UNIVERSITÄT KOBLENZ · LANDAU

Institut für MATHEMATIK

Grundlagen der Algebra und der elementaren Zahlentheorie

Skript zur Vorlesung
Sommersemester 2011

von

Dr. Dominik Faas
Institut für Mathematik
Fachbereich 7: Natur- und Umweltwissenschaften
Universität Koblenz-Landau

Literatur zur Vorlesung

- Friedhelm Padberg: *Elementare Zahlentheorie Mathematik Primar- und Sekundarstufe* (Spektrum Akadademischer Verlag, 2008)
  - richtet sich in erster Linie an (angehende) Lehrkräfte
  - alle wesentlichen Inhalte der Vorlesung aus dem Bereich Zahlentheorie
  - sehr ausführlich
  - verständliche Beweise, viele Beispiele bzw. Aufgaben, interessante Anwendungen
- Harald Scheid: *Einführung in die Zahlentheorie* (Klett Studienbücher, 1972)
  - alle wesentlichen Inhalte der Vorlesung aus dem Bereich Zahlentheorie, Grundlagen der Theorie der Gruppen und Ringe
  - formal und präzise
  - Beweise, viele Aufgaben
- Harald Scheid, Lutz Warlich: *Mathematik für Lehramtskandidaten Band II: Algebraische Strukturen und Zahlbereiche* (Akademische Verlagsgesellschaft, 1974)
  - richtet sich in erster Linie an (angehende) Lehrkräfte
  - grundlegender Zugang zu algebraischen Strukturen (Gruppen, Ringe, Körper), Anwendung auf Zahlbereichserweiterungen, und die natürlichen Zahlen
  - formal und präzise
  - Beweise, Beispiele
- Hans-Joachim Gorski, Susanne Müller-Philipp: *Leitfaden Arithmetik* (vieweg, 1999)
  - richtet sich in erster Linie an (angehende) Lehrkräfte
  - viele Inhalte der Vorlesung aus dem Bereich Zahlentheorie
  - ausführliche Beweise, viele Beispiele bzw. Aufgaben
- Alan Bell: *Algebraische Strukturen* (Raeber Verlag, 1966)
  - grundlegender Zugang zu algebraischen Strukturen (Gruppen, Ringe, Körper) mit geeigneten Beispielen, Permutationsgruppen
  - theoretischer Zugang
  - Beweise, Aufgaben

- Jürg Krämer: *Zahlen für Einsteiger: Elemente der Algebra und Aufbau der Zahlbereiche* (vieweg, 2008)
  - richtet sich in erster Linie an (angehende) Lehrkräfte
  - viele Inhalte der Vorlesung aus dem Bereich Zahlentheorie, Systematisierung mit Hilfe algebraischer Strukturen (Gruppen, Ringe, Körper)
  - formal und präzise
  - Beweise, Beispiele
- Jürgen Wolfard: *Einführung in die Zahlentheorie und Algebra* (vieweg studium,1996)
  - richtet sich in erster Linie an (angehende) Lehrkräfte
  - viele Inhalte der Vorlesung aus dem Bereich Zahlentheorie, Systematisierung mit Hilfe algebraischer Strukturen (Gruppen, Ringe, Körper)
  - sehr formal und präzise
  - Beweise, Aufgaben
  - geht weit über die Inhalte der Vorlesung hinaus
- Stefan Müller-Stach, Jens-Piontkowski: *Elementare und algebraische Zahlentheorie Ein moderner Zugang zu klassischen Themen* (vieweg, 2006)
  - richtet sich in erster Linie an (angehende) Lehrkräfte
  - viele Inhalte der Vorlesung aus dem Bereich Zahlentheorie, weitergehendes Studium der Zahlentheorie mit Hilfe algebraischer Strukturen (Gruppen, Ringe, Körper)
  - sehr formal und präzise
  - Beweise, Beispiele
  - geht weit über die Inhalte der Vorlesung hinaus

Bezeichnungen

Wir benutzen (manchmal) die folgenden Symbole:

$\forall$	:	für alle
$\exists$	:	es existiert (mindestens) ein
$\nexists$	:	es existiert kein
$\exists!$	:	es existiert genau ein
$\wedge$	:	und
$\vee$	:	oder
$\dot{\vee}$	:	entweder oder

Wichtig für uns sind (unter anderem) die folgenden Mengen:

$\mathbb{N} = \{1, 2, 3, \ldots\}$	Menge der natürlichen Zahlen
$\mathbb{N}_0 = \mathbb{N} \cup \{0\} = \{0, 1, 2, 3, \ldots\}$	Menge der natürlichen Zahlen und der 0
$\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$	Menge der ganzen Zahlen
$\mathbb{Q} = \left\{\frac{a}{b};\ a, b \in \mathbb{Z},\ b \neq 0\right\}$	Menge der rationalen Zahlen

0 Die ganzen Zahlen — Einleitung

In weiten Teilen dieser Vorlesung widmen wir uns dem Studium der ganzen Zahlen. Die Menge der ganzen Zahlen

$$\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$$

kann wie folgt eingeordnet werden:

$$\boxed{\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q}} \subset \mathbb{R} \subset \mathbb{C}$$

Dabei sind

$$\mathbb{N} = \{a \in \mathbb{Z};\ a > 0\} = \{1, 2, 3, \ldots\} \quad \text{(Menge der positiven ganzen Zahlen)}$$
$$\mathbb{Q} = \left\{\frac{a}{b};\ a, b \in \mathbb{Z},\ b \neq 0\right\} \quad \text{(Menge der Brüche (Quotienten) ganzer Zahlen)}$$

Bemerkung 0.1. *(Verknüfungen in $\mathbb{Z}$)*

- *(Addition) Zwei ganze Zahlen $a, b \in \mathbb{Z}$ können addiert werden und man erhält als Ergebnis wieder eine ganze Zahl $a + b \in \mathbb{Z}$.*

$$3 + 5 = 8, \quad (-19) + 7 = -12, \quad (-1) + (-5) = -6, \quad \ldots$$

- *(Kommutativgesetz und Assoziativgesetz der Addition) Für alle $a, b, c \in \mathbb{Z}$ gilt: $a + b = b + a$ und $(a + b) + c = a + (b + c)$.*

$$(-19) + 7 = -12 = 7 + (-19), \quad (\underbrace{2 + 3}_{=5}) + 4 = 9 = 2 + (\underbrace{3 + 4}_{=7})$$

- *(Neutrales Element der Addition) Es existiert eine ganze Zahl* $0 \in \mathbb{Z}$ *mit* $a + 0 = 0 + a = a$ *für alle* $a \in \mathbb{Z}$.

$$0 + 4 = 4, \quad (-23) + 0 = -23, \quad \dots$$

- *(Inverse Elemente bzgl. der Addition) Zu jeder ganzen Zahl* $a \in \mathbb{Z}$ *gibt es eine ganze Zahl* $-a \in \mathbb{Z}$ *mit* $a + (-a) = (-a) + a = 0$.

  additiv invers zu 3 *ist* -3, *additiv invers zu* -12 *ist* 12, *additiv invers zu* 0 *ist* 0

- *(Subtraktion) Basierend auf der Addition und der Existenz der Inversen kann die Subtraktion definiert werden:* $a - b \overset{def}{=} a + (-b) \in \mathbb{Z}$ *für* $a, b \in \mathbb{Z}$

$$10 - 6 = 4, \quad 22 - 100 = -78 \quad -12 - (-5) = -7, \quad \dots$$

- *(Äquivalenzumformungen mit der Addition) Für alle* $a, b, c \in \mathbb{Z}$ *gilt die Äquivalenz:* $a = b \Leftrightarrow a + c = b + c$

$$x + 10 = 5 \Leftrightarrow x + 10 + (-10) = 5 + (-10) \qquad \big(\Leftrightarrow x = -5\big)$$

- *(Multiplikation) Zwei ganze Zahlen* $a, b \in \mathbb{Z}$ *können multipliziert werden und man erhält als Ergebnis wieder eine ganze Zahl* $a \cdot b \in \mathbb{Z}$.

$$8 \cdot 3 = 24, \quad 2 \cdot (-5) = -10, \quad (-1) \cdot (-12) = 12 \quad \dots$$

- *(Kommutativgesetz und Assoziativgesetz der Multiplikation) Für alle* $a, b, c \in \mathbb{Z}$ *gilt:* $a \cdot b = b \cdot a$ *und* $(a \cdot b) \cdot c = a \cdot (b \cdot c)$

$$(-4) \cdot 6 = -24 = 6 \cdot (-4), \quad (\underbrace{(-4) \cdot 5}_{=-20}) \cdot 6 = -120 = (-4) \cdot (\underbrace{5 \cdot 6}_{=30})$$

- *(Neutrales Element der Multiplikation) Es existiert eine ganze Zahl* $1 \in \mathbb{Z}$ *mit* $a \cdot 1 = 1 \cdot a = x$ *für alle* $a \in \mathbb{Z}$.

$$1 \cdot 7 = 7, \quad (-8) \cdot 1 = -8, \quad \dots$$

- *Zu* $x \in \mathbb{Z}$ *nennt man ein Element* $y \in \mathbb{Z}$ *multiplikativ invers zu* x, *falls* $x \cdot y = 1$ *ist. Die einzigen ganzen Zahlen, die ein multiplikativ Inverses in* $\mathbb{Z}$ *haben sind* -1 *und* 1. *Eine Division ganzer Zahlen (mit Ergebnis in* $\mathbb{Z}$*) ist im Allgemeinen nicht möglich.*

  mult. invers zu 1 *ist* 1, *mult. invers zu* -1 *ist* -1, *zu* 2 *exist. kein mult. Inverses in* $\mathbb{Z}$

- *(Distributivgesetz) Für alle* $a, b, c \in \mathbb{Z}$ *gilt:* $a \cdot (b + c) = a \cdot b + a \cdot c$

$$2 \cdot (\underbrace{5 + (-8)}_{=-3}) = -6 = \underbrace{2 \cdot 5}_{=10} + \underbrace{2 \cdot (-8)}_{=-16}$$

- *(Nullprodukt) Für alle $a, b \in \mathbb{Z}$ gilt die Äquivalenz:* $a \cdot b = 0 \;\Leftrightarrow\; a = 0$ *oder* $b = 0$

$$3 \cdot 0 = 0, \quad 0 \cdot (-4) = 0, \quad 0 \cdot 0 = 0, \quad \underbrace{3}_{\neq 0} \cdot \underbrace{5}_{\neq 0} \neq 0$$

- *(Kürzungsregel) Für alle $a, b, c \in \mathbb{Z}$ mit $c \neq 0$ gilt die Äquivalenz:* $a = b \;\Leftrightarrow\; a \cdot c = b \cdot c$

$$10 = 5 \cdot x \;\Leftrightarrow\; 2 \cdot 5 = x \cdot 5 \overset{5 \neq 0}{\Leftrightarrow} 2 = x$$

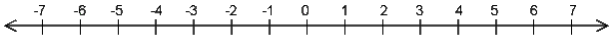
Bemerkung 0.2. *(Größenrelation in $\mathbb{Z}$)*
Es gibt eine Relation $\leq$ auf $\mathbb{Z}$ mit folgenden Eigenschaften:

- *$\leq$ ist eine totale Ordnungsrelation, das heißt, für alle $a, b, c \in \mathbb{Z}$ gilt:*
  - *(Reflexivität) $a \leq a$*
  - *(Transitivität) Aus $a \leq b$ und $b \leq c$ folgt $a \leq c$.*
  - *(Antisymmetrie) Aus $a \leq b$ und $b \leq a$ folgt $a = b$.*
  - *(Totalität) Es gilt stets $a \leq b$ oder $b \leq a$.*

  Falls $a \leq b$ gilt, sagt man: a ist kleiner oder gleich b.

- *(Abgeleitete Relationen) Mithilfe der Relation $\leq$ definiert man $a < b$ (a ist kleiner als b), falls $a \leq b$ und $a \neq b$ gilt. Statt $a \leq b$ schreibt man auch $b \geq a$ (b ist größer oder gleich a) und statt $a < b$ schreibt man auch $b > a$ (b ist größer als a).*

- *(Anordnung auf der Zahlengeraden) Jede ganze Zahl entspricht einem Punkt auf der Zahlengeraden:*



  Dabei gilt $a < b$ genau dann, wenn b einem Punkt entspricht, der weiter rechts auf der Zahlengerade liegt, als der a zugeordnete Punkt.

- *(Verträglichkeit mit der Addition) Für $a, b, c \in \mathbb{Z}$ gilt:*

$$\left\{ \begin{array}{rcl} a \leq b & \Leftrightarrow & a + c \leq b + c \\ a < b & \Leftrightarrow & a + c < b + c \end{array} \right\}$$

  Insbesondere ist $n + m \in \mathbb{N}$, falls $n, m \in \mathbb{N}$ sind.

- *(Verträglichkeit mit der Multiplikation) Für $a, b, c \in \mathbb{Z}$ gilt:*

$$\left\{ \begin{array}{rcl} a \leq b & \Leftrightarrow & a \cdot c \leq b \cdot c \\ a < b & \Leftrightarrow & a \cdot c < b \cdot c \end{array} \right\} \quad , \quad \text{falls } c > 0$$

$$\left\{ \begin{array}{rcl} a \leq b & \Leftrightarrow & a \cdot c \geq b \cdot c \\ a < b & \Leftrightarrow & a \cdot c > b \cdot c \end{array} \right\} \quad , \quad \text{falls } c < 0$$

  Insbesondere ist $n \cdot m \in \mathbb{N}$, falls $n, m \in \mathbb{N}$ sind.

- *(Existenz eines Minimums für Teilmengen von $\mathbb{N}$) Jede nichtleere Teilmenge von $\mathbb{N}$ hat ein kleinstes Element (Minimum).*

Bemerkung 0.3. *(Potenzen)*
Für $a \in \mathbb{Z}$ und $n \in \mathbb{N}_0$ definiert man $a^n \in \mathbb{Z}$ durch

$$a^n \overset{def}{=} \underbrace{a \cdot a \cdot \ldots \cdot a}_{n\text{-mal}} \ (\text{falls } n > 0) \quad \text{und} \quad a^0 \overset{def}{=} 1$$

Es gilt stets $1^n = 1$ und $0^m = 0$ (falls $m > 0$). Außerdem gelten die Potenzgesetze: Für alle $a, b \in \mathbb{Z}$ und alle $n, m \in \mathbb{N}_0$ ist:

$$(a \cdot b)^n = a^n \cdot b^n, \quad a^n \cdot a^m = a^{n+m}, \quad (a^n)^m = a^{n \cdot m}$$

Bemerkung 0.4. *(Betrag)*
Für $a \in \mathbb{Z}$ definiert man den **Betrag** *von a als*

$$|a| \overset{def}{=} \begin{cases} a & , \ \text{falls } a \geq 0 \\ -a & , \ \text{falls } a < 0 \end{cases}$$

Duch $|a - b|$ wird der Abstand zweier ganzer Zahlen $a, b \in \mathbb{Z}$ auf der Zahlengeraden angegeben. Für alle $a, b \in \mathbb{Z}$ und alle $n \in \mathbb{N}$ gelten:

$$|a| \geq 0, \quad |a \cdot b| = |a| \cdot |b|, \quad |a^n| = |a|^n, \quad |a + b| \leq |a| + |b|, \quad |a| = 0 \ \Leftrightarrow \ a = 0$$

1 Teilbarkeit

Frage.
Für welche $a, b \in \mathbb{Z}$ ist eine Division $b : a = x$ mit Ergebnis $x \in \mathbb{Z}$ möglich? Umformuliert ergibt sich $b = x \cdot a$ $\big($falls $a \neq 0$ ist$\big)$. Es stellt sich also die Frage, ob zu gegebenen $a, b \in \mathbb{Z}$ ein $x \in \mathbb{Z}$ mit $b = x \cdot a$ existiert.

- *Für $b = 30$ und $a = 5$: Ja, $x = 6$.*
- *Für $b = 34$ und $a = 3$: Nein.* $\big(11 \cdot 3 = 33 < 34 < 36 = 12 \cdot 3\big)$

Den Begriff der Teilbarkeit kann also definiert werden, ohne die Division direkt zu benutzen.

Definition 1.1. *(Teilbarkeit)*
Für $a, b \in \mathbb{Z}$ defniert man $a \mid b$, falls eine Zahl $x \in \mathbb{Z}$ existiert mit $x \cdot a = b$.
Man sagt dann: a ist ein Teiler von b (kurz: a teilt b), oder umgekehrt: b ist ein Vielfaches von a. Falls a kein Teiler von b ist, so schreibt man $a \nmid b$.

Beispiel.

- $5 \mid 30$, *denn* $6 \cdot 5 = 30$. $\big(5$ *ist ein Teiler von* 30 *bzw.* 30 *ist ein Vielfaches von* $5.\big)$
- $(-4) \mid 104$, *denn* $(-26) \cdot (-4) = 104$.
- $8 \mid (-8)$, *denn* $(-1) \cdot 8 = -8$.
- $(-8) \mid 8$, *denn* $(-1) \cdot (-8) = 8$.
- $3 \nmid 34$, *denn es gibt* <u>kein</u> $x \in \mathbb{Z}$ *mit* $x \cdot 3 = 34$.

