Elemente der Zahlentheorie

(Lehramt)

Dr. Theo Overhagen
Mathematik
Universität Siegen

Literatur

[1] Bartholomé, Rung, Kern: Zahlentheorie für Einsteiger. Vieweg-Teubner 2010 (e-book Unibibliothek Siegen).

[2] Benölken, Gorski, Müller-Philipp: Leitfaden Arithmetik. Springer Spektrum 2018 (e-book Unibibliothek Siegen).

[3] Burton: Handbuch der elementaren Zahlentheorie, Heldermann 2005.

[4] Padberg: Elementare Zahlentheorie. Spektrum Akad.Verlag 2008.

[5] Padberg, Büchter: Vertiefung Mathematik Primarstufe - Arithmetik/Zahlentheorie. Springer Spektrum 2014 (e-book Unibibliothek Siegen).

[6] Reiss, Schmieder: Basiswissen Zahlentheorie. Springer Spektrum 2014 (e-book Unibibliothek Siegen).

[7] Scheid: Zahlentheorie. Spektrum Akad.Verlag 2006.

[8] Scheid, Schwarz: Elemente der Arithmetik und Algebra. Springer Spektrum 2015 (e-book Unibibliothek Siegen).

0 Vorwort

Zu Beginn der Entwicklung der Mathematik als logischer Wissenschaft im antiken Griechenland standen neben den geometrischen Objekten die Zahlen im Mittelpunkt des Interesses. Dabei verstand man unter Zahlen im wesentlichen die ganzen Zahlen und Verhältnisse ganzer Zahlen (rationale Zahlen), i.a. aber nicht irrationale Zahlen wie $\sqrt{2}$ oder π. (Die Notwendigkeit der Untersuchung der irrationalen Zahlen ergab sich eigentlich aus Entdeckungen in der Geometrie, insbesondere der Inkommensurabilität von bestimmten Strecken wie von Seite und Diagonalen eines Quadrats.) Entsprechend wurde die Lehre von den Zahlen, auch Zahlentheorie oder Arithmetik genannt, von den Mathematikern der griechischen Antike sehr weit entwickelt.

Wir werden uns in dieser Vorlesung im wesentlichen mit Problemen der Teilbarkeit innerhalb der Menge der ganzen Zahlen beschäftigen. Die Aussagen waren größtenteils auch schon in der Antike bekannt. Natürlich hat sich die Zahlentheorie als mathematische Disziplin weiterentwickelt, zum Beispiel in die analytische und die algebraische Zahlentheorie, die diophantische Approximation und die Geometrie der Zahlen.

Als bekannt wird vorausgesetzt die Einführung der Menge $\mathbb{N}$ der natürlichen Zahlen durch die Peano-Axiome:

Gelten für eine Menge $\mathbb{N}$ und eine Funktion $f : \mathbb{N} \to \mathbb{N}$ folgende Eigenschaften:

P1: $1 \in \mathbb{N}$, d.h. die Eins ist eine natürliche Zahl,

P2: Für alle $x \in \mathbb{N}$ gilt $f(x) \neq 1$, d.h. die Eins ist kein Nachfolger irgendeiner natürlichen Zahl,

P3: Für alle $x, y \in \mathbb{N}$ mit $x \neq y$ gilt $f(x) \neq f(y)$, d.h. verschiedene Zahlen haben verschiedene Nachfolger,

P4: Enthält eine Teilmenge $T \subset \mathbb{N}$ das Element 1 und mit jedem $x \in T$ auch $f(x)$, dann ist $T = \mathbb{N}$,

dann heißt $\mathbb{N}$ **Menge der natürlichen Zahlen**.

Weiter werden als bekannt vorausgesetzt die Einführung der Addition und Multiplikation in $\mathbb{N}$ mit den entsprechenden Rechenregeln

- Assoziativität und Kommutativität von $+$ und $\cdot$, Multiplikation von Summen (Distributivität),
- die Eigenschaften von 0 bezüglich der Addition und der 1 bezüglich der Multiplikation,

sowie die Erweiterungen von $\mathbb{N}$ auf die Menge $\mathbb{Z}$ der ganzen Zahlen und von $\mathbb{Z}$ auf die Menge $\mathbb{Q}$ der rationalen Zahlen.

Mathematik als logische Wissenschaft ist dadurch gekennzeichnet, dass Eigenschaften von bestimmten zu untersuchenden Objekten nicht nur wahrgenommen und festgestellt werden, sondern durch logische Schlüsse aus vorher als wahr angenommenen Aussagen („Axiomen“) oder als wahr erkannten Aussagen („Sätzen“) hergeleitet („bewiesen“) werden.

Als wesentliche Beweismethoden benutzen wir den

- **direkten Beweis** (aus Aussage A folgt Aussage B, kurz $A \Longrightarrow B$),
- den **Beweis durch Widerspruch**
  (angenommen, Aussage A ist wahr und Aussage B ist falsch, dann ergibt sich ein Widerspruch zur einer vorher als wahr bewiesenen Aussage; daher muss Aussage B wahr sein.).
  Er ist sehr ähnlich zum **indirekten Beweis**
  (man zeigt: wenn B falsch ist, dann ist A auch falsch, kurz $\neg B \Longrightarrow \neg A$),
- und den **Beweis durch vollständige Induktion**, eine Beweismethode, die sich aus der Gültigkeit des Peano-Axioms (P4) ergibt und daher sich für den Nachweis von Eigenschaften natürlicher Zahlen anbietet.

Die Funktion aus den Peano-Axiomen sortiert die natürlichen Zahlen nach ihrer Größe, gibt also eine Beziehung zwischen je zwei natürlichen Zahlen an. In der Mathematik werden solche Beziehungen durch den Begriff der **Relation** ausgedrückt als Menge von Paaren einer Grundmenge (hier z.B. $\mathbb{N}$), die in dieser Beziehung stehen bzw. die Relation erfüllen.

Spezielle als bekannt vorausgesetzte Arten von Relationen sind die **Ordnungsrelationen** (zum Beispiel „$<$“ in $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ oder $\mathbb{R}$) und die **Äquivalenzrelationen**.

Die Funktion aus den Peano-Axiomen erzeugt die bekannte Ordnungsrelation $<$ in $\mathbb{N}$, und aus dem Induktionsaxiom (P4) folgt der

Wohlordnungssatz: Zu jeder nichtleeren Teilmenge M der natürlichen Zahlen gibt es kleinstes Element, d.h. ein eindeutig bestimmtes $x \in M$ mit $x \leq n$ für alle $n \in M$.

Zahlentheorie galt lange Zeit zwar als „Perle der Mathematik“, aber auch als wenig relevant für Anwendungen.

Wir tauschen aber zunehmend über die ziemlich offenen Kommunikationswege des Internets sensible Daten (Geldtransfers, Kreditkartennummern usw.). Das ist nur möglich, wenn diese Daten sicher verschlüsselt werden.

Hier stellt die Zahlentheorie (noch) geeignete Hilfsmittel zur Verfügung, und sie entwickelt für eine Zukunft mit noch mehr Computer-Rechenleistung geeignete Alternativ-Methoden.

Zu dieser Entwicklung ein aktueller dpa-Bericht:

08. Januar 2010: In einer Gemeinschaftsaktion haben internationale Institute einen 768-Bit-Schlüssel geknackt. Schon bald wollen sie den 1024-Bit-Schlüssel auslesen. Experten warnen vor großen Sicherheitslücken.

Die heute gebräuchlichen Schlüssel zur Sicherung etwa von Kreditkartennummern im Internet könnten nach Erkenntnissen von Forschern schon in einigen Jahren unsicher werden. Ein internationales Team unter Bonner Beteiligung hat jetzt einen 768 Bit langen Schlüssel geknackt. Das sei eine Zahl mit 232 Stellen und damit Weltrekord, teilte die Universität Bonn am Freitag mit.

Damit sind die Forscher dem aktuell gängigen Schlüssel von 1024 Bit schon ein Stück näher gekommen. Die Forscher nutzten ein Computernetzwerk. Auf einem herkömmlichen PC hätte das Knacken dieses Schlüssels nach ihren Angaben rund 2.000 Jahre gedauert.

Viele Verfahren zur Verschlüsselung sensibler Daten beruhen darauf, dass es äußerst schwierig ist, große Zahlen in ihre sogenannten Primfaktoren zu zerlegen. Primfaktoren sind diejenigen Primzahlen, die multipliziert die gesuchte Zahl ergeben. So hat etwa die Zahl 21 die Primfaktoren 3 und 7 (3 mal 7 gleich 21). Drei US-Forscher entwickelten 1977 ein Verfahren zur Datenverschlüsselung und nutzten es später auch kommerziell. Ihre nach ihren Initialen RSA"genannte Technik steckt inzwischen in jedem Internet-Browser. Ein kleines Programm verschlüsselt dort etwa Kreditkartennummern so, dass böswillige Lauscher mit ihnen nichts anfangen können.

