VO Zahlentheorie

(Modul: “Elementare Algebra” (EAL))

Markus Fulmek

Sommersemester 2015

Dieses Skriptum basiert auf einer Mitschrift [**1**] zur Vorlesung *Zahlentheorie*, die Professor Christoph Baxa im Sommersemester 2008 gehalten hat. Ergänzendes Material habe ich aus dem 50 Jahre älteren Lehrbuch [**2**] von Hardy und Wright hinzugefügt.
Für die Vorlesung sind eigentlich nur sehr wenig Voraussetzungen (abgesehen vom sicheren Beherrschen der Grundrechnungsarten für ganze und rationale Zahlen;-) erforderlich: Aus der Analysis Konvergenzbegriff und die geometrische Reihe, aus der linearen Algebra und Geometrie elementare Kenntnisse über affine Abbildungen (Drehungen, Spiegelungen) sowie Grundbegriffe aus elementarer Mengenlehre und aus Algebra (Gruppen, Ringe, Körper). Ich wiederhole am Beginn des Skriptums einige grundlegende Begriffe (ohne jeden Anspruch auf Vollständigkeit).
Das Skriptum entstand als Vorbereitung für meine Vorlesung im Sommersemester 2015: Es enthält sicher noch immer Fehler und Ungereimtheiten; für alle diesbezüglichen Hinweise bin ich sehr dankbar. Herzlichen Dank für Hinweise auf Fehler, die ich bereits ausgebessert habe, schulde ich

- Herrn Professor Christoph Baxa,
- Herrn Dr. Marko Thiel,
- Herrn Johann Gehringer,
- Herrn Dr. Robin Sulzgruber,
- Herrn Martin Zehetbauer,
- Herrn Edwin Glassner.

Markus Fulmek, 10. Juni 2015.

Inhaltsverzeichnis

KAPITEL 1

Teilbarkeit im Ring der ganzen Zahlen

1.1. Einige grundlegende Begriffe vorweg

Die Zahlentheorie, die wir hier betrachten, beschäftigt sich mit den Eigenschaften der ganzen Zahlen $\mathbb{Z} = \{\dots, -3, -2, -1, 0, 1, 2, \dots\}$, der rationalen Zahlen $\mathbb{Q}$ und der reellen Zahlen $\mathbb{R}$ (mit einem deutlichen Schwergewicht auf den *ganzen Zahlen*).
Wir brauchen für das folgende einige grundlegende Begriffe aus Mengenlehre und (elementarer) Algebra sowie bekannte Tatsachen über reelle, rationale und ganze Zahlen, die wir hier (kurz und keineswegs vollständig!) wiederholen.

1.1.1. Die ganzen Zahlen als Teilmenge der reellen Zahlen. Man kann sich die ganzen Zahlen geometrisch vorstellen als Punkte auf einer Geraden, die von einem fest gewählten Punkt 0 durch Schritte (nach links oder rechts) einer festgelegten Länge 1 erreicht werden können, siehe Abbildung 1.
Wie üblich bezeichnen wir die Menge der ganzen Zahlen mit $\mathbb{Z}$, die Menge der rationalen Zahlen mit $\mathbb{Q}$ und die Menge der reellen Zahlen mit $\mathbb{R}$. Die Menge der natürlichen Zahlen $\{1, 2, 3, \dots\}$ bezeichnen wir mit $\mathbb{N}$, und die Menge der nicht–negativen ganzen Zahlen $\{0, 1, 2, \dots\} = \mathbb{N} \cup \{0\}$ bezeichnen wir mit $\mathbb{N}_0$.
Für die ersten n natürlichen Zahlen verwende ich das Symbol $[n]$, also

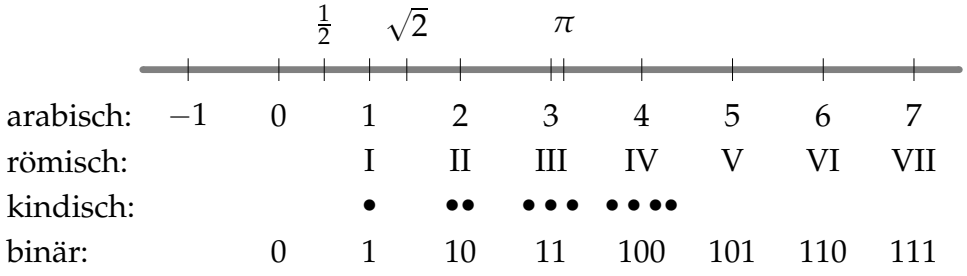
$$[n] := \{1, 2, \dots, n\}.$$

1.1.2. Relationen.

DEFINITION 1.1.1 (Relation, partielle Ordnung, Totalordnung, Wohlordnung). *Sei S eine Menge: Eine* Relation *R auf S ist (ganz abstrakt) eine Teilmenge des cartesischen Produkts, also*

$$R \subseteq S \times S.$$

ABBILDUNG 1. Illustration: Die ganzen Zahlen und verschiedene Arten, sie zu bezeichnen.



Normalerweise beschreibt man aber R (etwas konkreter) durch ein "zweistelliges Symbol", z.B. "$\sim$", mit der Bedeutung

$$x \sim y :\Longleftrightarrow (x,y) \in R : \text{ "}x \text{ steht in Relation } R \text{ zu } y\text{"}.$$

Eine Relation, die wir typischerweise mit dem Symbol $\preceq$ bezeichnen, heißt Halbordnung *oder* partielle Ordnung *auf S, wenn sie die folgenden drei Eigenschaften hat:*

Reflexivität: $s \preceq s$ *für alle* $s \in S$,
Antisymmetrie: $s_1 \preceq s_2$ *und* $s_2 \preceq s_1 \implies s_1 = s_2$,
Transitivität: $s_1 \preceq s_2$ *und* $s_2 \preceq s_3 \implies s_1 \preceq s_3$ *für alle* $s_1, s_2, s_3 \in S$.

Wenn $x \preceq y$, aber $x \neq y$, schreiben wir auch $x \prec y$.
Sei $T \subseteq S$: Ein Element $m \in T$ mit der Eigenschaft

$$(s \preceq m \implies s = m \text{ oder } s \notin T \text{ für alle } s \in S) \iff \nexists t \in T : \ t \prec m$$

heißt minimales Element *von T.*
Eine Halbordnung $\preceq$ heißt Totalordnung, *wenn für je zwei Elemente $s_1, s_2 \in S$ gilt*

$$s_1 \preceq s_2 \text{ oder } s_2 \preceq s_1$$

(d.h.: Je zwei Elemente sind vergleichbar).
Eine Totalordnung heißt Wohlordnung, *wenn jede Teilmenge $T \subseteq S$ ein* Minimum *m hat, also ein Element m mit der Eigenschaft*

$$m \preceq t \text{ für alle } t \in T.$$

(Wegen Antisymmetrie ist ein solches minimales Element immer eindeutig.)

BEISPIEL 1.1.2. *Für $n \in \mathbb{N}$ ist die* Potenzmenge $2^{[n]}$ *(also die Familie aller Teilmengen von $[n]$) partiell geordnet durch die Mengeninklusion $\subseteq$; dies ist aber keine Totalordnung.*
Die Standardordnung $\leqslant$ ist auf $\mathbb{N}$ eine Wohlordnung, aber nicht auf $\mathbb{Z}$, denn es gibt z.B. kein minimales Element für ganz $\mathbb{Z}$. Natürlich hat aber jede nicht–leere *Teilmenge $A \subseteq \mathbb{Z}$, $A \neq \emptyset$, die nach oben (unten) beschränkt ist, ein größtes (kleinstes) Element.*

DEFINITION 1.1.3. *Auf $\mathbb{R}$ (und damit auch auf $\mathbb{Z}$) betrachten wir die "übliche" Ordnung $\leqslant$. Dies ist eine Totalordnung, die mit der Addition und der Multiplikation in folgendem Sinn verträglich ist:*

$$\begin{aligned} x \geqslant y &\iff x + z \geqslant y + z \text{ für alle } x, y, z \in \mathbb{R}, \\ x \geqslant y &\iff x \cdot z \geqslant y \cdot z \text{ für alle } x, y, z \in \mathbb{R}, z > 0, \\ x \geqslant y &\iff x \cdot z \leqslant y \cdot z \text{ für alle } x, y, z \in \mathbb{R}, z < 0. \end{aligned}$$

Wie üblich, nennen wir eine reelle Zahl x

- *positiv, wenn $x > 0$,*
- *nicht–negativ, wenn $x \geqslant 0$,*
- *nicht–positiv, wenn $x \leqslant 0$,*
- *negativ, wenn $x < 0$.*

Den Absolutbetrag *von x bezeichnen wir mit $|x|$:*

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

DEFINITION 1.1.4 (Äquivalenzrelation). *Sei S eine Menge: Eine Relation, die wir typischerweise mit dem Symbol $\simeq$ bezeichnen, heißt* Äquivalenzrelation *auf S, wenn sie die folgenden drei Eigenschaften hat:*

Reflexivität: $s \simeq s$ *für alle* $s \in S$,
Symmetrie: $s_1 \simeq s_2 \iff s_2 \simeq s_1$,
Transitivität: $s_1 \simeq s_2$ *und* $s_2 \simeq s_3 \implies s_1 \simeq s_3$ *für alle* $s_1, s_2, s_3 \in S$.

Sei $s \in S$: Die Menge

$$\left\{s' \in S \colon\ s' \simeq s\right\}$$

heißt die Äquivalenzklasse *von s; wir bezeichnen sie typischerweise mit $\overline{s}$.*

DEFINITION 1.1.5 (Partition). *Sei S eine Menge. Eine Familie von Teilmengen $S_i \subseteq S$*

$$\{S_i \colon\ i \in I\},$$

die mit Indices aus einer Menge I bezeichnet seien, heißt Partition *von S, wenn gilt:*

- $S = \bigcup_{i \in I} S_i$,
- $i \neq j \in I \implies S_i \cap S_j = \emptyset$,
- $S_i \neq \emptyset$ *für alle* $i \in I$.

Die Teilmengen S_i werden in diesem Zusammenhang auch als Blöcke *der Partition bezeichnet.*
Die ersten beiden Bedingungen bedeuten, daß S eine disjunkte Vereinigung *aller Blöcke S_i, $i \in I$, ist: Das kürzen wir ab mit*

$$S = \dot{\bigcup}_{i \in I} S_i.$$

Ein Repräsentantensystem *(oder eine* Transversale*) $\mathcal{R}$ einer Partition $\{S_i \colon\ i \in I\}$ von S ist eine Teilmenge von S, die aus jedem Block S_i* genau ein *Element (einen sogenannten* Repräsentanten *von S_i) enthält.*

BEOBACHTUNG 1.1.6. *Bezeichne $\simeq$ eine Äquivalenzrelation auf einer Menge S: Dann ist die* Menge aller Äquivalenzklassen

$$\{\overline{s} \colon\ s \in S\}$$

eine Partition *von S.*
Umgekehrt ist durch eine beliebige Partition

$$S = \bigcup_{i \in I} S_i$$

von S eine Äquivalenzrelation gegeben, und zwar durch

$$s \simeq s' :\iff s, s' \text{ gehören zum selben Block } S_i.$$

Aufgabe 1: *Betrachte folgende Partition der Menge* $[9] = \{1,2,3,4,5,6,7,8,9\} \subset \mathbb{N}$*:*

$$[9] = \{1,4,7\} \dot{\cup} \{2,5,8\} \dot{\cup} \{3,6,9\}.$$

Gib ein Repräsentantensystem für diese Partition an und versuche die Äquivalenzrelation "kompakt" zu beschreiben, die diese Blöcke als Äquivalenzklassen hat.

Hinweis: Betrachte die Differenzen von zwei beliebigen Elementen, die in einem Block liegen.

1.1.3. Elementare Algebra.

DEFINITION 1.1.7. *Sei S eine Menge, auf der eine* zweistellige Verknüpfung *gegeben ist, das ist eine Funktion*

$$f\colon\ S \times S \to S,$$

die meist mit einem Symbol wie "$+$" oder "$\cdot$" bezeichnet wird (aber auch mit $\times, \oplus, \otimes, \cdot$) in dem Sinne, daß nicht $f(s_0, s_1)$ geschrieben wird, sondern $s_0 + s_1$ oder $s_0 \cdot s_1$ (aber auch $s_0 \times s_1$, $s_0 \oplus s_1$, $s_0 \otimes s_1$ — je nachdem, welches Symbol für die Verknüpfung verwendet wird).
Sei also S eine Menge mit der zweistelligen Verknüpfung "$\cdot$", und sei $X \subseteq S$ eine Teilmenge von S und $s \in S$ ein Element in S. Dann bezeichnet

$$s \cdot X := \{s \cdot x\colon\ x \in X\}$$

bzw.

$$X \cdot s := \{x \cdot s\colon\ x \in X\}$$

Sei $Y \subseteq S$ eine weitere Teilmenge von S. Dann bezeichnet

$$X \cdot Y := \{x \cdot y\colon\ x \in X \text{ und } y \in Y\}.$$

BEISPIEL 1.1.8. *Wenn wir die Menge $\mathbb{Z}$ der ganzen Zahlen mit der (gewöhnlichen) Multiplikation $\cdot$ als zweistelliger Verknüpfung betrachten, dann ist z.B. $2 \cdot \mathbb{Z}$ die Menge der geraden Zahlen.*

Aufgabe 2: *Seien $A := \{-1, 2, -4\}$ und $B := \{-1, -2\}$ zwei Teilmengen ganzer Zahlen, also $A \subset \mathbb{Z}$ und $B \subset \mathbb{Z}$. Betrachte die "ganz normalen" zweistelligen Verknüpfungen $+$ (Addition) und $\cdot$ (Multiplikation) auf $\mathbb{Z}$ und bilde die Mengen $A + 2 \cdot B$ und $2 + A \cdot B$.*

DEFINITION 1.1.9 (Halbgruppe, Gruppe). *Eine* Halbgruppe *ist ein Paar $(G, \odot)$, bestehend aus einer Menge G und einer zweistelligen Verknüpfung $\odot$ auf G mit folgender Eigenschaft:*

- *Für alle $a, b, c \in G$ gilt: $(a \odot b) \odot c = a \odot (b \odot c)$. (Assoziativität.)*

*Die (Halb–)*Gruppenoperation $\odot$ *bestimmt also eine Abbildung $G \times G \to G$ durch $(a, b) \mapsto a \odot b$.*
Eine Halbgruppe $(G, \odot)$ heißt Gruppe, *wenn darüber hinaus gilt:*

- *Es gibt ein* neutrales Element $\mathbb{n} \in G$, *sodaß für alle $a \in G$ gilt: $a \odot \mathbb{n} = \mathbb{n} \odot a = a$. (Existenz eines neutralen Elements.)*
- *Für alle $a \in G$ existiert ein* inverses Element $a^{-1} \in G$ *mit $a \odot a^{-1} = a^{-1} \odot a = \mathbb{n}$. (Existenz eines inversen Elements.)*

Die Anzahl der Elemente von G wird auch als die Ordnung *der Gruppe G bezeichnet und mit* ord G *abgekürzt: Eine Gruppe G mit* ord $G < \infty$ *heißt* endliche Gruppe.
Eine Gruppe $(G, \odot)$ heißt abelsch *oder* kommutativ, *wenn zusätzlich gilt:*

- *Für alle $a, b \in G$ gilt $a \odot b = b \odot a$. (Kommutativität.)*

Das Symbol $\odot$ für die Gruppenoperation ist natürlich nicht das einzig mögliche: Oft schreibt man auch "$\cdot$" oder "$\circ$" (*multiplikative Schreibweise*; dann verwendet man anstelle des Symbols "$\mathbb{n}$" auch **1**), aber auch "$+$" oder "$\oplus$" (*additive Schreibweise*; dann verwendet man anstelle des Symbols "$\mathbb{n}$" auch **0** und schreibt $-a$ statt a^{-1} für das inverse Element).

BEISPIEL 1.1.10. *Die Menge* $\mathbb{Q}\setminus\{0\}$ *aller rationalen Zahlen ohne* 0 *bildet mit der Multiplikation eine (kommutative) Gruppe; ihr neutrales Element ist die rationale Zahl* 1. *Die Menge* $\mathbb{Q}$ *bildet mit der Addition eine (kommutative) Gruppe; ihr neutrales Element ist die rationale Zahl* 0.

DEFINITION 1.1.11 (Untergruppe). *Eine nichtleere Teilmenge* $U \subseteq G$ *bildet eine* Untergruppe $(U, \odot)$ *von* $(G, \odot)$*, wenn gilt:*

- $a, b \in U \implies a \odot b \in U$ *(Abgeschlossenheit bezüglich* $\odot$*; also* $U \odot U \subseteq U$*.)*
- $a \in U \implies a^{-1} \in U$ *(Abgeschlossenheit bezüglich Inversenbildung.)*

Wir schreiben dann $U \sqsubseteq G$*, und es gilt äquivalent das einfache* Untergruppenkriterium*:*

$$U \sqsubseteq G :\Longleftrightarrow \left(a, b \in U \implies a \odot b^{-1} \in U\right). \tag{1.1}$$

DEFINITION 1.1.12 (Ring, Nullteiler). *Ein* Ring *ist ein Tripel* $(R, \oplus, \odot)$ *bestehend aus einer Menge R und zwei zweistelligen Verknüpfungen* $\oplus$ *(Addition) und* $\odot$ *(Multiplikation) auf R mit folgenden Eigenschaften:*

- $(R, \oplus)$ *ist eine abelsche Gruppe,*
- $(R, \odot)$ *ist eine Halbgruppe (d.h., die Multiplikation ist* assoziativ*),*
- *für alle* $a, b, c \in R$ *gilt* $a \odot (b \oplus c) = a \odot b \oplus a \odot c$ *und* $(a \oplus b) \odot c = a \odot c \oplus b \odot c$ *(*Distributivität*.)*

Das neutrale Element $\mathtt{n}$ *von* $(R, \oplus)$ *heißt* Nullelement *des Rings R; in der Regel wird dafür das Symbol* $\mathbf{0}$ *verwendet. (Der triviale Fall, daß R* nur *aus dem Nullelement besteht, wird als* Nullring *bezeichnet*[1]*.)*

Ein Ring R heißt kommutativ*, falls die Multiplikation kommutativ ist, also wenn für alle* $a, b \in R$ *gilt:* $a \odot b = b \odot a$*. Ein Ring muß keineswegs kommutativ sein: Wenn man das betonen möchte, spricht man von einem* nichtkommutativen *Ring. Wenn die Halbgruppe* $(R, \odot)$ *ein neutrales Element besitzt, heißt R ein* Ring mit Eins *oder ein* unitärer Ring*. Dieses neutrale Element heißt dann das* Einselement *des Rings; in der Regel wird dafür das Symbol* $\mathbf{1}$ *verwendet. In einem unitären Ring R ist die Menge der (multiplikativ) invertierbaren Elemente*

$$R^\star := \left\{a \in R\colon\ \exists a^{-1} \in R \text{ mit } a \cdot a^{-1} = a^{-1} \cdot a = \mathbf{1}\right\}$$

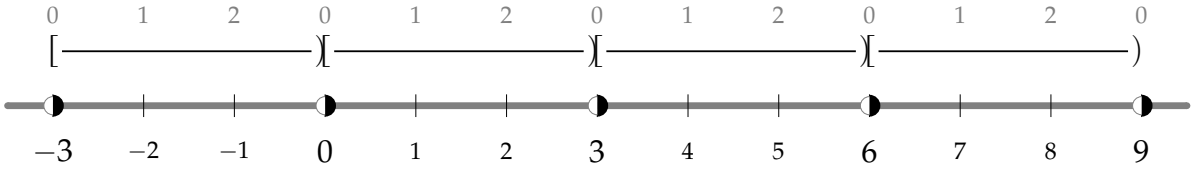
nicht leer (denn $\mathbf{1} \in R^\star$*): Diese invertierbaren Elemente heißen* Einheiten *des Rings; mit der Multiplikation in R ist* $R^\star$ *eine Gruppe, die sogenannte* Einheitengruppe *von R.*

Zwei Elemente $a, b \in R\setminus\{\mathbf{0}\}$ *mit der Eigenschaft* $a \odot b = \mathbf{0}$ *heißen* Nullteiler*. Ein Ring, der keine Nullteiler enthält, heißt* nullteilerfrei*. Ein kommutativer nullteilerfreier Ring mit Eins heißt* Integritätsbereich *oder* Integritätsring*.*

BEISPIEL 1.1.13. $\mathbb{Z}$ *ist ein Integritätsbereich mit Einheitengruppe* $\{1, -1\} \simeq \mathbb{Z}_2$*.*

[1] Für unsere Zwecke ist der Nullring uninteressant: Er spielt nur für sehr abstrakte (kategorientheoretische) Betrachtungen eine Rolle.

ABBILDUNG 2. Illustration: Division mit Rest durch 3.



DEFINITION 1.1.14 (Schiefkörper, Körper). *Ein unitärer Ring* $(R, \oplus, \odot)$ *mit der zusätzlichen Eigenschaft, daß* $(R \setminus \{\mathbf{0}\}, \odot)$ *eine* Gruppe *ist, heißt ein* Schiefkörper *oder* Divisionsring. *Wenn diese* multiplikative Gruppe *zusätzlich* abelsch *(*kommutativ*) ist (also wenn* R *ein* kommutativer *Ring mit Eins ist), dann heißt* R *ein* Körper. *Für einen Körper verwenden wir meist die Symbole* $\mathbb{K}$ *oder* $\mathbb{F}$ *(Körper heißt auf Englisch* Field*), manchmal auch* $\mathbb{L}$*, und die (multiplikative) Einheitengruppe eines Körpers* $\mathbb{K}$ *bezeichnen wir mit* $\mathbb{K}^\star = (\mathbb{K} \setminus \{\mathbf{0}\}, \odot)$

BEISPIEL 1.1.15. $\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{F}_p \simeq \mathbb{Z}_p$

Da Algebra hier nicht unser Thema ist, halten wir zunächst einfach nur fest:

- Die Menge der ganzen Zahlen bildet mit den Verknüpfungen
  - Addition, die wir (wie üblich) mit "$+$" bezeichnen,
  - und Multiplikation, die wir (wie üblich) mit "$\cdot$" bezeichnen,

  einen *kommutativen* Ring mit 1 (d.h., es gilt[2] $a \cdot b = b \cdot a$ für alle $a, b \in \mathbb{Z}$, und es gilt $a \cdot 1 = 1 \cdot a = a$ für alle $a \in \mathbb{Z}$).
- $\mathbb{Z}$ ist *nullteilerfrei*, d.h.: $a \cdot b = 0 \implies a = 0$ oder $b = 0$. Ein nullteilerfreier kommutativer Ring mit 1 heißt auch *Integritätsbereich*: $\mathbb{Z}$ ist also ein Integritätsbereich. Insbesondere gilt in $\mathbb{Z}$: Aus $a \cdot x = b \cdot x$ und $x \neq 0$ folgt $a = b$.

Abstrakte Algebra ist aber *sehr nützlich* und macht viele Argumente einfacher und durchsichtiger (wenn man sich einmal an die Abstraktheit gewöhnt hat;-).

1.2. Division mit Rest

Der folgende Satz ist *grundlegend* für unsere weiteren Überlegungen:

SATZ 1.2.1 (Division mit Rest). *Seien* $n, d \in \mathbb{Z}, d \neq 0$*. Dann gibt es* eindeutig bestimmte *Zahlen* $q, r \in \mathbb{Z}$*, sodaß*

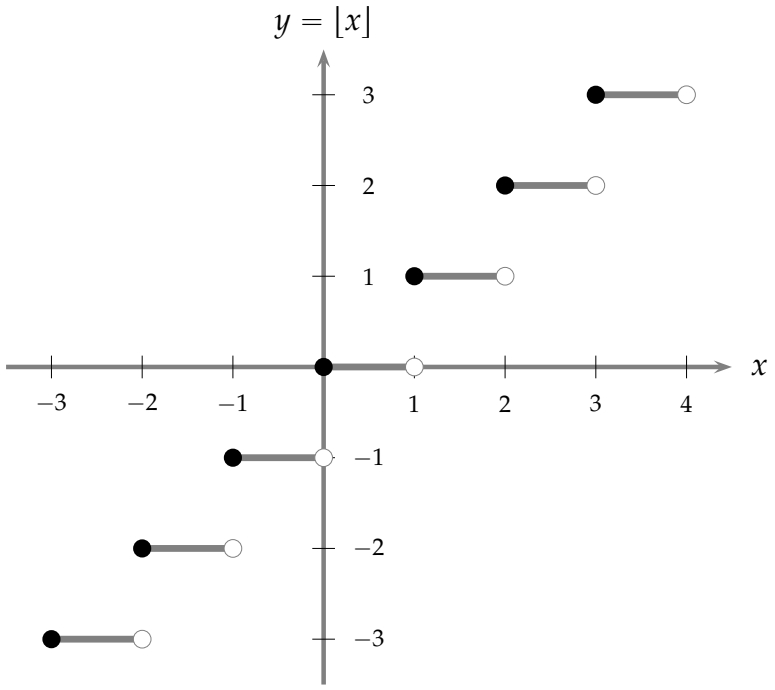
$$n = q \cdot d + r \text{ mit } 0 \leqslant r < |d|. \tag{1.2}$$

Wenn man sich die Zahlen "geometrisch" vorstellt (vergleiche Abbildung 1), dann ist diese Aussage offensichtlich: Die Menge der *Vielfachen* von d,

$$\{k \cdot d : \ k \in \mathbb{Z}\} = \{\dots, -2 \cdot d, -1 \cdot d, 0, 1 \cdot d, 2 \cdot d, 3 \cdot d, \dots\}$$

[2] Die Addition ist auch kommutativ, also $a + b = b + a$ für alle $a, b \in \mathbb{Z}$: Aber das ist bei allen Ringen so und wird daher nicht "extra erwähnt"; es *gibt* aber Ringe mit nicht–kommutativer Multiplikation.

ABBILDUNG 3. Illustration: Graph der Funktion $x \mapsto \lfloor x \rfloor$.



bildet einen "Raster", sodaß jede ganze Zahl n in einem (eindeutigen) "Intervall" liegt:

$$n \in \{q \cdot d, q \cdot d + 1, \ldots, q \cdot d + (|d| - 1)\} \text{ für ein } q \in \mathbb{Z},$$

und das heißt natürlich, daß n in der Form (1.2) dargestellt werden kann (Abbildung 2 illustriert diesen Gedanken für $d = 3$).
Wir geben aber noch einen "formaleren" Beweis für Satz 1.2.1.

DEFINITION 1.2.2 (Nächstkleinere ganze Zahl). *Für $x \in \mathbb{R}$ bezeichne $\lfloor x \rfloor$ die* nächstkleinere ganze Zahl *an x (oft auch* Gaußklammer *von x genannt und mit $[x]$ bezeichnet), die wie folgt definiert ist:*

$$\lfloor x \rfloor := \max \{k \in \mathbb{Z} \colon \ k \leqslant x\}.$$

Abbildung 3 zeigt (ausschnittsweise) den Graphen der Funktion $\lfloor x \rfloor \colon \ \mathbb{R} \to \mathbb{R}$.

BEMERKUNG 1.2.3. *Es gilt offensichtlich*

$$\lfloor x \rfloor \leqslant x < \lfloor x \rfloor + 1 \text{ für alle } x \in \mathbb{R}. \tag{1.3}$$

Es ist aber i.a. nicht $\lfloor -x \rfloor = -\lfloor x \rfloor$*: Z.B. ist* $\left\lfloor \frac{5}{2} \right\rfloor = \left\lfloor 2 + \frac{1}{2} \right\rfloor = 2$, *aber* $\left\lfloor -\frac{5}{2} \right\rfloor = \left\lfloor -3 + \frac{1}{2} \right\rfloor = -3$.

Aufgabe 3: *Seien $m, n \in \mathbb{N}$. Wieviele Vielfache von m (also Zahlen der Gestalt $k \cdot m$ mit $k \in \mathbb{Z}$) gibt es in der Menge der Zahlen $[n] := \{1, 2, \ldots, n\}$?*

BEWEIS VON SATZ 1.2.1. Sei $q = \left\lfloor \frac{n}{d} \right\rfloor$. Dann gilt gemäß (1.3)

$$q \leqslant \frac{n}{d} < q + 1. \tag{1.4}$$

Falls $q \cdot d = n$, dann ist

$$n = q \cdot d + 0$$

offensichtlich eine Darstellung entsprechend (1.2) (mit $r = 0$), und diese Darstellung ist *eindeutig*. Denn sei

$$n = q' \cdot d + r'$$

eine *andere* derartige Darstellung, dann gilt für $\lambda := q - q'$:

$$n = \underbrace{(q - \lambda)}_{q'} \cdot d + \underbrace{\lambda \cdot d}_{r'};$$

aber $|r'| \geqslant |d|$ für $\lambda \neq 0$.

Andernfalls ist $\frac{n}{d} > q$, und wir unterscheiden hier die Fälle $d > 0$ und $d < 0$: Für $d > 0$ ist (1.4) nun äquivalent mit

$$q \cdot d < n < q \cdot d + d \iff 0 < n - q \cdot d < d = |d|;$$

und für $r := n - q \cdot d$ gilt dann:

$$n = q \cdot d + r \text{ mit } 0 < r < |d|.$$

Für $d < 0$ ist (1.4) nun äquivalent mit

$$q \cdot d > n > q \cdot d + d \iff |d| = -d > n - q \cdot d - d > 0;$$

und für $r := n - (q + 1) \cdot d$ gilt dann wieder, wie behauptet:

$$n = (q + 1) \cdot d + r \text{ mit } 0 < r < |d|.$$

Und wenn solche Darstellungen von n schon gegeben sind, so gilt natürlich

$$\text{für } d > 0 : q \cdot d < n < q \cdot d + d \iff q < \frac{n}{d} < q + 1,$$
$$\text{für } d < 0 : (q + 1) \cdot d < n < q \cdot d \iff q < \frac{n}{d} < q + 1.$$

Und das heißt $q = \left\lfloor \frac{n}{d} \right\rfloor$: Die Zahlen q und r sind also auch hier *eindeutig*. □

1.3. Teilbarkeit

DEFINITION 1.3.1 (Teilbarkeit in $\mathbb{Z}$). *Seien $d, n \in \mathbb{Z}$: Wir sagen "d teilt n", wenn es eine Zahl $k \in \mathbb{Z}$ gibt sodaß $n = k \cdot d$, und schreiben dafür $d \mid n$. Klarerweise ist dann auch $k = \frac{n}{d}$ ein Teiler von n: Man nennt k dann den* Komplementärteiler *des Teilers d von n.*

Wenn $d \mid n$ gilt, dann sagen wir auch (äquivalent)

- *d ist ein* Teiler *von n,*
- *n ist ein* Vielfaches *von d.*

Jede Zahl $n \in \mathbb{Z}$ ist immer durch ± 1 und durch $\pm n$ teilbar:

$$n = 1 \cdot n = (-1) \cdot (-n) .$$

Die Menge der Teiler von $n \in \mathbb{Z}$ ist also niemals leer, weil sie immer die trivialen Teiler *± 1 und $\pm n$ enthält. Wenn n noch weitere Teiler hat, so heißen diese* echte Teiler *von n.*

BEMERKUNG 1.3.2. *Teilbarkeit ist* nur für ganze Zahlen *interessant: Für rationale oder reelle Zahlen z und $d \neq 0$ gibt es ja* immer *ein q mit $z = d \cdot q$.*
Ich erwähne diese Selbstverständlichkeit hier, weil ich immer wieder folgenden "Anfängerfehler" beobachtet habe: Wenn man zeigen will, daß eine (kompliziert beschriebene) ganze Zahl n durch eine (ebenfalls kompliziert beschriebene) ganze Zahl d teilbar ist, dann genügt es nicht, *eine* Zahl *q zu konstruieren, sodaß*

$$n = d \cdot q$$

gilt: Man muß auch zeigen, daß q eine ganze *Zahl ist!*

Aufgabe 4: *Zeige $(a-b) \mid (a^n - b^n)$ für alle $a, b \in \mathbb{Z}$ und alle $n \in \mathbb{N}$.*

Aufgabe 5: *Zeige: Wenn $m \mid n$ dann $(a^m - b^m) \mid (a^n - b^n)$ (mit $a, b \in \mathbb{Z}$, $m, n \in \mathbb{N}$).*

Aufgabe 6: *Zeige: Wenn $2 \nmid n$ für ein $n \in \mathbb{N}$ dann $8 \mid (n^2 + 23)$.*

Aufgabe 7: *Zeige: Wenn $3 \nmid n$ für ein $n \in \mathbb{N}$ dann $3 \mid (n^2 + 23)$.*

Aufgabe 8: *Zeige: Wenn $2 \nmid a$ und $2 \nmid b$ (mit $a, b \in \mathbb{Z}$) dann $2 \mid (a^2 + b^2)$ aber $4 \nmid (a^2 + b^2)$.*

Aufgabe 9: *Zeige: Wenn $7 \mid (a^2 + b^2)$ (mit $a, b \in \mathbb{Z}$) dann $7 \mid a$ und $7 \mid b$.*

Aufgabe 10: *Finde alle $n \in \mathbb{N}$, die $(n+1) \mid (n^2 + 1)$ erfüllen.*

Aufgabe 11: *Zeige $6 \mid (n^3 - n)$ für alle $n \in \mathbb{N}$.*

Aufgabe 12: *Zeige $13 \mid \left(4^{2n+1} + 3^{n+2}\right)$ für alle $n \in \mathbb{N}_0$.*

Hinweis: Induktion nach n.

Aufgabe 13: *Zeige $169 \mid (3^{3n+3} - 26n - 27)$ für alle $n \in \mathbb{N} \cup \{0\}$.*

Aufgabe 14: *Zeige $n^2 \mid \left((n+1)^n - 1\right)$ für alle $n \in \mathbb{N}$.*

Aufgabe 15: *Zeige $(1^3 + 2^3 + \cdots + n^3) \mid \left(3(1^5 + 2^5 + \cdots + n^5)\right)$ für alle $n \in \mathbb{N}$.*

Aufgabe 16: *Beweise, daß $f(n) := \dfrac{n^5}{5} + \dfrac{n^3}{3} + \dfrac{7 \cdot n}{15} \in \mathbb{N}$ für alle $n \in \mathbb{N}$.*

Hinweis: Betrachte $f(n+1) - f(n)$.

Direkt aus der Definition der Teilbarkeit ergeben sich folgende einfache Beobachtungen:

BEOBACHTUNG 1.3.3. *Für alle $n \in \mathbb{Z} \setminus \{0\}$ gilt*

$$d \mid n \implies |d| \leqslant |n|. \tag{1.5}$$

Denn $|n| = |d| \cdot |k|$ *und* $|k| \geqslant 1$. *Insbesondere ist die Menge aller Teiler von* n *immer* endlich.

