprechen:

- Suche nach einer Regelmäßigkeit (*Gaußsche Erkundungsstrategie*)
- Zeichne eine Figur (*Visualisierungsstrategie*)
- Formuliere ein äquivalentes Problem (*Umformulierungsstrategie*)
- Modifiziere das Problem (*Modifizierungsstrategie*)
- Wähle effektive Bezeichnungen
- Nutze Symmetrie (*Symmetriestrategie*)
- Zerlege in Einzelfälle (*Fallunterscheidungsstrategie*)
- Arbeite rückwärts (*Rückwärtsstrategie*)
- Argumentiere mit Widerspruch (*Beweis durch Widerspruch*)
- Beachte Parität (Teilaspekt der *Invarianzstrategie*)
- Ziehe Extremfälle in Betracht (*Extremfallstrategie*)
- Verallgemeinere (*Verallgemeinerungsstrategie*)

Einige dieser Strategien spielen bei uns eine andere Rolle: Die “Wahl effektiver Bezeichnungen” wird zur *Mathematisierung* gerechnet, die “Beachtung der Parität” stellt einen Teilaspekt der *Invarianzstrategie* dar, und “Widerspruchsargumente” werden fast ausschließlich bei Beweisen oder bei Problemen mit Beweisaufforderung verwendet.

Am Anfang von Kapitel 1 wird darauf hingewiesen, dass man sich bei einem Problem nicht schnell auf eine Lösungsstrategie festlegen soll, weil dadurch ein

“psychologischer Block” entstehen kann, der verhindert, dass man bessere oder weitere Strategien in Betracht zieht. Jeder der zwölf Abschnitte des ersten Kapitels beginnt mit einer kurzen Einführung, auf die einige Beispiele mit ausführlichen Lösungen folgen. Die anschließend zusammengestellten Probleme lassen sich mit der betreffenden Strategie in Angriff nehmen. Ihre Lösung ist aber nicht in dem Buch sondern in der angeführten Quelle zu finden. Den Schluss bildet jeweils ein kurzer Ausblick auf geeignete Probleme in anderen Teilen des Buches.

Bei unserer Behandlung der Problemlösestrategien im nächsten Abschnitt folgen wir diesem Aufbau - abgesehen von der Problemzusammenstellung - und übernehmen auch einige Beispiele.

Das zweite Kapitel ist der *vollständigen Induktion* und dem *Schubfachschluss* gewidmet. Beide Hilfsmittel werden als “Prinzipien” eingeführt und an Beispielen erläutert. Zwei zusätzliche Abschnitte stellen den Nutzen heraus, den die *Rückwärtsstrategie* und die *Verallgemeinerungsstrategie* beim Ansatz der vollständigen Induktion bringen können. Ein weiterer Abschnitt behandelt die *Rekursion* als spezielle *Zurückführungsstrategie*.

Die übrigen sechs Kapitel beschreiben zu verschiedenen Teilgebieten der Mathematik jeweils Ergebnisse, die beim Problemlösen vor allem in mathematischen Wettbewerben eine Rolle spielen können. So enthält das dritte Kapitel mit dem Titel “Arithmetik” die grundlegenden Methoden der elementaren Zahlentheorie und die Arithmetik der komplexen Zahlen. Nur sehr wenige der bereitgestellten Aussagen über Teilbarkeit, Kongruenzen, eindeutige Primfaktorzerlegung und Stellenwertsysteme werden begründet, wobei der jeweilige Beweis als Lösung eines Problems erscheint. Die gleiche Struktur haben auch die weiteren fünf Kapitel über Algebra, Summation, reelle Analysis, Ungleichungen und Geometrie.

## **Problem-Solving Strategies**

Das letzte der hier vorzustellenden Bücher [5] ist zugleich das anspruchsvollste. Es wendet sich unter anderem an TrainerInnen und TeilnehmerInnen von Mathematikwettbewerben sowie an “high school”-LehrerInnen, die Problemveranstaltungen durchführen oder die für “Problemecken” in Zeitschriften zuständig sind. Der Autor, ARTHUR ENGEL, trainierte von 1976 bis 1990 die deutsche IMO-Mannschaft und war 1989 Vorsitzender der IMO-Jury.

Die vierzehn Kapitel des 403-seitigen Buches haben eine ähnliche Struktur wie die acht Kapitel von [13]. Im Unterschied zu [13] gibt es zu fast allen der mehr als 1300 Probleme mindestens einen Lösungshinweis. Zwei Strategien werden in eigenen Kapiteln mit den Titeln “*Das Invarianzprinzip*” und “*Das Extremalprinzip*” behandelt. Zwei weitere Kapitel sind dem “*Schubfachprinzip*” und dem “*Induktionsprinzip*” gewidmet. Im zweiten Fall wird anstelle von gelösten Beispielen auf die obigen Bücher von PÓLYA verwiesen, und ähnlich wie in unserer Aufgabe 2.1 werden 15 Eigenschaften der Fibonacci-Folge als Übungsmaterial angeboten.

Im letzten Kapitel mit dem Titel “Weitere Strategien” kommen neben mathematischen Sachverhalten die *Abstiegsstrategie* und die *Rückwärtsstrategie* vor. Alle diese Strategien und die *Symmetriestrategie* treten auch in anderen Kapiteln auf, wo sie durch Fettdruck hervorgehoben sind. “Färbungsbeweise” und “Spiele” sind zwei Titel, die speziellen Problemtypen entsprechen. Im ersten Fall handelt es sich um einen Teilaspekt der *Invarianzstrategie*, und im zweiten geht es überwiegend um *Zweipersonen-Gewinnspiele* wie das *Nimspiel* in unserer Aufgabe 2.9 oder das *Auf-und-ab-Spiel* des *Safe-Programms*. Die übrigen sieben Kapitel behandeln Probleme zu den folgenden mathematischen Teilgebieten: Zahlentheorie, Geometrie, abzählende Kombinatorik, Ungleichungen, Folgen, Polynome und Funktionalgleichungen.

Bei einigen Beispiellösungen spürt man, dass ENGEL mehr als zehn Jahre Trainer der deutschen IMO-Mannschaft war, die unter seiner Anleitung sehr erfolgreich wurde: Er beschreibt Suchstrategien, weist auf Schwierigkeiten hin und gibt oft Alternativen an. Zwei der schönsten genetischen Lösungen übernehmen wir bei den Problemen 43 und 53, und bei weiteren Lösungsdarstellungen sind sie Vorbild.

## 6.3 Problemlösestrategien

Bevor wir einzelne Problemlösestrategien ausführlich mit Beispielen erläutern, wollen wir mit einer Gliederung für bessere Übersicht und damit für leichteren Zugang sorgen. Mit der Unterscheidung von *Methodik* und *Heuristik* erfassen wir die beiden Enden einer Skala, die von sicheren, zielgerichteten Verfahren bis zu vagen, tastenden Vorgehensweisen reicht. So gehören unter anderem die “Tätigkeiten” *Mathematisieren*, *Beweisen*, *Modellbilden* und *Algorithmisieren* zur

Methodik. Davon spielen hier nur die ersten beiden eine Rolle, wobei auf die Beweisverfahren nicht weiter eingegangen wird, weil sie in den früheren Kapiteln genügend ausführlich dargestellt wurden.

Das Übersetzen einer Problemsituation oder eines entsprechenden Textes in die formale Sprache der Mathematik kann dagegen schon weit in die Heuristik reichen, weil etwa Umformulierungen oder eine günstigere Parameterwahl nötig sind, um eine Lösung zu finden (vgl. [13]). Im Unterschied zu vielen “Denksportaufgaben” ist es aber bei den Wettbewerbsproblemen nicht sehr schwierig, den mathematischen Sachverhalt beziehungsweise das Aufgabenziel zu erfassen. Die meisten der Probleme in diesem Buch liegen sogar bereits in weitgehend mathematisierter Form vor. Für Unerfahrene ist es allerdings zum Beispiel bei den Problemen 47, 55, 58, 60 und 61 nicht einfach, einen geeigneten Ansatz zu finden. Anders als für IMO-TeilnehmerInnen, die an zwei Tagen jeweils drei Aufgaben in  $4\frac{1}{2}$  Stunden lösen sollen, spielt hier der Zeitaspekt keine Rolle bei der Bewertung des Schwierigkeitsgrades.

Um eine grobe Übersicht zu erhalten, “hierarchisieren” wir zunächst die für die elementare Zahlentheorie infrage kommenden Problemlösestrategien, indem wir drei Typen unterscheiden.

- **Globale Strategien** umfassen die Suche nach Regelmäßigkeiten oder nach Ansatzpunkten für konkrete Strategien, die Brauchbarkeitsanalyse bei ähnlichen Problemen oder Sätzen, die Problemabwandlung und die Erzeugung von Problemketten (*Gaußsche Erkundungsstrategie, Umformulierungsstrategie, Modifizierungsstrategie, Verallgemeinerungsstrategie*)
- **Lokale Strategien** strukturieren ein gegebenes Problem und nutzen seine Besonderheiten (*Rückwärtsstrategie, Pólyasche Brückenstrategie, Invarianzstrategie, Symmetriestrategie, Fallunterscheidungsstrategie, Zurückführungsstrategie, Extremfallstrategie, Visualisierungsstrategie*)
- **Mikrostrategien** benutzen Gesetzmäßigkeiten und Schlussweisen des betreffenden mathematischen Teilgebiets, um Material für die Aufstellung und zum Bestätigen oder Verwerfen von Vermutungen auf dem Weg zu einer Lösung zu erhalten (*Kernbruchstrategie, Klammerungsstrategie, Exponentenvergleichsstrategie, Wechselwegnahmestrategie, Abstiegsstrategie*).

## Gaußsche Erkundungsstrategie

Diese am häufigsten anzuwendende Strategie ist schwer zu beschreiben, weil bei ihr typische Merkmale (“Signale”) fehlen und weil sie oft nur in Verbindung mit anderen Strategien zum Ziel führt. So dient sie meistens der Suche nach “Ansatzpunkten” für solche konkreteren Strategien oder dem Aufdecken von Strukturen. Bei der Einführung der *Gaußschen Erkundungsstrategie* mit der Lösung von Problem 1 (Seite 31) wurde durch die Behandlung von Spezialfällen zunächst die Einsatzmöglichkeit der *Rückwärtsstrategie* erkannt, die schließlich zur Anwendung der *Kernbruchstrategie* führte.

Zum Aufdecken von Strukturen gehört meistens eine Materialsammlung in Form einer Tabelle mit Werten für kleine Parameter. Beim “häuslichen” Problemlösen ist dafür ein Computeralgebrasystem sehr empfehlenswert. Die dann vorliegende Aufgabe, Regelmäßigkeiten zu erkennen und zu nutzen, ähnelt schon der Forschungsarbeit des problemlösenden Mathematikers. Wir bringen deshalb ein leichtes und ein schweres Beispiel. Für ersteres modifizieren wir das Problem 1.1.2 aus [13], um mehrere Aspekte für den häufig auftretenden Problemtyp darstellen zu können, bei dem eine Aussage für sehr große Parameterwerte (meistens die Jahreszahl des Wettbewerbs oder der IMO) gezeigt werden soll. Bemerkenswert ist hier, wie “Beobachtungen” zu Vermutungen über Allgemeingültigkeit werden, und wie aufgrund von weiteren Beobachtungen Vermutungen für einzelne Beweisschritte aufzustellen sind. Manchmal können dabei längere Ketten von Vermutungen entstehen, bevor sich ein Beweis führen lässt.

### Problem 62

Für  $n \in \mathbb{N}$  und  $k \in \mathcal{A}_3$  sei  $S_{n,k} := \sum_{j=0}^n \binom{n}{k+3j}$ , wobei  $\binom{n}{k+3j}$  für  $k+3j \leq n$  die in (3.23) eingeführten Binomialkoeffizienten sind und  $\binom{n}{k+3j} = 0$  für  $k+3j > n$  gilt. Leiten Sie für  $S_{n,k}$  eine “geschlossene Form” her, das heißt eine Darstellung ohne Summen- oder Produktzeichen und ohne rekursiv oder implizit definierte Terme.

(In [13] lautet die Aufgabe: Stellen Sie eine Vermutung bezüglich des Wertes von  $S_{100,1}$  auf.)

Als Materialsammlung verwenden wir die folgende Tabelle:

| $n$ | $\binom{n}{0}$ | $\binom{n}{1}$ | $\binom{n}{2}$ | $\binom{n}{3}$ | $\binom{n}{4}$ | $\binom{n}{5}$ | $\binom{n}{6}$ | $\binom{n}{7}$ | $S_{n,0}$       | $S_{n,1}$       | $S_{n,2}$       |
|-----|----------------|----------------|----------------|----------------|----------------|----------------|----------------|----------------|-----------------|-----------------|-----------------|
| 0   | 1              | 0              | 0              | 0              | 0              | 0              | 0              | 0              | 1 <sup>+</sup>  | 0               | 0               |
| 1   | 1              | 1              | 0              | 0              | 0              | 0              | 0              | 0              | 1               | 1               | 0 <sup>-</sup>  |
| 2   | 1              | 2              | 1              | 0              | 0              | 0              | 0              | 0              | 1               | 2 <sup>+</sup>  | 1               |
| 3   | 1              | 3              | 3              | 1              | 0              | 0              | 0              | 0              | 2 <sup>-</sup>  | 3               | 3               |
| 4   | 1              | 4              | 6              | 4              | 1              | 0              | 0              | 0              | 5               | 5               | 6 <sup>+</sup>  |
| 5   | 1              | 5              | 10             | 10             | 5              | 1              | 0              | 0              | 11              | 10 <sup>-</sup> | 11              |
| 6   | 1              | 6              | 15             | 20             | 15             | 6              | 1              | 0              | 22 <sup>+</sup> | 21              | 21              |
| 7   | 1              | 7              | 21             | 35             | 35             | 21             | 7              | 1              | 43              | 43              | 42 <sup>-</sup> |

Aus den letzten drei Spalten können wir zunächst folgende Beobachtungen entnehmen:

- i) In jeder Zeile stehen zwei gleiche Zahlen.
- ii) Der jeweils davon verschiedene Wert ist abwechselnd um 1 größer (durch <sup>+</sup> markiert) oder um 1 kleiner (durch <sup>-</sup> gekennzeichnet).
- iii) Bei  $(n, k) = (1, 2)$  beginnend liegen die abweichenden Werte auf parallelen, nach links geneigten Strecken.

Beachten wir, dass der Index  $k$  des abweichenden Wertes als  $k = \text{mod}(-n, 3)$  geschrieben werden kann, so lassen sich die drei Beobachtungen als Vermutungen mathematisieren:

$$(6.1) \quad S_{n, \text{mod}(2-n, 3)} = S_{n, \text{mod}(1-n, 3)} = S_{n, \text{mod}(-n, 3)} - (-1)^n =: T_n.$$

Zusammen mit der Gleichung

$$S_{n,0} + S_{n,1} + S_{n,2} = 2^n,$$

die für  $x = 1$  aus (3.23) folgt, können wir nun schon wegen  $3T_n + (-1)^n = 2^n$  die gesuchte geschlossene Form von  $S_{n,k}$  als Vermutung formulieren:

$$(6.2) \quad S_{n,k} = \frac{1}{3}(2^n - (-1)^n) + (-1)^n \eta_{n,k} \quad \text{mit} \quad \eta_{n,k} := \begin{cases} 1, & \text{wenn } 3 \mid (n+k), \\ 0, & \text{sonst.} \end{cases}$$

Für Problem 1.1.2 aus [13] ergibt sich daraus  $S_{100,1} = \frac{1}{3}(2^{100} - 1)$ . Die dort folgende Aussage, dass “der formale Beweis für diese Vermutung eine einfache Anwendung der vollständigen Induktion” ist, trifft nicht zu, weil hier wie auch bei vielen anderen Induktionsbeweisen zu Problemlösungen der Induktionsschritt nicht auf der Hand liegt sondern gesucht werden muss. Dazu betrachten wir

in der obigen Tabelle aufeinanderfolgende Zeilen. Die drei beobachtbaren Fälle zusammenfassend vermuten wir

$$(6.3) \quad S_{n+1,k} = S_{n,k} + S_{n,\text{mod}(k-1,3)} \text{ für alle } n \in \mathbb{N} \text{ und jedes } k \in \mathcal{A}_3.$$

Der Beweis mit Hilfe der hier als bekannt vorauszusetzenden Rekursionsformel

$$\binom{n+1}{i+1} = \binom{n}{i+1} + \binom{n}{i}$$

erfolgt durch Fallunterscheidung. Für  $k \in \{1, 2\}$  erhalten wir

$$S_{n+1,k} = \sum_{j=0}^{n+1} \binom{n+1}{k+3j} = \sum_{j=0}^n \binom{n}{k+3j} + \sum_{j=0}^n \binom{n}{k-1+3j} = S_{n,k} + S_{n,k-1}.$$

Im Falle  $k=0$  muss der erste Summand gesondert behandelt werden:

$$\begin{aligned} S_{n+1,0} &= \sum_{j=0}^{n+1} \binom{n+1}{3j} = \binom{n+1}{0} + \sum_{j=1}^{n+1} \binom{n}{3j} + \sum_{j=1}^{n+1} \binom{n}{3j-1} \\ &= \binom{n}{0} + \sum_{j=1}^n \binom{n}{3j} + \sum_{i=0}^n \binom{n}{2+3i} = S_{n,0} + S_{n,2}. \end{aligned}$$

Erst jetzt ist ein einfacher Beweis von (6.2) mit vollständiger Induktion möglich, wenn man noch durch Fallunterscheidung  $\eta_{m+1,k} = 1 - \eta_{m,k} - \eta_{m,\text{mod}(k-1,3)}$  für alle  $m \in \mathbb{N}$  und jedes  $k \in \mathcal{A}_3$  nachweist.

Das folgende Beispiel E14 aus Kapitel 6 von [5] wird von ENGEL als eines der schwierigsten Probleme bezeichnet, die bei einem Mathematikwettbewerb für SchülerInnen gestellt wurden. Das Problem und seine Lösung stammen von EULER, der aber nichts davon veröffentlicht hat.

### Problem 63

Beweisen Sie, dass es zu jedem  $n \in \mathbb{N}_3$  ein Paar  $(x, y) \in \mathbb{N}_1^2$  mit  $2 \nmid xy$  gibt, sodass  $2^n = 7x^2 + y^2$  gilt.

Wir bringen dieses Problem aus “psychologischen” Gründen, weil im Unterschied etwa zu den zahlreichen Problemen in [10] bei SchülerInnenwettbewerben stets eine “Lösbarkeitsgarantie mit Schwierigkeitsbeschränkung” vorliegt, wodurch sogar eine Art von *Brückenstrategie* möglich ist, die wir hier anwenden werden. Als Materialsammlung erhält man durch “systematisches Probieren” leicht die folgende Tabelle, indem man bei festem  $n \in \{3, \dots, 10\}$  das kleinste ungerade  $x \in \mathbb{N}_1$  bestimmt, für das  $2^n - 7x^2$  eine Quadratzahl ist.

| $n$ | 3 | 4 | 5 | 6 | 7  | 8 | 9  | 10 |
|-----|---|---|---|---|----|---|----|----|
| $x$ | 1 | 1 | 1 | 3 | 1  | 5 | 7  | 3  |
| $y$ | 1 | 3 | 5 | 1 | 11 | 9 | 13 | 31 |

Auf den ersten Blick ist keine Gesetzmäßigkeit zu erkennen. Aber der obige “Vertrauensschutz” erlaubt die Annahme, dass die Werte in jeder Spalte nur durch die Zahlen in der Vorgängerspalte bestimmt sind. Als zweckmäßige Bezeichnung bietet es sich dann an, die Lösungskomponenten als Glieder  $x_n$  und  $y_n$  von zwei Folgen zu schreiben. Die “psychologische Brückenstrategie” lässt sich nun folgendermaßen formulieren: Wenn die Lösung nicht zu schwierig ist, dann gibt es rekursive Darstellungen

$$(6.4) \quad x_{n+1} = ax_n + by_n, \quad y_{n+1} = cx_n + dy_n \quad \text{mit } a, b, c, d \in \mathbb{Q} \text{ für alle } n \in \mathbb{N}_3.$$

Die Tabelle zeigt, dass  $a, b, c$  und  $d$  nicht ganz unabhängig von  $x_n$  und  $y_n$  sein können, weil  $a = b = \frac{1}{2}$  für  $n \in \{3, 5, 8\}$  den richtigen  $x_{n+1}$ -Wert ergibt, während für  $n \in \{4, 6, 7, 9\}$  nicht einmal ungerade Zahlen herauskommen. In diesen Fällen liefert aber  $a = \frac{1}{2}$ ,  $b = -\frac{1}{2}$  oder  $a = -\frac{1}{2}$ ,  $b = \frac{1}{2}$  den korrekten  $x_{n+1}$ -Wert. Damit liegt die Vermutung nahe, dass sich zumindest  $x_{n+1}$  mit Fallunterscheidung aus  $x_n$  und  $y_n$  berechnen lässt, wobei die letzten beiden Fälle noch zusammengefasst werden können, wenn wir in (6.4) Betragsbildung zulassen.

Dieser “unnatürliche” Ansatz mit Beträgen, die wegen des Quadrierens in  $7x_n^2 + y_n^2$  eigentlich unnötig sind, sollte zu der Idee führen, auch negative Lösungskomponenten zuzulassen, um die obigen Fallunterscheidungen zu vermeiden. Wir versuchen also, die vorhandenen Lösungswerte so mit Vorzeichen zu versehen, dass die Rekursionsgleichung  $x_{n+1} = \frac{1}{2}(x_n + y_n)$  durchgängig gilt. Da  $x_{n+1}$  ungerade sein soll, muss zusätzlich  $x_n \equiv y_n \pmod{4}$  für alle  $n \in \mathbb{N}_3$  gelten. Indem wir mit  $x_3 = y_3 = x_4 = 1$  beginnen, setzen wir  $y_4 := -3$ , damit  $y_4 \equiv x_4 \pmod{4}$  ist, und fahren jeweils mit der Bildung des arithmetischen Mittels sowie der Vorzeichenanpassung der  $y_n$  fort. Dann erhalten wir die modifizierte Tabelle

| $n$   | 3 | 4  | 5  | 6  | 7  | 8 | 9   | 10  |
|-------|---|----|----|----|----|---|-----|-----|
| $x_n$ | 1 | 1  | -1 | -3 | -1 | 5 | 7   | -3  |
| $y_n$ | 1 | -3 | -5 | 1  | 11 | 9 | -13 | -31 |

Um herauszufinden, ob  $y_n$  auch einer durchgängigen Rekursionsgleichung genügt, wenden wir noch einmal eine *Brückenstrategie* an, indem wir überlegen, wodurch ein Zusammenhang zwischen den Lösungspaaren von  $2^n = 7x_n^2 + y_n^2$  und  $2^{n+1} =$

$7x_{n+1}^2 + y_{n+1}^2$  zustande kommen kann. Am einfachsten ist das Substituieren von  $2^n$  in der zweiten Gleichung durch die rechte Seite der ersten:

$$7x_{n+1}^2 + y_{n+1}^2 = 2(7x_n^2 + y_n^2).$$

Einsetzen von  $x_{n+1} = \frac{1}{2}(x_n + y_n)$  und Auflösen nach  $y_{n+1}^2$  ergibt dann

$$y_{n+1}^2 = 14x_n^2 + 2y_n^2 - \frac{7}{4}(x_n + y_n)^2 = \frac{1}{4}(7x_n - y_n)^2.$$

Die Zahlenwerte der zweiten Tabelle erfordern für  $y_{n+1}$  die Wahl der mit -1 multiplizierten Klammer, sodass

$$(6.5) \quad x_{n+1} = \frac{1}{2}(x_n + y_n), \quad y_{n+1} = \frac{1}{2}(-7x_n + y_n) \quad \text{für jedes } n \in \mathbb{N}_3$$

die gesuchten Rekursionsgleichungen sind, wenn wir zeigen können, dass  $x_{n+1} \equiv y_{n+1} \pmod{4}$  für alle  $n \in \mathbb{N}_3$  gilt. Offenbar verhindern die Faktoren  $\frac{1}{2}$  in (6.5) einen direkten Nachweis. Lösen wir die erste Gleichung nach  $y_n$  auf und setzen das Ergebnis in die zweite ein, so erhalten wir  $y_{n+1} = x_{n+1} - 4x_n$ . Indexverschiebung und Substitution in der ersten Gleichung ergibt  $x_{n+1} = x_n - 2x_{n-1}$ . Analoges Eliminieren von  $x_n$  liefert  $-7x_{n+1} = y_{n+1} - 4y_n$  und damit  $y_{n+1} = y_n - 2y_{n-1}$ . Diese Rekursionsgleichungen vom Typ der Fibonacci-Folge fassen wir zusammen:

$$(6.6) \quad \begin{aligned} x_{n+1} &= x_n - 2x_{n-1}, & y_{n+1} &= y_n - 2y_{n-1} \quad \text{für alle } n \in \mathbb{N}_4 \text{ und} \\ x_3 &= x_4 = y_3 = 1, & y_4 &= -3. \end{aligned}$$

Mit Fallunterscheidung und vollständiger Induktion erhalten wir nun sogar

$$(6.7) \quad x_n \equiv y_n \equiv 2 - (-1)^n \pmod{4} \quad \text{für alle } n \in \mathbb{N}_4.$$

Die in [5] wiedergegebene Lösung mit Beträgen und mit Fallunterscheidung, die von einem Mitglied der deutschen IMO-Mannschaft stammt, ist zweifellos “näherliegend” als die hier verwendete *Verallgemeinerungsstrategie* durch Vergrößerung der zugelassenen Zahlenmenge. Unser Vorgehen ist einerseits eine Anwendung des Rats in Kapitel 1 von [13], sich nicht schnell auf eine Lösungsstrategie festzulegen, und es belegt andererseits die in Kapitel 2 von [7] erläuterten Vorteile, die sich ergeben, wenn man ein Problem nicht nur löst, sondern aus der Lösung auch Lehren zieht. In unserem Fall haben wir zusätzlich zwei einfache Rekursionsgleichungspaare gefunden. Außerdem werden wir in *Problem 81* (Seite 231) als Beispiel für die *Abstiegsstrategie* mit Hilfe von (6.5) zeigen, dass es zu jedem  $n \in \mathbb{N}_3$  genau ein Paar  $(x, y) \in \mathbb{N}_1^2$  mit  $2 \nmid xy$  und  $2^n = 7x^2 + y^2$  gibt.