Die jetzt geknackte Zahl trägt die nüchterne Bezeichnung RSA-768, das heißt, sie hat 768 Bit. In Dezimalschreibweise entspricht das 232 Stellen. Damit handelt es sich um das größte Zahlenungetüm von allgemeiner Form, das bislang in seine Primfaktoren zerlegt wurde. "Die Zerlegung eines 1024-Bit-Schlüssels wäre um drei Größenordnungen schwieriger als das jetzt abgeschlossene Projekt", sagte Prof. Jens Franke vom Institut für Mathematik der Universität Bonn. Dennoch werde der erste 1024-Bit-Schlüssel vermutlich noch vor Ende des Jahrzehnts geknackt. (Quelle: dpa)

1 Teilbarkeitslehre

1.1 Teilbarkeit, Division mit Rest

Ein typisches Alltagsproblem von Eltern ist, eine vorgegebene Anzahl von z.B. Bonbons gerecht zu verteilen, d.h. so, dass jedes Kind die gleiche Anzahl von Bonbons erhält.

Wir gehen von einer vorhandenen Anzahl von 18 Bonbons aus. Dann ist eine solche Verteilung offensichtlich möglich, wenn man 1 Kind, 2, 3, 6, 9 oder 18 Kinder hat. In den anderen Fällen hat man Schwierigkeiten: Es bleibt ein Restbestand von Bonbons übrig, d.h. entweder manche Kinder haben weniger Bonbons als die anderen oder man isst den Rest selbst auf.

Da man die Bonbons im allgemeinen nicht teilen kann, kommt als mathematisches Modell nur das Rechnen innerhalb der Menge $\mathbb{Z}$ der ganzen Zahlen in Frage, d.h. wir dürfen zwar addieren, subtrahieren und multiplizieren, aber nicht immer dividieren.

Definition 1.1.1 *Gegeben seien zwei ganze Zahlen $a, b \in \mathbb{Z}$.*
Gibt es eine weitere ganze Zahl $k \in \mathbb{Z}$ mit

$$a = k \cdot b,$$

dann heißt b **Teiler** *von a, und a heißt* **Vielfaches** *von b.*

k heißt **Komplementärteiler** *von a zu b.*

Man sagt: „b teilt a“ oder „a ist Vielfaches von b“ oder „Die Division von a durch b geht auf“.

Beispiele 1.1.2

(1) 18 hat die Teiler

$$1, 2, 3, 6, 9, 18, -1, -2, -3, -6, -9, -18.$$

Die zugehörigen Komplementärteiler sind

$$18, 9, 6, 3, 2, 1, -18, -9, -6, -3, -2, -1.$$

(2) -24 hat die Teiler

$$\pm 1, \pm 2, \pm 3, \pm 4, \pm 6, \pm 8, \pm 12, \pm 24.$$

Die zugehörigen Komplementärteiler sind

$$\pm 24, \pm 12, \pm 8, \pm 6, \pm 4, \pm 3, \pm 2, \pm 1.$$

(3) 1 ist Teiler jeder ganzen Zahl.

(4) Jede ganze Zahl ist Teiler der Zahl 0, aber 0 ist nur Teiler von sich.

Bemerkungen 1.1.3

(1) Die Teilbarkeit ist eine Relation, d.h. eine Beziehung zwischen den beteiligten Zahlen a und b. Im folgenden schreiben wir kurz

$$b \mid a \qquad :\Longleftrightarrow \qquad b \text{ teilt } a.$$

(2) „b teilt a“ und „a ist Vielfaches von b“ sind nur verschiedene Bezeichnungen für die **Teilbarkeitsrelation** $b \mid a$.

(3) Für das Rechnen in der Menge $\mathbb{Q}$ der rationalen Zahlen ist die obige Definition sinnlos, da jede rationale Zahl außer 0 Teiler jeder anderen rationalen Zahl ist.

(4) Offensichtlich spielen für die Gültigkeit der Teilbarkeitsrelation die Vorzeichen von a und b keine Rolle, d.h. es gilt

$$b \mid a \qquad \Longleftrightarrow \qquad (-b) \mid a \qquad \Longleftrightarrow \qquad b \mid (-a) \qquad \Longleftrightarrow \qquad (-b) \mid (-a).$$

Will man alle Teiler einer fest vorgegebenen Zahl a bestimmen, dann ist folgender Satz nützlich, der die Teilbarkeitsrelation in Beziehung zu der Ordnungsrelation in $\mathbb{N}$ bringt:

Satz 1.1.4 *Es seien $a, b \in \mathbb{Z}$, $a \neq 0$, beliebige ganze Zahlen. Dann gilt:*

(a)
$$b \mid a \qquad \Longrightarrow \qquad -|a| \leq b \leq |a|.$$

Speziell für $a, b \in \mathbb{N}$ gilt
$$b \mid a \qquad \Longrightarrow \qquad 0 < b \leq a.$$

(b) a hat höchstens $2 \cdot |a|$ Teiler aus $\mathbb{Z}$ und höchstens $|a|$ Teiler aus $\mathbb{N}$.

Bei der Bestimmung aller Teiler einer ganzen Zahl $a \neq 0$ kann man sich auf die Untersuchung der Teiler $b \in \mathbb{N}$, $b \leq |a|$, beschränken. Der nächste Satz vereinfacht die Bestimmung:

Satz 1.1.5 *Seien $a, x, y \in \mathbb{N}$ mit $x \leq y$ und $a = x \cdot y$. Dann gilt $x \leq \sqrt{a}$.*

Bemerkung 1.1.6

Hat man alle positiven Teiler x von $a \in \mathbb{Z} \setminus \{0\}$ mit $x \leq \sqrt{|a|}$ gefunden, dann ergeben sich die anderen positiven Teiler als deren Komplementärteiler.

Beispiel 1.1.7

Für $a = 240$ (mit $\sqrt{240} < 16$) ergeben sich als positive Teiler x mit $x \leq \sqrt{a}$

$$1, 2, 3, 4, 5, 6, 8, 10, 12, 15.$$

Die zugehörigen Komplementärteiler sind

$$240, 120, 80, 60, 48, 40, 30, 24, 20, 16.$$

Die Teilbarkeitsrelation hat ähnliche Eigenschaft wie die Ordnungsrelation $<$ auf $\mathbb{N}$:

Satz 1.1.8 *Für alle $a, b, c \in \mathbb{Z}$ gilt:*

(a) $a \mid a$. *(Reflexivität)*

(b) Aus $a \mid b$ und $b \mid c$ folgt $a \mid c$. *(Transitivität)*

(c) Aus $a \mid b$ und $b \mid a$ folgt $|a| = |b|$.

Es ist nicht erstaunlich, dass die Teilbarkeitsrelation, die mit Hilfe der Multiplikation definiert ist, in gewisser Weise mit der Multiplikation verträglich ist.

Aber auch für ganzzahlige **Linearkombinationen** zweier ganzer Zahlen a und b, d.h. Zahlen der Form $m \cdot a + n \cdot b$ mit $m, n \in \mathbb{Z}$, kann man entsprechende Feststellungen machen:

Satz 1.1.9 *Seien $a, b, c, d \in \mathbb{Z}$. Dann gilt:*

(a) Aus $b \mid a$ und $d \mid c$ folgt $(b \cdot d) \mid (a \cdot c)$.

(b) Ist c gemeinsamer Teiler von a und b, d.h. es gilt $c \mid a$ und $c \mid b$, dann teilt c auch jede Linearkombination von a und b, speziell auch die Summe, die Differenz und jedes ganzzahlige Vielfache von a und b.

(c) Gilt $a = b + c$ und d teilt zwei der Zahlen a, b, c, dann teilt d auch die dritte.

Wenn die Verteilung der Bonbons nicht aufgeht, d.h. die Anzahl der Kinder kein Teiler der Anzahl der Bonbons ist, dann kann man auch an alle Kinder gleich viele Bonbons verteilen, aber es bleibt ein Rest.

Wir verallgemeinern dies auf ganze Zahlen:

Definition 1.1.10 *Gegeben seien zwei ganze Zahlen $a, b \in \mathbb{Z}$.*

Gibt es ganze Zahlen $k, r \in \mathbb{Z}$ mit

$$a = k \cdot b + r, \qquad 0 \leq r < b,$$

dann heißt r **Rest** *bei Division von a durch b.*

Beispiele 1.1.11

(1) Es gilt:
$$5 = 1 \cdot 3 + 2,$$
d.h. 2 ist Rest bei Division von 5 durch 3.

(2) Analog gilt:
$$-11 = (-4) \cdot 3 + 1,$$
d.h. 1 ist Rest bei Division von -11 durch 3, und
$$2 = 0 \cdot 3 + 2,$$
d.h. 2 ist Rest bei Division von 2 durch 3.

Bemerkungen 1.1.12

(1) Division von a durch b ergibt genau dann den Rest 0, wenn b Teiler von a ist.