Wir haben für alle $n \in \mathbb{Z}$ *folgende* äquivalente *Aussagen:*

$$d \mid n \iff (-d) \mid n \iff d \mid (-n) \iff (-d) \mid (-n),$$

denn

$$n = d \cdot k \iff n = (-d) \cdot (-k) \iff -n = d \cdot (-k) \iff -n = (-d) \cdot k.$$

Das kann man auch so zusammenfassen:

$$d \mid n \iff |d| \mid |n|. \tag{1.6}$$

Für die Frage "ist d *ein Teiler von* n*?" kann man also immer* $d \geqslant 0$ *und* $n \geqslant 0$ *annehmen.*

Für alle $n \in \mathbb{Z}$ *gilt* $1 \mid n$ *(denn* $n = 1 \cdot n$*) und* $n \mid 0$ *(denn* $0 = 0 \cdot n$*), also*

- 1 *ist ein Teiler* jeder *ganzen Zahl,*
- 0 *ist ein Vielfaches* jeder *ganzen Zahl.*

Andrerseits folgt aus $d \mid \pm 1$ *(d.h. ja* $1 = |d| \cdot |k|$*) sofort* $d = \pm 1$*, und aus* $0 \mid n$ *(d.h. ja* $n = 0 \cdot k$*) sofort* $n = 0$*; also*

- ± 1 *ist kein Vielfaches irgendeiner andren Zahl außer* ± 1*,*
- 0 *ist kein Teiler irgendeiner andren Zahl außer* 0*.*

Für alle $f \in \mathbb{Z} \setminus \{0\}$ *gilt*

$$d \mid n \iff f \cdot d \mid f \cdot n, \tag{1.7}$$

denn

$$n = d \cdot k \iff f \cdot n = (f \cdot d) \cdot k.$$

Ebenso gilt

$$d_i \mid n_i \text{ für } i = 1, 2, \ldots, m \implies \left(\prod_{i=1}^{m} d_i \right) \mid \left(\prod_{i=1}^{m} n_i \right), \tag{1.8}$$

denn

$$n_i = d_i \cdot k_i \text{ für } i = 1, 2, \ldots, m \implies \prod_{i=1}^{m} n_i = \left(\prod_{i=1}^{m} d_i \right) \cdot \left(\prod_{i=1}^{m} k_i \right).$$

Für die elementare Bestimmung aller (positiven) Teiler einer (positiven) Zahl n ist folgende Tatsache nützlich:

PROPOSITION 1.3.4. *Seien* $n, k, d \in \mathbb{N}$ *mit* $n = d \cdot k$*: Dann gilt zumindest eine der Ungleichungen*

$$d \leqslant \sqrt{n} \text{ oder } k \leqslant \sqrt{n}.$$

BEWEIS. Angenommen nicht: Dann wäre

$$d \cdot k > \sqrt{n} \cdot \sqrt{n} = n,$$

ein Widerspruch. □

BEISPIEL 1.3.5. *Wir wollen alle Teiler von $n = -60$ bestimmen: Da jeder Teiler von -60 auch Teiler von $+60$ ist (und umgekehrt), bestimmen wir (äquivalent) die Teiler von $60 \in \mathbb{N}$. Da $7 < \sqrt{60} < 8$, brauchen wir nur die Teilbarkeit bis höchstens 7 untersuchen: Alle Teiler ergeben sich dann aus der Tabelle*

Teiler $\leqslant 7$	*Komplementärteiler* $\geqslant 8$	*Gleichung*
1	*60*	$60 = 1 \cdot 60$
2	*30*	$60 = 2 \cdot 30$
3	*20*	$60 = 3 \cdot 20$
4	*15*	$60 = 4 \cdot 15$
5	*12*	$60 = 5 \cdot 12$
6	*10*	$60 = 6 \cdot 10$

Aufgabe 17: *Finde alle positiven Teiler von a) 1799 b) 997.*

1.3.1. Teilbarkeit als Ordnungsrelation auf $\mathbb{N}$.

PROPOSITION 1.3.6. *Seien $l, m, n \in \mathbb{Z}$. Dann gilt:*

$$m \mid n \text{ und } n \mid m \implies m = \pm n, \tag{1.9}$$

$$l \mid m \text{ und } m \mid n \implies l \mid n. \tag{1.10}$$

BEWEIS. Aus $n = k \cdot m$ und $m = d \cdot n$ folgt

$$n = (k \cdot d) \cdot n,$$

also $k \cdot d = 1$ und daher $k = d = \pm 1$; damit ist (1.9) gezeigt.
Aus $m = k \cdot l$ und $n = d \cdot m$ folgt

$$n = (k \cdot d) \cdot l,$$

also $l \mid n$; damit ist auch (1.10) gezeigt. □

KOROLLAR 1.3.7 (Teilbarkeit ist Ordnungsrelation auf $\mathbb{N}$). *Auf der Menge $\mathbb{N}$ definiert die Teilbarkeitsrelation eine* Ordnungsrelation $\preceq$*:*

$$a \preceq b :\Longleftrightarrow a \mid b.$$

Diese Ordnungsrelation ist in folgendem Sinne "kompatibel" mit der gewöhnlichen Ordnungsrelation $\leqslant$ auf $\mathbb{N}$:

$$a \preceq b \implies a \leqslant b.$$

BEWEIS. Wir müssen die drei Eigenschaften einer Ordnungsrelation nachweisen:

- Reflexivität: $a \mid a$ für alle $a \in \mathbb{N}$ ist klarerweise richtig,
- Antisymmetrie: $a \mid b$ und $b \mid a \implies a = b$ folgt aus (1.9) (da $a, b \in \mathbb{N}$, folgt aus $a = \pm b$ natürlich $a = b$),
- Transitivität: Ergibt sich sofort aus (1.10).

Die "Kompatibilität" der Teilbarkeitsrelation mit der gewöhnlichen Ordnungsrelation folgt aus (1.5). □

BEMERKUNG 1.3.8. *Es gibt tatsächlich Situationen, in denen man die* Gleichheit *zweier (kompliziert beschriebenen)* natürlichen *Zahlen m, n am einfachsten dadurch nachweist, daß man zeigt: $m \mid n$ und $n \mid m$. (Aber Achtung: Wenn $m, n \in \mathbb{Z}$, dann folgt daraus nur $m = \pm n$.)*

1.3.2. (Größte) gemeinsame Teiler und (kleinste) gemeinsame Vielfache.

DEFINITION 1.3.9 (gemeinsame Teiler und gemeinsame Vielfache). *Sei $n \in \mathbb{N}$, seien $z_1, z_2, \ldots, z_n \in \mathbb{Z}$ fix gewählte ganze Zahlen.*

Eine Zahl $d \in \mathbb{Z}$ mit der Eigenschaft

$$d \mid z_1 \text{ und } d \mid z_2 \text{ und } \cdots d \mid z_n$$

(das heißt also: d teilt alle *Zahlen z_i, $i = 1, 2, \ldots, n$) heißt ein* gemeinsamer Teiler *von $z_1, z_2, \ldots, z_n$, und wir schreiben für diesen Sachverhalt abkürzend:*

$$d \mid z_1, z_2, \ldots, z_n.$$

Eine Zahl $v \in \mathbb{Z}$ mit der Eigenschaft

$$z_1 \mid v \text{ und } z_2 \mid v \text{ und } \cdots z_n \mid v$$

(das heißt also: v ist ein Vielfaches aller *Zahlen z_i, $i = 1, 2, \ldots, n$) heißt ein* gemeinsames Vielfaches *von $z_1, z_2, \ldots, z_n$, und wir schreiben für diesen Sachverhalt abkürzend:*

$$z_1, z_2, \ldots, z_n \mid v.$$

BEOBACHTUNG 1.3.10. *Die* Menge *aller gemeinsamen Teiler von $z_1, z_2, \ldots, z_n$ ist niemals leer, denn sie enthält immer die Zahl 1 ($1 \mid r$ für alle $r \in \mathbb{Z}$). Wenn* nicht alle *$z_i = 0$ sind, dann ist sie ist außerdem beschränkt: Denn für jeden gemeinsamen Teiler d gilt dann $|d| \leqslant \min\{|z_i| : \ z_i \neq 0\}$.*

Die Menge *aller gemeinsamen Vielfachen von $z_1, z_2, \ldots, z_n$ ist auch niemals leer, denn sie enthält immer die Zahl 0 ($r \mid 0$ für alle $r \in \mathbb{Z}$). Wenn* alle *$z_i \neq 0$, dann ist auch die* Menge *aller* positiven *gemeinsamen Vielfachen von $z_1, z_2, \ldots, z_n$ niemals leer, denn sie enthält dann immer die Zahl $|z_1 \cdot z_2 \cdots z_n| > 0$.*

DEFINITION 1.3.11 (größter gemeinsamer Teiler und kleinstes gemeinsames Vielfaches). *Sei $n \in \mathbb{N}$, seien $z_1, z_2, \ldots, z_n \in \mathbb{Z}$ fix gewählte ganze Zahlen.*

Wenn nicht alle *$z_i = 0$ sind, dann heißt die* größte *Zahl in der Menge der gemeinsamen Teiler von $z_1, z_2, \ldots, z_n$ (wenig überraschend;-)* größter gemeinsamer Teiler *von $z_1, z_2, \ldots, z_n$, diese Zahl wird auch mit* $\mathrm{ggT}(z_1, z_2, \ldots, z_n)$ *bezeichnet.*

Wenn alle $z_i \neq 0$ sind, dann heißt die kleinste *Zahl in der Menge der* positiven *gemeinsamen Vielfachen*[3] *von $z_1, z_2, \ldots, z_n$ (auch nicht überraschend;-)* kleinstes gemeinsames Vielfaches *von $z_1, z_2, \ldots, z_n$, diese Zahl wird auch mit* $\mathrm{kgV}(z_1, z_2, \ldots, z_n)$ *bezeichnet*[4].

BEISPIEL 1.3.12. *Bestimme* $\mathrm{ggT}(12, -8)$*: Die positiven Teiler von 12 (bzw. -8) sind 1, 2, 3, 4, 6, 12 (bzw. 1, 2, 4, 8). Gemeinsame Teiler sind 1, 2, 4, also ist* $\mathrm{ggT}(12, -8) = 4$.

[3] Die Menge der *negativen* gemeinsamen Vielfachen ist ja entweder leer (wenn ein $z_i = 0$ ist) oder nach unten unbeschränkt und hat daher kein kleinstes Element.

[4] Wenn ein $z_i = 0$ ist, dann müßte man $\mathrm{kgV}(z_1, z_2, \ldots, z_n) = 0$ setzen.

Direkt aus der Definition erhält man:

BEOBACHTUNG 1.3.13. *Sei $n \in \mathbb{N}$, seien $z_1, z_2, \ldots, z_n \in \mathbb{Z}$ fix gewählte ganze Zahlen; nicht alle $z_i = 0$. Da* $\mathrm{ggT}(z_1, \ldots, z_n) \geqslant 1$, *kann man sich für seine Bestimmung auf die* positiven *Teiler der Zahlen z_i beschränken.*
Es gilt:

$$\begin{aligned}\mathrm{ggT}(z_1, \ldots, z_n) &= \mathrm{ggT}(|z_1|, \ldots, |z_n|),\\ \mathrm{ggT}(z_1, \ldots, z_n, 0) &= \mathrm{ggT}(z_1, \ldots, z_n),\\ \mathrm{ggT}(z_1, \ldots, z_n, z_n) &= \mathrm{ggT}(z_1, \ldots, z_n).\end{aligned}$$

Außerdem hängt der größte gemeinsame Teiler natürlich nicht von der Reihenfolge *der Zahlen $z_1, \ldots, z_n$ ab; es ist also z.B.* $\mathrm{ggT}(z_1, z_2, z_3) = \mathrm{ggT}(z_2, z_3, z_1)$[5].
Zusammenfassend: *Man kann bei der Bestimmung des größten gemeinsamen Teilers der Zahlen $z_1, \ldots, z_k$ o.B.d.A. voraussetzen, daß diese* positiv, verschieden *und* absteigend geordnet *sind, also $z_1 > z_2 > \cdots > z_n > 0$.*

DEFINITION 1.3.14 ($\mathbb{Z}$–Linearkombination). *Sei $n \in \mathbb{N}$, seien $z_1, z_2, \ldots, z_n \in \mathbb{Z}$ fix gewählte Zahlen. Dann nennen wir jede Summe von Produkten der Gestalt*

$$\lambda_1 \cdot z_1 + \lambda_2 \cdot z_2 + \cdots + \lambda_n \cdot z_n \in \mathbb{Z},$$

wobei $\lambda_1, \lambda_2, \ldots, \lambda_n$ beliebige Zahlen aus $\mathbb{Z}$ sind, eine $\mathbb{Z}$–Linearkombination *von $z_1, z_2, \ldots, z_n$.*

BEOBACHTUNG 1.3.15. *Sei $n \in \mathbb{N}$, seien $z_1, z_2, \ldots, z_n \in \mathbb{Z}$ fix gewählte Zahlen, sei d ein gemeinsamer Teiler von $z_1, z_2, \ldots, z_n$: Dann teilt d auch* jede $\mathbb{Z}$*–Linearkombination von $z_1, z_2, \ldots, z_n$.*

BEWEIS. Sei $\lambda_1, \lambda_2, \ldots, \lambda_n \in \mathbb{Z}$ beliebig und $m = \lambda_1 \cdot z_1 + \lambda_2 \cdot z_2 + \cdots + \lambda_n \cdot z_n$. Die Voraussetzung, daß d ein gemeinsamer Teiler ist, bedeutet:

$$\text{Für alle } i, 1 \leqslant i \leqslant n, \text{ gibt es ein } k_i \text{ sodaß } z_i = d \cdot k_i.$$

Also können wir d herausheben:

$$m = d \cdot \left(\underbrace{\lambda_1 \cdot k_1 + \lambda_2 \cdot k_2 + \cdots + \lambda_n \cdot k_n}_{\in \mathbb{Z}} \right),$$

und das heißt definitionsgemäß $d \mid m$. □

PROPOSITION 1.3.16. *Sei $n \in \mathbb{N}$, seien $z_1, z_2, \ldots, z_n \in \mathbb{Z} \setminus \{0\}$ fix gewählte ganze Zahlen. Dann gilt für* jedes *gemeinsame Vielfache v von $z_1, z_2, \ldots, z_n$:*

$$\mathrm{kgV}(z_1, z_2, \ldots, z_n) \mid v$$

BEWEIS. Sei $k := \mathrm{kgV}(z_1, z_2, \ldots, z_n)$. Wir führen Division mit Rest durch:

$$v = q \cdot k + r \text{ mit } 0 \leqslant r < k.$$

Dann ist aber $r = 1 \cdot v - q \cdot k$ eine $\mathbb{Z}$–Linearkombination der Zahlen v und k, die *beide* durch *alle* Zahlen z_i, $i = 1, 2, \ldots, n$ teilbar sind. Dann ist aber nach Beobachtung 1.3.15 auch r selbst durch alle z_i teilbar, d.h., $r \geqslant 0$ ist ein *nicht–negatives*

[5] Allgemein formuliert: $\mathrm{ggT}(z_1, z_2, \ldots z_n) = \mathrm{ggT}\left(z_{\pi(1)}, z_{\pi(2)}, \ldots, z_{\pi(n)}\right)$ für alle Permutationen $\pi \in \mathfrak{S}_n$.

gemeinsames Vielfaches von $z_1, z_2, \ldots, z_n$. Nach Definition des *kleinsten* gemeinsamen Vielfachen kann r aber nicht *positiv* sein (denn $r < \text{kgV}(z_1, z_2, \ldots, z_n)$); also ist $r = 0$. □

DEFINITION 1.3.17 (Ideal). *Sei $n \in \mathbb{N}$, seien $z_1, z_2, \ldots, z_n \in \mathbb{Z}$ fix gewählte Zahlen. Die Menge* aller $\mathbb{Z}$*–Linearkombinationen von $z_1, z_2, \ldots, z_n$ heißt das von $z_1, \ldots, z_n$ erzeugte* Ideal*, wir bezeichnen es mit $(\!(z_1, \ldots, z_n)\!)$:*

$$(\!(z_1, \ldots, z_n)\!) := \{\lambda_1 \cdot z_1 + \lambda_2 \cdot z_2 + \cdots + \lambda_n \cdot z_n : \ \lambda_1, \lambda_2, \ldots, \lambda_n \in \mathbb{Z}\} \subseteq \mathbb{Z}.$$

BEISPIEL 1.3.18. *Das Ideal, das von den Zahlen $2, 4, 6, 8$ erzeugt wird, ist definitionsgemäß*

$$(\!(2, 4, 6, 8)\!) = \{\lambda \cdot 2 + \mu \cdot 4 + \nu \cdot 6 + \psi \cdot 8 : \ \lambda, \mu, \nu, \psi \in \mathbb{Z}\}.$$

Das können wir aber auch schreiben als

$$\left\{ 2 \cdot \underbrace{(1 \cdot \lambda + 2 \cdot \mu + 3 \cdot \nu + 4 \cdot \psi)}_{\text{nimmt alle Werte in } \mathbb{Z} \text{ an!}} : \ \lambda, \mu, \nu, \psi \in \mathbb{Z} \right\} = 2 \cdot \mathbb{Z}.$$

BEOBACHTUNG 1.3.19. *Sei $n \in \mathbb{N}$, seien $z_1, z_2, \ldots, z_n \in \mathbb{Z}$ fix gewählte Zahlen. Die Menge $S := (\!(z_1, \ldots, z_n)\!)$ ist klarerweise nicht leer, weil sie* immer 0 *enthält:*

$$0 \in (\!(z_1, \ldots, z_n)\!) \subseteq \mathbb{Z}.$$

Wenn nicht $z_1 = z_2 = \cdots = z_n = 0$ gilt, dann enthält S auch immer positive *Zahlen. Außerdem gilt:*

$$\begin{aligned} x \in S, \rho \in \mathbb{Z} &\implies \rho \cdot x \in S, \\ x, y \in S &\implies x + y \in S. \end{aligned}$$

Insbesondere gilt also: $1 \in S \implies S = \mathbb{Z}$.

Der folgende Satz ist von grundlegender Bedeutung:

SATZ 1.3.20 (Darstellung des ggT). *Sei $n \in \mathbb{N}$, seien $z_1, z_2, \ldots, z_n \in \mathbb{Z}$ fix gewählte ganze Zahlen; nicht alle gleich 0. Dann gilt:*

Die kleinste positive Zahl in $(\!(z_1, \ldots, z_n)\!)$ ist *der* $\text{ggT}(z_1, z_2, \ldots, z_n)$*!*

Also:

$$\begin{aligned} \text{ggT}(z_1, z_2, \ldots, z_n) &= \min\left((\!(z_1, z_2, \ldots, z_n)\!) \cap \mathbb{N}\right) \\ &= \min\{|\lambda_1 \cdot z_1 + \lambda_2 \cdot z_2 + \cdots + \lambda_n \cdot z_n| : \ \lambda_1, \lambda_2, \ldots, \lambda_n \in \mathbb{Z}\}. \end{aligned} \tag{1.11}$$

BEWEIS. Sei

$$m = \mu_1 \cdot z_1 + \mu_2 \cdot z_2 + \cdots + \mu_n \cdot z_n \tag{1.12}$$

die kleinste positive Zahl in $(\!(z_1, \ldots, z_n)\!)$, sei $d = \text{ggT}(z_1, z_2, \ldots, z_n)$. Gemäß Beobachtung 1.3.15 gilt $d \mid m$, und daraus folgt $d \leqslant m$. Wenn wir zeigen können, daß auch $m \leqslant d$ gilt, dann sind wir fertig. Dazu genügt es zu zeigen, daß m ein *gemeinsamer Teiler* von $z_1, z_2, \ldots, z_n$ ist (denn nach Definition des *größten* gemeinsamen Teilers folgt dann natürlich $m \leqslant d$). Division mit Rest liefert jedenfalls

$$z_i = q_i \cdot m + r_i \text{ mit } 0 \leqslant r_i < m$$

für $i = 1, 2, \ldots, n$. Dann setzen wir die Darstellung (1.12) von m in $r_i = z_i - q_i \cdot m$ ein und erhalten so offensichtlich *auch* eine *nicht–negative* $\mathbb{Z}$–Linearkombination von $z_1, z_2, \ldots, z_n$, für die folgende Ungleichungskette gilt:

$$0 \leqslant r_i = -(q_i \cdot \mu_1) \cdot z_1 - \cdots - (q_i \cdot \mu_i - 1) \cdot z_i - \cdots - (q_i \cdot \mu_n) \cdot z_n < m.$$

Da m die *kleinste positive* $\mathbb{Z}$–Linearkombination von $z_1, z_2, \ldots, z_n$ ist, muß $r_i = 0$ und somit $m \mid z_i$ gelten für alle $i = 1, 2, \ldots, n$: m ist also ein gemeinsamer Teiler. □

KOROLLAR 1.3.21. *Sei $n \in \mathbb{N}$, seien $z_1, z_2, \ldots, z_n \in \mathbb{Z}$ fix gewählte Zahlen; nicht alle gleich 0. Dann gilt für alle $\zeta_1, \ldots, \zeta_{n-1} \in \mathbb{Z}$:*

$$\mathrm{ggT}\,(z_1, \ldots, z_{n-1}, z_n) = \mathrm{ggT}\left(z_1, \ldots, z_{n-1}, z_n + \sum_{i=1}^{n-1} \zeta_i \cdot z_i\right).$$

BEWEIS. Nach Satz 1.3.20 genügt es zu zeigen:

$$(\!(z_1, \ldots, z_{n-1}, z_n)\!) = (\!(z_1, \ldots, z_{n-1}, z_n + \sum_{i=1}^{n-1} \zeta_i \cdot z_i)\!). \tag{1.13}$$

Jede $\mathbb{Z}$–Linearkombination der rechten Seite von (1.13) ist auch in der linken Seite enthalten, denn

$$\mu_1 \cdot z_1 + \cdots + \mu_{n-1} \cdot z_{n-1} + \mu_n \cdot \left(z_n + \sum_{i=1}^{n-1} \zeta_i \cdot z_i\right) = (\mu_1 + \mu_n \cdot \zeta_1) \cdot z_1 + \cdots + (\mu_{n-1} + \mu_n \cdot \zeta_{n-1}) \cdot z_{n-1} + \mu_n \cdot z_n.$$

Also ist

$$(\!(z_1, \ldots, z_{n-1}, z_n + \sum_{i=1}^{n-1} \zeta_i \cdot z_i)\!) \subseteq (\!(z_1, \ldots, z_{n-1}, z_n)\!).$$

Es ist aber auch *jede* $\mathbb{Z}$–Linearkombination der linken Seite von (1.13) in der rechten Seite enthalten, denn

$$\lambda_1 \cdot z_1 + \cdots + \lambda_{n-1} \cdot z_{n-1} + \lambda_n \cdot z_n = (\lambda_1 - \lambda_n \cdot \zeta_1) \cdot z_1 + \cdots (\lambda_{n-1} - \lambda_n \cdot \zeta_{n-1}) \cdot z_{n-1} + \lambda_n \cdot \left(z_n + \sum_{i=1}^{n-1} \zeta_i \cdot z_i\right)$$

Also ist auch

$$(\!(z_1, \ldots, z_{n-1}, z_n)\!) \subseteq (\!(z_1, \ldots, z_{n-1}, z_n + \sum_{i=1}^{n-1} \zeta_i \cdot z_i)\!),$$

und wir sind fertig. □

KOROLLAR 1.3.22. *Sei $n \in \mathbb{N}$, seien $z_1, z_2, \ldots, z_n \in \mathbb{Z}$ fix gewählte ganze Zahlen; nicht alle gleich 0. Dann gilt für* jeden *gemeinsamen Teiler d von $z_1, z_2, \ldots, z_n$:*

$$d \mid \mathrm{ggT}\,(z_1, z_2, \ldots, z_n).$$

BEWEIS. Gemäß Satz 1.3.20 stimmt der $\mathrm{ggT}(z_1, z_2, \ldots, z_n)$ mit einer $\mathbb{Z}$–Linearkombination von $z_1, z_2, \ldots, z_n$ überein, und diese wird nach Beobachtung 1.3.15 von *jedem* gemeinsamen Teiler von $z_1, z_2, \ldots, z_n$ geteilt. □

Proposition 1.3.16 und Korollar 1.3.22 können wir wie folgt zusammenfassen (um die ständige Einschränkung "nicht alle $z_i = 0$" zu vermeiden, formulieren wir dies für *natürliche* Zahlen):

MERKSATZ 1.3.23. *Sei $n \in \mathbb{N}$, seien $z_1, z_2, \ldots, z_n \in \mathbb{N}$ fix gewählte natürliche Zahlen. Dann gilt:*

- Jeder *gemeinsame Teiler von $z_1, z_2, \ldots, z_n$ teilt auch* $\mathrm{ggT}(z_1, z_2, \ldots, z_n)$,
- Jedes *gemeinsame Vielfache von $z_1, z_2, \ldots, z_n$ ist auch ein Vielfaches von* $\mathrm{kgV}(z_1, z_2, \ldots, z_n)$.

Die bisherigen Erkenntnisse über den größten gemeinsamen Teiler können wir auch wie folgt zusammenfassen:

KOROLLAR 1.3.24 (Charakterisierung des ggT). *Sei $n \in \mathbb{N}$, seien $z_1, z_2, \ldots, z_n \in \mathbb{Z}$ fix gewählte Zahlen; nicht alle gleich 0. Dann ist $d = \mathrm{ggT}(z_1, z_2, \ldots, z_n)$ durch folgende Eigenschaften bestimmt:*

- $d \geqslant 1$,
- $d \mid z_1, z_2, \ldots, z_n$*: D.h., d ist ein* gemeinsamer *Teiler von $z_1, z_2, \ldots, z_n$,*
- $d' \mid z_1, z_2, \ldots, z_n \implies d' \mid d$*: D.h.,* jeder *gemeinsame Teiler von $z_1, z_2, \ldots, z_n$ teilt $d = \mathrm{ggT}(z_1, z_2, \ldots, z_n)$.*

KOROLLAR 1.3.25 (Charakterisierung des kgV). *Sei $n \in \mathbb{N}$, seien $z_1, z_2, \ldots, z_n \in \mathbb{Z}\setminus\{0\}$ fix gewählte Zahlen Dann ist $v = \mathrm{kgV}(z_1, z_2, \ldots, z_n)$ durch folgende Eigenschaften bestimmt:*

- $v \geqslant 1$,
- $z_1, z_2, \ldots, z_n \mid v$*: D.h., v ist ein* gemeinsames *Vielfaches von $z_1, z_2, \ldots, z_n$,*
- $z_1, z_2, \ldots, z_n \mid v' \implies v \mid v'$*: D.h.,* jedes *gemeinsame Vielfache von $z_1, z_2, \ldots, z_n$ ist ein Vielfaches von $v = \mathrm{kgV}(z_1, z_2, \ldots, z_n)$.*

KOROLLAR 1.3.26. *Sei $n \in \mathbb{N}$, seien $z_1, z_2, \ldots, z_n \in \mathbb{Z}$ fix gewählte Zahlen; nicht alle gleich 0. Sei $d = \mathrm{ggT}(z_1, z_2, \ldots, z_n)$. Dann gilt:*

$$\mathrm{ggT}(l \cdot z_1, l \cdot z_2, \ldots, l \cdot z_n) = d \cdot |l| \text{ für alle } l \in \mathbb{Z}\setminus\{0\}, \tag{1.14}$$

$$\mathrm{ggT}\left(\frac{z_1}{d}, \frac{z_2}{d}, \ldots, \frac{z_n}{d}\right) = 1. \tag{1.15}$$

BEWEIS. Wir verwenden die Charakterisierung aus Korollar 1.3.24 für die erste Behauptung (1.14): O.B.d.A. ist $l > 0$ (siehe Beobachtung 1.3.13); klarerweise ist dann $d \cdot |l| = d \cdot l \geqslant 1$.Weiters gibt es für alle $i = 1, \ldots, n$ ein $q_i \in \mathbb{Z}$ sodaß

$$d \mid z_i \iff z_i = d \cdot q_i \iff l \cdot z_i = (l \cdot d) \cdot q_i \iff (l \cdot d) \mid (l \cdot z_i). \tag{1.16}$$

Also gilt $(l \cdot d) \mid (l \cdot z_1), \ldots, (l \cdot z_n)$, und daher gilt für $d' := \mathrm{ggT}(l \cdot z_1, \ldots, l \cdot z_n)$

$$(l \cdot d) \mid d'.$$

Andrerseits ist offensichtlich, daß l *auch* ein gemeinsamer Teiler von $l \cdot z_1, l \cdot z_2, \ldots, l \cdot z_n$ ist, also ist

$$l \mid d' \iff d' = l \cdot e \text{ für ein } e \in \mathbb{N}.$$

Wenn wir nun die Kette von Äquivalenzen (1.16) mit e statt d von rechts nach links durchgehen, erkennen wir $e \mid z_1, z_2, \ldots, z_n$: Dann folgt aber

$$e \mid d \implies \underbrace{(l \cdot e)}_{=d'} \mid (l \cdot d) .$$

Wir haben also für die *positiven* Zahlen $l \cdot d$ und d' gezeigt:

$$(l \cdot d) \mid d' \text{ und } d' \mid (l \cdot d) ,$$

daher ist $(l \cdot d) = d'$ (und wir haben ein Beispiel für Bemerkung 1.3.8 gesehen). Die zweite Behauptung (1.15) ergibt sich aus der ersten:

$$d = \mathrm{ggT}\,(z_1, \ldots, z_n) = \mathrm{ggT}\left(d \cdot \frac{z_1}{d}, \ldots, d \cdot \frac{z_n}{d}\right) = d \cdot \mathrm{ggT}\left(\frac{z_1}{d}, \ldots, \frac{z_n}{d}\right). \qquad \square$$

1.3.2.1. *Die Lineare Diophantische Gleichung.*

DEFINITION 1.3.27 (Diophantische Gleichung). *Eine* diophantische Gleichung[6] *ist eine eine Gleichung der Form*

$$f\,(x_1, x_2, x_3, \ldots, x_n) = 0,$$

wobei f ein Polynom mit ganzzahligen Koeffizienten in den Variablen $x_1, x_2, x_3, \ldots, x_n$ ist: Im Unterschied zu einer "gewöhnlichen" Polynomgleichung sucht man nur ganzzahlige *Lösungen.*

BEISPIEL 1.3.28. *Zum Beispiel ist*

$$1 \cdot x_1^2 + 1 \cdot x_2^2 - 1 \cdot x_3^2 = 0$$

eine diophantische Gleichung, die (unter anderen) die ganzzahlige Lösung $x_1 = 3$, $x_2 = 4$ und $x_3 = 5$ hat (jede Lösung dieser speziellen diophantischen Gleichung heißt übrigens pythagoräisches Tripel*; wegen des offensichtlichen Zusammenhangs mit dem* Pythagoräischen Lehrsatz*.).*
Allgemeiner ist für alle $n \in \mathbb{N}$

$$1 \cdot x_1^n + 1 \cdot x_2^n - 1 \cdot x_3^n = 0$$

eine diophantische Gleichung: Daß diese spezielle Gleichung, die man auch in der Form

$$a^n + b^n = c^n$$

schreiben kann, für $n > 2$ keine *Lösung in natürlichen Zahlen hat, ist der* Große Satz von Fermat*, der im 17. Jahrhundert von Pierre de Fermat formuliert, aber erst 1994 von Andrew Wiles und Richard Taylor bewiesen wurde.*

KOROLLAR 1.3.29 (Lineare Diophantische Gleichung). *Sei $n \in \mathbb{N}$, seien $a_1, \ldots, a_n \in \mathbb{Z}\setminus\{0\}$. Die* lineare diophantische Gleichung

$$a_1 \cdot x_1 + a_2 \cdot x_2 + \cdots + a_n \cdot x_n - c = 0 \tag{1.17}$$

hat genau dann eine Lösung*, wenn*

$$\mathrm{ggT}\,(a_1, a_2, \ldots, a_n) \mid c.$$

[6] Benannt nach dem griechischen Mathematiker Diophantos von Alexandria, der vermutlich um 250 n.Chr. gelebt hat.

BEWEIS. Sei $d = \mathrm{ggT}(a_1, a_2, \ldots, a_n)$. Dann teilt d auch *jede* $\mathbb{Z}$–Linearkombination

$$a_1 \cdot x_1 + a_2 \cdot x_2 + \cdots + a_n \cdot x_n,$$

und wenn es eine Lösung der Gleichung (1.17) gibt, dann gibt es eine solche $\mathbb{Z}$–Linearkombination, die gleich c ist: Also muß d auch c teilen.

Wenn umgekehrt $d \mid c$ gilt, dann ist also $c = d \cdot k$. Aus Satz 1.3.20 wissen wir, daß wir d darstellen können als

$$d = a_1 \cdot y_1 + a_2 \cdot y_2 + \cdots + a_n \cdot y_n.$$

Daraus ergibt sich aber sofort eine Lösung von (1.17):

$$c = d \cdot k = a_1 \cdot (k \cdot y_1) + a_2 \cdot (k \cdot y_2) + \cdots + a_n \cdot (k \cdot y_n). \qquad \square$$

Aufgabe 18: *Es seien $a, b, c \in \mathbb{Z}$. Zeige: Wenn die lineare diophantische Gleichung $a \cdot x + b \cdot y = c$ lösbar ist, ist ihre Lösungsmenge durch $\left\{ \left(x_0 - \frac{b}{d} \cdot t, y_0 + \frac{a}{d} \cdot t \right) : \ t \in \mathbb{Z} \right\}$ gegeben. Dabei ist $(x_0, y_0) \in \mathbb{Z}^2$ eine beliebige Lösung der gegebenen linearen diophantischen Gleichung (d.h. $a \cdot x_0 + b \cdot y_0 = c$) und $d = \mathrm{ggT}(a, b)$.*

Hinweis: Was ist die Differenz $(x_0 - x_1, y_0 - y_1)$ zweier Lösungen (x_0, y_0), (x_1, y_1) der diophantischen Gleichung?

1.3.3. Der Euklidische Algorithmus. Die Charakterisierung des größten gemeinsamen Teilers als kleinste positive Zahl in einer Menge von $\mathbb{Z}$–Linearkombinationen erwies sich zwar als sehr nützlich (zum Beispiel konnten wir damit vollständig klären, wann eine lineare diophantische Gleichung eine Lösung hat), aber sie liefert kein sehr praktikables Verfahren, um den größten gemeinsamen Teiler wirklich zu *bestimmen*. Eine auf Satz 1.3.20 basierende *Heuristik*[7] würde etwa so aussehen:

```
/* Sei n ∈ ℕ, seien z_1,...,z_n ∈ ℕ */
abbruch ← 0
while abbruch = 0 do
  d ← irgendeine ℤ–Linearkombination von z_1, ..., z_n
  if d ist gemeinsamer Teiler von z_1, ..., z_n then
    abbruch ← 1
  end if
end while
return d
```

BEISPIEL 1.3.30. *In "günstigen" Fällen kann diese Heuristik rasch zum Ziel führen:* $\mathrm{ggT}(111, 129, 243) = 3$ *erhalten wir z.B. sofort aus der Darstellung*

$$3 = 1 \cdot 243 - 1 \cdot 129 - 1 \cdot 111$$

zusammen mit der Beobachtung, daß $3 \mid 111, 129, 243$.

Für $n = 2$ gibt es aber einen *Algorithmus* (also ein methodisches, zielführendes Verfahren), der seit über 2000 Jahren bekannt ist: Den *Euklidischen Algorithmus*.

[7] Als Heuristik bezeichnet man jedes Verfahren, das durch "geschickte Mutmaßungen" eine gute (aber im allgemeinen nicht die optimale) Lösung liefert.

SATZ 1.3.31 (Euklidischer Algorithmus). *Der folgende Algorithmus liefert für zwei Zahlen* $a, b \in \mathbb{N}$ *den* ggT (a, b)*:*

if $b > a$ **then**
  $a \leftrightarrow b$ /* Vertausche a und b. */
end if
$n \leftarrow a, d \leftarrow b$ /* Dividend & Divisor: Ab nun gilt immer $0 < d \leqslant n$. */
/* Wiederholte Division mit Rest: $n = d \cdot q + r$ mit $0 \leqslant r < d$ */
repeat
  $n = d \cdot q + r$ /* JEDER gemeinsame Teiler von n und d teilt r!!! */
  $n \leftarrow d, d \leftarrow r$
until $d = 0$
return n /* Der Rückgabewert ist der letzte Rest $r \neq 0$ */

BEWEIS. Bei jedem Algorithmus ist zunächst die Frage zu stellen, ob er überhaupt *abbricht*. Dazu verdeutlichen wir uns, was bei der wiederholten Division mit Rest passiert. Sei $r_0 := a$ und $r_1 := b$, dann werden der Reihe nach folgende Rechenschritte ausgeführt:

$$\begin{aligned} r_0 &= r_1 \cdot q_0 + r_2,\ 0 \leqslant r_2 < r_1 \\ r_1 &= r_2 \cdot q_1 + r_3,\ 0 \leqslant r_3 < r_2 \\ r_2 &= r_3 \cdot q_2 + r_4,\ 0 \leqslant r_4 < r_3 \\ r_3 &= r_4 \cdot q_3 + r_5,\ 0 \leqslant r_5 < r_4 \\ &\vdots \end{aligned}$$

Die Folge der Reste, die im Wiederholungsschritt auftreten, ist also strikt fallend

$$r_1 > r_2 > r_3 > r_4 > \dots,$$

aber nach unten durch 0 beschränkt (alle $r_i \geqslant 0$) und kann daher nicht unendlich lang sein: Es gibt also ein n mit $r_{n+1} = 0$, und der Algorithmus liefert den *letzten nichtverschwindenden Rest* r_n.