Bemerkung. *(Teilbarkeit in $\mathbb{Q}$)*
Kann man den Begriff der Teilbarkeit analog für rationale Zahlen definieren? Ein Versuch:

$$\text{Für } p, q \in \mathbb{Q}: \quad p \mid q \overset{def}{\Leftrightarrow} \exists x \in \mathbb{Q} \text{ mit } q = x \cdot p$$

Damit erhält man $p \mid q$ für <u>alle</u> *$p, q \in \mathbb{Q}$ mit $q \neq 0$. Der Teilbarkeitsbegriff kann in gleicher Weise für die rationalen Zahlen definiert werden, ist dort aber nicht besonders interessant.*

Satz 1.2. *(Eigenschaften der Teilbarkeitsrelation)*

(a) Für alle $a, b, c \in \mathbb{Z}$ gilt:

- *$a \mid a$ (Reflexivität)*
- *Aus $a \mid b$ und $b \mid c$ folgt $a \mid c$. (Transitivität)*
- *Aus $a \mid b$ und $b \mid a$ folgt $a = b$ oder $a = -b$. (Antisymmterie liegt "nur bis aufs Vorzeichen" vor.)*

Die Teilbarkeitsrelation ist also eine Quasiordnung aber keine Halbordnung auf

$\mathbb{Z}$. *Auf* $\mathbb{N}$ *ist die Teilbarkeitsrelation hingegen eine Halbordnung, d.h. sie ist reflexiv, transitiv und antisymmetrisch.*

(b) *Weder auf* $\mathbb{Z}$ *noch auf* $\mathbb{N}$ *ist die Teilbarkeitsrelation total, d.h. es gibt Zahlen* $a, b \in \mathbb{N}$ *mit* $a \nmid b$ *und* $b \nmid a$.

(c) *Weitere Eigenschaften der Teilbarkeitsrelation sind (für* $a, b, \tilde{a}, \tilde{b} \in \mathbb{Z}$ *beliebig):*

- *Es gilt die Äquivalenz:*

$$a \mid b \quad \Leftrightarrow \quad (-a) \mid b \quad \Leftrightarrow \quad a \mid (-b) \quad \Leftrightarrow \quad (-a) \mid (-b)$$

  (Teilbarkeit ist also "unabhängig vom Vorzeichen".)

- *Es gilt* $a \mid 0$ *und* $1 \mid a$.
- *Aus* $a \mid b$ *und* $b \neq 0$ *folgt* $|a| \leq |b|$.
- *Aus* $a \mid b$ *und* $\tilde{a} \mid \tilde{b}$ *folgt* $(a \cdot \tilde{a}) \mid (b \cdot \tilde{b})$.
- *Falls* $a \mid b$ *gilt (und* $a \neq 0$ *ist), so ist* $\frac{b}{a} \in \mathbb{Z}$ *und es gilt* $\left(\frac{b}{a}\right) \mid b$. *Man nennt* $\frac{b}{a}$ *den* **Komplementärteiler** *zu* a *(von* b*).*

$$\begin{aligned} b = 36: \qquad & \textit{Komplementärteiler zu } a = 3 \textit{ ist } \frac{36}{3} = 12. \\ & \textit{Komplementärteiler zu } a = 1 \textit{ ist } 36. \\ & \textit{Komplementärteiler zu } a = 6 \textit{ ist } 6. \end{aligned}$$

(d) *Für* $a, b, c \in \mathbb{Z}$ *gilt:*

$$(a \cdot b) \mid c \quad \Rightarrow \quad a \mid c \textit{ und } b \mid c$$

Die umgekehrte Implikation ist im allgemeinen falsch.

(e) *Es gilt der* **Satz über die Vielfachensumme**, *d.h. für alle* $a, b, c, u, v \in \mathbb{Z}$ *gilt:*

$$\begin{aligned} & a \mid b \textit{ und } a \mid c \quad \Rightarrow \quad a \mid (ub + vc) \\ \textit{Insbesondere:} \quad & a \mid b \textit{ und } a \mid c \quad \Rightarrow \quad a \mid (b + c) \textit{ und } a \mid (b - c) \end{aligned}$$

Definition 1.3. *(Teiler- und Vielfachenmenge)*

(a) *Für* $a \in \mathbb{Z}$ *definiert man die* **Teilermenge** *von* a *als die Menge aller positiven Teiler von* a, *also:*

$$T(a) \stackrel{def}{=} \{x \in \mathbb{N};\ x \mid a\} \subset \mathbb{N}$$

Für $a_1, a_2, \ldots, a_k \in \mathbb{Z}$ *heißt weiterhin*

$$T(a_1, a_2, \ldots, a_k) \stackrel{def}{=} T(a_1) \cap T(a_2) \cap \ldots \cap T(a_k) = \{x \in \mathbb{N};\ x \mid a_j \textit{ für alle } j = 1, \ldots, k\} \subset \mathbb{N}$$

gemeinsame Teilermenge *von* $a_1, a_2, \ldots, a_k$.

(b) *Für* $a \in \mathbb{Z}$ *definiert man die* **Vielfachenmenge** *von* a *als die Menge aller positiven Vielfachen von* a, *also:*

$$V(a) \stackrel{def}{=} \{x \in \mathbb{N};\ a \mid x\} \subset \mathbb{N}$$

Für $a_1, a_2, \ldots, a_k \in \mathbb{Z}$ heißt weiterhin

$$V(a_1, a_2, \ldots, a_k) \overset{def}{=} V(a_1) \cap V(a_2) \cap \ldots \cap V(a_k) = \{x \in \mathbb{N};\ a_j \mid x \text{ für alle } j = 1, \ldots, k\} \subset \mathbb{N}$$

gemeinsame Vielfachenmenge *von $a_1, a_2, \ldots, a_k$.*

Beispiel.

- $T(12) = \{1, 2, 3, 4, 6, 12\}$
- $T(-12) = \{1, 2, 3, 4, 6, 12\}$
- $T(90) = \{1, 2, 3, 5, 6, 9, 10, 15, 18, 30, 45, 90\}$
- $T(11) = \{1, 11\}$
- $T(32) = \{1, 2, 4, 8, 16, 32\}$
- $T(36) = \{1, 2, 3, 4, 6, 9, 12, 18, 36\}$
- $T(12, 90) = \{1, 2, 3, 4, 6, 12\} \cap \{1, 2, 3, 5, 6, 9, 10, 15, 18, 30, 45, 90\} = \{1, 2, 3, 6\}$
- $T(12, 90, 32) = \{1, 2\}$
- $T(12, 36) = \{1, 2, 3, 4, 6, 12\} \cap \{1, 2, 3, 4, 6, 9, 12, 18, 36\} = \{1, 2, 3, 4, 6, 12\} = T(12)$
- $T(11, 12) = \{1\}$
- $V(2) = \{2, 4, 6, 8, \ldots\} = \{a \in \mathbb{N};\ a \text{ gerade}\}$
- $V(15) = \{15, 30, 45, 60, \ldots\}$
- $V(2, 15) = \{2, 4, 6, 8, \ldots\} \cap \{15, 30, 45, 60, \ldots\} = \{30, 60, \ldots\}$

Bemerkung 1.4. *(Eigenschaften von Teiler- und Vielfachenmenge)*

(a) Elemente von Teiler- bzw. Vielfachenmenge einer Zahl $a \in \mathbb{Z}$ sind definitionsgemäß nur die positiven Teiler bzw. Vielfache von a, also gilt stets $T(a), V(a) \subset \mathbb{N}$.

(b) Offenbar gilt $T(a) = T(-a)$ und $V(a) = V(-a)$ für alle $a \in \mathbb{Z}$.

(c) Zur Anzahl der positiven Teiler einer Zahl $a \in \mathbb{Z}$ beachte man:

- *Es gilt $T(0) = \mathbb{N}$.*
- *Es gilt $T(1) = T(-1) = \{1\}$.*
- *Für alle $a \in \mathbb{Z} \setminus \{-1, 0, 1\}$ gilt $2 \leq |T(a)| \leq |a|$.*
  (Man beachte dabei, dass stets $1, a \in T(a)$ gilt.)

Teilermengen sind (mit Ausnahme der Teilermenge der 0) also insbesondere immer endlich.

(d) Man nennt zwei Zahlen $a, b \in \mathbb{Z} \setminus \{0\}$ **teilerfremd***, falls $T(a, b) = \{1\}$ gilt. Die Zahlen 1 und -1 sind zu jeder weiteren Zahl teilerfremd.*

(e) Es gilt $V(0) = \varnothing$ *und* $V(1) = \mathbb{N}$. *Für* $a \in \mathbb{Z} \setminus \{0\}$ *gilt* $V(a) = \{n \cdot |a|;\ n \in \mathbb{N}\}$ *und folglich* $|V(a)| = \infty$.

(f) Für $a, b \in \mathbb{Z}$ *gilt die Äquivalenz:*

$$a \mid b \quad \Leftrightarrow \quad T(a) \subset T(b) \quad \Leftrightarrow \quad T(a,b) = T(a) \quad \Leftrightarrow \quad V(b) \subset V(a) \quad \Leftrightarrow \quad V(a,b) = V(b)$$

Bemerkung 1.5. *(Hassediagramme bzw. Teilerdiagramme)*

(a) Eine gegebene endliche Teilmenge $M \subset \mathbb{N}$ *kann mit einem* **Hassediadramm** *bezüglich der Teilbarkeitsrelation (strukturiert) dargestellt werden. Dabei sind folgende Regeln einzuhalten:*

- *Alle Elemente von* M *kommen vor (Knoten).*
- *Sind* $x, y \in M$ *mit* $x \neq y$ *und* $x \mid y$, *so muss* y *höher als* x *stehen.*
- *Sind* $x, y \in M$ *mit* $x \neq y$, *so werden* x *und* y *mit einem Strich (Kante) verbunden, falls* $x \mid y$ *gilt, aber kein* $z \in M \setminus \{x, y\}$ *mit* $x \mid z$ *und* $z \mid y$ *existiert.*

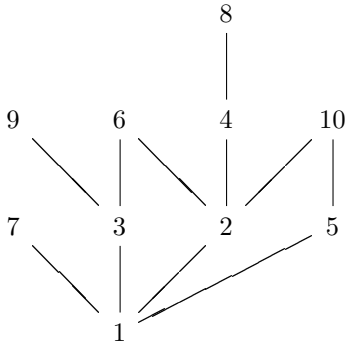
In einem solchen Hassediagramm gilt dann stets:
Sind $x, y \in M$ *mit* $x \neq y$, *so gilt* $x \mid y$ *genau dann, wenn* y *höher als* x *steht und* x *und* y *(über eine oder mehrere Kanten) miteinander verbunden sind.*

(b) Insbesondere für $M = T(a)$ $\big($*mit einer Zahl* $a \in \mathbb{Z} \setminus \{0\}\big)$ *erhält man dabei ein* **Teilerdiagramm** *von* a. *Es stellt alle Teiler von* a *und ihre Teilbarkeitsbeziehungen untereinander dar.*

(c) Ein Hassediagramm kann auch für eine beliebige Halbordnung $\preccurlyeq$ *auf einer endlichen Menge* M *erstellt werden: Zwei Elemente von* M *(Knoten) werden mit einem Strich (Kante) verbunden, falls* $x \preccurlyeq y$ *gilt, aber kein* $z \in M \setminus \{x, y\}$ *mit* $x \preccurlyeq z$ *und* $z \preccurlyeq y$ *existiert. (In diesem Fall muss* y *höher als* x *stehen.)*

Beispiel.

- *Hassediagramm der Menge* $M = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$ *bezüglich der Teilbarkeitsrelation*



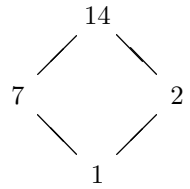
- *Hassediagramm der Menge* $M = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$ *bezüglich der Größen-*

relation $\leq$*:*

$$10 \text{ —— } 9 \text{ —— } 8 \text{ —— } 7 \text{ —— } 6 \text{ —— } 5 \text{ —— } 4 \text{ —— } 3 \text{ —— } 2 \text{ —— } 1$$

(*um 90° im Uhrzeigersinn zu drehen*)

- *Teilerdiagramm von* 14 : $T(14) = \{1, 2, 7, 14\}$

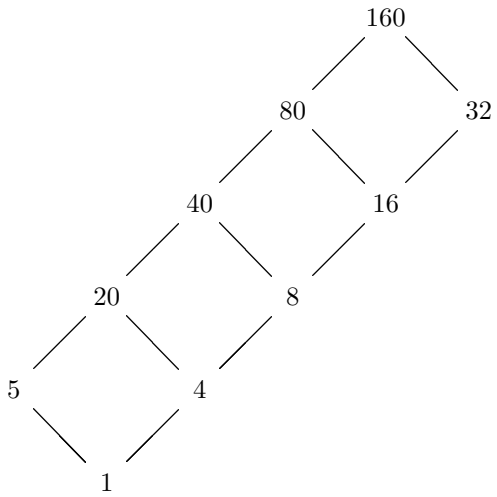


- *Teilerdiagramm von* 243 : $T(243) = \{1, 3, 9, 27, 81, 243\}$

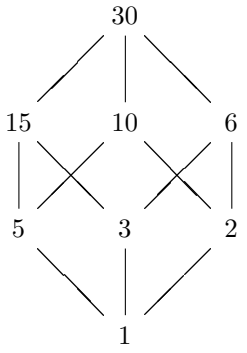
$$243 \text{ —— } 81 \text{ —— } 27 \text{ —— } 9 \text{ —— } 3 \text{ —— } 1$$

(*um 90° im Uhrzeigersinn zu drehen*)

- *Teilerdiagramm von* 160 : $T(160) = \{1, 2, 4, 5, 8, 10, 16, 20, 32, 40, 80, 160\}$

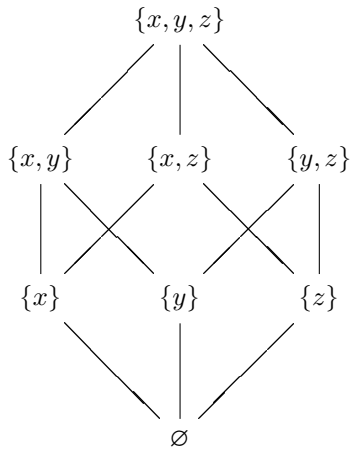


- *Teilerdiagramm von* 30 : $T(30) = \{1, 2, 3, 5, 6, 10, 15, 30\}$



- *Hassediagramm der Menge M aller Teilmengen der 3-elementigen Menge $\{x, y, z\}$ bezüglich der Inklusion $\subseteq$:*

$$M = \big\{\ \varnothing, \{x\}, \{y\}, \{z\}, \{x, y\}, \{x, z\}, \{y, z\}, \{x, y, z\}\big\}$$



Satz 1.6. *(Division mit Rest)*
Gegeben sei eine beliebige Zahl $m \in \mathbb{N}$. Dann existieren zu jeder Zahl $a \in \mathbb{Z}$ eindeutige Zahlen $q \in \mathbb{Z}$ und $r \in \{0, \ldots, m-1\}$ mit

$$a = q \cdot m + r \qquad (\textit{im Fall } a > 0 \textit{ schreibt man auch } \quad a : m = q \textit{ Rest } r)$$

Die Zahl r wird als **Rest** *bei Division von a durch m bezeichnet und ist die eindeutig bestimmte Zahl $r \in \{0, \ldots, m-1\}$ mit $m \mid (a - r)$. Es gilt genau dann $m \mid a$, wenn $r = 0$ ist.*

Beispiel.

- $a = 30,\ m = 7$

  $30 = \ldots = (-1)\cdot 7 + 37 = 0\cdot 7 + 30 = 1\cdot 7 + 23 = 2\cdot 7 + 16 = 3\cdot 7 + 9 = \boxed{4 \cdot 7 + 2} = 5\cdot 7 + (-5) = 6\cdot 7 + (-12) = \ldots$

  Also: $q = 4,\ r = 2 \ \Rightarrow\ \boxed{30 : 7 = 4 \textit{ Rest } 2}$ *Es ist* $2 \in \{0, \ldots, 6\}$ *mit* $7 \mid (30 - 2)$.

- $\boxed{42 : 6 = 7 \textit{ Rest } 0}$ *Es ist* $0 \in \{0, \ldots, 5\}$ *mit* $6 \mid (42 - 0)$.

- $a = -30,\ m = 7 \ \Rightarrow\ q = -5,\ r = 5$ $\big(\textit{denn } -30 = (-5) \cdot 7 + 5 \textit{ und } 5 \in \{0, \ldots, 6\}\big)$
  Es ist $5 \in \{0, \ldots, 6\}$ *mit* $7 \mid (-30 - 5)$.

2 Primzahlen und Primzahlzerlegung

Definition 2.1. *(Primzahlen)*
Eine Zahl $p \in \mathbb{N}$ *heißt* **Primzahl**, *falls* $|T(p)| = 2$. *(Man sagt dann auch:* p **ist prim**.*) Wir schreiben*

$$\mathbb{P} \overset{def}{=} \{p \in \mathbb{N};\ p \text{ ist Primzahl}\} \subset \mathbb{N}.$$

Eine Zahl $n \in \mathbb{N}$ *mit* $n \geq 2$, *die keine Primzahl ist, heißt* **zusammengesetzte Zahl**.

Beispiel.

- $|T(17)| = |\{1, 17\}| = 2 \ \Rightarrow\ 17$ *ist eine Primzahl*
- $|T(25)| = |\{1, 5, 25\}| = 3 > 2 \ \Rightarrow\ 25$ *ist eine zusammengesetzte Zahl*
- *Die zehn kleinsten Primzahlen sind:* $2, 3, 5, 7, 11, 13, 17, 19, 23, 29$

Bemerkung 2.2. *(Eigenschaften von Primzahlen)*

(a) Die Zahl 1 *ist keine Primzahl, denn es ist* $|T(1)| = |\{1\}| = 1$.