Bei den Problemen 2, 5, 7, 10, 11, 12, 13, 15, 20, 23, 24, 31, 35, 37, 43, 44, 45, 49, 52, 58, 60 und 61 kann die *Erkundungsstrategie* auf dem Wege zur Lösung

weiterhelfen. Die übrigen 38 Probleme lassen sich ohne diese Strategie in Angriff nehmen. Hier und im Folgenden wird aber nicht ausgeschlossen, dass es auch bei aufgezählten Problemen Umstände geben kann, die eine Lösung ohne die betreffende Strategie ermöglichen - zum Beispiel, wenn entsprechende Vorkenntnisse vorhanden sind.

## Umformulierungsstrategie

Ist ein Problem (überwiegend) als Text gegeben, so stellt schon das *Mathematisieren* eine Umformulierung dar. Da diese "Technik" im Mathematikunterricht und im Mathematikstudium geübt wird, gehen wir hier nicht explizit darauf ein. Wenn aber weder die mathematische Form des Problems noch eine Anwendung der *Erkundungsstrategie* eine Idee liefert, empfiehlt es sich häufig, das Problem so umzuformulieren, dass sich eine äquivalente Aussage ergibt, die einfacher ist oder auf irgend eine Weise Erfolg verspricht. Für solche Umformulierungen stehen einige Standardverfahren zur Verfügung: algebraische Operationen, Substitution oder Wechsel von Variablen, Nutzung umkehrbar eindeutiger Zuordnungen und die Umdeutung in der Sprache eines anderen mathematischen Gebiets (z. B. Algebra, Geometrie oder Kombinatorik).

Die meisten Beweise dieses Buches enthalten mehr oder weniger starke Umformulierungen durch logische Schlüsse oder durch algebraische Operationen in Gleichungen, Ungleichungen beziehungsweise Kongruenzen. Die wirkungsvollste Folge solcher Darstellungsänderungen findet sich im Beweis des *quadratischen Reziprozitätsgesetzes* (Seite 114). Dort wird für das mit Hilfe von Halbsystemen definierte Jacobi-Symbol gezeigt, dass

$$\left(\frac{n}{m}\right) \left(\frac{m}{n}\right) = (-1)^{\text{card } \mathcal{G}} = (-1)^{\text{card } \mathcal{R}} \text{ für alle } (m, n) \in \mathbb{U}^2 \text{ mit } \text{ggT}(m, n) = 1$$

gilt, wobei  $\mathcal{G}$  und  $\mathcal{R}$  Gitterpunktmenge sind, die durch algebraische Operationen gewonnen werden und die sich mit der *Visualisierungsstrategie* in Beziehung setzen lassen.

Ein ähnliches Beispiel, in dem die Umformungen der Vorbereitung einer weiteren Strategie dienen, werden wir bei der Behandlung der *Visualisierungsstrategie* bringen. Hier folgen die Probleme 1.3.6 und 1.3.4 aus [13] als Beispiele zu den Standardverfahren der Nutzung umkehrbar eindeutiger Zuordnungen und der Umdeutung in der Sprache der Kombinatorik.

**Problem 64**

Bestimmen Sie für jedes  $n \in \mathbb{N}$  die Anzahl der Quadrupel  $(a, b, c, d) \in \mathbb{N}^4$  mit  $a \leq b \leq c \leq d \leq n$ .

Da wir noch kein ähnliches Problem behandelt haben, probieren wir die *Erkundungsstrategie* und erhalten für  $n = 0, 1, 2$  die Anzahlen 1, 5 und 15. Aber bereits für  $n=2$  ist es mühsam, die 15 Quadrupel zu erfassen. Deshalb versuchen wir die *Brückenstrategie*, indem wir fragen, welche vergleichbaren Objekte wir schon zählen können.

Bei dem Beweis des *Satzes über die Möbius-Summe* (Seite 65) haben wir verwendet, dass der Binomialkoeffizient  $\binom{r}{k}$  für eine Zahl mit  $r$  verschiedenen Primteilern die Anzahl der Teiler mit  $k$  Primfaktoren ist. Für eine beliebige Menge mit  $r$  Elementen kann man mit Hilfe der *Umformulierungsstrategie* nachweisen, dass die Anzahl der  $k$ -elementigen Teilmengen  $\binom{r}{k}$  ist, indem man den Elementen Zahlenvariable  $x_1, \dots, x_r$  umkehrbar eindeutig zuordnet und einerseits in der Summendarstellung des ausmultiplizierten Produkts  $\prod_{i=1}^r (1 + x_i)$  die Faktoren der Summanden jeweils als Elemente von Teilmengen deutet, sowie andererseits nach dem Zuweisen der Zahlenvariablen  $x$  zu allen Variablen  $x_i$ ,  $i \in \mathcal{I}_r$ , aus der Binomialformel (3.23) die Anzahl der Summanden mit  $k$  Faktoren aus  $\{x_1, \dots, x_r\}$  entnimmt.

Wir setzen  $\mathcal{Q}_n := \{(a, b, c, d) \in \mathbb{N}^4; a \leq b \leq c \leq d \leq n\}$  und versuchen, die Quadrupel auf vierelementige Teilmengen einer Menge mit möglichst kleinen Zahlen aus  $\mathbb{N}$  abzubilden. Die Teilmengen bestehen aus verschiedenen Zahlen, die der Einfachheit halber nach ihrer Größe geordnet seien. Damit ist  $\{0, 1, 2, 3\}$  diejenige vierelementige Teilmenge von  $\mathbb{N}$ , die die kleinstmöglichen Zahlen enthält. Werden die Quadrupel lexikografisch angeordnet, so liegt es nahe, diese Teilmenge dem ersten Quadrupel  $(0, 0, 0, 0)$  zuzuordnen. Allgemein gilt  $0 \leq a < b + 1 < c + 2 < d + 3 \leq n + 3$  für jedes  $(a, b, c, d) \in \mathcal{Q}_n$ , sodass  $\{a, b + 1, c + 2, d + 3\}$  eine Teilmenge von  $\mathcal{A}_{n+4}$  darstellt, die als Bild von  $(a, b, c, d)$  gewählt werden kann.

Ist  $\mathcal{T}_n := \{\mathcal{B} \subseteq \mathcal{A}_{n+4}; \text{card } \mathcal{B} = 4\}$ , so müssen wir also nur noch zeigen, dass

$$q : \mathcal{Q}_n \rightarrow \mathcal{T}_n, (a, b, c, d) \mapsto \{a, b + 1, c + 2, d + 3\}$$

eine bijektive Abbildung darstellt.

Sind  $(a_0, a_1, a_2, a_3)$  und  $(b_0, b_1, b_2, b_3)$  verschiedene Quadrupel aus  $\mathcal{Q}_n$  und ist für  $k := \min \{i \in \mathcal{A}_4 ; a_i \neq b_i\}$  ohne Beschränkung der Allgemeinheit  $a_k < b_k$ , so gilt  $a_k + k \notin \{b_0, b_1 + 1, b_2 + 2, b_3 + 3\}$  aufgrund der Größenbeziehungen in den Quadrupeln und den zugeordneten Teilmengen. Damit ist  $q$  injektiv. Die Surjektivität von  $q$  ergibt sich, weil zu jeder Teilmenge  $\{u, v, w, x\}$  von  $\mathcal{T}_n$  mit  $u < v < w < x$  das Urbild  $(u, v - 1, w - 2, x - 3) \in \mathcal{Q}_n$  existiert. Zusammenfassend erhalten wir also

$$\text{card } \mathcal{Q}_n = \text{card } \mathcal{T}_n = \binom{n+4}{4} \text{ für jedes } n \in \mathbb{N}.$$

**Problem 65**

Beweisen Sie, dass

$$\sum_{i=0}^k \binom{m}{i} \binom{n}{k-i} = \binom{m+n}{k}$$

für alle  $m, n \in \mathbb{N}_1$  und jedes  $k \in \mathcal{I}_{m+n}$  gilt.

Wird für die Binomialkoeffizienten die explizite Darstellung aus der Fußnote von Seite 65 verwendet, so ist keine Beweismöglichkeit zu erkennen. Dagegen führt die obige Deutung der Binomialkoeffizienten als Anzahlen von Teilmengen schnell zum Ziel. Sind nämlich  $\mathcal{A}$  und  $\mathcal{B}$  disjunkte Mengen mit  $\text{card } \mathcal{A} = m$  und  $\text{card } \mathcal{B} = n$ , so ergibt sich einerseits für die Vereinigungsmenge  $\mathcal{S} := \mathcal{A} \cup \mathcal{B}$ , dass  $\text{card } \mathcal{S} = m + n$  und  $\text{card } \{\mathcal{C} \subseteq \mathcal{S} ; \text{card } \mathcal{C} = k\} = \binom{m+n}{k}$  gilt.

Andererseits lassen sich alle Teilmengen  $\mathcal{C}$  von  $\mathcal{S}$  als Vereinigung  $\mathcal{C} = (\mathcal{C} \cap \mathcal{A}) \cup (\mathcal{C} \cap \mathcal{B})$  darstellen, und jede Vereinigung  $\mathcal{C}_A \cup \mathcal{C}_B$  mit  $\mathcal{C}_A \subseteq \mathcal{A}$  und  $\mathcal{C}_B \subseteq \mathcal{B}$  ist eine Teilmenge von  $\mathcal{S}$ . Wird nun

$$A_{i,j} := \text{card } \{\mathcal{C} \subseteq \mathcal{S} ; \text{card } (\mathcal{C} \cap \mathcal{A}) = i, \text{card } (\mathcal{C} \cap \mathcal{B}) = j\} \text{ für } i, j \in \mathbb{N}$$

gesetzt, so gilt

$$A_{i,j} = \binom{m}{i} \binom{n}{j},$$

weil die  $i$ -elementigen Teilmengen von  $\mathcal{A}$  und die  $j$ -elementigen Teilmengen von  $\mathcal{B}$  unabhängig voneinander gewählt werden können. Da für  $i > m$  oder  $j > n$  keine entsprechende Teilmenge existiert, ist in diesen Fällen  $A_{i,j} = 0$  - in Übereinstimmung mit der expliziten Darstellung der Binomialkoeffizienten. Beim Zählen der  $k$ -elementigen Teilmengen von  $\mathcal{S}$  sind alle Teilmengenvereinigungen mit  $i + j = k$  zu berücksichtigen. Damit folgt

$$\binom{m+n}{k} = \sum_{i=0}^k A_{i,k-i} = \sum_{i=0}^k \binom{m}{i} \binom{n}{k-i}.$$

Ein ganz anderer Beweis ist mit der *Methode des Koeffizientenvergleichs* möglich, die bei der Behandlung der *Verallgemeinerungsstrategie* skizziert wird. Multipliziert man die beiden Polynome

$$(1+x)^m = \sum_{j=0}^m \binom{m}{j} x^j \quad \text{und} \quad (1+x)^n = \sum_{l=0}^n \binom{n}{l} x^l,$$

so ergibt sich einerseits

$$(1+x)^m (1+x)^n = (1+x)^{m+n} = \sum_{k=0}^{m+n} \binom{m+n}{k} x^k$$

und andererseits

$$\left( \sum_{j=0}^m \binom{m}{j} x^j \right) \left( \sum_{l=0}^n \binom{n}{l} x^l \right) = \sum_{k=0}^{m+n} \sum_{i=0}^k \binom{m}{i} \binom{n}{k-i} x^k.$$

Ein “*Koeffizientenvergleichssatz*” der linearen Algebra liefert dann die Gleichheit der Koeffizienten (siehe Seite 206).

Die *Umformulierungsstrategie* kann bei den folgenden Problemen dieses Buches hilfreich sein: 6, 27, 33, 34, 35, 37, 40, 41, 42, 46, 47, 57 und 59. Nicht immer erfolgt die Anwendung gleich nach dem Mathematisieren.

## Modifizierungsstrategie

Diese Strategie, bei deren Darstellung wir [13] folgen, kam in den früheren Kapiteln nicht explizit vor. Wie bei der *Umformulierungsstrategie* geht es um die Lösung eines “Ersatzproblems”  $B$  anstelle des gegebenen Problems  $A$ . Die *Umformulierungsstrategie* führt von  $A$  ausgehend zu einem “äquivalenten” Problem  $B$ , wobei äquivalent bedeutet, dass die Lösung des einen Problems jeweils die Lösung des anderen impliziert. Bei der *Modifizierungsstrategie* wird dagegen von der Lösung eines Hilfsproblems  $B$  auf die Lösung von  $A$  geschlossen aber meistens nicht umgekehrt. Insbesondere gibt es oft keinen naheliegenden Weg zum Finden von  $B$ .

Selbst bei den für diese Strategie typischen Formulierungen “Es genügt zu zeigen, dass ...”, “Wir dürfen annehmen, dass ...” oder “Ohne Beschränkung der Allgemeinheit ...” wird in der Regel die *Erkundungsstrategie* benötigt, um auf die entsprechende Modifikation zu kommen.

Enge Zusammenhänge mit der *Modifizierungsstrategie* liegen bei der *Verallgemeinerungsstrategie*, der *Zurückführungsstrategie*, der *Rückwärtsstrategie* und der

*Symmetriestrategie* vor, wobei die ersten beiden meistens als Spezialfälle angesehen werden können, die wir aber wegen ihrer Leistungsfähigkeit in eigenen Abschnitten behandeln. Das folgende Problem 1.4.3 aus [13] ist in Kapitel 6 von [5] als E12 mit zwei Lösungen zu finden.

### Problem 66

Bestimmen Sie alle  $(x, y, z) \in \mathbb{Z}^3$  mit  $x^2 + y^2 + z^2 = 2xyz$ .

Es sei  $\mathcal{L} := \{(u, v, w) \in \mathbb{Z}^3 ; u^2 + v^2 + w^2 = 2uvw\}$ . Dann gilt  $(0, 0, 0) \in \mathcal{L}$ , und aus  $(x, y, z) \in \mathcal{L} \setminus \{(0, 0, 0)\}$  folgt  $xyz > 0$ , sodass mit  $(x, y, z)$  auch  $(|x|, |y|, |z|)$  in  $\mathcal{L} \setminus \{(0, 0, 0)\}$  liegt. Deshalb dürfen wir als erste Modifikation  $(x, y, z) \in \mathcal{L} \cap \mathbb{N}_1^3$  annehmen.

Setzen wir nun  $k := \min \{\nu_2(x), \nu_2(y), \nu_2(z)\}$  und  $x_1 := 2^{-k}x$ ,  $y_1 := 2^{-k}y$ ,  $z_1 := 2^{-k}z$ , so erhalten wir durch Einsetzen und Kürzen

$$(6.8) \quad x_1^2 + y_1^2 + z_1^2 = 2^{k+1}x_1y_1z_1 \text{ mit } 2 \nmid \text{ggT}(x_1, y_1, z_1) \text{ und } k \in \mathbb{N}.$$

Hier handelt es sich um eine "echte" Modifikation, weil die Lösungssuche bei (6.8) weder eine Zurückführung noch eine Verallgemeinerung des Ausgangsproblems darstellt.

In (6.8) ist die rechte Seite gerade, sodass nicht alle Summanden der linken Seite ungerade sein können. Wegen  $2 \nmid \text{ggT}(x_1, y_1, z_1)$  ist deshalb genau eine Komponente gerade, und es gilt  $x_1^2 + y_1^2 + z_1^2 \equiv 2 \pmod{4}$  - im Widerspruch zu  $4 \mid (2^{k+1}x_1y_1z_1)$ . Da jedes Tripel aus  $\mathcal{L} \setminus \{(0, 0, 0)\}$  zu einer Lösung von (6.8) führen würde, ist also  $\mathcal{L} = \{(0, 0, 0)\}$ .

Dieses Beispiel steht für eine Klasse von Problemen, bei denen eine Lösungsmenge zu bestimmen ist. Nachdem durch Probieren oder mit einfachen Schlüssen Lösungen einer Aussage  $A$  gefunden sind, ist die Hauptaufgabe dann aber der Nachweis, dass es keine weiteren Lösungen gibt. Die *Modifizierungsstrategie* liefert als Folgerung aus  $A$  eine meistens naheliegende Aussage  $B$ , und die *Kontraposition* "Aus  $\neg B$  folgt  $\neg A$ " hilft als eigentliche Anwendung der Strategie bei der Abgrenzung der Lösungsmenge.

Alle Probleme, die bei uns - abgesehen von der *Verallgemeinerungsstrategie* und der *Zurückführungsstrategie* - den Einsatz der *Modifizierungsstrategie* zulassen,

sind von diesem Typ: 3, 6, 8, 12, 18, 30, 38, 54 und 56. Bei der Formulierung dieser Probleme kann man ein *Signal* feststellen: Es sind stets Zahlenmengen, Paarmengen, Tripelmengen oder Ähnliches zu *bestimmen* oder zu *suchen*.

## Verallgemeinerungsstrategie

In den früheren Kapiteln ist diese Strategie bereits in drei wichtigen Formen vorgekommen:

- i) “Zahlbereichsvergrößerung” führte bei dem Beweis des *Satzes über vollständige Quotienten und Näherungsbrüche* (Seite 25) und bei *Problem 63* (Seite 195) zum Ziel.
- ii) Das *Jacobi-Symbol* als Verallgemeinerung des *Legendre-Symbols* ermöglichte unter anderem mit Hilfe des *Satzes über untere Multiplikativität* (Seite 113) die erheblich vereinfachte Berechnung des Legendre-Symbols.
- iii) Am Schluss des Ausblicks auf Seite 162 wurde darauf hingewiesen, dass alle leistungsfähigen Primzahltests und Faktorisierungsalgorithmen anstelle der natürlichen Zahlen höhere mathematische Strukturen wie zum Beispiel Klassengruppen oder Zahlkörper verwenden.

Denkt man sich den zunehmenden Verallgemeinerungsgrad von i), ii) und iii) weiter fortgesetzt, so kommt man schließlich zu der gegenwärtig dominierenden Strategie der forschenden Mathematiker, die oft ihren SchülerInnen raten: “Be wise, generalize!”. Seit mehr als zweihundert Jahren sind die meisten Lösungen von bedeutenden mathematischen Problemen durch Verallgemeinerungen der zugrunde liegenden Theorien gefunden worden. Ein besonders prägnantes Beispiel ist die Lösung des Problems von FERMAT durch WILES (siehe Seite 15).

Mit den folgenden vier Problemen versuchen wir, die Vielfalt der Einsatzmöglichkeiten dieser Strategie anzudeuten. Das erste Beispiel schließt an Problem 1.12.1 aus [13] an.

### Problem 67

Bestimmen Sie eine geschlossene Form von  $\sum_{k=1}^n k2^{-k}$  für jedes  $n \in \mathbb{N}_1$ .

Die Suche nach einer ähnlichen Summe, für die wir eine geschlossene Form kennen, führt zur *geometrischen Summe*

$$(6.9) \quad \sum_{k=0}^n x^k = \frac{1 - x^{n+1}}{1 - x} \text{ für jedes } x \in \mathbb{R} \setminus \{1\} \text{ und für alle } n \in \mathbb{N}.$$

Die Variable  $x$  erlaubt hier die Anwendung von Methoden der Analysis. In unserem Falle ergibt Differentiation

$$\sum_{k=1}^n kx^{k-1} = \frac{1 - (n+1)x^n + nx^{n+1}}{(1-x)^2}.$$

Multiplikation beider Seiten mit  $x$  und Einsetzen von  $x = \frac{1}{2}$  liefert dann die gesuchte Darstellung

$$\sum_{k=1}^n k2^{-k} = 2 - \frac{n+2}{2^n} \text{ für jedes } n \in \mathbb{N}.$$

Mit wiederholter Differentiation und durch Linearkombination der eventuell mit  $x$ -Potenzen multiplizierten Ergebnisse erhält man auch für alle Summen der Form  $\sum_{k=0}^n P(k) a^k$  mit einem Polynom  $P$ , dessen Koeffizienten rationale Zahlen sind, und mit  $a \in \mathbb{Q}$  eine geschlossene Form mit Werten aus  $\mathbb{Q}$ , sodass diese Summanden ein *Signal* für die Anwendung der geometrischen Summe bilden.

Eine zweite Klasse von Summen mit einer geschlossenen “rationalen” Form ergibt sich durch Einsetzen rationaler Zahlen in Polynome, die durch Differentiation oder Integration aus der *Binomialformel* (3.23) entstehen, wobei die *Binomialkoeffizienten* als *Signal* anzusehen sind. Werden die Binomialkoeffizienten durch die Summendarstellung (3.23) definiert, so erhält man durch Differentiation und *Koeffizientenvergleich* die Rekursionsformel

$$\binom{n}{k} = \frac{n}{k} \binom{n-1}{k-1} \text{ für alle } n \in \mathbb{N}_1 \text{ und jedes } k \in \mathcal{I}_n,$$

mit der sich die explizite Darstellung in der Fußnote auf Seite 65 genetisch herleiten lässt. Wegen des Zusammenhangs mit der Verallgemeinerungsstrategie werden wir auf zwei Arten des Koeffizientenvergleichs am Schluss dieses Unterabschnitts ausführlicher eingehen.

Das folgende Problem 2.4.3 aus [13] stellt ein Beispiel für die Anwendung der Verallgemeinerungsstrategie bei Beweisen mit vollständiger Induktion dar. Manchmal ist es nämlich zweckmäßig, den Induktionsschritt für eine allgemeinere Aussage als die vorliegende durchzuführen.

**Problem 68**

Es sei  $(f_n)_n$  die in Aufgabe 2.1 durch  $f_1 := 1$ ,  $f_2 := 1$  und  $f_{n+2} := f_{n+1} + f_n$  für jedes  $n \in \mathbb{N}_1$  definierte *Fibonacci-Folge*. Beweisen Sie, dass  $f_m^2 + f_{m+1}^2 = f_{2m+1}$  für alle  $m \in \mathbb{N}_1$  gilt.

Setzen wir  $\mathcal{M} := \{k \in \mathbb{N}_1 ; f_k^2 + f_{k+1}^2 = f_{2k+1}\}$ , so ist  $1 \in \mathcal{M}$ , und für  $n \in \mathcal{M}$  folgt als Ansatz des Induktionsschritts

$$\begin{aligned} f_{n+1}^2 + f_{n+2}^2 &= f_{n+1}^2 + (f_n + f_{n+1})^2 \\ &= (f_{n+1}^2 + f_n^2) + 2f_n f_{n+1} + f_{n+1}^2 \\ &= f_{2n+1} + (2f_n f_{n+1} + f_{n+1}^2). \end{aligned}$$

Der Beweis könnte also abgeschlossen werden, wenn

$$(6.10) \quad 2f_m f_{m+1} + f_{m+1}^2 = f_{2m+2} \text{ für alle } m \in \mathbb{N}_1$$

bekannt wäre. Der Versuch, diese Aussage mit vollständiger Induktion zu beweisen, führt aber wieder auf die ursprüngliche Gleichung. Zur Lösung der dadurch entstehenden Schwierigkeit werden in [13] die beiden Aussagen etwas umständlich miteinander “gekoppelt”. Das lässt sich vermeiden, wenn man beachtet, dass (6.10) zu

$$(6.11) \quad f_m f_{m+1} + f_{m+1} f_{m+2} = f_{2m+2} \text{ für alle } m \in \mathbb{N}_1$$

äquivalent ist; denn nun kann vermutet werden, dass die allgemeinere Aussage

$$(6.12) \quad f_m f_{n-1} + f_{m+1} f_n = f_{m+n} \text{ für alle } (m, n) \in \mathbb{N}_1 \times \mathbb{N}_2$$

gilt, die die ursprüngliche Gleichung und (6.11) als Spezialfälle für  $n = m + 1$  und  $n = m + 2$  enthält. Für (6.12) verläuft der folgende Induktionsbeweis ohne Probleme.