Dieses r_n ist tatsächlich ein *gemeinsamer Teiler* von a, b, denn

$$\begin{aligned} r_{n-1} = r_n \cdot q_n &\implies r_n \mid r_{n-1} \\ r_{n-2} = r_{n-1} \cdot q_{n-1} + r_n &\implies r_n \mid r_{n-2} \\ r_{n-3} = r_{n-2} \cdot q_{n-2} + r_{n-1} &\implies r_n \mid r_{n-3} \\ &\vdots \end{aligned}$$

Also schließlich: $r_n \mid r_0 = a$ und $r_n \mid r_1 = b$.

Andrerseits erhalten wir durch "sukzessives Einsetzen" in dieser Gleichungskette

$$\begin{aligned} r_n = r_{n-2} - r_{n-1} \cdot q_{n-1} &\implies r_n \text{ ist } \mathbb{Z}\text{–Linearkombination von } r_{n-1} \text{ und } r_{n-2} \\ r_{n-1} = r_{n-3} - r_{n-2} \cdot q_{n-2} &\implies r_n \text{ ist } \mathbb{Z}\text{–Linearkombination von } r_{n-2} \text{ und } r_{n-3} \\ r_{n-2} = r_{n-4} - r_{n-3} \cdot q_{n-3} &\implies r_n \text{ ist } \mathbb{Z}\text{–Linearkombination von } r_{n-3} \text{ und } r_{n-4} \\ &\vdots \end{aligned}$$

daß r_n eine $\mathbb{Z}$–Linearkombination von a, b ist, daher teilt *jeder* gemeinsame Teiler d von a, b auch r_n. □

BEISPIEL 1.3.32. *Bestimme* $\mathrm{ggT}(97, 44)$*:*

$$\begin{aligned} 97 &= 2 \cdot 44 + 9, \\ 44 &= 9 \cdot 4 + 8, \\ 9 &= 1 \cdot 8 + 1, \\ 8 &= 8 \cdot 1 + 0. \end{aligned}$$

Das ergibt $\mathrm{ggT}(97, 44) = 1$.
Wenn wir (beginnend mit der vorletzten Gleichung) sukzessive von unten in die Gleichungskette einsetzen, erhalten wir

$$\begin{aligned} 1 &= 1 \cdot 9 - 1 \cdot 8 \\ &= 1 \cdot 9 - (1 \cdot 44 - 4 \cdot 9) = 5 \cdot 9 - 1 \cdot 44 \\ &= 5 \cdot (1 \cdot 97 - 2 \cdot 44) - 1 \cdot 44 \\ &= 5 \cdot 97 - 11 \cdot 44 \end{aligned}$$

eine Darstellung des größten gemeinsamen Teilers 1 *als* $\mathbb{Z}$*–Linearkombination von* 97 *und* 44.

BEMERKUNG 1.3.33. *Die Darstellung des größten gemeinsamen Teilers als* $\mathbb{Z}$*–Linearkombination ist* nicht *eindeutig: Für das vorige Beispiel sehen wir zunächst*

$$98 = (98 \cdot 5) \cdot 97 - (98 \cdot 11) \cdot 44$$

und erhalten daraus sofort eine andere Darstellung:

$$1 = (98 \cdot 5 - 1) \cdot 97 - (98 \cdot 11) \cdot 44 = 489 \cdot 97 - 1078 \cdot 44.$$

Aufgabe 19: *Bestimme mit dem euklidischen Algorithmus:*
a) $\mathrm{ggT}(7469, 2464)$ *b)* $\mathrm{ggT}(2689, 4001)$ *c)* $\mathrm{ggT}(2947, 3997)$ *d)* $\mathrm{ggT}(1109, 4999)$

Aufgabe 20: *Finde mit Hilfe des euklidischen Algorithmus* $x, y \in \mathbb{Z}$ *derart, daß*
a) $243 \cdot x + 198 \cdot y = 9$ *b)* $71 \cdot x - 50 \cdot y = 1$ *c)* $43 \cdot x + 64 \cdot y = 1$ *d)* $93 \cdot x - 81 \cdot y = 3$

Aufgabe 21: *Zeige: Wenn* $\mathrm{ggT}(a, 4) = \mathrm{ggT}(b, 4) = 2$ *(mit* $a, b \in \mathbb{Z}$*) dann* $\mathrm{ggT}(a + b, 4) = 4$.

Aufgabe 22: *Zeige: Wenn* $a, b \in \mathbb{Z}$ *und* $\mathrm{ggT}(a, b) = 1$ *dann* $\mathrm{ggT}(a + b, a - b) \in \{1, 2\}$.

Aufgabe 23: *Zeige: Für alle* $k \in \mathbb{Z}$ *gilt* $\mathrm{ggT}(2 \cdot k + 1, 9 \cdot k + 4) = 1$.

Aufgabe 24: *Bestimme* $\mathrm{ggT}(4 \cdot k + 1, 5 \cdot k + 2)$ *für alle* $k \in \mathbb{Z}$.

Aufgabe 25: *Bestimme* $\mathrm{ggT}(2 \cdot k - 1, 9 \cdot k + 4)$ *für alle* $k \in \mathbb{Z}$.

PROPOSITION 1.3.34. *Sei* $n \in \mathbb{N}$*, seien* $z_1, z_2, \ldots, z_n \in \mathbb{Z}$ *fix gewählte Zahlen; nicht alle gleich* 0*. Dann gilt für* $z_{n+1} \in \mathbb{Z}$ *beliebig:*

$$\mathrm{ggT}(z_1, \ldots, z_n, z_{n+1}) = \mathrm{ggT}(\mathrm{ggT}(z_1, \ldots, z_n), z_{n+1}). \tag{1.18}$$

BEWEIS. Bezeichne d die linke Seite und d' die rechte Seite von (1.18). Dann gilt $d \mid d'$, denn

$$d \mid z_1, \ldots, z_n \text{ und } d \mid z_{n+1} \implies d \mid \operatorname{ggT}(z_1, \ldots, z_n), z_{n+1}.$$

Aber umgekehrt gilt $d' \mid d$, denn

$$d' \mid \operatorname{ggT}(z_1, \ldots, z_n), z_{n+1} \implies d' \mid z_1, \ldots, z_{n+1}.$$

Da $d, d' > 0$ folgt also $d = d'$ (und wir haben noch ein Beispiel für Bemerkung 1.3.8 gesehen). □

Es ist klar, daß man durch wiederholte Anwendung von Proposition 1.3.34 nicht nur den größten gemeinsamen Teiler von mehr als 2 Zahlen finden kann, sondern auch dessen Darstellung als $\mathbb{Z}$–Linearkombination:

BEISPIEL 1.3.35. *Wir zeigen* $\operatorname{ggT}(6, 10, 15) = 1$ *und konstruieren* $x, y, z \in \mathbb{Z}$ *mit* $x \cdot 6 + y \cdot 10 + z \cdot 15 = 1$. *Dazu bestimmen wir zuerst* $\operatorname{ggT}(6, 10)$ *mit dem Euklidischen Algorithmus:*

$$\begin{aligned} 10 &= 1 \cdot 6 + 4 \\ 6 &= 1 \cdot 4 + 2 \\ 4 &= 2 \cdot 2 + 0. \end{aligned}$$

Wir sehen also $\operatorname{ggT}(6, 10) = 2$, *und durch sukzessives Einsetzen von unten in die Gleichungskette erhalten wir die Darstellung* $2 = 2 \cdot 6 - 10$.
Nun wissen wir: $\operatorname{ggT}(6, 10, 15) = \operatorname{ggT}(\operatorname{ggT}(6, 10), 15) = \operatorname{ggT}(2, 15)$ *und bestimmen nun* $\operatorname{ggT}(2, 15)$ *mit dem Euklidischen Algorithmus:*

$$\begin{aligned} 15 &= 7 \cdot 2 + 1 \\ 2 &= 2 \cdot 1 + 0, \end{aligned}$$

und erhalten sofort die Darstellung $1 = 1 \cdot 15 - 7 \cdot 2$, *in die wir die zuvor gefundene Darstellung von* 2 *einsetzen:*

$$1 = 1 \cdot 15 - 7 \cdot (2 \cdot 6 - 10) = \underbrace{(-14)}_{=x} \cdot 6 + \underbrace{7}_{=y} \cdot 10 + \underbrace{1}_{=z} \cdot 15.$$

(In diesem sehr einfachen Fall sieht man "mit freiem Auge" auch eine andre Darstellung: $1 = 1 \cdot 10 + 1 \cdot 6 - 1 \cdot 15$.*)*

Zur Bestimmung des größten gemeinsamen Teilers von mehr als 2 natürlichen Zahlen gibt es aber auch folgende Verallgemeinerung des Euklidischen Algorithmus: Seine Gültigkeit folgt direkt aus Beobachtung 1.3.13 zusammen mit Korollar 1.3.21.

SATZ 1.3.36 (Verallgemeinerter Euklidischer Algorithmus). *Sei* $n \in \mathbb{N}$. *Der folgende Algorithmus liefert für* n *Zahlen* $z_1 > z_2 > \cdots > z_n \in \mathbb{N}$ *den* $\operatorname{ggT}(z_1, \ldots, z_n)$:

```
/* In jedem Wiederholungsschritt wird eine Liste von n verschiedenen,
absteigend geordneten natürlichen Zahlen (z_1,...,z_n) bearbeitet. */
while n > 1 do
  d ← z_n /* Divisor ist kleinste Zahl der Liste */
  if d = 1 then
    return 1 /* ggT(z_1,...,1) = 1 */
```

end if
for $i = 1$ **to** $n - 1$ **do**
$z_i = d \cdot q_i + r_i$ `/* Bestimme die Reste bei Division durch` q `*/`
end for
`/* Bilde nun neue Liste, OHNE den ggT zu ändern!!! */`
$(z_1, \ldots, z_{n-1}, z_n) \leftarrow (r_1, \ldots, r_{n-1}, z_n)$ `/* Korollar 1.3.21!!! */`
"Entferne Nullen und doppelte Elemente aus der neuen Liste, ordne sie absteigend."
$n \leftarrow$ "Länge der neuen Liste" `/* Beobachtung 1.3.13!!! */`
end while
return z_1 `/* Der Rückgabewert ist das einzige Element der Liste */`

BEWEIS. Der Beweis ist in den Kommentaren zum Algorithmus bereits enthalten; er wird durch die offensichtliche Beobachtung

$$\mathrm{ggT}(z) = |z|$$

abgeschlossen. □

BEISPIEL 1.3.37. *Wir illustrieren den verallgemeinerten Euklidischen Algorithmus:*

$$\begin{aligned}
\mathrm{ggT}(721, 613, 114) &= \mathrm{ggT}(114, 43, 37) \quad \leftarrow 721{=}6{\cdot}114{+}37,\ 613{=}5{\cdot}114{+}43 \\
&= \mathrm{ggT}(37, 6, 3) \quad \leftarrow 114{=}3{\cdot}37{+}3,\ 43{=}1{\cdot}37{+}6 \\
&= \mathrm{ggT}(3, 1) \quad \leftarrow 37{=}12{\cdot}3{+}1, 6{=}2{\cdot}3{+}0 \\
&= 1.
\end{aligned}$$

Aufgabe 26: *Bestimme* $\mathrm{ggT}(56049, 14601, 43803)$.

Aufgabe 27: *Finde* $x, y, z \in \mathbb{Z}$ *sodaß*
a) $6 \cdot x + 10 \cdot y + 15 \cdot z = 1$, *b)* $21 \cdot x + 15 \cdot y + 35 \cdot z = 1$.

DEFINITION 1.3.38 (relativ prim). *Sei* $n \in \mathbb{N}$. *Die Zahlen* $z_1, \ldots, z_n \in \mathbb{Z}$ *heißen* relativ prim *(oder* teilerfremd*), wenn* $\mathrm{ggT}(z_1, \ldots, z_n) = 1$*; sie heißen* paarweise relativ prim *(oder* paarweise teilerfremd*), wenn* $\mathrm{ggT}(z_i, z_j) = 1$ *für alle* $1 \leqslant i < j \leqslant n$.

Klarerweise gilt: Sind $z_1, \ldots, z_n \in \mathbb{Z}$ *paarweise* relativ prim, dann sind sie auch relativ prim.

SATZ 1.3.39. *Seien* $x, y, z \in \mathbb{Z} \setminus \{0\}$. *Dann gilt:*

$$z|(x{\cdot}y) \text{ und } \mathrm{ggT}(z,x){=}1 \implies z \mid y, \tag{1.19}$$

$$x,y|z \text{ und } \mathrm{ggT}(x,y){=}1, \implies (x \cdot y) \mid z \tag{1.20}$$

$$\mathrm{ggT}(x,y,z){=}1 \implies \mathrm{ggT}(x, z) \cdot \mathrm{ggT}(y, z) = \mathrm{ggT}((x \cdot y), z), \tag{1.21}$$

$$\mathrm{ggT}(x,z){=}\mathrm{ggT}(y,z){=}1 \implies \mathrm{ggT}((x \cdot y), z) = 1. \tag{1.22}$$

BEWEIS. Wenn $\mathrm{ggT}(z, x) = 1$, dann gibt es eine Darstellung als $\mathbb{Z}$–Linearkombination:

$$1 = \lambda \cdot x + \mu \cdot z.$$

Dann ist aber auch

$$y = 1 \cdot y = \lambda \cdot (x \cdot y) + \mu \cdot (z \cdot y)\,.$$

Klarerweise gilt $z \mid (z \cdot y)$; wenn auch $z \mid (x \cdot y)$ gilt, folgt also $z \mid y$: Damit ist (1.19) gezeigt.

Wenn $x, y \mid z$, dann ist $z = y \cdot k$ für ein $k \in \mathbb{Z}$ und $x \mid (y \cdot k)$: Wenn $\mathrm{ggT}\,(x, y) = 1$, dann folgt aus (1.19)

$$x \mid k \implies (y \cdot x) \mid (y \cdot k) = z,$$

und damit ist auch (1.20) gezeigt.

Sei $a = \mathrm{ggT}\,(x, z)$, $b = \mathrm{ggT}\,(y, z)$ und $c = \mathrm{ggT}\,((x \cdot y), z)$. Dann gibt es Darstellungen

$$\begin{aligned} a &= \lambda_x \cdot x + \lambda_z \cdot z, \\ b &= \mu_y \cdot y + \mu_z \cdot z. \end{aligned}$$

Also ist

$$(a \cdot b) = (x \cdot y) \cdot \left(\lambda_x \cdot \mu_y\right) + z \cdot \left(\lambda_x \cdot \mu_z \cdot x + \mu_y \cdot \lambda_z \cdot y + \lambda_z \cdot \mu_z \cdot z\right),$$

und daraus folgt

$$c \mid (a \cdot b)\,.$$

Sei $d = \mathrm{ggT}\,(a, b)$: Dann gilt $d \mid x, y, z \implies d \mid \mathrm{ggT}\,(x, y, z)$; wenn also $\mathrm{ggT}\,(x, y, z) = 1$ gilt, dann muß auch $d = 1$ gelten. Außerdem gilt

$$a \mid x, z \implies a \mid (x \cdot y), z \text{ und } b \mid y, z \implies b \mid (x \cdot y), z,$$

und daher gilt $a, b \mid c$; aus (1.20) folgt daher

$$(a \cdot b) \mid c;$$

und damit ist auch (1.21) gezeigt.

Es gilt natürlich

$$\mathrm{ggT}\,(x, y, z) \mid \mathrm{ggT}\,(x, z), \mathrm{ggT}\,(y, z)\,.$$

Wenn $\mathrm{ggT}\,(x, z) = \mathrm{ggT}\,(y, z) = 1$, dann ist also auch $\mathrm{ggT}\,(x, y, z) = 1$, und (1.22) folgt direkt aus (1.21). □

Aufgabe 28: *Gegeben seien $a, b, c, d \in \mathbb{Z}$ mit $b, d \neq 0$ und $\mathrm{ggT}\,(a, b) = \mathrm{ggT}\,(c, d) = 1$. Zeige:*

$$\frac{a}{b} + \frac{c}{d} \in \mathbb{Z} \implies b \in \{d, -d\}\,.$$

Aufgabe 29: *Zeige für $a, b_1, \ldots, b_k \in \mathbb{Z}$, daß*

$$\mathrm{ggT}\,(a, b_1 \cdot b_2 \cdots b_k) = 1 \iff \mathrm{ggT}\,(a, b_i) = 1 \text{ für } 1 \leqslant i \leqslant k.$$

1.4. Primzahlen und die eindeutige Primfaktorzerlegung

DEFINITION 1.4.1 (Primzahl). *Eine Zahl $p > 1 \in \mathbb{N}$, die als positive Teiler* nur 1 *und p besitzt (die also nur die* trivialen *Teiler hat), heißt* prim *oder* Primzahl.

Beachte: 1 *ist definitionsgemäß* keine *Primzahl. Wir bezeichnen die* Menge aller Primzahlen *mit* $\mathbb{P}$*:*

$$\mathbb{P} = \{2, 3, 5, 7, 11, 13, 17, 19, 23, 29, \dots\}.$$

Außerdem bezeichnen wir die n–te Primzahl mit $\mathbf{p}(n)$*: Also* $\mathbf{p}(1) = 2, \mathbf{p}(2) = 3, \mathbf{p}(3) = 5, \dots$.

LEMMA 1.4.2. *Sei $p \in \mathbb{P}$, $n \in \mathbb{Z}$, dann gilt:*

$$\operatorname{ggT}(p, n) > 1 \iff p \mid n.$$

BEWEIS. Die Richtung ($\Longleftarrow$) ist klar: $p \mid n \implies \operatorname{ggT}(p, n) = p > 1$.

Die Richtung ($\Longrightarrow$) ist auch klar: Falls $d = \operatorname{ggT}(n, p) > 1$, dann gilt definitionsgemäß $d \mid p, n$, also nach Definition einer Primzahl $d = p$ und somit $p \mid n$. □

SATZ 1.4.3. *Es sei $p > 1 \in \mathbb{N}$, dann sind äquivalent:*

(1) *p ist Primzahl,*
(2) *für alle $a, b \in \mathbb{Z}$ gilt: $p \mid (a \cdot b) \implies p \mid a$ oder $p \mid b$,*
(3) *wenn $p = (x \cdot y)$ für $x, y \in \mathbb{Z}$, dann gilt $x = \pm 1$ oder $y = \pm 1$.*

BEWEIS. (1) $\Longrightarrow$ (2): Wenn $p \mid a$, dann ist nichts mehr zu zeigen. Wenn aber $p \nmid a$, dann ist nach Lemma 1.4.2 $\operatorname{ggT}(a, p) = 1$, und aus (1.19) in Satz 1.3.39 folgt $p \mid b$.

(2) $\Longrightarrow$ (3): $p = (x \cdot y) \implies p \mid (x \cdot y)$, und aus (2) folgt o.B.d.A. $p \mid x$. Dann ist aber $|x| \geqslant |p|$ und

$$|p| = |x \cdot y| = |x| \cdot |y| \geqslant |p| \cdot |y| \implies |y| \leqslant 1 \implies y = \pm 1.$$

(3) $\Longrightarrow$ (1): Sei d ein Teiler von p, dann ist $p = k \cdot d$, und aus (3) folgt $d = \pm 1$ oder $k = \pm 1 \implies d = \pm p$. □

Mit Induktion ergibt sich aus Satz 1.4.3 (2) sofort:

MERKSATZ 1.4.4 (Erster Euklidischer Satz). *Wenn eine Primzahl ein Produkt teilt, dann teilt sie mindestens einen Faktor. Formal: Sei $p \in \mathbb{P}$; sei $n \in \mathbb{N}$, $z_1, \dots, z_n \in \mathbb{Z}$. Dann*

$$p \mid (z_1 \cdot z_2 \cdots z_n) \implies p \mid z_i \text{ für (mindestens) ein } i = 1, \dots, n.$$

LEMMA 1.4.5. *Sei $n \in \mathbb{N}, n \geqslant 2$. Dann ist die zweitkleinste Zahl in der Menge aller positiven Teiler von n eine Primzahl*[8]*:*

$$\min\{d \in \mathbb{N}, d \geqslant 2 \colon\ d \mid n\} \in \mathbb{P}.$$

[8] Die kleinste Zahl in dieser Menge ist 1.

BEWEIS. Da $n \geqslant 2$, *gibt* es einen positiven Teiler $d \geqslant 2$ von n:

$$\{d \in \mathbb{N}, d \geqslant 2 \colon\ d \mid n\} \neq \varnothing,$$

also enthält diese Menge ein kleinstes Element q. Angenommen, q wäre nicht prim: Dann gäbe es einen Teiler m von q mit $m > 1$ und $m < q$, aber

$$m \mid q \mid n \implies m \mid n :$$

also $m \in \{d \in \mathbb{N}, d \geqslant 2 \colon\ d \mid n\}$ und $m < q$, ein Widerspruch. □

MERKSATZ 1.4.6. *Eine Primzahl $p \in \mathbb{P}$, die eine Zahl $n \in \mathbb{Z}$ teilt, heißt ein* Primteiler *von n: Lemma 1.4.5 besagt einfach, daß jede ganze Zahl z mit $|z| > 1$ einen Primteiler hat.*

SATZ 1.4.7 (Zweiter Euklidischer Satz). *Es gibt unendlich viele Primzahlen.*

BEWEIS. Angenommen, es gäbe nur endlich viele Primzahlen $p_1, \ldots, p_n$. Betrachte $N := 1 + p_1 \cdot p_2 \cdots p_n$, dann ist $N \geqslant 2$, und nach Lemma 1.4.5 hat N einen Primteiler p. Diese Primzahl p müßte nach Voraussetzung eine der Primzahlen $p_1, \ldots, p_n$ sein, also

$$p \mid N, (p_1 \cdot p_2 \cdots p_n) \implies p \mid N - (p_1 \cdot p_2 \cdots p_n)\,,$$

d.h.: $p \mid 1 \implies p \leqslant 1$, ein Widerspruch. □

SATZ 1.4.8 (Eindeutige Primfaktorzerlegung). *Sei $z \in \mathbb{N}$, $z \geqslant 2$. Dann lässt sich z als Produkt von (nicht notwendigerweise verschiedenen) Primzahlen darstellen:*

$$z = p_1 \cdot p_2 \cdots p_k \text{ für } p_1, p_2, \ldots, p_k \in \mathbb{P}.$$

Diese Darstellung heißt Primfaktorzerlegung *von z; sie ist bis auf die Reihenfolge der Faktoren* eindeutig*, d.h., wenn*

$$z = q_1 \cdot q_2 \cdots q_m \text{ für } q_1, q_2, \ldots, q_m \in \mathbb{P}.$$

eine zweite solche Produktdarstellung von z ist, dann ist $k = m$, und es gibt eine Permutation[9] *$\pi \in \mathfrak{S}_k$, sodaß $q_i = p_{\pi(i)}$ für $1 \leqslant i \leqslant k$.*

BEWEIS. Die Existenz dieser Faktorisierung in Primzahlen zeigen wir mit Induktion nach z: Der Induktionsanfang $z = 2$ ist klar: 2 *ist* ja eine Primzahl (die Faktorisierung besteht also aus einem einzigen Faktor).

Für den Induktionsschritt sei die Behauptung schon für alle $k < z$ gezeigt. z hat einen Primteiler q: Wenn $z = q$ ist, dann hat z natürlich eine Faktorisierung (mit dem einzigen Primfaktor $q = z$). Andernfalls ist $z = q \cdot m$ mit $m < z$, sodaß es nach Induktionsvoraussetzung eine Faktorisierung $m = p_1 \cdots p_n$ mit $p_1, \ldots, p_n \in \mathbb{P}$ gibt. Also ist $z = q \cdot p_1 \cdots p_n$ eine Faktorisierung in Primzahlen, wie behauptet.

Die Eindeutigkeit der Primfaktorzerlegung ergibt sich aus Satz 1.4.3 (2): Sei

$$z = p_1 \cdot p_2 \cdots p_k = q_1 \cdot q_2 \cdots q_m$$

die *kleinste* natürliche Zahl mit zwei *verschiedenen* Primfaktorzerlegungen. Dann gilt $p_1 \mid z \implies p_1 \mid q_i \implies p_1 = q_i$ für ein i, $1 \leqslant i \leqslant m$. Aber das hieße

[9] Eine Permutation $\pi \in \mathfrak{S}_k$ ist eine *Anordnung* der Zahlen aus $[k] = \{1, 2, \ldots, k\}$.

$p_2 \cdot p_3 \cdots p_k < z$ ist eine natürliche Zahl mit zwei verschiedenen Primfaktorzerlegungen

$$p_2 \cdot p_3 \cdots p_k = q_1 \cdot \cdots \cdot \not{q_i} \cdots q_m,$$

ein Widerspruch zur Minimalität von z. □

BEMERKUNG 1.4.9. *Die Primfaktorzerlegung einer natürlichen Zahl $z \geqslant 2$ können wir auch folgendermaßen schreiben:*

$$z = \prod_{p \in \mathbb{P}} p^{\alpha_p}, \tag{1.23}$$

wobei $\alpha_p \in \mathbb{N}_0$ angibt, wie oft die Primzahl p in der Primfaktorzerlegung von z vorkommt. Dies ist ein "formal unendliches" Produkt (es läuft über alle *Primzahlen), aber die Exponenten α_p sind nur für jene* endlich vielen *Primzahlen > 0, für die $p \mid z$ gilt: Das heißt, in diesem Produkt sind nur* endlich *viele Faktoren $\neq 1$. Diese Darstellung "funktioniert" auch für die Zahl* 1*:*

$$1 = \prod_{p \in \mathbb{P}} p^0.$$

Sei $\{p_1, \ldots, p_n\} = \{p \in \mathbb{P} \colon\ p \mid z\}$ die Menge der Primteiler von z, dann können wir die Primfaktorzerlegung auch so schreiben:

$$z = p_1^{\beta_1} \cdots p_n^{\beta_n} = \prod_{\substack{p \in \mathbb{P} \\ p \mid z}} p^{\alpha_p}.$$

1.4.1. Bestimmung von ggT und kgV mit Primfaktorzerlegung.

LEMMA 1.4.10. *Seien $a, b \in \mathbb{N}$ mit Primfaktorenzerlegungen*

$$a = \prod_{p \in \mathbb{P}} p^{\alpha_p} \text{ und } b = \prod_{p \in \mathbb{P}} p^{\beta_p}.$$

Dann gilt:

$$a \cdot b = \prod_{p \in \mathbb{P}} p^{\alpha_p + \beta_p}, \tag{1.24}$$

$$a \mid b \iff \alpha_p \leqslant \beta_p \text{ für alle } p \in \mathbb{P}. \tag{1.25}$$

BEWEIS. Die Behauptung (1.24) folgt aus der für alle $x \in \mathbb{C}, m, n \in \mathbb{N}_0$ richtigen Tatsache

$$x^m \cdot x^n = x^{m+n}. \tag{1.26}$$

Denn die Primfaktorzerlegungen sind ja nur *formal* unendliche Produkte: Faktoren ungleich 1 liefert nur die *endliche* Menge der Primzahlen, die a oder b teilen, d.h., für

$$\mathbb{P}' := \{p \in \mathbb{P} \colon\ p \mid a \text{ oder } p \mid b\} \text{ mit } \left|\mathbb{P}'\right| < \infty$$

gilt

$$a = \prod_{p \in \mathbb{P}'} p^{\alpha_p} \text{ und } b = \prod_{p \in \mathbb{P}'} p^{\beta_p} :$$

Und für diese *endlichen* Produkte folgt alles aus (1.26) (und der Kommutativität der Multiplikation):

$$a \cdot b = \prod_{p \in \mathbb{P}'} \left(p^{\alpha_p} \cdot p^{\beta_p} \right) = \prod_{p \in \mathbb{P}'} \left(p^{\alpha_p + \beta_p} \right).$$

Die zweite Behauptung (1.25) ergibt sich aus der ersten (1.24): Für ($\Longrightarrow$) überlegen wir:

$$a \mid b \implies \exists c \in \mathbb{N} \colon \; b = a \cdot c.$$

Sei die Primfaktorzerlegung von c

$$c = \prod_{p \in \mathbb{P}} p^{\gamma_p} \text{ mit } \gamma_p \geqslant 0 \text{ für alle } p \in \mathbb{P},$$

dann gilt also

$$\beta_p = \alpha_p + \gamma_p \text{ für alle } p \in \mathbb{P} \implies \beta_p \geqslant \alpha_p \text{ für alle } p \in \mathbb{P}.$$

Für ($\Longleftarrow$) überlegen wird: Aus $\beta_p \geqslant \alpha_p$ für alle $p \in \mathbb{P}$ folgt

$$\delta_p := \beta_p - \alpha_p \geqslant 0 \text{ für alle } p \in \mathbb{P},$$
$$\delta_p := \beta_p - \alpha_p > 0 \text{ nur für endliche viele } p \in \mathbb{P}'.$$

Dann folgt für

$$d = \prod_{p \in \mathbb{P}} p^{\delta_p}$$

aus (1.24) natürlich $a \cdot d = b \implies a \mid b$. □

SATZ 1.4.11. *Sei $n \in \mathbb{N}$, seien $z_1, \ldots, z_n \in \mathbb{N}$ mit Primfaktorzerlegungen*

$$z_i = \prod_{p \in \mathbb{P}} p^{\alpha_{i,p}},$$

$i = 1, \ldots, n$. Dann gilt:

$$\operatorname{ggT}(z_1, \ldots, z_n) = \prod_{p \in \mathbb{P}} p^{\min\{\alpha_{i,p} : i = 1, \ldots, n\}}, \tag{1.27}$$

$$\operatorname{kgV}(z_1, \ldots, z_n) = \prod_{p \in \mathbb{P}} p^{\max\{\alpha_{i,p} : i = 1, \ldots, n\}}. \tag{1.28}$$

BEWEIS. Sei $d := \prod_{p \in \mathbb{P}} p^{\min\{\alpha_{1,p}, \ldots, \alpha_{n,p}\}}$. Dann folgt aus (1.25)

$$d \mid z_1, \ldots z_n \text{ und } d' \mid z_1, \ldots, z_n \implies d' \mid d,$$

also ist $d = \operatorname{ggT}(z_1, \ldots, z_n)$ (siehe Korollar 1.3.24).

Sei $v := \prod_{p \in \mathbb{P}} p^{\max\{\alpha_{1,p}, \ldots, \alpha_{n,p}\}}$. Dann folgt aus (1.25)

$$z_1, \ldots z_n \mid v \text{ und } z_1, \ldots, z_n \mid v' \implies v \mid v',$$

also ist $v = \operatorname{kgV}(z_1, \ldots, z_n)$ (siehe Korollar 1.3.25). □

BEISPIEL 1.4.12. *Sei $a = 8100 = 2^2 \cdot 3^4 \cdot 5^2$, $b = 24696 = 2^3 \cdot 3^2 \cdot 7^3$: Dann ist $\operatorname{ggT}(a, b) = 2^2 \cdot 3^2 \cdot 5^0 \cdot 7^0 = 36$ und $\operatorname{kgV}(a, b) = 2^3 \cdot 3^4 \cdot 5^2 \cdot 7^3 = 5556600$.*

KOROLLAR 1.4.13. *Seien $a, b \in \mathbb{N}$. Dann gilt*

$$a \cdot b = \mathrm{ggT}(a,b) \cdot \mathrm{kgV}(a,b). \tag{1.29}$$

BEWEIS. Da für *alle* $x, y \in \mathbb{R}$

$$x + y = \max\{x,y\} + \min\{x,y\}$$

gilt, folgt die Behauptung sofort aus (1.27), (1.28) und (1.24). □

KOROLLAR 1.4.14. *Sei $n \in \mathbb{N}, n \leqslant 2$ und $z_1, \ldots, z_n \in \mathbb{N}$. Dann sind äquivalent:*

(1) *$z_1, \ldots, z_n$ sind paarweise relativ prim,*
(2) $\mathrm{kgV}(z_1, \ldots, z_n) = z_1 \cdots z_n$.

BEWEIS. Wir bezeichnen die Primfaktorzerlegungen der Zahlen z_i mit

$$z_i = \prod_{p \in \mathbb{P}} p^{\alpha_{i,p}}.$$

$z_1, \ldots, z_n$ paarweise relativ prim ist gleichbedeutend mit:

$$\text{für alle } p \in \mathbb{P} \text{ ist } \textit{höchstens} \text{ ein } \alpha_{i,p} > 0;\ i = 1, \ldots, n.$$

Und das ist gleichbedeutend mit:

$$\text{für alle } p \in \mathbb{P} \text{ ist } \sum_{i=1}^{n} \alpha_{i,p} = \max\left\{\alpha_{1,p}, \ldots, \alpha_{n,p}\right\}.$$

Und das ist gemäß (1.28) gleichbedeutend mit:

$$\mathrm{kgV}(z_1, \ldots, z_n) = z_1 \cdots z_n.$$ □

Aufgabe 30: *Zeige: Wenn $a \cdot b = c^n$ (mit $a, b, c, n \in \mathbb{N}$ und $\mathrm{ggT}(a,b) = 1$) dann sind a und b ebenfalls n–te Potenzen natürlicher Zahlen.*

Aufgabe 31: *Zeige: Sind $n_1, \ldots, n_k \in \mathbb{Z}\setminus\{0\}$ so gilt $\mathrm{kgV}(\ell \cdot n_1, \ldots, \ell \cdot n_k) = |\ell| \cdot \mathrm{kgV}(n_1, \ldots, n_k)$ für alle $\ell \in \mathbb{Z}\setminus\{0\}$.*

Aufgabe 32: *Zeige: Ist $k \geqslant 2$ und $n_1, \ldots, n_k \in \mathbb{Z}\setminus\{0\}$ so gilt*

$$\mathrm{kgV}(\mathrm{kgV}(n_1, \ldots, n_{k-1}), n_k) = \mathrm{kgV}(n_1, \ldots, n_k).$$

1.4.2. Wissenswertes über Primzahlen. Die Primzahlen sind zwar einfach definiert, bergen aber dennoch schwierige Fragen, von denen bis heute keineswegs alle beantwortet sind.

1.4.2.1. *Die Verteilung der Primzahlen.*

SATZ 1.4.15. *Die Menge $\mathbb{P}$ aller Primzahlen enthält beliebig große Lücken, in folgendem Sinn: Für alle $n \in \mathbb{N}$ gibt es eine Folge*

$$a+1, a+2, \ldots, a+n$$

von n aufeinanderfolgenden natürlichen Zahlen, die keine Primzahl enthält.

BEWEIS. Wähle einfach $a = (n+1)! + 1 = 1 \cdot 2 \cdot 3 \cdots (n+1) + 1$: Dann gilt für alle $d = 1, 2, \ldots, n$

$$(d+1) \mid a + d \text{ und } 1 < (d+1) < a + d.$$

Jede der n Zahlen $a + d$ hat also einen nichttrivialen Teiler und ist daher nicht prim. □

BEMERKUNG 1.4.16. *Sei* $\pi\colon\ \mathbb{R} \to \mathbb{N}$ *die Funktion, die jeder Zahl* x *die Anzahl der Primzahlen zwischen* 1 *und* x *zuordnet:*

$$\pi(x) = |\{p \in \mathbb{P}\colon\ p \leqslant x\}|.$$

Dann besagt der Primzahlsatz[10]*:*

$$\pi(x) \sim \frac{x}{\log x} \textit{ für } \quad x \to \infty. \tag{1.30}$$

(Das bedeutet $\lim\limits_{x\to\infty} \frac{\pi(x)}{\frac{x}{\log x}} = 1$*.)*

Um die Primzahlen zu finden, die kleinergleich x *sind, kann man das* Sieb des Eratosthenes *anwenden:*

"Schreibe alle Zahlen von 2 bis $\lfloor x \rfloor$ auf"
while "Es gibt noch Zahlen, die nicht gestrichen oder eingeringelt wurden"
do
"Ringle die erste solche Zahl ein, streiche alle ihre Vielfachen"
end while`/* Die eingeringelten Zahlen sind die Primzahlen! */`

Aufgabe 33: *Zeige: Bezeichnet* $\mathbf{p}(n)$ *die* n*–te Primzahl, so ist* $\mathbf{p}(n) \leqslant 2^{2^{n-1}}$.

