Elementare Zahlentheorie

Daniel Smertnig

SS 2022

Version vom 14. Juni 2022

Inhaltsverzeichnis

Vorbemerkungen und Notation

Wir bezeichnen mit $\mathbb{N} = \{1, 2, 3, \ldots\}$ die natürlichen Zahlen, und setzen $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$. Mit $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ bezeichnen wir die ganzen, rationalen, reellen Zahlen. Es gilt $\mathbb{N} \subsetneq \mathbb{N}_0 \subsetneq \mathbb{Z} \subsetneq \mathbb{Q} \subsetneq \mathbb{R}$. Für $a, b \in \mathbb{Z}$ bezeichnet $[a, b] = \{ x \in \mathbb{Z} \mid a \leq x \leq b \}$ das diskrete Intervall von a bis b. Ist $a \in \mathbb{N}_0$, so sei $\mathbb{N}_{\geq a} = \{ b \in \mathbb{N} \mid b \geq a \}$. Analoge Schreibweise verwenden wir mitunter für $\mathbb{Z}$ und $\mathbb{R}$.

Partielle Ordnungen

Sei $\emptyset \neq M$ eine Menge. Eine Relation $\preceq$ auf M heißt *partielle Ordnung* (auf M), wenn für alle $a, b, c \in M$ gilt:

- (Reflexivität) $a \preceq a$.
- (Transitivität) Aus $a \preceq b$ und $b \preceq c$ folgt $a \preceq c$.
- (Antisymmetrie) Aus $a \preceq b$ und $b \preceq a$ folgt $a = b$.

Man nennt dann $(M, \preceq)$ eine *partiell geordnete Menge*. Die Relation $\preceq$ ist eine *Totalordnung* wenn weiters $a \preceq b$ oder $b \preceq a$ für alle $a, b \in M$ gilt.

Die Mengen $\mathbb{Z}$ (sowie auch $\mathbb{Q}$ und $\mathbb{R}$) sind in üblicher Weise total geordnet. Für $x \in \mathbb{R}$ ist der *Absolutbetrag* gegeben durch

$$|x| = \begin{cases} x & \text{falls } x \geq 0, \\ -x & \text{falls } x < 0. \end{cases}$$

Für jedes $x \in \mathbb{R}$ gibt es dann ein $e \in \{\pm 1\}$ mit $x = e|x|$. Wegen $e^2 = 1$ gilt dann auch $|x| = ex$. Für $x, y \in \mathbb{R}$ gilt $|x| = |y|$ genau dann wenn $x = \pm y$.

Induktionsprinzip

Für die natürlichen Zahlen gilt das Induktionsprinzip, das dem Beweis durch vollständige Induktion zugrunde liegt. Dieses lässt sich auf mehrere äquivalente Weisen formulieren, von denen wir uns einige in Erinnerung rufen.

- (Wohlordnungsprinzip) Jede nicht-leere Teilmenge $A \subset \mathbb{N}_0$ enthält ein kleinstes Element.
- Jede nach unten [oben] beschränkte nicht-leere Teilmenge $A \subset \mathbb{Z}$ enthält ein kleinstes [größtes] Element.
- (Induktionsprinzip) Ist $A \subset \mathbb{N}_0$, so dass gilt:
  - (Induktionsanfang) Es gibt ein $a_0 \in A$, und
  - (Induktionsschritt) für jedes $a \in A$ ist $a + 1 \in A$,

  dann ist $\{a \in \mathbb{N}_0 \mid a \geq a_0\} \subset A$.
- (Induktionsprinzip, 2. Form) Sei $A \subset \mathbb{N}_0$, so dass für alle $a \in A$ gilt: Aus $\{ x \in \mathbb{N}_0 \mid x < a \} \subset A$ folgt $a \in A$. Dann ist $A = \mathbb{N}_0$.

1 Teilbarkeit in den ganzen Zahlen

1.1 Division mit Rest

Die Division mit Rest ist uns aus der Schule als ein Rechenverfahren bekannt, zum Beispiel

$$\begin{array}{r} 1137 : 12 = 94 \\ 57 \\ 9 \text{ R.} \end{array}$$

Ausgehend von $a = 1137$ und $b = 12$ haben wir $q = 94$ und $r = 9$ berechnet. Was zeichnet diese beiden Zahlen eigentlich aus?

Satz 1.1 (Division mit Rest). *Seien $a \in \mathbb{Z}$ und $b \in \mathbb{N}$. Dann existieren eindeutig bestimmte $q \in \mathbb{Z}$ und $r \in \mathbb{N}_0$ mit $0 \leq r < b$, so dass gilt $a = bq + r$. Ist $a \geq 0$ so ist auch $q \geq 0$.*

Beweis. *Existenz:* Wir betrachten die Menge

$$S = \{\, a - bq \mid q \in \mathbb{Z} \,\}.$$

Wegen $b \geq 1$ ist $a - b(-|a|) = a + b|a| \geq 0$ und deshalb $S \cap \mathbb{N}_0$ nicht leer. Nach dem Wohlordnungsprinzip besitzt $S \cap \mathbb{N}_0$ ein kleinstes Element $r = \min(S \cap \mathbb{N}_0)$. Sei weiters $q \in \mathbb{Z}$ so gewählt, dass gilt $r = a - bq$. Wir müssen noch $r < b$ zeigen. Angenommen es wäre $r \geq b$. Dann ist

$$0 \leq r - b = a - b(q + 1),$$

also $r - b \in S \cap \mathbb{N}_0$, im Widerspruch zur Minimalität von r.

Eindeutigkeit: Angenommen, es ist $a = bq + r = bq' + r'$ mit $q, q' \in \mathbb{Z}$ und $r, r' \in [0, b-1]$. Es folgt

$$b(q - q') = r' - r,$$

und weiter

$$b|q - q'| = |r' - r|. \tag{1.1}$$

Wegen $0 \leq r < b$ und $0 \leq r' < b$ gilt $|r' - r| < b$. Weil $q - q'$ eine ganze Zahl ist, kann Gleichung (1.1) also nur gelten wenn $|q - q'| = 0$, also $q = q'$, ist. Daraus folgt dann, wieder mit Gleichung (1.1), auch $r = r'$.

$a \geq 0$ *impliziert* $q \geq 0$*:* Ist $q < 0$, so ist wegen $q \in \mathbb{Z}$ bereits $q \leq -1$. Es folgt $bq \leq -b < -r$ und damit $a = bq + r < 0$. □

Definition 1.2. Sind $a \in \mathbb{Z}$, $b \in \mathbb{N}$ und ist $a = bq + r$ mit $q \in \mathbb{Z}$, $r \in \mathbb{N}_0$ und $0 \leq r < b$, so heißt q der *Quotient* und r der *Rest* der Division von a durch b.

Beispiel. (1) Jedes $a \in \mathbb{Z}$ lässt sich darstellen in der Form $a = 4k$, $a = 4k+1$, $a = 4k+2$ oder $a = 4k + 3$ mit $k \in \mathbb{Z}$. Ist a eine Quadratzahl, so gilt $a = 4k$ oder $a = 4k + 1$ mit $k \in \mathbb{Z}$.

Beweis: Sei $a = b^2$ mit $b \in \mathbb{Z}$. Dann gibt es $l \in \mathbb{Z}$ und $s \in \{0, 1\}$ mit $b = 2l + s$. Also gilt $a = b^2 = 4(l^2 + ls) + s^2$. Es ist $s^2 = 0$ falls $s = 0$, und $s^2 = 1$ falls $s = 1$.

(2) Keine Zahl der Form 11, 111, 1111, 11111, ... ist eine Quadratzahl. Denn es ist

$$\underbrace{111\ldots11}_{n \text{ mal}} = \underbrace{111\ldots1111}_{n-2 \text{ mal}} \cdot 100 + 11 = \underbrace{111\ldots1111}_{n-2 \text{ mal}} \cdot 25 \cdot 4 + 2 \cdot 4 + 3.$$

Damit ergibt die Zahl bei Division durch 4 den Rest 3, und kann somit keine Quadratzahl sein.

1.2 Teilbarkeit

Definition 1.3. Eine ganze Zahl b heißt *teilbar* durch die ganze Zahl a, geschrieben

$$a \mid b,$$

wenn es ein $k \in \mathbb{Z}$ gibt mit $b = ak$.

Man sagt dann auch „a teilt b“, „b ist ein Vielfaches von a“ oder „a ist ein Teiler von b“, manchmal auch „a geht in b auf“. Die Schreibweise $a \nmid b$ drückt aus, dass b nicht durch a teilbar ist.

Beispiel. Es ist $3 \mid -18$, denn $3 \cdot (-6) = -18$, aber $4 \nmid 9$, denn es gibt kein $k \in \mathbb{Z}$ mit $4k = 9$.

Wir halten einige elementare Eigenschaften der Teilbarkeitsrelation fest. Im Weiteren werden wir diese oft verwenden ohne ausdrücklich Bezug darauf zu nehmen.

Lemma 1.4. *Seien $a, b, c, d \in \mathbb{Z}$.*

(1) $a \mid 0, \quad 1 \mid a, \quad a \mid a.$

(2) $a \mid b \iff |a| \mid |b| \iff \pm a \mid \pm b.$

(3) $a \mid b$ *und* $b \mid c \implies a \mid c.$

(4) $a \mid b$ *und* $c \mid d \implies ac \mid bd$.

(5) *Seien* $n \in \mathbb{N}$, $a_1, \ldots, a_n, x_1, \ldots, x_n \in \mathbb{Z}$. *Ist* $a \mid a_i$ *für alle* $i \in [1, n]$, *so gilt auch* $a \mid a_1x_1 + \cdots + a_nx_n$.

(6) *Ist* $c \neq 0$, *so gilt* $a \mid b \iff ac \mid bc$.

(7) $a \mid b$ *und* $b \neq 0 \implies |a| \leq |b|$.

(8) $a \mid b$ *und* $b \mid a \iff |a| = |b| \iff a = \pm b$.
Insbesondere: $a \mid 1 \iff a = \pm 1$ *und* $0 \mid a \iff a = 0$.

(9) $(\mathbb{N}_0, |)$ *und* $(\mathbb{N}, |)$ *sind partiell geordnete Mengen.*

Beweis. (1) Wegen $0 = a0$ und $a = a1$.

(2) Seien $|a| = ea$ und $|b| = fb$ mit $e, f \in \{\pm 1\}$. Wegen $e^2 = 1$ ist auch $a = e|a|$.

Wir zeigen zuerst die erste Äquivalenz.

„$\Rightarrow$“ Sei $k \in \mathbb{Z}$ mit $b = ak$. Dann ist $b = e|a|k$ und darum $|b| = fb = fe|a|k$. Wegen $fek \in \mathbb{Z}$ folgt $|a| \mid |b|$.

„$\Leftarrow$“ Sei $k \in \mathbb{Z}$ mit $|b| = k|a|$. Dann ist $fb = kea$ und wegen $f^2 = 1$ auch $b = fkea$. Wegen $fke \in \mathbb{Z}$ folgt $a \mid b$.

Die zweite Äquivalenz folgt wegen $|\pm a| = |a|$ und $|\pm b| = |b|$.

(3) Seien $k, l \in \mathbb{Z}$ mit $b = ak$ und $c = bl$. Dann ist $c = bl = (ak)l = a(kl)$.

(4) Seien $k, l \in \mathbb{Z}$ mit $b = ak$ und $d = cl$. Dann ist $bd = (ak)(cl) = ac(kl)$.

(5) Seien $b = ak$ und $c = al$ mit $k, l \in \mathbb{Z}$. Dann ist $bx+cy = (ak)x+(al)y = a(kx+ly)$ und deshalb $a \mid bx + cy$.

(6) Ist $a \mid b$, so folgt $ac \mid bc$ aus (4). Ist umgekehrt $ac \mid bc$ so gibt es $k \in \mathbb{Z}$ mit $bc = ack$. Wegen $c \neq 0$ ist c kürzbar und deshalb $b = ak$, also $a \mid b$.

(7) Wegen (2) ist $|a| \mid |b|$. Sei $k \in \mathbb{Z}$ mit $|b| = |a|k$. Wegen $|b| > 0$ muss gelten $k > 0$, und deshalb bereits $k \geq 1$ (wegen $k \in \mathbb{Z}$). Dann ist aber $|b| = |a|k \geq |a|1 = |a|$.

(8) Wir wissen $|a| = |b| \iff a = \pm b$, es genügt also die erste Äquivalenz zu zeigen. Dazu bemerken zuerst: $0 \mid b \implies b = 0$, denn $0 \mid b$ bedeutet, dass es ein $k \in \mathbb{Z}$ gibt mit $b = 0k = 0$. Ist also $a = 0$, so ist auch $b = 0$ und umgekehrt. In diesem Fall gilt die Äquivalenz trivialerweise.

Wir können nun $a \neq 0$ und $b \neq 0$ annehmen.

„$\Rightarrow$“ Sei zuerst $a \mid b$ und $b \mid a$. Aus (7) folgt $|a| \leq |b| \leq |a|$. Deshalb ist $|a| = |b|$.

„$\Leftarrow$“ Ist $|a| = |b|$, so gibt es ein $e \in \{\pm 1\}$ mit $a = eb$. Wegen $e^2 = 1$ gilt dann auch $b = ae$. Somit ist $a \mid b$ und $b \mid a$.

(9) Die Relation $|$, eingeschränkt auf $\mathbb{N}_0$, oder $\mathbb{N}$, ist reflexiv, transitiv und antisymmetrisch, nach (1), (3) und (8). □

Bemerkung. (1) Die Teilbarkeitsrelation auf $\mathbb{Z}$ ist transitiv und reflexiv, jedoch nicht antisymmetrisch, da $a \mid b$ und $b \mid a$ bloß $a = \pm b$ impliziert.

(2) Auf $\mathbb{N}_0$ ist $\mid$ keine Totalordnung, denn $2 \nmid 3$ und $3 \nmid 2$.

Definition 1.5. Für $a \in \mathbb{Z}$ bezeichne

$$T(a) \coloneqq \{\, b \in \mathbb{N}_0 \mid b \mid a \,\}$$

die Menge aller nicht-negativen Teiler von a.

Es gilt $T(0) = \mathbb{N}_0$. Für $a \neq 0$ gilt $\{1, a\} \subseteq T(a) \subseteq [1, |a|]$ nach Lemma 1.4. In diesem Fall ist also $T(a)$ die Menge der *positiven* Teiler von a. Insbesondere ist $T(a)$ für $a \neq 0$ eine nichtleere endliche Menge. Sind $a_1, \ldots, a_n \in \mathbb{Z}$ mit $n \geq 1$, so ist $T(a_1) \cap \cdots \cap T(a_n)$ die Menge der *gemeinsamen Teiler* von $a_1, \ldots, a_n$.

1.3 Größter gemeinsamer Teiler und kleinstes gemeinsames Vielfaches

Definition 1.6. Seien $n \in \mathbb{N}$ und $a_1, \ldots, a_n \in \mathbb{Z}$.

(1) Eine nicht-negative Zahl $d \in \mathbb{N}_0$ heißt *größter gemeinsamer Teiler* (*ggT*) von $a_1, \ldots, a_n$, wenn gilt

   (i) $d \mid a_i$ für alle $i \in [1, n]$.

   (ii) Ist $d' \in \mathbb{N}_0$ mit $d' \mid a_i$ für alle $i \in [1, n]$, so folgt $d' \mid d$.

   Wir schreiben dann $d = \mathrm{ggT}(a_1, \ldots, a_n)$.

(2) Eine nicht-negative Zahl $e \in \mathbb{N}_0$ heißt *kleinstes gemeinsames Vielfaches* (*kgV*) von $a_1, \ldots, a_n$, wenn gilt

   (i) $a_i \mid e$ für alle $i \in [1, n]$.

   (ii) Ist $e' \in \mathbb{N}_0$ mit $a_i \mid e'$ für alle $i \in [1, n]$, so folgt $e \mid e'$.

   Wir schreiben dann $e = \mathrm{kgV}(a_1, \ldots, a_n)$.

(3) $a_1, \ldots, a_n$ heißen *teilerfremd* wenn gilt $\mathrm{ggT}(a_1, \ldots, a_n) = 1$. Die Zahlen $a_1, \ldots, a_n$ heißen *paarweise teilerfremd* wenn gilt $\mathrm{ggT}(a_i, a_j) = 1$ falls $i \neq j$.

Die Eindeutigkeit, insbesondere aber die Existenz, eines größten gemeinsamer Teilers, beziehungsweise kleinsten gemeinsamen Vielfachen, sind nicht offensichtlich; wir kommen in der nachfolgenden Bemerkung auf die Eindeutigkeit und in Korollar 1.8 auf die Existenz zurück.

Beispiel. (1) Es ist $T(\pm 2) = \{1, 2\}$, $T(\pm 6) = \{1, 2, 3, 6\}$, $T(\pm 15) = \{1, 3, 5, 15\}$. Die (nicht-negativen) gemeinsamen Teiler von 2 und 6 sind $T(2) \cap T(6) = \{1, 2\}$; deshalb ist $\mathrm{ggT}(2, 6) = 2$. Wegen $T(6) \cap T(15) = \{1, 3\}$ folgt $\mathrm{ggT}(6, 15) = 3$, und wegen $T(2) \cap T(15) = \{1\}$ ist $\mathrm{ggT}(2, 15) = 1$.

(2) Es ist $T(10) = \{1, 2, 5, 10\}$. Damit ist $T(10) \cap T(15) = \{1, 5\}$ und $T(6) \cap T(10) = \{1, 2\}$. Es folgt $\mathrm{ggT}(6, 10) = 2$, $\mathrm{ggT}(10, 15) = 5$, $\mathrm{ggT}(6, 15) = 3$, aber $\mathrm{ggT}(6, 10, 15) = 1$. Das heißt 6, 10, 15 sind teilerfremd aber nicht paarweise teilerfremd.

Bemerkung. (1) Der größte gemeinsame Teiler, ist — so er existiert — eindeutig: Angenommen $d, d' \in \mathbb{N}_0$ sind größte gemeinsame Teiler von $a_1, \ldots, a_n$. Dann ist $d \mid d'$ und $d' \mid d$. Aus Lemma 1.4(8) folgt $d = |d| = |d'| = d'$.

Analog zeigt man, dass das kleinste gemeinsame Vielfache eindeutig bestimmt ist. Damit sind die Schreibweisen $\mathrm{ggT}(a_1, \ldots, a_n)$ und $\mathrm{kgV}(a_1, \ldots, a_n)$ sinnvoll.

(2) Nach Lemma 1.4(8) ist $0 = \mathrm{ggT}(a_1, \ldots, a_n)$ genau dann, wenn $a_1 = \ldots = a_n = 0$.

[Beweis: „⇐“ Für alle $j \in [1, n]$ ist $0 \mid a_j$; für $x \in \mathbb{Z}$ ist $x \mid 0$. Deshalb ist $0 = \mathrm{ggT}(a_1, \ldots, a_n)$. „⇒“ Für alle $j \in [1, n]$ ist $0 \mid a_j$ und deshalb $a_j = 0$.]]

Genauso ist $0 = \mathrm{kgV}(a_1, \ldots, a_n)$ genau dann, wenn es ein $i \in [1, n]$ gibt mit $a_i = 0$. [Beweis: „⇐“ Trivialerweise gilt $a_j \mid 0$ für alle $j \in [1, n]$. Ist $e' \in \mathbb{N}_0$ mit $a_j \mid e'$ für alle $j \in [1, n]$, so folgt wegen $a_i = 0$ notwendigerweise $e' = 0$, also $0 \mid e'$. Deshalb ist $0 = \mathrm{kgV}(a_1, \ldots, a_n)$. „⇒“ Es gilt $a_j \mid a_1 \cdots a_n$ für alle $j \in [1, n]$ und deshalb $0 = \mathrm{kgV}(a_1, \ldots, a_n) \mid a_1 \cdots a_n$. Dann muss aber gelten $a_1 \cdots a_n = 0$ und deshalb gibt es ein $i \in [1, n]$ mit $a_i = 0$.]

Diese trivialen Spezialfälle sollen uns im Weiteren nicht wirklich interessieren.

(3) Der größte gemeinsame Teiler, beziehungsweise das kleinste gemeinsame Vielfache, hängen offensichtlich nur von der Menge $A = \{a_1, \ldots, a_n\}$, nicht aber von der Vielfachheit oder Reihenfolge der vorkommenden Elemente, ab.

(4) $\mathrm{ggT}(a_1, \ldots, a_n) = \mathrm{ggT}(|a_1|, \ldots, |a_n|)$ und $\mathrm{kgV}(a_1, \ldots, a_n) = \mathrm{kgV}(|a_1|, \ldots, |a_n|)$.

(5) Mit Hilfe der zuvor eingeführten Notation lässt sich die Definition des ggTs auch wie folgt abkürzen: $d \in \mathbb{N}_0$ ist größter gemeinsamer Teiler von $a_1, \ldots, a_n$, wenn gilt $d \in T(a_1) \cap \cdots \cap T(a_n)$ und ist $d' \in T(a_1) \cap \cdots \cap T(a_n)$, so folgt $d' \mid d$. Das heißt, $\mathrm{ggT}(a_1, \ldots, a_n) = \max_{|}(T(a_1) \cap \cdots \cap T(a_n))$ (das Maximum bezüglich der Partialordnung $|$).

Definiert man $V(a_i) = \{\, k|a_i| : k \in \mathbb{N}_0 \,\}$ so ist analog $\mathrm{kgV}(a_1, \ldots, a_n) = \min_{|}(V(a_1) \cap \cdots \cap V(a_n))$.

Satz 1.7 (Charakterisierungen des ggTs). *Seien $n \in \mathbb{N}$, $a_1, \ldots, a_n \in \mathbb{Z}$ und $d \in \mathbb{N}$. Dann sind äquivalent:*

(a) $d \in T(a_1) \cap \cdots \cap T(a_n)$ *und es existieren $x_1, \ldots, x_n \in \mathbb{Z}$ mit $d = a_1x_1 + \cdots + a_nx_n$.*

(b) $d = \mathrm{ggT}(a_1, \ldots, a_n)$.

Ist zumindest eines der $a_1, \ldots, a_n$ von Null verschieden, so ist weiters äquivalent:

(c) $d \in T(a_1) \cap \cdots \cap T(a_n)$ *und für jede weitere Zahl* $d' \in T(a_1) \cap \cdots \cap T(a_n)$ *gilt* $d' \leq d$. *Das heißt,*

$$d = \max_{\leq}(T(a_1) \cap \cdots \cap T(a_n)).$$

Beweis. Ist $a_1 = \cdots = a_n = 0$, so gelten (a) und (b) genau dann wenn $d = 0$. Wir nehmen nun an, dass zumindest eines der $a_1, \ldots, a_n$ von Null verschieden ist.

(a) $\Rightarrow$ (b): Ist $d' \mid a_i$ für alle $i \in [1, n]$, so folgt aus Lemma 1.4(5) auch $d' \mid a_1x_1 + \cdots + a_nx_n = d$.

(b) $\Rightarrow$ (c): Aufgrund der Definition des größten gemeinsamen Teilers ist $d' \mid d$ und deshalb $d' \leq d$ nach Lemma 1.4(7).

(c) $\Rightarrow$ (a): Sei

$$M = \{\, a_1x_1 + \cdots + a_nx_n \mid x_1, \ldots, x_n \in \mathbb{Z} \,\}.$$

Mit Wahl von $x_i = a_i$ folgt $0 < a_1^2 + \cdots + a_n^2 \in M$, also ist $M \cap \mathbb{N}$ nicht leer. Deshalb besitzt $M \cap \mathbb{N}$ ein kleinstes Element, d'. Wegen $d \mid a_i$ für alle $i \in [1, n]$ folgt aus Lemma 1.4(5) auch $d \mid d'$ und somit $d \leq d'$. Wir zeigen nun $d' \leq d$, woraus dann $d = d'$ folgt.