(2) Die Division mit Rest in $\mathbb{Z}$ kann man auch sinnvoll auf Mengen anderer Objekte verallgemeinern. Man braucht dazu eine Multiplikation in dieser Menge und eine Relation, die misst, dass das Restelement „kleiner“ als der Teiler ist.

In $\mathbb{Z}$ ist diese Relation die übliche Kleinerrelation.

Betrachtet man als Objekte Polynome mit Koeffizienten z.B. aus $\mathbb{Q}$ oder $\mathbb{R}$, die übliche Multiplikation von Polynomen und als Relation die Ordnung nach dem Grad der Polynome, dann ergibt sich die aus der Schule bekannte **Polynomdivision**.

Aus der Erfahrung weiß man, dass bei vorgebener Bonbon- und Kinderzahl sowie maximaler gleichmäßiger Aufteilung immer die gleiche Anzahl von Bonbons übrig bleibt. Auch die Anzahl der Bonbons je Kind ist durch Bonbon- und Kinderzahl festgelegt.

Für die Division mit Rest in $\mathbb{Z}$ kann man dies mit Hilfe des Wohlordnungssatzes beweisen:

Satz 1.1.13 *Es seien $a \in \mathbb{Z}$, $b \in \mathbb{N}$. Dann gibt es eindeutig bestimmte $k, r \in \mathbb{Z}$ mit*
$$a = k \cdot b + r \qquad \textit{und} \qquad 0 \leq r < b.$$

1.2 Teiler, Primzahlen

Wir betrachten eine ganze Zahl $a \in \mathbb{Z}$, $a \neq 0$, und bezeichnen im folgenden mit
$$T_a := \{n \in \mathbb{N};\, n \mid a\}$$
die Menge der positiven Teiler von a.

Satz 1.2.1 *Für $a, b \in \mathbb{N}$ gilt*
$$a \mid b \qquad \Longleftrightarrow \qquad T_a \subset T_b.$$

Nach 1.1.4 (2) hat T_a höchstens $|a|$ Elemente.

Andererseits sind 1 und $|a|$ immer Teiler, d.h. T_a hat für $|a| \neq 1$ mindestens die 2 Elemente 1 und $|a|$. Man nennt diese Teiler **triviale Teiler**.

Alle anderen positiven Teiler von a nennt man **echte Teiler** von a (für diese gilt also $1 < b < |a|$).

Entsprechend definiert man triviale und echte Vielfache einer ganzen Zahl a.

Definition 1.2.2 *Eine natürliche Zahl $a \in \mathbb{N}$, $a \neq 1$, heißt* **Primzahl**, *wenn a keine echten Teiler hat, und sonst heißt a* **zusammengesetzt**.

Beispiele und Bemerkungen 1.2.3

(1) Die zehn kleinsten Primzahlen sind

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29.$$

(2) Die Zahlen 1 und -1 spielen in diesem Zusammenhang eine besondere Rolle: Sie sind die einzigen ganzen Zahlen, deren Teilermenge aus genau einem Element besteht. Man nennt sie auch **Einheiten**. 1 ist also per definitionem keine Primzahl.

Wir können damit die ganzen Zahlen nach der Anzahl der Elemente ihrer Teilermenge klassifizieren:

$a = 0$	$\Longleftrightarrow$	T_a	hat unendlich viele Elemente.
$a = \pm 1$	$\Longleftrightarrow$	T_a	hat genau 1 Element.
$\|a\|$ ist Primzahl	$\Longleftrightarrow$	T_a	hat genau 2 Elemente.
$\|a\|$ ist zusammengesetzt	$\Longleftrightarrow$	T_a	hat endlich viele, aber mehr als 2 Elemente.

(3) Ist $a \in \mathbb{N}$, $a > 1$, keine Primzahl, dann hat a mindestens einen echten Teiler $b \in \mathbb{N}$ mit $1 < b < a$. Mit dem zugehörigen Komplementärteiler $c \in \mathbb{N}$ gilt

$$a = b \cdot c,$$

d.h. a ist als Produkt kleinerer natürlicher Zahlen darstellbar. Das erklärt die Bezeichnung „zusammengesetzt“.

Zusammengesetzte Zahlen haben nach Definition echte Teiler. Der nächste Satz sagt aus, dass es immer solche Teiler gibt, die selbst eine Primzahl sind. Man nennt solche Teiler **Primteiler**

Satz 1.2.4 *Sei $a \in \mathbb{N}$. Dann ist die kleinste natürliche Zahl $b \neq 1$, die a teilt, eine Primzahl.*

Will man alle Primzahlen bis zu einer bestimmten Zahl $n \in \mathbb{N}$ mit Hilfe der Definition bestimmen, dann ist das ein mühsames und zähes Unterfangen. Von **Eratosthenes** (von Kyrene, ca. 275-194 v.Chr.) stammt ein einfacher und effektiver Algorithmus zur Bestimmung aller dieser Primzahlen, das sogenannte **Sieb des Eratosthenes**:

Schritt 1: Schreibe alle natürlichen Zahlen von 1 bis n auf. Streiche die 1.

Schritt 2: Ist das Quadrat der kleinsten Zahl, die weder gestrichen noch gekennzeichnet ist, größer als n, dann ist die Menge der nicht gestrichenen Zahlen gleich der Menge der Primzahlen $\leq n$, und man ist fertig.

Schritt 3: Sonst kennzeichnet man diese kleinste Zahl (als Primzahl) und streicht alle ihre echten Vielfachen.

Schritt 4: Fahre mit Schritt 2 fort.

Beispiel 1.2.5

$n = 99$. $\boxed{7}$ bedeutet die gekennzeichnete Primzahl 7, *4* die gestrichene Zahl 4, **73** die sich nach Abbruch ergebende Primzahl 73. Es gilt $\sqrt{99} < 10$.

	$\boxed{2}$	$\boxed{3}$	4	$\boxed{5}$	6	$\boxed{7}$	*8*	*9*	*10*
11	*12*	**13**	*14*	*15*	*16*	**17**	*18*	**19**	*20*
21	*22*	**23**	*24*	*25*	*26*	*27*	*28*	**29**	*30*
31	*32*	*33*	*34*	*35*	*36*	**37**	*38*	*39*	*40*
41	*42*	**43**	*44*	*45*	*46*	**47**	*48*	*49*	*50*
51	*52*	**53**	*54*	*55*	*56*	*57*	*58*	**59**	*60*
61	*62*	*63*	*64*	*65*	*66*	**67**	*68*	*69*	*70*
71	*72*	**73**	*74*	*75*	*76*	*77*	*78*	**79**	*80*
81	*82*	**83**	*84*	*85*	*86*	*87*	*88*	**89**	*90*
91	*92*	*93*	*94*	*95*	*96*	**97**	*98*	*99*	

Bemerkungen 1.2.6

(1) Die 1 wird gestrichen, da sie nach Definition keine Primzahl ist.

(2) Im Schritt 3 streicht man alle echten Vielfachen der gefundenen Primzahl. Mit diesem Verfahren werden auch irgendwann automatisch alle Vielfachen der zusammengesetzten Zahlen gestrichen, da für jede zusammengesetzte Zahl nach Satz 1.2.4 der kleinste natürliche Teiler ungleich 1 eine Primzahl ist, und damit ein solches Vielfaches schon als Vielfaches dieser Primzahl gestrichen wird.

(3) Hat man alle echten Vielfachen einer Zahl gestrichen, dann ist die erste darauffolgende nichtgestrichene Zahl eine Primzahl. Wäre sie zusammengesetzt, dann hätte sie einen kleineren Primteiler und wäre als echtes Vielfaches dieses Primteilers gestrichen worden.

(4) Das Verfahren stoppt im Schritt 2, wenn alle zu untersuchenden Zahlen größer als $\sqrt{n}$ sind. Alle noch nicht gestrichenen Zahlen sind dann Primzahlen. Sonst wäre eine solche Zahl a zusammengesetzt, d.h. es gibt $b, c \in \mathbb{N}$ mit $1 < b \leq c < n$ und $a = b \cdot c$, d.h. a ist echtes Vielfaches von b. Da a nicht gestrichen ist, muss $b > \sqrt{n}$ gelten. Daraus ergibt sich aber

$$a = b \cdot c > \sqrt{n} \cdot \sqrt{n} = n$$

im Widerspruch zu $a \leq n$. Daher muss a Primzahl sein.