Hinweis: Verwende den Beweis des zweiten Euklidischen Satzes (Satz 1.4.7) und Induktion.

BEOBACHTUNG 1.4.17. *Keine Primzahl* $p > 2$ *ist durch* 2 *teilbar: Bei Division von* $p > 2$ *durch* 4 *treten also nur die Reste* 1 *oder* 3 *auf. Wir drücken das so aus: Jede Primzahl* $p > 2$ *ist* von der Gestalt $4 \cdot k + 1$ *oder* $4 \cdot k + 3$ *(für ein gewisses* $k \in \mathbb{N}_0$*). Außerdem ist das Produkt zweier Zahlen der Gestalt* $4 \cdot l + 1$ *oder der Gestalt* $4 \cdot l + 3$ immer *von der Gestalt* $4 \cdot k + 1$*:*

$$\begin{aligned}(4 \cdot l + 1) \cdot (4 \cdot m + 1) &= 16 \cdot l \cdot m + 4 \cdot l + 4 \cdot m + 1 \\ &= 4 \cdot (4 \cdot l \cdot m + l + m) + 1, \\ (4 \cdot l + 3) \cdot (4 \cdot m + 3) &= 16 \cdot l \cdot m + 12 \cdot l + 12 \cdot m + 9 \\ &= 4 \cdot (4 \cdot l \cdot m + 3 \cdot l + 3 \cdot m + 2) + 1.\end{aligned}$$

SATZ 1.4.18. *Es gibt unendlich viele Primzahlen der Gestalt* $4 \cdot k + 3$*.*

BEWEIS. Angenommen, es gäbe nur *endlich* viele Primzahlen der Gestalt $4 \cdot k + 3$; ihre Menge sei

$$\mathbb{P}' = \{p_1, \ldots p_s\} \text{ (offenbar ist } \{3, 7, 11, 19, 23\} \subset \mathbb{P}').$$

Dann sei $N := p_1^2 \ldots p_s^2 + 2$: Nach Beobachtung 1.4.17 hat N die Gestalt $4 \cdot k + 3$; insbesondere gilt $2 \nmid N$.

[10] Der Primzahlsatz wurde unabhängig voneinander 1896 von *Hadamard* und *de la Vallee Poussin* bewiesen.

Sei $q_1 \cdots q_r$ die Primfaktorzerlegung von N. Es sind alle $q_i > 2$ und daher von der Gestalt $4 \cdot k + 1$ oder $4 \cdot k + 3$; sie können aber nach Beobachtung 1.4.17 nicht *alle* von der Gestalt $4 \cdot k + 1$ sein, also gibt es mindestens ein i mit $q_i = 4 \cdot k + 3$: Nach Annahme müßte das gleich einem $p \in \mathbb{P}'$ sein. Dann würde für dieses $p = q_i$ also gelten:

$$p \mid N, \left(p_1^2 \cdots p_s^2\right) \implies p \mid \underbrace{N - \left(p_1^2 \cdots p_s^2\right)}_{2},$$

ein Widerspruch. □

Aufgabe 34: *Zeige: Es gibt unendlich viele Primzahlen der Gestalt $3k + 2$ (mit $k \in \mathbb{Z}$).*

Aufgabe 35: *Zeige: Es gibt unendlich viele Primzahlen der Gestalt $6k + 5$ (mit $k \in \mathbb{Z}$).*

1.4.2.2. *Spezielle Primzahlen.*

SATZ 1.4.19. *Sei $k \in \mathbb{N}$. Dann gilt:*

$$2^k + 1 \in \mathbb{P} \implies k = 2^n \text{ für ein } n \in \mathbb{N}, \tag{1.31}$$

$$2^k - 1 \in \mathbb{P} \implies k \in \mathbb{P}. \tag{1.32}$$

BEWEIS. Für (1.31) zeigen wir die (äquivalente) Umkehrung:

$$k \neq 2^n \text{ für alle } n \in \mathbb{N} \implies 2^k + 1 \notin \mathbb{P}.$$

Wenn k *keine* Zweierpotenz ist, dann hat k also einen *echten ungeraden* Teiler m: $k = n \cdot m$ mit $1 < m, n < k$ und n ungerade. Dann folgt aus der bekannten *Teleskopsumme* (*abbrechende geometrische Reihe*)

$$\begin{aligned}(x - y) \cdot \sum_{i=0}^{n-1} x^i \cdot y^{n-1-i} &= x^n + \sum_{i=0}^{n-2} x^{i+1} \cdot y^{n-1-i} - y^n - \underbrace{\sum_{i=1}^{n-1} x^i \cdot y^{n-i}}_{i \to i+1} \\ &= x^n - y^n + \sum_{i=0}^{n-2} \underbrace{\left(x^{i+1} \cdot y^{n-1-i} - x^{i+1} \cdot y^{n-i-1}\right)}_{0} \\ &= x^n - y^n \end{aligned} \tag{1.33}$$

für alle $x, y \in \mathbb{C}$, $n \in \mathbb{N}$ sofort

$$2^k + 1 = 2^{m \cdot n} + 1 = (2^m)^n - (-1)^n = \underbrace{(2^m - (-1))}_{\in \mathbb{Z}} \cdot \underbrace{\sum_{i=0}^{n-1} (-1)^i \cdot (2^m)^{n-1-i}}_{\in \mathbb{Z}}.$$

Es gilt also

$$(2^m + 1) \mid \left(2^k + 1\right),$$

und wegen $1 < m < k$ ist $1 < 2^m + 1 < 2^k + 1$: $2^m + 1$ ist also ein *echter* Teiler von $2^k + 1$, also ist $2^k + 1 \notin \mathbb{P}$.

Auch für (1.32) zeigen wir die (äquivalente) Umkehrung:

$$k \notin \mathbb{P} \implies 2^k - 1 \notin \mathbb{P}.$$

Wenn $k \notin \mathbb{P}$, dann hat k *echte* Teiler: $k = n \cdot m$ mit $1 < m, n < k$. Wie zuvor folgt

$$2^k - 1 = (2^m)^n - 1^n = (2^m - 1) \cdot \sum_{i=0}^{n-2} \cdot (2^m)^i ,$$

also $(2^m - 1) \mid \left(2^k - 1\right)$, und wegen $1 < m < k$ ist $1 < 2^m - 1 < 2^k - 1$: $2^m - 1$ ist also ein *echter* Teiler von $2^k - 1$, also ist $2^k - 1 \notin \mathbb{P}$. □

Aufgabe 36: *Zeige: Sind $a, k \in \mathbb{N}$, $k > 1$ und ist $a^k - 1$ Primzahl, so muß $a = 2$ sein.*

Aufgabe 37: *Zeige: Sind $a, k \in \mathbb{N}\backslash\{1\}$ und ist $a^k + 1$ Primzahl, so muß a gerade und k eine Potenz von 2 sein.*

Aufgabe 38: *Es sei p eine Primzahl mit der Eigenschaft, daß $2^p - 1$ ebenfalls Primzahl ist und $n := 2^{p-1}(2^p - 1)$. Zeige, dass $\sum_{d|n} d = 2n$, d.h. die Summe der positiven Teiler von n (ohne n selbst) ist genau n. (Zahlen mit dieser Eigenschaft werden* vollkommen *genannt. Man kann zeigen, daß alle geraden vollkommenen Zahlen von dieser Gestalt sind.)*

BEMERKUNG 1.4.20. *Eine Primzahl der Gestalt $2^{2^k} + 1$ heißt* Fermatsche Primzahl. *Für $k = 0, 1, \ldots, 4$ ist $2^{2^k} + 1$ eine Primzahl:*

$$3, 5, 17, 257, 65537,$$

aber $2^{2^5} + 1 = 2^{32} + 1 = 4294967297 = 614 \cdot 6700417$ ist keine Primzahl. Es ist unbekannt, ob es unendlich viele Fermatsche Primzahlen gibt.
Eine Primzahl der Gestalt $2^p - 1$ heißt Mersennesche Primzahl. *$2^p - 1$ ist Primzahl für $p \in \{2, 3, 5, 7\}$, aber $2^{11} - 1 = 2047 = 23 \cdot 89$. Es ist unbekannt, ob es unendlich viele Mersennesche Primzahlen gibt. Für Zahlen der Gestalt $2^p - 1$ existiert aber ein besonders einfacher* Primzahltest*: Darum sind bekannte* wirklich große *Primzahlen oft Mersennesche Primzahlen.*

1.4.2.3. *Unbewiesene Vermutungen.* Zwei Zahlen $(p, p + 2)$, die beide Primzahlen sind, heißen *Primzahlzwilling*: Die ersten vier Primzahlzwillinge sind

$$(3, 5), (5, 7), (11, 13), (17, 19).$$

Es ist eine *unbewiesene* Vermutung, daß es *unendlich viele* Primzahlzwillinge gibt.

Aufgabe 39: *Zeige: Ist $p, p + 2$ ein Primzahlzwilling und $p > 3$ so gilt $12 \mid (p + (p + 2))$.*

Aufgabe 40: *Finde sämtliche Primzahldrillinge, d.h. alle Tripel $p, p + 2, p + 4$ von Primzahlen.*

Ebenfalls unbewiesen ist die *Goldbachsche Vermutung*, daß sich jede gerade Zahl $\geqslant 4$ als Summe von zwei Primzahlen darstellen läßt. (Für die ersten paar geraden Zahlen sind solche Darstellungen $4 = 2 + 2, 6 = 3 + 3, 8 = 5 + 3, 10 = 5 + 5, 12 = 7 + 5, \ldots$)

KAPITEL 2

Kongruenzen und Restklassenringe

2.1. Kongruenzrelation modulo m

DEFINITION 2.1.1 (Kongruenz). *Sei $m \in \mathbb{N}$ beliebig (aber fest) gewählt. Dann ist die* Kongruenzrelation modulo m *durch*

$$a \equiv b \pmod{m} :\iff m \mid (a-b) \text{ (in Worten: a ist kongruent b modulo m)}$$

definiert; in diesem Zusammenhang wird die Zahl m als Modul *bezeichnet. Falls $m \nmid (a-b)$, schreibt man $a \not\equiv b\,(m)$ und sagt: a ist inkongruent b modulo m.*

BEISPIEL 2.1.2. *Es ist $6 \equiv 24\,(9)$, da $9 \mid (6-24) = 18$; und $14 \equiv -1\,(5)$, da $5 \mid 14-(-1) = 15$.*

BEOBACHTUNG 2.1.3. *Die Kongruenzrelation modulo m ist eine* Äquivalenzrelation, *denn sie ist*

- *Reflexiv: $a \equiv a\,(m)$ für alle $a \in \mathbb{Z}$, da $m \mid (a-a) = 0$ für alle $a \in \mathbb{Z}$,*
- *Symmetrisch: $a \equiv b\,(m) \iff b \equiv a\,(m)$ für alle $a, b \in \mathbb{Z}$, da $m \mid (a-b) \iff m \mid (b-a)$ für alle $a, b \in \mathbb{Z}$,*
- *Transitiv: $a \equiv b\,(m), b \equiv c\,(m) \implies a \equiv c\,(m)$ für alle $a, b, c \in \mathbb{Z}$, da $m \mid (a-b), (b-c) \implies m \mid (a-b)+(b-c) = a-c$ für alle $a, b, c \in \mathbb{Z}$.*

Außerdem ist klar:

$$a \equiv b \pmod{m} \iff m \mid (a-b) \iff a - b = q \cdot m \text{ für ein } q \in \mathbb{Z},$$

das kann man auch so in Worte fassen:

- *$a \equiv b \pmod{m}$ bedeutet, daß sich a und b* um ein Vielfaches von m unterscheiden*: $a = b + q \cdot m$,*
- *$a \equiv b \pmod{m}$ bedeutet, daß a und b bei Division durch m* denselben Rest ergeben*: $b = d \cdot m + r \implies a = d \cdot m + r + q \cdot m = (d+q) \cdot m + r$.*

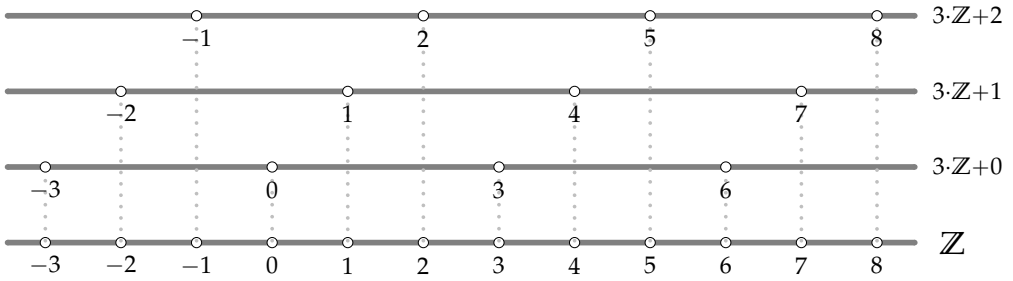
DEFINITION 2.1.4 (Restklasse modulo m). *Sei $m \in \mathbb{N}$. Jede Äquivalenzklasse der Kongruenzrelation modulo m wird als* Restklasse modulo m *bezeichnet. Die* Familie *der Restklassen modulo m bezeichnet man mit $\mathbb{Z}_m$. Es gilt also:*

$$\mathbb{Z}_m = \left\{ \underbrace{\{m \cdot d + r : \ d \in \mathbb{Z}\}}_{=:m\cdot\mathbb{Z}+r} : \ r = 0, 1, \ldots, m-1 \right\}.$$

(Abbildung 1 illustriert die Restklassen modulo 3.)

Sei $s \in \mathbb{Z}_m$ eine Restklasse modulo m: Jedes $a \in s$ wird Repräsentant *von s genannt. Die Restklasse s ist durch jeden ihrer Repräsentanten a eindeutig bestimmt (da zwei verschiedene Restklassen ja disjunkt sind): Man sagt "s ist die Restklasse* von *a" und*

ABBILDUNG 1. Veranschaulichung der Restklassen modulo 3.



bezeichnet dies mit $s = \overline{a}$. *(Der Repräsentant von* s *ist* nicht *eindeutig:* $s = \overline{a} = \overline{a + 1 \cdot m} = \overline{a + 2 \cdot m} = \cdots$.*)*

Wählt man aus jeder Äquivalenzklasse genau einen Repräsentanten, nennt man dies allgemein ein Repräsentantensystem*: Für* $\mathbb{Z}_m$ *nennt man so ein Repräsentantensystem ein* vollständiges Restsystem.

BEOBACHTUNG 2.1.5. *Ganz offensichtlich gilt für alle* $m \in \mathbb{N}$

$$|\mathbb{Z}_m| = m$$

und $\{0, 1, \ldots, m-1\}$ *ist ein vollständiges Restsystem für* $\mathbb{Z}_m$*. Ebenso sind aber auch* $\{m, m+1, \ldots m+m-1\}$ *oder* $\{-2 \cdot m, -1 \cdot m + 1, \ldots, (m-3) \cdot m + m - 1\}$ *vollständige Restsysteme für* $\mathbb{Z}_m$*.*

BEISPIEL 2.1.6. *Vollständige Restsysteme modulo* 4 *sind z.B.:* $\{0, 1, 2, 3\}$, $\{4, -3, -2, 3\}$ *oder* $\{97, 98, 99, 100\}$

Aufgabe 41: *Begründe: Wenn jemand heuer an einem Montag (Dienstag, ..., Samstag, Sonntag) Geburtstag hat, wird er oder sie nächstes Jahr an einem Dienstag (Mittwoch, ..., Sonntag, Montag) Geburtstag haben (vorausgesetzt keines der beiden Jahre ist ein Schaltjahr).*

Aufgabe 42: *Zeige für alle* $a, b \in \mathbb{Z}$ *und alle Primzahlen* p*: Wenn* $a^2 \equiv b^2 \pmod{p}$ *gilt, dann gilt* $p \mid (a-b)$ *oder* $p \mid (a+b)$.

Aufgabe 43: *Es sei* $f \in \mathbb{Z}[x]$*, d.h.:* f *sei ein* Polynom *mit ganzzahligen Koeffizienten. Zeige:*

$$f(a + t \cdot m) \equiv f(a) \pmod{m} \text{ für alle } m \in \mathbb{N} \text{ und alle } a, t \in \mathbb{Z}.$$

Aufgabe 44: *Zeige für alle* $a, b \in \mathbb{Z}$ *und alle Primzahlen* $p \in \mathbb{P}$*, daß* $(a+b)^p \equiv a^p + b^p \pmod{p}$.

Hinweis: Zeige $p \mid \binom{p}{i}$ *für* $1 \leqslant i \leqslant p-1$.

Aufgabe 45: *a) Bestimme die letzten beiden Ziffern der Dezimaldarstellung von* 7^n *für alle* $n \in \mathbb{N}$.

b) Bestimme die letzte Ziffer der Dezimaldarstellung von 2^n *für* $n \in \mathbb{N}$.

2.2. Der Restklassenring $\mathbb{Z}_m$

Man kann die Addition "$+$" und Multiplikation "$\cdot$" ganzer Zahlen so auf die Familie $\mathbb{Z}_m$ der Restklassen modulo m "übertragen", daß $(\mathbb{Z}_m, +, \cdot)$ ein *kommutativer Ring mit* 1 wird (der aber im allgemeinen *nicht* nullteilerfrei ist). Abstrakt geht das ganz schnell:

DEFINITION 2.2.1 (Addition und Multiplikation in $\mathbb{Z}_m$). *Sei $m \in \mathbb{N}$. Dann erklären wir eine zweistellige Verknüpfung "Addition" $\mathbb{Z}_m \times \mathbb{Z}_m \to \mathbb{Z}_m$ (die wir mit "$+$" bezeichnen) und eine zweistellige Verknüpfung "Multiplikation" $\mathbb{Z}_m \times \mathbb{Z}_m \to \mathbb{Z}_m$ (die wir mit "$\cdot$" bezeichnen) wie folgt:*

$$\underbrace{\overline{a} + \overline{b}}_{\text{plus in } \mathbb{Z}_m} := \underbrace{\overline{a + b}}_{\text{plus in } \mathbb{Z}} \tag{2.1}$$

$$\underbrace{\overline{a} \cdot \overline{b}}_{\text{mal in } \mathbb{Z}_m} := \underbrace{\overline{a \cdot b}}_{\text{mal in } \mathbb{Z}} \tag{2.2}$$

2.2.1. Wohldefiniertheit. Für diese coole Einführung von Addition und Multiplikation in $\mathbb{Z}_m$ müssen wir aber noch zeigen, daß das alles auch *wohldefiniert* ist!. Denn unsere Definition bedeutet genau besehen folgendes:

> Seien $s, t \in \mathbb{Z}_m$ zwei Restklassen modulo m. Dann *wähle willkürlich* einen Repräsentanten $a \in s$ und einen Repräsentanten $b \in t$; die Summe bzw. das Produkt der Restklassen s und t ist dann definiert als die Restklasse, die $a + b$ bzw. $a \cdot b$ enthält.

Die Definition enthält also eine *willkürliche Wahl* (der *Repräsentanten* a und b): *Wohldefiniertheit* bedeutet, daß das Ergebnis der Addition *nicht* von dieser Wahl abhängt! Um das klarzumachen betrachten wir ein Beispiel.

BEISPIEL 2.2.2 (Nicht wohldefinierte zweistellige Verknüpfung). *Wir betrachten folgende "Definition´´ einer zweistelligen Verknüpfung $\odot$: $\mathbb{Z}_3 \times \mathbb{Z}_3 \to \mathbb{Z}_3$:*

$$\overline{a} \odot \overline{b} := \overline{|a| + |b|}.$$

Wir betrachten die Restklasse $s = 3 \cdot \mathbb{Z} + 1$ und $t = 3 \cdot \mathbb{Z} + 0$ in $\mathbb{Z}_3$. Klarerweise gilt $s = \overline{1} = \overline{-2}$ (d.h., beide Zahlen $1, -2 \in s$ sind mögliche *Repräsentanten von s) und $t = \overline{0}$. Was soll nun $s \odot t$ sein?*

- *Wählen wir $1 \in s$, $0 \in t$ als Repräsentanten, so ergibt sich: $s \odot t = \overline{1}$,*
- *Wählen wir $-2 \in s$, $0 \in t$ als Repräsentanten, so ergibt sich: $s \odot t = \overline{2}$.*

Es ist aber $\overline{1} \neq \overline{2}$ in $\mathbb{Z}_3$, die "Definition" ist also in Wahrheit sinnlos[1], *da* nicht wohldefiniert.

Die in Definition 2.2.1 erklärte Addition und Multiplikation *ist* aber wohldefiniert: Dazu zeigen wir, daß die jeweiligen Ergebnisse der Rechenoperationen *nicht* von der Wahl der Repräsentanten abhängen. Betrachte zwei *verschiedene* Repräsentanten a, a' bzw. b, b' *derselben* Restklassen in $\mathbb{Z}_m$:

$$\overline{a'} = \overline{a} \iff a' = a + \alpha \cdot m \text{ für ein } \alpha \in \mathbb{Z},$$

$$\overline{b'} = \overline{b} \iff b' = b + \beta \cdot m \text{ für ein } \beta \in \mathbb{Z}.$$

[1] Die vermeintliche *Funktion* $\mathbb{Z}_3 \times \mathbb{Z}_3 \to \mathbb{Z}_3$ hat ja für $(\overline{1}, \overline{0})$ keinen eindeutigen Wert!!

Dann ist

$$\overline{a'} + \overline{b'} = \overline{a' + b'} = \overline{a + b + \underbrace{(\alpha + \beta)}_{\in\mathbb{Z}} \cdot m} = \overline{a + b} = \overline{a} + \overline{b},$$

$$\overline{a'} \cdot \overline{b'} = \overline{a' \cdot b'} = \overline{a \cdot b + \underbrace{(\alpha \cdot b + \beta \cdot a + \alpha \cdot \beta \cdot m)}_{\in\mathbb{Z}} \cdot m} = \overline{a \cdot b} = \overline{a} \cdot \overline{b}.$$

2.2.2. Ringstruktur von $\mathbb{Z}_m$. Nun ist aber ganz schnell zu sehen, daß $\mathbb{Z}_m$ mit den in Definition 2.2.1 erklärten Rechenoperationen tatsächlich ein kommutativer Ring mit 1 ist: Zum Beispiel folgt aus der Definition 2.2.1 ganz offensichtlich, daß $\overline{0}$ bzw. $\overline{1}$ die neutralen Elemente bezüglich Addition bzw. Multiplikation sind, daß die Rechenoperationen assoziativ und kommutativ sind, und daß $\overline{-a}$ das additiv Inverse von $\overline{a}$ ist (also "$-\overline{a} = \overline{-a}$") — dazu braucht man die Gleichungen (2.1) bzw. (2.2) nur anzusehen! Schauen wir z.B. das Distributivgesetz an:

$$\begin{aligned}
\overline{a} \cdot \left(\overline{b} + \overline{c}\right) &= \overline{a} \cdot \overline{(b + c)} \quad \leftarrow (2.1) \\
&= \overline{a \cdot (b + c)} \quad \leftarrow (2.2) \\
&= \overline{a \cdot b + a \cdot c} \quad \leftarrow \text{Distributivgesetz in } \mathbb{Z} \\
&= \overline{a \cdot b} + \overline{a \cdot c} \quad \leftarrow (2.1) \\
&= \overline{a} \cdot \overline{b} + \overline{a} \cdot \overline{c} \quad \leftarrow (2.2)
\end{aligned}$$

BEISPIEL 2.2.3. *Wir geben die Additions– und Multiplikationstafel von $\mathbb{Z}_4$ an:*

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{0}$	$\overline{1}$	$\overline{2}$

$\cdot$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{0}$	$\overline{2}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

Sichtlich ist $\overline{2} \cdot \overline{2} = \overline{0}$; d.h., $\overline{2}$ ist ein Nullteiler*: $\mathbb{Z}_4$ ist also* kein *Integrationsbereich.*

Wir fassen zusammen:

SATZ 2.2.4 (Ringstruktur von $\mathbb{Z}_m$). *$(\mathbb{Z}_m, +, \cdot)$ ist ein kommutativer Ring mit* 1*. Er ist nullteilerfrei genau dann, wenn $m \in \mathbb{P}$.*

BEWEIS. Daß $\mathbb{Z}_m$ ein kommutativer Ring mit 1 ist, haben wir schon gesehen. Für die zusätzliche Aussage überlegen wir: Seien $a, b \in \mathbb{Z}$ beliebig.

$$\overline{0} = \overline{a} \cdot \overline{b} = \overline{a \cdot b}$$

ist gleichbedeutend mit

$$a \cdot b \equiv 0 \pmod{m} \iff m \mid a \cdot b.$$

Wenn daraus *immer* folgt

$$a \equiv 0 \pmod{m} \text{ oder } b \equiv 0 \pmod{m} \iff m \mid a \text{ oder } m \mid b$$

(das ist gleichbedeutend mit der Nullteilerfreiheit von $\mathbb{Z}_m$), dann ist das gemäß Satz 1.4.3 genau dann der Fall, wenn m eine Primzahl ist. □

2.3. Rechnen mit Kongruenzen

Das "Rechnen mit Kongruenzen" kann einfacher werden, wenn man aus den entsprechenden Restklassen möglichst geeignete (meistens: betragsmäßig kleine) Repräsentanten wählt. "Abstrakt" steckt da die "Wohldefiniertheit" dahinter:

BEOBACHTUNG 2.3.1. *Sei $m \in \mathbb{N}$, sei $n > 1 \in \mathbb{N}$. Dann gilt ja:*

$$a_i \equiv b_i \,(m) \iff \overline{a_i} = \overline{b_i} \text{ in } \mathbb{Z}_m \text{ für } i = 1, \ldots, n,$$

und daraus folgt wegen "Wohldefiniertheit"

$$\overline{\sum_i^n a_i} = \overline{\sum_i^n b_i} \text{ in } \mathbb{Z}_m \iff \sum_i^n a_i \equiv \sum_i^n b_i \pmod{m},$$

$$\overline{\prod_i^n a_i} = \overline{\prod_i^n b_i} \text{ in } \mathbb{Z}_m \iff \prod_i^n a_i \equiv \prod_i^n b_i \pmod{m}.$$

Daraus folgt insbesondere auch: Sei $p(x) := c_k \cdot x^k + c_{k-1} \cdot x^{k-1} + \cdots + c_1 \cdot x + c_0$ ein Polynom *mit ganzzahligen Koeffizienten (also $c_i \in \mathbb{Z}$ für $i = 0, 1, \ldots, k$), dann gilt:*

$$a \equiv b \pmod{m} \implies p(a) \equiv p(b) \pmod{m}.$$

Was das konkret an "Rechenvereinfachungen" bedeuten kann, macht man sich am besten an einem Beispiel klar:

BEISPIEL 2.3.2. *Was ist der Rest von* $23679871 \cdot 624323718$ *bzw. von* $23679871 + 624323718$ *bei Division durch* 5*? Um diese Frage zu beantworten, ist es* nicht *notwendig, die Multiplikation bzw. Addition der großen Zahlen durchzuführen, denn man kann "modulo* 5 *reduzieren":*

$$23679871 \equiv 1 \pmod{5}$$
$$624323718 \equiv 8 \equiv 3 \pmod{5},$$

also gilt:

$$23679871 \cdot 624323718 \equiv 1 \cdot 3 \equiv 3 \pmod{5},$$
$$23679871 + 624323718 \equiv 1 + 3 \equiv 4 \pmod{5}.$$

BEOBACHTUNG 2.3.3. *Weitere "Rechenregeln" für Kongruenzen sind:*

- $a \equiv b \pmod{m}$ *und* $k \mid m \implies a \equiv b \pmod{|k|}$*:*
  Denn $|k| \mid m \mid (a - b) \implies |k| \mid (a - b)$.
- $a \equiv b \pmod{m}$ *und* $k \in \mathbb{N} \implies k \cdot a \equiv k \cdot b \pmod{k \cdot m}$*:*
  Denn $(a - b) = m \cdot d \implies k \cdot (a - b) = (m \cdot k) \cdot d$.
- $k \cdot a \equiv k \cdot b \pmod{m}$ *und* $k \in \mathbb{N} \implies a \equiv b \pmod{\frac{m}{\mathrm{ggT}(m,k)}}$*:*
  Denn $k \cdot (a - b) = m \cdot d \implies \frac{k}{\mathrm{ggT}(m,k)} \cdot (a - b) = \frac{m}{\mathrm{ggT}(m,k)} \cdot d \implies \frac{m}{\mathrm{ggT}(m,k)} \mid (a - b)$ *gemäß* (1.19) *in Satz 1.3.39, weil* $\mathrm{ggT}\left(\frac{k}{\mathrm{ggT}(m,k)}, \frac{m}{\mathrm{ggT}(m,k)}\right) = 1$ *gemäß* (1.15).
- $k \cdot a \equiv k \cdot b \pmod{m}$ *und* $\mathrm{ggT}(k, m) = 1 \implies a \equiv b \pmod{m}$*:*
  Spezialfall der vorhergehenden "Rechenregel".

- $a \equiv b \pmod{m}$ *und* $a \equiv b \pmod{n} \implies a \equiv b \pmod{\operatorname{kgV}(m,n)}$*:* *Denn* $m, n \mid (a-b) \implies \operatorname{kgV}(m,n) \mid (a-b)$ *gemäß Korollar 1.3.25.*
- $a \equiv b \pmod{m}, a \equiv b \pmod{n}, \operatorname{ggT}(m,n) = 1 \implies a \equiv b \pmod{m \cdot n}$*:* *Spezialfall der vorhergehenden "Rechenregel", denn gemäß Korollar 1.4.13 gilt* $\operatorname{ggT}(m,n) = 1 \implies \operatorname{kgV}(m,n) = m \cdot n$*.*
- *Sei* $m \in \mathbb{N}$ *mit Primfaktorzerlegung* $m = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$*, dann gilt* $a \equiv b \pmod{m}$ *genau dann, wenn für alle* $i = 1, \ldots, k$ $a \equiv b \pmod{p_i^{\alpha_i}}$ *gilt:* *Denn* $p_i^{\alpha_i} \mid m \mid (a-b) \implies p_i^{\alpha_i} \mid (a-b)$*, und umgekehrt folgt aus* $p_1^{\alpha_1}, \ldots, p_k^{\alpha_k} \mid (a-b)$ *sofort* $\operatorname{kgV}\left(p_1^{\alpha_1}, \ldots, p_k^{\alpha_k}\right) \mid (a-b)$ *(Korollar 1.3.25), und* $\operatorname{kgV}\left(p_1^{\alpha_1}, \ldots, p_k^{\alpha_k}\right) = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ *(Korollar 1.4.14).*

Aufgabe 46: *Bestimme den Rest der folgenden Divisionen mit Rest mittels Kongruenzen:*

a) $2^3 \cdot 3^6 \cdot 7^3 \cdot 13 \cdot 17 : 11$ *b)* $9^2 \cdot 11 \cdot 37 \cdot 41 : 7$

2.4. Lineare Kongruenzen

DEFINITION 2.4.1 (lineare Kongruenz). *Sei* $m \in \mathbb{N}$ *und* $a, b \in \mathbb{Z}$*. Man bezeichnet die Gleichung* $a \cdot x \equiv b \pmod{m}$ *als* lineare Kongruenz*. Gesucht sind dabei zunächst* $x \in \mathbb{Z}$*, die als Lösung dieser Kongruenz auftreten: Aber für eine Lösung* $x \in \mathbb{Z}$ *ist* jeder *Repräsentant von* $\overline{x} \in \mathbb{Z}_m$ *ebenfalls eine Lösung; man interessiert sich daher nur für modulo* m inkongruente *Lösungen. Das könnte man "cooler" auch so ausdrücken: Man sucht nach Lösungen der Gleichung*

$$\overline{a} \cdot \overline{x} \equiv \overline{b} \text{ in } \mathbb{Z}_m \text{ (also nicht in } \mathbb{Z}!)$$

SATZ 2.4.2. *Seien* $m \in \mathbb{N}$ *und* $a, b \in \mathbb{Z}$*. Die lineare Kongruenz* $a \cdot x \equiv b \pmod{m}$ *ist genau dann lösbar, wenn* $\operatorname{ggT}(a,m) \mid b$*. Wenn* $\operatorname{ggT}(a,m) \mid b$ *gilt, dann existieren genau* $\operatorname{ggT}(a,m)$ modulo m inkongruente *Lösungen.*

BEWEIS. Sei $d := \operatorname{ggT}(a,m)$. Wenn es eine Lösung $x \in \mathbb{Z}$ gibt, so bedeutet dies: Es gibt ein $k \in \mathbb{Z}$, sodaß

$$a \cdot x - b = m \cdot k \iff b = a \cdot x - m \cdot k$$

gilt. Dann folgt aber aus $d \mid a, m$ sofort $d \mid b$.
Für die Umkehrung überlegen wir: Es gibt jedenfalls ganze Zahlen x', k' mit

$$d = x' \cdot a + k' \cdot m.$$

Wenn also $b = d \cdot e$ gilt für ein $e \in \mathbb{Z}$, dann ist $x := x' \cdot e$ eine Lösung:

$$b = d \cdot e = x \cdot a + \left(k' \cdot e\right) \cdot m.$$

Abschließend zeigen wir: Wenn x_0 eine Lösung der linearen Kongruenz $a \cdot x \equiv b \pmod{m}$ ist, dann sind mit $m = d \cdot c$ (also $c = \frac{m}{d} \in \mathbb{Z}$) *alle modulo* m *inkongruenten* Lösungen durch

$$x_0 + 0 \cdot c, x_0 + 1 \cdot c, \ldots, x_0 + (d-1) \cdot c$$

gegeben. Denn zunächst ist klar, daß diese Zahlen tatsächlich Lösungen *sind*, denn es gilt für alle $i \in \mathbb{Z}$:

$$a \cdot (x_0 + i \cdot c) = a \cdot x_0 + i \cdot a \cdot c = a \cdot x_0 + i \cdot \frac{a}{d} \cdot m \equiv a \cdot x_0 \equiv b \pmod{m}.$$

Weiters gilt

$$x_0 + i \cdot c \equiv x_0 + j \cdot c \pmod{m} \implies \underbrace{d \cdot c}_{m} \mid (i-j) \cdot c \implies d \mid (i-j),$$

und für $0 \leqslant i, j \leqslant d-1$ kann das nur dann gelten, wenn $i = j$: Die angegebenen Lösungen sind also *paarweise inkongruent*.

Sei schließlich y_0 *irgendeine andere* Lösung der linearen Kongruenz:

$$a \cdot x_0 \equiv a \cdot y_0 \equiv b \pmod{m} \implies m \mid a \cdot (y_0 - x_0) \implies \frac{m}{d} \mid \frac{a}{d} \cdot (y_0 - x_0),$$

also nach (1.19) in Satz 1.3.39

$$\frac{m}{d} \mid (y_0 - x_0) \implies y_0 - x_0 = j \cdot \frac{m}{d} \text{ für ein } j \in \mathbb{Z}.$$

Das bedeutet aber: *Jede* Lösung ist von der Gestalt $x_0 + j \cdot c$. □

BEISPIEL 2.4.3. *Wir suchen eine Lösung der linearen Kongruenz* $4 \cdot x \equiv 6 \pmod{14}$. *Da* $\operatorname{ggT}(4, 14) = 2$ *und* $2 \mid 6$ *wissen wir, daß die Gleichung lösbar ist. Der Euklidische Algorithmus liefert*

$$14 = 3 \cdot 4 + 2 \implies 2 = 14 - 3 \cdot 4.$$

Daraus ergibt sich sofort

$$6 = -9 \cdot 4 + 3 \cdot 14 \implies 6 = -9 \cdot 4 \pmod{14}.$$

-9 *ist also eine Lösung, und* $-9 + 14 = -2$ *ist eine dazu modulo* 14 kongruente *Lösung. Wir wissen, daß es noch eine zweite modulo* 14 inkongruente *Lösung gibt, nämlich*

$$5 + 1 \cdot \frac{14}{2} = 12.$$

Also: In $\mathbb{Z}_{14}$ *hat die Gleichung* $\overline{4} \cdot x = \overline{6}$ *genau die Lösungsmenge* $\{\overline{5}, \overline{-2}\}$.