Setzen wir  $\mathcal{M}_n := \{k \in \mathbb{N}_1 ; f_k f_{n-1} + f_{k+1} f_n = f_{k+n}\}$  für festes  $n \in \mathbb{N}_2$ , so gilt  $\{1, 2\} \subset \mathcal{M}_n$  wegen  $f_{n+1} = f_1 f_{n-1} + f_2 f_n$  und  $f_{n+2} = f_{n+1} + f_n = f_{n-1} + 2f_n = f_2 f_{n-1} + f_3 f_n$ . Aus  $\{m-1, m\} \subset \mathcal{M}_n$  mit  $m \in \mathbb{N}_2$  folgt

$$\begin{aligned} f_{m+1+n} &= f_{m-1+n} + f_{m+n} \\ &= (f_{m-1} f_{n-1} + f_m f_n) + (f_m f_{n-1} + f_{m+1} f_n) \\ &= f_{m+1} f_{n-1} + f_{m+2} f_n, \end{aligned}$$

sodass auch  $m+1 \in \mathcal{M}_n$  ist, woraus sich  $\mathcal{M}_n = \mathbb{N}_1$  ergibt.

Das dritte Beispiel belegt noch einmal die im Anschluss an *Problem 63* erwähnten “Vorteile, die sich ergeben, wenn man ein Problem nicht nur löst, sondern aus der Lösung auch Lehren zieht”. Hier ist das Ziel die Verallgemeinerung des Problems selbst, um Problemtypen oder “Problemketten” zu erkennen.

### Problem 69

Suchen Sie unendlich viele Verallgemeinerungen von *Problem 63*.

Betrachten wir die Herleitung von (6.5), so bietet es sich an, die Zahl 7 in  $7x^2 + y^2$  und in  $y_{n+1} = \frac{1}{2}(-7x_n + y_n)$  durch  $a \in \mathbb{N}_1$  zu ersetzen und festzustellen, unter welchen Bedingungen sich bei dem Übergang von  $n$  zu  $n + 1$  ein nur von  $a$  abhängiger Faktor abspalten lässt. Für

$$x_{n+1} = \frac{1}{2}(x_n + y_n) \quad \text{und} \quad y_{n+1} = \frac{1}{2}(-ax_n + y_n)$$

ist also zu untersuchen, wann  $ax_{n+1}^2 + y_{n+1}^2$  ein ganzzahliges Vielfaches von  $ax_n^2 + y_n^2$  darstellt. Durch Einsetzen folgt

$$\begin{aligned} ax_{n+1}^2 + y_{n+1}^2 &= \frac{1}{4} (ax_n^2 + 2ax_ny_n + ay_n^2 + a^2x_n^2 - 2ax_ny_n + y_n^2) \\ &= b(ax_n^2 + y_n^2) \quad \text{mit } b := \frac{1}{4}(a + 1). \end{aligned}$$

Damit sind höchstens diejenigen  $a \in \mathbb{N}_1$  geeignet, für die  $a \equiv 3 \pmod{4}$  gilt. Setzen wir nun  $x_1 := 1$  und  $y_1 := 1$ , so erhalten wir  $ax_1^2 + y_1^2 = a + 1 = 4b$  und  $x_2 = 1$ ,  $y_2 = 1 - 2b$ . Analog zur Herleitung von (6.6) finden wir

$$x_{n+1} = x_n - bx_{n-1} \quad \text{und} \quad y_{n+1} = y_n - by_{n-1} \quad \text{für alle } n \in \mathbb{N}_2.$$

Damit ist einerseits  $\text{ggT}(x_n, b) = \text{ggT}(y_n, b) = 1$  für jedes  $n \in \mathbb{N}_1$ , und andererseits sind alle  $x_n$  und  $y_n$  ungerade, wenn  $a \equiv 7 \pmod{8}$  gilt. Daraus folgt wegen  $\text{ggT}(x_n, y_n) \mid 4b^n$ , dass  $x_n$  und  $y_n$  teilerfremd sind. Vollständige Induktion ergibt dann die folgenden Verallgemeinerungen von *Problem 63*:

Ist  $a \in \mathbb{N}_1$  mit  $a \equiv 7 \pmod{8}$ , so gibt es zu jedem  $n \in \mathbb{N}_1$  ein Paar  $(x, y) \in \mathbb{N}_1^2$  mit  $\text{ggT}(x, y) = 1$ , sodass  $4\left(\frac{a+1}{4}\right)^n = ax^2 + y^2$  gilt.

Im Anschluss an die *Probleme 65 und 67* haben wir die *Methode des Koeffizientenvergleichs* bei Polynomen erwähnt. Sie lässt sich durch den folgenden *Koeffizientenvergleichssatz* der linearen Algebra begründen ([15], Seite 65):

Sind  $P(x) = c_0 + c_1x + \cdots + c_nx^n$  und  $Q(x) = b_0 + b_1x + \cdots + b_mx^m$  mit  $0 \leq m \leq n$  Polynome, deren Werte an mehr als  $n$  verschiedenen Stellen übereinstimmen, so gilt  $b_i = c_i$  für  $i = 0, \dots, m$  und  $c_i = 0$  für  $i = m + 1, \dots, n$ , falls  $n > m$  ist.

In der reellen Analysis wird ein entsprechender Satz unter der stärkeren Voraussetzung bewiesen, dass die beiden Polynome für alle Argumente  $x$  übereinstimmen. Der einfache indirekte Beweis mit Abschätzungen lässt sich auf Potenzreihenfunktionen übertragen:

Stellen  $F := \left( x \rightarrow \sum_{k=0}^{\infty} a_k x^k, [-c, c] \right)$  und  $G := \left( x \rightarrow \sum_{k=0}^{\infty} b_k x^k, [-c, c] \right)$  mit  $c \in \mathbb{R}^+$  Potenzreihenfunktionen dar, die in  $[-c, c]$  definiert sind und die  $F(x) = G(x)$  für alle  $x \in [-c, c]$  erfüllen, so gilt  $a_k = b_k$  für jedes  $k \in \mathbb{N}$ .

Als letztes Beispiel für die Verallgemeinerungsstrategie suchen wir mit Hilfe dieses Satzes eine dritte Eigenschaft der Lösungen von *Problem 63*.

### Problem 70

Bestimmen Sie jeweils eine geschlossene Form für die Glieder der Folgen  $(x_{n+3})_{n \in \mathbb{N}}$  und  $(y_{n+3})_{n \in \mathbb{N}}$ , die bei der Lösung von *Problem 63* auftreten.

Wir benutzen die *Methode der erzeugenden Funktionen*, bei der die Glieder der zu untersuchenden Folge als Koeffizienten einer Potenzreihe gewählt werden, wobei der Konvergenzbereich zunächst keine Rolle spielt. Wir setzen also

$$f(z) := \sum_{k=3}^{\infty} x_k z^k \quad \text{und} \quad g(z) := \sum_{k=3}^{\infty} y_k z^k$$

und erhalten mit (6.6)

$$\sum_{k=3}^{\infty} x_{k+2} z^k = \sum_{k=3}^{\infty} x_{k+1} z^k - 2 \sum_{k=3}^{\infty} x_k z^k.$$

Multiplikation aller Summen mit  $z^2$  und Transformation der ersten beiden Summationsvariablen ergibt

$$\sum_{k=5}^{\infty} x_k z^k = z \sum_{k=4}^{\infty} x_k z^k - 2z^2 \sum_{k=3}^{\infty} x_k z^k.$$

Nach Einführung von  $f(z)$  folgt

$$f(z) (1 - z + 2z^2) = x_3 z^3 + (x_4 - x_3) z^4.$$

Entsprechend gewinnt man

$$g(z) (1 - z + 2z^2) = y_3 z^3 + (y_4 - y_3) z^4.$$

Wegen  $x_3 = x_4 = y_3 = 1$  und  $y_4 = -3$  erhalten wir also

$$f(z) = \frac{z^3}{1 - z + 2z^2} \text{ und } g(z) = \frac{z^3 - 4z^4}{1 - z + 2z^2}.$$

Mit  $\alpha := \frac{1}{2} + \frac{1}{2}\sqrt{-7}$  und  $\beta := \frac{1}{2} - \frac{1}{2}\sqrt{-7}$  ergibt *Partialbruchzerlegung*

$$f(z) = \frac{z^3}{\sqrt{-7}} \left( \frac{\alpha}{1 - \alpha z} - \frac{\beta}{1 - \beta z} \right) \text{ und } g(z) = z^3 \left( \frac{\alpha}{1 - \alpha z} + \frac{\beta}{1 - \beta z} \right).$$

Durch Entwicklung der Brüche als *geometrische Reihen* folgt

$$f(z) = \frac{1}{\sqrt{-7}} \sum_{k=0}^{\infty} (\alpha^{k+1} - \beta^{k+1}) z^{k+3} \text{ und } g(z) = \sum_{k=0}^{\infty} (\alpha^{k+1} + \beta^{k+1}) z^{k+3},$$

sodass wir durch Koeffizientenvergleich

$$x_{k+2} = \frac{1}{\sqrt{-7}} (\alpha^k - \beta^k) \text{ und } y_{k+2} = \alpha^k + \beta^k \text{ für jedes } k \in \mathbb{N}_1$$

erhalten. Da die geometrische Reihe  $\sum_{k=0}^{\infty} z^k$  den Konvergenzradius 1 hat, kann

bei der Anwendung des obigen Satzes über Potenzreihenfunktionen die Zahl  $c$  zwischen 0 und  $\frac{1}{\sqrt{2}}$  gewählt werden, weil  $\frac{1}{|\alpha|} = \frac{1}{|\beta|} = \frac{1}{\sqrt{2}}$  gilt.

Nachdem wir *Problem 63* durch Zulassen von negativen ganzen Zahlen gelöst haben, treten nun sogar komplexe Zahlen in den geschlossenen Formen auf. Entwickelt man  $\alpha^k$  und  $\beta^k$  mit Hilfe der *binomischen Formel*, so ergeben sich für  $x_{k+2}$  und  $y_{k+2}$  rationale Summen, die wir aber nicht als “geschlossen” ansehen.

Obwohl die Verallgemeinerungsstrategie sehr leistungsfähig ist, kann sie in unserer Sammlung nur bei den Problemen 11, 13 und 52 direkt eingesetzt werden. Bei Problem 11 ergibt sich dieses aus der Fragestellung, und bei den beiden anderen (und eventuell weiteren) Problemen ist die Verallgemeinerung im Rahmen der *Erkundungsstrategie* sinnvoll. Ihr besonderer Nutzen liegt also vor allem im Bereich der mathematischen Forschung. Wertvoll ist sie aber auch bei der eigenständigen Vertiefung - wie bei den Problemen 69 und 70.

## Rückwärtsstrategie

Bei der Lösung von *Problem 1* (Seite 31 ff.) wurde diese Strategie als eine der ältesten Problemlösemethoden eingeführt. Typisch für dieses Beispiel ist eine Sequenz von Aussagen, bei denen die jeweils nächste eine Antwort auf die Frage ist: “Woraus könnte die vorliegende Aussage folgen?” Ähnlich tritt bei dem Beweis des *Satzes über das Eratosthenes-Sieb* (Seite 66) eine “Gleichungskette” auf, bei der der strukturell kompliziertere Term der nachzuweisenden Gleichung am Anfang steht.

Das folgende Beispiel ist der “Ausschließungsteil” von Problem 7.4.6 in [13], wo mit Hilfe der *Modifizierungsstrategie* alle  $n \in \mathbb{N}_2$  bestimmt werden, für die  $\sum_{j=3}^{n+2} j^n = (n+3)^n$  gilt. Für  $n \in \{2, 3\}$  zeigt Einsetzen das Erfülltsein der Gleichung, während für  $n \in \{4, 5\}$  Ungleichheit vorliegt, weil die linke Seite modulo 2 zu  $n$  und die rechte zu  $n+1$  kongruent ist.

### Problem 71

Beweisen Sie, dass  $\sum_{j=3}^{n+2} j^n < (n+3)^n$  für alle  $n \in \mathbb{N}_6$  gilt.

Da die Anwendung der *Binomialformel* (3.23) auf der rechten Seite Summanden ergibt, die nicht mit denen auf der linken Seite vergleichbar sind, nutzen wir die Übereinstimmung aller Exponenten für eine “Normierung”, indem wir beide Seiten durch  $(n+3)^n$  teilen und die Summanden nach abnehmender Größe anordnen:

$$1 > \sum_{j=3}^{n+2} \left(\frac{j}{n+3}\right)^n = \sum_{k=1}^n \left(1 - \frac{k}{n+3}\right)^n.$$

Berechnen wir für  $n = 6$  und  $n = 7$  die Summanden, so erkennen wir, dass bei  $n = 6$  der  $k$ -te Summand für  $k \in \mathcal{I}_6$  kleiner als  $\frac{1}{2^k}$  ist und dass die entsprechenden Summanden bei  $n = 7$  noch kleiner werden. Damit würde sich die gesuchte Abschätzung ergeben, wenn wir zeigen könnten, dass

$$(6.13) \quad \left(1 - \frac{k}{n+3}\right)^n < \frac{1}{2^k} \text{ für jedes } n \in \mathbb{N}_6 \text{ und alle } k \in \mathcal{I}_n$$

gilt, weil dann mit Hilfe der *geometrischen Summe* (6.9) für  $x = \frac{1}{2}$  folgt, dass

$$\sum_{k=1}^n \left(1 - \frac{k}{n+3}\right)^n < \sum_{k=1}^n \frac{1}{2^k} = \frac{1 - \frac{1}{2^{n+1}}}{1 - \frac{1}{2}} - 1 < \frac{1}{1 - \frac{1}{2}} - 1 = 1$$

erfüllt ist.

Da die rechte Seite von (6.13) eine  $k$ -te Potenz ist, wäre es günstig, wenn wir  $1 - \frac{k}{n+3}$  nach oben durch eine  $k$ -te Potenz abschätzen könnten, deren Basis nicht von  $k$  abhängt. Dann müsste in einem letzten Rückwärtsschritt nur noch gezeigt werden, dass die  $n$ -te Potenz dieser Basis für alle  $n \in \mathbb{N}_6$  kleiner als  $\frac{1}{2}$  ist.

Für  $k = 2$  und  $n \in \mathbb{N}$  erhalten wir durch “quadratische Ergänzung”

$$1 - \frac{2}{n+3} < 1 - \frac{2}{n+3} + \frac{1}{(n+3)^2} = \left(1 - \frac{1}{n+3}\right)^2.$$

Ersetzen wir  $\frac{-1}{n+3}$  durch  $x$  und beachten, dass  $(1+2x)(1+x) = 1+3x+2x^2 \geq 1+3x$  gilt, so ergibt sich  $1+3x \leq (1+x)^3$  als eine weitere Anwendung der *Rückwärtsstrategie*, und wir erkennen, dass die Multiplikation mit  $1+x$  auf beiden Seiten der entsprechenden Ungleichung mit  $k$  anstelle von 3 sogar den Induktionsschritt für den Beweis der *Bernoullischen Ungleichung*

$$(6.14) \quad 1 + kx \leq (1+x)^k \text{ für alle } k \in \mathbb{N} \text{ und für jedes } x \in \mathbb{R} \text{ mit } x \geq -1$$

liefert.

Damit haben wir in (6.13)

$$\left(1 - \frac{k}{n+3}\right)^n \leq \left(1 - \frac{1}{n+3}\right)^{kn} = \left(\left(1 - \frac{1}{n+3}\right)^n\right)^k \text{ für alle } n \in \mathbb{N}_1 \text{ und } k \in \mathcal{I}_n.$$

Wegen  $\left(1 - \frac{1}{9}\right)^6 = 0,49327\dots < \frac{1}{2}$  genügt es nun zu zeigen, dass die Folge

$$\left(\left(1 - \frac{1}{n+9}\right)^{n+6}\right)_{n \in \mathbb{N}}$$

monoton fallend ist.

In [13] wird dazu die Ableitung der Funktion  $\left(x \mapsto \left(1 - \frac{1}{x+3}\right)^x, x \geq 6\right)$

betrachtet. Wir verwenden ebenfalls die *Verallgemeinerungsstrategie*, aber mit einer viel einfacheren Methode, die sogar in einem Schulbuch bei der Einführung der Exponentialfunktion gebraucht wird. Da wir  $\left(1 - \frac{1}{n+3}\right)^n \geq \left(1 - \frac{1}{n+4}\right)^{n+1}$

für jedes  $n \in \mathbb{N}_6$  beweisen wollen, versuchen wir herauszufinden, für welche  $x \in \mathbb{R}$  die Polynomrelation

$$(6.15) \quad \left(1 - \frac{x}{n+3}\right)^n \geq \left(1 - \frac{x}{n+4}\right)^{n+1} \text{ für alle } n \in \mathbb{N}_6$$

erfüllt ist. Dazu setzen wir  $f_n(x) := \left(1 - \frac{x}{n+4}\right)^{n+1} \left(1 - \frac{x}{n+3}\right)^{-n}$  für  $n \in \mathbb{N}_1$  und  $x < 4$ . Durch Differentiation erhalten wir dann

$$\begin{aligned} f'_n(x) &= \frac{n+1}{n+4} \left(1 - \frac{x}{n+4}\right)^n \left(1 - \frac{x}{n+3}\right)^{-n} + \frac{n}{n+3} \left(1 - \frac{x}{n+4}\right)^{n+1} \left(1 - \frac{x}{n+3}\right)^{-n-1} \\ &= \left(1 - \frac{x}{n+4}\right)^n \left(1 - \frac{x}{n+3}\right)^{-n-1} \frac{x-3}{(n+3)(n+4)}. \end{aligned}$$

Damit gilt  $f'_n(x) \leq 0$  für jedes  $n \in \mathbb{N}_1$  und alle  $x \leq 3$ . Wegen  $f_n(0) = 1$  ergibt der *Schrankensatz der (Elementar-) Analysis*<sup>2</sup>

$$f_n(x) \leq 1 \text{ für jedes } n \in \mathbb{N}_1 \text{ und alle } x \in \mathbb{R} \text{ mit } 0 \leq x \leq 3.$$

Also ist (6.15) für alle  $x$  mit  $0 \leq x \leq 3$  gültig, und für  $x = 1$  erhalten wir die Ungleichung des Induktionsschrittes bei dem Nachweis des monotonen Fallens von  $\left( \left( 1 - \frac{1}{n+9} \right)^{n+6} \right)_{n \in \mathbb{N}}$ . Durchlaufen wir nun die vier Rückwärtsschritte in umgekehrter Reihenfolge, so ist die Behauptung von Problem 71 bewiesen.

Bei der *Modifizierungsstrategie* wurde erwähnt, dass sie sich oft mit der *Rückwärtsstrategie* verwenden lässt. Noch enger hängen die *Brückenstrategie* und die *Zurückführungsstrategie* mit der *Rückwärtsstrategie* zusammen. Da sie aber wegen ihrer Leistungsfähigkeit in eigenen Abschnitten behandelt werden, überrascht es nicht, dass die *Rückwärtsstrategie* nur bei den Problemen 22, 34 und 54 in “reiner” Form zu gebrauchen ist. Als *Signal* kann häufig die Beobachtung dienen, dass einer schwachen Voraussetzung eine leicht umformbare Aussage gegenübersteht.

## Pólyasche Brückenstrategie

Die Bezeichnung *Brückenstrategie* haben wir im Anschluss an G. PÓLYA [19] eingeführt, nachdem bei dem zweiten Teil des Beweises für den *Satz über gerade vollkommene Zahlen* (Seite 57) abwechselnd *Vorwärtsschließen* und *Rückwärtsstrategie* benutzt wurden. Beim Problemlösen kann das *Vorwärtsschließen* auch mit Vor- oder Nachüberlegungen zu tun haben. So begann die Lösung von *Problem 63* (Seite 195) mit dem Bewusstmachen einer *psychologischen Brückenstrategie*, die auf einer “Lösbarkeitsgarantie mit Schwierigkeitsbeschränkung” bei Mathematikwettbewerben beruht. Auch bei dem folgenden Beispiel, das an Problem 2.2.1 aus [13] anschließt, ist das *Vorwärtsschließen* eher psychologischer Art, weil es nach der Anwendung der *Rückwärtsstrategie* zum Finden eines Induktionsschrittes zu einer **vertieften Einsicht** in die bereits bewiesene Aussage führt.

### Problem 72

Zeigen Sie, dass  $s(n) := \frac{1}{5}n^5 + \frac{1}{2}n^4 + \frac{1}{3}n^3 - \frac{1}{30}n \in \mathbb{N}$  für jedes  $n \in \mathbb{N}$  gilt, und stellen Sie  $s(n)$  als Linearkombination von Binomialkoeffizienten dar.

<sup>2</sup> Ist  $(x \mapsto f(x), x \in \mathcal{A})$  (elementar) differenzierbar mit  $s \leq f'(x)$  bzw.  $f'(x) \leq S$  für jedes  $x \in \mathcal{A}$ , so gilt  $s \leq \frac{f(u)-f(v)}{u-v}$  bzw.  $\frac{f(u)-f(v)}{u-v} \leq S$  für alle  $u, v \in \mathcal{A}$  mit  $u \neq v$ .

Setzen wir für einen Induktionsbeweis  $\mathcal{M} := \{k \in \mathbb{N}; s(k) \in \mathbb{N}\}$ , so gilt offensichtlich  $0 \in \mathcal{M}$ . Aber auf den ersten Blick ist es nicht ganz einfach, aus  $m \in \mathcal{M}$  auf  $m+1 \in \mathcal{M}$  zu schließen. Hier hilft die *Rückwärtsstrategie*, indem wir  $s(m+1)$  durch  $s(m)$  ausdrücken:

$$\begin{aligned} s(m+1) &= \frac{1}{5}(m+1)^5 + \frac{1}{2}(m+1)^4 + \frac{1}{3}(m+1)^3 - \frac{1}{30}(m+1) \\ &= \frac{1}{5}(m^5 + 5m^4 + 10m^3 + 10m^2 + 5m + 1) + \frac{1}{2}(m^4 + 4m^3 + 6m^2 + 4m + 1) \\ &\quad + \frac{1}{3}(m^3 + 3m^2 + 3m + 1) - \frac{1}{30}(m+1) \\ &= s(m) + m^4 + 2m^3 + 2m^2 + m + 2m^3 + 3m^2 + 2m + m^2 + m + 1. \end{aligned}$$

Da  $s(m) \in \mathbb{N}$  nach Induktionsvoraussetzung gilt und da die weiteren Summanden natürliche Zahlen oder 0 darstellen, ist auch  $s(m+1) \in \mathbb{N}$ . Mit  $m+1 \in \mathcal{M}$  ergibt also der *Induktionssatz* (Seite 12) die Lösung des ersten Teils.

Fügen wir der Gleichungskette für  $s(m+1)$  noch eine Zeile mit der Zusammenfassung der Summanden hinzu, so erkennen wir, dass wir zu früh aufgehört haben:

$$s(m+1) = s(m) + m^4 + 4m^3 + 6m^2 + 4m + 1 = s(m) + (m+1)^4.$$

Denn nun erhalten wir mit vollständiger Induktion die überraschende Darstellung

$$(6.16) \quad s(n) = \sum_{k=0}^n k^4 \text{ für jedes } n \in \mathbb{N},$$

aus der natürlich auch  $s(n) \in \mathbb{N}$  folgt.

Bei der rechten Seite von (6.16) handelt es sich um eine *Potenzsumme*, nämlich um die Summe der ersten  $n$  vierten Potenzen. Wegen der eigenartigen rationalen Koeffizienten in der vorgegebenen Polynomdarstellung von  $s(n)$  liegt es nahe, weitere Potenzsummen

$$P_m(n) := \sum_{k=0}^n k^m \text{ mit } m, n \in \mathbb{N}$$

zu berechnen, um eine Gesetzmäßigkeit zu finden.

Neben  $P_4(n) = s(n)$  sind  $P_0(n) = n+1$  und  $P_1(n) = \frac{1}{2}n^2 + \frac{1}{2}n$  schon bekannt. Wir erhalten eine Rekursionsformel für  $P_m(n)$ , weil man die Differenz  $P_{m+1}(n) - P_m(n) = (n+1)^{m+1}$  als Linearkombination von Potenzsummen  $P_i(n)$  mit  $i \in \mathcal{A}_{m+1}$  schreiben kann:

$$(n+1)^{m+1} = \sum_{k=0}^n ((k+1)^{m+1} - k^{m+1}) = \sum_{k=0}^n \sum_{i=0}^m \binom{m+1}{i} k^i = \sum_{i=0}^m \binom{m+1}{i} P_i(n).$$

Damit lassen sich zwar weitere Potenzsummen wie

$$P_2(n) = \frac{1}{3}n^3 + \frac{1}{2}n^2 + \frac{1}{6}n \text{ und } P_3(n) = \frac{1}{4}n^4 + \frac{1}{2}n^3 + \frac{1}{4}n^2$$

berechnen. Aber wir gewinnen keine Einsicht in die Struktur der Koeffizienten.