(b) Für $n \in \mathbb{N}$ *mit* $n \geq 2$ *sind die folgenden Aussagen äquivalent:*

(i) n *ist eine Primzahl.*

(ii) Es gilt $T(n) = \{1, n\}$.

(iii) Aus $x|n$ *mit* $x \in \mathbb{N}$ *folgt* $x = 1$ *oder* $x = n$.

(iv) Aus $n = x \cdot y$ *mit* $x, y \in \mathbb{N}$ *folgt* $x = 1$ *oder* $y = 1$ *(und entsprechend* $y = n$ *oder* $x = n$*)*.

Wir erkennen hier bereits verschiedene Aspekte von Primzahlen:

- *(Anzahl der Teiler) Primzahlen sind definitionsgemäß genau die Zahlen, die nur zwei (positive) Teiler haben, nämlich die Zahl* 1 *und sich selbst. (Alle zusammengesetzten Zahlen haben mehr als* 2 *Teiler.) Das Teilerdiagramm einer Primzahl* p *ist daher besonders einfach:*

- *(Unzerlegbarkeit) Primzahlen lassen sich (unter Nichtberücksichtigung der Reihenfolge) nur auf eine einzige Art und Weise als Produkt zweier natürlicher Zahlen schreiben, nämlich* $p = 1 \cdot p$ $(p \in \mathbb{P})$.
  - *Man kann* 30 *Plättchen zu mehreren verschiedenen Rechtecken anordnen, z.B. in einem* 5×6*-, in einem* 3×10*-, in einem* 2×15*- oder in einem* 1×30*-Rechteck.*

– *Will man* 31 *Plättchen in einem Rechteck anordnen, so gibt es nur auf die 'extreme' Möglichkeit eines* 1×31*-Rechtecks.*

(c) Ist $n \in \mathbb{N}$ *eine zusammengesetzte Zahl, so existieren also Zahlen* $x, y \in \mathbb{N}$ *mit* $x \geq 2$ *und* $y \geq 2$*, so dass* $n = x \cdot y$ *ist. Mindestens eine dieser beiden Zahlen* x, y *muss* $\leq \sqrt{n}$ *sein. Folglich hat jede zusammengesetzte Zahl* n *einen Teiler* a *mit* $2 \leq a \leq \sqrt{n}$*. Für* $n \in \mathbb{N}$ *gilt also:*

$$n \text{ ist prim} \quad \Leftrightarrow \quad \text{es gibt kein } a \in T(n) \text{ mit } 2 \leq a \leq \sqrt{n}$$

Man kann dies nutzen, um festzustellen, ob n *eine Primzahl ist:*

- $\boxed{\text{Ist } 137 \text{ eine Primzahl?}}$ *Wegen* $\sqrt{137} \approx 11.7$*, ist zu prüfen, ob eine der Zahlen* $2, \ldots, 11$ *ein Teiler von* 137 *ist.* 137 *ist eine Primzahl, denn:*

$$2 \nmid 137, \quad 3 \nmid 137, \quad 4 \nmid 137, \quad 5 \nmid 137, \quad 6 \nmid 137, \quad 7 \nmid 137$$
$$8 \nmid 137, \quad 9 \nmid 137, \quad 10 \nmid 137, \quad 11 \nmid 137$$

- $\boxed{\text{Ist } 209 \text{ eine Primzahl?}}$ *Wegen* $\sqrt{209} \approx 14.5$*, ist zu prüfen, ob eine der Zahlen* $2, \ldots, 14$ *ein Teiler von* 209 *ist.* 209 *ist keine Primzahl, denn:*

$$2 \nmid 209 \quad 3 \nmid 209, \quad 4 \nmid 209, \quad 5 \nmid 209, \quad 6 \nmid 209, \quad 7 \nmid 209$$
$$8 \nmid 209, \quad 9 \nmid 209, \quad 10 \nmid 209, \quad \boxed{11 \mid 209}, \quad 12 \nmid 209 \quad 13 \nmid 209, \quad 14 \nmid 209$$

Satz 2.3. *(Existenz eines Primfaktors)*
Jede Zahl $n \in \mathbb{N}$ *mit* $n \geq 2$ *hat einen kleinsten Teiler, der* > 1 *ist. Dieser ist stets eine Primzahl.* $\big($*Man nennt einen Teiler* $p \in T(n)$ *mit* $p \in \mathbb{P}$ **Primfaktor** *von* n*.*$\big)$

Beispiel.

- *Der kleinste Teiler von* $n = 20$*, der größer als* 1 *ist, ist* $p = 2 \in \mathbb{P}$*.*
- *Der kleinste Teiler von* $n = 25$*, der größer als* 1 *ist, ist* $p = 5 \in \mathbb{P}$*.*
- *Der kleinste Teiler von* $n = 29$*, der größer als* 1 *ist, ist* $p = n = 29 \in \mathbb{P}$*.*

Folgerung 2.4. *(Existenz eines kleinen Primfaktors)*
Aus 2.3 *und* 2.2 *(c) folgt: Jede zusammengesetzte Zahl* $n \in \mathbb{N}$ *hat einen Primfaktor* $p \in T(n)$ *mit* $2 \leq p \leq \sqrt{n}$*.*

- $\boxed{\text{Ist } 137 \text{ eine Primzahl?}}$ *Wegen* $\sqrt{137} \approx 11.7$*, ist zu prüfen, ob* 137 *einen Primfaktor hat, der* ≤ 11 *ist. Dafür kommen die Zahlen* $2, 3, 5, 7, 11$ *in Frage.* 137 *ist eine Primzahl, denn:*

$$2 \nmid 137, \quad 3 \nmid 137, \quad 5 \nmid 137, \quad 7 \nmid 137, \quad 11 \nmid 137$$

- $\boxed{\text{Ist } 209 \text{ eine Primzahl?}}$ *Wegen* $\sqrt{209} \approx 14.5$*, ist zu prüfen, ob* 209 *einen Primfaktor hat, der* ≤ 14 *ist. Dafür kommen die Zahlen* $2, 3, 5, 7, 11, 13$ *in Frage.* 209 *ist keine Primzahl, denn:*

$$2 \nmid 209 \quad 3 \nmid 209, \quad 5 \nmid 209, \quad 7 \nmid 209, \quad \boxed{11 \mid 209}, \quad 13 \nmid 209$$

Folgerung 2.5. *(Sieb des Eratosthenes)*
Ein Algorithmus, mit dem man herausfinden kann, welche der Zahlen $2, 3, \ldots, N$ *(für eine feste obere Grenze* $N \in \mathbb{N}$*) Primzahlen sind, ist das sogenannte* **Sieb des Eratosthenes**. *Man gehe dabei folgendermaßen vor:*

1. *Schreibe die Zahlen* $2, 3, \ldots, N$ *aufsteigend in eine Liste.*
2. *Markiere die kleinste Zahl in der Liste (also die* 2*) und streiche alle Vielfachen von* 2*, die größer oder gleich* 2^2 *sind.*
3. *Markiere die kleinste noch vorhandene, bisher noch nicht markierte Zahl* p *in der Liste und streiche alle Vielfachen von* p*, die größer oder gleich* p^2 *sind.*
4. *Wiederhole Schritt 3 solange bis die kleinste noch vorhandene, bisher noch nicht markierte Zahl in der Liste größer als* $\sqrt{N}$ *ist.*
5. *Markiere alle noch vorhandenen Zahlen in der Liste.*

Nach Durchführung dieses Verfahrens gilt: Die Primzahlen zwischen $2, \ldots, N$ *sind genau die markierten Zahlen und die zusammengesetzten Zahlen zwischen* $2, \ldots, N$ *sind genau die gestrichenen Zahlen.*

Beispiel.
Beim Sieb des Erathostenes mit $N = 240$ *streicht man die Vielfachen aller Primzahlen, die kleiner als* $\sqrt{240} \approx 15.5$ *sind, also die von* $2, 3, 5, 7, 11, 13$*. Man erhält:*

	2	**3**	×	**5**	×	**7**	×	×	×	**11**	×	13	×	×
×	*17*	×	*19*	×	×	×	*23*	×	×	×	×	×	*29*	×
31	×	×	×	×	×	*37*	×	×	×	*41*	×	*43*	×	×
×	*47*	×	×	×	×	×	*53*	×	×	×	×	×	*59*	×
61	×	×	×	×	×	*67*	×	×	×	*71*	×	*73*	×	×
×	×	×	*79*	×	×	×	*83*	×	×	×	×	×	*89*	×
×	×	×	×	×	×	*97*	×	×	×	*101*	×	*103*	×	×
×	*107*	×	*109*	×	×	×	*113*	×	×	×	×	×	×	×
×	×	×	×	×	×	*127*	×	×	×	*131*	×	×	×	×
×	*137*	×	*139*	×	×	×	×	×	×	×	×	×	*149*	×
151	×	×	×	×	×	*157*	×	×	×	×	×	*163*	×	×
×	*167*	×	×	×	×	×	*173*	×	×	×	×	×	*179*	×
181	×	×	×	×	×	×	×	×	×	*191*	×	*193*	×	×
×	*197*	×	*199*	×	×	×	×	×	×	×	×	×	×	×
211	×	×	×	×	×	×	×	×	×	×	×	*223*	×	×
×	*227*	×	*229*	×	×	×	*233*	×	×	×	×	×	*239*	×

Die hier verbliebenen Zahlen sind genau die Primzahlen zwischen 2 *und* 240*.*

Bemerkung 2.6. *(Häufigkeit von Primzahlen)*
Man definiert die Funktion

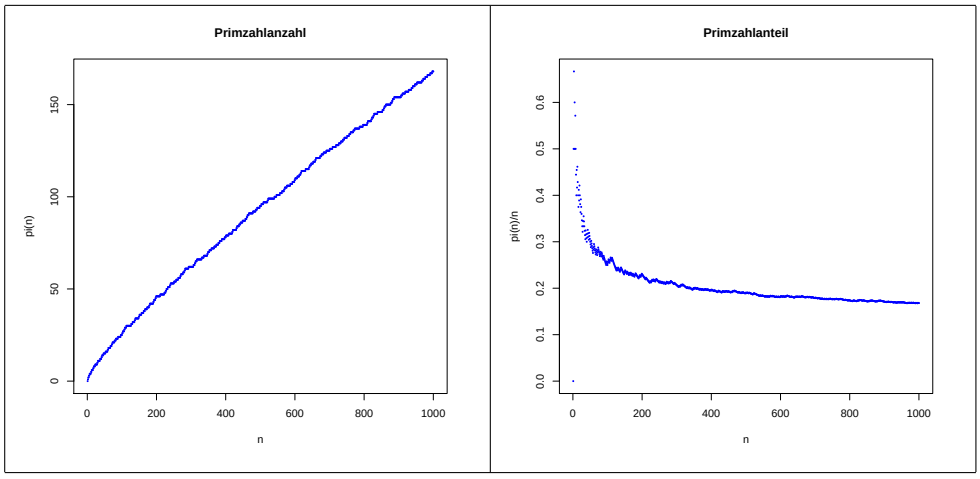
$$\pi : \mathbb{N} \to \mathbb{N},\ \pi(n) = |\{p \in \mathbb{P};\ p \leq n\}|$$

die zu einer Zahl $n \in \mathbb{N}$ angibt, wieviele Primzahlen sich unter den Zahlen $2, 3, \ldots, n$ befinden. Beispielsweise ist

$$\begin{aligned} \{p \in \mathbb{P};\ p \leq 10\} = \{2,3,5,7\} &\quad\Rightarrow\quad \pi(10) = 4 \\ \{p \in \mathbb{P};\ p \leq 17\} = \{2,3,5,7,11,13,17\} &\quad\Rightarrow\quad \pi(17) = 7 \\ \{p \in \mathbb{P};\ p \leq 18\} = \{2,3,5,7,11,13,17\} &\quad\Rightarrow\quad \pi(18) = 7 \end{aligned}$$

Frage. *(Anzahl der Primzahlen)*
Wieviele Primzahlen gibt es? Es ist zunächst nicht klar, ob die Menge $\mathbb{P}$ der Primzahlen endlich ist, oder ob es unendlich viele Primzahlen gibt. Etwas ungenau formuliert könnte man sagen: "Je größer eine Zahl ist, desto mehr Zahlen kommen als mögliche Teiler in Frage und desto unwahrscheinlicher ist es folglich, dass die Zahl eine Primzahl ist." Tatsächlich lässt sich feststellen, dass der Anteil der Primzahlen $\frac{\pi(n)}{n}$ an den Zahlen $1, \ldots, n$ mit wachsendem $n \in \mathbb{N}$ (tendenziell) abnimmt. Es gilt:

n	10	100	1000	10000	100000	1000000	10000000	100000000	1000000000
$\pi(n)$	4	25	168	1229	9592	78498	664579	5761455	50847534
$\frac{\pi(n)}{n} \approx$	0.4	0.25	0.168	0.123	0.095	0.078	0.066	0.058	0.051



Satz 2.7. *(Satz von Euklid)*
Es gibt unendlich viele Primzahlen.

Bemerkung. *(Größte bekannte Primzahl)*
Derzeit ist $2^{43112609} - 1$, eine Zahl mit 12978189 (dezimalen) Stellen, die größte bekannte Primzahl (http://de.wikipedia.org/wiki/Primzahl).

Bemerkung 2.8. *(Verteilung der Primzahlen)*
Die Verteilung der Primzahlen in den natürlichen Zahlen weist nur wenige erkennbare Regelmäßigkeiten auf. Wir wollen dennoch einige Beobachtungen diesbezüglich hier festhalten:

(a) Bei Division durch 6 *haben alle Primzahlen* $p \in \mathbb{P} \setminus \{2,3\}$ *als Rest* 5 *oder* 1. *(Welchen Rest können Primzahlen bei Division durch* 8 *bzw.* 10 *bzw.* 30 *haben?)*

(b) (Primzahlzwillige) Falls $p, p+2 \in \mathbb{P}$ *ist, nennt man das Paar* $(p, p+2)$ *einen* **Primzahlzwilling**. *Es ist bisher nicht bekannt, ob es unendlich viele Primzahlzwillinge gibt.*

Beispiele für Primzahlzwillinge:

$$(3,5), \quad (5,7), \quad (11,13), \quad (17,19), \quad (29,31), \quad \ldots, \quad (1997,1999), \quad \ldots$$

Der größte bisher bekannte Primzahlzwilling ist

$$\left(65516468355 \cdot 2^{333333} - 1 \ , \ 65516468355 \cdot 2^{333333} + 1\right)$$

(http://de.wikipedia.org/wiki/Primzahlzwilling)

(c) (Primzahllücken) Zu jeder Zahl $\ell \in \mathbb{N}$ *gibt es Zahlen* $n+1, \ldots, n+\ell$, *die alle keine Primzahlen sind.*

(d) (Häufigkeit von Primzahlen) Man kann beweisen, dass $\lim\limits_{n\to\infty} \frac{\pi(n)}{n} \cdot \ln(n) = 1$ *gilt. Insbesondere ist* $\lim\limits_{n\to\infty} \frac{\pi(n)}{n} = 0$.

Frage. *(Natürliche Zahlen als Produkte)*
Ausgehend von der Zahl 1 *sollen weitere natürliche Zahlen durch (wiederholte) Multiplikation gebildet werden. Welche Zahlen werden dabei als Faktoren benötigt, damit alle natürlichen Zahlen erzeugt werden können?*

Durch Multiplikation mit den Zahlen $2, 3, 5, 7$ *erhält man:*

	$\xrightarrow{\cdot 2}$						$\xrightarrow{\cdot 2}$						$\xrightarrow{\cdot 2}$					
	1	2	4	8	…		5	10	20	40	…		25	50	100	200	…	
	3	6	12	24	…		15	30	60	120	…		75	150	300	600	…	
$\cdot 3 \downarrow$	9	18	36	72	…	$\xrightarrow{\cdot 5}$	45	90	180	360	…	$\xrightarrow{\cdot 5}$	225	450	900	1800	…	…
	27	54	108	216	…		135	270	540	1080	…		675	1350	2700	5400	…	
	⋮	⋮	⋮	⋮	⋱		⋮	⋮	⋮	⋮	⋱		⋮	⋮	⋮	⋮	⋱	
	$\cdot 7 \downarrow$						$\cdot 7 \downarrow$						$\cdot 7 \downarrow$					
	7	14	28	56	…		35	70	140	280	…		175	350	700	1400	…	
	21	42	84	168	…		105	210	420	840	…		525	1050	2100	4200	…	
$\cdot 3 \downarrow$	63	126	252	504	…	$\xrightarrow{\cdot 5}$	315	630	1260	2520	…	$\xrightarrow{\cdot 5}$	1575	3150	6300	12600	…	…
	189	378	756	1512	…		945	1890	3780	7560	…		4725	9450	18900	37800	…	
	⋮	⋮	⋮	⋮	⋱		⋮	⋮	⋮	⋮	⋱		⋮	⋮	⋮	⋮	⋱	
	⋮						⋮						⋮					

Multipliziert man die so gefundenen Zahlen mit den Faktoren $4, 6, 8, 9, 10$*, so erhält man keine neuen Zahlen. Durch Multiplikation mit* 11 *hingegen, werden (ausschließlich) neue Zahlen erzeugt.*

Definition 2.9. *(Primfaktorzerlegung)*
Sei $n \in \mathbb{N}$ *mit* $n \geq 2$*. Sind* $p_1, p_2, \ldots, p_m \in \mathbb{P}$ *mit*

$$n = \prod_{j=1}^{m} p_j = p_1 \cdot p_2 \cdot \ldots \cdot p_m$$

so nennt man dieses Produkt eine **Primfaktorzerlegung (PFZ)** *von* n*.* (*Dabei besteht die PFZ einer Primzahl* $p \in \mathbb{P}$ *nur aus einem Faktor* $p_1 = p$*.*)

Satz 2.10. *(Hauptsatz der Elementaren Zahlentheorie)*
Zu jeder natürlichen Zahl $n \geq 2$ *existiert eine bis auf die Reihenfolge der Faktoren eindeutige PFZ.*

Beispiel.