In dem obigen Beispiel haben wir die Zahlen in 10-Reihen angeordnet. Schreibt man sie, beginnend mit der 2, in 6-Reihen auf, dann fällt auf, dass alle Primzahlen außer 2 und 3 in den Reihen unter der 5 bzw. der 7 stehen:

2	3	*4*	5	*6*	7
8	*9*	*10*	**11**	*12*	**13**
14	*15*	*16*	**17**	*18*	**19**
20	*21*	*22*	**23**	*24*	*25*
26	*27*	*28*	**29**	*30*	**31**
32	*33*	*34*	*35*	*36*	**37**
38	*39*	*40*	**41**	*42*	**43**
44	*45*	*46*	**47**	*48*	*49*
50	*51*	*52*	**53**	*54*	*55*
56	*57*	*58*	**59**	*60*	**61**
62	*63*	*64*	*65*	*66*	**67**
68	*69*	*70*	**71**	*72*	**73**
74	*75*	*76*	*77*	*78*	**79**
80	*81*	*82*	**83**	*84*	*85*
86	*87*	*88*	**89**	*90*	*91*
92	*93*	*94*	*95*	*96*	**97**
98	*99*				

Das gilt nicht nur für die Primzahlen unter 100, sondern für alle:

Satz 1.2.7 *Ist p eine Primzahl größer als 3, dann ist sie Vorgänger oder Nachfolger eines Vielfachen von 6, d.h. darstellbar in der Form*

$$p = 6n - 1 \qquad \textit{oder} \qquad p = 6n + 1 \qquad \textit{mit} \quad n \in \mathbb{N}.$$

Bemerkungen 1.2.8

(1) Die Umkehrung gilt natürlich nicht, wie das Beispiel $25 = 4 \cdot 6 + 1$ zeigt.

(2) Aussagen wie in dem vorigen Satz erleichtern die Untersuchung, ob eine Zahl Primzahl ist oder nicht: Man muss nur Zahlen der Form $6n \pm 1$ untersuchen.

Um die Anzahl der Primzahlen zu bestimmen, gehen wir zunächst experimentell vor und bestimmen den prozentualen Anteil der Primzahlen von 1 bis n:

Natürliche Zahlen bis	10	100	1.000	10.000	100.000	1.000.000
prozentualer Anteil an Primzahlen	40	25	16, 8	12, 3	9, 6	7, 8

Mit zunehmendem n treten immer seltener Primzahlen auf, d.h. es liegt die Vermutung nahe, dass ab einer bestimmten Grenze es gar keine Primzahlen mehr gibt.

Euklid zeigte aber schon vor 2.300 Jahren, dass nicht stimmt:

Satz 1.2.9 (Euklid) *Es gibt unendlich viele Primzahlen.*

Bemerkungen 1.2.10

(1) Damit ist der Versuch, die größte Primzahl zu bestimmen, zum Scheitern verurteilt.

Aus der Kryptografie kommt die Anforderung nach möglichst großen Primzahlen. Die größte derzeit bekannte ist die 2008 gefundene Zahl $2^{43.112.609} - 1$ mit 12.978.189 Dezimalstellen.

Man konzentriert sich bei der Suche auf die sogenannten **Mersenneschen Zahlen** der Form $2^p - 1$, wobei p eine Primzahl ist, und für den Nachweis muss man eine große Anzahl von Rechnern parallel arbeiten lassen.

Zur Verdeutlichung der Größenordnung: Auf einer karierten DIN-A-4-Seite sind ca 2.500 Kästchen aufgedruckt, auf einem Blatt also ca. 5.000. Trägt man in jedes Kästchen jeweils eine Ziffer der 2008 gefundenen Zahl ein, dann benötigt man ca. 2.600 Blätter.

Für die Liste der „Rekordprimzahlen“ zusammen mit dem Jahr der Entdeckung und der Stellenzahl im Dezimalsystem sei hier auf http://primes.utm.edu/largest oder den Aufsatz in Wikipedia über Primzahlen verwiesen.

(2) Der Beweis von Satz 1.2.9, der auf Euklid zurückgeht, macht nicht den naheliegenden Versuch, zu n vorgegebenen Primzahlen die nächstgrößere zu bestimmen. Wegen der unregelmäßigen Verteilung der Primzahlen wäre dies zum Scheitern verurteilt.

(3) Der Beweis ist konstruktiv, d.h. er liefert eine unendliche Teilfolge $(p'_k)_{k\in\mathbb{N}}$ der Primzahlen:

Sei $r \in \mathbb{N}, r \geq 2$. Die Primzahlen $p'_1, ..., p'_{r-1}$ seien bekannt. Weiter sei $p(n)$ der kleinste Primteiler von n und

$$n_r := p'_1 \cdot p'_2 \cdot \ldots \cdot p'_{r-1} + 1, \qquad p'_r := p(n_r).$$

Beginnt man z.B. mit $p_1 = 2$, dann erhält man

r	1	2	3	4	5	6	7	8
n_r	–	3	7	43	1.807	23.479	1.244.335	6.221.671
p'_r	2	3	7	43	13	53	5	6.221.671

Man erkennt hier auch, dass n_r durchaus zusammengesetzt sein kann, und dass die Folge (p'_i) i.a. nicht monoton wachsend ist.

Wie dicht können Primzahlen aufeinander folgen?

Da 2 die einzige gerade Primzahl ist, steht zwischen 2 Primzahlen größer als 3 mindestens eine (gerade) Zahl. Man nennt nun Paare von Primzahlen, deren Differenz genau 2 ist, **Primzahlzwillinge**.

Zum Beispiel sind

$$(3,5), \qquad (5,7), \qquad (11,13), \qquad (65.516.468.355\cdot 2^{333333} - 1, \quad 65.516.468.355\cdot 2^{333333} + 1)$$

Primzahlzwillinge. Das letzte Paar wurde 2009 gefunden, und jede der beiden Zahlen hat 100.355 Dezimalstellen. Bisher hat man aber noch keinen Satz gefunden, der aussagt, dass es unendlich viele Primzahlzwillinge gibt. (Quelle: http://primes.utm.edu/largest)

Analog kann man nach **Primzahldrillingen** $(p, p+2, p+6)$ wie z.B. $(41, 43, 47)$ oder $(107, 109, 113)$ suchen oder nach **Primzahlvierlingen** $(p, p+2, p+6, p+8)$ wie $(5, 7, 11, 13)$.

Auf der anderen Seite ist es interessant, wie groß die Lücken zwischen 2 aufeinanderfolgenden Primzahlen werden können, oder anders ausgedrückt, wie viele zusammengesetzte Zahlen aufeinander folgen können. Zum Beispiel sind $8, 9$ zwei, $8, 9, 10$ drei und $24, 25, 26, 27, 28$ fünf aufeinanderfolgende zusammengesetzte Zahlen.

Der nächste Satz nutzt das Produkt $n!$ („n Fakultät“) aller natürlichen Zahlen von 1 bis n und zeigt, dass es beliebig große Lücken geben kann:

Satz 1.2.11 *Zu jeder natürlichen Zahl $n > 1$ gibt es n aufeinanderfolgende zusammengesetzte Zahlen.*

Man kann aber auch Intervalle angeben, in denen auf jeden Fall eine Primzahl liegt:

Satz 1.2.12 *Für alle natürlichen Zahlen $n \geq 3$ gilt: Zwischen n und $n!$ liegt mindestens eine Primzahl.*

Bemerkung 1.2.13

Wegen $1! = 1$ und $2! = 2$ gilt der Satz erst ab $n > 2$.

Obwohl die Primzahlverteilung offensichtlich sehr unregelmäßig ist, kann man „asymptotische Aussagen“ über die Anzahl $\Pi(n)$ der Primzahlen $\leq n$ machen. Diese Funktion wird nämlich mit wachsendem n immer besser durch die Funktion $\dfrac{n}{\ln n}$ beschrieben, d.h. es gilt der von Gauß (1777-1855) und Legendre (1752–1833) vermutete und 1896 von Hadamard und delaValleePoussin bewiesene

Satz 1.2.14 (Großer Primzahlsatz)

$$\lim_{n\to\infty} \frac{\Pi(n)}{\frac{n}{log\, n}} = 1.$$

Seit der Antike sucht man nach einfachen Formeln, die im Idealfall alle Primzahlen in aufsteigender Folge liefern. Wegen der gezeigten Unregelmäßigkeit des Auftretens der Primzahlen ist die Existenz einer solchen Formel aber unwahrscheinlich.

Für Formeln in Form eines Polynoms gilt

Satz 1.2.15 *Es gibt kein Polynom*

$$p(x) = a_m x^m + a_{m-1} x^{m-1} + \ldots + a_1 x + a_0$$

vom Grad $m \geq 1$ und mit ganzzahligen Koeffizienten $a_i \in \mathbb{Z}$, das für alle $x \in \mathbb{Z}$ Primzahlen als Funktionswerte hat.

Bemerkungen 1.2.16

(1) Polynome vom Grad 0 sind die konstanten Funktionen $p(x) = a_0$ mit genau einem Funktionswert, d.h. für diese Polynome ist die Aussage sinnlos.

(2) Das Polynom $p(x) = x^2 + x + 41$ liefert für $x = 0, 1, 2, \ldots, 39$ Primzahlen, aber

$$p(40) = 1681 = 41 \cdot 41$$

ist zusammengesetzt.

Polynome mit ganzzahligen Koeffizienten, die nicht nur Primzahlen als Funktionswerte haben, aber unendlich viele verschiedene, findet man leicht, und zwar sogar lineare Polynome, z.B. $p(x) = 2x + 1$. Andererseits ist $p(x) = 2x + 4$ für kein $x \in \mathbb{N} \cup \{0\}$ eine Primzahl.