Deshalb versuchen wir die *Methode der erzeugenden Funktionen* (Seite 207) so anzuwenden, dass sich die Potenzen  $k^m$  mit den Potenzen der Reihenentwicklung der Exponentialfunktion verbinden lassen, wobei  $0! := 1$  ist:

$$\begin{aligned} R_n(x) &:= \sum_{m=0}^{\infty} P_m(n) \frac{x^m}{m!} = \sum_{m=0}^{\infty} \left( \sum_{k=0}^n k^m \right) \frac{x^m}{m!} \\ &= \sum_{k=0}^n \left( \sum_{m=0}^{\infty} \frac{1}{m!} (kx)^m \right) = \sum_{k=0}^n (e^x)^k \\ &= \frac{e^{(n+1)x} - 1}{e^x - 1} = \frac{e^{(n+1)x} - 1}{x} \frac{x}{e^x - 1}, \end{aligned}$$

wobei *Sätze der Analysis* die Vertauschung der Summanden, die stetige Ergänzung für  $x = 0$  und im Folgenden die Multiplikation von Potenzreihen ermöglichen.

Mit Hilfe der Exponentialreihe erhalten wir für den ersten Bruch die Reihenentwicklung

$$(6.17) \quad \frac{e^{(n+1)x} - 1}{x} = \sum_{i=0}^{\infty} \frac{(n+1)^{i+1}}{i+1} \frac{x^i}{i!}.$$

Der zweite Bruch definiert als erzeugende Funktion durch seine (für  $|x| < 2\pi$  konvergente) Reihenentwicklung

$$(6.18) \quad \frac{x}{e^x - 1} =: \sum_{j=0}^{\infty} B_j \frac{x^j}{j!}$$

eine Folge  $(B_j)_{j \in \mathbb{N}}$ , deren Glieder  $B_j$  nach JAKOB BERNOULLI<sup>3</sup> *Bernoullische Zahlen* heißen. Sie spielen in vielen Teilen der Mathematik eine Rolle.

Durch Multiplikation der Potenzreihen aus (6.17) und (6.18) folgt

$$R_n(x) = \sum_{m=0}^{\infty} \left( \sum_{i=0}^m B_{m-i} \binom{m}{i} \frac{(n+1)^{i+1}}{i+1} \right) \frac{x^m}{m!},$$

und Koeffizientenvergleich gemäß dem Potenzreihenvergleichssatz auf Seite 207 ergibt

$$(6.19) \quad P_m(n) = \sum_{i=0}^m B_{m-i} \frac{1}{i+1} \binom{m}{i} (n+1)^{i+1} \text{ für alle } m, n \in \mathbb{N}.$$

---

<sup>3</sup> JAKOB BERNOULLI (1654-1705) war Mathematiker und Physiker in Basel.

Speziell für  $n = 0$  erhalten wir die Rekursionsgleichungen

$$(6.20) \quad B_m = -\frac{1}{m+1} \sum_{i=1}^m \binom{m+1}{i+1} B_{m-i} \text{ für } m \in \mathbb{N}_1 \text{ und mit } B_0 = 1.$$

Damit können wir  $B_m$  für kleine  $m$  berechnen:

$$B_1 = -\frac{1}{2}, \quad B_2 = \frac{1}{6}, \quad B_3 = 0, \quad B_4 = -\frac{1}{30}, \quad B_5 = 0, \quad B_6 = \frac{1}{42}.$$

Der zweite Teil von *Problem 72* lässt sich mit der normalen *Brückenstrategie* lösen. Zunächst versuchen wir, mit der *Rückwärtsstrategie* zu klären, ob sich Binomialkoeffizienten als Summe von Binomialkoeffizienten mit einem Parameter  $k \in \mathcal{A}_{n+1}$  darstellen lassen. Dabei hilft uns die Idee der Differenzbildung, die wir bei der obigen Herleitung der Rekursionsformel für  $P_m(n)$  verwendet haben. Aus der Darstellung

$$(6.21) \quad \binom{k}{i} = \begin{cases} 1 & \text{für } i = 0 \text{ und } k \in \mathbb{N}, \\ \frac{1}{i!} k(k-1) \cdots (k-i+1) & \text{für } i \in \mathbb{N}_1 \text{ und } k \in \mathbb{N} \end{cases}$$

folgt unmittelbar  $\binom{k}{i} = \binom{k+1}{i+1} - \binom{k}{i+1}$ . Wird auf beiden Seiten summiert, so heben sich auf der rechten Seite aufeinanderfolgende Terme weg, und wegen  $\binom{0}{i+1} = 0$  erhalten wir

$$(6.22) \quad \sum_{k=0}^n \binom{k}{i} = \binom{n+1}{i+1} \text{ für alle } i, n \in \mathbb{N}.$$

Nun brauchen wir nur noch die Potenzen  $k^m$  als Linearkombinationen von Binomialkoeffizienten darzustellen. Schon für  $m \leq 3$  können wir das Bildungsgesetz erkennen:

$$k^2 = (k-1+1)k = (k-1)k + k = \binom{k}{2}2! + \binom{k}{1}1! \text{ und}$$

$$\begin{aligned} k^3 &= k \cdot k^2 = k \binom{k}{2}2! + k \binom{k}{1}1! = (k-2+2) \binom{k}{2}2! + (k-1+1) \binom{k}{1}1! \\ &= \binom{k}{3}3! + 2 \binom{k}{2}2! + \binom{k}{2}2! + \binom{k}{1}1! = \binom{k}{3}3! + 3 \binom{k}{2}2! + \binom{k}{1}1!. \end{aligned}$$

Einerseits erfolgt der Übergang von  $m$  zu  $m+1$  durch Multiplikation beider Seiten mit  $k$ . Andererseits ist auf der rechten Seite jeder Binomialkoeffizient  $\binom{k}{i}$  mit einem Faktor  $i!$  versehen, sodass  $\binom{k}{i}i!$  wegen (6.21) sogar ein Polynom in  $k$  mit ganzen Koeffizienten darstellt, das sich bei Multiplikation mit  $k$  wieder als ganzzahlige Linearkombination von zwei solchen Polynomen schreiben lässt:

$$(6.23) \quad k \binom{k}{i}i! = (k-i+i) \binom{k}{i}i! = \binom{k}{i+1}(i+1)! + i \binom{k}{i}i!.$$

Definieren wir also für  $m \in \mathbb{N}_1$  und  $i \in \mathcal{I}_m$  die Zahlen  $S(m, i)$  rekursiv durch

$$S(m, 1) = S(m, m) := 1, \quad S(m+1, i) := S(m, i-1) + i S(m, i), \quad i \in \mathcal{I}_m \setminus \{1\},$$

so ergibt vollständige Induktion mit dem oben beschriebenen Induktionsschritt

$$(6.24) \quad k^m = \sum_{i=1}^m S(m, i) \binom{k}{i} i! \text{ für alle } k \in \mathbb{N} \text{ und jedes } m \in \mathbb{N}_1.$$

Die natürlichen Zahlen  $S(m, i)$  heißen nach J. STIRLING<sup>4</sup> *Stirlingsche Zahlen zweiter Art*. Ähnlich wie die Binomialkoeffizienten entstammen sie der Kombinatorik. Mit Hilfe von (6.24) erhalten wir nun

$$P_m(n) = \sum_{k=0}^n \sum_{i=1}^m S(m, i) \binom{k}{i} i! = \sum_{i=1}^m S(m, i) i! \sum_{k=0}^n \binom{k}{i}$$

und mit (6.22) folgt

$$(6.25) \quad P_m(n) = \sum_{i=1}^m S(m, i) i! \binom{n+1}{i+1}.$$

In [5] (Seite 95) wird hierfür ein “kombinatorischer” Beweis skizziert.

Die normale *Brückenstrategie* hilft beim Lösen der Probleme 5, 7, 14, 33, 41, 48, 56 und 59. Die psychologischen Versionen können aber bei der Mehrzahl der Wettbewerbsprobleme im Verlauf der Lösungssuche genutzt werden. Als *Signal* lässt sich hier im Unterschied zur reinen *Rückwärtsstrategie* jeweils auch eine Aussage finden, die durch *Vorwärtsschließen* mit der Aussage des “anderen Ufers” verbindbar erscheint. Häufig kann dieser Findvorgang durch eine Warum-Frage eingeleitet werden.

## Invarianzstrategie

In [5] steht auf der ersten Seite des ersten Kapitels mit dem Titel “Das Invarianzprinzip” der Merkspruch: “Wenn Wiederholungen vorliegen, achte auf das, was sich nicht ändert.” Die Beispiele in [5] und auch in unseren früheren Kapiteln zeigen, dass dafür recht viele Relationen oder Eigenschaften infrage kommen.

Bei dem Beweis des *Kongruenzsatzes von Euler* (Seite 99) war es die *Reduziertheit* aller betrachteten Restsysteme, und bei der Einführung des *Jacobi-Symbols* (Seite 111) wurde die *Übereinstimmung von Vorzeichen* genutzt, die mit der sogenannten *Parität* (0 bzw. 1, gerade bzw. ungerade, + bzw. -) zusammenhängen. Der Beweis von E. LANDAU [12] für den *Dreiquadratesatz* (Seite 146) verwendete unter anderem die *Invarianz der Determinante* sowie von *Koeffizientenrelationen*, und der *Satz über Invarianten der Formenklassen* (Seite 154) enthält sogar vier invariante Eigenschaften.

---

<sup>4</sup> JAMES STIRLING (1692-1770) war Mathematiker unter anderem in Venedig.

Wir ergänzen das Beispiel E5 aus dem ersten Kapitel von [5] durch eine “genetische” Lösung.

### Problem 73

Es sei  $((a_n, b_n, c_n, d_n))_{n \in \mathbb{N}}$  eine Folge von Quadrupeln ganzer Zahlen mit  $a_{n+1} = a_n - b_n$ ,  $b_{n+1} = b_n - c_n$ ,  $c_{n+1} = c_n - d_n$  und  $d_{n+1} = d_n - a_n$  für jedes  $n \in \mathbb{N}$ . Zeigen Sie, dass die Folge  $(\max\{|a_n|, |b_n|, |c_n|, |d_n|\})_{n \in \mathbb{N}}$  unbeschränkt ist, wenn die Zahlen  $a_0, b_0, c_0, d_0$  nicht alle gleich sind.

Zur Vorbereitung geben wir drei Invarianten der Folge an, die sich leicht mit Hilfe der *Erkundungsstrategie* finden lassen. Für die Unbeschränktheit der Folge  $(\max\{|a_n|, |b_n|, |c_n|, |d_n|\})_{n \in \mathbb{N}}$  ist es notwendig, dass auch für jedes  $m \in \mathbb{N}_1$  die Zahlen  $a_m, b_m, c_m, d_m$  nicht gleich sind, weil andernfalls  $(a_{m+n}, b_{m+n}, c_{m+n}, d_{m+n}) = (0, 0, 0, 0)$  für alle  $n \in \mathbb{N}_1$  gilt.

Aus den für irgendein  $m \in \mathbb{N}$  erfüllten Gleichungen  $a_{m+1} = b_{m+1}$  und  $c_{m+1} = d_{m+1}$  folgt  $a_m + c_m = 2b_m$  und  $a_m + c_m = 2d_m$ , also  $b_m = d_m$ . Entsprechend ergibt sich  $c_m = a_m$  aus  $b_{m+1} = c_{m+1}$  und  $d_{m+1} = a_{m+1}$ . Kombination von  $c_m = a_m$  und  $a_m + c_m = 2d_m$  liefert schließlich  $a_m = d_m$ . Gilt also  $a_{m+1} = b_{m+1} = c_{m+1} = d_{m+1}$  für ein  $m \in \mathbb{N}$ , so folgt auch  $a_m = b_m = c_m = d_m$ . Als Anwendung der noch zu behandelnden *Abstiegsstrategie* können wir nun schließen, dass die Menge  $\{m \in \mathbb{N}; a_m = b_m = c_m = d_m\}$  kein Minimum besitzt, weil die Zahlen  $a_0, b_0, c_0, d_0$  als nicht gleich vorausgesetzt sind. Aufgrund des *Minimumsatzes* (Seite 11) muss die Menge also leer sein. Die Nichtgleichheit der Zahlen  $a_n, b_n, c_n, d_n$  für jedes  $n \in \mathbb{N}$  ist damit die erste invariante Eigenschaft der Quadrupelfolge. Den Spezialfall

$$(6.26) \quad (a_n, b_n, c_n, d_n) \neq (0, 0, 0, 0) \text{ für alle } n \in \mathbb{N}$$

werden wir später benutzen.

Schon wenige Zahlenbeispiele lassen erkennen, dass gemeinsame Teiler der Quadrupelzahlen eine Rolle spielen. Ist  $t$  ein Teiler von  $\text{ggT}(a_m, b_m, c_m, d_m)$  für irgendein  $m \in \mathbb{N}$ , so ergeben die Linearitätsaussage des *Satzes über Teilbarkeitsregeln* (Seite 18) und vollständige Induktion, dass auch  $t \mid \text{ggT}(a_{m+n}, b_{m+n}, c_{m+n}, d_{m+n})$  für alle  $n \in \mathbb{N}$  gilt. Damit folgt für jedes  $m \in \mathbb{N}$  die zweite invariante Eigenschaft

$$(6.27) \quad \text{ggT}(a_m, b_m, c_m, d_m) \mid \text{ggT}(a_{m+n}, b_{m+n}, c_{m+n}, d_{m+n}) \text{ für alle } n \in \mathbb{N}.$$

Ebenso leicht sieht man, dass  $2 \mid \text{ggT}(a_{n+4}, b_{n+4}, c_{n+4}, d_{n+4})$  für alle  $n \in \mathbb{N}$  erfüllt ist. Wegen (6.27) genügt es,

$$(6.28) \quad 2 \mid \text{ggT}(a_4, b_4, c_4, d_4)$$

zu zeigen. Das geschieht modulo 2 mit Fallunterscheidung. Indem wir  $[\text{mod}(a, 2), \text{mod}(b, 2), \text{mod}(c, 2), \text{mod}(d, 2)]$  anstelle von  $(a, b, c, d)$  schreiben, erhalten wir die Sequenzen  $[1, 0, 0, 0] \rightarrow [1, 0, 0, 1] \rightarrow [1, 0, 1, 0] \rightarrow [1, 1, 1, 1] \rightarrow [0, 0, 0, 0]$  und  $[1, 1, 1, 0] \rightarrow [0, 0, 1, 1]$ . Die Fortsetzung der zweiten Sequenz und die übrigen Fälle ergeben sich durch zyklische Vertauschung.

Eine zahlentheoretische Lösung von *Problem 73* folgt nun zusammen mit (6.26) durch die dritte invariante Eigenschaft

$$(6.29) \quad 2^k \mid \text{ggT}(a_{4k}, b_{4k}, c_{4k}, d_{4k}) \text{ für alle } k \in \mathbb{N}_1,$$

die wir mit vollständiger Induktion beweisen. Dazu sei

$$\mathcal{M} := \{k \in \mathbb{N}_1 ; 2^k \mid \text{ggT}(a_{4k}, b_{4k}, c_{4k}, d_{4k})\}.$$

Wegen (6.28) ist  $1 \in \mathcal{M}$ . Für  $m \in \mathcal{M}$  definieren wir die ganzen Zahlen  $a'_0 := 2^{-m}a_{4m}$ ,  $b'_0 := 2^{-m}b_{4m}$ ,  $c'_0 := 2^{-m}c_{4m}$  und  $d'_0 := 2^{-m}d_{4m}$  sowie für  $n \in \mathcal{A}_3$  rekursiv  $a'_{n+1} := a'_n - b'_n$ ,  $b'_{n+1} := b'_n - c'_n$ ,  $c'_{n+1} := c'_n - d'_n$ ,  $d'_{n+1} := d'_n - a'_n$ . Wegen (6.28) gilt dann  $2 \mid \text{ggT}(a'_4, b'_4, c'_4, d'_4)$ , und mit  $a'_4 = 2^{-m}a_{4m+4}$ ,  $b'_4 = 2^{-m}b_{4m+4}$ ,  $c'_4 = 2^{-m}c_{4m+4}$ ,  $d'_4 = 2^{-m}d_{4m+4}$  folgt  $m + 1 \in \mathcal{M}$ , sodass  $\mathcal{M} = \mathbb{N}_1$  ist.

Um das “genetische” Defizit der kurzen und eleganten Lösung in [5] aufzuzeigen, bringen wir die Übersetzung des ersten Abschnitts: «Es sei  $P_n = (a_n, b_n, c_n, d_n)$  das Quadrupel nach  $n$  Iterationen. Dann haben wir  $a_n + b_n + c_n + d_n = 0$  für  $n \geq 1$ . Wir sehen noch nicht, wie wir diese Invariante nutzen können. Aber eine geometrische Interpretation ist meistens hilfreich. Eine sehr wichtige Funktion für den Punkt  $P_n$  im 4-dimensionalen Raum ist das Quadrat seines Abstands vom Ursprung  $(0, 0, 0, 0)$ , nämlich  $a_n^2 + b_n^2 + c_n^2 + d_n^2$ . Wenn wir zeigen könnten, dass diese Quadratsummen keine obere Schranke haben, wären wir fertig.»

Auf diesen Ansatz können viele ProblemlöserInnen nur kommen, wenn sie entsprechende Vorkenntnisse haben. Dieser Mangel lässt sich mit der *Brückenstrategie* mildern, indem man eine Funktion  $f(u, v, w, x)$  sucht, für die  $(f_n)_{n \in \mathbb{N}}$  mit  $f_n := f(a_n, b_n, c_n, d_n)$  unbeschränkt wächst und bei der sich  $f_{n+1}$  möglichst leicht

zu  $f_n$  in Beziehung setzen lässt. Die einfachste Funktion  $f(u, v, w, x) := u + v + w + x$  kommt wegen der obigen Gleichung

$$(6.30) \quad a_n + b_n + c_n + d_n = 0 \text{ für alle } n \in \mathbb{N}_1$$

nicht infrage. Die naheliegenden Funktionen  $f(u, v, w, x) := \max\{|u|, |v|, |w|, |x|\}$  und  $f(u, v, w, x) := |u| + |v| + |w| + |x|$ , die wegen (6.26) wenigstens positive Glieder  $f_n$  ergeben, erlauben keine günstige Rekursion für  $f_n$ . Als nächste Funktion, deren Positivität zu  $(u, v, w, x) \neq (0, 0, 0, 0)$  äquivalent ist, bietet sich damit  $f(u, v, w, x) := u^2 + v^2 + w^2 + x^2$  an.

Setzen wir  $q_n := a_n^2 + b_n^2 + c_n^2 + d_n^2$ , so gilt zunächst

$$(6.31) \quad \begin{aligned} q_{n+1} &= (a_n - b_n)^2 + (b_n - c_n)^2 + (c_n - d_n)^2 + (d_n - a_n)^2 \\ &= 2q_n - 2(a_nb_n + b_nc_n + c_nd_n + d_na_n). \end{aligned}$$

Als Anwendung der gleich zu behandelnden *Symmetriestrategie* ergänzen wir  $s_n := 2a_nb_n + 2b_nc_n + 2c_nd_n + 2d_na_n$  durch die “fehlenden” acht Produkte  $a_n^2, 2a_nc_n, c_n^2, b_n^2, 2b_nd_n$  und  $d_n^2$ , sodass wir

$$(6.32) \quad s_n + (a_n + c_n)^2 + (b_n + d_n)^2 = (a_n + b_n + c_n + d_n)^2 = 0 \text{ für } n \in \mathbb{N}_1$$

wegen (6.30) erhalten. Durch Addition von (6.31) und (6.32) folgt

$$q_{n+1} = 2q_n + (a_n + c_n)^2 + (b_n + d_n)^2 \geq 2q_n \text{ für jedes } n \in \mathbb{N}_1,$$

und vollständige Induktion ergibt

$$q_n \geq 2^{n-1}q_1 \geq 2^{n-1} \text{ für alle } n \in \mathbb{N}_1.$$

Also ist  $(q_n)_{n \in \mathbb{N}}$  und damit auch  $(\max\{|a_n|, |b_n|, |c_n|, |d_n|\})_{n \in \mathbb{N}}$  unbeschränkt.

Die *Invarianzstrategie* lässt sich beim Lösen der Probleme 13, 50 und 53 einsetzen. Als *Signal* kann die Wiederholungseigenschaft aus dem anfangs zitierten Merkspruch von A. ENGEL dienen.

## Symmetriestrategie

In der Zahlentheorie bedeutet *Symmetrie* meistens wie in der Algebra, dass eine Funktion von mehreren Variablen beim Permutieren der Variablen in sich selbst übergeht. Durch diese Invarianz lässt sich beim Problemlösen manchmal die entscheidende Darstellung finden. Nicht selten kann auch durch eine erkannte oder herbeigeführte Symmetrie die Anzahl der zu untersuchenden Fälle verkleinert werden. Wir wählen als Beispiel Problem 1.6.11 aus [13], weil wir später eine Lösung mit Hilfe der *Klammerungsstrategie* bringen können.

**Problem 74**

Zeigen Sie, dass das Produkt von vier aufeinanderfolgenden Termen einer arithmetischen Progression ganzer Zahlen vermehrt um die vierte Potenz der gemeinsamen Differenz ein Quadrat darstellt.

Bezeichnen wir mit  $a$  die Startzahl, mit  $d$  die Differenz und mit  $x$  die gesuchte Basis, so lautet die Mathematisierung des Problems

$$(6.33) \quad a(a+d)(a+2d)(a+3d) + d^4 = x^2.$$

Nach Ausmultiplizieren des Produkts hat die linke Seite die symmetrische Form  $a^4 + 6a^3d + 11a^2d^2 + 6ad^3 + d^4$ . Versuchen wir deshalb einen symmetrischen Ansatz  $x = a^2 + yad + d^2$ , so folgt  $x^2 = a^4 + 2ya^3d + (y^2 + 2)a^2d^2 + 2yad^3 + d^4$ . Damit ergibt  $y = 3$  die gesuchte Lösung  $x = a^2 + 3ad + d^2$ .

Bei den Problemen 3, 6 und 56 kann die *Symmetriestrategie* verwendet werden. Zwei dieser Probleme lassen sich aber auch anders lösen. Die optische Regelmäßigkeit von Termen stellt ein *Signal* für Symmetrie dar.

**Fallunterscheidungsstrategie**

Diese Strategie tritt beim Problemlösen in natürlicher Weise auf, wenn man Teilprobleme mit verschiedenen Methoden lösen kann. Deshalb werden auch relativ viele Beweise von Sätzen der früheren Kapitel mit Fallunterscheidung geführt. Einige Beispiele sind der zweite Beweis der Eindeutigkeit bei dem *Hauptsatz* (Seite 49), der *Fermatsche Kongruenzsatz* (Seite 99), der *Wilsonsche Fakultätensatz* (Seite 102) und der *Satz über das Euler-Kriterium* (Seite 109). Wir wählen als Ergänzung Problem 1.1.7 aus [13], weil hier die Fallunterscheidung mit der *Erkundungsstrategie* zu kombinieren ist.

**Problem 75**

Für  $k \in \mathbb{N}_1$  seien die Folgen  $(s_{k,n})_{n \in \mathbb{N}_1}$  durch

$$s_{1,n} := n \text{ und } s_{k+1,n} := \begin{cases} s_{k,n} + 1, & \text{wenn } k \mid s_{k,n}, \\ s_{k,n} & \text{sonst,} \end{cases}$$

für alle  $n \in \mathbb{N}_1$  rekursiv definiert. Es sind diejenigen  $k \in \mathbb{N}_2$  zu bestimmen, bei denen  $s_{k,n} = k$  für jedes  $n \in \mathcal{I}_{k-1}$  gilt.

Als Startpunkt für die *Erkundungsstrategie* verwenden wir die folgende Tabelle.

|    |    |    |    |    |    |    |    |    |    |    |
|----|----|----|----|----|----|----|----|----|----|----|
| 1  | 2  | 3  | 4  | 5  | 6  | 7  | 8  | 9  | 10 | 11 |
| 2  | 3  | 4  | 5  | 6  | 7  | 8  | 9  | 10 | 11 | 12 |
| 3  | 3  | 5  | 5  | 7  | 7  | 9  | 9  | 11 | 11 | 13 |
| 4  | 4  | 5  | 5  | 7  | 7  | 10 | 10 | 11 | 11 | 13 |
| 5  | 5  | 5  | 5  | 7  | 7  | 10 | 10 | 11 | 11 | 13 |
| 6  | 6  | 6  | 6  | 7  | 7  | 11 | 11 | 11 | 11 | 13 |
| 7  | 7  | 7  | 7  | 7  | 7  | 11 | 11 | 11 | 11 | 13 |
| 8  | 8  | 8  | 8  | 8  | 8  | 11 | 11 | 11 | 11 | 13 |
| 9  | 9  | 9  | 9  | 9  | 9  | 11 | 11 | 11 | 11 | 13 |
| 10 | 10 | 10 | 10 | 10 | 10 | 11 | 11 | 11 | 11 | 13 |
| 11 | 11 | 11 | 11 | 11 | 11 | 11 | 11 | 11 | 11 | 13 |

Offensichtlich ist  $s_{k,1} = k$  für alle  $k \in \mathbb{N}_1$ , was unmittelbar durch vollständige Induktion gezeigt wird. Deshalb und wegen  $s_{1,n} = n$  für jedes  $n \in \mathbb{N}_1$  enthält die erste Spalte die Zeilenindizes und die erste Zeile die Spaltenindizes der Tabelle.