Seien $x_1, \ldots, x_n \in \mathbb{Z}$ mit $d' = \sum_{i=1}^{n} a_ix_i$. Durch Division mit Rest lässt sich jedes a_i schreiben als $a_i = q_id' + r_i$ mit $0 \leq r_i < d'$ und $q_i \in \mathbb{Z}$. Damit gilt, für jedes $i \in [1, n]$,

$$r_i = a_i - q_id' = a_i - q_i\Big(\sum_{j=1}^{n} a_jx_j\Big) = a_i(1 - q_ix_i) + \sum_{\substack{j=1 \\ i \neq j}}^{n} a_j(-q_ix_j).$$

Das heißt $r_i \in M$. Wegen $0 \leq r_i < d'$ und der Minimalität von d' in $M \cap \mathbb{N}$ folgt $r_i = 0$. Dann ist aber $a_i = q_id'$, also $d' \mid a_i$ für alle $i \in [1, n]$. Damit ist $d' \leq d$ nach Voraussetzung. □

Beispiel. Es ist $T(14) = \{1, 2, 7, 14\}$ und $T(9) = \{1, 3, 9\}$. Deshalb ist $1 = \mathrm{ggT}(9, 14)$ und es gilt $1 = 2 \cdot 14 - 3 \cdot 9$. Das ist aber nicht die einzige Lösung, denn es gilt auch $1 = (2 + 9k) \cdot 14 - (3 + 14k) \cdot 9$ für alle $k \in \mathbb{Z}$.

Die Eigenschaft (a) des größten gemeinsamen Teilers ist von zentraler Bedeutung. Der vorhergehende Beweis zeigt zwar die Existenz geeigneter Koeffizienten x_i, er liefert uns aber kein Verfahren um solche zu bestimmen. Diesen Umstand werden wir später mit Hilfe des euklidischen Algorithmus beheben.

Korollar 1.8. *Seien* $n \in \mathbb{N}$ *und* $a_1, \ldots, a_n \in \mathbb{Z}$. *Dann besitzen* $a_1, \ldots, a_n$ *einen größten gemeinsamen Teiler.*

Beweis. Ist $a_1 = \cdots = a_n = 0$, so ist $0 = \mathrm{ggT}(a_1, \ldots, a_n)$. Wir setzen von nun an voraus, dass es ein $i \in [1, n]$ gibt mit $a_i \neq 0$. Sei

$$M = \Big\{\, d' \in \mathbb{N} \;\Big|\; d' \mid a_j \text{ für alle } j \in [1, n] \,\Big\}.$$

Ist $d' \in M$ so folgt aus $d' \mid a_i$ auch $d' \leq a_i$ (nach Lemma 1.4(7)). Deshalb ist $M \subset [1, a_i]$ endlich. Wegen $1 \in M$ ist M auch nicht-leer und besitzt deshalb ein größtes Element d. Aufgrund von Satz 1.7 ist $d = \mathrm{ggT}(a_1, \ldots, a_n)$. □

Satz 1.9 (Charakterisierungen des kgVs). *Seien $n \in \mathbb{N}$, $a_1, \ldots, a_n \in \mathbb{Z} \setminus \{0\}$, und $e \in \mathbb{N}$. Dann sind äquivalent:*

(a) $e = \mathrm{kgV}(a_1, \ldots, a_n)$.

(b) $a_i \mid e$ *für alle* $i \in [1, n]$ *und für jede weitere Zahl* $e' \in \mathbb{N}$ *mit der Eigenschaft* $a_i \mid e'$ *für alle* $i \in [1, n]$ *gilt* $e \leq e'$. *Das heißt,*

$$e = \min{}_{\leq} \left\{ e' \in \mathbb{N} \;\middle|\; a_i \mid e' \text{ für alle } i \in [1, n] \right\}.$$

Beweis. (a) $\Rightarrow$ (b): Es ist $e \mid e'$ nach Definition des kleinsten gemeinsamen Vielfachen. Aus Lemma 1.4(7) folgt $e \leq e'$.

(b) $\Rightarrow$ (a): Sei $e' \in \mathbb{N}$ mit $a_i \mid e'$ für alle $i \in [1, n]$ und $d = \mathrm{ggT}(e, e')$. Dann ist $d \leq e$. Wegen $a_i \mid e$ und $a_i \mid e'$ folgt $a_i \mid d$ für alle $i \in [1, n]$ nach Definition des größten gemeinsamen Teilers. Aufgrund der Minimalität von e folgt $e \leq d$, also $e = d$. Dann ist aber $e \mid e'$, also $e = \mathrm{kgV}(a_1, \ldots, a_n)$. □

Korollar 1.10. *Seien $n \in \mathbb{N}$ und $a_1, \ldots, a_n \in \mathbb{Z}$. Dann besitzen $a_1, \ldots, a_n$ ein kleinstes gemeinsames Vielfaches.*

Beweis. Gibt es ein $i \in [1, n]$ mit $a_i = 0$ so ist $0 = \mathrm{kgV}(a_1, \ldots, a_n)$. Sei nun $a_i \neq 0$ für alle $i \in [1, n]$ und sei

$$M = \left\{ e' \in \mathbb{N} \;\middle|\; a_i \mid e' \text{ für alle } i \in [1, n] \right\}.$$

Wegen $|a_1 \cdots a_n| \in M$ ist M nicht leer und besitzt deshalb ein minimales Element e. Nach Satz 1.9 ist $e = \mathrm{kgV}(a_1, \ldots, a_n)$. □

Bemerkung zur Algebra. In den ganzen Zahlen werden oft auch die Eigenschaften aus Satz 1.7(c) beziehungsweise Satz 1.9(b) zur Definition des größten gemeinsamen Teilers beziehungsweise kleinsten gemeinsamen Vielfachen herangezogen.

Da in diese beiden Charakterisierungen aber die Totalordnung von $\mathbb{Z}$ einfließt, lassen Sie sich nicht unmittelbar auf allgemeinere Ringe erweitern. Unsere Definition hat den Vorteil, dass Sie sich leicht auf *Integritätsbereiche*, zum Beispiel Polynomringe über Körpern, wie $\mathbb{Q}[X]$ oder $\mathbb{R}[X]$, ausdehnen lässt. Man muss nur auf die Forderung verzichten, dass größter gemeinsamer Teiler und kleinstes gemeinsames Vielfaches stets positiv sind; sie sind dann — sofern sie existieren — eindeutig bestimmt bis auf Assoziierte. In Polynomringen über Körpern bedeutet dies, dass größter gemeinsamen Teiler und kleinstes gemeinsames Vielfaches bis auf die Multiplikation mit einer von Null verschiedenen Konstante eindeutig bestimmt sind.

Satz 1.11. *Seien $n \in \mathbb{N}$, $a, b, c, d, a_1, \ldots, a_n \in \mathbb{Z}$.*

(1) *Es gilt* $\operatorname{ggT}(da_1, \ldots, da_n) = |d| \operatorname{ggT}(a_1, \ldots, a_n)$.
Insbesondere: Ist $d \mid a_i$ für alle $i \in [1, n]$ und $d \neq 0$, so ist

$$\operatorname{ggT}(a_1, \ldots, a_n) = |d| \iff \operatorname{ggT}\left(\frac{a_1}{d}, \ldots, \frac{a_n}{d}\right) = 1.$$

(2) *Ist $d = \operatorname{ggT}(a, b)$, so gilt $a \mid bc \iff a \mid dc$.*
Insbesondere: Sind a, b teilerfremd so gilt $a \mid bc \iff a \mid c$.

(3) *Sind a und b teilerfremd, so folgt aus $a \mid c$ und $b \mid c$ auch $ab \mid c$.*

(4) *Ist $\operatorname{ggT}(a_i, b) = 1$ für alle $i \in [1, n]$, so ist auch $\operatorname{ggT}(a_1 \cdots a_n, b) = 1$.*
Insbesondere: Aus $\operatorname{ggT}(a, b) = 1$ folgt auch $\operatorname{ggT}(a^m, b^n) = 1$ für alle $m, n \in \mathbb{N}$.

Beweis. (1) Sei $c = \operatorname{ggT}(a_1, \ldots, a_n)$. Dann ist $|d|c \mid da_i$ für alle $i \in [1, n]$. Nach Satz 1.7 gibt es $x_1, \ldots, x_n \in \mathbb{Z}$ mit $c = a_1x_1 + \cdots + a_nx_n$. Sei $e \in \{-1, 1\}$ mit $|d| = ed$. Dann ist $|d|c = (da_1)(ex_1) + \cdots + (da_n)(ex_n)$. Wieder nach Satz 1.7 ist $|d|c = \operatorname{ggT}(da_1, \ldots, da_n)$.

(2) Die Richtung „$\Leftarrow$“ folgt wegen $d \mid b$. Wir zeigen „$\Rightarrow$“. Aufgrund von Satz 1.7 gibt es $x, y \in \mathbb{Z}$ mit $d = ax + by$. Dann ist $dc = axc + byc$ und wegen $a \mid axc$ und $a \mid byc$ folgt $a \mid dc$.

(3) Wegen $\operatorname{ggT}(a, b) = 1$ gibt es $x, y \in \mathbb{Z}$ mit $1 = ax + by$. Seien $k, l \in \mathbb{Z}$ mit $c = ak = bl$. Dann ist

$$c = c \cdot 1 = c(ax + by) = (ac)x + (bc)y = ab(lx) + ab(ky) = ab(lx + ky),$$

also $ab \mid c$.

(4) Seien $x_i, y_i \in \mathbb{Z}$ mit $a_ix_i + by_i = 1$. Dann ist

$$1 = \prod_{i=1}^{n} (a_ix_i + by_i) = \Big(\prod_{i=1}^{n} a_i\Big)\Big(\prod_{i=1}^{n} x_i\Big) + bM$$

mit $M \in \mathbb{Z}$. □

Satz 1.12. *Für $a, b \in \mathbb{Z}$ ist*

$$\operatorname{ggT}(a, b) \operatorname{kgV}(a, b) = |ab|.$$

Beweis. Ist $a = 0$ oder $b = 0$, so ist $\operatorname{kgV}(a, b) = 0$ und $ab = 0$. Wir nehmen im Weiteren $a \neq 0$ und $b \neq 0$ an. Wir können weiters ohne Einschränkung $a > 0$ und $b > 0$ annehmen, denn $|ab| = \big||a||b|\big|$, $\operatorname{ggT}(a, b) = \operatorname{ggT}(|a|, |b|)$ und $\operatorname{kgV}(a, b) = \operatorname{kgV}(|a|, |b|)$.

Dann ist $d = \operatorname{ggT}(a, b) \neq 0$ und $\frac{a}{d}, \frac{b}{d} \in \mathbb{Z}$. Damit gilt aber

$$a \,\Big|\, \frac{ab}{d} \quad \text{und} \quad b \,\Big|\, \frac{ab}{d}.$$

Wir behaupten $\frac{ab}{d} = \mathrm{kgV}(a,b)$. Dazu müssen wir noch zeigen: Ist $c \in \mathbb{Z}$ mit $a \mid c$ und $b \mid c$, so folgt $\frac{ab}{d} \mid c$. Sei also $c \in \mathbb{Z}$ mit $a \mid c$ und $b \mid c$. Wegen $a \mid c$ und $b \mid c$ folgt $d \mid c$. Deshalb ist $\frac{c}{d} \in \mathbb{Z}$,

$$\frac{a}{d} \,\Big|\, \frac{c}{d} \quad \text{und} \quad \frac{b}{d} \,\Big|\, \frac{c}{d}.$$

Aufgrund von Satz 1.11(1) sind $\frac{a}{d}$ und $\frac{b}{d}$ teilerfremd. Aus Satz 1.11(3) folgt deshalb

$$\frac{ab}{d^2} \,\Big|\, \frac{c}{d},$$

und schließlich $\frac{ab}{d} \mid c$. □

Lemma 1.13. *Seien $n \in \mathbb{N}$ mit $n \geq 2$ und $a_1, \ldots, a_n \in \mathbb{Z}$. Dann ist*

$$\mathrm{ggT}(a_1, \ldots, a_n) = \mathrm{ggT}(\mathrm{ggT}(a_1, \ldots, a_{n-1}), a_n)$$

und

$$\mathrm{kgV}(a_1, \ldots, a_n) = \mathrm{kgV}(\mathrm{kgV}(a_1, \ldots, a_{n-1}), a_n).$$

Beweis. Sei $d = \mathrm{ggT}(a_1, \ldots, a_n)$ und $d' = \mathrm{ggT}(a_1, \ldots, a_{n-1})$. Wir zeigen: $d \mid \mathrm{ggT}(d', a_n)$ und $\mathrm{ggT}(d', a_n) \mid d$. Wegen $d \mid a_i$ für alle $i \in [1,n]$ folgt $d \mid d'$. Damit ist aber auch $d \mid \mathrm{ggT}(d', a_n)$. Andererseits ist $\mathrm{ggT}(d', a_n) \mid a_n$ und $\mathrm{ggT}(d', a_n) \mid \mathrm{ggT}(a_1, \ldots, a_{n-1})$, also $\mathrm{ggT}(d', a_n) \mid a_i$ für alle $i \in [1,n]$. Damit ist $\mathrm{ggT}(d', a_n) \mid d$.

Sei $e = \mathrm{kgV}(a_1, \ldots, a_n)$ und $e' = \mathrm{kgV}(a_1, \ldots, a_{n-1})$. Wir zeigen: $\mathrm{kgV}(e', a_n) \mid e$ und $e \mid \mathrm{kgV}(e', a_n)$. Wegen $a_i \mid e$ für alle $i \in [1,n]$ folgt $e' \mid e$. Dann ist aber auch $\mathrm{kgV}(e', a_n) \mid e$. Andererseits ist $a_n \mid \mathrm{kgV}(e', a_n)$ und $\mathrm{kgV}(a_1, \ldots, a_{n-1}) \mid \mathrm{kgV}(e', a_n)$, also $a_i \mid \mathrm{kgV}(e', a_n)$ für alle $i \in [1,n]$. Damit ist $e \mid \mathrm{kgV}(e', a_n)$. □

Lemma 1.14. *Sei $n \in \mathbb{N}$. Sind $a_1, \ldots, a_n \in \mathbb{Z}$ paarweise teilerfremd, so ist*

$$\mathrm{kgV}(a_1, \ldots, a_n) = |a_1 \cdots a_n|.$$

Beweis. Durch Induktion nach n. Die Aussage ist trivial für $n = 1$. Sei nun $n \geq 2$. Nach Lemma 1.13 und Induktionsvoraussetzung ist

$$\mathrm{kgV}(a_1, \ldots, a_n) = \mathrm{kgV}(\mathrm{kgV}(a_1, \ldots, a_{n-1}), a_n) = \mathrm{kgV}(|a_1 \cdots a_{n-1}|, a_n).$$

Aus Satz 1.11(4) folgt $\mathrm{ggT}(a_1 \cdots a_{n-1}, a_n) = 1$ und deshalb nach Satz 1.12

$$\mathrm{kgV}(|a_1 \cdots a_{n-1}|, a_n) = |a_1 \cdots a_n|.$$ □

1.4 Der euklidische Algorithmus

Eine Möglichkeit den größten gemeinsamen Teiler von Zahlen $a_1, \ldots, a_n$ zu bestimmen besteht – nach Satz 1.7 – darin, alle positiven gemeinsamen Teiler der a_i zu bestimmen, und davon den größten zu wählen. Das funktioniert, weil es, außer im Trivialfall $a_1 = \cdots = a_n = 0$, nur endlich viele gemeinsame Teiler der a_i gibt, weil $d \mid a_i$ stets $d \leq a_i$ impliziert. In der Praxis erweist sich dieses Verfahren, insbesondere bei großen Zahlen, aber als nicht zweckmäßig, weil es zu ineffizient ist.

Der *euklidische Algorithmus* liefert ein effizientes Verfahren um den größten gemeinsamen Teiler zweier Zahlen zu bestimmen. In Kombination mit Lemma 1.13 und Satz 1.12 erlaubt er die Bestimmung des größten gemeinsamen Teilers, beziehungsweise kleinsten gemeinsamen Vielfachen, einer beliebigen (endlichen) Menge von Zahlen.

Wir halten vorweg fest, dass stets $\operatorname{ggT}(a,b) = \operatorname{ggT}(|a|,|b|) = \operatorname{ggT}(|b|,|a|)$ und $\operatorname{ggT}(a,0) = a$ gilt, so dass wir im Folgenden $a > b > 0$ annehmen dürfen.

Der euklidische Algorithmus basiert auf der iterativen Anwendung der folgenden Beobachtung.

Lemma 1.15. *Sind $a, b, q, r \in \mathbb{Z}$ mit $a = bq + r$, so ist $\operatorname{ggT}(a,b) = \operatorname{ggT}(b,r)$.*

Beweis. Sei $d = \operatorname{ggT}(a,b)$ und $d' = \operatorname{ggT}(b,r)$. Dann ist $d \mid a$ und $d \mid b$ und deshalb, nach Lemma 1.4(5), auch $d \mid a - bq = r$. Deshalb ist $d \mid d'$. Andererseits ist, wegen $d' \mid b$ und $d' \mid r$, ebenfalls nach Lemma 1.4(5), auch $d' \mid bq + r = a$ und deshalb $d' \mid d$. Es folgt $d = d'$. □

Wollen wir nun $\operatorname{ggT}(a,b)$ bestimmen, so benutzen wir die Division mit Rest

$$a = bq_1 + r_1 \quad \text{mit } 0 \leq r_1 < b,\ q_1 \in \mathbb{Z},$$

um das Problem auf die Bestimmung von $\operatorname{ggT}(b, r_1)$ zu reduzieren. Ist $r_1 = 0$, so ist $\operatorname{ggT}(b, r_1) = \operatorname{ggT}(b, 0) = b$. Andernfalls wiederholen wir die Division mit Rest und erhalten

$$b = r_1 q_2 + r_2 \quad \text{mit } 0 \leq r_2 < r_1,\ q_2 \in \mathbb{Z}.$$

Ist nun $r_2 = 0$, so ist $\operatorname{ggT}(b, r_1) = \operatorname{ggT}(r_1, r_2) = r_1$. Ist $r_2 \neq 0$, so setzen wir fort

$$\begin{aligned}
r_1 &= r_2 q_3 + r_3 && \text{mit } 0 \leq r_3 < r_2,\ q_3 \in \mathbb{Z},\\
&\ldots\\
r_{i-2} &= r_{i-1} q_i + r_i && \text{mit } 0 \leq r_i < r_{i-1},\ q_i \in \mathbb{Z},\\
&\ldots\\
r_{n-2} &= r_{n-1} q_n + r_n && \text{mit } 0 \leq r_n < r_{n-1},\ q_n \in \mathbb{Z},\\
r_{n-1} &= r_n q_{n+1} + \underbrace{0}_{r_{n+1}} && \text{mit } q_{n+1} \in \mathbb{Z},
\end{aligned}$$

bis wir schließlich den Rest 0 erhalten. Wegen $b > r_1 > r_2 > \ldots \geq 0$ passiert das nach höchstens b Schritten. Dann ist

$$\mathrm{ggT}(a,b) = \mathrm{ggT}(b,r_1) = \cdots = \mathrm{ggT}(r_{i-1},r_i) = \cdots = \mathrm{ggT}(r_n,0) = r_n.$$

Zusammenfassend haben wir Folgendes gezeigt.

Satz 1.16 (Euklidischer Algorithmus). *Seien $a \in \mathbb{Z}$ und $b \in \mathbb{N}$. Es sei $r_{-1} = a$, $r_0 = b$, und für $i \in \mathbb{N}$ seien $r_i \in \mathbb{N}_0$ und $q_i \in \mathbb{Z}$ mittels Division mit Rest rekursiv definiert durch*

$$\begin{cases} r_{i-2} = r_{i-1}q_i + r_i \quad \textit{mit} \quad 0 \leq r_i < r_{i-1} & \textit{falls } r_{i-1} \neq 0. \\ r_i = q_i = 0 & \textit{falls } r_{i-1} = 0. \end{cases}$$

Dann gibt es ein minimales $n \in \mathbb{N}_0$ mit $r_{n+1} = 0$ und es ist $\mathrm{ggT}(a,b) = r_n$.

Außerdem liefert der euklidische Algorithmus auch ein Verfahren um $r_n = \mathrm{ggT}(a,b)$ als Linearkombination von a und b auszudrücken: Aus dem ersten Schritt ergibt sich $r_1 = a - bq_1$. Setzt man dies in den zweiten Schritt ein, so folgt $r_2 = b - r_1q_2 = b - (a - bq_1)q_2 = (-q_2)a + (1 + q_1q_2)b$. Fährt man weiter so fort, erhält man schließlich r_n als Linearkombination von a und b. Die dabei entstehenden Koeffizienten lassen sich durch folgende Rekursion ausdrücken. Dieses Verfahren wird oft als *erweiterter euklidischer Algorithmus* bezeichnet.

Satz 1.17. *Seien $r_{-1} = a \in \mathbb{Z}$, $r_0 = b \in \mathbb{N}$. Seien weiters $n \in \mathbb{N}_0$ und r_i, $q_i \in \mathbb{Z}$ für $i \in [1,n]$ so definiert wie in Satz 1.16. Wir definieren rekursiv $x_0 = 0$, $x_1 = 1$, $y_0 = 1$, $y_1 = -q_1$,*

$$x_i = x_{i-2} - q_ix_{i-1} \quad \textit{und} \quad y_i = y_{i-2} - q_iy_{i-1} \quad \textit{für } i \in [2,n].$$

Dann ist $\mathrm{ggT}(a,b) = x_na + y_nb$.

Beweis. Wir behaupten allgemeiner $r_i = x_ia + y_ib$ für alle $i \in [0,n]$, und zeigen dies durch Induktion nach i. Für $i = 0$ ist $r_0 = b = 0 \cdot a + 1 \cdot b$ und für $i = 1$ ist $r_1 = a - bq_1 = 1 \cdot a + (-q_1)b$.

Sei $i \geq 2$ und die Aussage gelte für $i-1$ und $i-2$. Es ist, nach Induktionsvoraussetzung,

$$\begin{aligned} r_i &= r_{i-2} - r_{i-1}q_i = (x_{i-2}a + y_{i-2}b) - (x_{i-1}a + y_{i-1}b)q_i \\ &= (x_{i-2} - q_ix_{i-1})a + (y_{i-2} - q_iy_{i-1})b \\ &= x_ia + y_ib. \end{aligned}$$

Mit $i = n$ folgt wegen $r_n = \mathrm{ggT}(a,b)$ die Aussage. □

Bemerkung. (1) Der euklidische Algorithmus, zusammen mit Satz 1.12 und Lemma 1.13, liefert einen weiteren Beweis für die Existenz des größten gemeinsamen Teilers und kleinsten gemeinsamen Vielfachen (Korollar 1.8 und 1.10).

Der erweiterte euklidische Algorithmus liefert einen direkten und konstruktiven Beweis für die Richtung (b) $\Rightarrow$ (a) von Satz 1.7 im Fall $n = 2$. Man bezeichnet diese Aussage, dass sich $\mathrm{ggT}(a, b)$ als $\mathbb{Z}$-Linearkombination von a und b schreiben lässt, auch als *Lemma von Bezóut*. Der Fall $n > 2$ kann dann mit Hilfe von Lemma 1.13 gezeigt werden.

(2) Sei $a > b > 0$. Wir haben bereits beobachtet, dass der euklidische Algorithmus höchstens b Schritte braucht. Mit ein wenig mehr Aufwand kann man zeigen, dass er stets weniger als $5 \log_{10} b + 1$ Schritte braucht (Lamè, 1844). Das macht den Algorithmus sehr effizient: Die Laufzeit ist (schlimmstenfalls) proportional zur Anzahl der Dezimalziffern der kleineren Zahl, b.