Satz 1.2.17 *Gegeben sei die lineare Funktion $p(x) = ax + b$ mit $a, b \in \mathbb{Z}$.*

(a) Haben a und b außer 1 einen weiteren gemeinsamen Teiler, dann ist höchstens ein Funktionswert von $p(x)$ eine Primzahl.

(b) Haben a und b nur 1 als gemeinsamen positiven Teiler, dann gibt es unendlich viele verschiedene Funktionswerte, die Primzahlen sind.

1.3 Hauptsatz der elementaren Zahlentheorie

Nach Satz 1.2.4 hat jede zusammengesetzte Zahl mindestens einen Primteiler. Ziel dieses Abschnitts ist zu zeigen, dass man jede zusammengesetzte Zahl als Produkt nur von Primzahlen darstellen kann, und dass diese Darstellung in gewisser Weise eindeutig ist. Eine charakteristische Eigenschaft der Primzahlen gibt

Satz 1.3.1 *Sei $n \in \mathbb{N}$, $n \geq 2$. Dann gilt:*

$$n \text{ ist Primzahl} \quad \Longleftrightarrow \quad \text{für alle } a, b \in \mathbb{Z} \text{ mit } \quad n \mid (a \cdot b) \quad \text{gilt} \quad n \mid a \text{ oder } n \mid b.$$

Die Aussage des Satzes gilt auch für Produkte mehrerer Zahlen:

Korollar 1.3.1.1 *Sei $n \in \mathbb{N}$, $n \geq 2$. Dann gilt:*

$$n \text{ ist Primzahl} \quad \Longleftrightarrow \quad \text{für alle } k \in \mathbb{N},\ k > 1, \quad a_i \in \mathbb{Z}, 1 \leq i \leq k, \text{ mit } n \mid (a_1 \cdot \ldots \cdot a_k) \text{ gilt:}$$
$$\text{es gibt mindestens ein } i, 1 \leq i \leq k, \text{ mit } n \mid a_i.$$

Speziell heißt das: Teilt eine Primzahl ein Produkt endlich vieler ganzer Zahlen, dann teilt sie mindestens einen der Faktoren.

Damit erhält man folgenden

Satz 1.3.2 (Hauptsatz der elementaren Zahlentheorie) *Jede natürliche Zahl $n \geq 2$ läßt sich als Produkt von endlich vielen Primzahlen schreiben. Bis auf die Reihenfolge der Faktoren ist die Darstellung eindeutig.*

Man nennt eine solche Darstellung **Primfaktorzerlegung** von n.

Der Algorithmus aus dem Beweis ergibt ein Verfahren zur Bestimmung einer Primfaktorzerlegung. Zum Beispiel erhält man

$$1960 = 2 \cdot 2 \cdot 2 \cdot 5 \cdot 7 \cdot 7.$$

Sortiert man die Primfaktoren nach der Größe und fasst gleiche Faktoren in einer Potenz zusammen, dann erhält man die nach dem Hauptsatz eindeutig bestimmte **kanonische Primfaktorzerlegung**

$$n = p_1^{m_1} \cdot p_2^{m_2} \cdot \ldots \cdot p_r^{m_r}$$

einer natürlichen Zahl $n \geq 2$, und dabei sind $p_1, p_2, \ldots, p_r$ Primzahlen mit

$$p_1 < p_2 < \ldots < p_r$$

und $m_1, m_2, \ldots, m_r$ natürliche Zahlen.

Bemerkungen 1.3.3

(1) Die Menge der natürlichen Zahlen wird üblicherweise durch die Peano-Axiome definiert, und diese beschreiben unter anderem, wie man jede natürliche Zahl aus der Anfangszahl 1 allein durch fortgesetzte Addition mit 1 erzeugen kann.

Der Hauptsatz der elementaren Zahlentheorie zeigt andererseits, dass man die Menge $\mathbb{N}$ der natürlichen Zahlen (außer 1) mit Hilfe der Multiplikation aus der Menge der Primzahlen erzeugen kann. Die Primzahlen sind also die entsprechenden multiplikativen Bausteine, und sie können nicht durch kleinere Bausteine ersetzt werden.

(2) Der Hauptsatz wäre falsch, wenn man 1 als Primzahl festlegen würde. Zum Beispiel für 12 ergäben sich die (verschiedenen) kanonischen Primfaktorzerlegungen

$$12 = 2^2 \cdot 3 = 1 \cdot 2^2 \cdot 3 = 1^{25} \cdot 2^2 \cdot 3.$$

(3) Läßt man in der Darstellung einer natürlichen Zahl $n > 1$ auch zusammengesetzte Faktoren zu, dann gilt die Eindeutigkeitsaussage natürlich nicht. Zum Beispiel gilt

$$90 = 2 \cdot 3 \cdot 15 = 2 \cdot 5 \cdot 9 = 3 \cdot 5 \cdot 6 = 3 \cdot 3 \cdot 10$$

und dabei haben wir nur Produkte mit 3 Faktoren betrachtet.

(4) Aus der Erfahrung nimmt man die Aussage des Hauptsatzes leicht für selbstverständlich an. Man kann die Teilbarkeitslehre aber leicht auf andere Mengen (Ringe) verallgemeinern mit entsprechenden Festlegungen für „teilbar“, „Primzahl“ usw., und dort gilt der Hauptsatz i.a. nicht.

Als (zugegebenermaßen künstliches) Beispiel betrachten wir die Zahlenmenge

$$V := \{1\} \cup \{4n;\ n \in \mathbb{N}\} = \{1, 4, 8, 12, 16, \ldots\}.$$

Für $a, b \in V$ soll gelten: a teilt b genau dann, wenn es ein $k \in V$ gibt mit $b = a \cdot k$. $a \in V$ heißt „prim in V“, wenn a nur die Teiler 1 und a hat.

Die ersten 5 in V primen Zahlen sind $4, 8, 12, 20, 24$ und es gilt

$$96 \in V \qquad \text{und} \qquad 96 = 4 \cdot 24 = 8 \cdot 12.$$

(5) In der kanonischen Primfaktorzerlegung kommen nur die tatsächlichen Primteiler von n vor. Für allgemeine Überlegungen ist es manchmal nützlich, n formal als Produkt unendlich vieler Primzahlpotenzen darzustellen:

Ist $(p_1, p_2, \ldots)$ die monoton wachsende Folge aller Primzahlen, dann schreibt man

$$n = p_1^{m_1} \cdot p_2^{m_2} \cdot \ldots$$

mit nichtnegativen ganzen Zahlen $m_1, m_2, \ldots$.

$$1320 = 2^3 \cdot 3^1 \cdot 5^1 \cdot 7^0 \cdot 11^1 \cdot 13^0 \cdot \ldots.$$

1.4 Teilermenge, Teileranzahl

Wegen der Transitivität der Teilbarkeitsrelation und dem Hauptsatz 1.3.2 kann man die Teiler einer natürlichen Zahl mit bekannter Primfaktorzerlegung gut beschreiben:

Satz 1.4.1 *Sei $n \in \mathbb{N}$, $n \geq 2$, mit kanonischer Primfaktorzerlegung*

$$n = p_1^{m_1} \cdot p_2^{m_2} \cdot \ldots \cdot p_r^{m_r}.$$

$d \in \mathbb{N}$ ist genau dann Teiler von n, wenn

$$d = p_1^{k_1} \cdot p_2^{k_2} \cdot \ldots \cdot p_r^{k_r}$$

mit $0 \leq k_i \leq m_i$, $1 \leq i \leq r$.

Man kann alle Teiler von n mit Hilfe eines **Baumdiagramms** darstellen. Als Beispiel ist hier das Baumdiagramm der Zahl

$$1960 = 2^3 \cdot 5^1 \cdot 7^2,$$

aufgeführt, die die Primteiler $p_1 = 2$ mit Vielfachheit $m_1 = 3$, $p_2 = 5$ mit Vielfachheit $m_2 = 1$ und $p_3 = 7$ mit Vielfachheit $m_3 = 2$ hat.

Von einem Punkt, der **Wurzel** des Baums, geht für jede mögliche Primzahlpotenz von p_1 in der kanonischen Primfaktorzerlegung eines Teilers ein **Ast** ab. Bei unserem Beispiel ergeben sich für $p_1 = 2$ die möglichen Exponenten $k = 0$, 1, 2 oder 3, d.h. es gehen $m_1 = 4$ Äste ab.