Es erscheint nicht allzu gewagt, als Antwort auf die Aufforderung des Problems die folgende **Vermutung** aufzustellen:

*Es gilt  $s_{k,n} = k$  für jedes  $n \in \mathcal{I}_{k-1}$  genau dann, wenn  $k$  eine Primzahl ist.*

Wegen der Definition der Folgenglieder müssen zum Finden des aus zwei Fällen bestehenden Beweises die Folgen  $S_n := (s_{k,n})_{k \in \mathbb{N}_1}$ , deren Anfangselemente für  $n \leq 11$  in den Spalten der Tabelle stehen, untersucht werden. Diese Folgen wachsen für jedes  $n \in \mathbb{N}_1$  monoton, weil die Differenz aufeinanderfolgender Glieder 0 oder 1 ist. Da  $s_{k,1} = k$  für alle  $k \in \mathbb{N}_1$  gilt, sei im Folgenden  $n \in \mathbb{N}_2$  fest gewählt.

Charakteristisch sind die ‘‘Sprungstellen’’ von  $S_n$ , die mit bestimmten Teilern der Folgenglieder zusammenhängen. Bei der rekursiven Definition dieser Teilerfolgen  $(t_i)_{i \in \mathbb{N}}$  nutzen wir, dass es wegen des monotonen Wachsens von  $S_n$  zu jedem  $k \in \mathbb{N}_1$  genau ein  $i \in \mathbb{N}$  mit  $s_{k,n} = n + i$  gibt:

$$t_0 := 1 \text{ und } t_{i+1} := \min \{d \in \mathbb{N}_2 ; d > t_i \text{ und } d \mid (n + i + 1)\} \text{ für } i \in \mathbb{N}.$$

Dabei muss mit vollständiger Induktion gezeigt werden, dass  $t_{i+1}$  für jedes  $i \in \mathbb{N}$  erklärt ist. Im Induktionsschritt folgt aus  $t_i \mid (n + i)$ , dass sich der *Minimumsatz* (Seite 11) anwenden lässt, weil die Menge  $\{d \in \mathbb{N}_2 ; d > t_i \text{ und } d \mid (n + i + 1)\}$  wegen  $n + i + 1 > t_i$  nicht leer ist. Ebenfalls mit vollständiger Induktion ergibt sich nun für jedes  $i \in \mathbb{N}$  als Präzisierung der obigen Sprungstellenaussage

$$(6.34) \quad s_{k,n} = n + i \text{ für alle } k \in \mathbb{N}_1 \text{ mit } t_{i-1} < k \leq t_i,$$

wobei  $t_{-1} := 0$  gesetzt wird, damit 0 in der Induktionsmenge  $\mathcal{M} := \{i \in \mathbb{N}; s_{k,n} = n + i \text{ für alle } k \in \mathbb{N}_1 \text{ mit } t_{i-1} < k \leq t_i\}$  liegt, weil  $s_{k,n} = n$  nur für  $k = 1$  gilt. Ist  $j \in \mathcal{M}$  und  $h := t_j$ , so folgt wegen  $s_{h,n} = n + j$  und  $t_j \mid (n + j)$ , dass  $h$  einen Teiler von  $s_{h,n}$  darstellt. Damit ist  $m := t_j + 1$  der kleinste Index mit  $s_{m,n} = n + j + 1$ . Im Falle  $t_{j+1} > t_j + 1$  gilt aufgrund der Minimalteilereigenschaft von  $t_{j+1}$  auch  $s_{k,n} = n + j + 1$  für alle  $k$  mit  $t_j + 1 < k \leq t_{j+1}$ . Also ist  $j + 1 \in \mathcal{M}$ , und der *Induktionssatz* (Seite 12) ergibt  $\mathcal{M} = \mathbb{N}$ .

i) Um den **ersten Fall**, nämlich den “dann”-Fall unserer Vermutung beweisen zu können, benötigen wir noch zwei weitere in der Tabelle erkennbare Eigenschaften der Folgen  $S_n$ . Am auffälligsten ist in  $S_n$  für  $n \in \mathbb{N}_2$  das Vorhandensein eines endlichen “Größerabschnitts” mit  $s_{k,n} > k$  und eines darauf folgenden unendlichen “Gleichbereichs”, in dem  $s_{k,n} = k$  erfüllt ist. Mit vollständiger Induktion kann leicht gezeigt werden, dass aus  $s_{i,n} = i$  für ein  $i \in \mathbb{N}_1$  die Gleichungen

$$(6.35) \quad s_{j,n} = j \text{ für alle } j \in \mathbb{N}_i$$

folgen, weil jeweils  $s_{j+1,n} = j + 1$  wegen  $j \mid s_{j,n}$  gilt.

Also ist für jedes  $n \in \mathbb{N}_2$  die Existenz eines  $g \in \mathbb{N}_1$  mit  $s_{g,n} = g$  nachzuweisen.

Dazu setzen wir  $c_i := \frac{n+i}{t_i}$  für jedes  $i \in \mathbb{N}$ . Wegen  $t_i \mid (n + i)$  gilt  $c_i \in \mathbb{N}_1$  für alle  $i \in \mathbb{N}$ . Ist  $h \in \mathbb{N}$  mit  $c_h > 1$ , so sind  $n + h > t_h$  und  $\frac{n+h+1}{t_h+1} < \frac{n+h}{t_h}$  äquivalent,

womit  $c_{h+1} = \frac{n+h+1}{t_{h+1}} \leq \frac{n+h+1}{t_h+1} < \frac{n+h}{t_h} = c_h$  folgt. Da also  $\{h \in \mathbb{N}; c_h > 1\}$  eine

endliche Menge darstellt, gibt es ein  $m \in \mathbb{N}$  mit  $c_m = 1$ . Damit gilt  $t_m = n + m$ , und wegen (6.34) erhalten wir  $n + m = s_{t_m,n}$ , also  $g = s_{g,n}$  mit  $g := t_m$ .

Jetzt legt die Tabelle die Vermutung nahe, dass  $\min \{k \in \mathbb{N}_1; s_{k,n} = k\} = \min \{p \in \mathbb{P}; p > n\}$  gilt. Diese Annahme erweist sich zwar als falsch, weil zum Beispiel  $s_{27,23} = 27 < 29$  ist. Aber sie lenkt unsere Aufmerksamkeit auf die Zahlen  $q = q(n) := \min \{p \in \mathbb{P}; p > n\}$ , von denen wir leicht zeigen können, dass

$$(6.36) \quad s_{q,n} = q \text{ für jedes } n \in \mathbb{N}_2$$

gilt. Ist  $i \in \mathbb{N}$  der nach (6.34) eindeutig bestimmte Index mit  $s_{t_i,n} = q$ , so folgt  $t_i \mid q$  aufgrund der Definition von  $t_i$ . Da  $s_{1,n} = n < q$  im Falle  $t_i = 1$  gilt, muss  $t_i > 1$  sein. Also ist  $t_i = q$ .

Nun lässt sich der Beweis des ersten Falles rasch abschließen. Ist  $k \in \mathbb{P}$  und  $n \in \mathcal{I}_{k-1}$ , so gilt  $q \leq k$  aufgrund der Definition von  $q$ . Wegen (6.36) und (6.35) folgt  $s_{k,n} = k$  für jedes  $n \in \mathcal{I}_{k-1}$ .

ii) Im **zweiten Fall**, nämlich der “nur dann”-Aussage verleiten die Zahlen unter den Treppenstufen der Tabelle zu der Vermutung, dass  $s_{n+1,n} = q$  für jedes  $n \in \mathbb{N}_2$

mit  $n + 1 \notin \mathbb{P}$  gilt. Spätestens das (kleinste) Gegenbeispiel  $s_{24,23} = 27$  veranlasst uns, die schwächste für den Beweis verwendbare Aussage  $s_{n+1,n} \geq n + 2$  für jedes  $n \in \mathbb{N}_2$  mit  $n + 1 \notin \mathbb{P}$  anzusteuern. Offenbar spielt hier die Sprungstelle von  $n + 1$  nach  $n + 2$  eine Rolle. Wegen  $s_{2,n} = n + 1$  für alle  $n \in \mathbb{N}_1$  und aufgrund der Monotonie von  $S_n$  ist  $s_{k,n} \geq n + 2$  für alle  $k \in \mathbb{N}_2$  mit  $k \geq t_1 + 1$ . Der *Satz über den kleinsten Primteiler* (Seite 47) ergibt  $t_1 = kP(n + 1)$ , sodass  $t_1 + 1 \leq n + 1$  wegen  $n + 1 \notin \mathbb{P}$  gilt. Also folgt  $s_{n+1,n} \geq n + 2$  für jedes  $n \in \mathbb{N}_2$  mit  $n + 1 \notin \mathbb{P}$ .

Da es zahlreiche Möglichkeiten der Fallunterscheidung gibt, bietet sich diese Strategie bei relativ vielen Problemen fast von selbst an. Sinnvoll ist sie sicher bei den Problemen 9, 15, 18, 26, 27, 28, 29, 30, 37, 39, 40, 45, 51, 53, 55, 56, 57, 60 und 61. Neben der “dann und nur dann”- oder “genau dann”-Formulierung, die im obigen Beispiel auftrat, findet man als *Signale* vor allem Aufforderungen, (Teil-) Mengen mit gegebenen Eigenschaften zu bestimmen oder ihre Nichtexistenz nachzuweisen.

## Zurückführungsstrategie

Während bei der *Fallunterscheidungsstrategie* ein Problem in mehrere Teilprobleme zerlegt wird, die sich weitgehend unabhängig voneinander lösen lassen, folgt die Lösung eines Problems mit der *Zurückführungsstrategie* durch Zurückführung auf Spezialfälle, die in [19] (z. B. 1. Band, Seite 170) “führende Spezialfälle” heißen. Im Buchtext ist es bei dem *Satz über den Euklidischen Algorithmus* (Seite 20) der Fall  $c = 1$ , bei dem *Satz über pythagoreische Tripel* (Seite 38) der Fall teilerfremder Komponenten und bei dem *Zweiquadratesatz* (Seite 141) der Primzahlfall.

Das nächste Beispiel betrifft die Folgen  $(\text{mod}(f_n, m))_n$  für jedes  $m \in \mathbb{N}_2$ , wobei  $(f_n)_n$  die in Aufgabe 2.1 definierte und in *Problem 68* behandelte *Fibonacci-Folge* darstellt. Wir zeigen zunächst, dass jede dieser “Restefolgen” rein periodisch ist. Für festes  $m \in \mathbb{N}_2$  und für  $a \in \mathbb{N}_1$  sei  $r(a) := \text{mod}(a, m) = a - m \left\lfloor \frac{a}{m} \right\rfloor$ . Insbesondere sei  $r_n := r(f_n)$ . Mit  $a = r(a) + km$ ,  $k := \left\lfloor \frac{a}{m} \right\rfloor$ , und  $b = r(b) + lm \in \mathbb{N}_1$ ,  $l := \left\lfloor \frac{b}{m} \right\rfloor$ , folgt  $r(a \pm b) = r(a) \pm r(b) + (k \pm l)m - m \left\lfloor \frac{r(a) \pm r(b)}{m} \right\rfloor - m(k \pm l) = r(r(a) \pm r(b))$ .

Betrachten wir nun die Paare aufeinanderfolgender Reste  $(r_n, r_{n+1})$  für  $n \in \mathbb{N}_1$ , so stellt  $(r_n, r_{n+1}) \mapsto (r_{n+1}, r_{n+2})$  eine Abbildung dar, bei der das Bildpaar wegen  $r_{n+2} = r(f_n + f_{n+1}) = r(r_n + r_{n+1})$  durch das Urbildpaar vollständig bestimmt ist. Analog lässt sich das Urbildpaar  $(r_n, r_{n+1})$  wegen  $r(f_{n+2} - f_{n+1}) =$

$r(r_{n+2} - r_{n+1})$  eindeutig aus dem Bildpaar berechnen. Da  $r_k$  für jedes  $k \in \mathbb{N}_1$  in  $\mathcal{A}_m$  liegt, existieren höchstens  $m^2$  verschiedene Paare. Unter den ersten  $m^2 + 1$  Paaren gibt es also aufgrund des *Schubfachsatzes* (Seite 85) ein erstes, das sich wiederholt. Wegen der Eindeutigkeit der Bildpaare treten alle nachfolgenden Paare periodisch auf. Aus der eindeutigen Bestimmtheit der Urbildpaare folgt, dass es keine Vorperiode geben kann, d. h.  $(r_n)_n$  ist rein periodisch.

### Problem 76

Für  $m \in \mathbb{N}_2$  sei  $\lambda(m)$  die kleinste Periodenlänge der rein periodischen Folge  $(\text{mod}(f_n, m))_n$ , wobei  $(f_n)_n$  die in Aufgabe 2.1 definierte *Fibonacci-Folge* ist. Beweisen Sie, dass  $\lambda(m) \notin \mathbb{P}$  für alle  $m \in \mathbb{N}_3$  gilt.

Für die Zurückführung auf einen Spezialfall benötigen wir zunächst ein allgemeines Ergebnis über beliebige rein periodische Folgen  $(a_n)_n$ . Ist  $\mathcal{P}$  die Menge der Periodenlängen von  $(a_n)_n$  und  $p := \min \mathcal{P}$ , so folgt  $kp \in \mathcal{P}$  für jedes  $k \in \mathbb{N}_1$  durch vollständige Induktion mit dem Induktionsschritt  $a_{m+kp+p} = a_{m+kp} = a_m$ , wobei diese und die folgenden beiden Gleichungsketten für alle  $m \in \mathbb{N}_1$  gelten. Sind  $s, t \in \mathcal{P}$ , so ergibt sich  $s+t \in \mathcal{P}$  wegen  $a_{m+(s+t)} = a_{m+s} = a_m$ . Ist außerdem  $t \geq s$ , so erhalten wir  $t-s \in \mathcal{P} \cup \{0\}$  durch  $a_{m+(t-s)} = a_{(m+t-s)+s} = a_{m+t} = a_m$ . Für beliebige  $i \in \mathcal{P}$  setzen wir  $k := \left\lceil \frac{i}{p} \right\rceil$ . Dann ist  $i - kp = \text{mod}(i, p) \in \mathcal{A}_p$ , und es folgt  $i - kp \in \mathcal{P} \cup \{0\}$ . Wegen der Minimalität von  $p$  muss also  $i = kp$  gelten.

Sind in unserem Falle  $j, m \in \mathbb{N}_2$  mit  $j \mid m$ , so ist  $\lambda(m)$  wegen  $\text{mod}(\text{mod}(f_n, m), j) = \text{mod}(f_n, j)$  auch die Länge einer Periode von  $(\text{mod}(f_n, j))_n$ . Mit dem vorher Bewiesenen erhalten wir also  $\lambda(j) \mid \lambda(m)$  für alle  $j, m \in \mathbb{N}_2$  mit  $j \mid m$ .

Als Anwendung der *Erkundungsstrategie* berechnen wir nun einige minimale Perioden, wobei wir beachten, dass jede solche Periode mit den Resten 1 und 0 endet, weil dann mit den Resten 1 und 1 der Anfang der minimalen Periode folgt. Die minimalen Perioden für  $m = 2, 3$  und  $4$  sind  $(1,1,0)$ ,  $(1,1,2,0,2,2,1,0)$  und  $(1,1,2,3,1,0)$ . Diese und weitere Beispiele führen uns zu der Vermutung, dass  $2 \mid \lambda(p)$  und  $\lambda(p) > 2$  für alle  $p \in \mathbb{P}_3$  gilt. Da jedes  $m \in \mathbb{N}_3$  durch 4 oder durch ein  $p \in \mathbb{P}_3$  teilbar ist und wegen  $\lambda(4) = 6$  sind dann  $m = 4$  und  $m = p \in \mathbb{P}_3$  unsere führenden Spezialfälle. Im Folgenden sei also  $p \in \mathbb{P}_3$  und  $\lambda := \lambda(p)$ .

Die Struktur von minimalen Perioden mit mehreren Nullen wie bei  $m = 3$  veranlasst uns, die Abkürzung  $\varkappa = \varkappa(p) := \min \{k \in \mathbb{N}_1 ; p \mid f_k\}$  einzuführen. Mit

(6.12) erhalten wir dann  $f_{\varkappa+t} = f_{\varkappa}f_{t-1} + f_{\varkappa+1}f_t = f_{\varkappa}(f_{t-1} + f_t) + f_{\varkappa-1}f_t$  für alle  $t \in \mathbb{N}_1$ . Damit folgt  $f_{\varkappa+t} \equiv f_{\varkappa-1}f_t \pmod{p}$ , und vollständige Induktion ergibt  $f_{g\varkappa+t} \equiv f_{\varkappa-1}^g f_t \pmod{p}$  für jedes  $g \in \mathbb{N}_1$ . Als Spezialfall der für alle  $n \in \mathbb{N}_2$  mit vollständiger Induktion zu beweisenden Aussage  $\text{ggT}(f_{n-1}, f_n) = 1$  gilt  $p \nmid f_{\varkappa-1}$ . Die letzte Kongruenz und der *Satz über Restklassenkörper* (Seite 90) ergeben dann, dass  $p \mid f_n$  und  $\varkappa \mid n$  äquivalent sind. Setzen wir nun  $t = \varkappa - 1$  und  $o := \text{ord}_p(f_{\varkappa-1})$ , so erhalten wir  $f_{o\varkappa-1} \equiv f_{\varkappa-1}^o \equiv 1 \pmod{p}$  und  $f_{i\varkappa-1} \equiv f_{\varkappa-1}^i \not\equiv 1 \pmod{p}$  für  $1 \leq i < o$ , falls  $o > 1$  ist. Damit sind  $\text{mod}(f_{o\varkappa-1}, p) = 1$  und  $\text{mod}(f_{o\varkappa}, p) = 0$  die Schlusszahlen der minimalen Periode, und es gilt  $\lambda = o\varkappa$ .

Für den abschließenden Nachweis, dass aus  $2 \nmid \varkappa$  stets  $2 \mid o$  folgt, benutzen wir die leicht zu vermutende Aussage  $f_n^2 = f_{n-1}f_{n+1} - (-1)^n$  für jedes  $n \in \mathbb{N}_2$ , die sich durch vollständige Induktion beweisen lässt, indem auf beiden Seiten  $f_n f_{n+1}$  addiert wird. Mit  $n = \varkappa$  und wegen  $f_{\varkappa+1} = f_{\varkappa} + f_{\varkappa-1} \equiv f_{\varkappa-1} \pmod{p}$  ergibt sich  $f_{\varkappa-1}^2 \equiv (-1)^{\varkappa} \pmod{p}$ , sodass  $o = 4$  im Falle  $2 \nmid \varkappa$  gilt. Damit erhalten wir  $2 \mid \lambda$  für alle  $p \in \mathbb{P}_3$ . Wegen  $f_1 = f_2 = 1$  und  $o \geq 1$  ist  $\lambda \geq \varkappa > 2$ . Da also die führenden Spezialfälle  $\lambda(4)$  und  $\lambda(p)$  für  $p \in \mathbb{P}_3$  keine Primzahlen sind, folgt  $\lambda(m) \notin \mathbb{P}$  für alle  $m \in \mathbb{N}_3$ .

Bei den Problemen 4, 22, 25, 29, 41, 51, 54, 58 und 60 lohnt es sich, die Zurückführung auf Spezialfälle zu beachten. Eine Allaussage mit der Möglichkeit einer multiplikativen Zerlegung kann oft als *Signal* für die *Zurückführungsstrategie* angesehen werden.

## Extremfallstrategie

In [5] wird das “Extremalprinzip” in einem eigenen Kapitel als universell einsetzbare Problemlösemethode mit teilweise extrem kurzen Beweisen behandelt. Die 17 einführenden Beispiele stammen aus der Geometrie, Graphentheorie, Kombinatorik und Zahlentheorie. Wie bei dem Beweis des *Induktionssatzes* (Seite 12) hängt die *Extremfallstrategie* in der Zahlentheorie mit dem *Minimumsatz* oder dem *Maximumsatz* (Seite 11) zusammen und zwar meistens in Verbindung mit einem Widerspruchsbeweis. Als Beispiel bringen wir Problem 3.27 aus [5].

### Problem 77

Zeigen Sie, dass es unter je 15 teilerfremden Zahlen aus  $\mathcal{I}_{1992} \setminus \{1\}$  mindestens eine Primzahl gibt.

Man nimmt an, dass die Zahlen  $n_1, \dots, n_{15}$ , die die Bedingungen des Problems erfüllen, alle zerlegbar sind. Schreibt man aufgrund des *Satzes über den kleinsten Primteiler* (Seite 47)  $q_i := kP(n_i)$  für  $i = 1, \dots, 15$  und setzt  $q := \max\{q_1, \dots, q_{15}\}$ , so stellen  $q_1, \dots, q_{15}$  verschiedene Primzahlen dar, weil  $n_1, \dots, n_{15}$  als teilerfremd vorausgesetzt wurden. Damit ist  $q \geq p_{15} = 47$ . Für die Zahl  $n_j$  mit  $q = kP(n_j)$  folgt dann  $n_j \geq q^2 \geq 47^2 = 2209$  - im Widerspruch zur vorgegebenen Schranke 1992.

Die Probleme 33, 43 und 55 lassen sich mit drei verschiedenen Varianten der *Extremfallstrategie* in Angriff nehmen. Unter allen Problemen im Buchtext, die in der Aufgabenstellung die Suche nach etwas "Kleinstem" oder "Größtem" enthalten, ist Problem 55 das einzige, bei dem die *Extremfallstrategie* anwendbar ist. Solche Minimierungs- oder Maximierungsaufforderungen sind also **kein Signal** bei den Problemen 16, 19, 21, 38, 44, 51 und 60. Auch sonst gibt es bei dieser Strategie keine deutlichen Signale. Ähnlich ist die Situation bei der *Abstiegsstrategie*, die wir am Schluss als einen nur in der Zahlentheorie vorkommenden Spezialfall der *Extremfallstrategie* behandeln werden.

## Visualisierungsstrategie

Bei dem Beweis des *Quadratischen Reziprozitätsgesetzes* (Seite 114) war eine Figur sehr hilfreich. Aber es wurde auch erwähnt, dass sich die zugehörige *Visualisierungsstrategie* in der Zahlentheorie nur selten einsetzen lässt. In unserer Problemsammlung kommt sie - abgesehen von Problem 25, bei dem die Figur zur Aufgabenstellung gehört, - überhaupt nicht vor. Wir bringen trotzdem das Beispiel 1.2.3 aus [13], weil dabei die geometrische Deutung von arithmetischen Termen nicht auf der Hand liegt.

### Problem 78

Beweisen Sie, dass  $\sum_{k=1}^{n-1} \left[ \frac{km}{n} \right] = \frac{1}{2}(m-1)(n-1)$  für alle  $m, n \in \mathbb{N}_2$  mit  $\text{ggT}(m, n) = 1$  gilt.

Das Vorgehen bei dem Beweis des *Quadratischen Reziprozitätsgesetzes* legt es nahe, die Summanden  $\left[ \frac{km}{n} \right]$  als Gitterpunktanzahlen zu deuten. Setzen wir  $P_k := \left( k, \frac{km}{n} \right)$ ,  $k = 1, \dots, n-1$ , so liegen die Punkte  $P_k$  auf der Geraden  $\text{Graph}(x \mapsto \frac{mx}{n}, x \in \mathbb{R})$ . Für  $km \geq n$  ist dann  $\left[ \frac{km}{n} \right]$  die Anzahl der Punkte  $(k, j)$ ,  $j =$

$1, \dots, \left\lfloor \frac{km}{n} \right\rfloor$ , die sich alle auf der Verbindungsstrecke von  $(k, 0)$  und  $P_k$  befinden. Wegen  $\text{ggT}(m, n) = 1$  und  $k \leq n - 1$  stellt keiner der Punkte  $P_1, \dots, P_{n-1}$  einen Gitterpunkt dar. Deshalb ist  $\sum_{k=1}^{n-1} \left\lfloor \frac{km}{n} \right\rfloor$  die Anzahl der Gitterpunkte im Innern des Dreiecks  $\mathcal{D}$  mit den Eckpunkten  $(0, 0)$ ,  $(n, 0)$ ,  $(n, m)$  (siehe Abbildung 6.1).