Man kann die Lösungen aber auch ohne den Euklidischen Algorithmus finden; unter Verwendung der "Rechenregeln für Kongruenzen" (siehe Beobachtung 2.3.3):

$$\begin{aligned}
4 \cdot x \equiv 6 \pmod{14} &\iff 2 \cdot (2 \cdot x) \equiv 2 \cdot 3 \pmod{14} \\
&\iff 2 \cdot x \equiv 3 \pmod{7} \\
&\iff 2 \cdot x \equiv 3 + 7 = 10 = 2 \cdot 5 \pmod{7} \\
&\iff x \equiv 5 \pmod{7} \\
&\iff x \equiv 5 \pmod{14} \text{ oder } x \equiv 5 + 7 = 12 \pmod{14}.
\end{aligned}$$

Aufgabe 47: *Für welche* $a \in \mathbb{Z}$ *sind die folgenden linearen Kongruenzen lösbar?*

a) $11x \equiv a \pmod{80}$ *b)* $12x \equiv a \pmod{16}$ *c)* $3x \equiv 5 \pmod{a}$ *d)* $ax \equiv 11 \pmod{17}$

Aufgabe 48: *Löse die folgenden linearen Kongruenzen (soferne das möglich ist):*

a) $8 \cdot x \equiv 12 \pmod{19}$ *b)* $8 \cdot x \equiv 12 \pmod{160}$ *c)* $8 \cdot x \equiv 12 \pmod{28}$

2.4.1. Simultane lineare Kongruenzen und der Chinesische Restsatz.

DEFINITION 2.4.4 (simultane lineare Kongruenz). *Sei $k \in \mathbb{N}$, seien $m_1, \ldots, m_k \in \mathbb{N}$ und $b_1, \ldots, b_k \in \mathbb{Z}$. Das System von Kongruenzgleichungen*

$$\begin{aligned} x &\equiv b_1 \pmod{m_1} \\ x &\equiv b_2 \pmod{m_2} \\ &\vdots \\ x &\equiv b_k \pmod{m_k} \end{aligned} \tag{2.3}$$

heißt simultane lineare Kongruenz*: Gesucht sind $x \in \mathbb{Z}$, die alle k Kongruenzen erfüllen.*

BEMERKUNG 2.4.5. *Man würde vielleicht erwarten, daß ein System linearer Kongruenzgleichungen aus* allgemeineren *Kongruenzen der Gestalt*

$$a_i \cdot x \equiv b_i \pmod{m_i}$$

bestehen sollte, aber die spezielle Form (2.3) *(alle $a_i = 1$) ist keine echte Einschränkung: Denn wenn für eine der allgemeineren Gleichungen $d_i = \mathrm{ggT}(a_i, m_i) \nmid b_i$ gilt, dann gibt es ja* überhaupt *keine Lösung; andernfalls kann man jede der allgemeineren Gleichungen durch äquivalente Gleichungen*

$$a_i \cdot x \equiv b_i \pmod{m_i} \iff \frac{a_i}{d_i} x \equiv \frac{b_i}{d_i} \pmod{\frac{m_i}{d_i}}$$

ersetzen, und

$$\mathrm{ggT}\left(\frac{a_i}{d_i}, \frac{m_i}{d_i}\right) = 1 \implies 1 = c_i \cdot \frac{a_i}{d_i} + \lambda_i \cdot \frac{m_i}{d_i} \text{ für gewisse } c_i, \lambda_i \in \mathbb{Z}$$

bedeutet ja $1 \equiv c_i \cdot \frac{a_i}{d_i} \pmod{\frac{m_i}{d_i}}$, also

$$\frac{a_i}{d_i} x \equiv \frac{b_i}{d_i} \pmod{\frac{m_i}{d_i}} \iff x \equiv \frac{b_i}{d_i} \cdot c_i \pmod{\frac{m_i}{d_i}},$$

und diese äquivalenten Gleichungen sind von der speziellen Form (2.3)*.*

Die Gleichungen der speziellen Form (2.3) sind "einzeln" natürlich alle lösbar, dennoch kann das System der simultanen Kongruenzen insgesamt unlösbar sein, z.B. widersprechen die Kongruenzen

$$\begin{aligned} x &\equiv 1 \pmod{8} \\ x &\equiv 3 \pmod{4} \end{aligned}$$

einander, denn $x \equiv 3 \pmod 4 \iff x \equiv 3 \pmod 8$ oder $x \equiv 7 \pmod 8$: Solche widersprüchlichen Kongruenzen können nicht auftreten, wenn die Moduln $m_1, \ldots, m_k$ in (2.3) paarweise relativ prim sind:

SATZ 2.4.6 (Chinesischer Restsatz). *Sei $k \in \mathbb{N}$, seien $m_1, \ldots, m_k \in \mathbb{N}$ und $b_1, \ldots, b_k \in \mathbb{Z}$. Wenn $m_1, \ldots, m_k$ paarweise relativ prim sind, dann besitzen die simultanen Kongruenzen* (2.3) *modulo $m_1 \cdots m_k$ genau eine Lösung (d.h., für je zwei Lösungen x_1, x_2 gilt $x_1 \equiv x_2 \pmod{m_1 \cdots m_k}$).*

BEWEIS. Sei

$$M_i := m_1 \cdots \cancel{m_i} \cdots m_k = \frac{m_1 \cdots m_k}{m_i}.$$

Da die m_i paarweise relativ prim sind, ist ggT $(m_i, M_i) = 1$. Also gibt es für alle $i = 1, \ldots, k$ Zahlen $y_i, \lambda_i \in \mathbb{Z}$ mit

$$1 = y_i \cdot M_i + \lambda_i \cdot m_i,$$

und das heißt für alle $i = 1, \ldots, k$

$$1 \equiv y_i \cdot M_i \pmod{m_i}, \text{ aber } 0 \equiv y_j \cdot M_j \pmod{m_i} \text{ für } j \neq i.$$

Also ist

$$x = b_1 \cdot M_1 \cdot y_1 + \cdots + b_i \cdot M_i \cdot y_i + \cdots + b_k \cdot M_k \cdot y_k \equiv b_i \pmod{m_i}$$

eine Lösung der simultanen Kongruenz (2.3).
Wenn es eine zweite Lösung y gibt, dann folgt aus

$$m_1, \ldots, m_k \mid (x - y)$$

zunächst kgV $(m_1, \ldots, m_k) \mid (x - y)$. Aber kgV $(m_1, \ldots, m_k) = m_1 \cdots m_k$, weil die m_i paarweise relativ prim sind (siehe Korollar 1.4.14): Also gibt es *genau eine* modulo $m_1 \cdots m_k$ inkongruente Lösung. □

BEISPIEL 2.4.7. *Betrachte die simultane Kongruenz*

$$\begin{aligned} x &\equiv 2 \pmod 3 \\ x &\equiv 3 \pmod 5 \\ x &\equiv 2 \pmod 7 \end{aligned}$$

- *Verwende den Beweis von Satz 2.4.6:* $m_1 = 3, m_2 = 5, m_3 = 7$ *sind paarweise relativ prim. Setze* $M_1 = m_2 \cdot m_3 = 5 \cdot 7 = 35$, $M_2 = m_1 \cdot m_3 = 3 \cdot 7 = 21$, $M_3 = m_1 \cdot m_2 = 3 \cdot 5 = 15$ *und löse:*

$$\begin{array}{rl} 35 \cdot y_1 \equiv 1 & \pmod 3 \\ 2 \cdot y_1 \equiv 1 & \pmod 3 \\ 2 \cdot y_1 \equiv 4 & \pmod 3 \\ y_1 \equiv 2 & \pmod 3 \\ y_1 = 2 & \end{array} \qquad \begin{array}{rl} 21 \cdot y_2 \equiv 1 & \pmod 5 \\ y_2 \equiv 1 & \pmod 5 \\ y_2 = 1 & \end{array} \qquad \begin{array}{rl} 15 \cdot y_3 \equiv 1 & \pmod 7 \\ y_3 \equiv 1 & \pmod 7 \\ y_3 = 1 & \end{array}$$

Setze nun

$$x = b_1 \cdot M_1 \cdot y_1 + b_2 \cdot M_2 \cdot y_2 + b_3 \cdot M_3 \cdot y_3 = 2 \cdot 35 \cdot 2 + 3 \cdot 21 \cdot 1 + 2 \cdot 15 \cdot 1 = 233 \equiv 23 \pmod{105},$$

und 23 *ist offensichtlich eine Lösung.*

- *Die Lösung kann man aber auch durch sukzessives Einsetzen finden: Zunächst ist*

$$x \equiv 2 \pmod 3 \implies x = 2 + 3 \cdot t$$

für ein $t \in \mathbb{Z}$, *also*

$$2 + 3 \cdot t \equiv 3 \pmod 5 \iff 3 \cdot t \equiv 1 \equiv 6 \pmod 5 \implies t \equiv 2 \pmod 5,$$

also $t = 2 + 5 \cdot s$ *für ein* $s \in \mathbb{Z}$ *und somit* $x = 2 + 3 \cdot t = 2 + 3 \cdot (2 + 5 \cdot s) = 8 + 15 \cdot s$. *Nochmals einsetzen ergibt*

$$8 + 15 \cdot s \equiv 2 \pmod 7 \implies s \equiv -6 \equiv 1 \pmod 7 \implies s = 1 + 7 \cdot u,$$

also schließlich $x = 8 + 15 \cdot s = 23 + 105 \cdot u$.

Aufgabe 49: *Löse die folgenden simultanen Kongruenzen:*
a) $x \equiv 1 \pmod 7$, $x \equiv 4 \pmod 9$, $x \equiv 3 \pmod 5$,
b) $x \equiv 1 \pmod{20}$, $x \equiv 9 \pmod{21}$, $x \equiv 20 \pmod{23}$.

Aufgabe 50: *Finde alle modulo* $20 \cdot 21 \cdot 23$ *inkongruenten Lösungen des folgenden Systems:*

$$7 \cdot x \equiv 8 \pmod{20}, \quad 5 \cdot x \equiv -6 \pmod{21}, \quad 9 \cdot x \equiv 13 \pmod{23}.$$

2.5. Einheitengruppe in $\mathbb{Z}_m$: Prime Restklassen

DEFINITION 2.5.1 (Nullteiler und Einheiten). *Sei* $(R, +, \cdot)$ *ein kommutativer Ring mit* $\mathbf{1}$ *(der nicht der triviale Nullring ist, also* $\mathbf{0} \neq \mathbf{1}$*).*

Elemente $a, b \in R \setminus \{0\}$ *heißen Nullteiler, wenn* $a \cdot b = \mathbf{0}$.

Wenn es in R *keine Nullteiler gibt, wird* R Integritätsbereich *(oder* Integritätsring*) genannt.*

Ein $a \in R$ *heißt* Einheit, *wenn es ein* $b \in R$ *gibt mit* $a \cdot b = \mathbf{1}$ *gibt:* b *ist also das* inverse Element *zu* a *in bezug auf die Multiplikation*[2]. *Die Menge aller Einheiten von* R *wird* Einheitengruppe *von* R *genannt und mit* $R^\star$ *bezeichnet.*

Wir halten folgende Tatsachen fest:

BEOBACHTUNG 2.5.2. *Sei* R *ein kommutativer Ring mit* $\mathbf{1}$ *(nichttrivial, also* $\mathbf{1} \neq \mathbf{0}$*).*

- *Die Menge der Nullteiler von* R *und* $R^\star$ *sind disjunkt.*
- $(R^\star, \cdot)$ *ist eine* abelsche Gruppe.
- $(R, +, \cdot)$ *ist genau dann ein* Körper, *wenn* $R^\star = R \setminus \{\mathbf{0}\}$.

BEWEIS. Sei $x \in R^\star$ beliebig. Sei $b \in R$ mit $x \cdot b = \mathbf{0}$. Da $x \in R^\star$, gibt es definitionsgemäß ein multiplikatives Inverses x^{-1} von x, also $x^{-1} \cdot x = \mathbf{1}$. Daraus folgt aber $x^{-1} \cdot x \cdot b = x^{-1} \cdot \mathbf{0}$, also $b = \mathbf{0}$: x kann also kein Nullteiler sein.

$R^\star$ ist *abgeschlossen* unter der (assoziativen und kommutativen) Ringmultiplikation $\cdot$, denn für $x, y \in R^\star$, für die es *definitionsgemäß* inverse Elemente x^{-1}, y^{-1} gibt, ist auch $x \cdot y \in R^\star$:

$$(x \cdot y) \cdot \left(y^{-1} \cdot x^{-1}\right) = \mathbf{1} \text{ (d.h., } x \cdot y \text{ hat auch ein inverses Element).}$$

Klarerweise fungiert $\mathbf{1} \in R^\star$ als neutrales Element in $(R^\star, \cdot)$, und definitionsgemäß gibt es für jedes $x \in R^\star$ ein multiplikatives Inverses.

Ein kommutativer Ring mit $\mathbf{1}$ ist genau dann ein Körper, wenn jedes Element $x \neq \mathbf{0}$ ein multiplikatives Inverses hat. □

[2] Algebraisch ausgedrückt: a und b sind *invertierbare Elemente* in der *Halbgruppe* $(R, \cdot)$.

BEISPIEL 2.5.3. *Der Restklassenring* $\mathbb{Z}_6 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}\}$ *hat Nullteiler:* $\overline{2} \cdot \overline{3} = \overline{6} = \overline{0}$ *und* $\overline{4} \cdot \overline{3} = \overline{12} = 0$, *seine Einheitengruppe* $\mathbb{Z}_6^\star$ *ist* $\{\overline{1}, \overline{5}\}$, *da* $\overline{1} \cdot \overline{1} = \overline{1}$ *und* $\overline{5} \cdot \overline{5} = \overline{25} = \overline{1}$.

Für den Restklassenring $\mathbb{Z}_5 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}\}$ *sind hingegen alle Elemente* $\neq \mathbf{0}$ *Einheiten, denn* $\overline{1} \cdot \overline{1} = \overline{2} \cdot \overline{3} = \overline{4} \cdot \overline{4} = \overline{1}$*:* $\mathbb{Z}_5^\star = \mathbb{Z}_5 \backslash \{\mathbf{0}\}$*;* Z_5 *ist also ein Körper und enthält insbesondere keine Nullteiler.*

BEOBACHTUNG 2.5.4. *Sei* $m \in \mathbb{N}$, *dann gilt für alle* $a, b \in \mathbb{Z}$*:*

$$a \equiv b \pmod{m} \implies \mathrm{ggT}(a, m) = \mathrm{ggT}(b, m).$$

BEWEIS. Sei $d_a := \mathrm{ggT}(a, m)$ und $d_b := \mathrm{ggT}(b, m)$. Aus $a \equiv b \mod m$ folgt

$$b = a + k \cdot m \text{ für ein } k \in \mathbb{Z} \implies d_a \mid b \implies d_a \mid d_b$$

und ganz analog $d_b \mid d_a$, also $d_a = d_b$. □

DEFINITION 2.5.5 (prime Restklasse). *Sei* $m \in \mathbb{N}$ *und* $a \in \mathbb{Z}$. *Die Restklasse* $\overline{a} \in \mathbb{Z}_m$ *heißt* prime Restklasse*, wenn* $\mathrm{ggT}(a, m) = 1$. *(Das ist* wohldefiniert *nach Beobachtung 2.5.4.)*

SATZ 2.5.6. *Sei* $m \in \mathbb{N}$, $m > 1$. *Dann gilt für alle* $a \in \mathbb{Z}$*:*

$$\overline{a} \in \mathbb{Z}_m^\star \iff \overline{a} \text{ ist prime Restklasse in } \mathbb{Z}_m.$$

BEWEIS. Für $a \in \mathbb{Z}_m^\star$ gibt es *definitionsgemäß* eine Lösung der *linearen Kongruenz*

$$a \cdot x \equiv 1 \pmod{m},$$

und eine solche Lösung gibt es genau dann, wenn $\mathrm{ggT}(a, m) \mid 1$ (nach Satz 2.4.2), also $\mathrm{ggT}(a, m) = 1$. □

KOROLLAR 2.5.7. *Sei* $m \in \mathbb{N}$, $m > 1$*:* $\mathbb{Z}_m$ *ist genau dann ein Körper, wenn* $m \in \mathbb{P}$.

BEWEIS. Für $m \in \mathbb{P}$ sind alle Restklassen in $\mathbb{Z}_m \backslash \{\overline{0}\}$ *prim* und daher nach Satz 2.5.6 *invertierbar*: $\mathbb{Z}_m$ ist also ein *Körper*.

Für $m \notin \mathbb{P}$ gibt es ganze Zahlen $a, b > 1$ mit $m = a \cdot b$. Dann sind aber $\overline{a}, \overline{b}$ Nullteiler in $\mathbb{Z}_m$, denn $\overline{a} \cdot \overline{b} = \overline{a \cdot b} = \overline{m} = \overline{0}$: $\mathbb{Z}_m$ kann also kein Körper sein. □

DEFINITION 2.5.8 (prime Restklassengruppe). *Die abelsche Gruppe* $\mathbb{Z}_m^\star$ *(also die* Einheitengruppe *in* $\mathbb{Z}_m$*) heißt* prime Restklassengruppe *modulo* m.

SATZ 2.5.9 (Satz von Wilson). *Sei* $m \in \mathbb{N}, m > 1$, *dann gilt:*

$$m \in \mathbb{P} \iff (m-1)! \equiv -1 \pmod{m}.$$

BEWEIS. Die rechte Seite der Äquivalenz können wir in $\mathbb{Z}_m$ auch so schreiben:

$$\overline{1 \cdot 2 \cdots (m-1)} = \overline{1} \cdot \overline{2} \cdots \overline{m-1} = \prod_{\overline{a} \in \mathbb{Z}_m \backslash \{\overline{0}\}} \overline{a} = \overline{-1}.$$

Für die Richtung ($\implies$) beobachten wir zunächst, daß die Behauptung für $m = 2$ erfüllt ist:

$$1! = 1 \equiv -1 \pmod{2}.$$

Sei also $m \in \mathbb{P}$, $m > 2$. Dann ist $\mathbb{Z}_m$ ein Körper, also besitzen die Restklassen $\overline{1}, \overline{2}, \ldots, \overline{m-1}$ alle ein multiplikatives Inverses: $\mathbb{Z}_m \setminus \{\overline{0}\} = \mathbb{Z}_m^\star$. Wir müssen also zeigen:

$$\prod_{\overline{a} \in \mathbb{Z}_m^\star} \overline{a} = \overline{-1}. \tag{2.4}$$

Hier gilt $\overline{a}^{-1} = \overline{a}$ genau dann, wenn $\overline{a} = \overline{1}$ oder $\overline{a} = \overline{m-1} = \overline{-1}$:

$$\overline{a}^{-1} = \overline{a} \iff a^2 - 1 \equiv 0 \pmod{m} \iff m \mid (a+1) \cdot (a-1),$$

und das ist *äquivalent* (die nichttriviale Richtung folgt aus Satz 1.4.3) mit

$$m \mid a+1 \text{ oder } m \mid a-1,$$

was wiederum gleichbedeutend ist mit

$$\overline{a+1} = \overline{a} - \overline{-1} = \overline{0} \text{ oder } \overline{a-1} = \overline{a} - \overline{1} = \overline{0}.$$

$\mathbb{Z}_m^\star$ ist also eine Vereinigung von disjunkten Teilmengen

- $\{\overline{1}, \overline{-1}\}$,
- und $\frac{m-3}{2}$ *zweielementigen* Teilmengen von Elementen $\left\{\overline{a}, \overline{a^{-1}}\right\}$, deren Produkte natürlich *immer* $\overline{1}$ ergeben: $\overline{a} \cdot \overline{a^{-1}} = \overline{1}$.

Daraus folgt sofort (2.4).
Für die umgekehrte Richtung ($\Longleftarrow$) argumentieren wir:

$$m \notin \mathbb{P} \implies d \mid m \text{ für ein } d \in \mathbb{Z},\ 1 < d < m,$$

also $d \mid (m-1)!$ und $d \mid m$: Es kann dann aber nicht $m \mid (m-1)! + 1$ gelten, denn sonst würde $d \mid 1$ folgen; ein Widerspruch. □

Aufgabe 51: *Zeige: Für jede Primzahl $p \neq 2$ gilt* $1^2 \cdot 3^2 \cdot 5^2 \cdots (p-2)^2 \equiv (-1)^{(p+1)/2} \pmod{p}$.

Aufgabe 52: *Sei $n \in \mathbb{N}$. Zeige: Wenn $n > 4$ keine Primzahl ist, dann gilt* $(n-1)! \equiv 0 \pmod{n}$.

DEFINITION 2.5.10 (Ordnung einer Gruppe). *Sei $(G, \cdot)$ eine Gruppe. Die Anzahl $|G|$ der Elemente von G wird die* Ordnung *von G genannt und mit* ord (G) *bezeichnet.*

DEFINITION 2.5.11 (Eulersche φ-Funktion). *Die* Eulersche φ–Funktion $\mathbb{N} \to \mathbb{N}$ *ist defininert durch*

$$\varphi(m) = |\{k \in [m] : \ \mathrm{ggT}(k, m) = 1\}|.$$

Es ist also insbesondere $\varphi(1) = 1$. Für $m > 1$ folgt aus Satz 2.5.6 $\varphi(m) = |\mathbb{Z}_m^\star|$: $\varphi(m)$ ist also die Ordnung *der Einheitengruppe $\mathbb{Z}_m^\star$.*

LEMMA 2.5.12. *Sei $p \in \mathbb{P}$, $\alpha \in \mathbb{N}$. Dann ist $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1} = p^{\alpha-1} \cdot (p-1)$.*

BEWEIS. Von den p^α Zahlen

$$1, 2, \ldots, p^\alpha$$

sind *genau* die Vielfachen von p *nicht* relativ prim zu p^α, also die $p^{\alpha-1}$ Zahlen

$$1 \cdot p, 2 \cdot p, \ldots, \left(p^{\alpha-1} - 1\right) \cdot p, p^{\alpha-1} \cdot p.$$

Also ist die Anzahl der zu p^α relativ primen Zahlen in $[p^\alpha]$ genau $p^\alpha - p^{\alpha-1}$. □

DEFINITION 2.5.13 (vollständiges bzw. primes Restsystem modulo m). *Sei $m \in \mathbb{N}$.*
Eine m–elementige Teilmenge von $\mathbb{Z}$ heißt vollständiges Restsystem *modulo m, wenn sie aus* jeder *Restklasse genau ein Element enthält.*
Eine $\varphi(m)$–elementige Teilmenge von $\mathbb{Z}$ heißt primes Restsystem *modulo m, wenn sie aus* jeder primen *Restklasse genau ein Element enthält.*

Es ist klar:

BEOBACHTUNG 2.5.14. *$\{r_1, \ldots, r_m\}$ ist genau dann ein vollständiges Restklassensystem modulo m, wenn $r_i \not\equiv r_j \pmod{m}$ für alle $1 \leqslant i \neq j \leqslant m$ gilt.*
$\left\{r_1, \ldots, r_{\varphi(m)}\right\}$ ist genau dann ein primes Restklassensystem modulo m, wenn $r_i \not\equiv r_j \pmod{m}$ für alle $1 \leqslant i \neq j \leqslant \varphi(m)$ und $\operatorname{ggT}(r_i, m) = 1$ für $1 \leqslant i \leqslant \varphi(m)$ gilt.

SATZ 2.5.15. *Seien $m, n \in \mathbb{N}$ mit $\operatorname{ggT}(m, n) = 1$. Seien*

$$R := \left\{r_1, \ldots, r_{\varphi(m)}, r_{\varphi(m)+1}, \ldots, r_m\right\}$$
$$S := \left\{s_1, \ldots, s_{\varphi(n)}, s_{\varphi(n)+1}, \ldots, s_n\right\}$$

zwei vollständige *Restsysteme modulo m bzw. n, die zwei* prime *Restsysteme modulo m bzw. n als Teilmengen enthalten:*

$$R' := \left\{r_1, \ldots, r_{\varphi(m)}\right\} \subseteq R$$
$$S' := \left\{s_1, \ldots, s_{\varphi(n)}\right\} \subseteq S$$

Sei $a \in \mathbb{Z}$ mit $\operatorname{ggT}(a, m) = 1$. Dann ist

$$a \cdot R = \left\{a \cdot r_1, \ldots, a \cdot r_{\varphi(m)}, a \cdot r_{\varphi(m)+1}, \ldots, a \cdot r_m\right\}$$
$$a \cdot R' = \left\{a \cdot r_1, \ldots, a \cdot r_{\varphi(m)}\right\} \subseteq a \cdot R$$

ebenfalls ein vollständiges bzw. primes Restsystem modulo m.
Weiters ist

$$n \cdot R + m \cdot S := \left\{n \cdot r_i + m \cdot s_j \colon\ 1 \leqslant i \leqslant m, 1 \leqslant j \leqslant n\right\}$$
$$n \cdot R' + m \cdot S' := \left\{n \cdot r_i + m \cdot s_j \colon\ 1 \leqslant i \leqslant \varphi(m), 1 \leqslant j \leqslant \varphi(n)\right\}$$

ein vollständiges bzw. primes Restsystem modulo $m \cdot n$.

BEWEIS. Alle Elemente in $a \cdot R$ sind paarweise verschieden modulo m (und daher auch alle Elemente aus $a \cdot R' \subseteq a \cdot R$), denn aus $a \in \mathbb{Z}_m^\star$ folgt $a \cdot r_i \not\equiv a \cdot r_j \pmod{m}$ für $1 \leqslant i \neq j \leqslant m$: Also ist $a \cdot R$ ein vollständiges Restsystem modulo m.
Außerdem folgt aus $\operatorname{ggT}(r_i, m) = \operatorname{ggT}(a, m) = 1$ auch $\operatorname{ggT}(a \cdot r_i, m) = 1$: Also ist $a \cdot R'$ ein primes Restsystem modulo m.
Es sind aber auch alle Elemente in $n \cdot R + m \cdot S$ (und daher auch alle Elemente aus $n \cdot R' + m \cdot S' \subseteq n \cdot R + m \cdot S$) paarweise verschieden modulo $m \cdot n$: Denn aus

$$n \cdot r_i + m \cdot s_k \equiv n \cdot r_j + m \cdot s_l \pmod{m \cdot n}$$

folgen

$$n \cdot r_i + m \cdot s_k \equiv n \cdot r_j + m \cdot s_l \pmod{m} \text{ und } n \cdot r_i + m \cdot s_k \equiv n \cdot r_j + m \cdot s_l \pmod{n},$$

und daraus folgt

$$\begin{aligned} n \cdot r_i \equiv n \cdot r_j \pmod{m} &\implies r_i \equiv r_j \pmod{m} \leftarrow \text{ggT}(m,n)=1, \\ m \cdot s_k \equiv m \cdot s_l \pmod{n} &\implies s_k \equiv s_l \pmod{n} \leftarrow \text{ggT}(m,n)=1, \end{aligned}$$

und daher gilt $r_i = r_j$ und $s_k = s_l$. Also ist $n \cdot R + m \cdot S$ ein vollständiges Restsystem modulo $m \cdot n$.
Wir müssen noch zeigen:

$$\begin{aligned} x \in \left(n \cdot R' + m \cdot S'\right) &\implies \text{ggT}\,(x, m \cdot n) = 1, \\ y \in (n \cdot R + m \cdot S) \setminus \left(n \cdot R' + m \cdot S'\right) &\implies \text{ggT}\,(y, m \cdot n) > 1. \end{aligned}$$

Sei $x = n \cdot r_i + m \cdot s_j \in (n \cdot R' + m \cdot S')$: Wenn es eine Primzahl $p \in \mathbb{P}$ gibt mit $p \mid x$ und $p \mid m \cdot n$, dann folgt $p \mid m$ oder $p \mid n$. Es gelte o.B.d.A. $p \mid n$, dann folgt aber auch $p \mid m \cdot s_j$, und aus $\text{ggT}\,(m,n) = 1$ folgt $p \nmid m$, also muß $p \mid s_j$ gelten, und daraus folgt $p \mid \text{ggT}\left(n, s_j\right)$, ein Widerspruch: Denn $s_j \in S' \implies \text{ggT}\left(n, s_j\right) = 1$.
Sei $y = n \cdot r_i + m \cdot s_j \in (n \cdot R + m \cdot S) \setminus (n \cdot R' + m \cdot S')$. Sei o.B.d.A. $s_j \in S \setminus S'$, also $\text{ggT}\left(s_j, n\right) > 1$. Dann gibt es eine Primzahl $p \in \mathbb{P}$ mit

$$p \mid s_j, n \implies p \mid y, m \cdot n \implies p \mid \text{ggT}\,(y, m \cdot n)\,.$$

Also ist $n \cdot R' + m \cdot S'$ ein primes Restsystem modulo $m \cdot n$. □

Aus dem Satz ergibt sich sofort:

KOROLLAR 2.5.16. *Wenn $m, n \in \mathbb{N}$ und $\text{ggT}\,(m,n) = 1$, dann gilt $\varphi\,(m \cdot n) = \varphi\,(m) \cdot \varphi\,(n)$.* □

KOROLLAR 2.5.17. *Sei $m \in \mathbb{N}$ mit Primfaktorzerlegung $m = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$. Dann gilt:*

$$\begin{aligned} \varphi\,(m) &= \left(p_1^{\alpha_1} - p_1^{\alpha_1 - 1}\right) \cdots \left(p_k^{\alpha_k} - p_k^{\alpha_k - 1}\right) \qquad (2.5) \\ &= \left(\prod_{i=1}^{k} p_i^{\alpha_i}\right) \cdot \left(\prod_{i=1}^{k} \left(1 - \frac{1}{p_i}\right)\right) \\ &= m \cdot \prod_{p \mid m} \left(1 - \frac{1}{p}\right) \end{aligned}$$

BEWEIS. Aus Korollar 2.5.16 folgt mit Induktion nach k:

$$\varphi\,(m) = \varphi\left(p_1^{\alpha_1}\right) \cdots \varphi\left(p_k^{\alpha_k}\right).$$

Gleichung (2.5) ergibt sich also sofort aus Lemma 2.5.12. (Die restlichen Gleichungen sind einfache Umformungen). □

Aufgabe 53: *Eine unbewiesene Vermutung über die Eulersche φ-Funktion besagt: Zu jedem $m \in \mathbb{N}$ gibt es ein $n \in \mathbb{N}$ mit $n \neq m$ und $\varphi(n) = \varphi(m)$. Zeige diese Vermutung für ungerades m.*

Aufgabe 54: *Zeige: Zu jedem $m \in \mathbb{N}$ gibt es nur endlich viele $n \in \mathbb{N}$ mit der Eigenschaft $\varphi(n) = m$.*

Aufgabe 55: *Zeige für $k, \ell \in \mathbb{N}$: Wenn $k \mid \ell$ dann $\varphi(k) \mid \varphi(\ell)$.*

Aufgabe 56: *Seien $m, n \in \mathbb{N}$, sei $d = \mathrm{ggT}(m, n)$. Zeige:*

$$\varphi(m \cdot n) = \varphi(m) \cdot \varphi(n) \cdot \frac{d}{\varphi(d)}.$$

DEFINITION 2.5.18 (Ordnung eines Gruppenelements). *Sei $(G, \cdot)$ eine Gruppe mit neutralem Element $\mathbb{n}_G$, sei $a \in G$. Betrachte die Menge*

$$M := \left\{ j \in \mathbb{N} \colon\ a^j = \mathbb{n}_G \right\} \subseteq \mathbb{N}.$$

Dann ist die Ordnung *von a gleich*

$$\mathrm{ord}(a) = \begin{cases} \min M & \text{wenn } M \neq \varnothing, \\ \infty & \text{wenn } M = \varnothing. \end{cases}$$

(Die Ordnung eines Elementes a ist also die kleinste *Potenz a^j, für die $a^j = \mathbb{n}_G$ gilt.)*

LEMMA 2.5.19. *Sei $(G, \cdot)$ eine Gruppe mit neutralem Element $\mathbb{n}_G$, sei $a \in G$ mit endlicher Ordnung. Dann gilt:*

$$a^n = \mathbb{n}_G \in G \iff \mathrm{ord}(a) \mid n.$$

BEWEIS. Sei $m := \mathrm{ord}(a) \in \mathbb{N}$. Die Richtung ($\Longleftarrow$) ist klar:

$$n = d \cdot m \implies a^n = (a^m)^d = \mathbb{n}_G^d = \mathbb{n}_G.$$

Für die Richtung ($\Longrightarrow$) führen Division mit Rest durch:

$$n = q \cdot m + r \text{ mit } 0 \leqslant r < m.$$

Dann ist

$$\mathbb{n}_G = a^n = (a^m)^q \cdot a^r = a^r \ \leftarrow \text{denn } a^m = \mathbb{n}_G.$$

Nach Definition der Ordnung eines Gruppenelements gilt aber

$$a^r = \mathbb{n}_G \implies r \geqslant m \text{ oder } r \notin \mathbb{N}.$$

Es muß also $r \notin \mathbb{N}$ gelten, also $r = 0 \implies n = q \cdot m$. □

BEOBACHTUNG 2.5.20. *Sei $(G, \cdot)$ eine Gruppe, sei $a \in G$. Dann bildet die Menge*

$$\langle a \rangle := \left\{ a^k \colon\ k \in \mathbb{Z} \right\} \subseteq G$$

selbst eine Gruppe mit Multiplikation

$$a^i \cdot a^j = a^{i+j},$$

neutralem Element $a^0 = \mathbb{n}_G$ und inversem Element $\left(a^i\right)^{-1} = a^{-i}$. Also ist $\langle a \rangle$ eine Untergruppe *von G, ihre Ordnung ist gleich* $\mathrm{ord}(a)$*: Wenn diese Ordnung* endlich *ist, also* $\mathrm{ord}(a) = m \in \mathbb{N}$*, dann entspricht die* Multiplikation *in $\langle a \rangle$ der* Addition *in $\mathbb{Z}_m$, in folgendem Sinn: Die Abbildung*

$$\psi \colon\ \langle a \rangle \to \mathbb{Z}_m,\ a^i \mapsto \overline{i}$$

ist wohldefiniert, *denn*

$$a^i = a^j \iff a^{i-j} = \mathbb{n}_G \iff m \mid (i-j) \iff \overline{i} = \overline{j}. \ \leftarrow \textit{gemäß Lemma 2.5.19}$$

Aus dieser Kette von Äquivalenzen ergibt sich auch sofort, daß ψ bijektiv *ist, denn* surjektiv *ist ja klar, und* injektiv *folgt aus*

$$\psi\left(a^j\right) = \psi\left(a^i\right) \iff \overline{j} = \overline{i} \iff a^i = a^j,$$

und ψ *"übersetzt Multiplikation in Addition*[3]*":*

$$\underbrace{a^i \cdot a^j}_{\text{mult. in } \langle a\rangle} = a^{i+j} \mapsto \overline{i+j} = \underbrace{\overline{i} + \overline{j}}_{\text{add. in } \mathbb{Z}_m}.$$

BEISPIEL 2.5.21. *Die prime Restklassengruppe*

$$\mathbb{Z}_{15}^\star = \left\{\overline{1}, \overline{2}, \overline{4}, \overline{7}, \overline{8}, \overline{11}, \overline{13}, \overline{14}\right\}$$

(deren neutrales Element die Restklasse $\overline{1} \in \mathbb{Z}_{15}$ *ist) enthält das Element* $a = \overline{2}$*, und es gilt*

$$\langle a\rangle = \left\{a, a^2, a^3, a^4\right\} = \left\{\overline{2}, \overline{4}, \overline{8}, \overline{16} = \overline{1}\right\}.$$

Es ist also offensichtlich $\operatorname{ord} a = 4$*, und die Multiplikation in* $\langle a\rangle$ *"übersetzt sich" in die Addition in* $\mathbb{Z}_4$ *durch die Abbildung*

$$a = a^1 \mapsto \overline{1}, a^2 \mapsto \overline{2}, a^3 \mapsto \overline{3}, a^4 = a^0 \mapsto \overline{0}.$$

PROPOSITION 2.5.22. *Sei* $G = (G, \cdot)$ *eine Gruppe und* $H \sqsubseteq G$ *eine Untergruppe von* G *(also eine Teilmenge, die selbst die Struktur einer Gruppe hat). Dann ist die Menge von Teilmengen ("Blöcken")*

$$\{g \cdot H \colon\ g \in G\}$$

eine Partition[4] *von* G*, deren Blöcke*[5] *alle* dieselbe Mächtigkeit *haben.*

BEWEIS. Klarerweise ist

$$G = \bigcup_{g \in G} g \cdot H.$$

Ebenso klar ist, daß jeder Block $g \cdot H$ nicht leer ist (denn $g \in g \cdot H$).
Zu zeigen ist also noch, daß zwei *verschiedene* Blöcke *disjunkt* sind:

$$z \in (a \cdot H) \cap (b \cdot H) \implies z = a \cdot x = b \cdot y \text{ für gewisse } x, y \in H.$$

Das heißt:

$$a = b \cdot \underbrace{y \cdot x^{-1}}_{\in H} \implies a \cdot h = b \cdot \underbrace{y \cdot x^{-1} \cdot h}_{\in H} \text{ für alle } h \in H \implies a \cdot H \subseteq b \cdot H,$$

und genauso erhält man auch $b \cdot H \subseteq a \cdot H$: Wenn Blöcke nicht disjunkt sind, dann sind sie überhaupt gleich. Also ist $\{g \cdot H \colon\ g \in G\}$ tatsächlich eine Partition von G.
Die Abbildung

$$\phi_g \colon\ H \to g \cdot H,\ x \mapsto g \cdot x \text{ für } x \in H$$

[3] In der Sprache der Algebra: ψ ist ein *Isomorphismus* zwischen $\langle a\rangle$ und $\mathbb{Z}_m$.