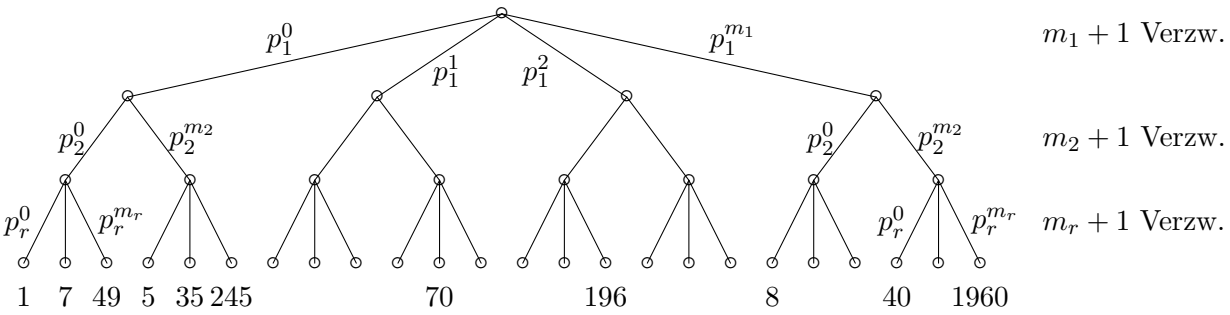
Von jedem Endpunkt dieser Äste verzweigt man weiter in m_2+1 Äste, von jedem der neuen Endpunkte in $m_3 + 1$ Äste usw. Zum Beispiel ist

Zum Schluss entspricht jeder Endpunkt der letzten Äste einem Teiler, bei unserem Beispiel dem Punkt ganz links der Teiler

$$d = p_1^0 \cdot p_2^0 \cdot \ldots \cdot p_r^0 = 1$$

und dem Punkt ganz rechts der Teiler

$$d = p_1^{m_1} \cdot p_2^{m_2} \cdot \ldots \cdot p_r^{m_r} = n.$$



Dann gilt: Jeder Weg von der Wurzel des Baumdiagramms zu einem Endpunkt entspricht einem Teiler und umgekehrt, und man erhält

Satz 1.4.2 *Eine natürliche Zahl $n > 1$ mit kanonischer Primfaktorzerlegung*

$$n = p_1^{m_1} \cdot p_2^{m_2} \cdot \ldots \cdot p_r^{m_r}$$

hat genau

$$\tau(n) := (m_1 + 1) \cdot (m_2 + 1) \cdot \ldots (m_r + 1)$$

verschiedene Teiler.

$\tau(n)$ heißt **Teileranzahlfunktion** und gibt für jede natürliche Zahl die Anzahl der positiven ganzzahligen Teiler an.

Beispiele 1.4.3

(1) 1960 hat genau $\tau(1960) = (3 + 1) \cdot (1 + 1) \cdot (2 + 1) = 24$ verschiedene Teiler.
Der kleinste ist $1 = 2^0 \cdot 5^0 \cdot 7^0$, der größte $1960 = 2^3 \cdot 5^1 \cdot 7^2$.

(2) Für eine Primzahl p gilt $\tau(p) = 2$. Ist $n = p^m$ Potenz einer Primzahl, dann gilt $\tau(n) = m + 1$.

Wir addieren nun alle positiven ganzzahligen Teiler einer natürlichen Zahl n. Die Summe bezeichnen wir mit $\sigma(n)$ und nennen die entsprechende Funktion **Teilersummenfunktion**.

Beispiele 1.4.4

(1) Es gilt

$$\sigma(1) = 1, \qquad \sigma(2) = 3, \qquad \sigma(3) = 4, \qquad \sigma(4) = 7, \qquad \sigma(6) = 12, \qquad \sigma(12) = 28.$$

(2) Für eine Primzahl p gilt $\sigma(p) = p + 1$.

Ist $n = p^m$ Potenz einer Primzahl, dann gilt $\sigma(p^m) = \dfrac{p^{m+1} - 1}{p - 1}$.

(3) Für $n = 1960$ erhält man $\sigma(1960) = 5130$.

Mit Hilfe von vollständiger Induktion zeigt man

Satz 1.4.5 *Für eine natürliche Zahl n mit kanonischer Primfaktorzerlegung*

$$n = p_1^{m_1} \cdot p_2^{m_2} \cdot \ldots \cdot p_r^{m_r}$$

gilt

$$\begin{aligned}\sigma(n) &= \sigma\big(p_1^{m_1} \cdot p_2^{m_2} \cdot \ldots \cdot p_r^{m_r}\big) = \sigma\big(p_1^{m_1}\big) \cdot \sigma\big(p_2^{m_2}\big) \cdot \ldots \cdot \sigma\big(p_r^{m_r}\big) \\ &= \frac{p_1^{m_1+1}-1}{p_1-1} \cdot \frac{p_2^{m_2+1}-1}{p_2-1} \cdot \ldots \cdot \frac{p_r^{m_r+1}-1}{p_r-1}.\end{aligned}$$

Da jede natürliche Zahl n Teiler von sich selbst ist, ist $\sigma(n)$ für $n > 1$ immer größer als n. Wie die Beispiele aus 1.4.7 zeigen, kann $\sigma(n)$ kleiner, gleich oder größer $2n$ sein, d.h. die Summe der positiven ganzzahligen Teiler außer n ist kleiner, gleich oder größer n.

In der Zahlenmystik des Pythagoras (ca.550 v.Chr) spielten natürliche Zahlen n, die gleich der Summe ihrer von n verschiedenen natürlichen Teiler sind, d.h. für die $\sigma(n) = 2n$ gilt, eine ausgezeichnete Rolle. Sie werden **vollkommene Zahlen** genannt.

6 ist zum Beispiel eine vollkommene Zahl.

Für die geraden vollkommenen Zahlen gilt

Satz 1.4.6 (Euklid-Euler) *Sei n eine gerade natürliche Zahl. Dann gilt:*

$$\begin{aligned}&n \text{ ist vollkommen} \quad \Leftrightarrow \quad \text{es gibt ein } k \in \mathbb{N}, \quad k \geq 2, \text{ mit} \\ &\qquad\qquad\qquad\qquad n = 2^{k-1} \cdot (2^k - 1) \qquad \text{und} \quad 2^k - 1 \text{ prim.}\end{aligned}$$

Bemerkungen 1.4.7

(1) Primzahlen der Form $2^k - 1$ heißen **Mersennesche Primzahlen**. $2^k - 1$ kann nur dann prim sein, wenn k prim ist.

Es gibt Primzahlen k, so dass die zugehörige Mersennesche Zahl zusammengesetzt ist:

$$2^{11} - 1 = 2047 = 23 \cdot 89.$$

Es ist nicht bekannt, ob es unendlich viele Mersennesche Primzahlen gibt.

(2) Bis heute kennt man keine vollkommene ungerade Zahl, aber auch keinen Beweis, der die Existenz einer solchen ausschließt.

Für die Aussagen über die Funktionen $\tau(n)$ und $\sigma(n)$ war die Darstellung der Teilermenge T_n mit Hilfe eines Baumdiagramms sehr nützlich. Allerdings gibt ein solches Diagramm nicht die Teilbarkeitsbeziehungen der Teiler untereinander wieder.

Zur Darstellung dieser zusätzlichen Eigenschaft sind sogenannte **Hasse-Diagramme** nützlich.

Dazu ordnet man jedem Teiler von n umkehrbar eindeutig einen Punkt der Zeichenebene zu.

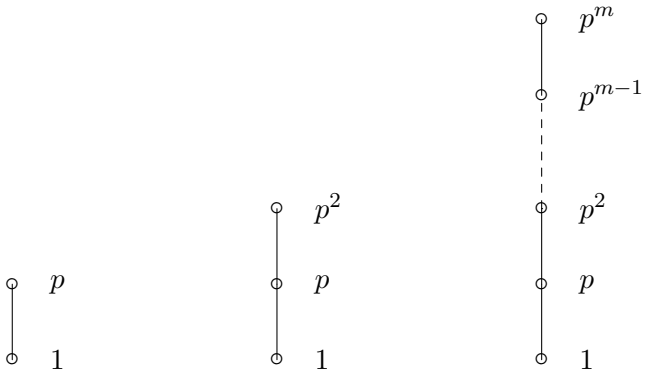
Sind $a, b \in \mathbb{N}$ Teiler von n und gilt zusätzlich $a \mid b$, dann verbindet man a mit b durch einen Pfeil von a nach b. Das entstehende Diagramm ist allerdings schon bei kleinem n sehr unübersichtlich, so dass man „selbstverständliche“ Teilbarkeitsbeziehungen wegläßt wie zum Beispiel

$$a \mid a, \qquad 1 \mid a.$$

Weiter läßt man Pfeile weg, die sich aus der Transitivität ergeben, d.h. wenn ein Pfeil von a nach b und ein Pfeil von b nach c existiert, trägt man den Pfeil von a nach c nicht ein.