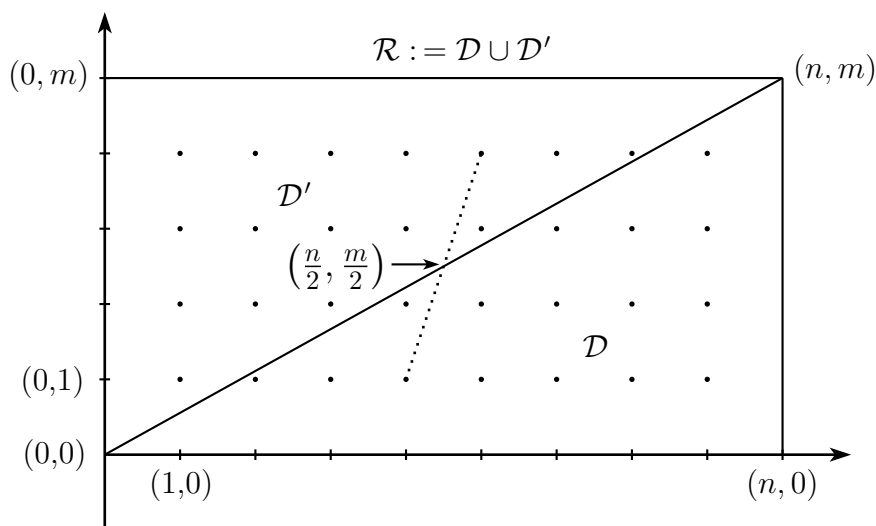


Abbildung 6.1: Die Punkt Mengen  $\mathcal{D}$ ,  $\mathcal{D}'$  und  $\mathcal{R}$  (für  $m = 5$  und  $n = 9$ )

Durch die Punktspiegelung  $(u, v) \mapsto (n - u, m - v)$  mit dem Fixpunkt  $\left(\frac{n}{2}, \frac{m}{2}\right)$  wird  $\mathcal{D}$  auf das Dreieck  $\mathcal{D}'$  mit den Eckpunkten  $(n, m)$ ,  $(0, m)$ ,  $(0, 0)$  abgebildet. Die Vereinigung von  $\mathcal{D}$  und  $\mathcal{D}'$  stellt das Rechteck  $\mathcal{R}$  mit den Eckpunkten  $(0, 0)$ ,  $(n, 0)$ ,  $(n, m)$ ,  $(0, m)$  dar. Der Durchschnitt ist die Verbindungsstrecke von  $(0, 0)$  und  $(n, m)$ , auf der nur die beiden Randpunkte Gitterpunkte sind, weil die Punkte  $P_k$  für  $k = 1, \dots, n - 1$  aus den oben genannten Gründen keine ganzzahlige zweite Koordinate haben.

Die Gitterpunkte im Innern von  $\mathcal{D}$  und  $\mathcal{D}'$  werden durch die Punktspiegelung bijektiv aufeinander abgebildet. Die Vereinigung der beiden Gitterpunkt Mengen ergibt die  $(m - 1)(n - 1)$  Gitterpunkte im Innern des Rechtecks  $\mathcal{R}$ . Damit stellt  $\frac{1}{2}(m - 1)(n - 1)$  die Anzahl der Gitterpunkte im Innern von  $\mathcal{D}$  dar, womit die Aussage des Problems bewiesen ist.

## Kernbruchstrategie

Hiermit beginnt die kleine Gruppe der zur elementaren Zahlentheorie gehörenden *Mikrostrategien*. Da wir *Problem 1* (Seite 31) mit Hilfe der *Kernbruchstrategie*

gelöst haben und da anschließend der *Satz über pythagoreische Tripel* (Seite 38) mit dieser Strategie gewonnen wurde, bringen wir hier kein weiteres Beispiel. Bei den Problemen 3, 14 und 30 kann die *Kernbruchstrategie* zumindest für eine alternative Lösung verwendet werden. Ein deutliches *Signal* ist meistens das Auftreten einer Gleichung zwischen Produkten mit jeweils zwei Faktoren, die Parameter enthalten.

## Klammerungsstrategie

Diese Strategie wurde im Buchtext bei den Vorüberlegungen zum *Satz über pythagoreische Tripel* (Seite 38) eingeführt. Dort steht auch als *Signal* die Möglichkeit, eine Gleichung mit mindestens einer Summe durch Klammerung so umzuformen, dass sich auf beiden Seiten Produkte ergeben. Manchmal schließt - wie bei den pythagoreischen Tripeln - die *Kernbruchstrategie* daran an. Meistens nutzt man diese Darstellung aber mit Hilfe des *Hauptsatzes (der elementaren Zahlentheorie)* (Seite 49) - wie bei *Problem 79* zur *Exponentenvergleichsstrategie*, die wir anschließend behandeln werden.

Bei der folgenden zu *Problem 74* (Seite 219) angekündigten zweiten Lösung ist die Klammerung sogar nur Teil der *Brückenstrategie* zum Finden der Quadratbasis  $x$ . Gehen wir von der mathematischen Form (6.33) des Problems aus, so ergibt Klammerung von  $x^2 - d^4$  die Produktgleichung

$$a(a+d)(a+2d)(a+3d) = (x-d^2)(x+d^2).$$

Da die Differenz der beiden Klammern auf der rechten Seite  $2d^2$  beträgt, besteht die "Brücke" in der Überlegung, welche Klammernprodukte der linken Seite dieselbe Differenz ergeben. Offensichtlich ist

$$(a+d)(a+2d) = a^2 + 3ad + 2d^2 = a(a+3d) + 2d^2,$$

sodass  $x - d^2 = a^2 + 3ad$  gesetzt werden kann.

Bei den Problemen 3, 4, 12, 14, 18, 27 und 40 lässt sich die *Klammerungsstrategie* in einer der drei Varianten einsetzen, allerdings nicht immer bei der nächstliegenden Lösung.

## Exponentenvergleichsstrategie

Hier geht es immer um die Anwendung des *Hauptsatzes* (Seite 49). Bei dem folgenden Beispiel 3.3.6 aus [13] ist - wie oben angekündigt - zunächst die *Klammerungsstrategie* zu benutzen.

**Problem 79**

Bestimmen Sie alle  $n \in \mathbb{N}_1$ , für die  $2^8 + 2^{11} + 2^n$  eine Quadratzahl darstellt.

Aus der Mathematisierung  $2^8 + 2^{11} + 2^n = m^2$  mit  $m \in \mathbb{N}_1$  folgt wegen  $2^8 + 2^{11} = 2^8(1 + 2^3) = 48^2$ , dass  $2^n = (m - 48)(m + 48)$  gilt. Aufgrund des *Hauptsatzes* gibt es also Exponenten  $s, t \in \mathbb{N}$ , sodass  $m - 48 = 2^s$ ,  $m + 48 = 2^t$  und  $s + t = n$  erfüllt ist. Durch Subtraktion der ersten Gleichung von der zweiten erhalten wir

$$2^s(2^{t-s} - 1) = 2^5 \cdot 3.$$

Da  $2^{t-s} - 1$  ungerade ist, ergibt der auf dem *Hauptsatz* beruhende *Exponentenvergleich*  $s = 5$  und  $t = 7$ . Damit ist  $n = 12$  der einzige Exponent, der zu einer Quadratzahl (nämlich  $m^2 = 80^2$ ) führt.

In unserer Sammlung lässt sich die *Exponentenvergleichsstrategie* nur bei Problem 30 mit dem deutlichen *Signal* einer Potenzgleichung einsetzen.

**Wechselwegnahmestrategie**

In der Zahlentheorie beruht die auf Seite 67 erwähnte *Methode der Wechselwegnahme* beziehungsweise die zugehörige *Ein- und Ausschaltformel* auf dem *Satz über das Eratosthenes-Sieb* (Seite 66). Im Buchtext wird sie bei der oberen Abschätzung im Beweis des *Satzes über  $\pi(x)$ -Abschätzungen* (Seite 67) verwendet, woran dann Teil b) des *Satzes über die Eulersche  $\varphi$ -Funktion* (Seite 98) anschließt. Auch der *Umkehrsatz von Möbius* (Seite 140) hängt damit zusammen.

Das entscheidende Hilfsmittel ist der *Satz über die Möbius-Summe* (Seite 65). Die im Beweis dieses Satzes auftretenden *Binomialkoeffizienten*  $\binom{r}{k}$  werden bei den Vorüberlegungen zur Lösung von *Problem 64* (Seite 199) mit der *Umformulierungsstrategie* als Anzahlen von  $k$ -elementigen Teilmengen einer Menge mit  $r$  Elementen gedeutet. Damit gehört dieses Problem - wie auch *Problem 65* - zum Grenzbereich von Zahlentheorie und Kombinatorik. In unserer Problemsammlung haben außerdem die Probleme 31, 55 und 58 mit Anzahlen von Teilmengen zu tun, wobei nur Problem 55 die *Ein- und Ausschaltformel* des *Satzes über das Eratosthenes-Sieb* benötigt. Wir bringen deshalb als Ergänzung ein Problem, das mit der folgenden *Verallgemeinerung der Ein- und Ausschaltformel* aus [5] (Seite 99), die auch *Siebformel* heißt, gelöst werden kann.

### Verallgemeinerte Ein- und Ausschaltformel oder Siebformel

Sind  $\mathcal{E}_1, \dots, \mathcal{E}_n$  mit  $n \in \mathbb{N}_2$  endliche, nicht leere Mengen, so gilt

$$(6.37) \quad \text{card}(\mathcal{E}_1 \cup \dots \cup \mathcal{E}_n) = \sum_{k=1}^n (-1)^{k+1} \sum_{1 \leq i_1 < \dots < i_k \leq n} \text{card}(\mathcal{E}_{i_1} \cap \dots \cap \mathcal{E}_{i_k}).$$

Für  $a \in \mathcal{E}_1 \cup \dots \cup \mathcal{E}_n$  sei  $j := \text{card}\{k \in \mathcal{I}_n; a \in \mathcal{E}_k\}$ . Da  $\mathcal{E}_1 \cup \dots \cup \mathcal{E}_n$  als Menge das Element  $a$  genau einmal enthält, müssen wir zeigen, dass  $a$  auf der rechten Seite von (6.37) auch nur einmal gezählt wird. Indem wir beachten, dass  $a$  für genau  $\binom{j}{k}$   $k$ -tupel  $(i_1, \dots, i_k)$  mit  $k \leq j$  in  $\mathcal{E}_{i_1} \cap \dots \cap \mathcal{E}_{i_k}$  vorkommt, erhalten wir

$$\sum_{k=1}^j (-1)^{k+1} \binom{j}{k} = 1 - \sum_{k=0}^j (-1)^k \binom{j}{k} = 1 - (1-1)^j = 1.$$

Jedes Element  $a$  wird also auf beiden Seiten von (6.37) genau einmal berücksichtigt.

Für das nächste Problem benötigen wir drei Bezeichnungen. Die Menge der bijektiven Abbildungen von  $\mathcal{I}_n$  nach  $\mathcal{I}_n$  wird mit  $\mathbf{S}_n$  abgekürzt. Jedes der  $n!$  Elemente von  $\mathbf{S}_n$  heißt *Permutation* von  $\mathcal{I}_n$ . Ist  $\sigma \in \mathbf{S}_n$ , so wird  $j \in \mathcal{I}_n$  *Fixpunkt* von  $\sigma$  genannt, wenn  $\sigma(j) = j$  gilt.

#### Problem 80

Es sei  $u_n$  die Anzahl der Permutationen von  $\mathcal{I}_n$ , die keinen Fixpunkt haben.

Zeigen Sie, dass

$$\frac{1}{3}n! \leq u_n \leq \frac{1}{2}n!$$

für alle  $n \in \mathbb{N}_2$  gilt.

Da sich die Menge der Permutationen, die keinen Fixpunkt besitzen, für die Anwendung der *Siebformel* nicht in einfacher Weise als Vereinigung von Permutationsmengen darstellen lässt, betrachten wir ihr Komplement in  $\mathbf{S}_n$ , nämlich die Menge der Permutationen mit mindestens einem Fixpunkt. Ist  $v_n$  ihre Elementzahl, so gilt zunächst

$$(6.38) \quad u_n = n! - v_n.$$

Setzen wir  $\mathcal{F}_i := \{\sigma \in \mathbf{S}_n; \sigma(i) = i\}$  für jedes  $i \in \mathcal{I}_n$ , so ergibt sich einerseits  $v_n = \text{card}(\mathcal{F}_1 \cup \dots \cup \mathcal{F}_n)$ , und andererseits können wir auf die Mengen  $\mathcal{F}_i$  die *Siebformel* anwenden:

$$v_n = \sum_{k=1}^n (-1)^{k+1} \sum_{1 \leq i_1 < \dots < i_k \leq n} \text{card}(\mathcal{F}_{i_1} \cap \dots \cap \mathcal{F}_{i_k}).$$

Aus der Definition von  $\mathcal{F}_i$  folgt

$$\mathcal{F}_{i_1} \cap \dots \cap \mathcal{F}_{i_k} = \{\sigma \in \mathbf{S}_n; \sigma(i_1) = i_1, \dots, \sigma(i_k) = i_k\}.$$

Damit gilt  $\text{card}(\mathcal{F}_{i_1} \cap \dots \cap \mathcal{F}_{i_k}) = (n - k)!$ , und wir erhalten

$$v_n = \sum_{k=1}^n (-1)^{k+1} \binom{n}{k} (n - k)! = n! \sum_{k=1}^n (-1)^{k+1} \frac{1}{k!}.$$

Mit (6.38) und wegen  $0! = 1$  ergibt sich also

$$u_n = n! \sum_{k=0}^n (-1)^k \frac{1}{k!} \text{ für jedes } n \in \mathbb{N}_1.$$

Setzen wir nun  $w_n := \frac{1}{n!} u_n$ , so gilt

$$w_{2n+2} = w_{2n} - \frac{1}{(2n+1)!} + \frac{1}{(2n+2)!} = w_{2n} - \frac{2n+1}{(2n+2)!} < w_{2n},$$

$$w_{2n+1} = w_{2n-1} + \frac{1}{(2n)!} - \frac{1}{(2n+1)!} = w_{2n-1} + \frac{2n}{(2n+1)!} > w_{2n-1} \text{ und}$$

$$w_{2n+2} = w_{2n+1} + \frac{1}{(2n+2)!} > w_{2n+1} \text{ für jedes } n \in \mathbb{N}_1.$$

Damit folgt  $w_{2n-1} < w_{2n+1} < w_{2n+2} < w_{2n}$  für jedes  $n \in \mathbb{N}_1$ , und mit Fallunterscheidung sowie vollständiger Induktion erhalten wir

$$\frac{1}{3} = w_3 \leq w_n \leq w_2 = \frac{1}{2} \text{ für alle } n \in \mathbb{N}_2.$$

Problem 2.5.13 in [13] enthält einen Tipp zum Herleiten der Rekursionsformel  $u_{n+1} = n(u_n + u_{n-1})$  für alle  $n \in \mathbb{N}_1$ , und in Problem 2.5.14 wird  $w_n$  für  $n \in \mathbb{N}_2$  als Wahrscheinlichkeit gedeutet.

## Abstiegsstrategie

Abschließend betrachten wir als Variante der *Extremfallstrategie* eine der ältesten Problemlösemethoden. Sie wurde schon im fünften Jahrhundert v. Chr. im Prinzip von den Pythagoreern für “Inkommensurabilitätsnachweise” in der Elementargeometrie verwendet. Dabei heißen zwei Strecken einer Figur *inkommensurabel*, wenn es keine Strecke gibt, deren Länge mit je einer natürlichen Zahl multipliziert die Längen der zu vergleichenden Strecken ergibt. Die Pythagoreer begründeten zum Beispiel die Inkommensurabilität von Seiten und Diagonalen

im regelmäßigen Fünfeck, indem sie aus der gegenteiligen Annahme die Existenz von zwei Folgen immer kürzer werdender Strecken erschlossen, deren Längen ganzzahlige Vielfache einer festen Streckenlänge sind, was im Widerspruch zur Beschränktheit der Vielfachenmengen steht.

Später wurde klar, dass diese Inkommensurabilitätsnachweise zugleich *Irrationalitätsbeweise* für einige der Streckenlängen darstellen. Heute wird die Methode vor allem in der Zahlentheorie verwendet, um zu zeigen, dass eine Aussage - meistens eine Polynomgleichung - keine Lösung besitzt, der sich in gesetzmäßiger Weise eine positive ganze Zahl  $m$  zuordnen lässt. Aus der Annahme, dass es eine solche Lösung gibt, wird die Existenz einer streng monoton fallenden Folge natürlicher Zahlen erschlossen - im Widerspruch zur Endlichkeit von  $\mathcal{A}_m$ .

Mit der *Extremfallstrategie* würde  $m$  als minimales Element der Menge aller natürlichen Zahlen definiert, die den Lösungen zuzuordnen sind. Wendet man den Induktionsschluss, der bei der *Abstiegsstrategie* die Existenz der monoton fallenden Folge liefert, auf das minimale Element  $m$  an, so ergibt sich sofort ein Widerspruch.

Da die *Extremfallstrategie* also logisch einfacher ist als die *Abstiegsstrategie*, wird sie heute meistens anstelle der Letzteren verwendet. So haben wir auch bei dem Beweis des *Zweiquadratesatzes* (Seite 141) diese Variante vorgezogen. In unserer Sammlung ist die *Abstiegsstrategie* nur bei Problem 44 einzusetzen. Wohl aus historischen Gründen findet sie sich in Lehrbüchern der Zahlentheorie unter der Bezeichnung *descente infinie* ("unendlicher Abstieg"). P. DE FERMAT, der sich als Entdecker dieser Methode ansah, gab ihr den Namen und konstatierte, dass er damit alle seine zahlentheoretischen Ergebnisse gefunden habe.

Mit dem folgenden letzten Problem erweitern wir zum dritten Mal die Aussage von *Problem 63* (Seite 195). Die *Abstiegsstrategie* ergibt hier allerdings keinen "unendlichen Abstieg", weil der "Abstiegsschritt" für einen genügend kleinen Wert der zugeordneten Folge nicht mehr gültig ist. Dafür tritt schon vor dem Erreichen dieses Wertes ein Widerspruch ein.

### **Problem 81**

Beweisen Sie, dass es zu jedem  $n \in \mathbb{N}_3$  **genau ein** Paar  $(x, y) \in \mathbb{N}_1^2$  mit  $2^n = 7x^2 + y^2$  und  $2 \nmid xy$  gibt.

Mit  $(x_{n+3})_{n \in \mathbb{N}}$  und  $(y_{n+3})_{n \in \mathbb{N}}$  bezeichnen wir wieder die Folgen ganzer Zahlen, die  $2^n = 7x_n^2 + y_n^2$  für jedes  $n \in \mathbb{N}_3$  sowie (6.5), (6.6) und (6.7) erfüllen. Nun nehmen wir an, dass es ein  $m \in \mathbb{N}_4$  und ein Paar  $(\bar{x}_m, \bar{y}_m) \in \mathbb{Z}^2$  mit

$$(6.39) \quad 2^m = 7\bar{x}_m^2 + \bar{y}_m^2, \quad 2 \nmid \bar{x}_m \bar{y}_m \quad \text{und} \quad (|\bar{x}_m|, |\bar{y}_m|) \neq (|x_m|, |y_m|)$$

gibt. Außerdem sei durch die Vorzeichenwahl

$$(6.40) \quad \bar{x}_m \equiv \bar{y}_m \equiv 2 - (-1)^m \pmod{4}.$$

Denken wir uns die Zuordnung von (6.5) durch die Abbildung

$$\varphi : \mathbb{Q}^2 \rightarrow \mathbb{Q}^2, \quad (x, y) \mapsto \left( \frac{1}{2}x + \frac{1}{2}y, \frac{-7}{2}x + \frac{1}{2}y \right)$$

in der Form  $(x_{n+1}, y_{n+1}) = \varphi(x_n, y_n)$  für jedes  $n \in \mathbb{N}_3$  gegeben, so benötigen wir für die *Abstiegsstrategie* die Umkehrabbildung

$$\psi : \mathbb{Q}^2 \rightarrow \mathbb{Q}^2, \quad (X, Y) \mapsto \left( \frac{1}{4}X - \frac{1}{4}Y, \frac{7}{4}X + \frac{1}{4}Y \right),$$

die man zum Beispiel durch Auflösen des Gleichungssystems in (6.5) nach  $x_n$  und  $y_n$  findet. Die Hintereinanderausführung von  $\varphi$  und  $\psi$  ergibt - der Umkehrreigenschaft entsprechend -

$$(6.41) \quad \begin{aligned} \varphi(\psi(X, Y)) &= \left( \frac{1}{2} \left( \frac{1}{4}X - \frac{1}{4}Y \right) + \frac{1}{2} \left( \frac{7}{4}X + \frac{1}{4}Y \right), \right. \\ &\quad \left. \frac{-7}{2} \left( \frac{1}{4}X - \frac{1}{4}Y \right) + \frac{1}{2} \left( \frac{7}{4}X + \frac{1}{4}Y \right) \right) \\ &= (X, Y) \quad \text{für alle } (X, Y) \in \mathbb{Q}^2. \end{aligned}$$

Mit Hilfe von  $\psi$  definieren wir

$$(6.42) \quad (\bar{x}_{m-1}, \bar{y}_{m-1}) := \psi(\bar{x}_m, \bar{y}_m) = \left( \frac{1}{4}\bar{x}_m - \frac{1}{4}\bar{y}_m, \frac{7}{4}\bar{x}_m + \frac{1}{4}\bar{y}_m \right).$$

Wegen (6.40) gilt dann  $(\bar{x}_{m-1}, \bar{y}_{m-1}) \in \mathbb{Z}^2$ , und mit (6.39) folgt

$$(6.43) \quad \begin{aligned} 7\bar{x}_{m-1}^2 + \bar{y}_{m-1}^2 &= \frac{7}{16}(\bar{x}_m - \bar{y}_m)^2 + \frac{1}{16}(7\bar{x}_m + \bar{y}_m)^2 \\ &= \frac{1}{16}(7\bar{x}_m^2 - 14\bar{x}_m\bar{y}_m + 7\bar{y}_m^2 + 49\bar{x}_m^2 + 14\bar{x}_m\bar{y}_m + \bar{y}_m^2) \\ &= \frac{1}{2}(7\bar{x}_m^2 + \bar{y}_m^2) = 2^{m-1}, \end{aligned}$$

d. h.  $(\bar{x}_{m-1}, \bar{y}_{m-1})$  stellt ein Lösungspaar von  $2^{m-1} = 7x^2 + y^2$  dar. Wegen (6.42) und (6.41) ist außerdem

$$(6.44) \quad \varphi(\bar{x}_{m-1}, \bar{y}_{m-1}) = (\bar{x}_m, \bar{y}_m).$$

Bezüglich  $(\bar{x}_{m-1}, \bar{y}_{m-1})$  unterscheiden wir jetzt die drei Fälle  $2 \nmid \bar{x}_{m-1}\bar{y}_{m-1}$ ,  $2 \mid \bar{x}_{m-1}\bar{y}_{m-1}$  mit  $\bar{x}_{m-1} \neq 0$  sowie  $\bar{x}_{m-1} = 0$ .

i) Sind  $\bar{x}_{m-1}$  und  $\bar{y}_{m-1}$  beide ungerade, so muss  $\bar{x}_{m-1} \equiv \bar{y}_{m-1} \pmod{4}$  gelten, weil sonst wegen (6.44)  $2 \mid \bar{x}_m \bar{y}_m$  im Widerspruch zur Voraussetzung folgen würde. Wäre nun  $(|\bar{x}_{m-1}|, |\bar{y}_{m-1}|) = (|x_{m-1}|, |y_{m-1}|)$ , so ergäbe sich  $(\bar{x}_{m-1}, \bar{y}_{m-1}) = (x_{m-1}, y_{m-1})$  oder  $(\bar{x}_{m-1}, \bar{y}_{m-1}) = (-x_{m-1}, -y_{m-1})$ . Beide Gleichungen führten aber mit (6.44) zu dem Widerspruch  $(|\bar{x}_m|, |\bar{y}_m|) = (|x_m|, |y_m|)$ . Im Falle  $2 \nmid \bar{x}_{m-1} \bar{y}_{m-1}$  gilt also auch  $(|\bar{x}_{m-1}|, |\bar{y}_{m-1}|) \neq (|x_{m-1}|, |y_{m-1}|)$ .

ii) Wäre  $\bar{x}_{m-1} \bar{y}_{m-1}$  gerade und  $\bar{x}_{m-1} \neq 0$ , so würden wir auf folgende Weise einen Widerspruch erhalten. Mit  $g := \nu_2(\text{ggT}(\bar{x}_{m-1}, \bar{y}_{m-1}))$ ,  $\hat{x} := 2^{-g} \bar{x}_{m-1}$  und  $\hat{y} := 2^{-g} \bar{y}_{m-1}$  ergäbe (6.43)  $2^3 \leq 7\hat{x}^2 + \hat{y}^2 = 2^{m-1-2g}$ , sodass  $\hat{x}$  und  $\hat{y}$  beide ungerade sein müssten. Wegen  $\bar{x}_m = \frac{1}{2}(\bar{x}_{m-1} + \bar{y}_{m-1}) = 2^{g-1}(\hat{x} + \hat{y})$  und  $g \geq 1$  wäre dann aber  $\bar{x}_m$  gerade.

iii) Der Fall  $\bar{x}_{m-1} = 0$  könnte wegen (6.42) nur eintreten, wenn  $\bar{x}_m = \bar{y}_m$  wäre. Dann ergäbe (6.39), dass  $\bar{x}_m = \bar{y}_m = 1$  sein müsste, womit wir für  $m = 3$  den Widerspruch  $(\bar{x}_3, \bar{y}_3) = (x_3, y_3)$  erhielten.