- $50 = 2 \cdot 5 \cdot 5 = 5 \cdot 2 \cdot 5 = 5 \cdot 5 \cdot 2$
- $9450 = 2 \cdot 3 \cdot 3 \cdot 3 \cdot 5 \cdot 5 \cdot 7 \overset{z.B.}{=} 5 \cdot 3 \cdot 2 \cdot 3 \cdot 5 \cdot 7 \cdot 3$
- $3007 = 31 \cdot 97$
- $16807 = 7 \cdot 7 \cdot 7 \cdot 7 \cdot 7$
- $13 = 13$

Folgerung 2.11. *(Kanonische und normierte PFZ)*
Sei $n \in \mathbb{N}$ *mit* $n \geq 2$*.*

(a) Es existieren eindeutige Primzahlen $p_1, \ldots, p_k \in \mathbb{P}$ *mit* $p_1 < p_2 < \ldots < p_k$ *und eindeutige* $e_1, \ldots, e_k \in \mathbb{N}$ *mit*

$$n = \prod_{j=1}^{k} {p_j}^{e_j} = {p_1}^{e_1} \cdot {p_2}^{e_2} \cdot \ldots \cdot {p_k}^{e_k}$$

Diese Darstellung von n *heißt* **kanonische PFZ** *von* n*.*

(b) Ist $\mathbb{P} = \{p_1, p_2, p_3, \ldots\}$ *mit* $p_1 < p_2 < p_3 < \ldots$*, so existieren eindeutige Zahlen* $e_1, e_2, e_3, \ldots \in \mathbb{N}_0$*, von denen nur endlich viele* $e_j \neq 0$ *sind, mit:*

$$n = \prod_{j=1}^{\infty} {p_j}^{e_j} = {p_1}^{e_1} \cdot {p_2}^{e_2} \cdot {p_3}^{e_3} \cdot \ldots$$

Diese Darstellung von n *heißt* **normierte PFZ** *von* n*.* (*Für unendlich viele* j *ist der zur Primzahl* p_j *gehörende Exponent* $e_j = 0$*, so dass sich in diesen Fällen* ${p_j}^{e_j} = 1$ *ergibt. Das Produkt besteht also nur 'formal' aus unendlich vielen Faktoren.*)

Beispiel.

- *Für* $n = 50$*:*

$$\begin{aligned} &\textit{Kanonische PFZ:} && \boxed{50 = 2^1 \cdot 5^2} \\ &\big(\textit{also:} && p_1 = 2,\ p_2 = 5 \ \textit{und}\ e_1 = 1,\ e_2 = 2\big) \\ &\textit{Normierte PFZ:} && \boxed{50 = 2^1 \cdot 3^0 \cdot 5^2 \cdot 7^0 \cdot 11^0 \cdot \ldots} \\ &\big(\textit{also:} && p_1 = 2,\ p_2 = 3,\ p_3 = 5,\ p_4 = 7,\ p_5 = 11,\ \ldots \\ &&\textit{und}\quad & e_1 = 1,\ e_2 = 0,\ e_3 = 2,\ e_4 = 0,\ e_5 = 0,\ \ldots\big) \end{aligned}$$

- *Für* $n = 257499$*:*

$$\begin{aligned} &\textit{Kanonische PFZ:} && \boxed{257499 = 3^4 \cdot 11^1 \cdot 17^2} \\ &\big(\textit{also:} && p_1 = 3,\ p_2 = 11\ \ p_3 = 17 \textit{und}\ e_1 = 4,\ e_2 = 1,\ e_3 = 2\big) \\ &\textit{Normierte PFZ:} && \boxed{257499 = 2^0 \cdot 3^4 \cdot 5^0 \cdot 7^0 \cdot 11^1 \cdot 13^0 \cdot 17^2 \cdot 19^0 \cdot 23^0 \cdot \ldots} \\ &\big(\textit{also:} && e_2 = 4,\ e_5 = 1,\ e_7 = 2 \ \textit{und alle anderen}\ e_j = 0\big) \end{aligned}$$

Bemerkung 2.12. *(PFZ der Zahl* 1*)*
Der Vollständigkeit halber bezeichnet man das sogenannte "leere Produkt" als PFZ der Zahl $1 \in \mathbb{N}$*. In der normierten PFZ von* 1 *sind alle Exponenten* $e_j = 0$*, also:*

$$1 = \prod_{j=1}^{\infty} {p_j}^0$$

Bemerkung. *(Primzahlen als Bausteine der natürlichen Zahlen)*
Wir haben nun einen weiteren (wesentlichen) Aspekt von Primzahlen erkannt. Ausgehend von der Zahl 1 *kann jede natürliche Zahl durch (wiederholte) Multiplikation mit Primzahlen erzeugt werden. Man kann dabei die Reihenfolge der Faktoren beliebig verändern, abgesehen davon ist die Produktdarstellung aber eindeutig.*

Satz 2.13. *(Zusammenhang zwischen PFZ und Produktbildung bzw. Teilbarkeit)*
Gegeben seien natürliche Zahlen $n, m \in \mathbb{N}$ *mit den normierten PFZ'en*

$$n = \prod_{j=1}^{\infty} {p_j}^{e_j} \quad \textit{und} \quad m = \prod_{j=1}^{\infty} {p_j}^{f_j}$$

(a) Die normierte PFZ des Produkts ist:

$$n \cdot m = \prod_{j=1}^{\infty} {p_j}^{e_j + f_j}$$

(b) m *ist genau dann ein Teiler von* n*, wenn alle* $f_j \le e_j$ *sind. In diesem Fall gilt*

$$n : m = \prod_{j=1}^{\infty} {p_j}^{e_j - f_j} \in \mathbb{N}$$

Beispiel.

- $n = 60984$ *und* $m = 168$*:*

$$\begin{array}{rcl} 60984 & = & 2^3 \cdot 3^2 \cdot 5^0 \cdot 7^1 \cdot 11^2 \cdot 13^0 \cdot 17^0 \cdot \ldots \\ 168 & = & 2^3 \cdot 3^1 \cdot 5^0 \cdot 7^1 \cdot 11^0 \cdot 13^0 \cdot 17^0 \cdot \ldots \\ \hline \big(10245312 = \big)\ 60984 \cdot 168 & = & 2^6 \cdot 3^3 \cdot 5^0 \cdot 7^2 \cdot 11^2 \cdot 13^0 \cdot 17^0 \cdot \ldots \end{array}$$

Es gilt $168 \mid 60984$*, denn alle Exponenten in der PFZ von* 168 *sind kleiner oder gleich als die entsprechenden Exponenten in der PFZ von* 60984*. Man erhält:*

$$\big(363 = \big)\ 60984 : 168 = 2^0 \cdot 3^1 \cdot 5^0 \cdot 7^0 \cdot 11^2 \cdot 13^0 \cdot 17^0 \cdot \ldots$$

- $n = 1650$ *und* $m = 225$*:*

$$\begin{array}{rcl} 1650 & = & 2^1 \cdot 3^1 \cdot 5^2 \cdot 7^0 \cdot 11^1 \cdot 13^0 \cdot 17^0 \cdot \ldots \\ 225 & = & 2^0 \cdot 3^2 \cdot 5^2 \cdot 7^0 \cdot 11^0 \cdot 13^0 \cdot 17^0 \cdot \ldots \\ \hline \big(371250 = \big)\ 1650 \cdot 225 & = & 2^1 \cdot 3^3 \cdot 5^4 \cdot 7^0 \cdot 11^1 \cdot 13^0 \cdot 17^0 \cdot \ldots \end{array}$$

Es gilt $225 \nmid 1650$*, denn der Exponent zur Primzahl* 3 *ist in der PFZ von* 225 *größer als in der PFZ von* 1650 $\big(e_2 = 2 > 1 = f_2\big)$*.*

Folgerung 2.14. *(Primzahlkriterium)*
Für eine natürliche Zahl $p \in \mathbb{N}$ *mit* $p \geq 2$ *sind die folgenden Bedingungen äquivalent:*

(i) p *ist eine Primzahl.*

(ii) Für alle $a, b \in \mathbb{Z}$ *mit* $p \mid (a \cdot b)$ *gilt* $p \mid a$ *oder* $p \mid b$*.*

(iii) Für alle $a_1, \ldots, a_k \in \mathbb{Z}$ *mit* $p \mid (a_1 \cdot \ldots \cdot a_k)$ *gilt* $p \mid a_j$ *für (mindestens) ein* j*.*

Beispiel.

- *Für die zusammengesetzte Zahl* 20 *gilt (beispielsweise):*

$$\begin{array}{rl} & 20 \mid (22 \cdot 30) \quad \textit{aber} \quad 20 \nmid 22 \ \textit{und}\ 20 \nmid 30 \\ \textit{oder einfacher:} & 20 \mid (4 \cdot 5) \quad \textit{aber} \quad 20 \nmid 4 \ \textit{und}\ 20 \nmid 5 \end{array}$$

- *Für die Primzahl* 11 *gilt:* $11 \mid (a \cdot b) \ \Rightarrow\ 11 \mid a \ \vee\ 11 \mid b$*.*

Folgerung 2.15. *(Teilbarkeitskriterium)*
Zwei beliebige Zahlen $a, b \in \mathbb{Z} \setminus \{0\}$ *sind genau dann teilerfremd, wenn sie keinen gemeinsamen Primfaktor haben. Damit gilt für teilerfremde* a, b *(vergleiche* 1.2*):*

$$(a \cdot b) \mid x \quad \Leftrightarrow \quad a \mid x \ \textit{und}\ b \mid x$$

Definition 2.16. *(Teileranzahlfunktion)*
Wir nennen die Funktion

$$\tau : \mathbb{N} \to \mathbb{N},\ \tau(n) = |T(n)|$$

die jeder natürlichen Zahl die Anzahl ihrer (positiven) Teiler zuordnet, **Teileranzahlfunktion**. (*Offenbar gilt* $\tau(1) = 1$, $\tau(p) = 2$ *für alle* $p \in \mathbb{P}$ *und* $\tau(n) > 2$ *für alle zusammengesetzten Zahlen* $n \in \mathbb{N}$.)

Beispiel.

- *Für* $n = 250$*:* $\quad T(250) = \{1, 2, 5, 10, 25, 50, 125, 250\} \;\Rightarrow\; \tau(250) = 8$
- *Für* $n = 64$*:* $\quad T(64) = \{1, 2, 4, 8, 16, 32, 64\} \;\Rightarrow\; \tau(64) = 7$
- *Für* $n = 6615$*:*

  $T(6615) = \{1, 3, 5, 7, 9, 15, 21, 27, 35, 45, 49, 63, 105, 135, 147, 189, 245, 315, 441, 735, 945, 1323, 2205, 6615\}$

  $\Rightarrow\; \tau(6615) = 24$

Folgerung 2.17. *(Zusammenhang zwischen PFZ, Teilermenge und Teileranzahl)*

(a) Gegeben sei eine Zahl $n \in \mathbb{N}$ *mit (kanonischer) PFZ* $n = \prod_{j=1}^{k} {p_j}^{e_j}$*. Dann gilt:*

$$T(n) = \left\{ \prod_{j=1}^{k} {p_j}^{f_j};\ 0 \le f_j \le e_j \text{ für alle } j = 1, \ldots, k \right\}$$

Daraus kann man folgern, dass $\tau(n) = \prod_{j=1}^{k} (e_j + 1)$ *gilt.*

(b) Ist die normierte PFZ $n = \prod_{j=1}^{\infty} {p_j}^{e_j}$ *von* n *gegeben, so gilt entsprechend*

$$T(n) = \left\{ \prod_{j=1}^{\infty} {p_j}^{f_j};\ 0 \le f_j \le e_j \text{ für alle } j = 1, 2, \ldots \right\} \quad \text{und} \quad \tau(n) = \prod_{j=1}^{\infty} (e_j + 1)$$

Beispiel.

- *Für* $\boxed{n = 250 = 2^1 \cdot 5^3}$*: Die Teiler von* 250 *haben eine PFZ*

  $$2^{f_1} \cdot 5^{f_2} \quad \text{mit } f_1 \in \{0, 1\} \text{ und } f_2 \in \{0, 1, 2, 3\}$$

  Also:

	$f_2 = 0$	$f_2 = 1$	$f_2 = 2$	$f_2 = 3$
$f_1 = 0$	$2^0 \cdot 5^0 = 1$	$2^0 \cdot 5^1 = 5$	$2^0 \cdot 5^2 = 25$	$2^0 \cdot 5^3 = 125$
$f_1 = 1$	$2^1 \cdot 5^0 = 2$	$2^1 \cdot 5^1 = 10$	$2^1 \cdot 5^2 = 50$	$2^1 \cdot 5^3 = 250$

  Damit hat die Zahl 250 *genau* $(1 + 1) \cdot (3 + 1) = 2 \cdot 4 = 8$ *positive Teiler.*

- *Für* $\boxed{n = 14739 = 3^1 \cdot 17^3}$*: Die Teiler von* 14739 *haben eine PFZ*

  $$3^{f_1} \cdot 17^{f_2} \quad \text{mit } f_1 \in \{0, 1\} \text{ und } f_2 \in \{0, 1, 2, 3\}$$

  Also:

	$f_2 = 0$	$f_2 = 1$	$f_2 = 2$	$f_2 = 3$
$f_1 = 0$	$3^0 \cdot 17^0 = 1$	$3^0 \cdot 17^1 = 17$	$3^0 \cdot 17^2 = 289$	$3^0 \cdot 17^3 = 4913$
$f_1 = 1$	$3^1 \cdot 17^0 = 3$	$3^1 \cdot 17^1 = 51$	$3^1 \cdot 17^2 = 867$	$3^1 \cdot 17^3 = 14739$

  Damit hat die Zahl 14739 *ebenfalls genau* $2 \cdot 4 = 8$ *positive Teiler.*

- *Für* $\boxed{n = 64 = 2^6}$*: Die Teiler von* 64 *haben eine PFZ*

$$2^{f_1} \quad \textit{mit } f_1 \in \{0,1,2,3,4,5,6\}$$

Also:

$f_1 = 0$	$f_1 = 1$	$f_1 = 2$	$f_1 = 3$	$f_1 = 4$	$f_1 = 5$	$f_1 = 6$
$2^0 = 1$	$2^1 = 2$	$2^2 = 4$	$2^3 = 8$	$2^4 = 16$	$2^5 = 32$	$2^6 = 64$

Die Zahl 64 *hat genau* $6 + 1 = 7$ *positive Teiler.*

- *Für* $\boxed{n = 6615 = 3^3 \cdot 5^1 \cdot 7^2}$*: Die Teiler von* 6615 *haben eine PFZ*

$$3^{f_1} \cdot 5^{f_2} \cdot 7^{f_3} \quad \textit{mit } f_1 \in \{0,1,2,3\},\ f_2 \in \{0,1\} \textit{ und } f_3 \in \{0,1,2\}$$

	$f_1 = 0$	
	$f_2 = 0$	$f_2 = 1$
$f_3 = 0$	$3^0 \cdot 5^0 \cdot 7^0 = 1$	$3^0 \cdot 5^1 \cdot 7^0 = 5$
$f_3 = 1$	$3^0 \cdot 5^0 \cdot 7^1 = 7$	$3^0 \cdot 5^1 \cdot 7^1 = 35$
$f_3 = 2$	$3^0 \cdot 5^0 \cdot 7^2 = 49$	$3^0 \cdot 5^1 \cdot 7^2 = 245$

	$f_1 = 1$	
	$f_2 = 0$	$f_2 = 1$
$f_3 = 0$	$3^1 \cdot 5^0 \cdot 7^0 = 3$	$3^1 \cdot 5^1 \cdot 7^0 = 15$
$f_3 = 1$	$3^1 \cdot 5^0 \cdot 7^1 = 21$	$3^1 \cdot 5^1 \cdot 7^1 = 105$
$f_3 = 2$	$3^1 \cdot 5^0 \cdot 7^2 = 147$	$3^1 \cdot 5^1 \cdot 7^2 = 735$

	$f_1 = 2$	
	$f_2 = 0$	$f_2 = 1$
$f_3 = 0$	$3^2 \cdot 5^0 \cdot 7^0 = 9$	$3^2 \cdot 5^1 \cdot 7^0 = 45$
$f_3 = 1$	$3^2 \cdot 5^0 \cdot 7^1 = 63$	$3^2 \cdot 5^1 \cdot 7^1 = 315$
$f_3 = 2$	$3^2 \cdot 5^0 \cdot 7^2 = 441$	$3^2 \cdot 5^1 \cdot 7^2 = 2205$

	$f_1 = 3$	
	$f_2 = 0$	$f_2 = 1$
$f_3 = 0$	$3^3 \cdot 5^0 \cdot 7^0 = 27$	$3^3 \cdot 5^1 \cdot 7^0 = 135$
$f_3 = 1$	$3^3 \cdot 5^0 \cdot 7^1 = 189$	$3^3 \cdot 5^1 \cdot 7^1 = 945$
$f_3 = 2$	$3^3 \cdot 5^0 \cdot 7^2 = 1323$	$3^3 \cdot 5^1 \cdot 7^2 = 6615$

Die Zahl 6615 *hat genau* $(3 + 1) \cdot (1 + 1) \cdot (2 + 1) = 24$ *positive Teiler.*

- *Die Zahl* $2^4 \cdot 7^2 \cdot 11^3 \cdot 23^2 \cdot 37 \cdot 101 = 2062874882992$ *hat genau*

$$(4 + 1) \cdot (2 + 1) \cdot (3 + 1) \cdot (2 + 1) \cdot (1 + 1) \cdot (1 + 1) = 720$$

positive Teiler.