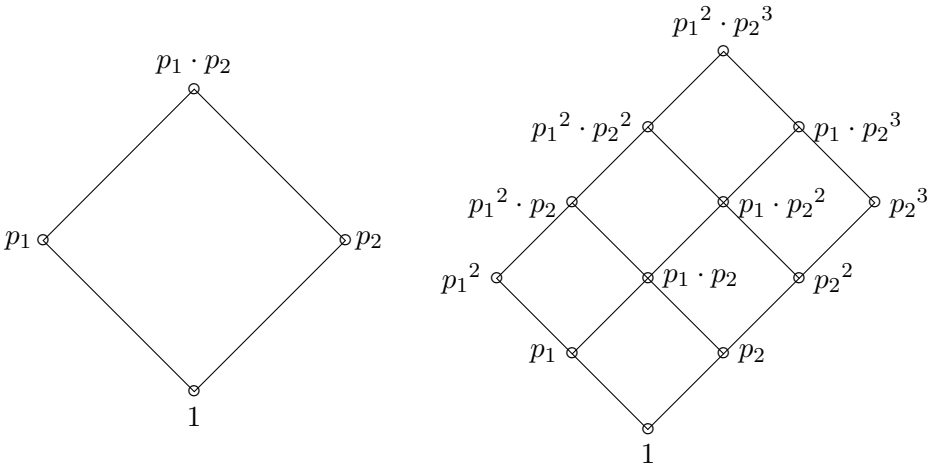
Ordnet man die zu den Teilern gehörenden Punkten so an, dass die restlichen Pfeile alle nach oben zeigen, kann man auch die Pfeilspitzen weglassen.

Für Primzahlen p und Primzahlpotenzen p^m ergibt sich

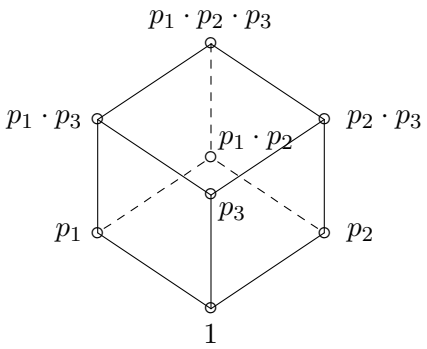


Hat n zwei oder drei verschiedene Primteiler, dann ergeben sich 2- bzw. 3-dimensionale Hasse-Diagramme.

Zum Beispiel für $n = p_1 \cdot p_2$ bzw. $n = {p_1}^2 \cdot {p_2}^3$ erhält man



und für $n = p_1 \cdot p_2 \cdot p_3$



Für 4 oder mehr verschiedene Primfaktoren bräuchte man höherdimensionale Darstellungen, die uns aber nicht so ohne weiteres zugänglich sind. Betrachtet allerdings nur Teilermengen T_n für $n \leq 1000$, dann tritt das Problem für ungerades n gar nicht und für gerades n genau 16-mal auf.

1.5 Größter gemeinsamer Teiler, kleinstes gemeinsames Vielfaches, euklidischer Algorithmus

Die durch den Bruch

$$\frac{841568}{631176}$$

dargestellte Zahl q kann man offensichtlich einfacher darstellen, indem man Zähler und Nenner durch den gemeinsamen Teiler 2 „kürzt“. Die beiden Zahlen haben aber noch andere gemeinsame Teiler, und die einfachste Form der Darstellung dieser rationalen Zahl (Bruchzahl) durch einen Bruch ergibt sich durch Kürzen mit dem größten gemeinsamen Teiler

$$210392 = 2^3 \cdot 7 \cdot 13 \cdot 17^2$$

$$\frac{841568}{631176} = \frac{4 \cdot 210392}{3 \cdot 210392} = \frac{4}{3}.$$

Wir definieren den größten gemeinsamen Teiler direkt für mehrere (endlich viele) ganze Zahlen:

Definition 1.5.1 *Seien* $n_1, ..., n_k \in \mathbb{Z}$ *mit* $\sum_{i=1}^{k} n_i^2 > 0$. *Dann heißt*

$$d := max\{q \in \mathbb{N}; q \mid n_i \text{ für alle } 1 \leq i \leq k\}$$

größter gemeinsamer Teiler *von* $n_1, ..., n_k$.

Schreibweise: $d = \mathrm{ggT}(n_1, ..., n_k)$.

Ist $\mathrm{ggT}(n_1, ..., n_k) = 1$, *dann heißen die Zahlen* $n_1, ..., n_k$ **teilerfremd**.
Gilt sogar

$$\mathrm{ggT}(n_i, n_j) = 1 \text{ für alle } 1 \leq i, j \leq k, \quad i \neq j,$$

dann heißen die Zahlen $n_1, ..., n_k$ **paarweise teilerfremd**.

Bemerkungen 1.5.2

(1) Die Menge der gemeinsamen positiven ganzzahligen Teiler von $n_1, \ldots, n_k$ ist der Durchschnitt der Teilermengen der einzelnen Zahlen, d.h. es gilt

$$T(n_1, \ldots, n_k) := \{q \in \mathbb{N}; q \mid n_i \text{ für alle } 1 \leq i \leq k\} = T_{n_1} \cap \ldots \cap T_{n_k}.$$

Da 1 gemeinsamer Teiler aller ganzer Zahlen ist, ist $T(n_1, ..., n_k)$ nicht leer.

Andererseits gilt $d_i \leq |n_i|$ für jeden positiven ganzzahligen Teiler d_i von n_i und damit

$$d \leq \min\{|n_1|, |n_2|, \ldots, |n_k|\},$$

d.h. $T(n_1, ..., n_k)$ ist endlich, wenn auch nur eine der Zahlen $n_1, \ldots, n_k$ ungleich Null ist.

Damit folgt: $\mathrm{ggT}(n_1, ..., n_k)$ ist für beliebige Wahl von $k \in \mathbb{N}$, $n_1, n_2, \ldots, n_k \in \mathbb{Z}$ mit $\sum_{i=1}^{k} n_i^2 > 0$ immer definiert.

(2) Es gilt

$$T(n_1, ..., n_k) = T(n_1, ..., n_k, 0),$$

d.h. man kann sich auf den Fall $n_i \neq 0, 1 \leq i \leq k$, beschränken.

(3) Manchmal wird der größte gemeinsame Teiler von $n_1, \ldots, n_k$ mit $(n_1, ..., n_k)$ bezeichnet.

(4) Für $k = 2$ fallen die Begriffe „teilerfremd“ und „paarweise teilerfremd“ zusammen.

Für $k \geq 3$ ist die Eigenschaft „paarweise teilerfremd“ stärker, d.h. paarweise teilerfremde Zahlen sind immer auch teilerfremd, aber die Umkehrung gilt im allgemeinen nicht.

Beispiel: 6, 10, 15 sind teilerfremd, aber nicht paarweise teilerfremd.

Wie kann man nun für 2 oder mehr beliebige ganze Zahlen den größten gemeinsamen Teiler bestimmen?

Nach Satz 1.4.1 ist d gemeinsamer positiver ganzzahliger Teiler von $n_1, \ldots, n_k$ genau dann, wenn in der kanonischen Primfaktorzerlegung

$$d = {p_1}^{m_1} \cdot \ldots \cdot {p_r}^{m_r}$$

von d jeder Primfaktor p_j, $1 \leq j \leq r$, von d auch Primfaktor jeder der Zahlen $n_1, \ldots, n_k$ ist, und zwar mit Vielfachheit höchstens m_j.

Beispiele 1.5.3

(1) Für die beiden Zahlen

$$a = 1960 = 2^3 \cdot 5^1 \cdot 7^2, \qquad b = 686 = 2^1 \cdot 5^0 \cdot 7^3$$

ergibt sich

$$\mathrm{ggT}(1960, 686) = 2^1 \cdot 5^0 \cdot 7^2 = 98.$$

(2) Für die Zahlen

$$a = 1960 = 2^3 \cdot 5^1 \cdot 7^2 \cdot 13^0, \qquad b = 686 = 2^1 \cdot 5^0 \cdot 7^3 \cdot 13^0, \qquad c = 16900 = 2^2 \cdot 5^2 \cdot 7^0 \cdot 13^2$$

ergibt sich

$$\mathrm{ggT}(1960, 686, 16900) = 2^1 \cdot 5^0 \cdot 7^0 \cdot 13^0 = 2.$$

Mit der monoton wachsenden Folge $(p_i)_{i\in\mathbb{N}}$ aller Primzahlen und der Darstellung der (oBdA. natürlichen) Zahlen $n_1, n_2, \ldots, n_k$ als (formal) unendliches Produkt der entsprechenden Primzahlpotenzen folgt:

Satz 1.5.4 *Für $n_1, n_2, ..., n_k \in \mathbb{N}$ mit den kanonischen Primfaktorzerlegungen*

$$n_j = {p_1}^{m_{j1}} \cdot {p_2}^{m_{j2}} \cdot \ldots, \qquad m_{ji} \in \mathbb{N} \cup \{0\}, \quad i \in \mathbb{N}, \quad 1 \le j \le k,$$

gilt

$$\mathrm{ggT}(n_1, ..., n_k) = {p_1}^{\min(m_{11}, m_{21}, ..., m_{k1})} \cdot {p_2}^{\min(m_{12}, m_{22}, ..., m_{k2})} \cdot \ldots.$$

$\mathrm{ggT}(n_1, n_2)$ ist nicht nur bezüglich der Ordnungsrelation in $\mathbb{N}$ der größte gemeinsame Teiler, sondern auch bezüglich der Teilbarkeitsrelation:

Satz 1.5.5 *Seien $m, n_1, n_2 \in \mathbb{N}$.*

(a) Aus $m \mid n_1$ und $m \mid n_2$ folgt $m \mid \mathrm{ggT}(n_1, n_2)$.