[4] Achtung: Es kann $g \cdot H = g' \cdot H$ gelten für $g \neq g'$; der Block $g \cdot H$ wird aber nur *einmal* gezählt!

[5] Diese Blöcke heißen auch *Linksnebenklassen* von H.

ist eine *Bijektion*, denn ihre Umkehrabbildung ist einfach

$$\phi_g^{-1}\colon\ g \cdot H \to H,\ y \mapsto g^{-1} \cdot y \text{ für } y \in g \cdot H.$$

Also sind alle Blöcke gleichmächtig. □

BEISPIEL 2.5.23. *Wie wir gesehen haben, enthält die Gruppe $G = \mathbb{Z}_{15}^\star$ eine Untergruppe H der Ordnung 4, nämlich*

$$H = \left\langle \overline{2} \right\rangle.$$

Die 2 Blöcke der Partition

$$\{g \cdot H\colon\ g \in G\}$$

sind hier:

$$\overline{1} \cdot H = \overline{2} \cdot H = \overline{4} \cdot H = \overline{8} \cdot H = \left\{\overline{2}, \overline{4}, \overline{8}, \overline{1}\right\},$$
$$\overline{7} \cdot H = \overline{11} \cdot H = \overline{13} \cdot H = \overline{14} \cdot H = \left\{\overline{7}, \overline{11}, \overline{13}, \overline{14}\right\}.$$

KOROLLAR 2.5.24. *Sei $(G, \cdot)$ eine endliche Gruppe,* $\operatorname{ord}(G) = |G| = n \in \mathbb{N}$, *mit neutralem Element $\mathbb{n}_G$. Dann gilt für jede Untergruppe $H \sqsubseteq G$*

$$\operatorname{ord}(H) \mid \operatorname{ord}(G). \tag{2.6}$$

Insbesondere gilt für alle $a \in G$

$$\operatorname{ord}(a) \mid \operatorname{ord}(G), \tag{2.7}$$

und daraus folgt weiters

$$a^{\operatorname{ord}(G)} = \mathbb{n}_G. \tag{2.8}$$

BEWEIS. Gleichung (2.6) folgt sofort aus Proposition 2.5.22, Gleichung (2.7) folgt aus der Spezialisierung $H = \langle a \rangle$, und Gleichung (2.8) ergibt sich sofort aus (2.7)

$$a^{\operatorname{ord}(G)} = a^{\operatorname{ord}(a) \cdot k} = \left(a^{\operatorname{ord}(a)}\right)^k = \mathbb{n}_G^k = \mathbb{n}_G.$$

□

Aus diesen "abstrakt–algebraischen" Resultaten folgen sofort:

KOROLLAR 2.5.25 (Euler). *Sei $m \in \mathbb{N}, a \in \mathbb{Z}$ und* $\operatorname{ggT}(a, m) = 1$. *Dann gilt $a^{\varphi(m)} \equiv 1 \pmod{m}$.*

BEWEIS. Folgt sofort aus Gleichung (2.8) durch Spezialisierung $G = \mathbb{Z}_m^\star$ (mit neutralem Element $\overline{1}$ und $\operatorname{ord}(G) = \varphi(m)$) in Korollar 2.5.24:

$$\overline{a}^{\operatorname{ord}(G)} = \overline{1}.$$ □

KOROLLAR 2.5.26 (Kleiner Satz von Fermat). *Sei $p \in \mathbb{P}$, dann gilt für alle $a \in \mathbb{Z}$ mit $p \nmid a$*

$$a^{p-1} \equiv 1 \pmod{p}. \tag{2.9}$$

Für alle $a \in \mathbb{Z}$ gilt

$$a^p \equiv a \pmod{p}. \tag{2.10}$$

BEWEIS. Gleichung (2.9) folgt aus Korollar 2.5.25 durch Spezialisierung $m = p \in \mathbb{P}$ mit $\varphi(p) = p - 1$. Gleichung (2.10) ist für alle $a \in \mathbb{Z}$ mit $p \nmid a$ eine direkte Folgerung aus (2.9), für $p \mid a$ ist sie trivialerweise richtig. □

KAPITEL 3

p–adische (p–äre) Ziffernentwicklung

Wir sind es von Kindesbeinen an gewohnt, Zahlen im *Dezimalsystem* zu bezeichnen (und zwar mit arabischen Ziffern), sodaß wir vielleicht geneigt sind, die *Zahlen* mit diesen *Bezeichnungen* zu identifizieren. Aber diese Bezeichnungen sind keineswegs "naturgegeben": Z.B. erweist sich das *Binärsystem* (siehe Abbildung 1) für die Computerwissenschaft als viel geeigneter.

Wir wollen hier zunächst einmal betrachten, was unser "gewohntes" Zahlensystem (Dezimalzahlen) eigentlich bedeutet, und diese Überlegungen dann verallgemeinern.

3.1. Dezimalbruchentwicklung einer reellen Zahl

Sei $z \in \mathbb{R}$ eine reelle Zahl mit $z \geqslant 0$. Wir setzen

$$X := \lfloor z \rfloor \in \mathbb{N}_0 \text{ (d.h., } X \text{ ist der ganzzahlige Anteil von } z),$$
$$x := z - X \in [0,1) \text{ (d.h., } x \text{ ist der nicht–ganzzahlige Anteil von } z)$$

und schreiben z dann als

$$z = X + x, \tag{3.1}$$

wobei also

$$X \in \mathbb{N}_0 \text{ und } 0 \leqslant x < 1 \tag{3.2}$$

gilt.

3.1.1. Dezimalentwicklung einer nichtnegativen ganzen Zahl. Die Folge

$$(10^n)_{n=0}^{\infty} = (1, 10, 100, \dots)$$

wächst *unbeschränkt*, es gibt also (mindestens) ein $k \in \mathbb{N}_0$ sodaß $X < 10^k$: Die Menge aller derartigen $k \in \mathbb{N}_0$

$$\varnothing \neq \left\{ k \in \mathbb{N}_0 \colon \ X < 10^k \right\} \subseteq \mathbb{N}_0 \tag{3.3}$$

hat ein kleinstes Element[1], das wir mit m bezeichnen.

Wenn m gleich 0 ist, dann ist $X < 10^0 = 1$ und daher $X = 0$; andernfalls gilt für m:

$$10^{m-1} \leqslant X < 10^m. \tag{3.4}$$

Nun können wir X mit folgendem Algorithmus als Zahl im *Dezimalsystem* (auch *dekadisches System* oder *Zehnersystem* genannt) schreiben:

[1] Denn $\mathbb{N}_0$ ist *wohlgeordnet*.

/* Bestimme $m \in \mathbb{N}$, sodaß $10^{m-1} \leqslant X < 10^m$ */
$Y \leftarrow X$
$k \leftarrow m-1$
/* Ab hier gilt IMMER: $Y < 10^{k+1}$ */
while $k \geqslant 0$ **do**
  $Y = 10^k \cdot q + r$ /* Division mit Rest durch 10^k: $0 \leqslant q < 9$ */
  $c_k \leftarrow q$ /* Die '10^k-er-Ziffer' ist c_k */
  $Y \leftarrow Y - c_k \cdot 10^k$ /* Also $Y = r$, insbesondere: $Y < 10^k$ */
  $k \leftarrow k-1$ /* Also wieder: $Y < 10^{k+1}$ */
end while/* An dieser Stelle ist $Y = 0$ */
return $(c_0, c_1, \ldots, c_{m-1})$

Dieser Algorithmus bricht (klarerweise) nach m Schritten ab, und liefert die folgende Entwicklung von X:

$$X = c_{m-1} \cdot 10^{m-1} + c_{m-2} \cdot 10^{m-2} + \cdots + c_1 \cdot 10^1 + c_0 \cdot 10^0. \tag{3.5}$$

Wenn wir voraussetzen, daß für alle k mit $0 \leqslant k \leqslant m-1$ $c_k \in \{0, 1, \ldots, 9\}$ und $c_{m-1} \neq 0$ gilt, dann ist diese Darstellung *eindeutig*: Denn sei

$$X = b_{n-1} \cdot 10^{n-1} + b_{n-2} \cdot 10^{n-2} + \cdots + b_1 \cdot 10^1 + b_0 \cdot 10^0$$

eine *andere* Darstellung mit $b_k \in \{0, 1, \ldots, 9\}$ und $b_{n-1} \neq 0$, dann ist zunächst $X \geqslant 10^{n-1}$. Andrerseits ist

$$\begin{aligned} X &\leqslant 9 \cdot 10^{n-1} + 9 \cdot 10^{n-2} + \cdots + 9 \cdot 10^1 + 9 \cdot 10^0 \\ &= 9 \cdot \sum_{k=0}^{n-1} 10^k = 9 \cdot \frac{10^n - 1}{10 - 1} = 10^n - 1 < 10^n, \quad \leftarrow \text{Geometrische Reihe} \end{aligned}$$

also

$$10^{n-1} \leqslant X < 10^n \implies n = m.$$

Sei nun i, $0 \leqslant i \leqslant m-1$, der *größte* Index mit $c_i \neq b_i$, o.B.d.A. gelte $c_i > b_i$. Dann wäre also

$$X - X = \sum_{k=0}^{i} (b_k - c_k) \cdot 10^k = 0$$

und daher

$$10^i \leqslant \underbrace{(c_i - b_i)}_{>0} \cdot 10^i = \sum_{k=0}^{i-1} (b_k - c_k) \cdot 10^k \leqslant 9 \cdot \sum_{k=0}^{i-1} 10^k = 10^i - 1,$$

ein Widerspruch: Also gilt $c_i = b_i$ für alle i, $0 \leqslant i \leqslant m-1$. Wie gewohnt, schreiben wir die Summe (3.5) abkürzend als Folge (Ziffernfolge) ihrer Koeffizienten:

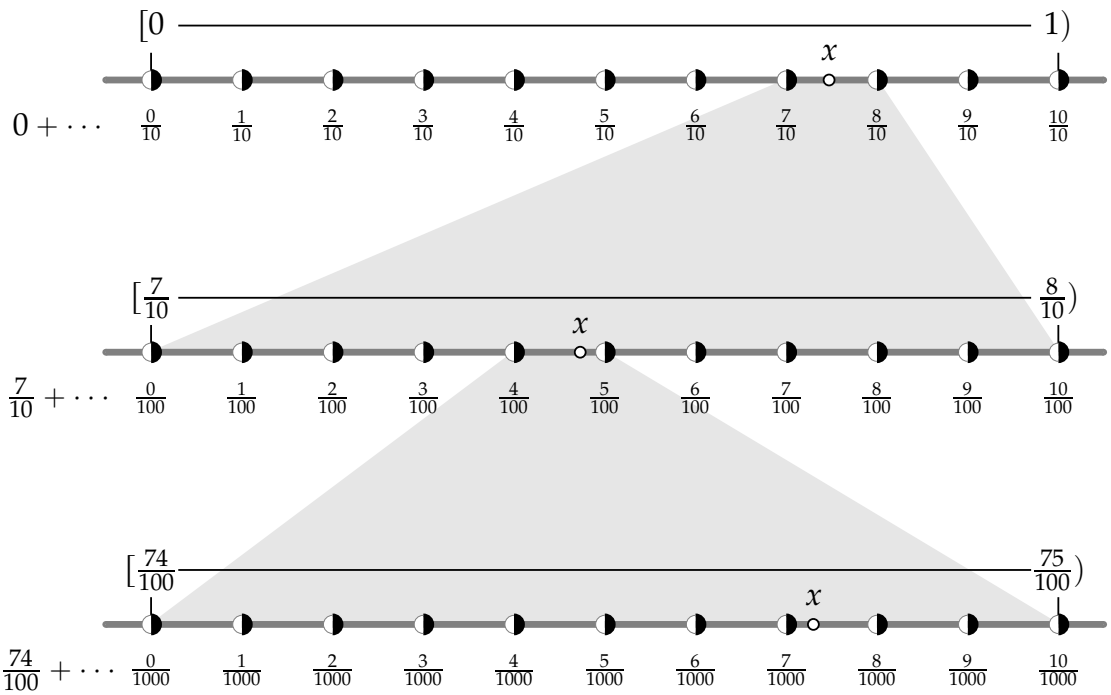
$$X = c_{m-1} c_{m-2} \ldots c_1 c_0$$

3.1.2. Dezimalentwicklung einer reellen Zahl $x \in [0,1)$. Nun wenden wir uns dem nicht–ganzzahligen Anteil $x \in [0,1)$ zu. Der folgende Algorithmus entwickelt x im Dezimalsystem:

$Y \leftarrow x$
$k \leftarrow 1$
$s_0 \leftarrow 0$
`/* Ab hier gilt IMMER:` $0 \leqslant Y < 1 \iff 0 \leqslant 10 \cdot Y < 10$ `*/`
while $Y \neq 0$ **do**
  $d_k \leftarrow \lfloor 10 \cdot Y \rfloor$ `/* Die '`10^{-k}`-er-Ziffer' ist` d_k, $0 \leqslant d_k \leqslant 9$ `*/`
  $Y \leftarrow 10 \cdot Y - d_k$ `/* Also wieder` $0 \leqslant Y < 1$ `*/`
  $s_k \leftarrow s_{k-1} + d_k \cdot 10^{-k}$ `/* Es gilt` $0 \leqslant x - s_k = Y \cdot 10^{-k} < 10^{-k}$ `*/`
  $k \leftarrow k + 1$
end while`/* Wenn diese Stelle erreicht wird, ist` $Y = 0$ `*/`
return $(d_0, d_1, \dots)$

Dieser Algorithmus muß im allgemeinen *nicht* abbrechen. Wenn man sich die Zahl x als einen Punkt auf der Zahlengerade vorstellt, kann man das Verfahren gut graphisch illustrieren, siehe Abbildung 1: Dort "sieht" man, wie der Algorithmus funktioniert.

ABBILDUNG 1. Illustration der ersten drei Schritte in der Dezimalbruchentwicklung für die Zahl $x = 0.7473$.



Insbesondere liefert der Algorithmus im k–ten Schritt die Teilsumme

$$s_k = \frac{d_1}{10} + \frac{d_2}{100} + \cdots + \frac{d_k}{10^k},$$

und da $|d_i| \leqslant 9$ für alle i gilt, ist die Reihe

$$\sum_{i=1}^{\infty} d_i \cdot \frac{1}{10^i} \leqslant 9 \cdot \sum_{i=1}^{\infty} \frac{1}{10^i} = 9 \cdot \left(\frac{1}{1 - \frac{1}{10}} - 1 \right) = 1$$

konvergent (*Majorantenkriterium* und *geometrische Reihe*). Weiters gilt

$$0 \leqslant x - s_k < 10^{-k} \text{ für alle } k,$$

also ist

$$\sum_{i=1}^{\infty} d_i \cdot \frac{1}{10^i} = \lim_{k \to \infty} s_k = x. \tag{3.6}$$

Wie gewohnt, schreiben wir die unendliche Reihe (3.6) abkürzend als Folge (Ziffernfolge: *Dezimalbruch*) ihrer Koeffizienten:

$$x = 0\,.\,d_1 d_3 d_3 \ldots$$

Aus dem Algorithmus sehen wir

$$d_{k+1} \cdot 10^{-k-1} + d_{k+2} \cdot 10^{-k-2} + \cdots = x - s_k < 10^{-k}.$$

In Verbindung mit

$$9 \cdot 10^{-k-1} + 9 \cdot 10^{-k-2} + \cdots = 9 \cdot 10^{-k-1} \sum_{i=0}^{\infty} 10^{-i} = \frac{9}{10^{k+1} \left(1 - \frac{1}{10}\right)} = 10^{-k}$$

ergibt sich daraus: Der Algorithmus liefert *niemals* eine Zahlenfolge für x, in der $d_i = 9$ gilt für alle i ab einem gewissen k. Insbesondere liefert der Algorithmus also *niemals* die (an sich richtige!) Darstellung

$$1 = 9 \cdot \sum_{i=1}^{\infty} \left(\frac{1}{10} \right)^i,$$

die der nicht–abbrechenden Dezimalbruchentwicklung

$$1.0 = 0.999999999999999 \ldots$$

entspricht. Aber abgesehen von dieser Einschränkung

$$\text{es gibt kein } k \in \mathbb{N}\colon \;\; d_i = 9 \text{ für alle } i > k \tag{3.7}$$

können *alle* Zahlenfolgen als Dezimalbruchentwicklungen auftreten; und diese Entwicklung ist unter dieser Einschränkung *eindeutig*. Denn sei

$$\sum_{i=1}^{\infty} \frac{a_i}{10^i} = \sum_{i=1}^{\infty} \frac{b_i}{10^i}$$

für zwei Ziffernfolgen $(a_i)_{i=1}^{\infty}$ und $(b_i)_{i=1}^{\infty}$, die beide der Einschränkung (3.7) genügen: Angenommen, die Menge $M = \{i \in \mathbb{N}\colon \; a_i \neq b_i\}$ ist nicht leer, dann sei $n = \min(M)$. O.B.d.A. können wir $a_n > b_n$ annehmen, dann haben wir

$$\frac{1}{10^n} \leqslant \frac{a_n - b_n}{10^n} = \sum_{i>n} \frac{b_i - a_i}{10^i} \leqslant \sum_{i>n} \frac{9}{10^i} = \frac{1}{10^n}.$$

Das kann nur richtig sein, wenn $a_n - b_n = 1$ und $b_i - a_i = 9$ für alle $i > n$; also $b_i = 9$ und $a_i = 0$ für alle $i > n$, und das heißt, daß $(b_i)_{i=1}^{\infty}$ die Einschränkung (3.7) verletzt; ein Widerspruch.

DEFINITION 3.1.1 (Dezimalbruch). *Die Zahl $z = X + y > 0$, mit der wir diesen Abschnitt begonnen haben, schreiben wir dann (wie gewohnt) als die durch einen* Dezimalpunkt *unterteilte Ziffernfolge (*Dezimalzahl *oder* Dezimalbruch*):*

$$z = c_{m-1}c_{m-2}\dots c_1c_0\,.\,d_1d_3d_3\dots$$

Man nennt diese Darstellung auch die Dezimalbruchentwiclung *Die Dezimalbruchentwicklung der Zahl $0 \in \mathbb{R}$ ist (natürlich) einfach $0.0000\dots$, und für die negative Zahl $-z$ ist die Dezimalbruchentwicklung (natürlich)*

$$-z = -c_{m-1}c_{m-2}\dots c_1c_0\,.\,d_1d_3d_3\dots$$

Wir haben mit den vorigen Überlegungen also bewiesen:

SATZ 3.1.2. *Jede Zahl $z \in \mathbb{R}$ hat eine Dezimalbruchentwicklung, die unter der Einschränkung* (3.7) *eindeutig ist.* □

3.1.3. Abbrechende und periodische Dezimalbrüche.

DEFINITION 3.1.3 (Periodische Dezimalbrüche). *Wenn die Reihe* (3.6) *in Wahrheit* endlich *ist, also wenn es ein $k \in \mathbb{N}$ gibt, sodaß $d_i = 0$ für alle $i > k$, dann nennt man den entsprechenden Dezimalbruch* abbrechend.
Ein Dezimalbruch, der nicht *abbricht, kann* periodisch *sein; z.B. ist*

$$\frac{1}{3} = 0.333333\dots, \quad \frac{1}{6} = 0.1666666, \quad \frac{1}{7} = 0.14285714285714\dots;$$

was wir abkürzend so schreiben:

$$\frac{1}{3} = 0.\dot{3}, \quad \frac{1}{6} = 0.1\dot{6}, \quad \frac{1}{7} = 0.\dot{1}42857\dot{}$$

Offensichtlich kann die Periode "gleich hinter dem Dezimalpunkt" beginnen: Dann nennt man den Dezimalbruch reinperiodisch. *Oder zwischen dem Dezimalpunkt und dem Anfang der Periode kommen ein oder mehrere Ziffern, die sich nicht periodisch wiederholen: Diese Ziffern nennt man die* Vorperiode *(oder* vorperiodische Stellen*), woran dann die* Periode *(oder die* periodischen Stellen*) anschließt: Dann nennt man den Dezimalbruch* gemischtperiodisch. *(Von unseren Beispielzahlen ist $\frac{1}{3}$ und $\frac{1}{7}$ reinperiodisch, $\frac{1}{6}$ ist gemischtperiodisch.)*

SATZ 3.1.4. *Jede Zahl $x \in S := (0,1) \cap \mathbb{Q} \subset \mathbb{Q}$ hat eine (unter der Einschränkung* (3.7) *eindeutige) Dezimalbruchentwicklung, die abbrechend oder periodisch ist; und umgekehrt stellt jede abbrechende oder periodische Dezimalbruchentwicklung eine rationale Zahl dar.*
Genauer gilt: Sei

$$x = \frac{p}{q} \text{ mit } p < q \in \mathbb{N} \text{ und } \operatorname{ggT}(p,q) = 1,$$

sei $q = 2^{\alpha} \cdot 5^{\beta} \cdot Q$ mit $\operatorname{ggT}(Q,10) = 1$, und sei $\mu := \max\{\alpha,\beta\}$.
Wenn $Q = 1$, dann bricht die Dezimalbruchentwicklung von x nach μ Stellen ab.

Wenn $Q > 1$, dann hat die Dezimalbruchentwicklung von x genau μ vorperiodische *Stellen und genau ν* periodische *Stellen, wobei ν die Ordnung von $\overline{10}$ in $\mathbb{Z}_Q^\star$ ist.*

BEWEIS. Die Dezimalbruchentwicklung (gemäß dem in Abschnitt 3.1.2 vorgestellten Algorithmus)

$$x = \frac{p}{q} = \sum_{j=1}^{\infty} d_j \cdot 10^{-j} = \lim_{k\to\infty} \underbrace{\sum_{j=1}^{k} d_j \cdot 10^{-j}}_{s_k} \tag{3.8}$$

bricht genau dann nach exakt k Stellen ab, wenn

$$x - s_{k-1} > 0 \text{ und } x - s_k = 0,$$

also wenn $10^k \cdot \frac{p}{q} \in \mathbb{N}$, aber $10^{k-1} \cdot \frac{p}{q} \notin \mathbb{N}$: Das ist äquivalent mit $q \mid 10^k$, aber $q \nmid 10^{k-1}$; und das ist äquivalent mit $q = 2^\alpha \cdot 5^\beta$ mit $k = \mu = \max\{\alpha, \beta\}$. Klarerweise ist jeder abbrechende Dezimalbruch rational.
Betrachten wir nun den Fall $\operatorname{ggT}(q, 10) = 1$, also $\alpha = \beta = 0$ und $q = Q$. Sei ν die Ordnung von $\overline{10}$ in $\mathbb{Z}_Q^\star = \mathbb{Z}_q^\star$, dann ist

$$10^\nu \cdot x = \frac{10^\nu \cdot p}{q} = \frac{(m \cdot q + 1) \cdot p}{q} = m \cdot p + \frac{p}{q} = m \cdot p + x \text{ für ein } m \in \mathbb{Z}. \tag{3.9}$$

Setze nun

$$y := \frac{m \cdot p}{10^\nu}.$$

Nach dem obigen hat y eine abbrechende Dezimalbruchentwicklung mit höchstens ν Stellen, also

$$y = \sum_{j=1}^{\nu} c_j \cdot 10^{-j},$$

und aus (3.9) folgt

$$x = \frac{y}{1 - 10^{-\nu}} = \sum_{i=0}^{\infty} y \cdot 10^{-i\cdot\nu} = \sum_{i=0}^{\infty} \sum_{j=1}^{\nu} c_j \cdot 10^{-j-i\cdot\nu}, \quad \leftarrow \text{geom. Reihe}$$

und das bedeutet sichtlich, daß x ein reinperiodischer Dezimalbruch mit einer Periode von höchstens ν Stellen ist. Das heißt

$$x = 0.\dot{a_1}a_2 \ldots \dot{a_\lambda},$$

wobei $\lambda \leqslant \nu$. Dann gilt aber

$$x = \frac{p}{q} = \left(a_1 \cdot 10^{-1} + a_2 \cdot 10^{-2} + \cdots + a_\lambda \cdot 10^{-\lambda}\right) \cdot \underbrace{\left(1 + 10^{-\lambda} + 10^{-2\cdot\lambda} + \cdots\right)}_{\frac{1}{1-10^{-\lambda}}}$$

$$= \frac{a_1 \cdot 10^{\lambda-1} + a_2 \cdot 10^{\lambda-2} + \cdots + a_\lambda \cdot 10^0}{10^\lambda - 1},$$

und da $\frac{p}{q}$ ein gekürzter Bruch ist, muß $q \mid 10^\lambda - 1$ gelten: Dies bedeutet aber $10^\lambda \equiv 1 \pmod{q}$, also gilt $\nu \mid \lambda \implies \nu \leqslant \lambda$. Wir haben also $\lambda = \nu$, und aus der

letzten Überlegung folgt natürlich ganz allgemein, daß *jeder* reinperiodische Dezimalbruch rational ist.
Wir müssen nun noch den Fall $x = \frac{p}{q} = \frac{p}{2^\alpha \cdot 5^\beta \cdot Q}$ mit $\mathrm{ggT}\,(p,q) = \mathrm{ggT}\,(Q,10) = 1$ betrachten. Dann ist

$$10^\mu \cdot x = \frac{p'}{Q} = X + \frac{P}{Q}$$

wobei $X, P \in \mathbb{Z}$ mit

$$0 \leqslant X < 10^\mu,\ 0 < P < Q,\ \mathrm{ggT}\,(P,Q) = 1.$$

Dann hat X eine eindeutige Darstellung

$$X = \sum_{i=1}^{\mu} b_i \cdot 10^{\mu - i}$$

und $\frac{P}{Q}$ hat nach dem obigen eine reinperiodische Dezimalbruchentwicklung mit genau ν periodischen Stellen

$$\frac{P}{Q} = 0.\dot{a_1}a_2 \ldots \dot{a_\nu}$$

Also hat $x = 10^{-\mu} \cdot \left(X + \frac{P}{Q}\right)$ die gemischtperiodische Dezimalbruchentwicklung

$$x = 0.b_1 b_2 \ldots b_\mu \dot{a_1} a_2 \ldots \dot{a_\nu}$$

und es ist klar, daß jeder gemischtperiodische Dezimalbruch rational ist. □

KOROLLAR 3.1.5. *Eine Zahl $z \in \mathbb{R}$ ist* nicht *rational genau dann, wenn z eine* nicht *abbrechende und* nicht *periodische Dezimalbruchentwicklung hat.* □

3.2. Entwicklung in anderen Zahlensystemen

Abgesehen davon, daß wir das Dezimalsystem *gewohnt* sind, gibt es keinen Grund, in den Überlegungen der vorigen Abschnitte gerade die Zahl 10 zu wählen; wir hätten alles auch für eine andere ganze Zahl $p > 1$ durchführen können: Dann hätten wir als Ziffernmenge $\{0, 1, \ldots, p-1\}$, und wir könnten jede positive reelle Zahl z als *p–adische Zahl* (oder *p–äre Zahl*) schreiben:

$$z = \underbrace{d_n \cdot p^n + \cdots d_1 \cdot p + d_0}_{\text{ganzzahliger Anteil } \lfloor z \rfloor} + \underbrace{d_{-1} \cdot p^{-1} + d_{-2} \cdot p^{-2} + \cdots}_{\text{nicht–ganzzahliger Anteil } z - \lfloor z \rfloor},$$

wobei

- $d_i \in \{0, 1, \ldots, p-1\}$ für alle $i \leqslant n$,
- wenn $z \geqslant 1$, dann ist $d_n > 0$ und $p^n \leqslant z < p^{n+1}$.

Zum Beispiel sind

$$\frac{21}{8} = 1 \cdot 2^1 + 0 \cdot 2^0 + 1 \cdot 2^{-1} + 0 \cdot 2^{-2} + 1 \cdot 2^{-3} = (10.101)_2$$

$$\frac{24954}{343} = 1 \cdot 7^2 + 3 \cdot 7^1 + 2 \cdot 7^0 + 5 \cdot 7^{-1} + 1 \cdot 7^{-2} + 6 \cdot 7^{-3} = (132.516)_7$$

zwei Zahlentwicklungen im 2–er System (*dyadisches System* oder *binäres System*) und im 7–er System (*heptadisches System*).

Man sieht leicht, daß die Überlegungen zur Entwicklung im Dezimalsystem gültig bleiben, wenn man 10 durch ein $p \in \mathbb{N}$, $p > 1$ ersetzt:

SATZ 3.2.1. *Sei $p \in \mathbb{N}$, $p > 1$. Dann kann jede positive reelle Zahl im p–adischen System (mit der Ziffernmenge $\{1, 2, \ldots, p-1\}$) geschrieben werden. Unter der Einschränkung, daß* unendlich viele *Ziffern dieser Darstellung* kleiner *als $p-1$ sind (diese Einschränkung ist "automatisch" erfüllt, wenn man die Zifferndarstellung mit dem in den vorigen Abschnitten vorgestellten Algorithmus ermittelt), ist die Darstellung im p–adischen System* eindeutig.

Ohne Beweis. □

3.3. Teilbarkeitsregeln für Dezimalzahlen

Von der Dezimalentwicklung einer ganzen Zahl z kann man in gewissen Fällen schnell Teilbarkeitseigenschaften ableiten.

SATZ 3.3.1. *Die natürliche Zahl $n \in \mathbb{N}$ habe die Darstellung*

$$n = a_k \cdot 10^k + a_{k-1} \cdot 10^{k-1} + \cdots + a_1 \cdot 10 + a_0$$

im dekadischen System. Dann gelten die folgenden Teilbarkeitsregeln*:*

$$\begin{aligned}
n \equiv a_0 \pmod 2 &\implies (2 \mid n) \iff 2 \mid a_0,\\
n \equiv a_0 + a_1 + \cdots + a_k \pmod 3 &\implies (3 \mid n) \iff 3 \mid a_0 + a_1 + \cdots + a_k,\\
n \equiv a_0 + 10 \cdot a_1 \pmod 4 &\implies (4 \mid n) \iff 4 \mid a_0 + 10 \cdot a_1,\\
n \equiv a_0 \pmod 5 &\implies (5 \mid n) \iff 5 \mid a_0,\\
n \equiv a_0 + 10 \cdot a_1 + 100 \cdot a_2 \pmod 8 &\implies (8 \mid n) \iff 8 \mid a_0 + 10 \cdot a_1 + 100 \cdot a_2,\\
n \equiv a_0 + a_1 + \cdots + a_k \pmod 9 &\implies (9 \mid n) \iff 9 \mid a_0 + a_1 + \cdots + a_k,\\
n \equiv a_0 - a_1 + \ldots (-1)^k a_k \pmod{11} &\implies (11 \mid n) \iff 11 \mid \sum_{i=0}^{k} (-1)^i a_i.
\end{aligned}$$

BEWEIS. Alle Aussagen folgen aus dem Rechnen mit Kongruenzen, wie wir es in Abschnitt 2.3 kennengelernt haben: Für $q \in \mathbb{N}$ betrachten wir statt der "großen Zahl"

$$n = a_k \cdot 10^k + a_{k-1} \cdot 10^{k-1} + \cdots + a_1 \cdot 10 + a_0$$

die modulo q "reduzierte" Zahl, wo jede Zehnerpotenz durch einen möglichst kleinen Repräsentanten modulo q ersetzt wird:

$$10^i = q \cdot m_i + r_i, \text{ mit } |r_i| \text{ möglichst klein}\colon\ 10^i \mapsto r_i,$$

also

$$n \equiv a_k \cdot r_k + a_{k-1} \cdot r_{k-1} + \cdots + a_1 \cdot r_1 + a_0 \cdot 1 \pmod q.$$

Die Teilbarkeitsregeln folgen dann sofort aus:

$$\begin{aligned}
10^i &\equiv 0 \pmod 2 \text{ und } \pmod 5 \text{ für alle } i \in \mathbb{N},\\
10^i &\equiv 1 \pmod 3 \text{ und } \pmod 9 \text{ für alle } i \in \mathbb{N},\\
10^i &\equiv 0 \pmod 4 \text{ für alle } i \in \mathbb{N},\ i \geqslant 2,\\
10^i &\equiv 0 \pmod 8 \text{ für alle } i \in \mathbb{N},\ i \geqslant 3,\\
10^i &\equiv (-1)^i \pmod{11} \text{ für alle } i \in \mathbb{N}_0. \qquad \square
\end{aligned}$$

BEMERKUNG 3.3.2. *Die Teilbarkeitsregeln für 3 und 9 kann man auch so ausdrücken: "Eine Zahl n ist genau dann durch 3 (bzw. 9) teilbar, wenn ihre* Ziffernsumme *durch 3 (bzw. 9) teilbar ist"; und für 11: "Eine Zahl n ist genau dann durch 11 teilbar, wenn ihre* alternierende Ziffernsumme *durch 11 teilbar ist".*
Teilbarkeit durch zusammengesetze Teiler kann man auf Teilbarkeit durch Teiler zurückführen, die paarweise relativ prim sind. Zum Beispiel erhält man sofort eine Teilbarkeitsregel für 6:

$$6 \mid n \iff 2 \mid n \text{ und } 3 \mid n \iff 2 \mid a_0 \text{ und } 3 \mid \sum_{i=0}^{k} a_i.$$

BEISPIEL 3.3.3. *Sei* $n = 9735$*:* $2 \mid n$, $3 \mid n$, $4 \nmid n$, $5 \mid n$, $6 \mid n$, $8 \nmid n$, $9 \nmid n$, $11 \mid n$.

Aufgabe 57: *Die Zahl* $n \in \mathbb{N}$ *habe die Dezimaldarstellung* $n = a_0 + 10 \cdot a_1 + 10^2 \cdot a_2 + \cdots + 10^k \cdot a_k$ *mit* $a_0, a_1, a_2, \ldots, a_k \in \{0, 1, 2, \ldots, 9\}$.
a) Beweise die folgenden Teilbarkeitsregel für 7: Die Zahl n ist genau dann durch 7 teilbar, wenn der folgende Ausdruck durch 7 teilbar ist:

$$(a_0 + 10 \cdot a_1 + 100 \cdot a_2) - (a_3 + 10 \cdot a_4 + 100 \cdot a_5) + (a_6 + 10 \cdot a_7 + 100 \cdot a_8) - + \cdots .$$

b) Zeige, daß eine völlig analoge Teilbarkeitsregel für die Teilbarkeit durch 13 gilt.
Verwende Teil a), um $7 \mid 194618851$ *zu überprüfen.*

Aufgabe 58: *Die Zahl* $n \in \mathbb{N}$ *habe die Dezimaldarstellung* $n = a_0 + 10 \cdot a_1 + 10^2 \cdot a_2 + \cdots + 10^k \cdot a_k$ *mit* $a_0, a_1, a_2, \ldots, a_k \in \{0, 1, 2, \ldots, 9\}$. *Beweise die folgenden Teilbarkeitsregeln:*
a) $13 \mid n \iff 13 \mid \left(4 \cdot a_0 + \left(a_1 + 10 \cdot a_2 + 10^2 \cdot a_3 + \cdots + 10^{k-1} \cdot a_k\right)\right)$
b) $17 \mid n \iff 17 \mid \left((-5 \cdot a_0 + \left(a_1 + 10 \cdot a_2 + 10^2 a_3 + \cdots + 10^{k-1} a_k\right)\right)$
c) $19 \mid n \iff 19 \mid \left(2 \cdot a_0 + \left(a_1 + 10 \cdot a_2 + 10^2 \cdot a_3 + \cdots + 10^{k-1} a_k\right)\right)$
Verwende Teil a), um $13 \mid 112697$ *zu überprüfen.*

Aufgabe 59: *Finde und beweise Teilbarkeitsregeln für Zahlen, die im heptadischen System dargestellt sind, für Teilbarkeit durch* 3, 8 *und* 9.