Bemerkung 2.18. *(PFZ und Teilerdiagramme)*
Sind im Teilerdiagramm einer natürlichen Zahl $n \geq 2$ *zwei Teiler* $x, y \in T(n)$ *mit einer Kante verbunden (so dass y höher als x steht), so ist der Quotient* $y : x$ *stets ein Primfaktor von n. Achtet man darauf, alle Kanten, die demselben Primfaktor zugeordnet werden können, mit gleicher Richtung und gleicher Länge einzutragen, so wird das Teilerdiagramm sehr übersichtlich (zumindest wenn n nicht mehr als drei verschiedene Primfaktoren hat). Die Zahl der Primfaktoren von n bestimmt dabei Aussehen und Struktur des Diagramms:*

- *Hat n nur einen Primfaktor (kanonische PFZ* $n = p^e$*), so ist das Teilerdiagramm eine Strecke, die in e Teilstrecken gleicher Länge aufgeteilt ist.* (*In diesem Fall ist die Teilbarkeitsrelation auf* $T(n)$ *total.*)
- *Hat n zwei Primfaktoren (kanonische PFZ* $n = {p_1}^{e_1} \cdot {p_2}^{e_2}$*), so ist das Teilerdiagramm ein Parallelogramm (bzw. Rechteck), dass in* $e_1 \cdot e_2$ *zueinander kongruente Parallelogramme (bzw. Rechtecke) aufgeteilt ist.*

- *Hat n drei Primfaktoren (kanonische PFZ $n = {p_1}^{e_1} \cdot {p_2}^{e_2} \cdot {p_3}^{e_3}$), so erscheint das Teilerdiagramm als Quader, der in $e_1 \cdot e_2 \cdot e_3$ zueinander kongruente Quader aufgeteilt ist.*
- *Hat n mehr als 3 Primfaktoren, so wird das Teilerdigramm leicht unübersichtlich, da mehr als 3 Dimensionen nicht gut dargestellt bzw. erfasst werden können.* $\big($*Die kleinste Zahl mit mehr als 3 Primfaktoren ist* $210 = 2 \cdot 3 \cdot 5 \cdot 7.\big)$

Beginnt man im Teilerdigramm bei der 1 und geht entlang der Kanten einen Weg nach oben, so erhält man die PFZ der Teiler von n, indem man immer den der jeweiligen Kante zugeordneten Primfaktor zur PFZ hinzufügt. Entsprechend kann man auch entlang Kanten nach unten gehen und dabei immer den entsprechenden Primfaktor streichen.

3 Größter gemeinsamer Teiler

Definition und erste Eigenschaften

Definition 3.1. *(Größter gemeinsamer Teiler)*
Für $a_1, \ldots, a_k \in \mathbb{Z}$ definiert man den **größten gemeinsamen Teiler** *als*

$$ggT(a_1, \ldots, a_k) \overset{def}{=} \max T(a_1, \ldots, a_k)$$

falls mindestens ein $a_j \neq 0$ ist. $\big($*Sind alle $a_j = 0$, so sei* $ggT(a_1, \ldots, a_k) \overset{def}{=} 0$.$\big)$

Beispiel.

- $T(12, 18) = \{1, 2, 3, 6\} \Rightarrow ggT(12, 18) = 6$
- $T(200, 130) = \{1, 2, 5, 10\} \Rightarrow ggT(200, 130) = 10$
- $T(15, 44) = \{1\} \Rightarrow ggT(15, 44) = 1$
- $T(6, 10, 14, 22, 26) = \{1, 2\} \Rightarrow ggT(6, 10, 14, 22, 26) = 2$

Bemerkung 3.2. *(Elementare Eigenschaften des ggT)*
Gegeben seien beliebige Zahlen $a_1, \ldots, a_k,\ b_1, \ldots, b_l \in \mathbb{Z}$.

(a) Falls mindestens eine der Zahlen $a_j \neq 0$ ist, ist die Teilermenge $T(a_1, \ldots, a_k)$ eine endliche und nichtleere Teilmenge von $\mathbb{N}$. Sie hat damit also ein maximales Element und somit ist Definition 3.1 sinnvoll.

(b) Es gilt $T(a_1, \ldots, a_k) = T(|a_1|, \ldots, |a_k|)$ und folglich $ggT(a_1, \ldots, a_k) = ggT(|a_1|, \ldots, |a_k|)$.

Beispiel: $T(-8, -20, 44, -84) = T(8, 20, 44, 84)\ \big(= \{1, 2, 4\}\big) \Rightarrow ggT(-8, -20, 44, -84) = ggT(8, 20, 44, 84)\ \big(= 4\big)$

(c) Gilt $\{a_1, \ldots, a_k\} = \{b_1, \ldots, b_l\} \subset \mathbb{Z}$, so ist $T(a_1, \ldots, a_k) = T(b_1, \ldots, b_l)$ und folglich $ggT(a_1, \ldots, a_k) = ggT(b_1, \ldots, b_l)$.

Beispiel: $T(33, 12, 12, 21, 12, 33) = T(12, 21, 33)\ \big(= \{1, 3\}\big) \Rightarrow ggT(33, 12, 12, 21, 12, 33) = ggT(12, 21, 33)\ \big(= 3\big)$

(d) Es gilt $T(a_1, \ldots, a_k, 0) = T(a_1, \ldots, a_k)$ und folglich $ggT(a_1, \ldots, a_k, 0) = ggT(a_1, \ldots, a_k)$.

Beispiel: $T(14, 35, 0) = T(14, 35)\ \big(= \{1, 7\}\big) \Rightarrow ggT(14, 35, 0) = ggT(14, 35)\ \big(= 7\big)$

(e) Es gilt $T(a_1, \ldots, a_k, 1) = \{1\}$ und folglich $ggT(a_1, \ldots, a_k, 1) = 1$.

Beispiel: $T(100, 200, 1) = \{1\} \Rightarrow ggT(100, 200, 1) = 1$

(f) Es gilt $ggT(a_1) = |a_1|$.

(g) Gilt $a_1 \mid a_2$, so ist $T(a_1, a_2) = T(a_1)$ und folglich $ggT(a_1, a_2) = |a_1|$.

Beispiel: $15 \mid 105 \Rightarrow T(15, 105) = T(15) \Rightarrow ggT(15, 105)\ \big(= 15\big)$

(h) Zwei Zahlen $a, b \in \mathbb{Z} \setminus \{0\}$ sind genau dann teilerfremd, wenn $ggT(a, b) = 1$ gilt.

Satz 3.3. *(Zusammenhang zwischen ggT und PFZ)*
Gegeben seien $a_1, a_2, \ldots, a_k \in \mathbb{N}$ mit den normierten PFZ'en:

$$a_1 = \prod_{j=1}^{\infty} p_j^{e_j^{(1)}}, \quad a_2 = \prod_{j=1}^{\infty} p_j^{e_j^{(2)}}, \quad \ldots, \quad a_k = \prod_{j=1}^{\infty} p_j^{e_j^{(k)}}$$

Dann sind die gemeinsamen Teiler $x \in T(a_1, \ldots, a_k)$ genau die Zahlen mit einer normierten PFZ

$$x = \prod_{j=1}^{\infty} p_j^{f_j} \quad \text{wobei } f_j \leq \min\left\{e_j^{(1)}, e_j^{(2)}, \ldots, e_j^{(k)}\right\} \text{ für alle } j \in \mathbb{N} \text{ gilt}$$

Folglich hat der größte gemeinsame Teiler dieser Zahlen die normierte PFZ:

$$ggT(a_1, \ldots, a_k) = \prod_{j=1}^{\infty} p_j^{\left(\min\left\{e_j^{(1)}, e_j^{(2)}, \ldots, e_j^{(k)}\right\}\right)}$$

Beispiel.

- $a_1 = 240,\ a_2 = 3300$*:*

$$\begin{aligned} 240 &= 2^4 \cdot 3^1 \cdot 5^1 \cdot 7^0 \cdot 11^0 \cdot 13^0 \cdot \ldots \\ 3300 &= 2^1 \cdot 3^1 \cdot 5^2 \cdot 7^0 \cdot 11^1 \cdot 13^0 \cdot \ldots \\ \hline ggT(240, 3300) &= 2^1 \cdot 3^1 \cdot 5^1 \cdot 7^0 \cdot 11^0 \cdot 13^0 \cdot \ldots \end{aligned}$$

  Also $ggT(240, 3300) = 30$

- $a_1 = 72,\ a_2 = 385$*:*

$$\begin{aligned} 72 &= 2^3 \cdot 3^2 \cdot 5^0 \cdot 7^0 \cdot 11^0 \cdot 13^0 \cdot \ldots \\ 385 &= 2^0 \cdot 3^0 \cdot 5^1 \cdot 7^1 \cdot 11^1 \cdot 13^0 \cdot \ldots \\ \hline ggT(72, 385) &= 2^0 \cdot 3^0 \cdot 5^0 \cdot 7^0 \cdot 11^0 \cdot 13^0 \cdot \ldots \end{aligned}$$

  Also $ggT(72, 385) = 1$

- $a_1 = 71148,\ a_2 = 24696,\ a_3 = 43120,\ a_4 = 92610$*:*

$$\begin{aligned} 71148 &= 2^2 \cdot 3^1 \cdot 5^0 \cdot 7^2 \cdot 11^2 \cdot 13^0 \cdot \ldots \\ 24696 &= 2^3 \cdot 3^2 \cdot 5^0 \cdot 7^3 \cdot 11^0 \cdot 13^0 \cdot \ldots \\ 43120 &= 2^4 \cdot 3^0 \cdot 5^1 \cdot 7^2 \cdot 11^1 \cdot 13^0 \cdot \ldots \\ 92610 &= 2^1 \cdot 3^3 \cdot 5^1 \cdot 7^3 \cdot 11^0 \cdot 13^0 \cdot \ldots \\ \hline ggT(71148, 24696, 43120, 92610) &= 2^1 \cdot 3^0 \cdot 5^0 \cdot 7^2 \cdot 11^0 \cdot 13^0 \cdot \ldots \end{aligned}$$

  Also $ggT(71148, 24696, 43120, 92610) = 98$

Folgerung 3.4. *(Weitere Eigenschaften des ggT)*
Gegeben seien beliebige Zahlen $a_1, \ldots, a_k \in \mathbb{Z}$.

(a) Für eine beliebige Zahl $x \in \mathbb{Z}$ *gilt die Äquivalenz:*

$$x | a_j \text{ für alle } j = 1, \ldots, k \quad \Leftrightarrow \quad x | ggT(a_1, \ldots, a_k)$$

Also ist $T(a_1, \ldots, a_k) = T\big(ggT(a_1, \ldots, a_k)\big)$

$$\underline{\text{Beispiel:}} \quad T(20, 50, 140) = \{1, 2, 5, 10\} = T(10) = T\left(ggT(20, 50, 140)\right)$$

(b) Es gilt $ggT(a_1, \ldots, a_k) = ggT\big(ggT(a_1, \ldots, a_{k-1}), a_k\big)$.

$$\underline{\text{Beispiel:}} \qquad ggT(242, 66, 165) = ggT\big(\underbrace{ggT(242, 66)}_{=22}, 165\big) = 11$$
$$ggT(242, 66, 165) = ggT\big(242, \underbrace{ggT(66, 165)}_{=33}\big) = 11$$

(c) Für jede Zahl $b \in \mathbb{Z}$ *gilt* $ggT(b \cdot a_1, \ldots, b \cdot a_k) = |b| \cdot ggT(a_1, \ldots, a_k)$.

$$\underline{\text{Beispiel:}} \quad ggT(6, 10, 16) = 2 \quad \textit{und} \quad ggT\big(\underbrace{7 \cdot 6}_{=42}, \underbrace{7 \cdot 10}_{=70}, \underbrace{7 \cdot 16}_{=112}\big) = 7 \cdot 2 = 14$$

(d) Für $a, b \in \mathbb{Z} \setminus \{0\}$ *sind die Zahlen* $\frac{a}{ggT(a,b)}$, $\frac{b}{ggT(a,b)} \in \mathbb{Z}$ *stets teilerfremd.*

$$\underline{\text{Beispiel:}} \quad ggT(100, 28) = 4 \quad \Rightarrow \quad \tfrac{100}{4}, \tfrac{28}{4} \in \mathbb{Z} \text{ sind teilerfremd}$$

Satz 3.5. *(Zusammenhang zwischen ggT und Division mit Rest)*

(a) Für alle $a, b, s \in \mathbb{Z}$ *gilt*

$$T(a, b) = T(a + s \cdot b, b) \quad \textit{und folglich} \quad ggT(a, b) = ggT(a + s \cdot b, b)$$

$$\underline{\text{Beispiel:}} \qquad ggT(20, 45) = ggT\big(20, \underbrace{45 + 3 \cdot 20}_{=105}\big) = 5$$
$$ggT(20, 45) = ggT\big(\underbrace{20 + 4 \cdot 45}_{=200}, 45\big) = 5$$
$$ggT(20, 45) = ggT\big(\underbrace{20 - 3 \cdot 45}_{=-115}, 45\big) = 5$$
$$ggT(20, 45) = ggT\big(20, \underbrace{45 - 2 \cdot 20}_{=5}\big) = 5$$
$$ggT(33, 147) = ggT\big(33, \underbrace{147 - 4 \cdot 33}_{=15}\big) = 3$$

(b) Seien $n, m \in \mathbb{N}$. *Bestimmt man die (nach* 1.6 *eindeutig existierenden) Zahlen* $q, r \in \mathbb{N}$ *mit* $0 \leq r < m$ *und* $n = q \cdot m + r$, *so gilt*

$$T(n, m) = T(r, m) \quad \textit{und} \quad ggT(n, m) = ggT(r, m)$$

Folgerung 3.6. *(Euklidischer Algorithmus)*
Gegeben seien $n, m \in \mathbb{N}$. Dann lässen sich $T(n,m)$ und $ggT(n,m)$ bestimmen, indem man (unter fortlaufender Anwendung von 3.5 (b)) immer wieder die Größere der beiden Zahlen durch den Rest bei Division der Größeren durch die Kleinere ersetzt. Dies tut man solange bis eine der beiden Zahlen 0 ist, die andere Zahl entspricht dann dem ggT von n und m. (Da die auftretenden Reste immer kleiner werden, kommt dieses Verfahren garantiert immer zum Ende.)

Beispiel.

- $n = 1088,\ m = 323$*:*

$$\begin{aligned} ggT(1088,323) &= ggT(119,323) && \text{denn } 1088 = 3\cdot 323 + 119 \\ &= ggT(119,85) && \text{denn } 323 = 2\cdot 119 + 85 \\ &= ggT(34,85) && \text{denn } 119 = 1\cdot 85 + 34 \\ &= ggT(34,17) && \text{denn } 85 = 2\cdot 34 + 17 \\ &= ggT(0,17) && \text{denn } 34 = 2\cdot 17 + 0 \\ &= ggT(17) = 17 \end{aligned}$$

- $n = 49,\ m = 450$*:*

$$\begin{aligned} ggT(49,450) &= ggT(49,9) && \text{denn } 450 = 9\cdot 49 + 9 \\ &= ggT(4,9) && \text{denn } 49 = 5\cdot 9 + 4 \\ &= ggT(4,1) && \text{denn } 9 = 2\cdot 4 + 1 \\ &= ggT(0,1) && \text{denn } 4 = 4\cdot 1 + 0 \\ &= ggT(1) = 1 \end{aligned}$$

Linearkombinationen ganzer Zahlen

Definition 3.7. *(Linearkombination)*
Für gegebene Zahlen $a, b \in \mathbb{Z}$ nennt man eine Zahl $c \in \mathbb{Z}$ **(ganzzahlige) Linearkombination** *von a und b, falls $x, y \in \mathbb{Z}$ mit $c = x\cdot a + y\cdot b$ existieren. Wir schreiben*

$$L(a,b) \overset{def}{=} \{c \in \mathbb{Z};\ c \text{ ist Linearkombination von } a \text{ und } b\} = \{x\cdot a + y\cdot b;\ x, y \in \mathbb{Z}\} \subset \mathbb{Z}$$

für die Menge der Linearkombinationen von a und b.

Beispiel.