(3) Als Variante der Division mit Rest kann man zeigen: für $a \in \mathbb{Z}$ und $b \in \mathbb{N}$ gibt es eindeutig bestimmte $q \in \mathbb{Z}$ und $r \in \mathbb{Z}$ mit $a = bq + r$ und $-b/2 < r \leq b/2$ (Übung). Verwendet man im euklidischen Algorithmus diese Division mit Rest, so braucht man mitunter noch weniger Schritte, da im allgemeinen der Rest im Absolutbetrag hier schneller kleiner wird (obere Schranken für den Absolutbetrag der Reste: $b/2 \to b/4 \to b/8 \to b/16$, ...).

1.5 Anwendungen

1.5.1 Reduzierte Bruchdarstellung

Nach Konstruktion der rationalen Zahlen[1] lässt sich jedes $x \in \mathbb{Q}$ in der Form $x = \frac{m}{n}$ mit $m, n \in \mathbb{Z}$ und $n \neq 0$ schreiben. Es ist aber a priori keineswegs klar, dass es eine eindeutige reduzierte („gekürzte“) Bruchdarstellung gibt.

Satz 1.18. *Sei $x \in \mathbb{Q}$. Dann gibt es eindeutig bestimmte $a \in \mathbb{Z}$ und $b \in \mathbb{N}$ mit*

$$x = \frac{a}{b} \quad \textit{und} \quad \mathrm{ggT}(a, b) = 1.$$

Man nennt a den reduzierten Zähler *und b den* reduzierten Nenner *von x.*

Beweis. *Existenz:* Es gibt $m \in \mathbb{Z}$ und $n \in \mathbb{Z} \setminus \{0\}$ mit $x = \frac{m}{n}$. Wegen $\frac{m}{n} = \frac{-m}{-n}$ können wir ohne Einschränkung $n \in \mathbb{N}$ annehmen. Sei $d = \mathrm{ggT}(m, n)$ und seien $a, b \in \mathbb{Z}$ mit $m = ad$ und $n = bd$. Wegen $n > 0$ ist auch $b > 0$. Dann ist

$$x = \frac{m}{n} = \frac{ad}{bd} = \frac{a}{b}.$$

[1] als Quotientenkörper von $\mathbb{Z}$

Hierbei ist $\mathrm{ggT}(a,b) = 1$ aufgrund von Satz 1.11(1).

Eindeutigkeit: Angenommen es sind $a, a' \in \mathbb{Z}$ und $b, b' \in \mathbb{N}$ mit

$$\frac{a}{b} = \frac{a'}{b'} \quad \text{und} \quad \mathrm{ggT}(a,b) = \mathrm{ggT}(a',b') = 1.$$

Dann ist $ab' = a'b$. Also gilt $b' \mid a'b$ und wegen $\mathrm{ggT}(b',a') = 1$ folgt $b' \mid b$ aus Satz 1.11(2). Genauso gilt $b \mid ab'$ und wegen $\mathrm{ggT}(b,a) = 1$ folgt $b \mid b'$. Damit ist $b = |b| = |b'| = b'$, und deshalb $ab = a'b$. Aufgrund der Kürzbarkeit von b folgt schließlich $a = a'$. □

1.5.2 Rationale Nullstellen ganzzahliger Polynome

Folgender Satz hilft beim Auffinden rationaler Nullstellen von Polynomen mit ganzzahligen Koeffizienten. Man beachte aber, dass ein ganzzahliges Polynom natürlich weitere Nullstellen (in $\mathbb{C}$) haben kann, die nicht rational sind.

Satz 1.19. *Sei $f = a_n X^n + a_{n-1}X^{n-1} + \cdots + a_1 X + a_0 \in \mathbb{Z}[X]$ ein Polynom mit $n \in \mathbb{N}_0$ und $a_0, \ldots, a_n \in \mathbb{Z}$. Ist $x \in \mathbb{Q}$ mit $f(x) = 0$ und $x = \frac{a}{b}$ mit $a \in \mathbb{Z}$, $b \in \mathbb{N}$ und $\mathrm{ggT}(a,b) = 1$, so gilt $a \mid a_0$ und $b \mid a_n$.*

Beweis. Es ist

$$0 = f\left(\frac{a}{b}\right) = \sum_{i=0}^{n} a_i \left(\frac{a}{b}\right)^i$$

Nach Multiplikation mit b^n erhalten wir

$$0 = \sum_{i=0}^{n} a_i a^i b^{n-i}.$$

Daraus folgt

$$a_n a^n = -\sum_{i=0}^{n-1} a_i a^i b^{n-i} = -b \underbrace{\sum_{i=0}^{n-1} a_i a^i b^{n-i-1}}_{\in\mathbb{Z}},$$

und damit $b \mid a_n a^n$. Wegen $1 = \mathrm{ggT}(b,a) = \mathrm{ggT}(b,a^n)$ folgt auch $b \mid a_n$ nach Satz 1.11(2).

Analog ist

$$a_0 b^n = -\sum_{i=1}^{n} a_i a^i b^{n-i} = -a \underbrace{\sum_{i=1}^{n} a_i a^{i-1} b^{n-i}}_{\in\mathbb{Z}},$$

und deshalb $a \mid a_0 b^n$. Wieder folgt wegen $1 = \mathrm{ggT}(a,b) = \mathrm{ggT}(a,b^n)$ hieraus $a \mid a_0$. □

Korollar 1.20. *Seien $m, n \in \mathbb{N}$. Ist m keine n-te Potenz in $\mathbb{Z}$ (also m nicht von der Form $m = a^n$ mit $a \in \mathbb{N}$), so ist $\sqrt[n]{m}$ irrational.*

Beweis. Wir nehmen an $z = \sqrt[n]{m}$ sei rational, das heißt $z \in \mathbb{Q}$. Dann ist $z = \frac{a}{b}$ mit $a \in \mathbb{N}$, $b \in \mathbb{N}$ und $\mathrm{ggT}(a, b) = 1$. Wegen $z^n = m$ ist z Nullstelle des ganzzahligen Polynoms $X^n - m$. Aus Satz 1.19 folgt $b \mid 1$, also $b = 1$. Dann ist aber $z = a \in \mathbb{N}$, und deshalb $m = a^n$ eine n-te Potenz in $\mathbb{N}$. □

Das vorhergehende Korollar impliziert sofort, dass $\sqrt{2}$, $\sqrt{3}$, $\sqrt{5}$, ... irrational sind. (Allgemeiner folgt, dass $\sqrt{p}$ für jede Primzahl p irrational ist; das wird im nächsten Abschnitt klar, sobald wir die Definition einer Primzahl haben.)

1.5.3 Lineare diophantische Gleichungen

Satz 1.21. *Seien $n \in \mathbb{N}$ und $c, a_1, \ldots, a_n \in \mathbb{Z}$. Die lineare diophantische Gleichung*

$$a_1X_1 + \cdots + a_nX_n = c \tag{1.2}$$

besitzt genau dann eine Lösung (in $\mathbb{Z}$) wenn gilt $\mathrm{ggT}(a_1, \ldots, a_n) \mid c$.

Beweis. Sei $d = \mathrm{ggT}(a_1, \ldots, a_n)$. Nach Satz 1.7 gibt es $x_1, \ldots, x_n \in \mathbb{Z}$ mit $d = a_1x_1 + \cdots + a_nx_n$.

„⇐“ Angenommen es ist $d \mid c$. Dann gibt es ein $k \in \mathbb{Z}$ mit $c = dk$ und damit ist $c = a_1(x_1k) + \cdots + a_n(x_nk)$.

„⇒“ Wir nehmen nun umgekehrt an, dass Gleichung (1.2) eine ganzzahlige Lösung besitzt, das heißt, es gibt $x_1, \ldots, x_n \in \mathbb{Z}$ mit $c = a_1x_1 + \cdots + a_nx_n$. Wegen $d \mid a_i$ für alle $i \in [1, n]$ folgt dann aus Lemma 1.4(5) auch $d \mid c$. □

Satz 1.22. *Seien $a, b, c \in \mathbb{Z}$ mit $ab \neq 0$. Seien weiters $d = \mathrm{ggT}(a, b)$ und $x, y \in \mathbb{Z}$ mit $d = ax + by$. Ist $d \mid c$, so ist die Lösungsmenge der diophantischen Gleichung*

$$aX + bY = c$$

gegeben durch

$$\left\{ \left(\frac{cx + bk}{d}, \frac{cy - ak}{d} \right) \;\middle|\; k \in \mathbb{Z} \right\} \subset \mathbb{Z}^2.$$

Beweis. Wegen $d \mid a$, $d \mid b$ und $d \mid c$ besteht die angegebene Menge aus Paaren ganzer Zahlen, und man rechnet sofort nach, dass es sich tatsächlich um Lösungen der Gleichung handelt.

Sei nun $(x', y') \in \mathbb{Z}^2$ eine beliebige Lösung der Gleichung, das heißt, $ax' + by' = c$. Dann ist $a(x' - \frac{c}{d}x) + b(y' - \frac{c}{d}y) = 0$. Setzen wir $u = x' - \frac{c}{d}x$ und $v = y' - \frac{c}{d}y$ so gilt also $au = -bv$ und weiter $\frac{a}{d}u = -\frac{b}{d}v$. Hierbei sind $\frac{a}{d}, \frac{b}{d} \in \mathbb{Z}$. Wegen $\mathrm{ggT}(\frac{a}{d}, \frac{b}{d}) = 1$ schließt man $\frac{a}{d} \mid v$ und $\frac{b}{d} \mid u$ aus Satz 1.11(2). Damit folgt $u = \frac{b}{d}k$ und $v = \frac{a}{d}l$ mit $k, l \in \mathbb{Z}$. Wegen $a \neq 0$ und $b \neq 0$, folgt aus $\frac{ab}{d^2}k = -\frac{ab}{d^2}l$ dann $l = -k$. Damit ist $x' = \frac{cx+bk}{d}$ und $y' = \frac{cy-ak}{d}$. □

Bemerkung. Die Lösungsmenge linearer diophantischer Gleichungen in mehr als zwei Unbestimmten kann iterativ bestimmt werden. Wir verweisen auf [Bun08, Kapitel 1, §3.5 und §3.6].

2 Primzahlen und der Fundamentalsatz der Arithmetik

2.1 Primzahlen

Jede natürliche Zahl a besitzt stets die trivialen positiven Teiler 1 und a. Jenen Zahlen ($\neq 1$) die keine weiteren positiven Teiler besitzen kommt in der Zahlentheorie eine ganz besondere Rolle zu.

Definition 2.1. Eine natürliche Zahl $p \in \mathbb{N}$ heißt *Primzahl*, wenn $p > 1$ und wenn 1 und p die einzigen positiven Teiler von p sind. Wir bezeichnen mit $\mathbb{P} \subset \mathbb{N}$ die Menge aller Primzahlen.

Beispiel. Die Primzahlen kleiner gleich 10 sind 2, 3, 5, 7.

Satz 2.2. *Für $p \in \mathbb{N}_{\geq 2}$ sind folgende Aussagen äquivalent:*

(a) *p ist eine Primzahl.*

(b) *Sind $a, b \in \mathbb{Z}$ mit $p \mid ab$, so folgt $p \mid a$ oder $p \mid b$.*

(c) *Ist $p = ab$ mit $a, b \in \mathbb{Z}$, so ist $a \in \{\pm 1\}$ oder $b \in \{\pm 1\}$.*

Beweis. (a) $\Rightarrow$ (b): Sei $p \mid ab$. Weil 1 und p die einzigen positiven Teiler von p sind, ist $\mathrm{ggT}(p, a) \in \{1, p\}$. Ist $\mathrm{ggT}(p, a) = p$ so ist $p \mid a$. Ist $\mathrm{ggT}(p, a) = 1$, so ist $p \mid b$ aufgrund von Satz 1.11(2).

(b) $\Rightarrow$ (c): Aus $p = ab$ folgt $p \mid ab$. Nach Voraussetzung gilt $p \mid a$ oder $p \mid b$. Durch eventuelle Vertauschung von a und b können wir ohne Einschränkung annehmen $p \mid a$. Dann ist $a = pk$ mit $k \in \mathbb{Z}$ und deshalb $p = ab = pkb$. Weil p kürzbar ist, folgt $1 = kb$ und somit $b \in \{\pm 1\}$.

(c) $\Rightarrow$ (a): Sei d ein positiver Teiler von p mit $d \neq 1$. Dann ist $p = dk$ mit $k \in \mathbb{N}$. Wegen $d \neq 1$ folgt nach Voraussetzung $k \in \{\pm 1\}$. Wegen $p > 0$ und $d > 0$ ist $k = 1$ und deshalb $d = p$. □

Lemma 2.3. *Seien $p \in \mathbb{P}$, $n \in \mathbb{N}$ und $a_1, \ldots, a_n \in \mathbb{Z}$. Ist $p \mid a_1 \cdots a_n$, so gibt es ein $i \in [1, n]$ mit $p \mid a_i$.*

Beweis. Induktion nach n. Die Aussage ist trivialerweise richtig für $n = 1$. Sei nun $n > 1$ und die Aussage gelte für $n - 1$. Es ist $p \mid (a_1 \cdots a_{n-1})a_n$ und weil p eine Primzahl ist folgt $p \mid a_1 \cdots a_{n-1}$ oder $p \mid a_n$ nach Satz 2.2(b). In letzterem Fall sind wir fertig (mit $i = n$), in ersterem folgt $p \mid a_i$ für ein $i \in [1, n-1]$ nach Induktionsvoraussetzung. □

Lemma 2.4. *Sei $a \in \mathbb{N}_{\geq 2}$, und sei $p = \min\{\, b \in \mathbb{N}_{\geq 2} \mid b \mid a \,\}$.*

(1) *p ist eine Primzahl.*

(2) *Ist a keine Primzahl, so ist $p \leq \sqrt{a}$.*

(3) *a ist genau dann eine Primzahl, wenn a von keinem $b \in \mathbb{N}$ mit $1 < b \leq \sqrt{a}$ geteilt wird.*

Beweis. Zuerst halten wir fest, dass a in der angegebenen Menge enthalten ist, diese also nicht-leer ist, und deshalb nach dem Wohlordnungsprinzip tatsächlich ein kleinstes Element p besitzt.

(1) Sei $b \in \mathbb{N}$ mit $b > 1$ und $b \mid p$. Dann ist wegen $p \mid a$ auch $b \mid a$ und außerdem $b \leq p$. Aufgrund der Minimalität von p folgt $b = p$. Also sind 1 und p die einzigen positiven Teiler von p.

(2) Sei $a = pb$ mit $b \in \mathbb{N}$. Da a keine Primzahl ist, ist $b > 1$. Nach Definition von p gilt dann $p \leq b$ und deshalb $p^2 \leq pb = a$, also $p \leq \sqrt{a}$.

(3) „⇒“ Ist a eine Primzahl, so sind 1 und a die einzigen Teiler von a.

„⇐“ Durch Widerspruch. Angenommen a ist keine Primzahl. Nach (2) ist p ein Teiler von a mit $1 < p < \sqrt{a}$. □

Bemerkung (Sieb des Eratosthenes). Lemma 2.4(3) bildet die Grundlage eines effizienten Verfahrens um alle Primzahlen in einem Intervall zu bestimmen, nämlich des *Siebs des Eratosthenes*. Möchte man alle Primzahlen p mit $a \leq p \leq b$ bestimmen, genügt es demnach alle Zahlen im diskreten Intervall $[a, b]$ aufzuschreiben und sukzessive die Vielfachen aller Primzahlen im Intervall $[2, \sqrt{b}]$ zu streichen. In den Übungen werden wir dieses Verfahren in der Praxis ausprobieren.

2.2 Fundamentalsatz der Arithmetik

Wir wollen nun zeigen, dass jede natürliche Zahl $a \geq 2$ in eindeutiger Weise als Produkt von Primzahlen $a = p_1 \cdots p_n$ mit $n \geq 1$ und $p_1, \ldots, p_n \in \mathbb{P}$ dargestellt werden kann. Mit der üblichen Konvention, dass das leere Produkt gleich der Eins ist, also $1 = \prod_{i=0}^{0} p_i$, gilt diese Darstellung auch für $a = 1$.

Satz 2.5. *Jede natürliche Zahl lässt sich als Produkt von Primzahlen darstellen. Diese Darstellung ist, bis auf die Reihenfolge der Faktoren, eindeutig.*

Insbesondere besitzt jedes $a \in \mathbb{N}$ eine eindeutige Darstellung $a = p_1^{e_1} \cdots p_n^{e_n}$ mit $n \in \mathbb{N}_0$, $e_1, \ldots, e_n \in \mathbb{N}$ und $p_1, \ldots, p_n \in \mathbb{P}$ mit $p_1 < \cdots < p_n$.

Beweis. Es genügt die erste Aussage zu zeigen; die Aussage unter "insbesondere" folgt dann unmittelbar durch Gruppierung gleicher Primfaktoren.

Existenz: Sei $a \in \mathbb{N}$. Wir führen den Beweis durch Induktion nach a. Ist $a = 1$, so ist a das leere Produkt. Sei nun $a > 1$ und die Aussage gelte für alle $a' \in \mathbb{N}$ mit $a' < a$. Nach Lemma 2.4(1) gibt es ein $p \in \mathbb{P}$ mit $p \mid a$. Dann ist $a = pb$ mit $b \in \mathbb{N}$. Wegen $p \geq 2$ ist $b < a$, und daher gibt es, nach Induktionsvoraussetzung, $m \in \mathbb{N}_0$ und $p_1, \ldots, p_m \in \mathbb{P}$ mit $b = p_1 \cdots p_m$. Dann ist aber $a = pp_1 \cdots p_m$.

Eindeutigkeit: Wir zeigen die Aussage wieder durch Induktion nach a. Ist $a = 1$ so, lässt sich a nur als das leere Produkt darstellen. Sei $a > 1$ und die Aussage gelte für alle $a' \in \mathbb{N}$ mit $a' < a$. Angenommen es ist $a = p_1 \cdots p_n = p'_1 \cdots p'_m$ mit $m, n \in \mathbb{N}$ und $p_1, \ldots, p_n, p'_1, \ldots, p'_m \in \mathbb{P}$.

Wegen $p_1 \mid p'_1 \cdots p'_m$ gibt es nach Lemma 2.3 ein $i \in [1, m]$ mit $p_1 \mid p'_i$. Nach einer eventuellen Umnummerierung der p'_i können wir annehmen $i = 1$, also $p_1 \mid p'_1$. Weil p'_1 eine Primzahl ist, folgt daraus $p_1 = p'_1$. Durch Kürzen folgt dann $p_2 \cdots p_n = p'_2 \cdots p'_m$. Wegen $p_2 \ldots p_n < a$ folgt aber nach Induktionsvoraussetzung $m = n$, und nach geeigneter Umnummerierung ist $p_i = p'_i$ für alle $i \in [2, n]$. □

Beispiel. Es ist $12 = 2 \cdot 3 \cdot 2 = 3 \cdot 2 \cdot 2$; hier ist die Darstellung mit $p_1 = 2$, $p_2 = 3$, $p_3 = 2$ und $p'_1 = 3$, $p'_2 = 2$, $p'_3 = 2$ eindeutig bis auf Umordnung. Verwenden wir eine Darstellung wie unter "Insbesondere" genannt, erhalten wir $12 = 2^2 \cdot 3$ also $p_1 = 2$, $p_2 = 3$, $e_1 = 2$, $e_2 = 1$.

Bemerkung. Die Zahl 1 ist keine Primzahl. Würde man 1 als Primzahl zulassen, so hätte man keine eindeutige Darstellung als Produkt von Primzahlen, da stets $a = p_1 \cdots p_n = 1p_1 \cdots p_n = 1^m p_1 \cdots p_n$ für beliebiges $m \in \mathbb{N}$ gilt.

2.3 Verteilung der Primzahlen

Fragen zur Verteilung der Primzahlen in den natürlichen Zahlen gehören seit jeher zu den zentralen Fragen der Zahlentheorie.

Satz 2.6 (Euklid). *Es gibt unendlich viele Primzahlen.*

Beweis. Angenommen $\mathbb{P}$ ist endlich. Sei dann $\mathbb{P} = \{p_1, \ldots, p_n\}$. Wir setzen $a = p_1 \cdots p_n + 1$. Wegen $2 \in \mathbb{P}$ ist $a > 1$. Nach Lemma 2.4 gibt es eine Primzahl p mit $p \mid a$. Dann muss aber $p = p_i$ für ein $i \in [1, n]$ gelten. Damit ist $p \mid a - p_1 \cdots p_n = 1$ und deshalb $p = 1$, ein Widerspruch dazu, dass p eine Primzahl ist. □

Folgende Verschärfung von Euklids Resultat sei hier ohne Beweis wiedergegeben. Der Beweis erfolgt üblicherweise mit Mitteln der analytischen Zahlentheorie. Einzelne Spezialfälle, zum Beispiel für Zahlen der Form $4k + 1$ oder Zahlen der Form $4k + 3$, lassen sich aber leicht elementar beweisen.

Satz 2.7 (Dirichlet, 1837). *Seien $a, b \in \mathbb{Z}$ mit $\mathrm{ggT}(a,b) = 1$. Dann gibt es unendlich viele Primzahlen der Form $ak + b$ mit $k \in \mathbb{Z}$.*

Definition 2.8. Die Funktion $\pi\colon \mathbb{R}_{\geq 0} \to \mathbb{N}_0$,

$$\pi(x) = |\{\, p \in \mathbb{P} \mid p \leq x \,\}|$$

heißt *Zählfunktion der Primzahlen.*

Satz 2.9 (Primzahlsatz, 1896). *Die Funktion $\pi(x)$ ist asymptotisch gleich $x/\log(x)$ für $x \to \infty$, das heißt*

$$\lim_{x\to\infty} \frac{\pi(x)}{x/\log(x)} = 1.$$

Achtung: In der Zahlentheorie bezeichnet $\log(x)$ den natürlich Logarithmus von x, mit Basis $e = 2,718\ldots$

Beweise des Primzahlsatzes erfolgen üblicherweise mit Mitteln der komplexen Analysis und werden entsprechend der analytischen Zahlentheorie zugerechnet. Der Satz wurde, unabhängig voneinander, zuerst von Hadamard und de la Vallée-Poussin 1896 bewiesen. Ein einfacher Beweis findet sich in [New80; Zag97]; siehe [Bun08, Kapitel 7, §3] für eine ausführlichere Darstellung.

Bemerkung. Das Studium der Primzahlzählfunktion π ist eng verknüpft mit dem Studium der Riemannschen ζ-Funktion, die für $s \in \mathbb{C}$ mit $\Re(s) > 1$ gegeben ist durch

$$\zeta(s) = \sum_{n\geq 1} \frac{1}{n^s} = \prod_{p\in\mathbb{P}} (1 - p^{-s})^{-1}.$$

Der Definitionsbereich der Funktion ζ lässt sich durch analytische Fortsetzung holomorph auf $\mathbb{C} \setminus \{1\}$ ausdehnen. (An der Stelle 1 besitzt ζ eine einfache Polstelle mit Residuum 1.)

Der Primzahlsatz folgt aus der Tatsache, dass ζ keine Nullstelle s mit $\Re(s) \geq 1$ besitzt. Allgemeiner weiß man, dass außer den „trivialen Nullstellen“ $-2, -4, -6, \ldots$, sämtliche Nullstellen von ζ im vertikalen Streifen $0 < \Re(s) < 1$ der komplexen Ebene liegen.