Mit finiter Induktion folgt nun, dass  $(\bar{x}_{m-k}, \bar{y}_{m-k}) := \psi^k(\bar{x}_m, \bar{y}_m) \in \mathbb{Z}^2$  mit  $2 \nmid \bar{x}_{m-k} \bar{y}_{m-k}$  für jedes  $k \in \mathcal{I}_{m-3}$  eine Lösung  $(x, y)$  von  $2^{m-k} = 7x^2 + y^2$  darstellt, wobei hier  $2^{m-k}$  die zugeordneten natürlichen Zahlen der *Abstiegsstrategie* sind. Für jede der Lösungen gilt  $(|\bar{x}_{m-k}|, |\bar{y}_{m-k}|) \neq (|x_{m-k}|, |y_{m-k}|)$ , was spätestens für  $k = m - 3$  einen Widerspruch zu der eindeutigen Lösbarkeit von  $2^3 = 7x^2 + y^2$  mit  $(x, y) \in \mathbb{N}_1^2$  ergibt.

Also existiert für jedes  $n \in \mathbb{N}_3$  nur ein Paar  $(x, y) \in \mathbb{N}_1^2$  mit  $2 \nmid xy$  und  $2^n = 7x^2 + y^2$ .

## 6.4 Hinweise zu den gestellten Problemen

Die folgende abschließende Tabelle enthält Zusammenfassungen und Ergänzungen zu den 60 nicht gelösten Problemen des Buches. Die Nummern in der ersten Spalte ermöglichen auch das Auffinden: Die Probleme 2 bis 13 stehen am Schluss des zweiten Kapitels ab Seite 45, auf das dritte Kapitel ab Seite 79 folgen die Probleme 14 bis 33, und am Ende des vierten Kapitels ab Seite 132 sind die Probleme 34 bis 61 zu finden. In der zweiten Spalte wird noch einmal angegeben, aus welchem Wettbewerb (Wb.) das Problem stammt. Die dritte Spalte gibt an, bei wievielen der im letzten Abschnitt vorgestellten Strategien (St.) das betreffende Problem aufgeführt ist. Da Sätze ähnlich wie Problemlösestrategien

einzusetzen sind, führen wir in der vierten Spalte (Sa.) auf, wieviele der folgenden Sätze bei dem jeweiligen Problem verwendet werden können: *Satz über die  $g$ -adische Zahlendarstellung* (Seite 40), *Satz über ein Primzahlkriterium* (Seite 63), *Schubfachsatz* (Seite 85), *Satz über Kongruenzregeln* (Seite 87), *Satz über Restklassenkörper* (Seite 90), *Satz über die Eulersche  $\varphi$ -Funktion* (Seite 98), *Kongruenzsatz von Euler* (Seite 99). Die letzte Spalte enthält für jedes der Probleme eine grobe Bewertung des Schwierigkeitsgrades (Sg.), wobei “1” leicht, “2” mittel und “3” schwer bedeutet.

| Nr. | Wb. | St. | Sa. | Sg. |
|-----|-----|-----|-----|-----|
| 2   | BWM | 1   | 1   | 1   |
| 3   | BWM | 3   | 0   | 2   |
| 4   | BWM | 3   | 0   | 2   |
| 5   | BWM | 2   | 0   | 2   |
| 6   | BWM | 2   | 0   | 2   |
| 7   | BWM | 2   | 0   | 2   |
| 8   | BWM | 1   | 0   | 2   |
| 9   | BWM | 1   | 0   | 2   |
| 10  | BWM | 1   | 0   | 2   |
| 11  | BWM | 2   | 0   | 2   |
| 12  | BWM | 3   | 0   | 2   |
| 13  | BWM | 3   | 0   | 1   |
| 14  | BWM | 3   | 0   | 2   |
| 15  | BWM | 2   | 0   | 1   |
| 16  | BWM | 1   | 0   | 1   |
| 17  | BWM | 0   | 0   | 1   |
| 18  | BWM | 3   | 0   | 2   |
| 19  | BWM | 0   | 0   | 2   |
| 20  | BWM | 1   | 0   | 3   |
| 21  | BWM | 0   | 0   | 1   |
| 22  | BWM | 2   | 0   | 2   |
| 23  | BWM | 1   | 0   | 2   |
| 24  | BWM | 1   | 0   | 2   |
| 25  | BWM | 1   | 0   | 1   |
| 26  | BWM | 1   | 0   | 1   |
| 27  | IMO | 3   | 0   | 2   |
| 28  | IMO | 1   | 0   | 1   |
| 29  | IMO | 2   | 1   | 3   |
| 30  | IMO | 4   | 0   | 2   |
| 31  | IMO | 1   | 1   | 3   |

| Nr. | Wb. | St. | Sa. | Sg. |
|-----|-----|-----|-----|-----|
| 32  | IMO | 0   | 0   | 2   |
| 33  | IMO | 3   | 1   | 2   |
| 34  | BWM | 2   | 1   | 3   |
| 35  | BWM | 2   | 1   | 2   |
| 36  | BWM | 0   | 1   | 1   |
| 37  | BWM | 3   | 0   | 2   |
| 38  | IMO | 1   | 2   | 2   |
| 39  | IMO | 1   | 1   | 1   |
| 40  | IMO | 3   | 0   | 1   |
| 41  | IMO | 3   | 1   | 2   |
| 42  | IMO | 1   | 0   | 1   |
| 43  | IMO | 2   | 1   | 2   |
| 44  | IMO | 2   | 0   | 2   |
| 45  | IMO | 2   | 0   | 2   |
| 46  | IMO | 1   | 0   | 2   |
| 47  | IMO | 1   | 0   | 2   |
| 48  | IMO | 1   | 2   | 2   |
| 49  | IMO | 2   | 0   | 2   |
| 50  | IMO | 1   | 1   | 2   |
| 51  | IMO | 2   | 0   | 2   |
| 52  | IMO | 2   | 1   | 2   |
| 53  | IMO | 2   | 0   | 2   |
| 54  | IMO | 3   | 1   | 3   |
| 55  | IMO | 3   | 1   | 2   |
| 56  | IMO | 3   | 1   | 2   |
| 57  | IMO | 2   | 0   | 2   |
| 58  | IMO | 2   | 1   | 3   |
| 59  | IMO | 2   | 1   | 3   |
| 60  | IMO | 3   | 0   | 3   |
| 61  | IMO | 2   | 0   | 2   |

# Satzverzeichnis

- Kardinalzahlpostulate* (Seite 8)
- Erzeugungspostulate* (Seite 9)
- Zugehörigkeitspostulate* (Seite 9)
- Anfängepostulat* (Seite 10)
- Nachfolgersatz* (Seite 10)
- Minimumsatz, Maximumsatz* (Seite 11)
- Induktionssatz* (Seite 12)
- Rekursionssatz* (Seite 13)
- Satz über Teilbarkeitsregeln* (Seite 18)
- Satz über die Teileranzahl* (Seite 18)
- Satz über Division mit Rest* (Seite 19)
- Satz über die ggT-Rekursion* (Seite 19)
- Satz über den Euklidischen Algorithmus* (Seite 20)
- Effizienzsatz* (Seite 22)
- Produktteilersatz* (Seite 23)
- Satz über die Kettenbruchentwicklung* (Seite 24)
- Satz über vollständige Quotienten und Näherungsbrüche* (Seite 25)
- Satz über die lineare diophantische Gleichung* (Seite 28)
- Gleichheitssatz* (Seite 35)
- Erweiterungssatz* (Seite 36)
- Satz über pythagoreische Tripel* (Seite 38)
- Satz über die g-adische Zahlendarstellung* (Seite 40)
- Satz über den kleinsten Primteiler* (Seite 47)
- Satz über die Primzahlmenge* (Seite 48)
- Hauptsatz (der elementaren Zahlentheorie)* (Seite 49)
- Teilbarkeitssatz* (Seite 53)
- Satz über die ggT- und kgV-Darstellung* (Seite 54)
- Satz über die Teileranzahlfunktion* (Seite 55)
- Satz über rationale k-te Wurzeln* (Seite 56)
- Satz über die Teilersummenfunktion* (Seite 57)
- Satz über gerade vollkommene Zahlen* (Seite 57)
- Satz über Primzahlen der Form  $2^m - 1$*  (Seite 59)
- Theorem über Mersenne-Primzahlen* (Seite 60)

- Theorem über regelmäßige Vielecke* (Seite 61)
- Satz über Primzahlen der Form  $2^t + 1$*  (Seite 61)
- Theorem über Fermat-Primzahlen* (Seite 62)
- Satz über ein Primzahlkriterium* (Seite 63)
- Satz über die Möbius-Summe* (Seite 65)
- Satz über das Eratosthenes-Sieb* (Seite 66)
- Satz über  $\pi(x)$ -Abschätzungen* (Seite 67)
- Theorem über Primzahlen in arithmetischen Folgen* (Seite 71)
- Theorem über  $\pi(x)$ -Approximation durch  $li(x)$*  (Seite 72)
- Theorem über Quotientenschachtelung* (Seite 73)
- Theorem über die Riemannsche Funktionalgleichung* (Seite 73)
- Theorem über das Wachstum von  $\pi(x)$*  (Seite 75)
- Theorem über Fastprimzahlzwillinge* (Seite 75)
- Satz über die Kongruenzrelation* (Seite 83)
- Satz über ein Kongruenzkriterium* (Seite 84)
- Schubfachsatz* (Seite 85)
- Satz über vollständige Restsysteme* (Seite 86)
- Satz über Kongruenzregeln* (Seite 87)
- Satz über Restklassenringe* (Seite 89)
- Satz über Restklassenkörper* (Seite 90)
- Satz über die lineare Kongruenz* (Seite 91)
- Satz über Kongruenzkürzung* (Seite 91)
- Satz über Kongruenzvergrößerung* (Seite 91)
- Satz über Kongruenzzusammenfassung* (Seite 92)
- Satz über modifizierte Restsysteme* (Seite 92)
- Satz über den ggT in Restklassen* (Seite 93)
- Satz über modifizierte reduzierte Restsysteme* (Seite 94)
- Theorem über Kreisteilungskörper* (Seite 97)
- Satz über die Eulersche  $\varphi$ -Funktion* (Seite 98)
- Fermatscher Kongruenzsatz* (Seite 99)
- Kongruenzsatz von Euler* (Seite 99)
- Satz über die Lösungsanzahl der linearen Kongruenz* (Seite 101)
- Wilsonscher Fakultätensatz* (Seite 102)
- Polynomkongruenzsatz von Lagrange* (Seite 103)
- Chinesischer Restsatz* (Seite 104)

- Satz über Modulreduktion* (Seite [107](#))
- Satz über die Anzahl quadratischer Reste* (Seite [108](#))
- Satz über das Euler-Kriterium* (Seite [109](#))
- Satz über Halbsysteme* (Seite [110](#))
- Übereinstimmungssatz (Lemma von Gauß)*, Seite [111](#))
- Satz über obere Kongruenzinvarianz* (Seite [112](#))
- Satz über obere Multiplikativität* (Seite [112](#))
- Satz über untere Multiplikativität* (Seite [113](#))
- Quadratisches Reziprozitätsgesetz* (Seite [114](#))
- Erster Ergänzungssatz* (Seite [117](#))
- Zweiter Ergänzungssatz* (Seite [117](#))
- Satz über untere Kongruenzinvarianz* (Seite [118](#))
- Satz über die allgemeine quadratische Kongruenz* (Seite [119](#))
- Satz über die Ordnung* (Seite [120](#))
- Satz über Ordnungsbeziehungen* (Seite [121](#))
- Satz über Primitivwurzeln* (Seite [122](#))
- Satz über ein Primitivwurzelkriterium* (Seite [123](#))
- Satz über Indizes* (Seite [128](#))
- Satz über die Faltung multiplikativer Funktionen* (Seite [138](#))
- Satz über die Summatorfunktion* (Seite [139](#))
- Umkehrsatz von Möbius* (Seite [140](#))
- Zweiquadratesatz (EULER)*, Seite [141](#))
- Vierquadratesatz (LAGRANGE)*, Seite [143](#))
- Dreiquadratesatz (LEGENDRE)*, Seite [146](#))
- Satz über Formenäquivalenz* (Seite [153](#))
- Satz über Invarianten der Formenklassen* (Seite [154](#))
- Satz über die Klassenanzahl* (Seite [155](#))
- Satz über eindeutige Repräsentanten* (Seite [156](#))
- Theorem über die Klassengruppe* (Seite [159](#))
- Satz über ganz-algebraische Zahlen* (Seite [165](#))
- Einheitensatz* (Seite [169](#))
- Theorem über Darstellungen als Primidealprodukt* (Seite [175](#))
- Theorem über die Idealklassengruppe* (Seite [179](#))
- Theorem über die Klassenzahlformel (DIRICHLET)*, Seite [180](#))
- Theorem über die Eulersche  $\sigma$ -Rekursion* (Seite [184](#))

# Symbolverzeichnis

|                            |    |                              |         |                            |          |                         |     |
|----------------------------|----|------------------------------|---------|----------------------------|----------|-------------------------|-----|
| card                       | 8  | $\Omega$                     | 53      | $a^{-1}, \frac{1}{a}$      | 102      | $\rho$                  | 165 |
| $\mathbb{N}$               | 9  | $\mathcal{I}_n$              | 54      | $\left(\frac{a}{p}\right)$ | 108      | $\delta$                | 165 |
| $\mathcal{A}_n$            | 9  | kgV                          | 54      | $\mathbb{U}$               | 110      | $R_{d,1}$               | 165 |
| $\mathbb{N}_k$             | 10 | $\sigma$                     | 56      | $m_-$                      | 110      | $f$                     | 166 |
| $\nu$                      | 10 | $M_p$                        | 59      | $\left(\frac{a}{m}\right)$ | 111      | $\{a, b\}_{\mathbb{Z}}$ | 166 |
| $\mathcal{M}$              | 12 | $F_n$                        | 61      | $\text{ord}_m(a)$          | 120      | $R_{d,f}$               | 166 |
| $\mathbb{Z}$               | 17 | $\pi(x)$                     | 62      | $\mathcal{P}_p$            | 124      | $D_f$                   | 166 |
|                            | 17 | $\mu$                        | 64      | $\mathcal{C}_{p,a}$        | 124      | $\mathcal{D}$           | 167 |
| †                          | 17 | $\binom{r}{k}$               | 65      | $\text{ind}_g a$           | 128      | $R_{d,f}^*$             | 167 |
| $d$                        | 18 | $\chi$                       | 72, 180 | $\text{ind } a$            | 128      | $\varepsilon_{d,f}$     | 169 |
| $\tau$                     | 18 | $\text{li}(x)$               | 72      | $\star$                    | 138      | $\widehat{R}_{d,f}$     | 173 |
| mod                        | 19 | $\mathbb{C}$                 | 73      | $\sigma_s$                 | 139      | $\mathbf{a}$            | 174 |
| ggT                        | 19 | $\zeta(s)$                   | 73      | $o$                        | 140      | $(a)$                   | 174 |
| $[q_1, \dots, q_n]$        | 24 | $\Gamma(s)$                  | 73      | $\mathcal{Q}_k$            | 141      | $\mathbf{a} \mathbf{b}$ | 174 |
| $\mathbb{R}, \mathbb{R}^+$ | 24 | $a \equiv b \pmod{m}$        | 83      | det                        | 146      | $cA$                    | 175 |
| $\mathbb{Q}, \mathbb{Q}^+$ | 24 | $\bar{a}$                    | 84      | $\mathcal{W}_F$            | 148, 152 | $\varsigma(A)$          | 176 |
| $P_k, Q_k$                 | 25 | $\mathbb{Z}/m\mathbb{Z}$     | 89      | $(a, b, c)$                | 152      | $F_{g,h}(x, y)$         | 178 |
| $\mathcal{L}(a, b, c)$     | 28 | $\mathbb{Z}_m$               | 89      | dis                        | 152      | $\mathcal{C}(D_f)$      | 179 |
| $\mathbb{P}$               | 47 | $\mathcal{R}_m$              | 92      | $\alpha$                   | 152, 164 | $\mathcal{F}(D_f)$      | 179 |
| $p_n$                      | 47 | $\mathcal{R}_m^*$            | 93      | $\delta_b$                 | 156      | $h(D_f)$                | 179 |
| $\mathbb{P}_a$             | 47 | $\mathcal{A}_m^*$            | 94      | $h$                        | 162      | $L(1, \chi)$            | 180 |
| $kP(n)$                    | 47 | $\varphi$                    | 94      | $\mathcal{S}$              | 163      | $P_m(n)$                | 212 |
| $(q_n)_n$                  | 48 | $\mathbb{Z}_m^*$             | 96      | $\mathbb{Q}(\sqrt{d})$     | 163      | $B_k$                   | 213 |
| $\nu_p$                    | 52 | $(\mathbb{Z}/m\mathbb{Z})^*$ | 96      | $\varsigma$                | 164      | $S(m, n)$               | 214 |
| $\omega$                   | 53 | $\mathbb{Q}(\zeta)$          | 97      | $R_d$                      | 165      |                         |     |

# GNU Free Documentation License

Version 1.2, November 2002

Copyright © 2000,2001,2002 Free Software Foundation, Inc.

51 Franklin St, Fifth Floor, Boston, MA 02110-1301, USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

## 0. PREAMBLE

The purpose of this License is to make a manual, textbook, or other functional and useful document *free* in the sense of freedom: to assure everyone the effective freedom to copy and redistribute it, with or without modifying it, either commercially or noncommercially. Secondly, this License preserves for the author and publisher a way to get credit for their work, while not being considered responsible for modifications made by others.

This License is a kind of “copyleft”, which means that derivative works of the document must themselves be free in the same sense. It complements the GNU General Public License, which is a copyleft license designed for free software.

We have designed this License in order to use it for manuals for free software, because free software needs free documentation: a free program should come with manuals providing the same freedoms that the software does. But this License is not limited to software manuals; it can be used for any textual work, regardless of subject matter or whether it is published as a printed book. We recommend this License principally for works whose purpose is instruction or reference.

## 1. APPLICABILITY AND DEFINITIONS

This License applies to any manual or other work, in any medium, that contains a notice placed by the copyright holder saying it can be distributed under the terms of this License. Such a notice grants a world-wide, royalty-free license, unlimited in duration, to use that work under the conditions stated herein. The “Document”, below, refers to any such manual or work. Any member of the public is a licensee, and is addressed as “you”. You accept the license if you copy, modify or distribute the work in a way requiring permission under copyright law.

A “Modified Version” of the Document means any work containing the Document or a portion of it, either copied verbatim, or with modifications and/or translated into another language.

A “Secondary Section” is a named appendix or a front-matter section of the Document that deals exclusively with the relationship of the publishers or authors of the Document to the Document’s overall subject (or to related matters) and contains nothing that could fall directly within that overall subject. (Thus, if the Document is in part a textbook of mathematics, a Secondary Section may not explain any mathematics.) The relationship could be a matter of historical connection with the subject or with related matters, or of legal, commercial, philosophical, ethical or political position regarding them.

The “Invariant Sections” are certain Secondary Sections whose titles are designated, as being those of Invariant Sections, in the notice that says that the Document is released under this License. If a section does not fit the above definition of Secondary then it is not allowed to be designated as Invariant. The Document may contain zero Invariant Sections. If the Document does not identify any Invariant Sections then there are none.

The “Cover Texts” are certain short passages of text that are listed, as Front-Cover Texts or Back-Cover Texts, in the notice that says that the Document is released under this License. A Front-Cover Text may be at most 5 words, and a Back-Cover Text may be at most 25 words.

A “Transparent” copy of the Document means a machine-readable copy, represented in a format whose specification is available to the general public, that is suitable for revising the document straightforwardly with generic text editors or (for images composed of pixels) generic paint programs or (for drawings) some widely available drawing editor, and that is suitable for input to text formatters or for automatic translation to a variety of formats suitable for input to text formatters. A copy made in an otherwise Transparent file format whose markup, or absence of markup, has been arranged to thwart or discourage subsequent modification by readers is not Transparent. An image format is not Transparent if used for any substantial amount of text. A copy that is not “Transparent” is called “Opaque”.

Examples of suitable formats for Transparent copies include plain ASCII without markup, Texinfo input format,  $\LaTeX$  input format, SGML or XML using a publicly available DTD, and standard-conforming simple HTML, PostScript or PDF designed for human modification. Examples of transparent image formats include PNG, XCF and JPG. Opaque formats include proprietary formats that can be read and edited only by proprietary word processors, SGML or XML for which the DTD and/or processing tools are not generally available, and the machine-generated HTML, PostScript or PDF produced by some word processors for output purposes only.

The “Title Page” means, for a printed book, the title page itself, plus such following pages as are needed to hold, legibly, the material this License requires to appear in the title page. For works in formats which do not have any title page as such, “Title Page” means the text near the most prominent

appearance of the work's title, preceding the beginning of the body of the text.

A section “Entitled XYZ” means a named subunit of the Document whose title either is precisely XYZ or contains XYZ in parentheses following text that translates XYZ in another language. (Here XYZ stands for a specific section name mentioned below, such as “Acknowledgements”, “Dedications”, “Endorsements”, or “History”.) To “Preserve the Title” of such a section when you modify the Document means that it remains a section “Entitled XYZ” according to this definition.

The Document may include Warranty Disclaimers next to the notice which states that this License applies to the Document. These Warranty Disclaimers are considered to be included by reference in this License, but only as regards disclaiming warranties: any other implication that these Warranty Disclaimers may have is void and has no effect on the meaning of this License.

## 2. VERBATIM COPYING

You may copy and distribute the Document in any medium, either commercially or noncommercially, provided that this License, the copyright notices, and the license notice saying this License applies to the Document are reproduced in all copies, and that you add no other conditions whatsoever to those of this License. You may not use technical measures to obstruct or control the reading or further copying of the copies you make or distribute. However, you may accept compensation in exchange for copies. If you distribute a large enough number of copies you must also follow the conditions in section 3.

You may also lend copies, under the same conditions stated above, and you may publicly display copies.

## 3. COPYING IN QUANTITY

If you publish printed copies (or copies in media that commonly have printed covers) of the Document, numbering more than 100, and the Document's license notice requires Cover Texts, you must enclose the copies in covers that carry, clearly and legibly, all these Cover Texts: Front-Cover Texts on the front cover, and Back-Cover Texts on the back cover. Both covers must also clearly and legibly identify you as the publisher of these copies. The front cover must present the full title with all words of the title equally prominent and visible. You may add other material on the covers in addition. Copying with changes limited to the covers, as long as they preserve the title of the Document and satisfy these conditions, can be treated as verbatim copying in other respects.

If the required texts for either cover are too voluminous to fit legibly, you should put the first ones listed (as many as fit reasonably) on the actual cover, and continue the rest onto adjacent pages.

If you publish or distribute Opaque copies of the Document numbering more than 100, you must either include a machine-readable Transparent copy along

with each Opaque copy, or state in or with each Opaque copy a computer-network location from which the general network-using public has access to download using public-standard network protocols a complete Transparent copy of the Document, free of added material. If you use the latter option, you must take reasonably prudent steps, when you begin distribution of Opaque copies in quantity, to ensure that this Transparent copy will remain thus accessible at the stated location until at least one year after the last time you distribute an Opaque copy (directly or through your agents or retailers) of that edition to the public.

It is requested, but not required, that you contact the authors of the Document well before redistributing any large number of copies, to give them a chance to provide you with an updated version of the Document.

#### 4. MODIFICATIONS

You may copy and distribute a Modified Version of the Document under the conditions of sections 2 and 3 above, provided that you release the Modified Version under precisely this License, with the Modified Version filling the role of the Document, thus licensing distribution and modification of the Modified Version to whoever possesses a copy of it. In addition, you must do these things in the Modified Version:

- A. Use in the Title Page (and on the covers, if any) a title distinct from that of the Document, and from those of previous versions (which should, if there were any, be listed in the History section of the Document). You may use the same title as a previous version if the original publisher of that version gives permission.
- B. List on the Title Page, as authors, one or more persons or entities responsible for authorship of the modifications in the Modified Version, together with at least five of the principal authors of the Document (all of its principal authors, if it has fewer than five), unless they release you from this requirement.
- C. State on the Title page the name of the publisher of the Modified Version, as the publisher.
- D. Preserve all the copyright notices of the Document.
- E. Add an appropriate copyright notice for your modifications adjacent to the other copyright notices.
- F. Include, immediately after the copyright notices, a license notice giving the public permission to use the Modified Version under the terms of this License, in the form shown in the Addendum below.
- G. Preserve in that license notice the full lists of Invariant Sections and required Cover Texts given in the Document's license notice.
- H. Include an unaltered copy of this License.