- $a = 9,\ b = 6$*:*

$39 \in L(9,6)$	*, denn (z.B.)*	$39 = 3\cdot 9 + 2\cdot 6$	*(also z.B.* $x = 3,\ y = 2$*)*
$3 \in L(9,6)$	*, denn (z.B.)*	$3 = 1\cdot 9 + (-1)\cdot 6$	*(also z.B.* $x = 1,\ y = -1$*)*
$-12 \in L(9,6)$	*, denn (z.B.)*	$-12 = (-2)\cdot 9 + 1\cdot 6$	*(also z.B.* $x = -2,\ y = 1$*)*
$0 \in L(9,6)$	*, denn (z.B.)*	$0 = (-6)\cdot 9 + 9\cdot 6$	*(also z.B.* $x = -6,\ y = 9$*)*
$7 \notin L(9,6)$	*, denn*	$3 \nmid 7$	*aber* $3 \mid (x\cdot a + y\cdot b)\ \ \forall x, y \in \mathbb{Z}$

- $a = 8,\ b = 5$*:*

$$\begin{array}{rlll} 12 \in L(8,5) & \text{, denn (z.B.)} & 12 = 4\cdot 8 + (-4)\cdot 5 & (\text{also z.B. } x = 4,\ y = -4) \\ 39 \in L(8,5) & \text{, denn (z.B.)} & 39 = (-2)\cdot 8 + 11\cdot 5 & (\text{also z.B. } x = -2,\ y = 11) \\ -39 \in L(8,5) & \text{, denn (z.B.)} & 39 = 2\cdot 8 + (-11)\cdot 5 & (\text{also z.B. } x = 2,\ y = -11) \\ 1 \in L(8,5) & \text{, denn (z.B.)} & 1 = 2\cdot 8 + (-3)\cdot 5 & (\text{also z.B. } x = 2,\ y = -3) \end{array}$$

Gibt es eine ganze Zahl, die keine Linearkombination von 8 *und* 5 *ist?*

Satz 3.8. *(Linearkombinationen sind genau die Vielfachen des ggT)*
Für gegebene Zahlen $a, b \in \mathbb{Z}$ ist $c \in \mathbb{Z}$ genau dann eine Linearkombination von a und b, falls c ein Vielfaches von $ggT(a,b)$ ist. Es gilt also:

$$L(a,b) = V\big(ggT(a,b)\big)$$

Folgerung 3.9. *(Spezialfälle)*

(a) Für $a, b \in \mathbb{Z}$ gilt $L(a,0) = V(a)$ und $L(0,b) = V(b)$. Außerdem ist $L(0,0) = \{0\}$.

(b) Sind $a, b \in \mathbb{Z} \setminus \{0\}$ teilerfremd, so gilt $L(a,b) = \mathbb{Z}$.

Bemerkung 3.10. *(Erweiterter Euklidischer Algorithmus)*
Seien $a, b \in \mathbb{Z} \setminus \{0\}$ gegeben.

(a) Nach 3.8 *ist $ggT(a,b)$ eine Linearkombination von a und b. Es existieren also Zahlen $x, y \in \mathbb{Z}$ mit $ggT(a,b) = x \cdot a + y \cdot b$. Mit dem* **erweiterten Euklidischen Algorithmus** *lassen sich solche Zahlen x, y bestimmen. Man beachte dabei zunächst:*
Sind zwei Linearkombinationen

$$c_1 = x_1 \cdot a + y_1 \cdot b, \quad c_2 = x_2 \cdot a + y_2 \cdot b \ \in L(a,b)$$

gegeben und dividiert man diese mit Rest (also z.B. $c_1 = q \cdot c_2 + r$ mit $0 \le r < c_2$), so ist der Rest r ebenfalls eine Linearkombination von a und b. Genauer gilt:

$$r = c_1 - q \cdot c_2 = x_1 \cdot a + y_1 \cdot b - q \cdot (x_2 \cdot a + y_2 \cdot b) = (x_1 - qx_2) \cdot a + (y_1 - qy_2) \cdot b$$

Beginnend mit

$$|a| = (\pm 1) \cdot a + 0 \cdot b \quad \text{und} \quad |b| = 0 \cdot a + (\pm 1) \cdot b$$

kann man daher durch fortlaufende Division mit Rest immer kleinere natürliche Zahlen als Linearkombination von a und b darstellen. Geht man dabei wie in 3.6 *vor, so erhält man (nach endlich vielen Schritten) $ggT(|a|,|b|) = ggT(a,b)$ als auftretenden Rest und findet damit auch die gesuchte Linearkombination $ggT(a,b) = x \cdot a + y \cdot b$.*

Beispiel: Für $a = 43$ und $b = 50$ bestimme $x, y \in \mathbb{Z}$ mit $ggT(a,b) = x \cdot 43 + y \cdot 50$:

(1)	$50 = 0 \cdot 43 + 1 \cdot 50$		
(2)	$43 = 1 \cdot 43 + 0 \cdot 50$		
		$50 = 1 \cdot 43 + 7$	
		$\Leftrightarrow \quad 7 = 50 - 1 \cdot 43$	$(R1)$
$(R1) \Rightarrow (3)$	$7 = (-1) \cdot 43 + 1 \cdot 50$		
		$43 = 6 \cdot 7 + 1$	
		$\Leftrightarrow \quad 1 = 43 - 6 \cdot 7$	$(R2)$
$(1),(2)$ *in* $(R2) \Rightarrow$	$1 = \big(1 \cdot 43 + 0 \cdot 50\big) - 6 \cdot \big((-1) \cdot 43 + 1 \cdot 50\big)$		
$\Rightarrow (4)$	$1 = 7 \cdot 43 + (-6) \cdot 50$		
		$7 = 7 \cdot 1 + 0$	
		dh. $1 = ggT(a,b)$	
Also z.B.:	$x = 7 \qquad y = -6$		

Beispiel: Für $a = 1088$ und $b = 323$ bestimme $x, y \in \mathbb{Z}$ mit $ggT(a,b) = x \cdot 1088 + y \cdot 323$:

(1)	$1088 = 1 \cdot 1088 + 0 \cdot 323$		
(2)	$323 = 0 \cdot 1088 + 1 \cdot 323$		
		$1088 = 3 \cdot 323 + 119$	
		$\Leftrightarrow \quad 119 = 1088 - 3 \cdot 323$	$(R1)$
$(R1) \Rightarrow (3)$	$119 = 1 \cdot 1088 + (-3) \cdot 323$		
		$323 = 2 \cdot 119 + 85$	
		$\Leftrightarrow \quad 85 = 323 - 2 \cdot 119$	$(R2)$
$(2),(3)$ *in* $(R2) \Rightarrow$	$85 = \big(0 \cdot 1088 + 1 \cdot 323\big) - 2 \cdot \big(1 \cdot 1088 + (-3) \cdot 323\big)$		
$\Rightarrow (4)$	$85 = (-2) \cdot 1088 + 7 \cdot 323$		
		$119 = 1 \cdot 85 + 34$	
		$\Leftrightarrow \quad 34 = 119 - 1 \cdot 85$	$(R3)$
$(3),(4)$ *in* $(R3) \Rightarrow$	$34 = \big(1 \cdot 1088 + (-3) \cdot 323\big) - 1 \cdot \big((-2) \cdot 1088 + 7 \cdot 323\big)$		
$\Rightarrow (5)$	$34 = 3 \cdot 1088 + (-10) \cdot 323$		
		$85 = 2 \cdot 34 + 17$	
		$\Leftrightarrow \quad 17 = 85 - 2 \cdot 34$	$(R4)$
$(4),(5)$ *in* $(R5) \Rightarrow$	$17 = \big((-2) \cdot 1088 + 7 \cdot 323\big) - 2 \cdot \big(3 \cdot 1088 + (-10) \cdot 323\big)$		
$\Rightarrow (6)$	$17 = (-8) \cdot 1088 + 27 \cdot 323$		
		$34 = 2 \cdot 17 + 0$	
		dh. $17 = ggT(a,b)$	
Also z.B.:	$x = -8 \qquad y = 27$		

(b) Ist c ein Vielfaches von $ggT(a,b)$, so existiert eine Zahl $z \in \mathbb{Z}$ mit $c = z \cdot ggT(a,b)$. Bestimmt man zunächst $\tilde{x}, \tilde{y} \in \mathbb{Z}$ mit $ggT(a,b) = \tilde{x} \cdot a + \tilde{y} \cdot b$ (wie in (a)), so erhält man

daraus:

$$c = \big(\underbrace{z \cdot \tilde{x}}_{\stackrel{def}{=} x}\big) \cdot a + \big(\underbrace{z \cdot \tilde{y}}_{\stackrel{def}{=} y}\big) \cdot b$$

Damit hat man c als Linearkombination von a und b dargestellt.

Beispiel: Für $a = 43$ und $b = 50$ bestimme $x, y \in \mathbb{Z}$ mit $12 = x \cdot 43 + y \cdot 50$:

$$(a) \quad \Rightarrow \quad 1 = 7 \cdot 43 + (-6) \cdot 50 \quad \stackrel{\cdot 12}{\Longrightarrow} \quad 12 = 84 \cdot 43 + (-72) \cdot 50$$

Beispiel: Für $a = 1088$ und $b = 323$ bestimme $x, y \in \mathbb{Z}$ mit $-51 = x \cdot 1088 + y \cdot 323$:

$$(a) \quad \Rightarrow \quad 17 = (-8) \cdot 1088 + 27 \cdot 323 \quad \stackrel{\cdot(-3)}{\Longrightarrow} \quad -51 = 24 \cdot 1088 + (-81) \cdot 323$$

Bemerkung. *(Kurzform des Erweiterten Euklidischen Algorithmus')*
Der in 3.10 (b) an Beispielen durchgeführte Erweiterte Euklidische Algorithmus, mit dem man zu $a, b \in \mathbb{Z} \setminus \{0\}$

1.) den größten gemeinsamen Teiler $ggT(a, b)$

2.) Zahlen $x, y \in \mathbb{Z}$ mit $a \cdot x + b \cdot y = ggT(a, b)$

bestimmen kann, lässt sich wie folgt auch verkürzt durchführen:

1.) Man teilt die größere der beiden Zahlen $|a|, |b|$ mit Rest durch die kleinere, also $|b| = q \cdot |a| + r$ $\big($falls $|b| > |a|\big)$. Nun ersetzt man die größere Zahl durch den aufgetretenen Rest $\big($man betrachtet also a und $r\big)$ und führt erneut eine Division mit Rest durch. Dies tut man solange bis der Rest 0 auftritt. Der unmittelbar zuvor aufgetretene (positive) Rest ist dann der ggt von a und b.

Beispiel: $a = 5608,\ b = -21378.$

(1)	21378	$=$	$3 \cdot 5608 + 4554$
(2)	5608	$=$	$1 \cdot 4554 + 1054$
(3)	4554	$=$	$4 \cdot 1054 + 338$
(4)	1054	$=$	$3 \cdot 338 + 40$
(5)	338	$=$	$8 \cdot 40 + 18$
(6)	40	$=$	$2 \cdot 18 + 4$
(7)	18	$=$	$4 \cdot 4 + \boxed{2}$
	$(4$	$=$	$2 \cdot 2)$

Also: $\boxed{ggT(a, b) = 2}$

Die aufgetretenen Gleichungen werden für den folgenden Schritt benötigt und müssen daher notiert werden $\big($bis auf die letzte Gleichung, die nur als Abbruchbedingung dient$\big)$

2.) Nun betrachtet man die letzte Gleichung und löst diese nach $ggT(a, b)$ auf. Der darin vorkommende Rest aus der vorherigen Gleichung wird dann ersetzt. Dann löst man die Klammern auf und ersetzt anschließend den Rest aus der Gleichung

davor. Geht man immer weiter so vor, so hat man schließlich $ggT(a,b)$ als Linearkombination von $|a|$ und $|b|$ dargestellt.

Zu obigem Beispiel:

$$\begin{aligned}
2 &\overset{(7)}{=} 18 - 4\cdot 4\\
&\overset{(6)}{=} 18 - 4\cdot(40 - 2\cdot 18)\\
&= 9\cdot 18 - 4\cdot 40\\
&\overset{(5)}{=} 9\cdot(338 - 8\cdot 40) - 4\cdot 40\\
&= 9\cdot 338 - 76\cdot 40\\
&\overset{(4)}{=} 9\cdot 338 - 76\cdot(1054 - 3\cdot 338)\\
&= 237\cdot 338 - 76\cdot 1054\\
&\overset{(3)}{=} 237\cdot(4554 - 4\cdot 1054) - 76\cdot 1054\\
&= 237\cdot 4554 - 1024\cdot 1054\\
&\overset{(2)}{=} 237\cdot 4554 - 1024\cdot(5608 - 4554)\\
&= 1261\cdot 4554 - 1024\cdot 5608\\
&\overset{(1)}{=} 1261\cdot(21378 - 3\cdot 5608) - 1024\cdot 5608\\
&= 1261\cdot 21378 - 4807\cdot 5608
\end{aligned}$$

Also $\boxed{2 = 1261\cdot 21378 - 4807\cdot 5608}$.

3.) Die Vorzeichen von x und y können ganz am Ende leicht angepasst werden.

Zu obigem Beispiel: Für $a = 5608$ und $b = -21378$ erhält man:

$\boxed{ggT(a,b) = 2 = (-4807)\cdot a + (-1261)\cdot b}$ *Also:* $\boxed{x = -4807 \text{ und } y = -1261}$

Diophantische Gleichungen

Der griechische Mathematiker Diophantos von Alexandria lebte zwischen 100 v. Chr. und 350 n. Chr. (genaue Daten nicht bekannt).

Definition 3.11. *(Lineare Diophantische Gleichungen)*
Sind $a,b,c \in \mathbb{Z}$ gegeben, so heißt die Gleichung

$$(*) \quad a\cdot x + b\cdot y = c \quad \textit{mit den beiden Unbekannten } x,y \in \mathbb{Z}$$

lineare Diophantische Gleichung. *Die* **Lösungsmenge** *der Gleichung $(*)$ ist definiert durch*

$$L_{(*)} \overset{def}{=} \{(x,y) \in \mathbb{Z}\times\mathbb{Z};\ a\cdot x + b\cdot y = c\} \subset \mathbb{Z}\times\mathbb{Z},$$

ihre Elemente heißen **Lösungen** *von $(*)$. Falls $L_{(*)} \neq \varnothing$ ist, heißt $(*)$* **lösbar**.

Beispiel.

- *Wir betrachten die (lineare) Diophantische Gleichung* $\boxed{(*)\ 8\cdot x+7\cdot y=11}$. *Eine Lösung von* $(*)$ *ist* $(x,y)=(4,-3)\in\mathbb{Z}\times\mathbb{Z}$. *Weitere Lösungen sind z.B.*

$$\ldots,\ (-10,13),\ (-3,5),\ (4,-3),\ (11,-11),\ (18,-19),\ \ldots\in L_{(*)}$$

- *Die Gleichung* $\boxed{(**)-6\cdot x+15\cdot y=9}$ *hat z.B. die Lösungen*

$$\ldots,\ (-9,-3),\ (-4,-1),\ (1,1),\ (6,3),\ (11,5),\ \ldots\in L_{(**)}$$

- *Die Gleichung* $\boxed{(***)-6\cdot x+15\cdot y=-8}$ *hat keine Lösungen* $(x,y)\in\mathbb{Z}\times\mathbb{Z}$.

Bemerkung 3.12. *(Spezialfälle)*

- *Wir betrachten* $\boxed{(*)\ a\cdot x+0\cdot y=c}$ *mit* $a,c\in\mathbb{Z}$ *und* $a\neq 0$. *Dann gilt:*
  - *Falls* $a\nmid c$ *gilt, ist* $(*)$ *nicht lösbar, also* $L_{(*)}=\varnothing$.
  - *Falls* $a\mid c$ *gilt, ist* $\frac{c}{a}\in\mathbb{Z}$. *Damit folgt:*

$$(x,y)\text{ löst }(*)\quad\Leftrightarrow\quad a\cdot x=c\quad\Leftrightarrow\quad x=\tfrac{c}{a}\text{ und }y\in\mathbb{Z}\text{ beliebig}$$

  Folglich ist dann $L_{(*)}=\left\{\left(\frac{c}{a},y\right);\ y\in\mathbb{Z}\right\}=\left\{\frac{c}{a}\right\}\times\mathbb{Z}$.

  Für $\boxed{(*)\ 3\cdot x+0\cdot y=12}$ *gilt z.B.* $L_{(*)}=\{\ldots,\ (4,-2),\ (4,-1),\ (4,0),\ (4,1),\ (4,2),\ \ldots\}$

- *Analog hat* $\boxed{(**)\ 0\cdot x+b\cdot y=c}$ *mit* $b,c\in\mathbb{Z}$ *und* $b\neq 0$ *die Lösungsmenge:*

$$L_{(**)}=\left\{\begin{array}{lll}\varnothing & , & \text{falls } b\nmid c\\ \left\{\left(x,\frac{c}{b}\right);\ x\in\mathbb{Z}\right\} & , & \text{falls } b\mid c\end{array}\right\}$$

  Die Gleichung $\boxed{(**)\ 0\cdot x+5\cdot y=-14}$ *ist nicht lösbar, also* $L_{(**)}=\varnothing$.