Hinweis: Siehe Satz 3.3.1!

KAPITEL 4

Quadratische Reste und das quadratische Reziprozitätsgesetz

In diesem Abschnitt werden wir die Lösbarkeit von quadratischen Kongruenzgleichungen

$$a \cdot x^2 + b \cdot x + c \equiv 0 \pmod{m} \tag{4.1}$$

(für $a, b, c \in \mathbb{Z}$, $m \in \mathbb{N}$) studieren.

4.1. Reduktion der allgemeinen quadratischen Kongruenz

Zunächst werden wir das Problem in vier Schritten auf eine spezielle, einfachere Gestalt zurückführen.

- Die Kongruenz (4.1) ist genau dann lösbar, wenn es ein $x \in \mathbb{Z}$ gibt mit

$$m \mid \left(a \cdot x^2 + b \cdot x + c\right) \iff 4 \cdot a \cdot m \mid \underbrace{\left(4 \cdot a^2 \cdot x^2 + 4 \cdot a \cdot b \cdot x + 4 \cdot a \cdot c\right)}_{=(2 \cdot a \cdot x + b)^2 + 4 \cdot a \cdot c - b^2},$$

  also genau dann, wenn die Kongruenz

$$(2 \cdot a \cdot x + b)^2 \equiv b^2 - 4 \cdot a \cdot c \pmod{4 \cdot a \cdot m}$$

  lösbar ist, also genau dann, wenn das Gleichungssystem

$$y^2 \equiv b^2 - 4 \cdot a \cdot c \pmod{4 \cdot a \cdot m}$$
$$y \equiv 2 \cdot a \cdot x + b \pmod{4 \cdot a \cdot m}$$

  lösbar ist. Die zweite dieser Gleichungen ist eine *lineare* Kongruenz, deren Lösbarkeit wir gemäß Satz 2.4.2 entscheiden können; interessant und neu ist also "nur mehr" die erste Gleichung vom Typ

$$x^2 \equiv a \pmod{m'} \text{ für } m' \in \mathbb{N}. \tag{4.2}$$

- Wenn m die Primfaktorzerlegung $m = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ besitzt, gilt

$$x^2 \equiv a \pmod{m} \text{ lösbar} \iff x^2 \equiv a \pmod{p_i^{\alpha_i}} \text{ lösbar für } 1 \leqslant i \leqslant k.$$

  Denn die eine Implikation ($\Longrightarrow$) ist klar, und die andre folgt aus dem Chinesischen Restsatz 2.4.6: Seien $x_1, \ldots, x_k \in \mathbb{Z}$ mit $x_i^2 \equiv a \pmod{p_i^{\alpha_i}}$ für $1 \leqslant i \leqslant k$, dann gibt es auch ein $\xi \in \mathbb{Z}$ mit $\xi \equiv x_i \pmod{p_i^{\alpha_i}}$, also auch $\xi^2 \equiv x_i^2 \equiv a \pmod{p_i^{\alpha_i}}$ für $1 \leqslant i \leqslant k$. Das heißt aber

$$p_1^{\alpha_1}, p_2^{\alpha_2}, \ldots, p_k^{\alpha_k} \mid \left(\xi^2 - a\right),$$

  also $\operatorname{kgV}\left(p_1^{\alpha_1}, p_2^{\alpha_2}, \ldots, p_k^{\alpha_k}\right) = m \mid \left(\xi^2 - a\right)$. In diesem Sinne ist es also ausreichend, Kongruenzen der folgenden Gestalt zu betrachten:

$$x^2 \equiv a \pmod{p^\alpha} \text{ für } p \in \mathbb{P}, \alpha \in \mathbb{N}. \tag{4.3}$$

- Es sei $p \in \mathbb{P}$, $\alpha \in \mathbb{N}$ und $a = p^\beta \cdot b$ mit $\beta \in \mathbb{N}_0$ und $\operatorname{ggT}(p, b) = 1$. Für $\beta \geqslant \alpha$ ist die Kongruenz (4.3) trivialerweise lösbar; für $\beta < \alpha$ ist (4.3) genau dann lösbar, wenn $2 \mid \beta$ und die Kongruenz $y^2 \equiv b \pmod{p^{\alpha-\beta}}$ lösbar ist: Denn für die eine Implikation ($\Longrightarrow$) sei $x_0 \in \mathbb{Z}$ eine Lösung. Deren Quadrat können wir in der Form $x_0^2 = p^\gamma \cdot y_0^2$ mit $\gamma \in \mathbb{N}_0$ und $\operatorname{ggT}\left(p, y_0^2\right) = 1$ schreiben, und offenbar gilt dann $2 \mid \gamma$. Wegen $p^\beta \mid p^\alpha \mid \left(x_0^2 - p^\beta \cdot b\right)$ folgt $p^\beta \mid x_0^2$ und somit $\beta \leqslant \gamma$; aber es kann natürlich nicht $\gamma > \beta$ gelten (denn sonst folgte aus $p^{\beta+1} \mid p^\alpha \mid (x_0^2 - p^\beta b)$ ebenso $p \mid b$, im Widerspruch zur Annahme): Also gilt $\gamma = \beta$ und daher $2 \mid \beta$; und schließlich gilt $p^\alpha \mid \left(x_0^2 - a\right)\big) = \left(p^\beta \cdot y_0^2 - p^\beta \cdot b\right) \implies p^{\alpha-\beta} \mid \left(y_0^2 - b\right)$. Für die umgekehrte Richtung ($\Longleftarrow$) sei $\beta = 2 \cdot \delta$ und $y_0 \in \mathbb{Z}$ eine Lösung der Kongruenz $y^2 \equiv b \pmod{p^{\alpha-\beta}}$, dann ist $\left(p^\delta \cdot y_0\right)^2 = p^\beta \cdot y_0^2 \equiv p^\beta \cdot b \equiv a \pmod{p^\alpha}$. In diesem Sinne ist es also ausreichend, Kongruenzen der folgenden Gestalt zu betrachten:

$$x^2 \equiv a \pmod{p^\alpha} \text{ für } p \in \mathbb{P}, \alpha \in \mathbb{N} \text{ und } \operatorname{ggT}(p, a) = 1. \tag{4.4}$$

- Ist die Kongruenz (4.3) lösbar, dann trivialerweise auch die Kongruenz $x^2 \equiv a \pmod{p}$. Für $p \neq 2$ und $\operatorname{ggT}(p, a) = 1$ gilt aber auch die Umkehrung! Dazu zeigen wir:

$$x^2 \equiv a \pmod{p^k} \text{ lösbar} \implies x^2 \equiv a \pmod{p^{k+1}} \text{ lösbar.}$$

Denn wenn $x_0 \in \mathbb{Z}$ eine Lösung von $x^2 \equiv a \pmod{p^k}$ ist, dann auch $x_0 + t \cdot p^k$ für alle $t \in \mathbb{Z}$. Nun ist aber

$$\begin{aligned}\left(x_0 + t \cdot p^k\right)^2 - a &= x_0^2 + 2 \cdot x_0 \cdot t \cdot p^k + t^2 \cdot p^{2k} - a \\ &\equiv \left(x_0^2 - a\right) + 2 \cdot x_0 \cdot t \cdot p^k \pmod{p^{k+1}} \\ &\equiv p^k \cdot \left(\underbrace{\frac{x_0^2 - a}{p^k}}_{\in \mathbb{Z}} + 2 \cdot x_0 \cdot t \right) \pmod{p^{k+1}},\end{aligned}$$

und wenn wir ein t finden, sodaß $p \mid \left(\frac{x_0^2 - a}{p^k} + 2 \cdot x_0 \cdot t\right)$, dann haben wir unsere Behauptung gezeigt, denn dann ist

$$\left(x_0 + t \cdot p^k\right)^2 - a \equiv 0 \pmod{p^{k+1}}.$$

Wir brauchen also eine Lösung der linearen Kongruenzgleichung (in der Variablen t):

$$2 \cdot x_0 \cdot t \equiv \frac{a - x_0^2}{p^k} \pmod{p}.$$

Für $p \neq 2$ und $p \nmid a \implies p \nmid x_0$ gilt aber $\operatorname{ggT}(2 \cdot x_0, p) = 1$ und diese Kongruenz *ist* lösbar (gemäß Satz 2.4.2)! Wenn $p \neq 2$, ist es in diesem Sinne also ausreichend, Kongruenzen der folgenden Gestalt zu betrachten:

$$x^2 \equiv a \pmod{p} \text{ für } p \in \mathbb{P} \text{ und } \operatorname{ggT}(p, a) = 1. \tag{4.5}$$

Aufgabe 60: *Es seien $a, b \in \mathbb{Z}$ und $p \in \mathbb{P}$. Zeige: Wenn $a^p \equiv b^p \pmod{p}$, dann gilt auch $a^p \equiv b^p \pmod{p^2}$.*

4.2. Der Fall $p = 2$

Den "Sonderfall" $p = 2$ (für den sich (4.4) *nicht* auf (4.5) zurückführen läßt) behandeln wir vorweg:

SATZ 4.2.1. *Sei $2 \nmid a$, dann gilt:*

(1) *Die Kongruenz $x^2 \equiv a \pmod{2}$ ist lösbar.*
(2) *Die Kongruenz $x^2 \equiv a \pmod{4}$ ist genau dann lösbar, wenn $a \equiv 1 \pmod{4}$.*
(3) *Für $\alpha \in \mathbb{N}, \alpha \geqslant 3$ ist die Kongruenz $x^2 \equiv a \pmod{2^\alpha}$ genau dann lösbar, wenn $a \equiv 1 \pmod{8}$*

BEWEIS. Die ersten zwei Behauptungen ergeben sich durch simples Überprüfen: Aus $2 \nmid a$ folgt für jede Lösung x_0 der Kongruenzen $2 \nmid x_0$; und in $\mathbb{Z}_2$ ist $\overline{1} = \overline{1}^2$ ja die *einzige* Restklasse $\overline{a}$ mit $2 \nmid a$, und in $\mathbb{Z}_4$ gibt es nur *zwei* solche Restklassen:

$$\overline{1}^2 = \overline{3}^2 = \overline{1} \text{ in } \mathbb{Z}_4.$$

Für die dritte Behauptung betrachten wir zunächst den Spezialfall $\alpha = 3$, also die Kongruenz $x^2 \equiv a \pmod{8}$: Wieder ergibt sich durch simples Überprüfen, daß die Quadrate aller vier Restklassen $\overline{a}$ mit $2 \nmid a$ immer $\overline{1}$ ergeben:

$$\overline{1}^2 = \overline{3}^2 = \overline{5}^2 = \overline{7}^2 = \overline{1} \text{ in } \mathbb{Z}_8.$$

Da aus $x_0^2 \equiv a \pmod{2^\alpha}$ für $\alpha \geqslant 3$ natürlich $x_0^2 \equiv a \pmod{8}$ folgt, ist damit auch die Implikation ($\Longrightarrow$) in der dritten Behauptung gezeigt. Für die umgekehrte Implikation ($\Longleftarrow$) zeigen wir (ganz analog den Überlegungen, die zu (4.5) führten): Sei $x_0^2 \equiv a \pmod{2^k}, k \geqslant 3$, dann ist auch $x_0 + 2^{k-1} \cdot t$ eine Lösung der Kongruenz für alle $t \in \mathbb{Z}$, denn

$$\left(x_0 + 2^{k-1} \cdot t\right)^2 = x_0^2 + 2 \cdot 2^{k-1} \cdot x_0 \cdot t + 2^{2k-2} \cdot t^2 \equiv x_0^2 \equiv a \pmod{2^k}.$$

Wir wollen nun zeigen, daß man ein $t_0 \in \mathbb{Z}$ finden kann, sodaß

$$\left(x_0 + 2^{k-1} \cdot t_0\right)^2 \equiv a \pmod{2^{k+1}}$$

(denn daraus ergibt sich induktiv unsere Behauptung):

$$\begin{aligned}\left(x_0 + 2^{k-1} \cdot t\right)^2 - a &= x_0^2 + 2^k \cdot x_0 \cdot t + \underbrace{2^{2k-2} \cdot t^2}_{\equiv 0 \pmod{2^{k+1}}} - a \quad \leftarrow k \geqslant 3 \Longrightarrow 2k-2 \geqslant k+1 \\ &\equiv x_0^2 - a + 2^k \cdot x_0 \cdot t \pmod{2^{k+1}} \\ &\equiv 2^k \cdot \left(\underbrace{\frac{x_0^2 - a}{2^k}}_{\in \mathbb{Z}} + x_0 \cdot t \right) \pmod{2^{k+1}}.\end{aligned}$$

Nach Satz 2.4.2 hat die lineare Kongruenz (in der Variablen t)

$$x_0 \cdot t \equiv \frac{a - x_0^2}{2^k} \pmod 2$$

eine Lösung t_0 (denn $2 \nmid a \implies 2 \nmid x_0$, also $\mathrm{ggT}(x_0, 2) = 1$), und für diese Lösung gilt $\left(x_0 + 2^{k-1} \cdot t\right)^2 - a \equiv 0 \pmod{2^{k+1}}$. □

4.3. Der Fall $p > 2$: Quadratische Reste und Nichtreste

Nun betrachten wir den (interessanteren) Fall $p > 2$.

DEFINITION 4.3.1 (quadratische Reste und Nichtreste). *Es sei $p \neq 2$ eine Primzahl und $a \in \mathbb{Z}$ mit $p \nmid a$. Man sagt, a sei* quadratischer Rest *modulo p, wenn die Kongruenz $x^2 \equiv a \pmod p$ lösbar ist. Ist diese Kongruenz nicht lösbar, wird a* quadratischer Nichtrest *modulo p genannt.*

LEMMA 4.3.2. *Sei $p \in \mathbb{P}$, $p \neq 2$ und $a \in \mathbb{Z}$ mit $p \nmid a$. Wenn a quadratischer Rest modulo p ist, dann gibt es* genau zwei *modulo p inkongruente Lösungen der Kongruenz $x^2 \equiv a \pmod p$.*

BEWEIS. Wenn wir *eine* Lösung $x_0 \in \mathbb{Z}$ gefunden haben, so ist $-x_0$ auch eine Lösung; und da $p \neq 2$, sind diese beiden Lösungen inkongruent modulo p (denn $1 \not\equiv -1 \pmod p$ für $p \neq 2$).
Sei $x_1 \in \mathbb{Z}$ eine beliebige Lösung von $x^2 \equiv a \pmod p$: Dann gilt

$$x_0^2 \equiv x_1^2 \pmod p \iff p \mid \left(x_0^2 - x_1^2\right) = (x_0 - x_1) \cdot (x_0 + x_1),$$

und da $p \in \mathbb{P}$, folgt

$$x_0 \equiv x_1 \pmod p \text{ oder } x_0 \equiv -x_1 \pmod p$$

(siehe Satz 1.4.3): Es gibt also keine andren Lösungen außer $\pm x_0$. □

LEMMA 4.3.3. *Sei $p \in \mathbb{P}$, $p \neq 2$: Von den $p - 1$ primen Restklassen modulo p sind* genau *die Hälfte quadratische Reste, nämlich $\overline{1^2}, \overline{2^2}, \ldots, \overline{\frac{p-1}{2}^2}$.*

BEWEIS. Klarerweise *sind* die Restklassen $\overline{1^2}, \overline{2^2}, \ldots, \overline{\frac{p-1}{2}^2}$ quadratische Reste: Sie sind alle *verschieden*, denn aus $k^2 \equiv l^2 \pmod p$ folgt ja (siehe Beweis von Lemma 4.3.2)

$$k \equiv l \pmod p \text{ oder } k \equiv -l \pmod p.$$

Für $k, l \in \left\{1, 2, \ldots, \frac{p-1}{2}\right\}$ gilt aber $2 \leqslant (k + l) \leqslant p - 1 \implies p \nmid (k + l)$; und

$$p \mid (k - l) \implies k = l.$$

Wenn man die *übrigen* Restklassen

$$\overline{\tfrac{p+1}{2}} = \overline{p - \tfrac{p-1}{2}} = \overline{-\tfrac{p-1}{2}},\ \overline{\tfrac{p+3}{2}} = \overline{p - \tfrac{p-3}{2}} = \overline{-\tfrac{p-3}{2}},\ \ldots,\ \overline{\tfrac{p+p-2}{2}} = \overline{p-1} = \overline{-1}$$

quadriert, ergeben sich aber keine zusätzlichen quadratischen Reste: Denn diese sind ja einfach die Restklassen $\overline{1}, \overline{2}, \ldots, \overline{\frac{p-1}{2}}$, multipliziert mit $\overline{-1}$. □

DEFINITION 4.3.4 (Legendre–Symbol). *Sei $p \in \mathbb{P},\ p \neq 2$ und $a \in \mathbb{Z}$. Das* Legendre–Symbol $\left(\frac{a}{p}\right)$ *ist definiert durch*

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{wenn } a \text{ quadratischer Rest modulo } p \text{ ist,} \\ 0 & \text{wenn } p \mid a, \\ -1 & \text{wenn } a \text{ quadratischer Nichtrest modulo } p \text{ ist.} \end{cases}$$

BEOBACHTUNG 4.3.5. *Wenn $a \equiv b \pmod{p}$, dann ist $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.*

SATZ 4.3.6. *Sei $p \in \mathbb{P},\ p \neq 2$ und $a \in \mathbb{Z}$. Dann gilt:*

$$a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \pmod{p} \tag{4.6}$$

BEWEIS. Falls $p \mid a$, ist $a \equiv 0 \pmod{p}$, und daraus folgt natürlich $a^{\frac{p-1}{2}} \equiv 0 = \left(\frac{a}{p}\right) \pmod{p}$.

Andernfalls ist a ein Element der *Einheitengruppe* $\mathbb{Z}_p^\star$ des Körpers $\mathbb{Z}_p$ (siehe Korollar 2.5.7): Für jedes x aus dem primen Restsystem $S := \{1, 2, \ldots, p-1\}$ modulo p gibt es *genau ein* $y \in S$, sodaß

$$x \cdot y \equiv a \pmod{p} \tag{4.7}$$

(Dieses $y \in S$ ist der Repräsentant der Restklasse $\overline{x^{-1}} \cdot \overline{a}$ in $\mathbb{Z}_p$).

Wenn a quadratischer *Nichtrest* ist, dann kann in (4.7) definitionsgemäß *niemals* $x = y$ gelten: Die Menge S zerfällt in diesem Fall also in $\frac{p-1}{2}$ verschiedene *zweielementige Teilmengen*

$$S = \dot{\bigcup}_{i=1}^{\frac{p-1}{2}} \{x_i, y_i\}$$

mit $x_i \cdot y_i \equiv a \pmod{p}$ für $1 \leqslant i \leqslant \frac{p-1}{2}$. Dann ist aber

$$(p-1)! = \prod_{j=1}^{p-1} j = \prod_{i=1}^{\frac{p-1}{2}} (x_i \cdot y_i) \equiv a^{\frac{p-1}{2}} \pmod{p},$$

und die Behauptung folgt aus dem Satz von Wilson 2.5.9:

$$(p-1)! \equiv -1 = \left(\frac{a}{p}\right) \pmod{p}.$$

Wenn a quadratischer *Rest* ist, dann gilt in (4.7) gemäß Lemma 4.3.2 *genau zweimal* $x = y$, nämlich für die beiden Lösungen x_0 und $p - x_0$: Die Menge S zerfällt in diesem Fall also in $\frac{p-3}{2}$ verschiedene *zweielementige Teilmengen* und zwei einpunktige Teilmengen

$$S = \{x_0\} \ \dot{\cup}\ \{p - x_0\} \ \dot{\cup}\ \left(\dot{\bigcup}_{i=1}^{\frac{p-3}{2}} \{x_i, y_i\}\right)$$

mit $x_i \cdot y_i \equiv a \pmod{p}$ für $1 \leqslant i \leqslant \frac{p-3}{2}$. Dann ist aber

$$(p-1)! = \prod_{j=1}^{p-1} j = \underbrace{x_0 \cdot (p - x_0)}_{\equiv -a \pmod{p}} \cdot \prod_{i=1}^{\frac{p-3}{2}} (x_i \cdot y_i) \equiv -a^{\frac{p-1}{2}} \pmod{p},$$

und die Behauptung folgt wieder aus dem Satz von Wilson 2.5.9:

$$-(p-1)! \equiv 1 = \left(\frac{a}{p}\right) \pmod{p}. \qquad \square$$

KOROLLAR 4.3.7 (Eulersches Kriterium). *$p \in \mathbb{P},\ p \neq 2$ und $a \in \mathbb{Z}$. Dann ist a quadratischer Rest modulo p genau dann, wenn $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$.* $\square$

KOROLLAR 4.3.8. *$p \in \mathbb{P},\ p \neq 2$ und $a_1, a_2 \in \mathbb{Z}$. Dann gilt:*

$$\left(\frac{a_1 \cdot a_2}{p}\right) = \left(\frac{a_1}{p}\right) \cdot \left(\frac{a_2}{p}\right), \tag{4.8}$$

woraus induktiv für $m \in \mathbb{N}$, $m \geqslant 2$ und $a_1, a_2 \ldots, a_m \in \mathbb{Z}$ sofort folgt:

$$\left(\frac{a_1 \cdot a_2 \cdots a_k}{p}\right) = \left(\frac{a_1}{p}\right) \cdot \left(\frac{a_2}{p}\right) \cdots \left(\frac{a_m}{p}\right).$$

BEWEIS. Die Behauptung folgt sofort aus (4.6):

$$\left(\frac{a_1 \cdot a_2}{p}\right) \equiv (a_1 \cdot a_2)^{\frac{p-1}{2}} \equiv a_1^{\frac{p-1}{2}} \cdot a_2^{\frac{p-1}{2}} \equiv \left(\frac{a_1}{p}\right) \cdot \left(\frac{a_2}{p}\right) \pmod{p}$$

$\square$

KOROLLAR 4.3.9 (Erster Ergänzungssatz). *Sei $p \in \mathbb{P},\ p \neq 2$. Dann ist*

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}.$$

Anders gesagt:

$$\left(\frac{-1}{p}\right) = \begin{cases} 1 & \text{wenn } p \equiv 1 \pmod{4}, \\ -1 & \text{wenn } p \equiv 3 \pmod{4}. \end{cases}$$

BEWEIS. Die Behauptung folgt sofort aus (4.6):

$$\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{p-1}{2}} \pmod{p} \implies \left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$$

$\square$

4.3.1. Das Gaußsche Lemma.

SATZ 4.3.10 (Gaußsches Lemma). *Sei* $p \in \mathbb{P},\ p \neq 2$ *und* $a \in \mathbb{Z}$ *mit* $\mathrm{ggT}(p,a) = 1$. *Betrachte die Menge der* $\frac{p-1}{2}$ *Restklassen*

$$\left\{\overline{1 \cdot a}, \overline{2 \cdot a}, \ldots, \overline{\frac{p-1}{2} \cdot a}\right\}$$

und wähle für jede dieser Restklassen $\overline{j \cdot a}$ *einen* Repräsentanten r_j, *der*

$$-\frac{p-1}{2} \leqslant r_j \leqslant \frac{p-1}{2} = -\frac{p-1}{2} + p - 1$$

erfüllt (klarerweise gibt es genau einen *solchen Repräsentanten). Sei* $\gamma_p(a)$ *die* Anzahl *dieser Repräsentanten, die kleiner Null sind; formal:*

$$\gamma_p(a) = \left|\left\{r_j \in \overline{j \cdot a} \colon\ 1 \leqslant j \leqslant \frac{p-1}{2} \text{ und } -\frac{p-1}{2} \leqslant r_j \leqslant \frac{p-1}{2}\right\} \cap (\mathbb{Z} \backslash \mathbb{N}_0)\right|.$$

Dann ist

$$\left(\frac{a}{p}\right) = (-1)^{\gamma_p(a)}. \tag{4.9}$$

BEWEIS. Aus $1 \leqslant |r_i| \leqslant \frac{p-1}{2}$ folgt klarerweise

$$\left\{|r_1|, \ldots, \left|r_{\frac{p-1}{2}}\right|\right\} \subseteq \left\{1, \ldots, \frac{p-1}{2}\right\}.$$

Es ist aber auch

$$|r_i| \neq \left|r_j\right| \text{ für } 1 \leqslant i \neq j \leqslant \frac{p-1}{2},$$

denn wenn $|r_i| = \left|r_j\right|$ für $1 \leqslant i, j \leqslant \frac{p-1}{2}$, dann muß

$$i \cdot a \equiv j \cdot a \pmod{p} \text{ oder } i \cdot a \equiv -j \cdot a \pmod{p}$$

gelten; weil $\overline{a} \neq \overline{0} \in \mathbb{Z}_p$ folgt also

$$i \equiv j \pmod{p} \text{ oder } i \equiv -j \pmod{p}.$$

Es ist aber $1 < (i+j) < p$ und daher $p \nmid (i+j)$, also muß $p \mid (i-j)$ gelten, und daraus folgt $i = j$ (wegen $|i-j| < \frac{p-1}{2}$).
Das heißt aber:

$$\begin{aligned}\left(\frac{p-1}{2}\right)! \cdot a^{\frac{p-1}{2}} &= (1 \cdot a) \cdot (2 \cdot a) \cdots \left(\left(\frac{p-1}{2}\right) \cdot a\right) \\ &\equiv r_1 \ldots r_{\frac{p-1}{2}} \pmod{p} \\ &\equiv (-1)^{\gamma_p(a)} |r_1| \ldots \left|r_{\frac{p-1}{2}}\right| \pmod{p} \\ &= (-1)^{\gamma_p(a)} \left(\frac{p-1}{2}\right)! \pmod{p},\end{aligned}$$

und aus $p \nmid \left(\frac{p-1}{2}\right)!$ folgt

$$(-1)^{\gamma_p(a)} \equiv a^{\frac{p-1}{2}} \pmod{p}.$$

Die Behauptung folgt daraus gemäß (4.6). □

Aufgabe 61: *Leite den ersten Ergänzungssatz aus dem Gaußschen Lemma ab.*

KOROLLAR 4.3.11 (Zweiter Ergänzungssatz). *Sei $p \in \mathbb{P},\ p \neq 2$. Dann ist*

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}.$$

Anders gesagt:

$$\left(\frac{2}{p}\right) = \begin{cases} 1 & \text{wenn } p \equiv \pm 1 \pmod 8, \\ -1 & \text{wenn } p \equiv \pm 3 \pmod 8. \end{cases}$$

BEWEIS. Nach dem Gaußschen Lemma 4.3.10 müssen wir bestimmen, wieviele Elemente der Menge

$$\left\{1 \cdot 2, 2 \cdot 2, \ldots, \frac{p-1}{2} \cdot 2\right\} = \{2, 4, \ldots, p-1\},$$

größer als $\frac{p-1}{2}$ sind, denn diese Anzahl ist natürlich $\gamma_p(2)$.
Das können wir auch so ausdrücken: Sei $m \in \mathbb{Z}$ sodaß

$$2 \cdot m \leqslant \frac{p-1}{2} < 2 \cdot (m+1),$$

dann ist

$$\gamma_p(2) = \frac{p-1}{2} - m.$$

Das rechnen wir einfach für alle möglichen Fälle aus:

- Fall $p = 8 \cdot k + 1$: Dann ist $\frac{p-1}{2} = 4 \cdot k$ und $m = 2 \cdot k$, also $\gamma_p(2) = 2 \cdot k$ und daher $\left(\frac{2}{p}\right) = (-1)^{2 \cdot k} = 1$.
- Fall $p = 8 \cdot k + 7$: Dann ist $\frac{p-1}{2} = 4 \cdot k + 3$ und $m = 2 \cdot k + 1$, also $\gamma_p(2) = 2 \cdot k + 2$ und daher $\left(\frac{2}{p}\right) = (-1)^{2 \cdot k + 2} = 1$.
- Fall $p = 8 \cdot k + 3$: Dann ist $\frac{p-1}{2} = 4 \cdot k + 1$ und $m = 2 \cdot k$, also $\gamma_p(2) = 2 \cdot k + 1$ und daher $\left(\frac{2}{p}\right) = (-1)^{2 \cdot k + 1} = -1$.
- Fall $p = 8 \cdot k + 5$: Dann ist $\frac{p-1}{2} = 4 \cdot k + 2$ und $m = 2 \cdot k + 1$, also $\gamma_p(2) = 2 \cdot k + 1$ und daher $\left(\frac{2}{p}\right) = (-1)^{2 \cdot k + 1} = -1$. □

Aufgabe 62: *Berechne* a) $\left(\frac{-1}{31}\right)$ b) $\left(\frac{-1}{17}\right)$ c) $\left(\frac{2}{41}\right)$ d) $\left(\frac{2}{47}\right)$.

Aufgabe 63: *Zeige: Es gibt unendlich viele Primzahlen der Gestalt $8 \cdot k + 7$.*

Hinweis: Angenommen, $p_1, \ldots, p_s$ wären alle solchen Primzahlen: Betrachte $N := (4 \cdot p_1 \cdots p_s)^2 - 2$ und verwende den zweiten Ergänzungssatz.

4.3.2. Das Quadratische Reziprozitätsgesetz.

SATZ 4.3.12 (Quadratisches Reziprozitätsgesetz). *Es seien $p \neq q \in \mathbb{P}\setminus\{2\}$ zwei verschiedene ungerade Primzahlen. Dann gilt:*

$$\left(\frac{p}{q}\right) \cdot \left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}} \tag{4.10}$$

Anders gesagt:

- $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$, *wenn* $p \equiv 1 \pmod 4$ *oder* $q \equiv 1 \pmod 4$;
- $\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right)$, *wenn* $p \equiv q \equiv 3 \pmod 4$.

BEWEIS. Nach dem Gaußschen Lemma 4.3.10 ist

$$\left(\frac{p}{q}\right) \cdot \left(\frac{q}{p}\right) = (-1)^{\gamma_q(p)+\gamma_p(q)},$$

und die Behauptung ist äquivalent zur Aussage

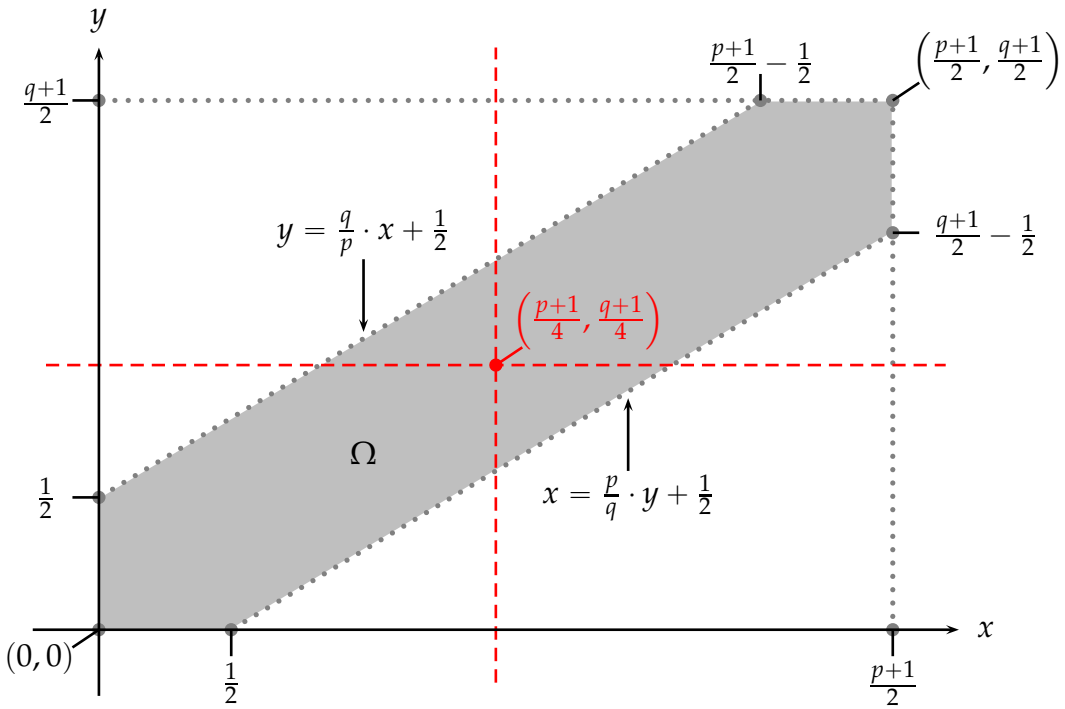
$$2 \nmid \left(\gamma_q(p) + \gamma_p(q)\right) \iff p \equiv q \equiv 3 \pmod 4.$$

Zum Beweis betrachten wir die folgende Menge

$$\Omega := \left\{(x,y) \in \mathbb{R}^2 \colon\ 0 < x < \frac{p+1}{2}, 0 < y < \frac{q+1}{2}, y < \frac{q}{p}\cdot x + \frac{1}{2}, x < \frac{p}{q}\cdot y + \frac{1}{2}\right\}.$$

Offenbar ist $\Omega \subset \mathbb{R}^2$ eine offene Menge: Abbildung 4.3.2 illustriert ihre sechseckige Gestalt.

ABBILDUNG 1. Illustration der Menge $\Omega \subset \mathbb{R}^2$ (graues Sechseck), mit Spiegelungsachsen (rot strichliert) und Bemaßung.



Die Elemente von $\mathbb{Z}^2 = \{(x,y) : \ x,y \in \mathbb{Z}\}$ werden *Gitterpunkte* genannt: Die Gitterpunkte sind also die Punkte der Ebene $\mathbb{R}^2$ mit ganzzahligen Koordinaten.

Wir behaupten, daß die Anzahl der Gitterpunkte in Ω genau $\gamma_p(q) + \gamma_q(p)$ ist, daß also für $\Omega_{\mathbb{Z}} := \Omega \cap \mathbb{Z}^2$ gilt:

$$|\Omega_{\mathbb{Z}}| = \left|\Omega \cap \mathbb{Z}^2\right| = \gamma_p(q) + \gamma_q(p). \tag{4.11}$$

Zunächst ist klar, daß $p \cdot y = q \cdot x$ für *kein* $(x,y) \in \Omega_{\mathbb{Z}}$ gelten kann: Denn sonst folgte aus $p \mid q \cdot x$ sofort $p \mid x$, im Widerspruch zu $1 \leqslant x < \frac{p+1}{2} < p$ (da $p > 1$).

Nun zeigen wir:

$$|\{(x,y) \in \Omega_Z : \ p \cdot y > q \cdot x\}| = \gamma_p(q),$$
$$|\{(x,y) \in \Omega_Z : \ p \cdot y < q \cdot x\}| = \gamma_q(p).$$

Aus Symmetriegründen[1] brauchen wir nur eine dieser Gleichungen zu zeigen; wir nehmen die erste: Sei $(x,y) \in \Omega_{\mathbb{Z}}$ mit $y > \frac{q}{p} \cdot x$, dann folgt aus der Definition von Ω auch $y < \frac{q}{p} \cdot x + \frac{1}{2}$, also insgesamt

$$\frac{q}{p} \cdot x < y < \frac{q}{p} \cdot x + \frac{1}{2} \iff q \cdot x < p \cdot y < q \cdot x + \frac{p}{2} \iff -\frac{p}{2} < q \cdot x - p \cdot y < 0.$$

Nun ist aber $x \in \left\{1, \ldots, \frac{p-1}{2}\right\}$, und die letzte Ungleichungskette können wir mit der Notation des Gaußschen Lemmas 4.3.10 (ersetze $a \to q$) reformulieren:

$$r_x < 0 \iff -\frac{p}{2} < \underbrace{q \cdot x - p \cdot y}_{\text{Repr. von } \overline{q \cdot x} \in \mathbb{Z}_p} < 0.$$

Also haben wir wie behauptet:

$$|\{(x,y) \in \Omega_Z : \ p \cdot y > q \cdot x\}| = \left|\left\{x \in \{1, \ldots, \frac{p-1}{2}\right\} : \ r_x < 0\}\right| = \gamma_p(q),$$

und (4.11) ist damit gezeigt.