- I. Preserve the section Entitled “History”, Preserve its Title, and add to it an item stating at least the title, year, new authors, and publisher of the Modified Version as given on the Title Page. If there is no section Entitled “History” in the Document, create one stating the title, year, authors, and publisher of the Document as given on its Title Page, then add an item describing the Modified Version as stated in the previous sentence.
- J. Preserve the network location, if any, given in the Document for public access to a Transparent copy of the Document, and likewise the network locations given in the Document for previous versions it was based on. These may be placed in the “History” section. You may omit a network location for a work that was published at least four years before the Document itself, or if the original publisher of the version it refers to gives permission.
- K. For any section Entitled “Acknowledgements” or “Dedications”, Preserve the Title of the section, and preserve in the section all the substance and tone of each of the contributor acknowledgements and/or dedications given therein.
- L. Preserve all the Invariant Sections of the Document, unaltered in their text and in their titles. Section numbers or the equivalent are not considered part of the section titles.
- M. Delete any section Entitled “Endorsements”. Such a section may not be included in the Modified Version.
- N. Do not retitle any existing section to be Entitled “Endorsements” or to conflict in title with any Invariant Section.
- O. Preserve any Warranty Disclaimers.

If the Modified Version includes new front-matter sections or appendices that qualify as Secondary Sections and contain no material copied from the Document, you may at your option designate some or all of these sections as invariant. To do this, add their titles to the list of Invariant Sections in the Modified Version’s license notice. These titles must be distinct from any other section titles.

You may add a section Entitled “Endorsements”, provided it contains nothing but endorsements of your Modified Version by various parties—for example, statements of peer review or that the text has been approved by an organization as the authoritative definition of a standard.

You may add a passage of up to five words as a Front-Cover Text, and a passage of up to 25 words as a Back-Cover Text, to the end of the list of Cover Texts in the Modified Version. Only one passage of Front-Cover Text and one of Back-Cover Text may be added by (or through arrangements made by) any one entity. If the Document already includes a cover text for the same

cover, previously added by you or by arrangement made by the same entity you are acting on behalf of, you may not add another; but you may replace the old one, on explicit permission from the previous publisher that added the old one.

The author(s) and publisher(s) of the Document do not by this License give permission to use their names for publicity for or to assert or imply endorsement of any Modified Version.

## 5. COMBINING DOCUMENTS

You may combine the Document with other documents released under this License, under the terms defined in section 4 above for modified versions, provided that you include in the combination all of the Invariant Sections of all of the original documents, unmodified, and list them all as Invariant Sections of your combined work in its license notice, and that you preserve all their Warranty Disclaimers.

The combined work need only contain one copy of this License, and multiple identical Invariant Sections may be replaced with a single copy. If there are multiple Invariant Sections with the same name but different contents, make the title of each such section unique by adding at the end of it, in parentheses, the name of the original author or publisher of that section if known, or else a unique number. Make the same adjustment to the section titles in the list of Invariant Sections in the license notice of the combined work.

In the combination, you must combine any sections Entitled “History” in the various original documents, forming one section Entitled “History”; likewise combine any sections Entitled “Acknowledgements”, and any sections Entitled “Dedications”. You must delete all sections Entitled “Endorsements.”

## 6. COLLECTIONS OF DOCUMENTS

You may make a collection consisting of the Document and other documents released under this License, and replace the individual copies of this License in the various documents with a single copy that is included in the collection, provided that you follow the rules of this License for verbatim copying of each of the documents in all other respects.

You may extract a single document from such a collection, and distribute it individually under this License, provided you insert a copy of this License into the extracted document, and follow this License in all other respects regarding verbatim copying of that document.

## 7. AGGREGATION WITH INDEPENDENT WORKS

A compilation of the Document or its derivatives with other separate and independent documents or works, in or on a volume of a storage or distribution medium, is called an “aggregate” if the copyright resulting from the compilation is not used to limit the legal rights of the compilation’s users beyond what

the individual works permit. When the Document is included in an aggregate, this License does not apply to the other works in the aggregate which are not themselves derivative works of the Document.

If the Cover Text requirement of section 3 is applicable to these copies of the Document, then if the Document is less than one half of the entire aggregate, the Document's Cover Texts may be placed on covers that bracket the Document within the aggregate, or the electronic equivalent of covers if the Document is in electronic form. Otherwise they must appear on printed covers that bracket the whole aggregate.

## 8. TRANSLATION

Translation is considered a kind of modification, so you may distribute translations of the Document under the terms of section 4. Replacing Invariant Sections with translations requires special permission from their copyright holders, but you may include translations of some or all Invariant Sections in addition to the original versions of these Invariant Sections. You may include a translation of this License, and all the license notices in the Document, and any Warranty Disclaimers, provided that you also include the original English version of this License and the original versions of those notices and disclaimers. In case of a disagreement between the translation and the original version of this License or a notice or disclaimer, the original version will prevail.

If a section in the Document is Entitled “Acknowledgements”, “Dedications”, or “History”, the requirement (section 4) to Preserve its Title (section 1) will typically require changing the actual title.

## 9. TERMINATION

You may not copy, modify, sublicense, or distribute the Document except as expressly provided for under this License. Any other attempt to copy, modify, sublicense or distribute the Document is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

## 10. FUTURE REVISIONS OF THIS LICENSE

The Free Software Foundation may publish new, revised versions of the GNU Free Documentation License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns. See <http://www.gnu.org/copyleft/>.

Each version of the License is given a distinguishing version number. If the Document specifies that a particular numbered version of this License “or any later version” applies to it, you have the option of following the terms and conditions either of that specified version or of any later version that has been

published (not as a draft) by the Free Software Foundation. If the Document does not specify a version number of this License, you may choose any version ever published (not as a draft) by the Free Software Foundation.

## **ADDENDUM: How to use this License for your documents**

To use this License in a document you have written, include a copy of the License in the document and put the following copyright and license notices just after the title page:

*Copyright (C) year your name.*

*Permission is granted to copy, distribute and/or modify this document under the terms of the GNU Free Documentation License, Version 1.2 or any later version published by the Free Software Foundation; with no Invariant Sections, no Front-Cover Texts, and no Back-Cover Texts. A copy of the license is included in the section entitled “GNU Free Documentation License”.*

If you have Invariant Sections, Front-Cover Texts and Back-Cover Texts, replace the “with... Texts.” line with this:

*with the Invariant Sections being list their titles, with the Front-Cover Texts being list, and with the Back-Cover Texts being list.*

If you have Invariant Sections without Cover Texts, or some other combination of the three, merge those two alternatives to suit the situation.

If your document contains nontrivial examples of program code, we recommend releasing these examples in parallel under your choice of free software license, such as the GNU General Public License, to permit their use in free software.

# Literaturverzeichnis

- [1] Borewicz, S. I. und Šafarevič, I. R.: Zahlentheorie. Birkhäuser Verlag Basel und Stuttgart 1966.
- [2] Cohen, H.: A Course in Computational Algebraic Number Theory. Springer-Verlag Berlin e.a. 1996<sup>3</sup>.
- [3] Dickson, L. E.: History of the Theory of Numbers. Carnegie Institute of Washington. Vol. I: 1919, Vol. II: 1920, Vol. III: 1923. Nachdruck bei Chelsea Publishing Company New York 1971.
- [4] Ebbinghaus, H. D., Hermes, H., Hirzebruch, F., Koecher, M., Mainzer, K., Neukirch, J., Prestel, A. und Remmert, R.: Zahlen. Springer-Verlag Berlin e.a. 1988<sup>2</sup>.
- [5] Engel, A.: Problem-Solving Strategies. Springer-Verlag New York e.a. 1998.
- [6] Euklid: Die Elemente; deutsche Übersetzung von C. Thaer. Friedr. Vieweg & Sohn Verlagsgesellschaft Braunschweig 1973.
- [7] de Finetti, B.: Die Kunst des Sehens in der Mathematik; deutsche Übersetzung von L. Bechtolsheim. Birkhäuser Verlag Basel und Stuttgart 1974.
- [8] Forster, O.: Algorithmische Zahlentheorie. Friedr. Vieweg & Sohn Verlagsgesellschaft Braunschweig/Wiesbaden 1996.
- [9] Gauß, C. F.: Disquisitiones arithmeticae, Lipsiae in commissis apud Gerh. Fleischer Iun. 1801; deutsche Übersetzung mit dem Titel "Untersuchungen über höhere Arithmetik" von H. Maser 1889. Nachdruck bei Chelsea Publishing Company New York 1965.

- [10] Guy, R. K.: *Unsolved Problems in Number Theory*. Springer-Verlag New York e.a. 1981.
- [11] Hardy, G. H. und Wright, E. M.: *Einführung in die Zahlentheorie*; deutsche Übersetzung von H. Ruoff. R. Oldenbourg München 1958.
- [12] Landau, E.: *Handbuch der Lehre von der Verteilung der Primzahlen*. Teubner Verlag Leipzig 1909. Nachdruck bei Chelsea Publishing Company New York 1953.
- [13] Larson, L. C.: *Problem-Solving Through Problems*. Springer-Verlag New York e.a. 1983<sup>2</sup>.
- [14] *Mathkompass*: Website <http://www.math.uni-muenster.de/u/mollerh>.
- [15] Möller, H.: *Algorithmische Lineare Algebra*. Friedr. Vieweg & Sohn Verlagsgesellschaft Braunschweig/Wiesbaden 1997.
- [16] Möller, H.: *Zahlgenese*. Hypertext-Buch in [14] 2011.
- [17] Pólya, G.: *Schule des Denkens. Vom Lösen mathematischer Probleme*; englisch 1944, deutsche Übersetzung von E. Behnke. Francke Verlag Bern und München 1967<sup>2</sup>.
- [18] Pólya, G.: *Mathematik und plausibles Schließen*. Zwei Bände; englisch 1954, deutsche Übersetzung von L. Bechtolsheim. Birkhäuser Verlag Basel und Stuttgart 1969<sup>2</sup>/1975<sup>2</sup>.
- [19] Pólya, G.: *Vom Lösen mathematischer Aufgaben. Einsicht und Entdeckung, Lernen und Lehren*. Zwei Bände; englisch 1961/1965, deutsche Übersetzung von L. Bechtolsheim. Birkhäuser Verlag Basel und Stuttgart 1966/1967.
- [20] Remmert, Reinhold und Ullrich, Peter: *Elementare Zahlentheorie*. Birkhäuser Verlag Basel, Boston 1987.
- [21] van der Waerden, B. L.: *Erwachende Wissenschaft. Ägyptische, babylonische und griechische Mathematik*; deutsche Übersetzung von H. Habicht. Birkhäuser Verlag Basel und Stuttgart 1966<sup>2</sup>.

# Index

- ABEL, N. H., 96  
BERNOULLI, JAK., 213  
BOLZANO, B., 9  
CANTOR, G., 8  
CHEN JING RUN, 75  
DEDEKIND, R., 9, 164, 174  
DESCARTES, R., 145, 185  
DICKSON, L. E., 15  
DIOPHANT, 27, 38, 143  
DIRICHLET, P. G., 71, 85, 99, 180  
ENGEL, A., 190, 195  
ERATOSTHENES, 63  
EUKLID, 8, 14, 37, 48, 50, 58  
EULER, L., 14, 58, 67, 94, 98, 99, 141, 184, 195  
FERMAT, P. DE, 15, 99, 141, 231  
FINETTI, B. DE, 187  
GALOIS, E., 97  
GAUß, C. F., 3, 15, 31, 61, 72, 83, 96, 106, 114, 124, 127, 140, 145, 156, 160, 161, 164, 179  
HADAMARD, J., 75  
HILBERT, D., 8  
IVORY, J., 98  
JACOBI, C. G. J., 111, 129  
KRONECKER, L., 15, 164  
KUMMER, E. E., 174  
LAGRANGE, J. L., 103, 143, 156, 170  
LANDAU, E., 146  
LARSON, L. C., 188  
LEGENDRE, A. M., 108, 145  
LEHMER, D. H., 60  
LUCAS, E., 60  
MERSENNE, M., 59  
MÖBIUS, A. F., 64  
PAPPUS, 34  
PEANO, G., 7  
PLATON, 34  
PÓLYA, G., 32, 59, 182, 211  
PYTHAGORAS, 37  
RIEMANN, B., 73  
SHANKS, D., 162  
STIRLING, J., 215  
SUN-TSU, 104  
TSCHEBYSCHIEFF, P. L., 72  
VALLÉE-POUSSIN, CH. DE LA, 75  
WARING, E., 102  
WILES, A., 15, 203  
WILSON, SIR J., 102  
ZERMELO, E., 51  
abelsch, 96  
Abstiegsstrategie, 142, 230  
algebraischer Zahlkörper, 174  
ambige Form, 161  
ambige Klasse, 162  
Analyse, 34  
Anfang, 9  
Anfangspostulat, 9

- Anzahlfunktion  
der Primpotenzteiler, 53  
der Primteiler, 53
- äquivalent, 153
- Äquivalenz, 153
- Äquivalenz von Formen, 146
- Äquivalenz von Idealen, 177
- Äquivalenzrelation, 146
- arithmetische Folge, 71
- Artinsche Vermutung, 127
- assoziiert, 102
- assoziierte Elemente, 173
- Auf-und-ab-Spiel, 182, 191
- Automorphismus, 97
- axiomatische Methode, 8
- Bernoullische Ungleichung, 210
- Bernoullische Zahlen, 213
- Beweistyp, 4
- binäre Addition, 44
- binäre quadratische Form, 152
- Binärsystem, 42
- Binomialformel, 65, 204
- Binomialkoeffizient, 65, 199
- Bruch, 13
- Bruchentwicklung  
g-adische, 125
- Brückenstrategie, 59, 195, 199, 211
- Bundeswettbewerb Mathematik, 4
- BWM, 4
- C-Menge, 8
- Canon Arithmeticus, 129
- CAS, 49, 76
- Composition, 158
- Computeralgebrasystem, 49, 193
- Descartessesches Schema, 185
- descente infinie, 231
- Determinante einer Form, 146
- Differenzen, 14
- diophantische Gleichung, 27
- Dirichlet-Charakter, 72
- Dirichlet-Faltung, 138
- Dirichlet-Reihe, 71
- Dirichletscher Schubfachschluss, 85
- diskreter Logarithmus, 129
- Diskriminante, 152, 164
- Diskriminante einer Ordnung, 166
- Disquisitiones arithmeticae, 3
- Divisionsalgorithmus, 126  
g-adischer, 126
- Dualsystem, 42
- dyadisches System, 42
- Ein- und Ausschaltformel, 67, 228
- Einheit, 167
- Einheitengruppe, 167
- Einheitsform, 159
- Einheitswurzeln, 97
- Einschränkung, 86
- Elementaranalyse, 211
- endliche Menge, 9
- Erkundungsstrategie, 31, 193, 219
- erzeugende Funktion, 207, 213
- Erzeugungspostulate, 9
- Euklid-Folge, 48
- Euklidischer Algorithmus, 20, 22
- Euklidisches Tupel, 20
- Euler-Kriterium, 109
- Eulersche  $\sigma$ -Rekursion, 184
- Eulersche  $\varphi$ -Funktion, 94
- Eulersche Identität, 143

- Exponentenvergleichsstrategie, 56, 227  
Extremfallstrategie, 224, 230  
Faktorzerlegung, 161  
Fallunterscheidungsstrategie, 219, 222  
Faltung, 138  
Fastprimzahlzwillinge, 75  
Fermat-Pell-Gleichungen, 27, 168, 172  
Fermat-Primzahl, 61  
Fiat-Shamir-Algorithmus, 100  
Fibonacci-Folge, 43, 205, 222  
 $\varphi$ -Funktion, 94  
finite Induktion, 21  
Fixpunkt, 229  
formale Darstellung, 52  
Formenklasse, 147  
 $g$ -adische Zahlendarstellung, 40  
Galois-Gruppe, 97  
 $\Gamma$ -Funktion, 73  
ganz-algebraisch, 164  
ganze Zahl, 13  
Gauß-Klammer, 19, 41  
Gaußsche Erkundungsstrategie, 31, 193  
gekappte Primzahlmenge, 47  
genetische Lösungsdarstellung, 185  
geometrische Reihe, 208  
geometrische Summe, 204  
geometrischer Ort, 185  
Geschlecht, 161  
geschlossene Form, 193  
ggT, 19, 54  
GIMPS, 60  
Gleichmächtigkeit, 8  
globale Strategie, 192  
Grad eines Polynoms, 101  
Grundeinheit, 169  
Grundperiodenlänge, 126  
Gruppe, 96  
    abelsche, 96  
Halbsystem, 110  
Hauptideal, 174  
Hauptordnung, 165  
Heuristik, 4, 32, 34, 191  
Hexadezimalsystem, 42  
Ideal, 174  
    ganzes, 176  
    gebrochenes, 176  
    invertierbares, 176  
ideale Zahl, 174  
Idealklasse, 177  
    im engeren Sinne, 177  
Idealklassengruppe, 177  
    im engeren Sinne, 177  
imaginär-quadratisch, 163  
IMO, 4, 190  
Index, 128  
Indexmenge, 54  
Induktion, 184  
    finite, 21  
    vollständige, 12  
Induktionsaxiom, 7  
Induktionsmenge, 12, 21  
inkommensurabel, 230  
Integrallogarithmus, 72  
Integritätsring, 90  
Internationale Mathematikolympiade, 4  
Invarianzstrategie, 99, 149, 215  
Inverses eines Ideals, 176  
Irrationalität von  $\sqrt{2}$ , 30

- Irrationalitätsbeweis, 231  
irreduzibel, 97  
irreduzibles Element, 173  
isomorph, 89
- Jacobi-Symbol, 111
- Kardinalzahl, 8  
Kardinalzahlpostulate, 8  
Kernbruch, 14, 35  
Kernbruchstrategie, 35, 38, 58, 226  
Kettenbruch, 24  
Kettenbruchalgorithmus, 25  
Kettenbruchentwicklung, 24, 170  
kgV, 54  
Klammerungsstrategie, 38, 227  
Klassenanzahl, 155  
Klassengruppe, 159  
Klassenzahl, 162, 179  
kleinstes gemeinsames Vielfaches, 54  
Koeffizientenvergleich, 201, 204, 206  
kommutativ, 96  
Kongruenz, 83  
Konjugation, 164  
Kontraposition, 59, 202  
Körper, 90  
Körpergrad, 97  
Kreisteilungskörper, 97  
Kreisteilungspolynom, 97  
Kryptographie, 100
- L-Reihe, 72, 180  
Legendre-Symbol, 108  
lineare Kongruenz, 91  
lokale Strategie, 192  
Lösung, 27, 101  
Lösungsgenese, 182
- Lucas-Lehmer-Test, 60
- Mathematisieren, 186, 198  
Mathkompass, 2, 8, 182  
Maximalordnung, 165  
Maximum, 11  
Mersenne-Primzahl, 59  
Methodik, 191  
methodischer Typ, 4  
Mikrostrategie, 192, 226  
Minimum, 11  
Möbius-Funktion, 64  
Modifizierungsstrategie, 201  
Modul, 83  
modulo, 83  
Multiplikation von Idealen, 174  
multiplikativ, 137
- Nachfolgerabbildung, 7, 10  
Näherungsbruch, 24  
Nimspiel, 44, 191  
Norm, 164  
Norm eines Ideals, 176  
Normgleichung, 165  
nullteilerfreier Ring, 90  
Numerustafel, 129
- Oktalsystem, 42  
Ordnung, 120, 162  
Ordnung in Zahlkörpern, 165
- PARI, 49  
Parität, 164, 215  
Partialbruchzerlegung, 208  
Peano-Axiome, 7  
Peano-Struktur, 7  
Pellsche Gleichungen, 27, 168, 172

- periodische Folge, [126](#)
- Permutation, [229](#)
- Pólyasche Brückenstrategie, [211](#)
- positiv-definit, [148](#), [153](#)
- Postulat-Methode, [8](#)
- Potenznichtrest, [106](#)
- Potenzrest, [106](#)
- Potenzsumme, [212](#)
- Primärzerlegung, [50](#)
- prime Restklasse, [93](#)
- prime Restklassengruppe, [96](#)
- primes Restsystem, [93](#)
- Primideal, [174](#)
- primitive Einheitswurzeln, [97](#)
- primitive Form, [154](#)
- primitive Wurzel, [122](#)
- Primitivwurzel, [122](#)
- Primpotenzdarstellung, [52](#)
- Primpotenzteileranzahl, [53](#)
- Primteileranzahl, [53](#)
- Primzahl, [14](#), [47](#)
- Primzahlfunktion, [62](#)
- psychologische Brückenstrategie, [196](#)
- psychologischer Block, [37](#)
- pythagoreische Tripel, [37](#)
  
- quadratfreie Zahl, [65](#)
- quadratische Form
  - binäre, [152](#)
  - ternäre, [146](#)
- quadratischer Zahlkörper, [163](#)
- Quadratwurzel modulo  $m$ , [100](#)
  
- rationale Zahl, [24](#)
- Rationalitätskriterium, [37](#)
- Reduktionsalgorithmus, [159](#), [160](#)
  
- reduzierte Form, [156](#)
- reduziertes Restsystem, [93](#)
- reell-quadratisch, [163](#)
- reelle Zahl, [24](#)
- reinperiodische Folge, [126](#)
- Rekursionsverfahren, [186](#)
- Repräsentant, [84](#), [156](#)
- Restklasse, [84](#)
- Restklassenkörper, [90](#)
- Restklassenring, [89](#)
- Reziprokenabbildung, [90](#)
- reziproker Rest, [102](#)
- Riemannsche Vermutung, [74](#)
- Riemannsche Zetafunktion, [73](#)
- Ring, [88](#)
  - kommutativer, [88](#)
  - mit Einselement, [88](#)
  - nullteilerfreier, [90](#)
- RSA-Verfahren, [100](#)
- Rückwärtsstrategie, [34](#), [58](#), [66](#), [209](#)
  
- Safe-Programm, [182](#), [191](#)
- SAGE, [49](#)
- Schließen
  - analoges, [184](#)
  - demonstratives, [183](#)
  - induktives, [184](#)
  - plausibles, [183](#)
- Schrankensatz, [211](#)
- Schubfachprinzip, [85](#)
- Schwierigkeitsgrad, [4](#)
- Sedezimalsystem, [42](#)
- Sieb des Eratosthenes, [63](#)
- Siebformel, [228](#)
- Siebverfahren, [75](#)
- $\sigma$ -Primzahlkriterium, [58](#)

- $\sigma$ -Rekursion, 184
- Signal, 203
- Spur, 164
- Standardhalbsystem, 112
- Stellenwertsystem, 40
- Stirlingsche Zahlen, 215
- Strategie
  - Abstiegs-, 142, 230
  - Brücken-, 59, 195, 199, 211
  - Erkundungs-, 31, 193, 219
  - Exponentenvergleichs-, 56, 227
  - Extremfall-, 224, 230
  - Fallunterscheidungs-, 219, 222
  - globale, 192
  - Invarianz-, 99, 149, 215
  - Kernbruch-, 35, 38, 58, 226
  - Klammerungs-, 38, 227
  - lokale, 192
  - Mikro-, 192, 226
  - Modifizierungs-, 201
  - Rückwärts-, 34, 58, 66, 209
  - Symmetrie-, 115, 218
  - Umformulierungs-, 198
  - Verallgemeinerungs-, 26, 110, 162, 197, 203, 210
  - Visualisierungs-, 115, 225
  - Wechselwegnahme-, 67, 228
  - Zurückführungs-, 21, 38, 143, 222
- Summatorfunktion, 138
- Superpositionsverfahren, 186
- Symmetriestrategie, 115, 218
- Synthese, 34
- systematisches Probieren, 195
- Teiler, 17, 167
- Teileranzahlfunktion, 18
- teilerfremd, 23
- Teilersummenfunktion, 56
- Teilnenner, 24
- ternäre quadratische Form, 146
- Theorem, 60
- Umformulierungsstrategie, 198
- unendliche Menge, 9
- unendlicher Abstieg, 142
- Verallgemeinerungsstrategie, 26, 110, 162, 197, 203, 210
- Vertreter, 84
- Visualisierungsstrategie, 115, 225
- vollkommene Zahl, 57
- vollständiger Quotient, 24
- vollständiges Restsystem, 85
- Vorwärtsschließen, 211
- Wechselwegnahmestrategie, 67, 228
- Wurzel, 101
- Zahlensystem, 8
- zahlentheoretische Funktion, 18, 137
- Zahlgenease, 8, 35
- $\mathbb{Z}$ -Basis, 178
  - zulässige, 178
- zerlegbare Form, 152
- zerlegbare Zahl, 62
- Zugehörigkeitspostulate, 9
- zulässige  $\mathbb{Z}$ -Basis, 178
- Zurückführungsstrategie, 21, 38, 143, 222
- Zweipersonen-Gewinnspiel, 191
- zyklische Vertauschung, 125