- *Schließlich ist* $\boxed{(***)\ 0\cdot x+0\cdot y=c}$
  - *unlösbar* $\left(\text{also } L_{(***)}=\varnothing\right)$, *falls* $c\neq 0$ *ist.*
  - *allgemeingültig* $\left(\text{also } L_{(***)}=\mathbb{Z}\times\mathbb{Z}\right)$, *falls* $c=0$ *ist.*

Bemerkung 3.13. *(Lösbarkeit einer Diophantischen Gleichung)*
Eine Diophantische Gleichung $\boxed{a\cdot x+b\cdot y=c}$ *mit gegebenen* $a,b,c\in\mathbb{Z}$ *ist genau dann lösbar, wenn* c *eine Linearkombination von* a *und* b *ist, also nach* 3.8 *genau dann, wenn* $ggT(a,b)\mid c$ *gilt. In diesem Fall können wir mit dem in* 3.10 *beschriebenen Vorgehen stets eine Lösung* (x_0,y_0) *der Gleichung bestimmen.*

Beispiele:

- *Die Lösung* $(7,-6)$ *von* $\boxed{(*)\ 1=x\cdot 43+y\cdot 50}$ *wurde in* 3.10 *(a) bestimmt.*
- *Die Lösung* $(24,-81)$ *von* $\boxed{(**)\ -51=x\cdot 1088+y\cdot 323}$ *wurde in* 3.10 *(b) bestimmt.*

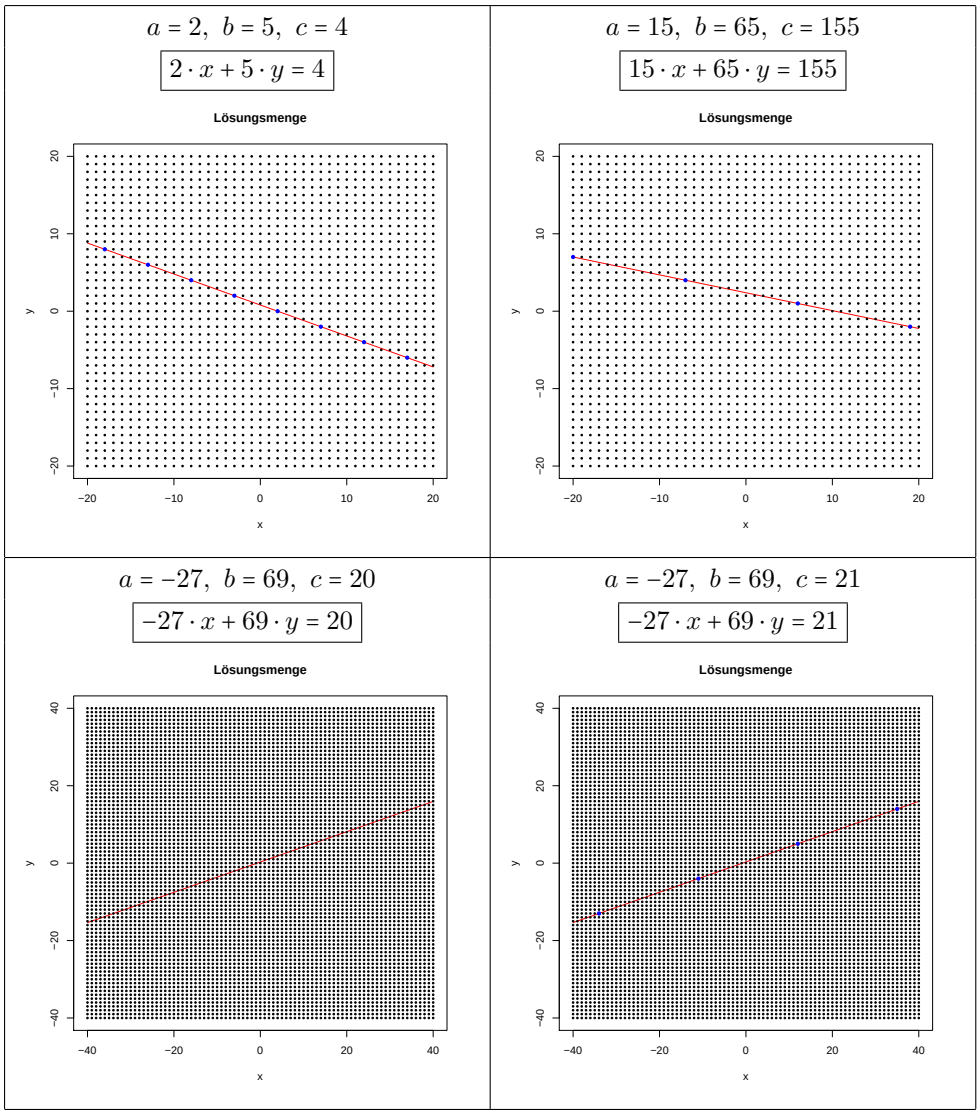
Bemerkung 3.14. *(Zeichnerische Lösung einer Diophantischen Gleichung)*
Gegeben sei eine Diophantische Gleichung $\boxed{(*)\ a \cdot x + b \cdot y = c}$ *mit* $a, b, c \in \mathbb{Z}$.

- *Wir betrachten zunächst den Fall* $b \neq 0$. *Für* $(x, y) \in \mathbb{Q} \times \mathbb{Q}$ *gilt die Äquivalenz:*

$$(x, y) \text{ löst } (*) \quad \Leftrightarrow \quad a \cdot x + b \cdot y = c \quad \Leftrightarrow \quad y = -\frac{a}{b} \cdot x + \frac{c}{b} \quad \Leftrightarrow \quad (x, y) \in g_{(*)}$$

wobei $g_{(*)}$ *die Gerade mit Steigung* $-\frac{a}{b}$ *und y-Achsenabschnitt* $\frac{c}{b}$ *ist. Die "rationalen Lösungen" von* $(*)$ *entsprechen also genau den Punkten auf der Geraden, das heißt:* $L_{(*)}^{(\mathbb{Q})} \overset{def}{=} \{(x, y) \in \mathbb{Q} \times \mathbb{Q};\ a \cdot x + b \cdot y = c\} = g_{(*)}$

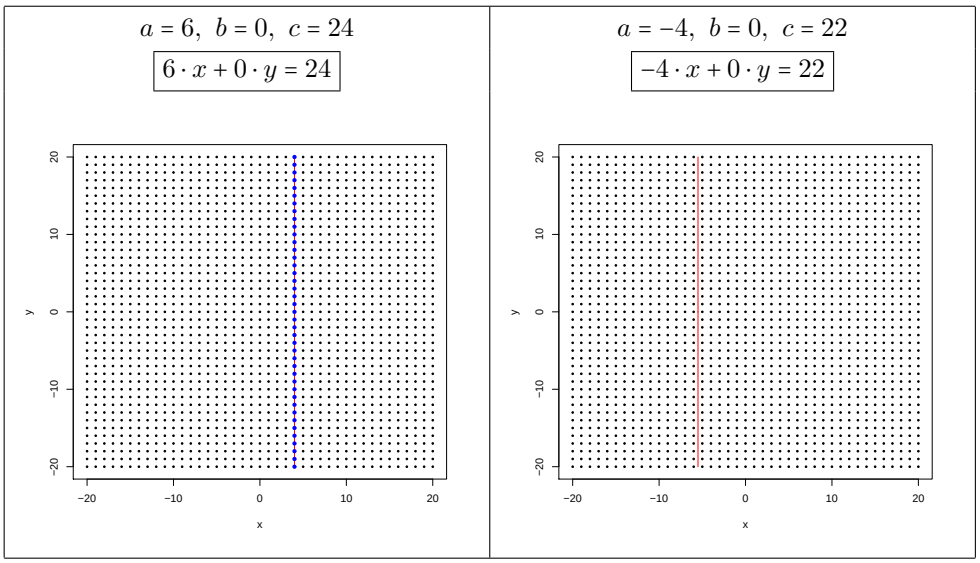
Die Punkte aus $\mathbb{Z} \times \mathbb{Z}$ *bilden ein "Gitter" in der Ebene. Die ganzzahligen Lösungen von* $(*)$ *sind genau die Punkte, in denen die Gerade* $g_{(*)}$ *dieses Gitter schneidet:* $L_{(*)} = g_{(*)} \cap (\mathbb{Z} \times \mathbb{Z})$



- *Im Fall $b = 0$ und $a \neq 0$ gilt für $(x, y) \in \mathbb{Q} \times \mathbb{Q}$:*

$$(x, y) \text{ löst } (*) \quad \Leftrightarrow \quad a \cdot x = c \quad \Leftrightarrow \quad x = \tfrac{c}{a} \quad \Leftrightarrow \quad (x, y) \in g_{(*)}$$

wobei $g_{(*)}$ die zur y-Achse parallele Gerade durch die Punkte $\left(\frac{c}{a}, y\right)$ $(y \in \mathbb{Q})$ ist. Wie im Fall $b \neq 0$ entsprechen die ganzzahligen Lösungen von $(*)$ den Schnittpunkten von $g_{(*)}$ mit dem Gitter $\mathbb{Z} \times \mathbb{Z}$.



Satz 3.15. *(Allgemeine Lösung einer Diophantischen Gleichung)*
Gegeben sei eine beliebige Diophantische Gleichung $\boxed{(*)\ a \cdot x + b \cdot y = c}$ *mit $a, b, c \in \mathbb{Z}$. Wir betrachten hier nur noch den Fall, dass $a \neq 0$ und $b \neq 0$ ist $\big($für $a = 0$ oder $b = 0$ siehe man 3.12$\big)$. Es gilt:*

(a) Falls $ggT(a, b) \nmid c$ gilt, so ist $L_{(*)} = \varnothing$.

(b) Falls a und b teilerfremd sind, ist $(*)$ auf jeden Fall lösbar und es gilt: Ist eine Lösung $(x_0, y_0) \in \mathbb{Z} \times \mathbb{Z}$ von $(*)$ bereits bestimmt, so ist ein beliebiges Zahlenpaar $(x, y) \in \mathbb{Z} \times \mathbb{Z}$ genau dann eine Lösung von $(*)$, falls eine Zahl $t \in \mathbb{Z}$ mit

$$x = x_0 + t \cdot b \quad \text{und} \quad y = y_0 - t \cdot a$$

existiert. Folglich ist dann $L_{(*)} = \{(x_0 + t \cdot b, y_0 - t \cdot a)\,;\ t \in \mathbb{Z}\}$.

(c) Falls $ggT(a, b) \mid c$ gilt, so ist $(*)$ lösbar. Mittels Division durch $ggT(a, b)$ erhält man die Äquivalenzumformung:

$$(*) \quad \Leftrightarrow \quad \left(\frac{a}{ggT(a,b)}\right) \cdot x \ + \ \left(\frac{b}{ggT(a,b)}\right) \cdot y \ = \ \left(\frac{c}{ggT(a,b)}\right)$$

Ist eine Lösung $(x_0, y_0) \in \mathbb{Z} \times \mathbb{Z}$ von $(*)$ bereits bestimmt, so ergibt sich:

$$L_{(*)} = \left\{\left(x_0 + t \cdot \frac{b}{ggT(a,b)} \ , \ y_0 - t \cdot \frac{a}{ggT(a,b)}\right);\ t \in \mathbb{Z}\right\}$$

Beispiel.
Wir bestimmen die Lösungsmenge einiger Diophantischer Gleichungen:

- *Wir betrachten* $\boxed{(*)\ 5\cdot x - 12\cdot y = -2}$ *(also:* $a=5,\ b=-12,\ c=-2$*)*

  1.) Es gilt $ggT(a,b)=1$*, also* $ggT(a,b)\mid c$*. Somit ist* $(*)$ *lösbar.*

  2.) Wir wollen zunächst eine Lösung $(x_0,y_0)\in L_{(*)}$ *bestimmen.*

  – *Zunächst gilt (Kurzform des Euklidischen Algorithmus'):*

$$\boxed{\begin{array}{l|rcl}(1) & 12 &=& 2\cdot 5+2\\ (2) & 5 &=& 2\cdot 2+1\\ & (2 &=& 2\cdot 1)\end{array}} \quad\Rightarrow\quad \boxed{\begin{array}{rcl}1 &\overset{(2)}{=}& 5-2\cdot 2\\ &\overset{(1)}{=}& 5-2\cdot(12-2\cdot 5)\\ &=& 5\cdot 5-2\cdot 12\end{array}}$$

  – *Nun folgt:*

$$\begin{aligned} 1 &= 5\cdot 5-2\cdot 12 = 5\cdot a+2\cdot b\\ \overset{\cdot(-2)}{\Longrightarrow}\quad -2 &= (-10)\cdot a+(-4)\cdot b\end{aligned}$$

  Damit haben wir eine Lösung $(x_0,y_0)=(-10,-4)$ *von* $(*)$ *gefunden.*

  3.) Da a,b *teilerfremd sind, gilt nach* 3.15 *(b), dass:*

$$\begin{aligned} L_{(*)} &= \left\{\ \big((-10)+t\cdot(-12),(-4)-t\cdot 5\big)\ ;\ t\in\mathbb{Z}\right\}\\ &= \{\ldots,\ \underbrace{(14,6)}_{t=-2},\ \underbrace{(2,1)}_{t=-1},\ \underbrace{(-10,-4)}_{t=0},\ \underbrace{(-22,-9)}_{t=1},\ \underbrace{(-34,-14)}_{t=2},\ \ldots\}\end{aligned}$$

- *Wir betrachten* $\boxed{(**)\ (-27)\cdot x+69\cdot y=20}$ *(also:* $a=-27,\ b=69,\ c=20$*)*

  1.) Es gilt $ggT(a,b)=3$*, also* $ggT(a,b)\nmid c$*. Somit ist* $L_{(**)}=\varnothing$*.*

- *Wir betrachten* $\boxed{(***)\ (-27)\cdot x+69\cdot y=21}$ *(also:* $a=-27,\ b=69,\ c=21$*)*

  1.) Es gilt $ggT(a,b)=3$*, also* $ggT(a,b)\mid c$*. Somit ist* $(*)$ *lösbar.*

  2.) Wir wollen zunächst eine Lösung $(x_0,y_0)\in L_{(*)}$ *bestimmen.*

  – *Zunächst gilt (Kurzform des Euklidischen Algorithmus'):*

$$\boxed{\begin{array}{l|rcl}(1) & 69 &=& 2\cdot 27+15\\ (2) & 27 &=& 1\cdot 15+12\\ (3) & 15 &=& 1\cdot 12+3\\ & (12 &=& 4\cdot 3)\end{array}} \quad\Rightarrow\quad \boxed{\begin{array}{rcl}3 &\overset{(3)}{=}& 15-1\cdot 12\\ &\overset{(2)}{=}& 15-1\cdot(27-1\cdot 15)\\ &=& 2\cdot 15-1\cdot 27\\ &\overset{(1)}{=}& 2\cdot(69-2\cdot 27)-1\cdot 27\\ &=& 2\cdot 69-5\cdot 27\end{array}}$$

  – *Nun folgt:*

$$\begin{aligned} 3 &= 2\cdot 69-5\cdot 27 = 5\cdot a+2\cdot b\\ \overset{\cdot(7)}{\Longrightarrow}\quad 21 &= 35\cdot a+14\cdot b\end{aligned}$$

Damit haben wir eine Lösung $(x_0, y_0) = (35, 14)$ *von* $(*)$ *gefunden.*

3.) Nach 3.15 *(c) gilt:*

$$\begin{aligned} L_{(***)} &= \left\{\left(35 + t \cdot \tfrac{69}{3}\ ,\ 14 - t \cdot \tfrac{-27}{3}\right);\ t \in \mathbb{Z}\right\} \\ &= \{(35 + t \cdot 23\ ,\ 14 + t \cdot 9);\ t \in \mathbb{Z}\} \\ &= \{\ldots,\ \underbrace{(-11,-4)}_{t=-2},\ \underbrace{(12,5)}_{t=-1},\ \underbrace{(35,14)}_{t=0},\ \underbrace{(58,23)}_{t=1},\ \underbrace{(81,32)}_{t=2},\ \ldots\} \end{aligned}$$

Anmerkung: Man hätte natürlich auch $(***)$ *zunächst mittels Division durch* $ggT(a,b) = 3$ *äquivalent umformen und dann die entstehende Gleichung*

$$(***) \quad \overset{:3}{\Leftrightarrow} \quad -9 \cdot x + 23 \cdot y = 7$$

lösen können.

Kleinstes gemeinsames Vielfaches

Definition 3.16. *(Kleinstes gemeinsames Vielfaches)*
Für $a_1, \ldots, a_k \in \mathbb{Z}$ *definiert man das* **kleinste gemeinsame Vielfache** *als*

$$kgV(a_1, \ldots, a_k) = \min V(a_1, \ldots, a_k)$$

falls alle $a_j \neq 0$ *sind.* $\big($*Ist mindestens ein* $a_j = 0$*, so sei* $kgV(a_1, \ldots, a_k) \overset{def}{=} 0$.$\big)$

Beispiel.

- $V(5,6) = \{30, 60, 90, 120, \ldots\} \ \Rightarrow\ kgV(5,6) = 30$
- $V(1,2,3,4) = \{12, 24, 36, 48, \ldots\} \ \Rightarrow\ kgV(1,2,3,4) = 12$
- $V(18,21,5) = \{630, 1260, 1890 \ldots\} \ \Rightarrow\ kgV(18,21,5) = 630$

Bemerkung 3.17. *(Elementare Eigenschaften des kgV)*
Gegeben seien beliebige Zahlen $a_1, \ldots, a_k \in \mathbb{Z}$.

(a) Falls alle Zahlen $a_j \neq 0$ *sind, ist die Teilermenge* $V(a_1, \ldots, a_k)$ *eine nichtleere Teilmenge von* $\mathbb{N}$*. Sie hat damit also ein minimales Element und somit ist Definition* 3.16 *sinnvoll.*

Falls (mindestens) ein $a_j = 0$ *ist, so ist* 0 *das einzige gemeinsame Vielfache von* $a_1, \ldots, a_k$ *in* $\mathbb{Z}$*. Da (nach unserer Definition)* $0 \notin \mathbb{N}$ *ist, folgt* $V(a_1, \ldots, a_k) = \varnothing$*. Die Definiton für diesen Fall* $kgV(a_1, \ldots, a_k) \overset{def}{=} 0$ *erscheint sinnvoll.*

(b) Es gilt $V(a_1, \ldots, a_k) = V(|a_1|, \ldots, |a_k|)$ *und folglich* $kgV(a_1, \ldots, a_k) = kgV(|a_1|, \ldots, |a_k|)$.