Die *Riemannsche Vermutung* besagt, dass für diese Nullstellen sogar $\Re(s) = \frac{1}{2}$ gilt. Ein Beweis der Riemannschen Vermutung – beziehungsweise besseres Wissen über die Verteilung Nullstellen von ζ – erlaubt genauere Aussagen über die Verteilung der Primzahlen, insbesondere bessere Fehlerterme bei der Approximation der Zählfunktion π. Die Riemannsche Vermutung ist äquivalent zu

$$\pi(x) = \mathrm{Li}(x) + O\big(\sqrt{x}\log(x)\big) \quad \text{für } x \to \infty \quad \text{mit} \quad \mathrm{Li}(x) = \int_2^x \frac{1}{\log(t)} dt.$$

Hierbei bildet $\mathrm{Li}(x)$ eine bessere Näherung von $\pi(x)$ als $x/\log(x)$, die beiden Funktionen sind aber asymptotisch äquivalent.

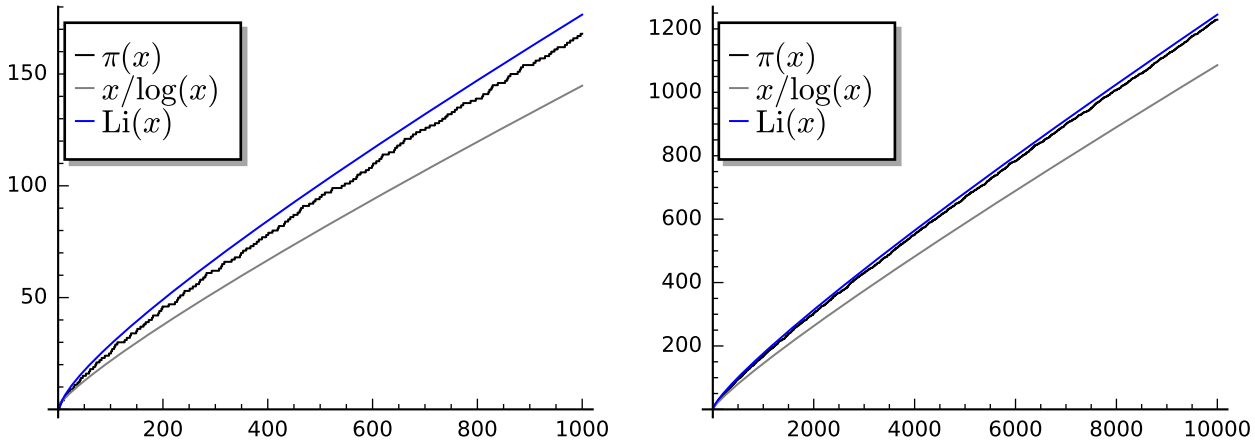

Abbildung 2.1: Primzahlzählfunktion $\pi(x)$ für $x \leq 1000$ und für $x \leq 10000$.

Der Primzahlsatz liefert zwar Aussagen über das asymptotische Verhalten der Zählfunktion, das bedeutet aber nicht, dass sich π auch so glatt verhält wie $x/\log(x)$.

Satz 2.10. *Zu jedem $n \in \mathbb{N}$ gibt es ein $N \in \mathbb{N}$ mit $\mathbb{P} \cap [N, N+n] = \emptyset$. Das heißt, $\mathbb{P}$ hat beliebig lange Lücken.*

Beweis. Sei $m = n + 1$. Keine der Zahlen

$$m! + 2,\ m! + 3,\ \ldots,\ m! + m$$

ist prim, da $i \mid m! + i$ für alle $i \in [2, m]$. Die Aussage folgt mit $N = m! + 2$. □

Andererseits gilt die *Bertrandsche Vermutung* (bewiesen 1852 von Tschebyscheff; hier ohne Beweis).

Satz 2.11 (Bertrandsche Vermutung). *Zu jedem $n \in \mathbb{N}_{\geq 2}$ gibt es eine Primzahl p mit $n < p < 2n$.*

Man vermutet auch, dass es auch unendlich viele Primzahlzwillinge gibt.

Vermutung (Primzahlzwillinge). Es gibt unendliche viele Primzahlen p für die auch $p + 2$ eine Primzahl ist.

Vor kurzem gelang hier ein Durchbruch; von einer vollständigen Lösung ist man dennoch weit entfernt.

Satz 2.12 (Zhang, 2013). *Für eine ganze Zahl $N < 70 \cdot 10^6$ gibt es unendlich viele Paare von Primzahlen $p < q$ mit $q - p \leq N$.*

Inzwischen weiß man $N \leq 246$ (Maynard 2014; Tao 2014). (Unter Annahme der verallgemeinerten Elliott-Halberstam Vermutung gilt $N \leq 6$.) Um die Vermutung über Primzahlzwillinge zu beweisen, müsste man zeigen $N \leq 2$.

2.4 Noch einmal Teilbarkeit, ggT und kgV

Aufgrund des Fundamentalsatzes ist folgende Definition sinnvoll.

Definition 2.13. Sei $a \in \mathbb{Z} \setminus \{0\}$ und $|a| = p_1 \cdots p_n$ mit $n \in \mathbb{N}_0$ und $p_1, \ldots, p_n \in \mathbb{P}$. Für $p \in \mathbb{P}$ sei die *p-adische Bewertung* von a

$$\mathrm{v}_p(a) = \left|\{\, i \in [1,n] \mid p = p_i \,\}\right| \in \mathbb{N}_0.$$

Das heißt, $\mathrm{v}_p(a)$ ist die Häufigkeit mit der die Primzahl p in der Primfaktorenzerlegung von $|a|$ auftritt.

Beispiel. Für $a = -6760 = -2^3 \cdot 5 \cdot 13^2$ ist $\mathrm{v}_2(a) = 3$, $\mathrm{v}_5(a) = 1$, $\mathrm{v}_{13}(a) = 2$ und $\mathrm{v}_p(a) = 0$ für alle $p \in \mathbb{P} \setminus \{2, 5, 13\}$. Für $a = 1$ ist $\mathrm{v}_p(a) = 0$ für alle $p \in \mathbb{P}$.

Wir fassen einige elementare Eigenschaften der p-adischen Bewertungsfunktionen zusammen.

Lemma 2.14. *Seien $a, b \in \mathbb{Z} \setminus \{0\}$.*

(1) *Es gibt nur endlich viele $p \in \mathbb{P}$ mit $\mathrm{v}_p(a) > 0$.*

(2) *$\mathrm{v}_p(a) = 0$ für alle $p \in \mathbb{P}$, genau dann wenn $a \in \{\pm 1\}$.*

(3) *$\mathrm{v}_p(ab) = \mathrm{v}_p(a) + \mathrm{v}_p(b)$.*

Beweis. (1) Klar, da jedes $a \in \mathbb{N}$ nur endlich viele Primteiler besitzt.

(2) Unmittelbar aus der Definition folgt $\mathrm{v}_p(\pm 1) = 0$ für alle $p \in \mathbb{P}$. Angenommen $a \notin \{\pm 1\}$. Dann ist $|a| > 1$ und nach Lemma 2.4 gibt es ein $p \in \mathbb{P}$ mit $p \mid |a|$. Dann ist $\mathrm{v}_p(a) \geq 1$.

(3) Sei $|a| = p_1 \cdots p_n$ und $b = q_1 \cdots q_m$ mit $n, m \in \mathbb{N}_0$ und $p_1, \ldots, p_n, q_1, \ldots, q_m \in \mathbb{P}$. Dann ist $|ab| = |a||b| = p_1 \cdots p_n q_1 \cdots q_m$ die eindeutige Primfaktorzerlegung von $|ab|$ und die Behauptung folgt unmittelbar aus der Definition von v_p. □

Mit dieser Definition lässt sich jedes $a \in \mathbb{Z} \setminus \{0\}$ darstellen als

$$a = \mathrm{sgn}(a) \prod_{p \in \mathbb{P}} p^{\mathrm{v}_p(a)},$$

wobei $\mathrm{sgn}(a) = 1$ falls $a > 0$ und $\mathrm{sgn}(a) = -1$ falls $a < 0$. Man beachte, dass dieses Produkt stets ein endliches Produkt ist, da $\mathrm{v}_p(a) = 0$ für alle bis auf endlich viele $p \in \mathbb{P}$ gilt.

Lemma 2.15. *Seien $a, b, a_1, \ldots, a_n \in \mathbb{Z} \setminus \{0\}$.*

(1) *$a \mid b \iff \mathrm{v}_p(a) \leq \mathrm{v}_p(b)$ für alle $p \in \mathbb{P}$.*

(2) *Es ist*

$$\operatorname{ggT}(a_1, \dots, a_n) = \prod_{p \in \mathbb{P}} p^{\min\{\mathrm{v}_p(a_1), \dots, \mathrm{v}_p(a_n)\}} \quad \textit{und}$$
$$\operatorname{kgV}(a_1, \dots, a_n) = \prod_{p \in \mathbb{P}} p^{\max\{\mathrm{v}_p(a_1), \dots, \mathrm{v}_p(a_n)\}}.$$

Beweis. (1): Weil $a \mid b$ äquivalent ist zu $|a| \mid |b|$, können wir $a, b \in \mathbb{N}$ annehmen. „$\Leftarrow$“: Für alle bis auf endlich viele $p \in \mathbb{P}$ ist $\mathrm{v}_p(b) = \mathrm{v}_p(a) = 0$. Außerdem ist stets $\mathrm{v}_p(b) - \mathrm{v}_p(a) \geq 0$. Deshalb ist

$$k = \prod_{p \in \mathbb{P}} p^{\mathrm{v}_p(b) - \mathrm{v}_p(a)} \in \mathbb{N}.$$

Und offensichtlich ist $ak = \pm b$, also $a \mid b$.

„$\Rightarrow$“: Sei $k \in \mathbb{Z}$ mit $ak = b$. Wegen $a \neq 0$ ist $k \neq 0$. Dann ist $\mathrm{v}_p(b) = \mathrm{v}_p(a) + \mathrm{v}_p(k) \geq \mathrm{v}_p(a)$ für alle $p \in \mathbb{P}$.

(2): Wir zeigen die Behauptung für den größten gemeinsamen Teiler; der Beweis für das kleinste gemeinsame Vielfache verläuft völlig analog. Sei

$$d = \prod_{p \in \mathbb{P}} p^{\min\{\mathrm{v}_p(a_1), \dots, \mathrm{v}_p(a_n)\}} \in \mathbb{N}.$$

Dann ist $\mathrm{v}_p(d) = \min\{\mathrm{v}_p(a_1), \dots, \mathrm{v}_p(a_n)\}$ für alle $p \in \mathbb{P}$. Aus (1) folgt $d \mid a_i$ für alle $i \in [1, n]$. Ist andererseits $d' \in \mathbb{N}$ mit $d' \mid a_i$ für alle $i \in [1, n]$, so folgt, wieder aus (1), die Ungleichung $\mathrm{v}_p(d') \leq \mathrm{v}_p(a_i)$ für alle $i \in [1, n]$ und $p \in \mathbb{P}$. Deshalb ist $\mathrm{v}_p(d') \leq \min\{\mathrm{v}_p(a_1), \dots, \mathrm{v}_p(a_n)\}$. Da dies für alle $p \in \mathbb{P}$ gilt, folgt unter einer weiteren Anwendung von (1) auch $d' \mid d$. □

Bemerkung. Unsere Definition der p-adischen Bewertungen hat den Schönheitsfehler, dass $\mathrm{v}_p(0)$ nicht definiert ist. Das ist mitunter lästig, weil man den Spezialfall der Null dann oft getrennt berücksichtigen muss.

Dies lässt sich wie folgt beheben: Man erweitert den Wertevorrat auf $\mathbb{N}_0 \cup \{\infty\}$, wobei $\infty > n$, $\infty + n = \infty$ und $\infty + \infty = \infty$ für alle $n \in \mathbb{N}_0$ gilt. Definiert man dann $\mathrm{v}_p(0) = \infty$, überlegt man sich sofort, dass Lemma 2.14(2),(3) und Lemma 2.15 auch gelten wenn ein oder mehrere der Zahlen Null sind. Damit Lemma 2.15(2) in dieser Form auch gültig bleibt wenn alle $a_i = 0$ sind (beim ggT) bzw. wenn ein $a_i = 0$ ist (beim kgV), muss man dabei allerdings die merkwürdig anmutendende Konvention $\prod_{p \in \mathbb{P}} p^{\infty} := 0$ treffen.

Bemerkung zur Algebra. Ein *Monoid* ist eine nicht-leere Menge H gemeinsam mit einer Verknüpfung $*\colon H \times H \to H$, so dass $*$ assoziativ ist (d.h., $a * (b * c) = (a * b) * c$ für alle $a, b, c \in H$), und es ein neutrales Element $1 \in H$ bezüglich $*$ gibt (d.h., $1 * a = a * 1 = a$ für alle $a \in H$).

Die Menge $(\mathbb{Z} \setminus \{0\})$ bildet mit der Multiplikation ein Monoid mit neutralem Element 1. Die Menge $\mathbb{N}_0$ bildet mit der Addition ein Monoid mit neutralem Element 0. Lemma 2.14(2),(3) impliziert, dass $\mathrm{v}_p \colon (\mathbb{Z} \setminus \{0\}, \cdot) \to (\mathbb{N}_0, +)$ ein Homomorphismus von Monoiden ist. Auch hier kann man die Null hinzunehmen, und erhält einen Homomorphismus $\mathrm{v}_p \colon \mathbb{Z} \to \mathbb{N}_0 \cup \{\infty\}$.

Liegen für die a_i also die Primfaktorisierungen vor, lassen sich ggT und kgV auf einen Blick bestimmen. Die Bestimmung der Primfaktorzerlegung einer beliebigen Zahl gilt aber als ein schwieriges Problem: Man kennt keine effizienten Algorithmen hierfür. Ist also die Primfaktorisierung der Zahlen noch nicht bekannt, bietet der euklidische Algorithmus das wesentlich effizientere Verfahren um ggT und kgV von großen Zahlen zu bestimmen.

Beispiel. Für

$$\begin{aligned} a &= 486200 = 2^3 \cdot 5^2 \cdot 11 \cdot 13 \cdot 17 \\ b &= 1226940 = 2^2 \cdot 3 \cdot 5 \cdot 11^2 \cdot 13^2 \\ c &= 2654652 = 2^2 \cdot 3 \cdot 7 \cdot 11 \cdot 13^2 \cdot 17 \end{aligned}$$

folgt

$$\begin{aligned} &\mathrm{ggT}(a,b,c) = 2^2 \cdot 11 \cdot 13 = 572, \\ &\mathrm{kgV}(a,b,c) = 2^3 \cdot 3 \cdot 5^2 \cdot 7 \cdot 11^2 \cdot 13^2 \cdot 17 = 1460058600. \end{aligned}$$

2.5 Fermat-/Mersenne-Zahlen und vollkommene Zahlen

Satz 2.16. *Seien $a \in \mathbb{N}_{\geq 2}$ und $n \in \mathbb{N}$.*

(1) *Ist $a^n + 1$ prim, so ist a gerade und $n = 2^k$ mit $k \in \mathbb{N}_0$.*

(2) *Ist $a^n - 1$ mit $n \geq 2$ prim, so ist $a = 2$ und n prim.*

Beweis. Wir zeigen zuerst: ($\star$) Sind $k, l \in \mathbb{N}$ mit $k \mid l$, so folgt $a^k - 1 \mid a^l - 1$.

Beweis davon: Ist $l = kk'$ mit $k' \in \mathbb{N}$, so folgt

$$a^l - 1 = (a^k)^{k'} - 1 = (a^k - 1) \sum_{j=0}^{k'-1} a^{jk}.$$

(1) Ist a ungerade, so ist $a^n + 1$ gerade und wegen $a^n + 1 > 2$ deshalb $a^n + 1 \notin \mathbb{P}$.

Sei $n = 2^k m$ mit m ungerade. Dann ist

$$a^n + 1 = a^{2^k m} + 1 = -\big((-a^{2^k})^m - 1\big) \quad \text{also nach } (\star) \quad a^{2^k} + 1 \mid a^n + 1.$$

Ist $a^n + 1 \in \mathbb{P}$, so muss wegen $1 < a^{2^k} + 1$ also gelten $a^{2^k} + 1 = a^n + 1$ und damit $n = 2^k$.

(2) Ist $a > 2$, so ist $1 < a - 1 < a^n - 1$. Wegen $a - 1 \mid a^n - 1$ (aufgrund von ($\star$)) ist dann $a^n - 1 \notin \mathbb{P}$. Ist n nicht prim, so gibt es ein $1 < m < n$ mit $m \mid n$. Dann ist $1 < a^m - 1 < a^n - 1$ und $a^m - 1 \mid a^n - 1$ (wieder ($\star$)). □

Definition 2.17. Für $n \in \mathbb{N}_0$ heißt die Zahl $F_n = 2^{2^n} + 1$ die *n-te Fermatsche Zahl*. Für $n \in \mathbb{N}$ heißt die Zahl $M_n = 2^n - 1$ die *n-te Mersennesche Zahl*.

Man nennt F_n, beziehungsweise M_n, eine *Fermatsche Primzahl*, beziehungsweise *Mersennesche Primzahl*, wenn sie prim ist.

Bemerkung. (1) $F_0 = 3$, $F_1 = 5$, $F_2 = 17$, $F_3 = 257$, $F_4 = 65537$ sind Primzahlen. Fermat vermutete (1640), dass auch die weiteren F_n Primzahlen sind. Euler zeigte 1732, dass $F_5 = 2^{32} + 1 = 4.294.967.297$ von 641 geteilt wird. Es ist derzeit keine weitere Fermatsche Primzahl bekannt. (Man vermutet, dass es keine weiteren gibt.)

Den Fermatschen Primzahlen kommt in der Elementargeometrie eine besondere Bedeutung zu: Das regelmäßige n-Eck ist genau dann mit Zirkel und Lineal konstruierbar wenn gilt $n = 2^k p_1 \cdots p_l$ mit verschiedenen Fermatschen Primzahlen p_1, $\ldots$, p_l. (Der Beweis erfolgt mit Mitteln der Algebra; Stichwort Galoistheorie.)

(2) Wir wissen, dass es unendlich viele Primzahlen gibt. Aber was ist die größte *bekannte* Primzahl? Hier hat sich geradezu ein Sport etabliert. Man untersucht immer größere Mersennesche Zahlen daraufhin ob Sie Primzahlen sind. (Zu testen ob eine Zahl eine Primzahl ist, ist auf effiziente Weise möglich. Die Primfaktorenzerlegung einer beliebigen Zahl zu bestimmen gilt hingegen als sehr schwieriges Problem für das kein effizienter Algorithmus bekannt ist).

Derzeit kennt man 51 Mersennesche Primzahlen. Die größte ist $M_{82.589.933}$, entdeckt am 7. Dezember 2018. Das ist eine Primzahl mit fast 25 Mio. Dezimalstellen.

Siehe http://www.mersenne.org und http://www.mersenne.org/primes/ für eine Liste aller bekannten Mersenneschen Primzahlen.

Definition 2.18. Für $n \in \mathbb{N}$ sei

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

die Summe der positiven Teiler von n.

Eine natürliche Zahl n heißt *vollkommen* wenn gilt $\sigma(n) = 2n$. Zum Beispiel ist $\sigma(6) = 1 + 2 + 3 + 6 = 12$ und deshalb 6 vollkommen. Die ersten vier vollkommenen Zahlen sind 6, 28, 496, 8128.

Es ist unbekannt, ob es ungerade vollkommene Zahlen gibt. Für gerade vollkommene Zahlen gibt es folgende Charakterisierung.

Satz 2.19. *Sei $n \in \mathbb{N}$ und $2 \mid n$. Dann ist n genau dann vollkommen, wenn es ein $k \geq 2$ gibt mit $n = 2^{k-1} M_k$ und weiters $M_k = 2^k - 1$ eine Primzahl ist.*

Beweis. „⇐“: Sei $n = 2^{k-1}M_k$ und $M_k \in \mathbb{P}$. Dann ist

$$\begin{aligned}\sigma(n) = \sigma(2^{k-1}M_k) &= \sum_{d|2^{k-1}} d + \sum_{d|2^{k-1}} dM_k = (1+M_k)\sum_{d|2^{k-1}} d \\ &= (1+M_k)\sum_{j=0}^{k-1} 2^j = 2^k(2^k-1) = 2n.\end{aligned}$$

„⇒“: Wir setzen an $n = 2^{k-1}m$ mit $k \geq 2$ und m ungerade. (Es gilt $k \geq 2$, weil wir $2 \mid n$ voraussetzen.) Dann ist nach Voraussetzung

$$2^k m = \sigma(2^{k-1}m) = \sum_{j=0}^{k-1} 2^j \sum_{d|m} d = (2^k-1)\sigma(m). \tag{2.1}$$

Weil $2^k - 1$ ungerade ist, gilt $2^k \mid \sigma(m)$, also $\sigma(m) = 2^k l$ mit $l \in \mathbb{N}$. Substituieren wir das auf der rechten Seite von Gleichung (2.1), und vergleichen mit der linken Seite, so folgt $m = (2^k - 1)l$.

Wäre $l > 1$, so wären $1, l, m$ verschiedene Teiler von m und deshalb $\sigma(m) \geq 1+l+m > 2^k l$, ein Widerspruch. Also ist $l = 1$ und $m = 2^k - 1$. Weiters ist $\sigma(m) = 2^k = m + 1$ und deshalb m eine Primzahl. □

Über Primzahlen und verwandte Themen gibt es noch sehr viele weitere interessante Sätze und Vermutungen. Das Buch *Die Welt der Primzahlen* von P. Ribenboim [Rib11] bietet eine leicht zugängliche Einführung, die weit über den Inhalt dieser Vorlesung hinausgeht.

3 Kongruenzen und Restklassenringe

3.1 Kongruenzen

Definition 3.1 (Kongruenz). Seien $m \in \mathbb{N}$ und $a, b \in \mathbb{Z}$. Dann heißt a *kongruent* (*zu*) b *modulo* m, geschrieben

$$a \equiv b \mod m,$$

wenn gilt $m \mid (a-b)$. Die Zahl m ist der *Modul* der Kongruenz. Ist a nicht kongruent zu b modulo m, so sagt man a ist *inkongruent* (*zu*) b *modulo* m und schreibt $a \not\equiv b \mod m$.

Für Kongruenz modulo m sind auch andere Schreibweisen üblich; zum Beispiel $a \equiv b \pmod{m}$, $a \equiv b \ (m)$, oder $a \equiv_m b$. Ist der Modul m aus dem Kontext klar, kann man auch abkürzen zu $a \equiv b$.

Beispiel. Es gilt $16 \equiv 2 \mod 7$, denn $7 \mid (16-2) = 14$. Es gilt $-1 \equiv 12 \mod 13$, denn $13 \mid (-1-12) = -13$. Andererseits ist $-1 \not\equiv 12 \mod 10$, denn $10 \nmid -13$.

Lemma 3.2. *Sei $m \in \mathbb{N}$.* Kongruenz modulo m *ist eine Äquivalenzrelation auf $\mathbb{Z}$, das heißt, für $a, b, c \in \mathbb{Z}$ gilt:*

- $a \equiv a \mod m$.
- $a \equiv b \mod m$ *genau dann wenn* $b \equiv a \mod m$.
- *Aus* $a \equiv b \mod m$ *und* $b \equiv c \mod m$ *folgt* $a \equiv c \mod m$.

Beweis. Es ist $m \mid (a-a) = 0$. Weiters ist $m \mid (a-b)$ genau dann wenn $m \mid -(a-b) = (b-a)$. Damit sind die ersten beiden Eigenschaften bewiesen. Sei nun $a \equiv b \mod m$ und $b \equiv c \mod m$, das heißt $m \mid (a-b)$ und $m \mid (b-c)$. Dann ist $m \mid (a-b)+(b-c) = a-c$ und deshalb $a \equiv c \mod m$. □

Insbesondere rechtfertigt die Symmetrie der Relation die Sprechweise „a und b sind [in]kongruent modulo m“, anstelle von „a ist [in]kongruent zu b modulo m“.