(b) Teilt m das Produkt $n_1 \cdot n_2$ und ist teilerfremd zu n_1, dann ist m Teiler von m_2, d.h.

$$m \mid (n_1 \cdot n_2) \quad \textit{und} \quad \mathrm{ggT}(m, n_1) = 1 \qquad \Longrightarrow \qquad m \mid n_2.$$

Die Bestimmung der Primfaktorzerlegungen der Zahlen n_1 und n_2 kann recht mühsam sein. Eine i.a. einfachere Methode zur Berechnung des größten gemeinsamen Teilers liefert der euklidische Algorithmus, der auf einer fortgesetzten Division mit Rest beruht.

Beispiel 1.5.6

Wir stellen die beiden natürliche Zahlen 1.029 und 91 durch Strecken entsprechender Länge dar und suchen mit der **Methode der Wechselwegnahme** ein möglichst großes gemeinsames Mass, mit den diese beiden Strecken gemeinsam ausgemessen werden können:

Dazu tragen wir die Strecke 91 so oft wie möglich auf der Strecke 1.029 ab, nämlich 11-mal. Es bleibt eine Reststrecke der Länge 28. Ein gemeinsames Maß der Strecken 1.029 und 91 muss auch die Differenzstrecke vollständig ausmessen können, also auch gemeinsames Maß der Strecken 91 und 28 sein.

Wieder tragen wir die Strecke 28 möglichst oft auf der Strecke 91 ab, nämlich 3-mal. Es ergibt sich eine Reststrecke der Länge 7, und unser gesuchtes gemeinsames Maß ist auch gemeinsames Maß der Strecken 28 und 7. Da aber 4-maliges Abtragen der Strecke 7 auf der Strecke 28 keinen Rest ergibt, haben wir das gemeinsame Maß 7 gefunden.

Als Algorithmus zur Bestimmung des größten gemeinsamen Teilers zweier natürlicher Zahlen a und b formuliert ergibt sich der

Euklidischer Algorithmus:

Schritt 1: Setze $l = 0$, $x_0 := a$ und $y_0 := b$.

Schritt 2: Teile x_l durch y_l mit Rest r_l. Ist $r_l = 0$, dann breche man ab.

Schritt 3: Sonst setze $l := l + 1$, $x_l := y_{l-1}$ und $y_l := r_{l-1}$ und fahre mit Schritt 2 fort.

Beispiel 1.5.7 $a = 64.589$, $b = 3.178$:

Durchlauf l	x_l	y_l	Division mit Rest $x_l = q_l \cdot y_l + r_l$	Rest r_l	$r_l > 0$?
0	64.589	3.178	$64.589 = 20 \cdot 3.178 + 1.029$	1.029	ja
1	3.178	1.029	$3.178 = 3 \cdot 1.029 + 91$	91	ja
2	1.029	91	$1.029 = 11 \cdot 91 + 28$	28	ja
3	91	28	$91 = 3 \cdot 28 + 7$	7	ja
4	28	7	$28 = 4 \cdot 7 + 0$	0	nein

Bemerkungen 1.5.8

(1) Ob man im 1. Schritt a durch b oder b durch a mit Rest dividiert, hat auf die Abschlußwerte von x und y keine Auswirkung:
Ist $a < b$ und teilt man a durch b, dann läuft der Algorithmus genau einen Schritt länger, als wenn man b durch a teilt.

(2) Bei jedem Schritt ist der Rest kleiner als der Divisor. Beim nächsten Schritt wird dieser Rest neuer Divisor, d.h. der neue Rest ist wieder kleiner. Die Reste bilden also eine streng monoton fallende Folge in $\mathbb{N}$, d.h. nach dem Wohlordnungsprinzip bricht der Algorithmus nach endlich vielen Schritten ab.

Der euklidische Algorithmus liefert das gewünschte Ergebnis:

Satz 1.5.9 *Führt man den euklidischen Algorithmus für $a, b \in \mathbb{N}$ durch, dann ist der Abschlußwert $y_l = r_{l-1}$ gleich dem größten gemeinsamen Teiler von a und b.*

Bemerkung 1.5.10

Der größte gemeinsame Teiler $\mathrm{ggT}(n_1, ..., n_k)$ läßt sich als ganzzahlige Linearkombination von $n_1, ..., n_k$ darstellen, d.h. es gibt Koeffizienten $x_i \in \mathbb{Z}$, $1 \leq i \leq k$, mit

$$\mathrm{ggT}(n_1, \ldots, n_k) = \sum_{i=1}^{k} x_i n_i.$$

Die Koeffizienten lassen sich mit Hilfe des euklidischen Algorithmus bestimmen.

Beispiel 1.5.11

Für $a = 64.589$, $b = 3.178$ ergibt sich

$$7 = -105 \cdot 64.589 + 2.134 \cdot 3.178,$$

also $x_1 = -105$, $x_2 = 2.134$.

Bei der Addition von Brüchen

$$\frac{a_1}{b_1} + \frac{a_2}{b_2} + \ldots + \frac{a_k}{b_k}$$

muss man die Brüche gleichnamig machen, d.h. auf einen gemeinsamen Nenner bringen. Da jeder der Brüche durch Erweitern auf diesen gemeinsamen Nenner gebracht werden muss, braucht man dazu also ein gemeinsames Vielfaches aller ursprünglicher Nenner.

$b_1 \cdot b_2 \cdot \ldots \cdot b_k$ ist sicher ein solches gemeinsames Vielfaches, aber im allgemeinen sehr groß und die sich neu ergebenden Zähler werden entsprechend groß. Da wir im allgemeinen mit kleinen Zahlen leichter rechnen, ist es sinnvoll, das kleinste gemeinsame Vielfache der Nenner, d.h. den **Hauptnenner**, zu bestimmen.

Definition 1.5.12 *Seien $n_1, ..., n_k \in \mathbb{Z}$ mit $n_i \neq 0$, $1 \leq i \leq k$. Dann heißt*

$$m := min\{v \in \mathbb{N};\ n_i \mid v \text{ für alle } 1 \leq i \leq k\}$$

kleinstes gemeinsames Vielfaches *von $n_1, ..., n_k$.*

Schreibweise: $m = \mathrm{kgV}(n_1, ..., n_k)$.

Sind die kanonischen Primfaktorzerlegungen der Zahlen $n_1, \ldots, n_k$ bekannt, dann gilt analog zur Bestimmung des größten gemeinsamen Teilers in Satz 1.5.4

Satz 1.5.13 *Für $n_1, n_2, ..., n_k \in \mathbb{N}$ mit den kanonischen Primfaktorzerlegungen*

$$n_j = {p_1}^{m_{j1}} \cdot {p_2}^{m_{j2}} \cdot \ldots, \qquad m_{ji} \in \mathbb{N} \cup \{0\}, \quad i \in \mathbb{N}, \quad 1 \leq j \leq k,$$

gilt

$$\mathrm{kgV}(n_1, ..., n_k) = {p_1}^{\max(m_{11}, m_{21}, ..., m_{k1})} \cdot {p_2}^{\max(m_{12}, m_{22}, ..., m_{k2})} \cdot \ldots.$$

Betrachtet nur zwei Zahlen, dann gilt für den größten gemeinsamen Teiler und das kleinste gemeinsame Vielfache

Satz 1.5.14 *Für $a, b \in \mathbb{Z}$, $a, b \neq 0$, gilt*

$$\mathrm{ggT}(a, b) \cdot \mathrm{kgV}(a, b) = a \cdot b.$$

Bemerkung 1.5.15

Für kgV und ggT von mehr als 2 Zahlen ist diese Aussage im allgemeinen falsch.

Beispiele 1.5.16 $1960 = 2^3 \cdot 5 \cdot 7^2$, $686 = 2 \cdot 7^3$, $16900 = 2^2 \cdot 5^2 \cdot 13^2$.

(1) $\mathrm{ggT}(1.960, 686) = 2 \cdot 7^2 = 98$, $\mathrm{kgV}(1.960, 686) = 2^3 \cdot 5 \cdot 7^3 = 13.720$ und

$$98 \cdot 13720 = 1344560 = 1960 \cdot 686.$$

(2) $\mathrm{ggT}(1.960, 686, 16.900) = 2^1 \cdot 5^0 \cdot 7^0 \cdot 13^0 = 2$,
$\mathrm{kgV}(1.960, 686, 16.900) = 2^3 \cdot 5^2 \cdot 7^3 \cdot 13^2 = 11593400$ und

$$2 \cdot 11593400 = 23186800 \neq 22723064000 = 1960 \cdot 686 \cdot 16900.$$