Um den Beweis abzuschließen müssen wir noch zeigen:

$$|\Omega_{\mathbb{Z}}| \text{ ist ungerade } \textit{genau dann, wenn } p \equiv q \equiv 3 \,(4).$$

Dazu betrachten wir die Abbildung

$$\varphi : \ \Omega \to \mathbb{R}^2, \ (x,y) \mapsto (x',y') = \left(\frac{p+1}{2} - x, \frac{q+1}{2} - y\right).$$

Geometrisch ist das eine *Drehung* um $180^\circ = \pi$ mit *Drehzentrum* $\left(\frac{p+1}{4}, \frac{q+1}{4}\right)$, die die Menge Ω *in sich* selbst abbildet:

$$\varphi(\Omega) = \Omega.$$

[1] Wir können ja die Rollen von p und q vertauschen!

Wenn man das nicht aus Linearer Algebra "mitbringt", erkennt man die Drehung als Hintereinanderausführung von zwei Spiegelungen mit den Spiegelungsachsen, die durch das Drehzentrum gehen und parallel zur x– bzw. y–Achse sind, oder man schaut einfach, was φ mit den Eckpunkten des Sechsecks macht (siehe Abbildung 4.3.2):

$$\begin{aligned}(0,0) &\leftrightarrow \left(\frac{p+1}{2}, \frac{q+1}{2}\right),\\ \left(0, \frac{1}{2}\right) &\leftrightarrow \left(\frac{p+1}{2}, \frac{q+1}{2} - \frac{1}{2}\right),\\ \left(\frac{1}{2}, 0\right) &\leftrightarrow \left(\frac{p+1}{2} - \frac{1}{2}, \frac{q+1}{2}\right).\end{aligned}$$

Klarerweise ist

$$(x,y) \in \Omega_{\mathbb{Z}} \iff \varphi(x,y) \in \Omega_{\mathbb{Z}};$$

die Menge $\Omega_{\mathbb{Z}}$ hat also eine Partition

- in zweielementige Blöcke $\{(x,y), \varphi(x,y)\}$,
- und eventuell *einen* einelementigen Block $\{(x,y) = \varphi(x,y)\}$, der aber *nur* auftritt, wenn der *einzige* Fixpunkt von ϕ (das ist das Drehzentrum $\left(\frac{p+1}{4}, \frac{q+1}{4}\right)$) ein *Gitterpunkt* in $\mathbb{Z}^2$ ist — und das ist genau dann der Fall, wenn $p \equiv q \equiv -1 \pmod 4$. □

Das quadratische Reziprozitätsgesetz wird meist in der Form

$$\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right) \cdot (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}$$

angewendet.

BEISPIEL 4.3.13. *Als Beispiel untersuchen wir die quadratische Kongruenzgleichung für $p = 61 \in \mathbb{P}$:*

$$x^2 \equiv -21 \pmod{61}.$$

Es gibt mehrere Wege, um die Lösbarkeit zu entscheiden, z.B.:

- *1. Variante:*

$$\left(\frac{-21}{61}\right) = \underbrace{\left(\frac{-1}{61}\right)}_{=(-1)^{30}=1} \cdot \left(\frac{3}{61}\right) \cdot \left(\frac{7}{61}\right) = \left(\frac{3}{61}\right) \cdot \left(\frac{7}{61}\right)$$

$$= \underbrace{(-1)^{1\cdot 30}}_{=1} \cdot \underbrace{\left(\frac{61}{3}\right)}_{=\left(\frac{1}{3}\right)=1} \cdot \left(\frac{7}{61}\right) = \left(\frac{7}{61}\right) = \underbrace{(-1)^{3\cdot 30}}_{=1} \cdot \underbrace{\left(\frac{61}{7}\right)}_{=\left(\frac{5}{7}\right)}$$

$$= \left(\frac{5}{7}\right) = \underbrace{(-1)^{2\cdot 3}}_{=1} \cdot \underbrace{\left(\frac{7}{5}\right)}_{=\left(\frac{2}{5}\right)} = \left(\frac{2}{5}\right) = (-1)^{\frac{24}{8}} = (-1)^3 = -1$$

- *2. Variante:*

$$\left(\frac{-21}{61}\right) = \left(\frac{40}{61}\right) = \left(\frac{2^2 \cdot 10}{61}\right) = \left(\frac{10}{61}\right) = \left(\frac{2}{61}\right) \cdot \left(\frac{5}{61}\right)$$
$$= \underbrace{(-1)^{\frac{3720}{8}}}_{=(-1)^{465}=-1} \cdot \left(\frac{5}{61}\right) = -\left(\frac{5}{61}\right) = -\underbrace{(-1)^{2\cdot 30}}_{=1} \cdot \underbrace{\left(\frac{61}{5}\right)}_{=\left(\frac{1}{5}\right)=1} = -1$$

Die quadratische Kongruenzgleichung ist also unlösbar.

Aufgabe 64: *Welche der folgenden Kongruenzen sind lösbar?*

a) $x^2 \equiv 59 \pmod{79}$ *b)* $x^2 \equiv 17 \pmod{41}$ $x^2 \equiv 29 \pmod{101}$

Aufgabe 65: *Es sei* $p \in \mathbb{P} \setminus \{2,3\}$. *Zeige, daß die Kongruenz* $x^2 \equiv -3 \pmod{p}$ *genau dann lösbar ist, wenn* $p \equiv 1 \pmod{6}$.

Hinweis: Berechne

$$\left(\frac{-3}{6k+1}\right) \text{ und } \left(\frac{-3}{6k+5}\right).$$

KAPITEL 5

Kettenbrüche

5.1. Endliche Kettenbrüche

DEFINITION 5.1.1 (endlicher Kettenbruch). *Sei* $n \in \mathbb{N}_0, a_0, a_1, \ldots, a_n; c_1, c_2, \ldots, c_n \in \mathbb{R}$. *Ein Ausdruck der Gestalt*

$$a_0 + \cfrac{c_1}{a_1 + \cfrac{c_2}{a_2 + \cfrac{c_3}{a_3 + \ddots \cfrac{\ddots}{a_{n-2} + \cfrac{c_{n-1}}{a_{n-1} + \cfrac{c_n}{a_n}}}}}} \tag{5.1}$$

den wir auch "platzsparender" in der Form

$$a_0 + \frac{c_1|}{|a_1} + \frac{c_2|}{|a_2} + \cdots + \frac{c_{n-1}|}{|a_{n-1}} + \frac{c_n|}{|a_n}$$

schreiben, wird endlicher Kettenbruch *genannt; unter der* Voraussetzung, *daß* keiner *der auftretenden* Nenner

$$N_j := a_j + \frac{c_{j+1}|}{|a_{j+1}} + \frac{c_{j+2}|}{|a_{j+2}} + \cdots + \frac{c_n|}{|a_n}, j = 1, 2, \ldots n,$$

gleich 0 *ist, das heißt also*

$$\begin{aligned}
N_n &= a_n \neq 0, \\
N_{n-1} &= a_{n-1} + \frac{c_n}{a_n} = a_{n-1} + \frac{c_n}{N_n} \neq 0, \\
N_{n-2} &= a_{n-2} + \frac{c_{n-1}}{a_{n-1} + \dfrac{c_n}{a_n}} = a_{n-2} + \frac{c_{n-1}}{N_{n-1}} \neq 0, \\
&\vdots \\
N_1 &= a_1 + \frac{c_2}{N_2} \neq 0.
\end{aligned}$$

(Der Nenner N_0 *ist dann der Kettenbruch* (5.1) *selbst.)*

Für den Kettenbruch (5.1) *definiert man* rekursiv *zwei Folgen* $(p_k)_{k\geqslant -2}$, $(q_k)_{k\geqslant -2}$ *wie folgt:*

$$p_k = a_k \cdot p_{k-1} + c_k \cdot p_{k-2} \text{ für } k \geqslant 0, \text{ Anfangsbedingung: } p_{-2} = 0, p_{-1} = 1,$$
$$q_k = a_k \cdot q_{k-1} + c_k \cdot q_{k-2} \text{ für } k \geqslant 0, \text{ Anfangsbedingung: } q_{-2} = 1, q_{-1} = 0. \quad (5.2)$$

SATZ 5.1.2. *Für den Kettenbruch* (5.1) *und die zugehörigen Folgen* (5.2) *gilt:*

$$\frac{p_k}{q_k} = a_0 + \frac{c_1|}{|a_1} + \cdots + \frac{c_k|}{|a_k} \text{ für } 0 \leqslant k \leqslant n.$$

(Wieder setzen wir voraus, daß alle Nenner dieser Kettenbrüche ungleich 0 *sind: Insbesondere ist also* $a_k \neq 0$ *für* $1 \leqslant k \leqslant n$ *vorausgesetzt!)*

BEWEIS. Induktion nach k: Für $k = 0$ ergibt sich

$$\frac{p_0}{q_0} = \frac{a_0 \cdot 1 + 0}{a_0 \cdot 0 + 1} = a_0,$$

der Induktionsanfang ist also richtig.
Für den Induktionsschritt $(k \to k+1)$ setze

$$a'_k := a_k + \frac{c_{k+1}}{a_{k+1}}. \leftarrow a_{k+1}\neq 0 \text{ nach Voraussetzung!}$$

Dann ist natürlich

$$a_0 + \frac{c_1|}{|a_1} + \cdots + \frac{c_k|}{|a_k} + \frac{c_{k+1}|}{|a_{k+1}} = a_0 + \frac{c_1|}{|a_1} + \cdots + \frac{c_k|}{|a'_k}.$$

Für

$$p'_k := a'_k \cdot p_{k-1} + c_k \cdot p_{k-2},$$
$$q'_k := a'_k \cdot q_{k-1} + c_k \cdot q_{k-2}$$

gilt dann nach Induktionsvoraussetzung:

$$\frac{p'_k}{q'_k} = a_0 + \frac{c_1|}{|a_1} + \ldots + \frac{c_k|}{|a'_k}.$$

Außerdem gilt:

$$p'_k - p_k = \left(a'_k - a_k\right) \cdot p_{k-1} = \frac{c_{k+1}}{a_{k+1}} \cdot p_{k-1},$$
$$q'_k - q_k = \left(a'_k - a_k\right) \cdot q_{k-1} = \frac{c_{k+1}}{a_{k+1}} \cdot q_{k-1}.$$

Daraus folgt aber

$$\frac{p_{k+1}}{q_{k+1}} = \frac{a_{k+1} \cdot p_k + c_{k+1} \cdot p_{k-1}}{a_{k+1} \cdot q_k + c_{k+1} \cdot q_{k-1}} = \frac{a_{k+1} \cdot \left(p'_k - \frac{c_{k+1}}{a_{k+1}} \cdot p_{k-1}\right) + c_{k+1} \cdot p_{k-1}}{a_{k+1} \cdot \left(q'_k - \frac{c_{k+1}}{a_{k+1}} \cdot q_{k-1}\right) + c_{k+1} \cdot q_{k-1}}$$
$$= \frac{p'_k}{q'_k} = a_0 + \frac{c_1|}{|a_1} + \cdots + \frac{c_{k+1}|}{|a_{k+1}},$$

und damit ist der Induktionsschritt gezeigt. □

SATZ 5.1.3. *Für den Kettenbruch* (5.1) *und die zugehörigen Folgen* (5.2) *gilt:*

$$p_k \cdot q_{k-1} - q_k \cdot p_{k-1} = (-1)^{k-1} \cdot c_1 \cdots c_k \text{ für } -1 \leqslant k \leqslant n. \tag{5.3}$$

(Für $k \leqslant 0$ ist das leere Produkt $c_1 \cdots c_k$ definitionsgemäß gleich 1*.)*

BEWEIS. Induktion nach k: Für $k = -1$ ist

$$p_{-1} \cdot q_{-2} - q_{-1} \cdot p_{-2} = 1 \cdot 1 - 0 \cdot 0 = 1,$$

und für $k = 0$ ist

$$p_0 \cdot q_{-1} - q_0 \cdot p_{-1} = a_0 \cdot 0 - 1 \cdot 1 = -1 :$$

Der Induktionsanfang ist also für $k = -1, 0$ gezeigt.

Für den Induktionsschritt $k - 1 \to k$ rechnen wir unter Verwendung der rekursiven Definition (5.2):

$$\begin{aligned} p_k \cdot q_{k-1} - q_k \cdot p_{k-1} &= (a_k \cdot p_{k-1} + c_k \cdot p_{k-2}) \cdot q_{k-1} - (a_k \cdot q_{k-1} + c_k \cdot q_{k-2}) \cdot p_{k-1} \\ &= c_k \cdot (p_{k-2} \cdot q_{k-1} - q_{k-2} \cdot p_{k-1}) \\ &= c_k \cdot (-1) \cdot (-1)^{k-2} \cdot c_1 \cdots c_{k-1}. \leftarrow \text{Induktionsvoraussetzung.} \end{aligned}$$ □

5.1.1. Regelmäßige Kettenbrüche.

DEFINITION 5.1.4 (Regelmäßige Kettenbrüche). *Ein Kettenbruch*

$$a_0 + \frac{c_1|}{|a_1} + \cdots + \frac{c_n|}{|a_n}$$

heißt regelmäßig, *wenn $a_0 \in \mathbb{Z}$, $c_i = 1$ für $1 \leqslant i \leqslant n$ und $a_1, \ldots, a_n \in \mathbb{N}$. (Bei einem regelmäßigen Kettenbruch ist "automatisch" garantiert, daß kein Nenner gleich* 0 *ist.) Statt $a_0 + \frac{1|}{|a_1} + \cdots + \frac{1|}{|a_n}$ schreibt man kürzer $[a_0; a_1, \ldots, a_n]$.*

SATZ 5.1.5. *Sei $\frac{a}{b} \in \mathbb{Q}$ (mit $a \in \mathbb{Z}, b \in \mathbb{N}$), dann gibt es $a_0 \in \mathbb{Z}$ und $a_1, \ldots, a_n \in \mathbb{N}$ mit*

$$\frac{a}{b} = [a_0; a_1, \ldots, a_n].$$

BEWEIS. Setze $r_0 := b$ und bestimme $\operatorname{ggT}(a, r_0)$ mit dem euklidischen Algorithmus:

$$\begin{aligned} a &= a_0 \cdot r_0 + r_1 \\ b &= a_1 \cdot r_1 + r_2 \\ r_1 &= a_2 \cdot r_2 + r_3 \\ &\vdots \\ r_{n-2} &= a_{n-2} \cdot r_{n-1} + r_n \\ r_{n-1} &= a_n \cdot r_n \end{aligned}$$

mit $r_0 > r_1 > r_2 > \cdots > r_{n-1} > r_n > 0$. Wir zeigen nun mit Induktion nach k, daß für $1 \leqslant k \leqslant n$ gilt:

$$\frac{a}{b} = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots + \cfrac{1}{a_{k-1} + \cfrac{r_k}{r_{k-1}}}}}}$$

Der Induktionsanfang ist offensichtlich: Für $k = 1$ ist $\frac{a}{b} = \frac{a}{r_0} = a_0 + \frac{r_1}{r_0}$. Für den Induktionsschritt $(k \to k+1)$ haben wir

$$r_{k-1} = a_k \cdot r_k + r_{k+1} \implies \frac{r_{k-1}}{r_k} = a_k + \frac{r_{k+1}}{r_k} \implies \frac{r_k}{r_{k-1}} = \frac{1}{a_k + \frac{r_{k+1}}{r_k}}$$

Für $k = n$ folgt also die Behauptung, da $\frac{r_n}{r_{n-1}} = \frac{1}{a_n}$. □

BEMERKUNG 5.1.6. *Die regelmäßige Kettenbruchentwicklung einer rationalen Zahl ist nicht eindeutig: Ist $a_n > 1$, so ist $[a_0; a_1, \ldots, a_n] = [a_0; a_1, \ldots, a_n - 1, 1]$.*

BEISPIEL 5.1.7. *Wir entwickeln $\frac{37}{49}$ in einen Kettenbruch; zunächst direkt:*

$$\frac{37}{49} = 0 + \cfrac{1}{\frac{49}{37}} = 0 + \cfrac{1}{1 + \frac{12}{37}} = 0 + \cfrac{1}{1 + \cfrac{1}{\frac{37}{12}}} = 0 + \cfrac{1}{1 + \cfrac{1}{3 + \frac{1}{12}}} = 0 + \cfrac{1}{1 + \cfrac{1}{3 + \cfrac{1}{11 + \frac{1}{1}}}}.$$

Also ist $\frac{37}{49} = [0; 1, 3, 12] = [0; 1, 3, 11, 1]$.

Oder wir verwenden den euklidischem Algorithmus (wie im Beweis von Satz 5.1.5), was sichtlich auf dasselbe hinausläuft:

$$\begin{aligned} 37 &= 0 \cdot 49 + 37\colon \ a_0 = 0, \\ 49 &= 1 \cdot 37 + 12\colon \ a_1 = 1, \\ 37 &= 3 \cdot 12 + 1\colon \ a_2 = 3, \\ 12 &= 12 \cdot 1 + 0\colon \ a_3 = 12. \end{aligned}$$

Aufgabe 66: *Entwickle $\frac{167}{61}$ und $\frac{61}{167}$ in regelmäßige Kettenbrüche.*

BEISPIEL 5.1.8. *Wir bestimmen den Wert des Kettenbruchs $[2; 1, 5, 2]$ unter Verwendung der Rekurrenzrelationen (5.2):*

$$\begin{aligned} p_{k+1} &= a_{k+1} \cdot p_k + p_{k-1}, \\ q_{k+1} &= a_{k+1} \cdot q_k + q_{k-1}, \end{aligned}$$

deren Werte wir in der folgenden Tabelle übersichtlich zusammenstellen:

k	-2	-1	0	1	2	3
a_k	—	—	2	1	5	2
p_k	0	1	2	3	17	37
q_k	1	0	1	1	6	13

Also ist $[2;1,5,2] = \frac{37}{13}$. *Dasselbe Ergebnis erhält man natürlich auch durch sukzessives Vereinfachen der Nenner:*

$$2 + \cfrac{1}{1 + \cfrac{1}{5 + \cfrac{1}{2}}} = 2 + \cfrac{1}{1 + \cfrac{2}{11}} = 2 + \frac{11}{13} = \frac{37}{13}.$$

DEFINITION 5.1.9 (Näherungsbruch). *Sei* $[a_0; a_1, \ldots, a_n]$ *ein regelmäßiger Kettenbruch. Dann wird* $\frac{p_k}{q_k} = [a_0; a_1, \ldots, a_k]$ *(für* $0 \leqslant k \leqslant n$*) der k–te* Näherungsbruch *von* $[a_0; a_1, \ldots, a_n]$ *genannt.*

BEISPIEL 5.1.10. *Die k–Näherungsbrüche von* $[2;1,5,2] = \frac{37}{13}$ *(siehe vorhergehendes Beispiel mit der Tabelle der Werte* p_k *und* q_k*) sind also der Reihe nach:*

$$2, 3, \frac{17}{6}, \frac{37}{13}.$$

BEMERKUNG 5.1.11. *Für einen* regelmäßigen *Kettenbruch* $[a_0; a_1, \ldots, a_n]$ *ist offensichtlich* $p_k, q_k \in \mathbb{Z}$ *für alle* $k \geqslant -2$*, und gemäß Satz 5.1.3 gilt für alle* $k \geqslant 0$

$$p_k \cdot q_{k-1} - q_k \cdot p_{k-1} = (-1)^{k-1} \implies \mathrm{ggT}\,(p_k, q_k) = 1.$$

Mit Induktion kann man ganz leicht zeigen:

$$q_k \geqslant 2^{\frac{k-1}{2}} \text{ für alle } k \geqslant 0,$$

d.h., die Folge $(q_k)_{k \geqslant 0}$ *ist eine Folge* natürlicher *Zahlen, die exponentiell wächst.*

SATZ 5.1.12. *Sei* $[a_0; a_1, \ldots, a_n]$ *ein regelmäßiger Kettenbruch. Dann gilt:*

$$p_k \cdot q_{k-2} - q_k \cdot p_{k-2} = (-1)^k \cdot a_k \text{ für } 0 \leqslant k \leqslant n. \tag{5.4}$$

BEWEIS. Das rechnen wir einfach nach; unter Verwendung der Rekurrenzrelationen (5.2):

$$\begin{aligned} p_k \cdot q_{k-2} - q_k \cdot p_{k-2} &= (a_k \cdot p_{k-1} + p_{k-2}) \cdot q_{k-2} - (a_k \cdot q_{k-1} + q_{k-2}) \cdot p_{k-2} \\ &= a_k \cdot (p_{k-1} \cdot q_{k-2} - q_{k-1} \cdot p_{k-2}) \\ &= (-1)^k \cdot a_k \quad \leftarrow \text{gemäß (5.3) in Satz 5.1.3.} \end{aligned}$$

□

KOROLLAR 5.1.13. *Sei* $[a_0; a_1, \ldots, a_n]$ *ein regelmäßiger Kettenbruch. Dann gilt:*

$$\frac{p_{2\cdot k}}{q_{2\cdot k}} < \frac{p_{2\cdot k+2}}{q_{2\cdot k+2}} \text{ für } 0 \leqslant k \leqslant \frac{n}{2} - 1,$$
$$\frac{p_{2\cdot k+1}}{q_{2\cdot k+1}} < \frac{p_{2\cdot k-1}}{q_{2\cdot k-1}} \text{ für } 1 \leqslant k \leqslant \frac{n-1}{2}.$$

BEWEIS. Aus (5.4) in Satz 5.1.12 folgt sofort:

$$\frac{p_k}{q_k} - \frac{p_{k-2}}{q_{k-2}} = \frac{p_k \cdot q_{k-2} - q_k \cdot p_{k-2}}{q_k \cdot q_{k-2}} = (-1)^k \frac{a_k}{q_k \cdot q_{k-2}},$$

und weil $a_k, q_k \in \mathbb{N}$ für $k \geqslant 0$ (Bemerkung 5.1.11) folgt die Behauptung. □

KOROLLAR 5.1.14. *Es seien $a \in \mathbb{Z}$ und $b \in \mathbb{N}$ mit $\mathrm{ggT}(a,b) = 1$. Der Bruch $\frac{a}{b}$ habe die Entwicklung in einen regelmäßigen Kettenbruch*

$$\frac{a}{b} = [a_0; a_1, \ldots, a_n] \quad (\textit{also } \frac{a}{b} = \frac{p_n}{q_n}).$$

Dann hat die lineare diophantische Gleichung

$$a \cdot x + b \cdot y = 1$$

die Lösung

$$(x,y) = \left((-1)^{n-1} \cdot q_{n-1}, (-1)^n \cdot p_{n-1}\right).$$

BEWEIS. Nach Voraussetzung ist $\frac{a}{b} = \frac{p_n}{q_n}$ mit $b > 0$ und $\mathrm{ggT}(a,b) = 1$; gemäß Bemerkung 5.1.11 ist aber auch $q_n > 0$ und $\mathrm{ggT}(p_n, q_n) = 1$: Es ist also $a = p_n$ und $b = q_n$, und wir rechnen einfach nach:

$$\begin{aligned} a \cdot q_{n-1} - b \cdot p_{n-1} &= p_n \cdot q_{n-1} - q_n \cdot p_{n-1} \\ &= (-1)^{n-1}, \quad \leftarrow \text{gemäß (5.3) in Satz 5.1.3} \end{aligned}$$

und daraus folgt natürlich die Behauptung. □

5.2. Unendliche regelmäßige Kettenbrüche

Wir verallgemeinern unsere Definition von regelmäßigen Kettenbrüchen ein bißchen, indem wir den letzten Term a_n durch

$$a_n + z \text{ für ein } z \in [0,1) \subset \mathbb{R}$$

ersetzen (dieser letzte Term ist also nur mehr dann in $\mathbb{N}$, wenn $z = 0$), und schreiben für den entsprechenden Kettenbruch

$$a_0 + \frac{1|}{|a_1} + \cdots + \frac{1|}{|a_n + z}$$

wieder kürzer $[a_0; a_1, \ldots, a_n + z]$. Dann können wir mit dem folgenden Algorithmus eine *beliebige* Zahl $\xi \in \mathbb{R}$ in einen Kettenbruch entwickeln:

`/* Bestimme regelmäßige Kettenbruchentwicklung für` $\xi \in \mathbb{R}$ `*/`
$a_0 \leftarrow \lfloor \xi \rfloor$
$z \leftarrow \xi - \lfloor \xi \rfloor$
$n \leftarrow 0$ `/* Ab hier gilt` *immer*`:` $\xi = [a_0; a_1, \ldots, a_n + z]$ `mit` $z \in [0,1)$ `*/`
while $z > 0$ **do**
  $n \leftarrow n + 1$
  $z \leftarrow \frac{1}{z}$
  $a_n \leftarrow \lfloor z \rfloor$
  $z \leftarrow z - \lfloor z \rfloor$ `/* Insgesamt:` $z_{\mathtt{alt}} = \frac{1}{a_n + z_{\mathtt{neu}}}$ `*/`
end while
return $[a_0; a_1, a_2, \ldots]$

Aus Satz 5.1.5 wissen wir, daß dieser Algorithmus für $\xi \in \mathbb{Q}$ abbricht. Für $\xi \in \mathbb{R}\backslash\mathbb{Q}$ sieht man sofort, daß die Größe z in der **while**–Schleife des Algorithmus auch *immer* irrational bleibt:

$$z \in \mathbb{R}\backslash\mathbb{Q} \implies \frac{1}{z} \in \mathbb{R}\backslash\mathbb{Q} \implies \frac{1}{z} - \underbrace{\left\lfloor \frac{1}{z} \right\rfloor}_{\in\mathbb{Z}} \in \mathbb{R}\backslash\mathbb{Q},$$

insbesondere also $z \neq 0$; d.h., der Algorithmus bricht für irrationale Zahlen ξ *nicht* ab.

DEFINITION 5.2.1 (Regelmäßiger Kettenbrüche). *Gemäß dem eben vorgestellten Algorithmus ordnen wir jedem $\xi \in \mathbb{R}$ einen (im allgemeinen* nicht *endlichen) regelmäßigen Kettenbruch zu:*

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots}}} = [a_0; a_1, a_2, \dots]$$

mit $a_0 \in \mathbb{Z}$ und $a_i \in \mathbb{N}$ für alle $i \in \mathbb{N}$.
Die Glieder $a_k \in \mathbb{N}$ der (im allgemeinen nicht endlichen Folge) $(a_k)_{k\in\mathbb{N}}$ werden Teilnenner *des Kettenbruchs genannt. Genau wie bei den endlichen Kettenbrüchen definiert man rekursiv die Folgen $(p_k)_{k\geqslant -2}^{\infty}$, $(q_k)_{k\geqslant -2}^{\infty}$ und die (endlichen!) Näherungsbrüche $\frac{p_n}{q_n} = [a_0; a_1, \dots, a_n]$: Alle Eigenschaften, die wir für endliche Teilfolgen $(p_k)_{k\geqslant -2}^{n}$, $(q_k)_{k\geqslant -2}^{n}$ und die* endlichen *Näherungsbrüche $[a_0; a_1, \dots, a_n]$ gezeigt haben, bleiben gültig.*

Diese Definition verallgemeinert offensichtlich Definition 5.1.4: Ab nun bezeichnen wir sowohl die "*endliche* Variante" als auch die "*unendliche* Variante" einfach als regelmäßige Kettenbrüche.

SATZ 5.2.2. *Sei $[a_0; a_1, a_2, \dots]$ ein regelmäßiger Kettenbruch, der* nicht *endlich ist. Dann konvergiert die Folge der Näherungsbrüche gegen eine irrationale Zahl:*

$$\lim_{n\to\infty} \left(\frac{p_n}{q_n} \right) = \xi \in \mathbb{R}\backslash\mathbb{Q}.$$

Es gilt:

$$\frac{p_0}{q_0} < \frac{p_2}{q_2} < \frac{p_4}{q_4} < \dots < \xi < \dots < \frac{p_5}{q_5} < \frac{p_3}{q_3} < \frac{p_1}{q_1}. \tag{5.5}$$

BEWEIS. Nach Korollar 5.1.13 ist

- $\left(\frac{p_{2\cdot k}}{q_{2\cdot k}}\right)_{k\geqslant 0}$ streng monoton wachsend,
- $\left(\frac{p_{2\cdot k+1}}{q_{2\cdot k+1}}\right)_{k\geqslant 0}$ streng monoton fallend.

Aus $p_k \cdot q_{k-1} - q_k \cdot p_{k-1} = (-1)^{k-1}$ ((5.3) aus Satz Satz 5.1.3) folgt

$$\frac{p_k}{q_k} - \frac{p_{k-1}}{q_{k-1}} = \frac{(-1)^{k-1}}{q_{k-1} \cdot q_k},$$

und weil $q_k \in \mathbb{N}$ für alle $k \geqslant -2$, folgt daraus zunächst

$$\frac{p_{2\cdot k}}{q_{2\cdot k}} < \frac{p_{2\cdot k-1}}{q_{2\cdot k-1}}$$

für alle $k \in \mathbb{N}$; zusammen mit der strengen Monotonie der Teilfolgen mit geraden/ungeraden Indizes folgt

$$\frac{p_{2\cdot m}}{q_{2\cdot m}} < \frac{p_{2\cdot k-1}}{q_{2\cdot k-1}}$$

für alle $m, k \in \mathbb{N}$, denn

$$\frac{p_{2\cdot m}}{q_{2\cdot m}} < \cdots < \frac{p_{2\cdot k}}{q_{2\cdot k}} < \frac{p_{2\cdot k-1}}{q_{2\cdot k-1}} \text{ wenn } m \leqslant k,$$

und

$$\frac{p_{2\cdot m}}{q_{2\cdot m}} < \frac{p_{2\cdot m-1}}{q_{2\cdot m-1}} < \cdots < \frac{p_{2\cdot k-1}}{q_{2\cdot k-1}} \text{ wenn } m \geqslant k.$$

Außerdem folgt

$$\left|\frac{p_k}{q_k} - \frac{p_{k-1}}{q_{k-1}}\right| = \frac{1}{q_{k-1}\cdot q_k} > 0 \text{ für alle } k \in \mathbb{N},$$

und

$$\lim_{k\to\infty} \frac{1}{q_{k-1}\cdot q_k} = 0,$$

denn q_k wächst exponentiell (siehe Bemerkung 5.1.11). Insgesamt bedeutet das aber, daß $\left(\frac{p_n}{q_n}\right)$ eine *Cauchy–Folge* ist, denn für $\epsilon > 0$ beliebig gibt es ein $m \in \mathbb{N}$ mit $0 < \frac{1}{q_{2\cdot m-1}\cdot q_{2\cdot m}} < \epsilon$, und *alle* Näherungsbrüche $\frac{p_n}{q_n}$ mit $n \geqslant 2\cdot m$ liegen im Intervall

$$\left[\frac{p_{2\cdot m}}{q_{2\cdot m}}, \frac{p_{2\cdot m-1}}{q_{2\cdot m-1}}\right]$$

und haben daher voneinander Abstand kleiner ϵ: Also *konvergiert* die Folge zunächst gegen ein $\xi \in \mathbb{R}$. Dieses ξ kann aber nicht rational sein, denn aus den obigen Überlegungen ist klar, daß *kein* Näherungsbruch gleich ξ ist; wäre $\xi = \frac{a}{b} \in \mathbb{Q}$, dann müßte also

$$\left|\frac{a}{b} - \frac{p_k}{q_k}\right| = \frac{|a\cdot q_k - b\cdot p_k|}{b\cdot q_k} > 0$$

für alle k gelten, also insbesondere

$$|a\cdot q_k - b\cdot p_k| \geqslant 1 \text{ für alle } k \in \mathbb{N}_0.$$

Das würde aber bedeuten:

$$0 < \frac{1}{b\cdot q_k} \leqslant \left|\frac{a}{b} - \frac{p_k}{q_k}\right| < \left|\frac{p_{k+1}}{q_{k+1}} - \frac{p_k}{q_k}\right| = \frac{1}{q_k\cdot q_{k+1}}$$

(denn $\xi = \frac{a}{b}$ liegt *zwischen* $\frac{p_{k+1}}{q_{k+1}}$ und $\frac{p_k}{q_k}$), und daraus würde folgen:

$$q_{k+1} < b \text{ für alle } k \in \mathbb{N}_0,$$

ein Widerspruch: q_k wächst exponentiell. □

BEMERKUNG 5.2.3. *Die regelmäßige Kettenbruchentwicklung für die* Eulersche Zahl *ist*

$$\mathbb{e} = [2; 1, 2, 1, 1, 4, 1, 1, 6, 1, \dots],$$

aber für viele irrationale Zahlen ist diese Entwicklung unbekannt*; z.B. für* $\sqrt[3]{2}$ *oder* π.

Aufgabe 67: *Finde für* $0 \leqslant n \leqslant 4$ *die Teilnenner* a_n *und Näherungsbrüche* $\frac{p_n}{q_n}$ *der Zahl* π.

Literaturverzeichnis

[1] C. Baxa. Vorlesung Zahlentheorie. Mitschrift von Felix Leditzky und Christoph Harrach, 2008.

[2] G.H. Hardy and E.M. Wright. *Einführung in die Zahlentheorie*. R. Oldenbourg, München, 1958.

Index

Verzeichnis von Symbolen und Abkürzungen

$|z|$: Absolutbetrag der komplexen Zahl z. 2

$\dot{\bigcup}$: disjunkte Vereinigung. 3

$\mathbb{C}$: Körper der komplexen Zahlen. 6

$\dot{\cup}$: disjunkte Vereinigung. 3

$\mathbb{F}$: Bezeichnung für einen Körper allgemein (englisch: field). 6
$\mathbb{K}^\star$: Multiplikative Gruppe des Körpers $\mathbb{K} \setminus \{0\}$. 5
$\lfloor x \rfloor$: Nächstkleinere ganze Zahl an x. 7

ggT $(n_1, \ldots, n_k)$: Größter gemeinsamer Teiler der Zahlen $n_1, \ldots, n_k$. 12

$(\!(X)\!)$: Ideal, das von X erzeugt wird.. 13

$\mathbb{K}$: Bezeichnung für einen Körper allgemein. 6
kgV $(n_1, \ldots, n_k)$: Kleinstes gemeinsames Vielfaches der Zahlen $n_1, \ldots, n_k$. 12

$\mathbb{L}$: Bezeichnung für einen Körper allgemein. 6
$\left(\frac{a}{p}\right)$: Legendre–Symbol. 65

$\mathbb{N}$: Menge der natürlichen Zahlen $\{1, 2, 3, \ldots\}$. 1
$\mathbb{N}_0$: Menge der nichtnegativen ganzen Zahlen $\{0, 1, 2, \ldots\}$. 1
$\mathfrak{n}$: Neutrales Element einer Gruppe G. 4
$[n]$: Menge der ersten n natürlichen Zahlen: $\{1, 2, \ldots, n\}$. 1
$\mathbf{p}\,(n)$: n–te Primzahl. 23

ord: Ordnung (einer Gruppe oder eines Elements einer Gruppe). 4

$\mathbb{P}$: Menge der Primzahlen $\{2, 3, 5, 7, 11, \ldots\}$. 23
$R\,[z]$: Ring der Polynome in der Variablen z mit Koeffizienten im Ring R. 34

$\mathbb{Q}$: Körper der rationalen Zahlen. 1

$\mathbb{R}$: Körper der reellen Zahlen. 1

$|$: Teilbarkeitsrelation: $k|n \iff \exists d \in \mathbb{Z}\ \ n = k \cdot d$. 8

$\mathbb{Z}$: Ring der ganzen Zahlen $\{\ldots, -2, -2, -1, 0, 1, 2, \ldots\}$. 1