Beispiel. Zwei Zahlen $a, b \in \mathbb{Z}$ sind kongruent modulo 2, genau dann wenn entweder a, b beide gerade oder beide ungerade sind. Die Zahlen a, b sind inkongruent modulo 2, wenn eine der beiden Zahlen gerade und die andere ungerade ist.

Satz 3.3. *Seien $m \in \mathbb{N}$ und $a, b \in \mathbb{Z}$. Die folgenden Aussagen sind äquivalent:*

(a) $a \equiv b \mod m$.

(b) *a und b lassen bei Division durch m den selben Rest.*

Beweis. Seien $q_1, q_2 \in \mathbb{Z}$ und $r_1, r_2 \in [0, m-1]$ mit $a = q_1 m + r_1$ und $b = q_2 m + r_2$.

(a) $\Rightarrow$ (b): Es ist $a - b = (q_1 - q_2)m + (r_1 - r_2)$. Wegen $m \mid a - b$ folgt $m \mid r_1 - r_2$. Weil $|r_1 - r_2| < m$ ist, ist das aber nur möglich, wenn gilt $r_1 = r_2$.

(b) $\Rightarrow$ (a): Wegen $r_1 = r_2$ gilt $a - b = (q_1 - q_2)m$ und deshalb $m \mid a - b$, also $a \equiv b \mod m$. □

3.1.1 Rechnen mit Kongruenzen

Satz 3.4 (Rechenregeln I). *Seien $m \in \mathbb{N}$ und $a, b, c, d \in \mathbb{Z}$.*

(1) *Aus $a \equiv b \mod m$ und $c \equiv d \mod m$ folgen $a \pm c \equiv b \pm d \mod m$ und $ac \equiv bd \mod m$.*

Die Aussagen gelten sinngemäß auch für Summen/Produkte von mehr als zwei Elementen. Insbesondere*: Aus $a \equiv b \mod m$ folgt $a^k \equiv b^k \mod m$ für alle $k \in \mathbb{N}$.*

(2) *Sei $f \in \mathbb{Z}[X]$ ein ganzzahliges Polynom, das heißt,*

$$f = \sum_{i=0}^{n} c_i X^i \quad \text{mit } n \in \mathbb{N}_0,\ c_1, \ldots, c_n \in \mathbb{Z}.$$

Aus $a \equiv b \mod m$ folgt dann $f(a) \equiv f(b) \mod m$.

(3) *Aus $a \equiv b \mod m$ folgt $\operatorname{ggT}(a, m) = \operatorname{ggT}(b, m)$.*

Beweis. (1) Es gilt $m \mid a-b$ und $m \mid c-d$. Dann ist aber $m \mid (a-b) \pm (c-d) = (a \pm c) - (b \pm d)$ und deshalb $a \pm c \equiv b \pm d \mod m$. Wegen $ac - bd = ac - bc + bc - bd = (a-b)c + b(c-d)$ ist auch $m \mid ac - bd$ und deshalb $ac \equiv bd \mod m$.

Die Aussagen für Summen/Produkte von mehr als zwei Elementen folgen durch eine einfache Induktion.

(2) Es ist $f(a) = \sum_{i=0}^{n} c_i a^i$ und $f(b) = \sum_{i=0}^{n} c_i b^i$. Aus (1) folgt

$$f(a) \equiv \sum_{i=0}^{n} c_i a^i \equiv \sum_{i=0}^{n} c_i b^i \equiv f(b) \mod m.$$

(3) Ist $d = \operatorname{ggT}(a, m)$ so folgt wegen $m \mid a - b$ auch $d \mid a - b$ und weiter $d \mid b = a - (a - b)$. Deshalb gilt $d \mid \operatorname{ggT}(b, m)$. Durch Vertauschen von a und b folgt auch $\operatorname{ggT}(b, m) \mid \operatorname{ggT}(a, m)$, also $\operatorname{ggT}(a, m) = \operatorname{ggT}(b, m)$. □

Beispiel. (1) $M_{82.589.933}$ ist die größte bekannte Primzahl (siehe Abschnitt 2.5). Wir wollen die letzte Dezimalziffer („Einerstelle“) dieser Zahl bestimmen: Dazu berechnen wir $r \in [0,9]$ mit $2^n - 1 \equiv r \mod 10$ für $n = 82.589.933$. Da n in Dezimaldarstellung gegeben ist, bietet es sich an zuerst 2^{10^k} modulo 10 zu betrachten:

$$2^{10^k} \equiv (2^{5^k})^{2^k} \equiv 2^{2^k} \mod 10 \quad \text{denn } 2^5 \equiv 32 \equiv 2 \mod 10.$$

Nun ist $2^{2^0} \equiv 2 \mod 10$, $2^{2^1} \equiv 4 \mod 10$, $2^{2^2} \equiv 16 \equiv 6 \mod 10$ und $2^{2^3} \equiv 36 \equiv 6 \mod 10$. Wir sehen insbesondere $6^2 \equiv 6 \mod 10$. Daraus schließen wir induktiv $6^k \equiv 6 \mod 10$ für alle $k \in \mathbb{N}$. [Beweis: Für $k \in \{1,2\}$ wissen wir das bereits. Für $k \geq 3$ ist dann nach Induktionsvoraussetzung $6^k \equiv 6^{k-1} \cdot 6 \equiv 6 \cdot 6 \equiv 6 \mod 10$.]

Insbesondere ist also für $k \geq 2$

$$2^{2^k} \equiv (2^4)^{2^{k-2}} \equiv 6^{2^{k-2}} \equiv 6 \mod 10.$$

Schließlich erhalten wir

$$\begin{aligned} 2^{82.589.933} - 1 &\equiv 2^{825.899 \cdot 10^2 + 3 \cdot 10 + 3} - 1 \equiv 6^{825.899} \cdot \underbrace{2^{3 \cdot 2}}_{64 \equiv 4} \cdot 2^3 - 1 \\ &\equiv 6 \cdot \underbrace{4 \cdot 8}_{32 \equiv 2} - 1 \equiv 6 \cdot 2 - 1 \equiv 2 - 1 \equiv 1 \mod 10. \end{aligned}$$

Die letzte Dezimalziffer von $M_{82.589.933}$ ist also 1.

(2) $F_5 = 2^{2^5} + 1 = 2^{32} + 1$ ist teilbar durch 641 und deshalb keine Primzahl: Wegen $640 = 2^7 \cdot 5$ folgt $2^7 \cdot 5 \equiv -1 \mod 641$ und weiter $2^{28} 5^4 \equiv 1 \mod 641$. Weiters ist $641 = 16 + 625 = 2^4 + 5^4$, also $2^4 \equiv -5^4 \mod 641$. Damit folgt

$$2^{32} \equiv 2^{28} \cdot 2^4 \equiv 2^{28} \cdot (-5^4) \equiv -1 \mod 641,$$

also $641 \mid 2^{32} + 1$.

Bemerkung: Warum sollten wir gerade 641 im Verdacht haben ein Teiler von F_5 zu sein? Man kann zeigen (siehe [Bun08, §3.2.11]), dass jeder Primteiler von F_n die Form $2^{n+2}k + 1$ für $k \in \mathbb{N}_0$ hat. Für F_5 kommen also die Zahlen 129, 257, 385, 513, 641, ... in Frage. Aber 129, 385 und 513 sind keine Primzahlen; $257 = F_3$ und wegen $\operatorname{ggT}(F_3, F_5) = 1$ [1] kommt dieses nicht als Teiler in Frage. Tatsächlich ist also 641 die kleinste Zahl die als Primteiler von F_5 in Frage kommt.

Bis jetzt haben wir Kongruenzen stets für einen festen Modul m betrachtet. In folgendem Satz fassen wir Rechenregeln für veränderliche Moduln zusammen.

[1] Man kann durch Induktion leicht zeigen, dass für alle $n \in \mathbb{N}$ gilt $F_n - 2 = \prod_{i=0}^{n-1} F_i$. Daraus schließt man $\operatorname{ggT}(F_m, F_n) = 1$ für $0 \leq m < n$. Damit erhält man auch einen weiteren Beweis für die Unendlichkeit von $\mathbb{P}$, da die Mengen der Primteiler der F_n nicht-leer und paarweise disjunkt sind.

Satz 3.5 (Rechenregeln II). *Seien $m, m' \in \mathbb{N}$ und $a, b, c \in \mathbb{Z}$.*

(1) *Ist $a \equiv b \mod m$ und $m' \mid m$, so gilt auch $a \equiv b \mod m'$.*

(2) *Aus $a \equiv b \mod m$ folgt $ac \equiv bc \mod m|c|$.*

(3)

$$ac \equiv bc \mod m \iff a \equiv b \mod \frac{m}{\mathrm{ggT}(c,m)}.$$

Insbesondere: *Ist $\mathrm{ggT}(c,m) = 1$ so ist $ac \equiv bc \mod m$ äquivalent zu $a \equiv b \mod m$.*

(4) *Seien $m_1, \ldots, m_n \in \mathbb{N}$ und $m = \mathrm{kgV}(m_1, \ldots, m_n)$. Dann gilt*

$$a \equiv b \mod m_i \text{ für alle } i \in [1,n] \iff a \equiv b \mod m.$$

Beweis. (1) Es gilt $m \mid a-b$ und $m' \mid m$. Aufgrund der Transitivität der Teilerrelation folgt auch $m' \mid a-b$.

(2) Aus $m \mid a-b$ folgt $mc \mid (a-b)c = ac-bc$. Es ist aber $mc \mid ac-bc$ genau dann wenn $m|c| \mid ac-bc$ nach Lemma 1.4(2).

(3) Sei $d = \mathrm{ggT}(c,m)$.

„$\Rightarrow$“ Aus $m \mid ac-bc = (a-b)c$ folgt nach Satz 1.11(2) auch $m \mid (a-b)d$. Wegen $d \mid m$ ist das äquivalent zu $\frac{m}{d} \mid a-b$.

„$\Leftarrow$“ Sei $c = dc'$ mit $c' \in \mathbb{Z}$. Nach (2) folgt $ad \equiv bd \mod m$, und dann weiter, nach Satz 3.4(1) auch $ac \equiv adc' \equiv bdc' \equiv bc \mod m$.

(4) Die Richtung „$\Leftarrow$“ folgt wegen $m_i \mid m$ aus (1).

„$\Rightarrow$“ Ist $m_i \mid a-b$ für alle $i \in [1,n]$, so ist nach Definition des kleinsten gemeinsamen Vielfachen auch $m \mid a-b$. □

Beispiel. Achtung!

- Im Allgemeinen kann man *nicht kürzen* ohne den Modul zu verändern. Es ist $2 \cdot 2 \equiv 2 \cdot 0 \equiv 0 \mod 4$, aber $2 \not\equiv 0 \mod 4$. Aber es gilt $2 \equiv 0 \mod 2$ (siehe (3)).
- Sind $k, l \in \mathbb{N}$ mit $k \equiv l \mod m$, so folgt im Allgemeinen *nicht* $a^k \equiv a^l \mod m$. Zum Beispiel ist $1 \equiv 6 \mod 5$, aber $2^1 \not\equiv 2^6 \equiv 64 \equiv 4 \mod 5$.

3.1.2 Restklassen

Wir haben bereits gesehen, dass *Kongruenz modulo m* eine Äquivalenzrelation auf $\mathbb{Z}$ ist.

Definition 3.6 (Restklassen). Sei $m \in \mathbb{N}$.

(1) Die Äquivalenzklassen der Äquivalenzrelation $\equiv_m$ heißen *Restklassen* (modulo m). Ist $a \in \mathbb{Z}$, so schreibt man $\overline{a} := [a] := [a]_m$ für die Restklasse von a.

(2) Jedes $b \in \overline{a}$ heißt *Repräsentant* der Restklasse $\overline{a}$.

(3) $\mathbb{Z}/m\mathbb{Z} = \{\, \overline{a} \mid a \in \mathbb{Z} \,\}$ sei die Menge der Restklassen modulo m.

Nach Definition gilt also $a \equiv b \mod m \Leftrightarrow \overline{a} = \overline{b}$.

Beispiel. Für $m = 4$ ist

$$\begin{aligned}
\overline{0} &= \{\ldots, -12, -8, -4, \mathbf{0}, 4, 8, 12 \ldots\},\\
\overline{1} &= \{\ldots, -11, -7, -3, \mathbf{1}, 5, 9, 13 \ldots\},\\
\overline{2} &= \{\ldots, -10, -6, -2, \mathbf{2}, 6, 10, 14 \ldots\},\\
\overline{3} &= \{\ldots, -9, -5, -1, \mathbf{3}, 7, 11, 15 \ldots\}.
\end{aligned}$$

Nach Satz 1.1 gehört jedes $x \in \mathbb{Z}$ zu genau einer dieser Restklassen. Es folgt $\mathbb{Z}/4\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}\}$.

Bemerkung. Manchmal sieht man auch die Notation $\mathbb{Z}_m$ für $\mathbb{Z}/m\mathbb{Z}$. Wir wollen diese Notation nicht verwenden, denn hier besteht Verwechslungsgefahr mit den *p-adischen Zahlen*, die in der Zahlentheorie üblicherweise auch mit $\mathbb{Z}_p$ für $p \in \mathbb{P}$ bezeichnet werden.

Die Notation $\mathbb{Z}/m\mathbb{Z}$ fügt sich außerdem in eine allgemeiner Notation der Algebra ein: Ist R ein *Ring* und I ein *Ideal* von R, so bezeichnet R/I den *Faktorring* (siehe auch die Bemerkung nach Satz 3.14). Hier betrachten wir den Spezialfall $R = \mathbb{Z}$ und $I = m\mathbb{Z}$.

Lemma 3.7. *Sei $m \in \mathbb{N}$ und $a \in \mathbb{Z}$. Dann ist*

$$\overline{a} = \{\, a + mk \mid k \in \mathbb{Z} \,\} = a + m\mathbb{Z}.$$

Beweis. „$\supset$": Sei $k \in \mathbb{Z}$ und $b = a + mk$. Dann ist $b - a = mk$, und deshalb $a \equiv b \mod m$, also $b \in \overline{a}$.

„$\subset$": Sei $b \in \mathbb{Z}$ mit $b \equiv a \mod m$. Dann ist $m \mid (b - a)$. Sei $k \in \mathbb{Z}$ mit $mk = b - a$, so ist $b = a + mk$. □

Satz 3.8. *Sei $m \in \mathbb{N}$. Sind $a_1, \ldots, a_m \in \mathbb{Z}$ paarweise inkongruent modulo m (das heißt, $a_i \not\equiv a_j \mod m$ für $i \neq j$), so ist*

$$\mathbb{Z}/m\mathbb{Z} = \{\overline{a_1}, \ldots, \overline{a_m}\}.$$

Insbesondere ist $\mathbb{Z}/m\mathbb{Z} = \{\overline{0}, \ldots, \overline{m-1}\}$ und $|\mathbb{Z}/m\mathbb{Z}| = m$.

Beweis. Wir zeigen zuerst $\mathbb{Z}/m\mathbb{Z} = \{\overline{0}, \ldots, \overline{m-1}\}$. Nach Definition von $\mathbb{Z}/m\mathbb{Z}$ gilt die Inklusion „$\supset$". Wir zeigen „$\subset$". Ist $\alpha \in \mathbb{Z}/m\mathbb{Z}$ so gibt es nach Definition ein $a \in \mathbb{Z}$ mit $\alpha = \overline{a}$. Sei $a = qm + r$ mit $q \in \mathbb{Z}$ und $r \in [0, m-1]$. Dann ist $a \equiv r \mod m$ und deshalb $\overline{a} = \overline{r}$, also $\overline{a} \in \{\overline{0}, \overline{1}, \ldots, \overline{m-1}\}$.

$|\mathbb{Z}/m\mathbb{Z}| = m$: Seien $i, j \in [0, m-1]$ mit $i \neq j$. Dann gilt $0 < |i-j| < m$, und deshalb $m \nmid i - j$, also $\overline{i} \neq \overline{j}$. Darum sind $\overline{0}, \ldots, \overline{m-1}$ paarweise verschieden und $|\mathbb{Z}/m\mathbb{Z}| = m$.

Seien schließlich $a_1, \ldots, a_m \in \mathbb{Z}$ paarweise inkongruent modulo m, und sei $A = \{\overline{a_1}, \ldots, \overline{a_m}\}$. Dann gilt $\overline{a_i} \neq \overline{a_j}$ für $i \neq j$. Darum ist $|A| = m$ und wegen $A \subset \mathbb{Z}/m\mathbb{Z}$ und $|\mathbb{Z}/m\mathbb{Z}| = m$ folgt $A = \mathbb{Z}/m\mathbb{Z}$. □

Definition 3.9. Eine Menge von m ganzen Zahlen, die paarweise inkongruent modulo m sind, heißt *vollständiges Restsystem modulo m*.

Neben $[0, m-1]$, dem *kleinsten nicht-negativen Restsystem modulo m*, bildet auch $\{x \in \mathbb{Z} \mid -m/2 < x \leq m/2\}$, das *absolut kleinste Restsystem modulo m*, ein wichtiges vollständiges Restsystem.

Beispiel. Die Zahlen 0, 1, 2, 3 bilden ein vollständiges Restsystem modulo 4. Dasselbe gilt aber auch für -1, 0, 1, 2, denn es gilt $3 \equiv -1 \mod 4$. Auch 24, 5, 42, 7 bilden ein vollständiges Restsystem modulo 4.

3.1.3 Lineare Kongruenzen

Seien $m \in \mathbb{N}$ und $a, b \in \mathbb{Z}$. Wir suchen $x \in \mathbb{Z}$ die $ax \equiv b \mod m$ erfüllen. Man sagt dann, x löst die *lineare Kongruenz*

$$aX \equiv b \mod m \tag{3.1}$$

(in einer Unbestimmten X).

Löst $x \in \mathbb{Z}$ die Kongruenz (3.1) und ist $x' \in \mathbb{Z}$ mit $x \equiv x' \mod m$, so löst auch x' die Kongruenz (3.1). Die Eigenschaft Lösung der Kongruenz zu sein kommt also einer ganzen Restklasse zu. Mit der *Lösungsanzahl* der Kongruenz (3.1) meint man deshalb die Anzahl der Restklassen die Lösungen von (3.1) enthalten. Bei fest gewähltem vollständigen Restsystem ist dies genau die Anzahl der Elemente im Restsystem, die (3.1) lösen.

Satz 3.10. *Die Kongruenz* (3.1) *ist genau dann lösbar wenn gilt* $\mathrm{ggT}(a, m) \mid b$. *Die Lösungsanzahl der Kongruenz ist dann* $\mathrm{ggT}(a, m)$.
Insbesondere: *Ist* $\mathrm{ggT}(a, m) = 1$ *so ist die Kongruenz* (3.1) *eindeutig lösbar.*

Beweis. Sei ohne Einschränkung $a \neq 0$ (ist $a = 0$ so können wir stattdessen $a = m$ setzen, ohne die Lösungsmenge zu verändern). Für $x \in \mathbb{Z}$ ist

$$ax \equiv b \mod m \iff m \mid (ax - b) \iff \text{es gibt ein } y \in \mathbb{Z} \text{ mit } b = ax - my.$$

Das heißt, die Kongruenz (3.1) ist genau dann lösbar, wenn die diophantische Gleichung $aX - mY = b$ eine Lösung in $\mathbb{Z}$ besitzt. Nach Satz 1.21 ist das äquivalent zu $\mathrm{ggT}(a, m) \mid b$.

Wir müssen noch die Lösungsanzahl ermitteln. Sei dazu $d = \mathrm{ggT}(a, m)$. Ist (x_0, y_0) eine Lösung von $aX - mY = b$, so ist die Gesamtmenge der Lösungen dieser diophantischen Gleichung, nach Satz 1.22, gegeben durch

$$\left\{ \left(x_0 + k\frac{m}{d}, y_0 + k\frac{a}{d} \right) \;\middle|\; k \in \mathbb{Z} \right\}.$$

Wir zählen nun die Lösungen (x, y) für die x im vollständigen Restsystem $[x_0, x_0 + (m-1)]$ modulo m liegt. Das ist aber offensichtlich genau dann der Fall, wenn

$$x \in \left\{ x_0 + k\frac{m}{d} \;\middle|\; k \in [0, d-1] \right\}.$$

Das heißt, die Lösungsanzahl ist d. □

3.1.4 Simultane lineare Kongruenzen / Chinesischer Restsatz

Satz 3.11 (Chinesischer Restsatz). *Sei $n \in \mathbb{N}$. Seien $m_1, \ldots, m_n \in \mathbb{N}$ paarweise teilerfremd. Sind $a_1, \ldots, a_n \in \mathbb{Z}$, so hat das Kongruenzensystem*

$$X \equiv a_i \mod m_i \quad \text{für alle } i \in [1, n],$$

eine Lösung. Diese ist eindeutig modulo $m_1 \cdots m_n$.
(Das heißt, es gibt ein $x \in \mathbb{Z}$ mit $x \equiv a_i \mod m_i$ für alle $i \in [1, n]$, und wenn $x' \in \mathbb{Z}$ eine weitere solche Zahl ist, dann gilt $x \equiv x' \mod m_1 \cdots m_n$.)

Beweis. *Existenz:* Für $i \in [1, n]$ sei

$$t_i = \prod_{\substack{j=1 \\ j \neq i}}^{n} m_j = \frac{m}{m_i} \qquad \text{mit } m = m_1 \cdots m_n.$$

Aus Satz 1.11(4) folgt $\mathrm{ggT}(t_i, m_i) = 1$. Daher gibt es $y_i \in \mathbb{Z}$ mit $y_i t_i \equiv 1 \mod m_i$. Wir betrachten nun die Zahl

$$x = \sum_{j=1}^{n} a_j y_j t_j.$$

Sei $i \in [1, n]$. Wegen $m_i \mid t_j$ für alle $j \neq i$, folgt

$$x \equiv a_i y_i t_i + \sum_{\substack{j=1 \\ j \neq i}}^{n} a_j y_j t_j \equiv a_i y_i t_i \equiv a_i \mod m_i.$$

Eindeutigkeit: Ist x' eine weitere Zahl mit $x' \equiv a_i \mod m_i$ für alle $i \in [1, n]$ so ist $x \equiv x' \mod m_i$ für alle $i \in [1, n]$. Aus Satz 3.5(4) folgt $x \equiv x' \mod \mathrm{kgV}(m_1, \ldots, m_n)$. Wegen Lemma 1.14 ist $\mathrm{kgV}(m_1, \ldots, m_n) = m_1 \cdots m_n$. □

Beispiel. Wir bestimmen alle $x \in \mathbb{Z}$ mit $x \equiv 2 \mod 3$, $x \equiv 4 \mod 5$ und $x \equiv 3 \mod 7$. Es ist $5 \cdot 7 \equiv 2 \mod 3$, $3 \cdot 7 \equiv 1 \mod 5$ und $3 \cdot 5 \equiv 1 \mod 7$. Nun folgt $2 \cdot 2 \equiv 1 \mod 3$. Also ist

$$x_0 = 5 \cdot 2 \cdot 35 + 4 \cdot 1 \cdot 21 + 3 \cdot 1 \cdot 15 = 350 + 84 + 45 = 479.$$

eine Lösung. Die Lösungsmenge ist $479 + 105\mathbb{Z} = 59 + 105\mathbb{Z}$.

3.2 Restklassenringe

Die Menge der Restklassen besitzt eine algebraische Struktur, die wir uns nun ansehen wollen. Das wird es uns erlauben Kongruenzen von einem modernen, algebraischen Standpunkt aus zu betrachten. Damit lassen sich viele klassischen Resultate der elementaren Zahlentheorie als Spezialfälle allgemeinerer Sätze der Algebra herleiten. Diese strukturelle Sichtweise schafft einen klareren Zugang.

Die folgende Definition einer abelschen Gruppe sollte aus der linearen Algebra bekannt sein.

Definition 3.12 (Gruppe). Eine *Gruppe* ist eine Menge $\emptyset \neq G$ mit einer Verknüpfung $*\colon G \times G \to G$ und einem neutralen Element $e \in G$, so dass für alle $a, b, c \in G$ gilt

- $a * (b * c) = (a * b) * c$,
- $a = e * a = a * e$,
- es gibt ein $a' \in G$ mit $a * a' = a' * a = e$.

Gilt weiters $a * b = b * a$ für alle $a, b \in G$, so heißt G *abelsch* (oder *kommutativ*).

Zu jedem a ist das Element a' mit der Eigenschaft $a * a' = a' * a = e$ eindeutig bestimmt. [*Beweis:* Seien $a', a'' \in G$ mit $a * a' = a' * a = e$ und $a * a'' = a'' * a = e$. Dann ist $a' = a' * e = a' * (a * a'') = (a' * a) * a'' = e * a'' = a''$.]

Man nennt a' das *Inverse von a*. Man schreibt dafür üblicherweise a^{-1} bei multiplikativ geschriebener Verknüpfung ($\cdot$ statt $*$), und $-a$ bei additiv geschriebener Verknüpfung ($+$ statt $*$).

Bemerkung. Formal besteht eine Gruppe aus der zugrundeliegenden Menge G, der Verknüpfung $*$ und dem neutralen Element e. (Wobei e durch G und $*$ bereits eindeutig bestimmt ist). Man schreibt dies oft kompakt als Tupel $(G, *)$ oder $(G, *, e)$. Sind das neutrale Element und/oder die Verknüpfung aus dem Kontext klar, so schreibt man aber auch oft kürzer einfach G.

Analoge Konventionen gelten für andere algebraische Strukturen, insbesondere Ringe, die wir in der nächsten Definition einführen.

Definition 3.13 (Ring). Ein *Ring* (*mit Eins*) ist eine Menge $\emptyset \neq R$ mit zwei Verknüpfungen $+, \cdot \colon R \times R \to R$ und Elementen $0, 1$, so dass für alle $a, b, c \in R$ gilt:

- R mit $+$ als Verknüpfung und 0 als neutralem Element ist eine abelsche Gruppe,
- $1a = a = a1$,
- $a(bc) = (ab)c$,
- $a(b + c) = ab + bc$ und $(b + c)a = ba + ca$.

Gilt weiters $ab = ba$ für alle $a, b \in R$, so heißt R *kommutativ*.

$\mathbb{Z}$ ist ein kommutativer Ring. Vereinfacht gesagt gelten in jedem kommutativen Ring die „üblichen" Rechenregeln, wie wir sie von $\mathbb{Z}$ kennen (außer Kürzungsregeln!), denn sie lassen sich aus obigen Axiomen herleiten. Weitere Beispiele für kommutative Ringe sind $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, aber auch die Polynomringe $\mathbb{Z}[X]$, $\mathbb{Q}[X]$, $\mathbb{R}[X]$.

Die Menge $\mathrm{Abb}(\mathbb{R}, \mathbb{R})$ aller Abbildungen $f \colon \mathbb{R} \to \mathbb{R}$ ist, mit punktweiser Verknüpfung, auch ein kommutativer Ring: Für $f, g \in \mathrm{Abb}(\mathbb{R}, \mathbb{R})$ definiert man $f + g$, beziehungsweise fg, durch

$$(f + g)(x) \coloneqq f(x) + g(x) \quad \text{und} \quad (fg)(x) \coloneqq f(x)g(x).$$

Satz 3.14. *Sei $m \in \mathbb{N}$. Mit den Verknüpfungen*

$$\overline{a} + \overline{b} \coloneqq \overline{a + b} \quad \textit{und} \quad \overline{a} \cdot \overline{b} \coloneqq \overline{ab} \quad \textit{für } a, b \in \mathbb{Z},$$

ist $\mathbb{Z}/m\mathbb{Z}$ ein kommutativer Ring mit Nullelement $\overline{0}$ und Einselement $\overline{1}$. Für $a \in \mathbb{Z}$ ist $-\overline{a} = \overline{-a}$.

Beweis. Wir müssen zuerst überprüfen dass $\overline{a + b}$ und $\overline{ab}$ unabhängig von der Wahl der Repräsentanten a, b sind. Seien also $a', b' \in \mathbb{Z}$ mit $\overline{a} = \overline{a'}$ und $\overline{b} = \overline{b'}$. Wir müssen zeigen: $\overline{a + b} = \overline{a' + b'}$ und $\overline{ab} = \overline{a'b'}$. Dies folgt aber unmittelbar aus Satz 3.4.

$\mathbb{Z}/m\mathbb{Z}$ ist eine abelsche Gruppe bezüglich $+$: Seien $\alpha, \beta, \gamma \in \mathbb{Z}/m\mathbb{Z}$. Dann gibt es a, b, $c \in \mathbb{Z}$ mit $\alpha = \overline{a}$, $\beta = \overline{b}$ und $\gamma = \overline{c}$. Es ist

$$\begin{aligned}(\alpha + \beta) + \gamma = (\overline{a} + \overline{b}) + \overline{c} = \overline{(a + b)} + \overline{c} = \overline{(a + b) + c} = \overline{a + (b + c)} \\ = \overline{a} + \overline{(b + c)} = \overline{a} + (\overline{b} + \overline{c}) = \alpha + (\beta + \gamma),\end{aligned}$$

weiters

$$\begin{aligned}\alpha + \beta = \overline{a} + \overline{b} = \overline{a + b} = \overline{b + a} = \overline{b} + \overline{a} = \beta + \alpha, \\ \alpha + \overline{0} = \overline{a} + \overline{0} = \overline{0} + \overline{a} = \overline{0 + a} = \overline{a} = \alpha\end{aligned}$$

und

$$\overline{-a} + \alpha = \alpha + \overline{-a} = \overline{a} + \overline{-a} = \overline{a + (-a)} = \overline{0}.$$

$\mathbb{Z}/m\mathbb{Z}$ ist ein kommutativer Ring: Man überprüft $\alpha(\beta\gamma) = (\alpha\beta)\gamma$, $\alpha\beta = \beta\alpha$ und $\overline{1}\alpha = \alpha\overline{1} = \alpha$ genauso nach wie gerade eben bei der Addition. Schließlich ist

$$\begin{aligned}(\beta+\gamma)\alpha = \alpha(\beta+\gamma) = \overline{a}(\overline{b}+\overline{c}) = \overline{a}\,\overline{b+c} = \overline{a(b+c)} = \overline{ab+ac} = \overline{ab}+\overline{ac}\\ = \overline{a}\,\overline{b}+\overline{a}\,\overline{c} = \alpha\beta+\alpha\gamma = \beta\alpha+\gamma\alpha.\end{aligned}$$

□

Definition 3.15. Man nennt $\mathbb{Z}/m\mathbb{Z}$ mit den Verknüpfungen aus Satz 3.14 den *Restklassenring* von $\mathbb{Z}$ modulo m.

Bemerkung zur Algebra. Sei R ein Ring. Eine Teilmenge $I \subset R$ heißt *Ideal* von R wenn für $a, b \in I$ und $r \in R$ gilt: $0 \in I$, $a+b \in I$, $-a \in I$, $ra \in I$ und $ar \in I$. Aus Lemma 1.4(5) folgt: Für jedes $m \in \mathbb{Z}$ bildet die Menge der Vielfachen von n, geschrieben $m\mathbb{Z} = \{\, mk \mid k \in \mathbb{Z} \,\}$, ein *Ideal* des Rings $\mathbb{Z}$.

Die obige Konstruktion der Restklassenringe $\mathbb{Z}/m\mathbb{Z}$ wird in der Algebra verallgemeinert: Sei R ein [kommutativer] Ring und I ein Ideal von R. Für $a \in R$ definiert man $a+I = \{\, a+x \mid x \in I \,\}$. Dann bildet $R/I = \{\, a+I \mid a \in R \,\}$ in natürlicher Weise einen [kommutativen] Ring, den *Faktorring* (auch genannt *Quotientenring* oder *Restklassenring*). Dabei ist $(a+I)(b+I) := ab+I$ und $(a+I)+(b+I) := (a+b)+I$.

Definition 3.16. Sei R ein Ring.

(1) Ein Element $a \in R$ heißt *Einheit* (oder *invertierbares Element*) von R, wenn es ein $a' \in R$ gibt mit $aa' = a'a = 1$. (Das Element a' ist dann – wie zuvor bei den Gruppen – eindeutig bestimmt, und man schreibt dafür a^{-1}.)

(2) $R^\times \subset R$ sei die Menge aller Einheiten von R.

(3) Ein kommutativer Ring R heißt *Körper* wenn $R \neq \{0\}$ und $R^\times = R \setminus \{0\}$.

(Das heißt, in einem Körper besitzt jedes von 0 verschiedene Element ein Inverses. Weiters schließen wir den degenerierten Fall des Nullrings $\{0\}$ aus.)

Beispiel. Es ist $\mathbb{Z}^\times = \{\pm 1\}$ und $\mathbb{Q}^\times = \mathbb{Q} \setminus \{0\}$. Die rationalen Zahlen $\mathbb{Q}$ bilden einen Körper, $\mathbb{Z}$ nicht.

Bemerkung. Für $x \in R$ gilt stets $0x = 0$. [*Denn:* $0x = (0+0)x = 0x+0x$, woraus durch Subtraktion von $0x$ schließlich $0x = 0$ folgt.] Ist $0 \neq 1$, also insbesondere $R \neq \{0\}$, so gibt es also kein $x \in R$ mit $0x = 1$. Also ist stets $0 \notin R^\times$. In einem Körper sind demnach alle Elemente invertierbar für die das potentiell möglich ist.

Lemma 3.17. *Sei R ein Ring.*

(1) $1 \in R^\times$,

(2) *Sind $a, b \in R^\times$, so ist auch $ab \in R^\times$ und $(ab)^{-1} = b^{-1}a^{-1}$.*

(3) *Ist $a \in R^\times$, so ist auch $a^{-1} \in R^\times$ und $(a^{-1})^{-1} = a$.*

(4) *$R^\times$ ist eine Gruppe mit Verknüpfung $\cdot$ und neutralem Element 1.*

Beweis. (1) Wegen $1 \cdot 1 = 1$ ist $1 \in R^\times$.

(2) Es ist $(ab)b^{-1}a^{-1} = a(bb^{-1})a^{-1} = a \cdot 1 \cdot a^{-1} = aa^{-1} = 1$ und analog $b^{-1}a^{-1}(ab) = 1$.

(3) Wegen $aa^{-1} = a^{-1}a = 1$ ist $a^{-1} \in R^\times$ mit $(a^{-1})^{-1} = a$.

(4) Wir überprüfen die definierenden Eigenschaften einer Gruppe. Es ist $1 \in R^\times$ nach (1). Weil für $a, b \in R^\times$ nach (2) auch $ab \in R^\times$, ergibt die Zuordnungsvorschrift $(a, b) \mapsto ab$ eine Verknüpfung $R^\times \times R^\times \to R^\times$.

Für $a, b, c \in R^\times$ gelten $a(bc) = (ab)c$ und $1a = a1$, weil dies sogar für alle $a, b, c \in R$ gilt. Schließlich ist für $a \in R^\times$ nach (3) auch a^{-1} in $R^\times$ und es gilt $aa^{-1} = a^{-1}a = 1$ nach Definition von a^{-1}. □

Sind $a, a' \in \mathbb{Z}$ mit $\overline{a} = \overline{a'}$, so folgt $\mathrm{ggT}(a, m) = \mathrm{ggT}(a', m)$ nach Satz 3.4(3) . Die Bedingung in folgendem Satz ist also vom Repräsentanten der Restklasse unabhängig.

Satz 3.18. *Sei $m \in \mathbb{N}$. Dann ist*

$$(\mathbb{Z}/m\mathbb{Z})^\times = \{\, \overline{a} \in \mathbb{Z}/m\mathbb{Z} \mid a \in \mathbb{Z} \text{ mit } \mathrm{ggT}(a, m) = 1 \,\}.$$

Beweis. Sei zuerst $a \in \mathbb{Z}$ mit $\mathrm{ggT}(a, m) = 1$. Dann gibt es nach Satz 3.10 ein $x \in \mathbb{Z}$ mit $ax \equiv 1 \mod m$. Das heißt $\overline{a}\,\overline{x} = \overline{1}$, also ist $\overline{a} \in (\mathbb{Z}/m\mathbb{Z})^\times$.

Sei nun $\alpha \in (\mathbb{Z}/m\mathbb{Z})^\times$. Seien weiters $a, x \in \mathbb{Z}$ mit $\alpha = \overline{a}$ und $\alpha^{-1} = \overline{x}$. Wegen $1 = \alpha\alpha^{-1} = \overline{a}\,\overline{x}$ folgt $ax \equiv 1 \mod m$. Also ist die lineare Kongruenz $aX \equiv 1 \mod m$ lösbar. Wieder nach Satz 3.10 gilt deshalb $\mathrm{ggT}(a, m) \mid 1$, also $\mathrm{ggT}(a, m) = 1$. □

Bemerkung. Sei $a \in \mathbb{Z}$ mit $\overline{a} \in (\mathbb{Z}/m\mathbb{Z})^\times$. Nach dem vorangegangenen Beweis erfüllt $b \in \mathbb{Z}$ genau dann $\overline{a}\overline{b} = \overline{1}$, wenn gilt $ab - my = 1$ für ein $y \in \mathbb{Z}$. Ein derartiges Paar $(b, -y)$ lässt sich aufgrund von $\mathrm{ggT}(a, m) = 1$ mit Hilfe des erweiterten euklidischen Algorithmus bestimmen.

Beispiel.
- $(\mathbb{Z}/5\mathbb{Z})^\times = \{\overline{1}, \overline{2}, \overline{3}, \overline{4}\}$ und deshalb ist $\mathbb{Z}/5\mathbb{Z}$ ein Körper (mit 5 Elementen).
- $(\mathbb{Z}/4\mathbb{Z})^\times = \{\overline{1}, \overline{3}\}$. Aber $\overline{2}$ ist eine von $\overline{0}$ verschiedene Nicht-Einheit in $\mathbb{Z}/4\mathbb{Z}$.

Satz 3.19. *Sei $m \in \mathbb{N}$. Der Restklassenring $\mathbb{Z}/m\mathbb{Z}$ ist genau dann ein Körper, wenn $m \in \mathbb{P}$.*

Beweis. Ist $m \in \mathbb{P}$, so ist $\mathrm{ggT}(a, m) = 1$ für alle $a \in [1, m-1]$. Deshalb ist $(\mathbb{Z}/m\mathbb{Z})^\times = \{\overline{1}, \ldots, \overline{m-1}\} = \mathbb{Z}/m\mathbb{Z} \setminus \{\overline{0}\}$. Wegen $m \geq 2$ ist auch $\mathbb{Z}/m\mathbb{Z} \neq \{\overline{0}\}$, und deshalb $\mathbb{Z}/m\mathbb{Z}$ ein Körper.

Angenommen m ist keine Primzahl. Ist $m = 1$ so ist $\mathbb{Z}/m\mathbb{Z} = \{\overline{0}\}$ der Nullring, und deshalb kein Körper. Sei $m > 1$. Dann gibt es ein $1 < a < m$ mit $a \mid m$. Dann ist aber $\mathrm{ggT}(a, m) = a > 1$ und deshalb $\overline{a} \notin (\mathbb{Z}/m\mathbb{Z})^\times$. Wegen $1 < a < m$ ist auch $\overline{a} \neq \overline{0}$, und deshalb $\mathbb{Z}/m\mathbb{Z}$ kein Körper. □

3.2.1 Chinesischer Restsatz für Restklassenringe

Der Chinesische Restsatz besitzt auch eine Formulierung für Restklassenringe.

Satz 3.20. *Seien $n \in \mathbb{N}$, seien $m_1, \ldots, m_n \in \mathbb{N}$ paarweise teilerfremd, und sei $m = m_1 \cdots m_n$. Dann gibt es Bijektionen*

$$\pi\colon \mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/m_1\mathbb{Z} \times \cdots \times \mathbb{Z}/m_n\mathbb{Z}, \quad a + m\mathbb{Z} \mapsto (a + m_1\mathbb{Z}, \ldots, a + m_n\mathbb{Z})$$

und

$$\pi^*\colon (\mathbb{Z}/m\mathbb{Z})^\times \to (\mathbb{Z}/m_1\mathbb{Z})^\times \times \cdots \times (\mathbb{Z}/m_n\mathbb{Z})^\times, \quad a + m\mathbb{Z} \mapsto (a + m_1\mathbb{Z}, \ldots, a + m_n\mathbb{Z})$$

Beweis. Sind $a, a' \in \mathbb{Z}$ mit $a+m\mathbb{Z} = a'+m\mathbb{Z}$, so ist nach Satz 3.5(1) auch $a+m_i\mathbb{Z} = a+m_i\mathbb{Z}$ für alle $i \in [1, n]$. Die Abbildungsvorschrift von π ist also tatsächlich unabhängig vom gewählten Repräsentanten a der Restklasse $a + m\mathbb{Z}$.

Sind $a, b \in \mathbb{Z}$ mit $\pi(a + m\mathbb{Z}) = \pi(b + m\mathbb{Z})$, so gilt $a + m_i\mathbb{Z} = b + m_i\mathbb{Z}$ und deshalb $a \equiv b \mod m_i$ für alle $i \in [1, n]$. Aus der Eindeutigkeitsaussage von Satz 3.11 folgt $a \equiv b \mod m$, also $a + m\mathbb{Z} = b + m\mathbb{Z}$. Das heißt, π ist injektiv.

Sind nun $a_1, \ldots, a_n \in \mathbb{Z}$ beliebig, so existiert nach Satz 3.11 ein $a \in \mathbb{Z}$ mit $a \equiv a_i \mod m_i$ für alle $i \in [1, n]$. Dann ist $\pi(a + m\mathbb{Z}) = (a_1 + m_1\mathbb{Z}, \ldots, a_n + m_n\mathbb{Z})$. Das heißt, π ist surjektiv. [2]

Um die Aussage für π^* zu zeigen, zeigen wir

(1) Für $a + m\mathbb{Z} \in (\mathbb{Z}/m\mathbb{Z})^\times$ gilt: $a + m_i\mathbb{Z} \in (\mathbb{Z}/m_i\mathbb{Z})^\times$ für alle $i \in [1, n]$.

(2) Sind $a_1, \ldots, a_n \in \mathbb{Z}$ mit $a_i + m_i\mathbb{Z} \in (\mathbb{Z}/m_i\mathbb{Z})^\times$ für alle $i \in [1, n]$, so ist

$$\pi^{-1}(a_1 + m_1\mathbb{Z}, \ldots, a_n + m_n\mathbb{Z}) \in (\mathbb{Z}/m\mathbb{Z})^\times.$$

Dann folgt, dass π^* die Einschränkung von π auf $(\mathbb{Z}/m\mathbb{Z})^\times$ mit Bildmenge $(\mathbb{Z}/m_1\mathbb{Z})^\times \times \cdots \times (\mathbb{Z}/m_n\mathbb{Z})^\times$ ist. Aufgrund der Bijektivität von π ist dann auch π^* bijektiv.

(1) Sei $b \in \mathbb{Z}$ mit $b + m\mathbb{Z} = (a + m\mathbb{Z})^{-1}$. Dann ist $ab \equiv 1 \mod m$, also auch $ab \equiv 1 \mod m_i$ für alle $i \in [1, n]$. Das heißt aber $(a + m_i\mathbb{Z})(b + m_i\mathbb{Z}) = ab + m_i\mathbb{Z} = 1 + m_i\mathbb{Z}$.

(2) Für $i \in [1, n]$ sei $b_i \in \mathbb{Z}$ mit $b_i + m_i\mathbb{Z} = (a_i + m\mathbb{Z})^{-1}$. Aufgrund der Surjektivität von π gibt es $a, b \in \mathbb{Z}$ mit $b + m_i\mathbb{Z} = b_i + m_i\mathbb{Z}$ and $a + m_i\mathbb{Z} = a_i + m_i\mathbb{Z}$ für alle $i \in [1, n]$. Dann ist $ab + m_i\mathbb{Z} = (a + m_i\mathbb{Z})(b + m_i\mathbb{Z}) = 1 + m_i\mathbb{Z}$ für alle $i \in [1, n]$, und deshalb, aufgrund der Injektivität von π, auch $(a + m\mathbb{Z})(b + m\mathbb{Z}) = ab + m\mathbb{Z} = 1 + m\mathbb{Z}$. □

Bemerkung zur Algebra. Für $\alpha, \beta \in \mathbb{Z}/m\mathbb{Z}$ gilt auch $\pi(\overline{1}) = (\overline{1}, \ldots, \overline{1})$, $\pi(\alpha+\beta) = \pi(\alpha)+\pi(\beta)$ und $\pi(\alpha\beta) = \pi(\alpha)\pi(\beta)$, wobei die Operationen am kartesischen Produkt koordinatenweise

[2] Man kann auch so argumentieren: π ist injektiv, und wegen $|\mathbb{Z}/m\mathbb{Z}| = m = m_1 \cdots m_n = |\mathbb{Z}/m_1\mathbb{Z} \times \cdots \times \mathbb{Z}/m_n\mathbb{Z}|$ deswegen auch surjektiv.

erklärt sind. Das heißt, π erhält die Ringstruktur. Man sagt π ist ein *Ringhomomorphismus*, bzw., da π bijektiv ist, sogar ein *Ringisomorphismus*.

Genauso gilt für $\alpha, \beta \in (\mathbb{Z}/m\mathbb{Z})^\times$ auch $\pi^*(\alpha\beta) = \pi^*(\alpha)\pi^*(\beta)$. Man sagt π^* ist ein *Gruppenhomomorphismus* (bzw. *Gruppenisomorphismus*).

Man kann allgemein leicht zeigen:

- Sind $R_1, \dots, R_n$ Ringe, so ist $R_1 \times \cdots \times R_n$ mit koordinatenweiser Addition und Multiplikation ein Ring.
- Ist $\pi\colon R \to S$ ein Ringisomorphismus, so ist $\pi|_{R^\times}\colon R^\times \to S^\times$ ein Gruppenisomorphismus.

Damit folgt obige Aussage über π^* unmittelbar aus der über π.

Die Konstruktion von π selbst lässt sich weiters durch Benutzung des *Homomorphiesatzes* (siehe Einführung in die Algebra) vereinfachen.

3.3 Prime Restklassen und die Eulersche Phi-Funktion

Wir wollen uns nun die Einheitengruppe des Restklassenrings $\mathbb{Z}/m\mathbb{Z}$ genauer ansehen.

Definition 3.21. Die *Eulersche Phi-Funktion* $\varphi\colon \mathbb{N} \to \mathbb{N}$ sei definiert durch

$$\varphi(m) = |(\mathbb{Z}/m\mathbb{Z})^\times| = |\{\, a \in [0, m-1] \mid \mathrm{ggT}(a, m) = 1 \,\}|, \qquad \text{für } m \in \mathbb{N}.$$

Ist $p \in \mathbb{P}$, so ist $\mathbb{Z}/p\mathbb{Z}$ ein Körper (Satz 3.19) und deshalb $\varphi(p) = p - 1$. (Für den Randfall $m = 1$ ist $\mathbb{Z}/1\mathbb{Z} = \{\overline{0} = \overline{1}\} = (\mathbb{Z}/1\mathbb{Z})^\times$ und deshalb $\varphi(1) = 1$.)

Satz 3.22 (Euler). *Seien $m \in \mathbb{N}$ und $a \in \mathbb{Z}$ mit $\mathrm{ggT}(a, m) = 1$. Dann ist*

$$a^{\varphi(m)} \equiv 1 \mod m.$$

Beweis. Wegen $\overline{a} \in (\mathbb{Z}/m\mathbb{Z})^\times$ ist die Abbildung

$$\mu_{\overline{a}} : (\mathbb{Z}/m\mathbb{Z})^\times \to (\mathbb{Z}/m\mathbb{Z})^\times,\ \overline{x} \mapsto \overline{a}\,\overline{x}$$

bijektiv (die Abbildungsvorschrift der Umkehrabbildung ist gegeben durch $\overline{x} \mapsto \overline{a}^{-1}\overline{x}$). Insbesondere ist $(\mathbb{Z}/m\mathbb{Z})^\times = \{\, \overline{a}\,\overline{x} : \overline{x} \in (\mathbb{Z}/m\mathbb{Z})^\times \,\}$.

Es gilt also

$$\prod_{\overline{x} \in (\mathbb{Z}/m\mathbb{Z})^\times} \overline{x} = \prod_{\overline{x} \in (\mathbb{Z}/m\mathbb{Z})^\times} \overline{a}\,\overline{x} = \overline{a}^{|(\mathbb{Z}/m\mathbb{Z})^\times|} \prod_{\overline{x} \in (\mathbb{Z}/m\mathbb{Z})^\times} \overline{x} = \overline{a}^{\varphi(m)} \prod_{\overline{x} \in (\mathbb{Z}/m\mathbb{Z})^\times} \overline{x}.$$

Weil $\overline{x}$ invertierbar ist, dürfen wir kürzen und erhalten $\overline{a}^{\varphi(m)} = 1$, also $a^{\varphi(m)} \equiv 1 \mod m$. □

Satz 3.23 (Kleiner Satz von Fermat). *Seien $p \in \mathbb{P}$ und $a \in \mathbb{Z}$ mit $p \nmid a$. Dann ist*

$$a^{p-1} \equiv 1 \mod p.$$

Insbesondere ist $a^p \equiv a \mod p$ für alle $a \in \mathbb{Z}$.

Beweis. Die erste Aussage folgt unmittelbar aus dem vorigen Satz, da $\operatorname{ggT}(a, p) = 1$ genau dann gilt wenn $p \nmid a$ und weiters $\varphi(p) = p - 1$.

Die Aussage „Insbesondere“ folgt für $p \nmid a$ indem man $a^{p-1} \equiv 1 \mod p$ mit a multipliziert. Ist $p \mid a$, so ist $a \equiv 0 \mod p$ und deswegen trivialerweise $a^p \equiv a \mod p$. □

Beispiel.

- Wir berechnen 11^{104} modulo 17. Es ist $\varphi(17) = 16$. Darum ist $11^{104} \equiv 11^{6\cdot 16+8} \equiv 11^8 \mod 17$. Wegen $11^2 \equiv (-6)^2 \equiv 36 \equiv 2 \mod 17$ folgt $11^8 \equiv 2^4 \equiv -1 \mod 17$.
- Der kleine Satz von Fermat kann verwendet werden, um zu zeigen, dass eine Zahl $m \in \mathbb{N}$ keine Primzahl ist: Findet man nämlich ein $a \in \mathbb{N}$ mit $a^{m-1} \not\equiv 1 \mod m$, so kann m nicht prim sein. In der Praxis probiert man kleine a um die Rechnung möglichst einfach zu halten.

  Wir demonstrieren das am Beispiel 119, und berechnen 2^{118} modulo 119. Wir schreiben zuerst 118 in Binärdarstellung: $118 = 2^6 + 2^5 + 2^4 + 2^2 + 2$. Es ist $2^{2^1} \equiv 4 \mod 119$, $2^{2^2} \equiv 16 \mod 119$, $2^{2^3} \equiv 18 \mod 119$, $2^{2^4} \equiv 86 \equiv -33 \mod 119$, $2^{2^5} \equiv 18 \mod 119$, $2^{2^6} \equiv 86 \equiv -33 \mod 119$. Darum ist

  $$2^{118} \equiv -33 \cdot 18 \cdot (-33) \cdot 16 \cdot 4 \equiv 30 \mod 119,$$

  also ist $119 \notin \mathbb{P}$.

Satz 3.24. *Ist $m = p_1^{e_1} \cdots p_r^{e_r}$ mit $p_1 < \cdots < p_r \in \mathbb{P}$ und $e_1, \ldots, e_n \in \mathbb{N}$, so gilt*

$$\varphi(m) = \prod_{i=1}^{r} p_i^{e_i - 1}(p_i - 1).$$

Insbesondere: *Für $p \in \mathbb{P}$ und $e \in \mathbb{N}$ ist $\varphi(p^e) = p^{e-1}(p-1)$.*

Beweis. Aufgrund von Satz 3.20 und der paarweisen Teilerfremdheit von $p_1^{e_1}, \ldots, p_r^{e_r}$ ist

$$\varphi(m) = |(\mathbb{Z}/m\mathbb{Z})^\times)| = |(\mathbb{Z}/p_1^{e_1})^\times \times \cdots \times (\mathbb{Z}/p_r^{e_r}\mathbb{Z})^\times| = \varphi(p_1^{e_1}) \cdots \varphi(p_r^{e_r}).$$

Es genügt also $\varphi(p^e) = p^{e-1}(p-1)$ für $p \in \mathbb{P}$ und $e \in \mathbb{N}$ zu zeigen. Das Intervall $[1, p^e]$ ist ein vollständiges Restsystem modulo p^e. Es gilt

$$M := \{ x \in [1, p^e] \mid \operatorname{ggT}(p^e, x) > 1 \} = \{ x \in [1, p^e] \mid p \mid x \} = \{ pk \mid k \in [1, p^{e-1}] \},$$

und deshalb $\varphi(p^e) = |\mathbb{Z}/p^e\mathbb{Z}| - |M| = p^e - p^{e-1} = p^{e-1}(p-1)$. □

3.4 Anwendungen

3.4.1 Teilbarkeitskriterien

Ist $g \in \mathbb{N}_{\geq 2}$, so besitzt jedes $a \in \mathbb{N}$ eine Darstellung der Form

$$a = \sum_{i=0}^{k} a_i g^i$$

mit $k \in \mathbb{N}_0$ und $a_0, \ldots, a_k \in [0, g-1]$. Dabei sind k und $a_0, \ldots, a_k$ durch a eindeutig bestimmt. Das lässt sich einfach durch sukzessive Division mit Rest beweisen. Allgemeiner betrachten wir im nächsten Abschnitt die g-adische Zifferndarstellung reeller Zahlen.

Satz 3.25. *Seien $g \in \mathbb{N}_{\geq 2}$, $a, d \in \mathbb{N}$ und $a = \sum_{i=0}^{k} a_i g^i$ mit $k \in \mathbb{N}_0$ und $a_0, \ldots, a_k \in \mathbb{Z}$.*

(1) *Ist $d \mid g-1$, so ist $d \mid a$ genau dann wenn $d \mid \sum_{i=0}^{k} a_i$.*

(2) *Ist $d \mid g+1$, so ist $d \mid a$ genau dann wenn $d \mid \sum_{i=0}^{k} (-1)^i a_i$.*

(3) *Ist $d \mid g^n$ für ein $n \in \mathbb{N}_0$, so ist $d \mid a$ genau dann wenn $d \mid \sum_{i=0}^{n-1} a_i g^i$ (mit der Konvention $a_i = 0$ für $i > k$).*

Beweis. (1) und (2): Es ist $g \equiv \varepsilon \mod d$ mit $\varepsilon = 1$ in (1) und $\varepsilon = -1$ in (2). Damit folgt

$$a \equiv \sum_{i=0}^{k} a_i g^i \equiv \sum_{i=0}^{k} \varepsilon^i a_i \mod d.$$

Das heißt, $d \mid a$ genau dann, wenn $d \mid \sum_{i=0}^{k} \varepsilon^i a_i$.

(3) Wegen $d \mid g^i$ für $i \geq n$ ist

$$\sum_{i=0}^{k} a_i g^i \equiv \sum_{i=0}^{n-1} a_i g^i,$$

woraus die Behauptung folgt. □

Beispiel. Sei $g = 10$ und $a = \sum_{i=0}^{k} a_i g^i$ mit $k \in \mathbb{N}_0$ und $a_0, \ldots, a_k \in [0, 9]$ die Dezimaldarstellung einer Zahl a. Dann gelten folgende Teilbarkeitsregeln.

(1) a ist teilbar durch 3 bzw. 9, genau dann wenn die Ziffersumme $\sum_{i=0}^{k} a_i$ durch 3 bzw. 9 teilbar ist (nach (1)).

(2) a ist teilbar durch 11, genau dann wenn die alternierende Ziffersumme $\sum_{i=0}^{k} (-1)^i a_i$ durch 11 teilbar ist (nach (2)).

(3) a ist teilbar durch 2 bzw. 5, genau dann wenn die "Einerziffer" a_0 durch 2 bzw. 5 teilbar ist (nach (3)).

(4) a ist teilbar durch 4, wenn $a_1 10 + a_0$ durch 4 teilbar ist (nach (3)). D.h. um Teilbarkeit durch 4 zu entscheiden müssen nur die letzten beiden Dezimalziffern betrachtet werden. Für ein Teilbarkeitskriterium 8 genügt es, wieder nach (3), die letzten drei Ziffern betrachten.

(5) a ist teilbar durch 6 (bzw. 10), genau dann, wenn a teilbar durch 2 und 3 (bzw. durch 2 und 5) ist. (Nach Satz 3.5(4))

(6) Für 7 gibt es keine ganz so einfache Teilbarkeitsregel. Man kann aber, zum Beispiel, die Regel aus Aufgabe 35 von Übungsblatt 9 sukzessive anwenden.

3.4.2 Kryptographie: Asymmetrische Verschlüsselungsverfahren

Bei symmetrischen ("traditionellen") Verschlüsselungsverfahren müssen zwei Personen, die miteinander vertraulich kommunizieren möchten, zuerst einen gemeinsamen und geheimen Schlüssel vereinbaren. Das ist sehr unpraktisch: Stellen Sie sich vor, eine Bank müsste mit jedem Ihrer Kunden zuerst einen geheimen Schlüssel vereinbaren, bevor vertrauliche Daten ausgetauscht werden können! Möchten n Personen jeweils miteinander kommunizieren, benötigen Sie $\binom{n}{2} \sim n^2$ Schlüssel.

Abhilfe schaffen *asymmetrische Verschlüsselungsverfahren* (*public key cryptography*). Die ersten dieser Verfahren wurden in den 1970ern entwickelt. Sie nutzen aus, dass gewisse zahlentheoretische Probleme keine (bekannte) effiziente Lösung haben. Zum Beispiel, dass es praktisch unmöglich ist die Primfaktorisierung einer natürlichen Zahl zu bestimmen, wenn die Primfaktoren nur groß genug sind.

Das bekannteste Verfahren hier ist das RSA-Verfahren (RSA steht für Rivest–Shamir–Adleman, die Erfinder des Verfahrens die es 1977 publiziert haben). Der Schlüssel teilt sich hier in zwei Teile auf: einen öffentlichen und einen geheimen Teil. Mit dem öffentlichen Teil kann man nur verschlüsseln, mit dem privaten Teil auch entschlüsseln. Somit kann jede der n Personen ihren öffentlichen Schlüssel ohne Bedenken öffentlich verbreiten — zur Kommunikation von n Personen untereinander sind nur n Schlüssel notwendig.

RSA Verfahren

Erzeugung eines Schlüsselpaares.

1. **Wähle zwei große Primzahlen** p, q**.** In der Praxis sollten p, q derzeit ca. 1024–2048 Bits haben, also ca. 300-600 Dezimalstellen. Wegen $\pi(10^{600}) \approx 10^{600}/600\log(10)$ gibt es mehr als 10^{596} solcher Primzahlen.
2. **Setze** $n = pq$**.**
3. **Wähle** $1 < e < \varphi(n) = (p-1)(q-1)$ **mit** $\mathrm{ggT}(e, \varphi(n)) = 1$**.**
4. **Berechne** d **mit** $de \equiv 1 \mod \varphi(n)$**.** (Euklidischer Algorithmus, wir können $0 \leq d \leq \varphi(n)$ annehmen.)

Der öffentliche Schlüssel ist das Paar (n, e). Der geheime Schlüssel ist die Zahl d. Die Zahlen p, q sowie $\varphi(n)$ müssen geheim bleiben, da damit d berechnet werden kann.

Verschlüsselung. Um eine Nachricht M zu verschlüsseln, muss diese zuerst in eine Folge von Zahlen $0 \leq m_i < n$ verwandelt werden (Dezimal- bzw. Binärblöcke). Für jedes solche m_i berechnet man dann $c_i \equiv m_i^e \mod n$. Die Folge der c_i ist jetzt die verschlüsselte Nachricht.

Entschlüsselung. Zur Entschlüsselung berechnet man c_i^d modulo n. Wegen $ed \equiv 1 \mod \varphi(n)$ ist $ed = 1 + k\varphi(n)$ mit $k \in \mathbb{Z}$ (wegen $d, e \geq 1$ sogar $k \in \mathbb{N}$) und deshalb nach dem Satz von Euler,

$$c_i^d \equiv m_i^{ed} \equiv m_i^{1+k\varphi(n)} \equiv m_i \mod n.$$[3]

Hierzu muss man d kennen. Die Sicherheit des Verfahrens beruht darauf, dass d in der Praxis nicht aus n und e berechnet werden kann ohne zusätzlich z.B. p und q zu kennen.

Bemerkung. (1) Um tatsächlich eine sichere Implementation von RSA zu erhalten sind zahlreiche weitere Aspekte zu beachten. Hier kann nur der grundsätzliche Algorithmus skizziert werden.

(2) Wenn Sie eine verschlüsselte Website (HTTPS) besuchen oder Nachrichten per E2E-verschlüsseltem Messenger austauschen, so vereinbart ihr Endgerät mit dem Server (HTTPS) bzw. mit dem anderen Endgerät (E2E) einen geheimen Schlüssel. Damit

[3] Ich schummle hier ein wenig, da der Satz von Euler nur anwendbar ist, wenn $\mathrm{ggT}(m_i, n) = 1$ gilt (d.h. $p \nmid m_i$ und $q \nmid m_i$). Einen vollständigen Beweis erhält man mit Hilfe des Chinesischen Restsatzes, wie folgt. Sei $l \in \{p, q\}$. Ist $l \nmid m_i$, dann gilt $m_i^{l-1} \equiv 1 \mod l$ aufgrund des kleinen Satzes von Fermat, und deshalb $c_i^d \equiv m_i^{1-(p-1)(q-1)k} \equiv m_i \mod l$. Ist $l \mid m_i$, dann gilt $c_i^d \equiv m_i^{ed} \equiv 0 \equiv m_i \mod l$. In jedem Fall ist also $c_i^d \equiv m_i \mod l$ für $l \in \{p, q\}$. Aufgrund der Eindeutigkeitsaussage des Chinesischen Restsatzes, bzw. Satz 3.5(4), und $n = pq$, folgt $c_i^d \equiv m_i \mod n$.

das möglich ist, auch wenn jemand die Verbindung abhört, greift man auch wieder auf Zahlentheorie zurück. Hier wird häufig der *Diffie–Hellman–Schlüsseltausch* Algorithmus benutzt. Dabei nutzt man aus, dass man für $a,\ n, m \in \mathbb{N}$ zwar sehr leicht $a^n \equiv b \mod m$ berechnen kann, dass es aber umgekehrt im allgemeinen für große Zahlen nicht möglich ist aus gegebenem a, b und m, den Exponenten n zu berechnen (*Diskreter-Logarithmus-Problem*).

Basierend auf dem Diskreten Logarithmusproblem gibt es auch Algorithmen für digitale Signaturen (z.B. DSA, Digital Signature Algorithm). In der Praxis arbeitet man hier heutzutage oft nicht mit der Gruppe $(\mathbb{Z}/m\mathbb{Z})^\times$ sondern mit *elliptischen Kurven*. Das erlaubt bei gleicher Sicherheit kürzere Schlüssel und höhere Effizienz.

(3) Sowohl Primfaktorisierungen als auch Diskrete Logarithmen können von Quantencomputern effizient berechnet werden (Algorithmus von Shor). Quantencomputer können derzeit in der Praxis nur mit sehr kleinen Zahlen arbeiten, womit diese Angriffe theoretischer Natur sind. Da die klassischen asymmetrischen Verschlüsselungsverfahren aber anfällig gegen Quantencomputern sind, arbeitet man bereits an Nachfolgern. Stichwort: *post-quantum cryptography*. Auch hier spielt die Zahlentheorie wieder eine ganz zentrale Rolle.

4 g-adische Zifferndarstellung

Bei der *g-adischen Zifferndarstellung* (auch bezeichnet als *Stellenwertsystem zur Basis g*), handelt es sich um eine nützliche Schreibweise für reelle Zahlen als (möglicherweise unendliche) Reihen von Potenzen einer festen Basiszahl $g \in \mathbb{N}_{\geq 2}$. Im Fall $g = 10$ ist dies nichts anderes als das allseits vertraute Dezimalsystem. Wir wiederholen kurz die wesentlichen Eigenschaften dieser Darstellung und wenden uns dann der g-adischen Zifferndarstellung rationaler Zahlen zu. Erst hier kommt die Zahlentheorie zum Zug: Perioden- und Vorperiodenlänge lassen sich zahlentheoretisch ausdrücken.

Ausführlichere Darstellungen findet man in [Bun08, Kapitel 5, §1] und [RU08, Kapitel 4]. Im zweiten Buch wird insbesondere auch auf das Rechnen (Addieren, Multiplizieren) in der g-adischen Zifferndarstellung eingegangen.

Satz & Definition 4.1. Sei $g \in \mathbb{N}_{\geq 2}$. Jedes $x \in \mathbb{R}_{>0}$ besitzt eine Darstellung

$$x = \sum_{i=d}^{\infty} a_i g^{-i}$$

mit $d \in \mathbb{Z}$, $a_i \in [0, g-1]$, $a_d \neq 0$ und unendlich vielen a_i, die von $g-1$ verschieden sind. (Das heißt, zu jedem $j \geq d$ gibt es ein $i \geq j$ mit $a_i \neq g-1$.) Dabei sind d und die Folge $(a_i)_{i \geq d}$ eindeutig bestimmt.

Man nennt $-d$ den *g-adischen Exponenten von x*, $(a_i)_{i \geq d}$ die *g-adische Ziffernfolge* von x und schreibt

$$x = (a_d \dots a_{-1} a_0, a_1 a_2 a_3 \dots)_g \qquad \text{falls } d \leq 0,$$

beziehungsweise

$$x = (0, \underbrace{0 \dots\dots 0}_{d-1 \text{ mal}} a_d a_{d+1} \dots)_g \qquad \text{falls } d > 0.$$

Diese Darstellung heißt *g-adische Zifferndarstellung* von a (oder auch: Zifferndarstellung von a zur Basis g). In den Fällen $g = 10$, $g = 60$, $g = 16$, $g = 8$, $g = 2$ sagt man auch Dezimal-, Sexagesimal-, Hexadezimal, Oktal-, Binärdarstellung.

Bemerkung. (1) Im Fall $g = 10$ verzichtet man üblicherweise auf eine Nennung der Basis, und schreibt einfach $x = a_d \dots a_{-1}a_0, a_1a_2a_3 \dots$ an Stelle von $x = (a_d \dots a_{-1}a_0, a_1a_2a_3 \dots)_{10}$.

(2) Wollen wir Zahlen aus $\mathbb{R}_{<0}$ darstellen, so erreichen wir das durch Hinzufügen eines Vorzeichens „−“. Die 0 lässt sich (eindeutig) darstellen, indem wir alle Ziffern gleich 0 setzen (allerdings gibt es hier keinen g-adischen Exponenten in obigem Sinn).

Dem Beweis von Satz & Definition 4.1 schicken wir noch eine Vorbemerkung und ein Lemma voraus.

Bemerkung. Seien $g \in \mathbb{N}_{\geq 2}$, $d \in \mathbb{Z}$ und $(a_i)_{i\geq d}$ eine Folge in $[0, g-1]$. Für $n \geq d$ ist

$$\sum_{i=d}^{n} |a_i g^{-i}| = \sum_{i=d}^{n} a_i g^{-i} \leq \sum_{i=d}^{n} (g-1) g^{-i} \leq (g-1) \sum_{i=d}^{n} g^{-i}.$$

Bei $\sum_{i=d}^{n} g^{-i}$ handelt es sich um die Partialsummen einer geometrischen Reihe, welche wegen $|g^{-1}| < 1$ konvergiert. Die Reihe $\sum_{i=d}^{\infty} a_i g^{-i}$ ist also nach dem Majorantenkriterium absolut konvergent. Wir erinnern uns weiters:

$$\sum_{i=d}^{\infty} g^{-i} = g^{-d} \frac{1}{1-g^{-1}} = g^{-d} \frac{g}{g-1} = \frac{g^{-(d-1)}}{g-1}.$$

Lemma 4.2 (Kennzeichnungssatz für die g-adische Ziffernentwicklung). *Seien $g \in \mathbb{N}_{\geq 2}$, $x \in \mathbb{R}_{>0}$, $d \in \mathbb{Z}$ und $(a_i)_{i\geq d}$ eine Folge in $[0, g-1]$. Dann sind äquivalent:*

(a) *$-d$ ist g-adischer Exponent und $(a_i)_{i\geq d}$ ist g-adische Ziffernfolge von x.*

(b) *$a_d \neq 0$ und für alle $n \geq d$ ist*

$$\sum_{i=d}^{n} a_i g^{-i} \leq x < \sum_{i=d}^{n} a_i g^{-i} + g^{-n}. \tag{4.1}$$

Beweis. (a) $\Rightarrow$ (b): Die Folge $(\sum_{i=d}^{n} a_i g^{-i})_{n\geq d}$ ist monoton wachsend. Wegen $x = \sum_{i=d}^{\infty} a_i g^{-i}$ folgt deshalb $\sum_{i=d}^{n} a_i g^{-i} \leq x$ für alle $n \geq d$.

Angenommen es gibt ein $n \geq d$ mit $x \geq \sum_{i=d}^{n} a_i g^{-i} + g^{-n}$. Dann ist

$$g^{-n} \leq x - \sum_{i=d}^{n} a_i g^{-i} = \sum_{i=n+1}^{\infty} a_i g^{-i} \leq \sum_{i=n+1}^{\infty} (g-1) g^{-i} = g^{-n}.$$

In obiger Ungleichungskette gilt also durchgehend Gleichheit, und es folgt

$$\sum_{i=n+1}^{\infty} (g - 1 - a_i) g^{-i} = 0.$$

Wegen $g-1-a_i \geq 0$ folgt daraus $a_i = g-1$ für alle $i > n$, im Widerspruch zur Voraussetzung dass unendlich viele der a_i von $g-1$ verschieden sind.

(b) $\Rightarrow$ (a): Aus (4.1) folgt durch Übergang zu den Grenzwerten auf der linken und rechten Seite, wegen $\lim_{n\to\infty} g^{-n} = 0$, unmittelbar

$$x = \sum_{i=d}^{\infty} a_i g^{-i}.$$

Angenommen es gibt ein $j \geq d$, so dass für alle $i > j$ gilt $a_i = g-1$. Dann ist

$$x = \sum_{i=d}^{\infty} a_i g^{-i} = \sum_{i=d}^{j} a_i g^{-i} + \sum_{i=j+1}^{\infty} a_i g^{-i} = \sum_{i=d}^{j} a_i g^{-i} + \sum_{i=j+1}^{\infty} (g-1) g^{-i} = \sum_{i=d}^{j} a_i g^{-i} + g^{-j}.$$

Das widerspricht der strikten Ungleichung in (4.1) für $n = j$. □

Bemerkung. Aus der letzten Rechnung sieht man auch, warum wir stets verlangen, dass unendlich viele g-adische Ziffern $\neq g-1$ sind. Es gäbe sonst Zahlen, die mehr als eine g-adische Zifferndarstellung besitzen. Ist nämlich $(a_i)_{i\geq -d}$ eine Folge in $[0, g-1]$, so dass es ein $j \geq d$ gibt mit $a_j \neq g-1$ und $a_i = g-1$ für alle $i > j$, so folgt

$$x = \sum_{i=-d}^{j} a_i g^{-i} + \sum_{i=j+1}^{\infty} (g-1) g^{-i} = \sum_{i=-d}^{j} a_i g^{-i} + g^{-j} = \sum_{i=-d}^{j-1} a_i g^{-i} + (a_j+1) g^{-j}.$$

Wir hätten also zwei verschiedene Darstellungen für x.

Konkrete Beispiele, für $g = 10$, wären $1 = 1{,}000\ldots = 0{,}999\ldots$ und gleichermaßen $0{,}423000\ldots = 0{,}422999\ldots$

Beweis (von Satz & Definition 4.1). *Existenz:* Sei $x \in \mathbb{R}_{>0}$. Die Folge $(g^{-i})_{i\in\mathbb{Z}}$ ist für $i \longrightarrow \infty$ streng monoton fallend und es gilt $\lim_{i\to\infty} g^{-i} = 0$ und $\lim_{i\to-\infty} g^{-i} = \infty$. Deshalb gibt es ein eindeutig bestimmtes $d \in \mathbb{Z}$ mit $g^{-d} \leq x < g^{-d+1}$. Wir definieren nun eine Folge $(a_i)_{i\geq d}$ rekursiv wie folgt: Es ist

$$g^{-d} = 1g^{-d} < 2g^{-d} < \cdots < (g-1)g^{-d} < gg^{-d} = g^{-d+1}.$$

Deshalb gibt es ein (eindeutig bestimmtes) $a_d \in [1, g-1]$ mit

$$a_d g^{-d} \leq x < (a_d+1) g^{-d}.$$

Sei nun $i > d$ und seien $a_d, \ldots, a_{i-1} \in [0, g-1]$ mit

$$\sum_{j=d}^{i-1} a_j g^{-j} \leq x < \sum_{j=d}^{i-1} a_j g^{-j} + g^{-(i-1)}$$

bereits bestimmt. Dann ist $0 \le \delta_i := x - \sum_{j=d}^{i-1} a_j g^{-j} < g^{-(i-1)}$. Wegen

$$0 = 0g^{-i} < 1g^{-i} < 2g^{-i} < \cdots < (g-1)g^{-i} < gg^{-i} = g^{-(i-1)}$$

gibt es ein (eindeutig bestimmtes) $a_i \in [0, g-1]$ mit $a_i g^{-i} \le \delta_i < (a_i+1)g^{-i}$. Für dieses gilt also

$$\sum_{j=d}^{i} a_j g^{-j} \le x < \sum_{j=d}^{i} a_j g^{-j} + g^{-i}.$$

Nach Lemma 4.2 ist $(a_i)_{i \ge d}$ g-adische Ziffernfolge von x.

Eindeutigkeit: Angenommen $(a_i)_{i \ge d}$ und $(a'_i)_{i \ge d'}$ sind g-adische Ziffernfolgen von x. Aus Lemma 4.2(b) (mit $n = d$) folgt

$$g^{-d} \le a_d g^{-d} \le x < a_d g^{-d} + g^{-d} \le (g-1)g^{-d} + g^{-d} = g^{-d+1}.$$

Also gilt $g^{-d} \le x < g^{-d+1}$ und gleichermaßen $g^{-d'} \le x < g^{-d'+1}$. Daraus folgt $g^{-d} < g^{-d'+1}$ und $g^{-d'} < g^{-d+1}$, woraus $d = d'$ folgt.

Angenommen es gibt nun ein $n \ge d$ mit $a_n \ne a'_n$. Sei dann n minimal mit dieser Eigenschaft. Wir nehmen ohne Einschränkung an $a_n < a'_n$, also $a_n + 1 \le a'_n$. Dann ist

$$\sum_{i=d}^{n} a_i g^{-i} \le x < \sum_{i=d}^{n} a_i g^{-i} + g^{-n} \le \sum_{i=d}^{n} a'_i g^{-i},$$

im Widerspruch zu Lemma 4.2. □

Ist $x \in \mathbb{R}$, so bezeichnet $\lfloor x \rfloor = \max\{ n \in \mathbb{Z} \mid n \le x \}$ die größte ganze Zahl kleiner oder gleich x. Für $x \ge 0$ ist $\{x\} = x - \lfloor x \rfloor$ der *gebrochenen Teil* von x. (Achtung! Die Notation birgt Verwechslungsgefahr mit der einelementigen Menge die x enthält. Was gemeint ist, muss man aus dem Kontext verstehen. Im Folgenden wird $\{x\}$ jedoch stets der gebrochene Teil sein.)

Korollar 4.3. *Seien $g \in \mathbb{N}_{\ge 2}$ und $x \in \mathbb{R}_{\ge 0}$.*

(1) *Es gibt genau ein $a_0 \in \mathbb{N}_0$ und genau eine Folge $(a_i)_{i \ge 1}$ in $[0, g-1]$ mit*

$$x = a_0 + \sum_{i=1}^{\infty} a_i g^{-i} \quad \text{und } a_i \ne g-1 \text{ für unendlich viele } i \ge 1.$$

(2) *Es ist $x \in \mathbb{N}_0$ genau dann, wenn $a_i = 0$ für alle $i \ge 1$.*

(3) *Die Folge $(a_i)_{i \ge 1}$ lässt sich rekursiv berechnen durch $a_0 = \lfloor x \rfloor$, $x_0 = \{x\}$,*

$$a_i = \lfloor g x_{i-1} \rfloor, \quad x_i = \{g x_{i-1}\} \quad \text{für alle } i \ge 1. \tag{4.2}$$

Man nennt $(a_i)_{i\geq 1}$ *die* g-adische Nachkommafolge *von* x.

Beweis. (1) *Existenz:* Für $x \in \mathbb{N}_0$ setzt man $a_0 = x$ und $a_i = 0$ für $i \geq 1$.

Für $x \notin \mathbb{N}_0$ sei $a_0 = \lfloor x \rfloor$. Sei dann $d \in \mathbb{Z}$ und $(a_i)_{i\geq d}$ die g-adische Ziffernentwicklung von $\{x\}$. Wegen $\{x\} < 1$ ist $d \geq 1$. Sei $a_i = 0$ für $i \in [1, d-1]$. Die so konstruierte Folge $(a_i)_{i\geq 0}$ erfüllt die gewünschten Eigenschaften.

Eindeutigkeit: Es ist $0 \leq \sum_{i=1}^{\infty} a_i g^{-i} \leq \sum_{i=1}^{\infty}(g-1)g^{-i} = 1$. Weil unendlich viele der a_i von $g-1$ verschieden sind, folgt aufgrund der Eindeutigkeitsaussage von Satz & Definition 4.1 sogar $0 \leq \sum_{i=1}^{\infty} a_i g^{-i} < 1$. Daraus folgt $a_0 \leq x < a_0 + 1$, also $a_0 = \lfloor x \rfloor$. Deshalb gilt weiter $\sum_{i=1}^{\infty} a_i g^{-i} = \{x\}$.

Ist $x \in \mathbb{N}_0$, so ist $\{x\} = 0$ und deshalb notwendigerweise $a_i = 0$ für alle $i \geq 1$.

Ist $x \notin \mathbb{N}_0$, so ist $\{x\} > 0$ und deshalb gibt es ein $i \geq 1$ mit $a_i \neq 0$. Mit $d = \min\{\, i \in \mathbb{N} \mid a_i \neq 0 \,\}$ ist dann $(a_i)_{i\geq d}$ die g-adische Ziffernfolge von $\{x\}$. Die Eindeutigkeit der Folge $(a_i)_{i\geq 1}$ folgt deshalb aus Satz & Definition 4.1.

(2) Klar nach (1).

(3) Wir zeigen zuerst mittels Induktion nach n:

$$\sum_{i=0}^{n} a_i g^{-i} = x - g^{-n} x_n. \tag{4.3}$$

Für $n = 0$ ist $a_0 = \lfloor x \rfloor = x - \{x\} = x - x_0$. Sei nun $n \geq 1$ und die Aussage gelte für $n-1$. Nach Definition ist $x_n = \{g x_{n-1}\} = g x_{n-1} - \lfloor g x_{n-1} \rfloor = g x_{n-1} - a_n$. Mit Hilfe der Induktionsvoraussetzung folgt

$$\sum_{i=0}^{n} a_i g^{-i} = x - g^{-(n-1)} x_{n-1} + a_n g^{-n} = x - g^{-n}(g x_{n-1} - a_n) = x - g^{-n} x_n.$$

Damit ist Gleichung (4.3) bewiesen. Durch Übergang zum Grenzwert für $n \to \infty$ folgt $x = \sum_{i=0}^{\infty} a_i g^{-i}$. Wegen $0 \leq x_i < 1$ ist stets $0 \leq a_i < g$.

Wir müssen noch zeigen, dass unendlich viele der a_i von $g-1$ verschieden sind. Angenommen, es existiert ein $j \geq 0$, so dass für alle $i > j$ gilt $a_i = g - 1$. Dann ist, nach Gleichung (4.3)

$$x_j = g^j \left(x - \sum_{i=0}^{j} a_i g^{-i} \right) = g^j \sum_{i=j+1}^{\infty} a_i g^{-i} = g^j \sum_{i=j+1}^{\infty} (g-1) g^{-i} = 1,$$

im Widerspruch zu $x_j < 1$. □

4.1 Rationale Zahlen

Definition 4.4. Sei $g \in \mathbb{N}_{\geq 2}$ und $(a_i)_{i\geq 1}$ eine Folge in $[0, g-1]$. Die Folge $(a_i)_{i\geq 1}$ heißt *periodisch* (oder: *schließlich periodisch*) wenn es $k, l \in \mathbb{N}$ gibt mit $a_{i+l} = a_i$ für alle $i \geq k$.

Sei $(a_i)_{i\geq 1}$ eine periodische Folge.

(1) Dann heißt

$$k_0 = \min\{\, k \in \mathbb{N}_0 \mid \text{es gibt ein } l \in \mathbb{N} \text{ mit } a_{i+l} = a_i \text{ für alle } i \geq k+1 \,\}$$

die *Vorperiodenlänge* von $(a_i)_{i\geq 1}$. Ist $k_0 \geq 1$, so heißt $(a_1, \ldots, a_{k_0})$ die *Vorperiode* von $(a_i)_{i\geq 1}$. Ist $k_0 = 0$, so heißt $(a_i)_{i\geq 1}$ *rein periodisch.*

(2) Ist $k_0 \in \mathbb{N}_0$ die Vorperiodenlänge von $(a_i)_{i\geq 1}$, so heißt

$$l_0 = \min\{\, l \in \mathbb{N} \mid a_{i+l} = a_i \text{ für } i \geq k_0 + 1 \,\}$$

die *Periodenlänge* von $(a_i)_{i\geq 1}$ und $(a_{k_0+1}, \ldots, a_{k_0+l_0})$ die *primitive Periode* von $(a_i)_{i\geq 1}$.

Sei $b^* \in \mathbb{N}$ mit $\mathrm{ggT}(b^*, g) = 1$. Dann ist $\overline{g} \in (\mathbb{Z}/b^*\mathbb{Z})^\times$. Betrachtet man die Menge $\{\, \overline{g}^k \in (\mathbb{Z}/b^*\mathbb{Z})^\times : k \in \mathbb{N} \,\}$, so muss es nach dem Schubfachprinzip $1 \leq k < l$ mit $\overline{g}^k = \overline{g}^l$ geben. Wegen der Invertierbarkeit von $\overline{g}$ folgt dann $\overline{g}^{l-k} = \overline{1}$. Es gibt also $n \in \mathbb{N}$ mit $\overline{g}^n = \overline{1}$. Wir definieren

$$\mathrm{ord}_{b^*}(g) := \min\{\, n \in \mathbb{N} \mid \overline{g}^n = \overline{1} \in (\mathbb{Z}/b^*\mathbb{Z})^\times \,\}.$$

Anders ausgedrückt ist $n \in \mathbb{N}$ minimal mit $g^n \equiv 1 \mod b^*$. Die Zahl $\mathrm{ord}_{b^*}(g)$ heißt *multiplikative Ordnung von g modulo* b^*. (In der Algebra ist das die *Ordnung* des Elements $\overline{g}$ in der multiplikativen Gruppe $(\mathbb{Z}/b^*\mathbb{Z})^\times$.)

Ist $g \in \mathbb{N}_{\geq 2}$, so lässt sich $b \in \mathbb{N}$ (in eindeutiger Weise) schreiben als $b = b^* b^{**}$ mit b^*, $b^{**} \in \mathbb{N}$ sodass gilt $\mathrm{ggT}(b^*, g) = 1$ und $b^{**} \mid g^k$ für ein $k \in \mathbb{N}_0$. Dazu wählt man b^* als den größten zu g teilerfremden Teiler von b, und $b^{**} = \frac{b}{b^*}$. Liegt die Primfaktorenzerlegung von b vor, so bedeutet dies nichts anderes, als dass b^* aus all jenen Primfaktoren von b besteht, die g nicht teilen, und b^{**} aus all jenen Primfaktoren, die g teilen.

Satz 4.5. *Sei $g \in \mathbb{N}_{\geq 2}$. Sei $x \in \mathbb{R}_{\geq 0}$, $a_0 = \lfloor x \rfloor$ und $(a_i)_{i\geq 1}$ die g-adische Nachkommafolge von x.*

(1) *$x \in \mathbb{Q}$ genau dann, wenn $(a_i)_{i\geq 1}$ periodisch ist.*

(2) *Sei $x = \frac{a}{b}$ mit $a \in \mathbb{N}_0$, $b \in \mathbb{N}$ und $\mathrm{ggT}(a, b) = 1$. Sei b^* der größte positive, zu g teilerfremde Teiler von b und sei $b^{**} = \frac{b}{b^*}$. Dann ist $\mathrm{ord}_{b^*}(g)$ die Periodenlänge und $\min\{\, k \in \mathbb{N}_0 \mid b^{**} \mid g^k \,\}$ die Vorperiodenlänge von $(a_i)_{i\geq 1}$.*

Beweis. (1) Sei zuerst $x \in \mathbb{Q}$, $x = \frac{a}{b}$ mit $a, b \in \mathbb{N}_0$, und sei $(a_i)_{i\geq 1}$ die g-adische Nachkommafolge von x. Sei $(x_i)_{i\geq 0}$ wie in Korollar 4.3(3). Wegen $x_0 b \in \mathbb{N}_0$ und $x_i = \{g x_{i-1}\} = g x_{i-1} - \lfloor g x_{i-1} \rfloor$ folgt durch Induktion $x_i b \in \mathbb{N}_0$ für alle $i \geq 0$. Wegen $0 \leq x_i < 1$ gilt also $b x_i \in [0, b-1]$. Weil $[0, b-1]$ endlich ist, muss es $k, l \in \mathbb{N}_0$ geben mit $k < l$ und $b x_k = b x_l$. Dann ist natürlich auch $x_k = x_l$. Aus Gleichung (4.2) folgt deshalb $x_{k+i} = x_{l+i}$ für alle $i \in \mathbb{N}_0$. Damit ist $(x_i)_{i\geq 0}$ periodisch, und wegen $a_i = \lfloor g x_i \rfloor$ gilt dasselbe für $(a_i)_{i\geq 1}$.

Sei nun $(a_i)_{i\geq 1}$ periodisch mit Vorperiodenlänge k und Periodenlänge l. Dann ist

$$\begin{aligned}
\{x\} &= \sum_{i=1}^{\infty} a_i g^{-i} = \sum_{i=1}^{k} a_i g^{-i} + \sum_{i=0}^{\infty}\sum_{j=1}^{l} a_{k+il+j} g^{-(k+il+j)} \\
&= \sum_{i=1}^{k} a_i g^{-i} + \sum_{i=0}^{\infty}\sum_{j=1}^{l} a_{k+j} g^{-(k+il+j)} = \sum_{i=1}^{k} a_i g^{-i} + \sum_{j=1}^{l} a_{k+j} g^{-j-k} \sum_{i=0}^{\infty} (g^{-l})^i \\
&= \sum_{i=1}^{k} a_i g^{-i} + \sum_{j=1}^{l} a_{k+j} g^{-j-k} \frac{g^l}{g^l - 1} \\
&= \frac{1}{g^k(g^l-1)} \underbrace{\left(\sum_{i=1}^{k} a_i g^{k-i}(g^l-1) + \sum_{j=1}^{l} a_{k+j} g^{l-j} \right)}_{\in \mathbb{N}_0} \in \mathbb{Q},
\end{aligned} \tag{4.4}$$

und deshalb auch $x = a_0 + \{x\} \in \mathbb{Q}$.

(2) Sei $(a_i)_{i\geq 1}$ periodisch mit Vorperiodenlänge k und Periodenlänge l. Sei weiters $m = \min\{\, t \in \mathbb{N}_0 \mid b^{**} \mid g^t \,\}$ und $n = \mathrm{ord}_{b^*}(g)$. Wir zeigen zuerst $m \leq k$ und $n \leq l$. Nach Gleichung (4.4) ist

$$\frac{a}{b} = \frac{A}{g^k(g^l-1)} \quad \text{mit } A \in \mathbb{N}_0.$$

Wegen $\mathrm{ggT}(a,b) = 1$ folgt $b \mid g^k(g^l-1)$. Daraus folgt nach Wahl von b^* und b^{**} weiter $b^* \mid g^l - 1$ und $b^{**} \mid g^k$, also $m \leq k$. Damit ist $g^l \equiv 1 \mod b^*$ und deshalb $n \leq l$ nach Definition der multiplikativen Ordnung.

Wegen $b^{**} \mid g^m$ und $b^* \mid g^n - 1$ folgt $b = b^* b^{**} \mid g^m(g^n-1)$, und deshalb $\{x\}g^m(g^n - 1) \in \mathbb{N}_0$. Nach Division mit Rest gibt es $q \in \mathbb{N}_0$ und $r \in [0, g^n - 2]$ mit

$$\{x\}g^m(g^n-1) = q(g^n-1) + r. \tag{4.5}$$

Wir schließen aus dieser Gleichung weiters $q < g^m$. Nun schreiben wir q und r mittels der g-adischen Ziffernentwicklung als

$$q = \sum_{i=0}^{m-1} q_{m-i} g^i \quad \text{und} \quad r = \sum_{i=0}^{n-1} r_{n-i} g^i$$

mit $r_1 \ldots, r_n, q_1, \ldots, q_m \in [0, g-1]$. Wegen $r < g^n - 1$ folgt auch, dass es ein $i \in [0, n-1]$ mit $r_i \neq g-1$ gibt.

Einsetzen in (4.5) ergibt

$$\{x\} = qg^{-m} + rg^{-m}(g^n - 1)^{-1} = \sum_{i=0}^{m-1} q_{m-i} g^{i-m} + g^{-m} \sum_{i=0}^{n-1} r_{n-i} g^{i-n} \sum_{j=0}^{\infty} (g^{-n})^j$$
$$= \sum_{i=1}^{m} q_i g^{-i} + g^{-m} \sum_{i=1}^{n} r_i g^{-i} \sum_{j=0}^{\infty} g^{-nj} = \sum_{i=1}^{m} q_i g^{-i} + \sum_{j=0}^{\infty} \sum_{i=1}^{n} r_i g^{-m-nj-i}.$$

Wegen $r_i \neq g-1$ für ein $i \in [1,n]$, handelt es sich hierbei um die g-adische Ziffernentwicklung von $\{x\}$. Wir sehen $a_1 = q_1, \ldots, a_m = q_m$, und $a_{m+i} = r_j$ für $i \in \mathbb{N}$, wenn $j \in [1,m]$ mit $j \equiv i \mod m$ ist.

Wegen $m \leq k$ und $n \leq l$, und der Minimalität von k beziehungsweise l, folgt daraus $m = k$ und $n = l$. □

Definition 4.6. Sei $x \in \mathbb{Q}_{\geq 0}$, $a_0 = \lfloor x \rfloor$, $(a_i)_{i \geq 1}$ die g-adische Nachkommafolge von x, k die Vorperiodenlänge und l die Periodenlänge von $(a_i)_{i \geq 1}$. Dann schreibt man

$$x = (a_0, a_1 \ldots a_k \overline{a_{k+1} \cdots a_{k+l}})_g.$$

Man sagt, die g-adische Ziffernentwicklung von x *bricht ab* wenn $l = 1$ und $a_{k+1} = 0$. In diesem Fall schreibt man

$$x = (a_0, a_1 \ldots a_k)_g.$$

Satz 4.7. *Sei $g \in \mathbb{N}_{\geq 2}$ und sei $x = \frac{a}{b} \in \mathbb{Q}_{\geq 0}$ mit $a \in \mathbb{N}_0$, $b \in \mathbb{N}$ und $\mathrm{ggT}(a,b) = 1$. Die g-adische Ziffernentwicklung von x bricht genau dann ab, wenn $b \mid g^m$ für ein $m \in \mathbb{N}_0$, das heißt, wenn jeder Primfaktor von b in g aufgeht.*

Beweis. Sei $(a_i)_{i \geq 1}$ die Nachkommafolge von x. Die Ziffernentwicklung bricht genau dann ab, wenn es ein $m \in \mathbb{N}_0$ gibt mit

$$\frac{a}{b} = \lfloor x \rfloor + \sum_{i=1}^{m} a_i g^{-i} = g^{-m} \underbrace{\left(g^m \lfloor x \rfloor + \sum_{i=1}^{m} a_i g^{m-i} \right)}_{\in \mathbb{N}_0}.$$

D.h., wenn es ein $m \in \mathbb{N}_0$ und ein $A \in \mathbb{N}_0$ gibt mit

$$\frac{a}{b} = \frac{A}{g^m}.$$

Wegen $\mathrm{ggT}(a,b) = 1$ ist das genau dann der Fall, wenn $b \mid g^m$. □

Literatur

[Bun08] Peter Bundschuh. *Einführung in die Zahlentheorie.* 6., überarbeitete und aktualisierte Auflage. Berlin: Springer, 2008, S. xiv + 336. ISBN: 978-3-540-76490-8/pbk.

[New80] D. J. Newman. "Simple analytic proof of the prime number theorem". In: *Amer. Math. Monthly* 87.9 (1980), S. 693–696. ISSN: 0002-9890.

[RU08] Reinhold Remmert und Peter Ullrich. *Elementare Zahlentheorie.* 3rd ed. Basel: Birkhäuser, 2008, S. 275. ISBN: 978-3-7643-7730-4/pbk.

[Rib11] Paulo Ribenboim. *Die Welt der Primzahlen.* updated. Geheimnisse und Rekorde. [Secrets and records], Translated from the 2004 English original by Jörg Richstein, Updated by Wilfrid Keller. Springer, Heidelberg, 2011, S. xxv+366. ISBN: 978-3-642-18078-1; 978-3-642-18079-8.

[Zag97] D. Zagier. "Newman's short proof of the prime number theorem". In: *Amer. Math. Monthly* 104.8 (1997), S. 705–708. ISSN: 0002-9890.