Beispiel: $V(-2,-5,8,-6) = T(2,5,8,6)\ \big(= \{120, 240, 360, 480, \ldots\}\big) \ \Rightarrow\ kgV(-2,-5,8,-6) = kgV(2,5,8,6)\ \big(= 120\big)$

(c) Gilt $\{a_1,\dots,a_k\} = \{b_1,\dots,b_l\} \subset \mathbb{Z}$*, so ist* $V(a_1,\dots,a_k) = V(b_1,\dots,b_l)$ *und folglich* $kgV(a_1,\dots,a_k) = kgV(b_1,\dots,b_l)$.

Beispiel: $V(5,2,5,2,2) = V(2,5)\ \big(= \{10,20,30,40\dots\}\big) \Rightarrow kgV(5,2,5,2,2) = kgV(2,5)\ \big(= 10\big)$

(d) Es gilt $V(a_1,\dots,a_k,1) = V(a_1,\dots,a_k)$ *und folglich* $kgV(a_1,\dots,a_k,1) = kgV(a_1,\dots,a_k)$.

Beispiel: $V(24,30,1) = V(24,30)\ \big(= \{120,240,360,480\dots,\}\big) \Rightarrow kgV(24,30,1) = kgV(24,30)\ \big(= 120\big)$

(e) Es gilt $kgV(a_1) = |a_1|$.

(f) Gilt $a_1 \mid a_2$*, so ist* $V(a_1,a_2) = V(a_2)$ *und folglich* $kgV(a_1,a_2) = |a_2|$.

Beispiel: $21 \mid 63 \Rightarrow V(21,63) = V(63) \Rightarrow kgV(21,63) = 63$

Satz 3.18. *(Zusammenhang zwischen kgV und PFZ)*
Gegeben seien $n_1,n_2,\dots,n_k \in \mathbb{N}$ *mit den normierten PFZ'en:*

$$n_1 = \prod_{j=1}^{\infty} p_j^{\,e_j^{(1)}}, \quad n_2 = \prod_{j=1}^{\infty} p_j^{\,e_j^{(2)}}, \quad \dots, \quad n_k = \prod_{j=1}^{\infty} p_j^{\,e_j^{(k)}}$$

Dann hat das kleinste gemeinsame Vielfache dieser Zahlen die normierte PFZ:

$$kgV(n_1,\dots,n_k) = \prod_{j=1}^{\infty} p_j^{\left(\max\left\{e_j^{(1)},e_j^{(2)},\dots,e_j^{(k)}\right\}\right)}$$

Beispiel.

- $a_1 = 6,\ a_2 = 28$*:*

$$\begin{array}{rcll} 6 & = & 2^1\cdot 3^1\cdot 5^0\cdot 7^0\cdot 11^0\cdot 13^0\cdot\dots & \\ 28 & = & 2^2\cdot 3^0\cdot 5^0\cdot 7^1\cdot 11^0\cdot 13^0\cdot\dots & \\ \hline kgV(6,28) & = & 2^2\cdot 3^1\cdot 5^0\cdot 7^1\cdot 11^0\cdot 13^0\cdot\dots & = 84 \end{array}$$

- $a_1 = 5000,\ a_2 = 363$*:*

$$\begin{array}{rcll} 1000 & = & 2^3\cdot 3^0\cdot 5^4\cdot 7^0\cdot 11^0\cdot 13^0\cdot\dots & \\ 363 & = & 2^0\cdot 3^1\cdot 5^0\cdot 7^0\cdot 11^2\cdot 13^0\cdot\dots & \\ \hline kgV(5000,363) & = & 2^3\cdot 3^1\cdot 5^4\cdot 7^0\cdot 11^2\cdot 13^0\cdot\dots & = 1815000 \end{array}$$

- $a_1 = 71148,\ a_2 = 24696,\ a_3 = 43120,\ a_4 = 92610$*:*

$$\begin{array}{rcll} 71148 & = & 2^2\cdot 3^1\cdot 5^0\cdot 7^2\cdot 11^2\cdot 13^0\cdot\dots & \\ 24696 & = & 2^3\cdot 3^2\cdot 5^0\cdot 7^3\cdot 11^0\cdot 13^0\cdot\dots & \\ 43120 & = & 2^4\cdot 3^0\cdot 5^1\cdot 7^2\cdot 11^1\cdot 13^0\cdot\dots & \\ 92610 & = & 2^1\cdot 3^3\cdot 5^1\cdot 7^3\cdot 11^0\cdot 13^0\cdot\dots & \\ \hline kgV(71148,24696,43120,92610) & = & 2^4\cdot 3^3\cdot 5^1\cdot 7^3\cdot 11^2\cdot 13^0\cdot\dots & = 89646480 \end{array}$$

Folgerung 3.19. *(Weitere Eigenschaften des kgV)*
Gegeben seien beliebige Zahlen $a_1, \ldots, a_k \in \mathbb{Z}$.

(a) Für eine beliebige Zahl $x \in \mathbb{Z}$ *gilt die Äquivalenz:*

$$a_j \mid x \text{ für alle } j = 1, \ldots, k \quad \Leftrightarrow \quad kgV(a_1, \ldots, a_k) \mid x$$

Also ist $V(a_1, \ldots, a_k) = V\big(kgV(a_1, \ldots, a_k)\big)$.

Beispiel: $V(3,4,5,6) = \{60, 120, 180, 240, \ldots\} = V(60) = V\left(kgV(3,4,5,6)\right)$

(b) Es gilt

$$kgV(a_1, \ldots, a_k) = kgV\big(kgV(a_1, \ldots, a_{k-1}), a_k\big)$$

Beispiel: $kgV(14,21,49) = kgV\big(\underbrace{kgV(14,21)}_{=42}, 49\big) = 294$

$kgV(14,21,49) = kgV\big(14, \underbrace{kgV(21,49)}_{=147}\big) = 294$

(c) Für jede Zahl $b \in \mathbb{Z}$ *gilt*

$$kgV(b \cdot a_1, \ldots, b \cdot a_k) = |b| \cdot kgV(a_1, \ldots, a_k)$$

Beispiel: $kgV(4,10,14) = 70$ *und* $kgV\big(\underbrace{2 \cdot 4}_{=8}, \underbrace{2 \cdot 10}_{=20}, \underbrace{2 \cdot 14}_{=28}\big) = 2 \cdot 70 = 140$

(d) Für zwei Zahlen $a, b \in \mathbb{Z}$ *gilt stets:*

$$ggT(a,b) \cdot kgV(a,b) = a \cdot b$$

(Damit hat man eine weitere Möglichkeit, $kgV(a,b)$ *zu berechnen. Für mehr als zwei Zahlen funktioniert dies allerdings nicht.)*
Folglich sind a, b *genau dann teilerfremd, wenn* $kgV(a,b) = a \cdot b$ *ist.*

Beispiel: $ggT(120,45) \cdot kgV(120,45) = 15 \cdot 360 = 5400 = 120 \cdot 45$

4 Kongruenzrelation und Restklassen

Kongruenzen

Definition 4.1. *(Kongruenzen)*
Gegeben sei eine natürliche Zahl $m \in \mathbb{N}$. Für $a, b \in \mathbb{Z}$ definiert man

$$a \equiv b \ mod \ m \qquad (a \ \textbf{\textit{ist kongruent zu}} \ b \ \textbf{\textit{modulo}} \ m)$$

falls $m \mid (a-b)$. (Ist a nicht kongruent zu b modulo m, so schreibt man $a \not\equiv b \ mod \ m$.)
Man nennt die Beziehung $a \equiv b \ mod \ m$ eine **Kongruenz** *zum* **Modul** *m.*

Beispiel.

- $12 \equiv 6 \ mod \ 3$, *denn* $3 \mid (12-6)$
- $27 \equiv 43 \ mod \ 4$, *denn* $4 \mid (27-43)$
- $-23 \equiv -12 \ mod \ 11$, *denn* $11 \mid ((-23)-(-12))$
- $0 \equiv 77 \ mod \ 7$, *denn* $7 \mid (0-77)$
- $1 \not\equiv 5 \ mod \ 3$, *denn* $3 \nmid (1-5)$
- $26 \not\equiv 43 \ mod \ 2$, *denn* $2 \nmid (26-43)$
- *Für alle $a, b \in \mathbb{Z}$ gilt $a \equiv b \ mod \ 1$ (denn es gilt ja stets $1 \mid (a-b)$).*
- *Für alle $a, b \in \mathbb{Z}$ gilt:*

$$a \equiv b \ mod \ 2 \quad \Leftrightarrow \quad a, b \text{ beide gerade } \underline{\text{oder}} \ a, b \text{ beide ungerade}$$

- *Gesucht sind Zahlen $x \in \mathbb{Z}$ mit $x \equiv 3 \ mod \ 7$. Für x können folgende Zahlen eingesetzt werden:*

$$\ldots, \quad -18, \quad -11, \quad -4, \quad 3, \quad ,10, \quad 17, \quad 24, \quad \ldots, \quad 7003, \quad 7010, \quad ,\ldots$$

Bemerkung 4.2. *(Eigenschaften der Kongruenzrelation)*
Sei $m \in \mathbb{N}$ gegeben.

(a) Die Kongruenzrelation modulo m ist eine Äquivalenzrelation auf $\mathbb{Z}$, das heißt für alle $a, b, c \in \mathbb{Z}$ gilt:

- *(Reflexivität)* $\quad a \equiv a \ mod \ m$
- *(Symmetrie)* $\quad a \equiv b \ mod \ m \ \Rightarrow \ b \equiv a \ mod \ m$
- *(Transitivität)* $\quad (a \equiv b \ mod \ m \ \wedge \ b \equiv c \ mod \ m) \ \Rightarrow \ a \equiv c \ mod \ m$

Für $a, b \in \mathbb{Z}$ mit $a \equiv b \ mod \ m$ gilt daher: $\quad x \equiv a \ mod \ m \ \Leftrightarrow \ x \equiv b \ mod \ m \ (x \in \mathbb{Z})$
Beispiel: Es gilt $17 \equiv 3 \ mod \ 7$. Daher gilt:

$$x \equiv 17 \ mod \ 7 \quad \Leftrightarrow \quad x \equiv 3 \ mod \ 7$$

(b) *Für* $a \in \mathbb{Z}$ *gilt:* $a \equiv 0 \mod m \Leftrightarrow m \mid a$.

Beispiel: *Die Zahlen* $a \in \mathbb{Z}$ *mit* $a \equiv 0 \mod 11$ *sind genau die Vielfachen von* 11, *also* $a \in \{\ldots, -33, -22, -11, 0, 11, 22, 33, \ldots\}$.

(c) *Wir betrachten eine Zahl* $a \in \mathbb{Z}$ *und dividieren sie (mit Rest) durch* m:

$$a = q \cdot m + r \qquad (\text{mit } q \in \mathbb{Z},\ r \in \{0, \ldots, m-1\})$$

Dann gilt $a \equiv r \mod m$.

Beispiel: *Dividiert man* 682 *mit Rest durch* $m = 12$, *so erhält man:* $682 = 56 \cdot 12 + 10$. *Somit ist* $682 \equiv 10 \mod 12$.

(d) *Wir betrachten zwei Zahlen* $a, b \in \mathbb{Z}$ *und dividieren beide (mit Rest) durch* m:

$$a = q_a \cdot m + r_a \quad \text{und} \quad b = q_b \cdot m + r_b \qquad (\text{mit } q_a, q_b \in \mathbb{Z},\ r_a, r_b \in \{0, \ldots, m-1\})$$

Dann gilt: $a \equiv b \mod m \Leftrightarrow r_a = r_b$

Beispiel: *Wir betrachten die Zahlen* 119, 74 *und* -13 *und den Modul* $m = 6$. *Division mit Rest durch* 6 *ergibt:*

$$119 = 19 \cdot 6 + 5, \quad 74 = 12 \cdot 6 + 2, \quad -13 = (-3) \cdot 6 + 5$$

Also lassen 119 *und* -13 *den Rest* 5 *und* 74 *den Rest* 2. *Daher ist:*

$$119 \equiv -13 \mod 6 \quad \underline{\text{aber}} \quad 119 \not\equiv 74 \mod 6 \ \underline{\text{und}}\ 74 \not\equiv (-13) \mod 6$$

Satz 4.3. *(Rechnen mit Kongruenzen)*
Für $k, m \in \mathbb{N}$ *und* $a, b, c \in \mathbb{Z}$ *gelten die folgenden Implikationen:*

(a) $a \equiv b \mod m \Leftrightarrow a + c \equiv b + c \mod m$

Beispiele: *Für* $x \in \mathbb{Z}$ *gilt:*

$$x - 13 \equiv 7 \mod 8 \overset{+13}{\Longleftrightarrow} x \equiv 20 \mod 8 \overset{4.2\ (a),(c)}{\Longleftrightarrow} x \equiv 4 \mod 8$$

und

$$3 \cdot x - 1 \equiv 4 \cdot x + 8 \mod 5 \overset{+(-3x-8)}{\Longleftrightarrow} -9 \equiv x \mod 5 \overset{4.2\ (a),(c)}{\Longleftrightarrow} x \equiv 1 \mod 5$$

(b) $a \equiv b \mod m \Rightarrow a \cdot c \equiv b \cdot c \mod m$ *(die umgekehrte Implikation ist falsch)*

Beispiele:

- *Für* $x \in \mathbb{Z}$ *gilt:*

$$x \equiv 2 \mod 6 \overset{\cdot 4}{\Longrightarrow} 4 \cdot x \equiv 8 \mod 6$$

Eine Äquivalenz liegt hier aber nicht vor: Gegenbeispiel $x = 5$

- *Für* $x \in \mathbb{Z}$ *gilt:*

$$x \equiv 7 \mod 18 \overset{\cdot 8}{\Longrightarrow} 8 \cdot x \equiv 56 \mod 18 \overset{4.2\ (a),(c)}{\Longleftrightarrow} 8 \cdot x \equiv 2 \mod 18$$

Eine Äquivalenz liegt hier aber nicht vor: Gegenbeispiel $x = 16$

- *Für $x \in \mathbb{Z}$ gilt:*

$$x \equiv 2 \ mod\ 5 \quad \overset{\cdot 4}{\Longrightarrow} \quad 4 \cdot x \equiv 8 \ mod\ 5$$

Für die umgekehrte Implikation ist kein Gegenbeispiel zu finden. Vermutung: In diesem Fall liegt eine Äquivalanz vor.

(c) Falls $ggT(c,m) = 1$ ist, gilt: $a \equiv b \ mod\ m \ \Leftrightarrow \ a \cdot c \equiv b \cdot c \ mod\ m$

Beispiele:

- *Wegen $ggT(4,5) = 1$ gilt für $x \in \mathbb{Z}$:*

$$x \equiv 2 \ mod\ 5 \quad \overset{\cdot 4}{\Longleftrightarrow} \quad 4 \cdot x \equiv 8 \ mod\ 5$$

- *Für $x \in \mathbb{Z}$ gilt:*

$$\begin{aligned} 11 \cdot x + 18 \equiv -15 \ mod\ 20 \quad &\Longleftrightarrow \quad 11 \cdot x \equiv -33 \ mod\ 20 \\ &\overset{ggT(11,20)=1}{\Longleftrightarrow} \quad x \equiv -3 \ mod\ 20 \\ &\Longleftrightarrow \quad x \equiv 17 \ mod\ 20 \end{aligned}$$

(d) $a \equiv b \ mod\ \frac{m}{ggT(c,m)} \ \Leftrightarrow \ a \cdot c \equiv b \cdot c \ mod\ m$

Beispiele:

- *Für $x \in \mathbb{Z}$ gilt:*

$$4 \cdot x \equiv 16 \ mod\ 6 \quad \Longleftrightarrow \quad x \equiv 4 \ mod \underbrace{\frac{6}{ggT(4,6)}}_{=\frac{6}{2}=3} \quad \Longleftrightarrow \quad x \equiv 1 \ mod\ 3$$

- *Für $x \in \mathbb{Z}$ gilt:*

$$-6 \cdot x \equiv 48 \ mod\ 15 \quad \Longleftrightarrow \quad x \equiv -8 \ mod \underbrace{\frac{15}{ggT(15,-6)}}_{=\frac{15}{3}=5} \quad \Longleftrightarrow \quad x \equiv 2 \ mod\ 5$$

(e) Im Fall $k \mid m$ gilt:

$$\begin{aligned} a \equiv b \ mod\ m \quad &\Rightarrow \quad a \equiv b \ mod\ k \\ a \equiv b \ mod\ k \quad &\Leftrightarrow \quad \text{es existiert ein } u \in \left\{0, 1, \ldots, \tfrac{m}{k} - 1\right\} \text{ mit } a \equiv b + u \cdot k \ mod\ m \end{aligned}$$

Beispiele:

- *Für $x \in \mathbb{Z}$ gilt:*

$$x \equiv 7 \ mod\ 20 \quad \overset{10|20}{\Longrightarrow} \quad x \equiv 7 \ mod\ 10$$

Eine Äquivalenz liegt hier nicht vor: Gegenbeispiel $x = 17$

- *Für $x \in \mathbb{Z}$ gilt:*

$$x \equiv 7 \ mod\ 20 \quad \overset{2|20}{\Longrightarrow} \quad x \equiv 7 \ mod\ 2 \quad \Longleftrightarrow \quad x \equiv 1 \ mod\ 2$$

Eine Äquivalenz liegt hier nicht vor: Gegenbeispiel $x = 3$

- *Die Kongruenz* $x \equiv 7 \ mod \ 10$ *soll (äquivalent) in Kongruenzen zum Modul* 40 *umgeformt werden. Wegen* $\frac{40}{10} = 4$ *gilt:*

$$\begin{aligned} x \equiv 7 \ mod \ 10 \quad &\Longleftrightarrow \quad \exists \ u \in \{0,1,2,3\} \ mit \ x \equiv 7 + u \cdot 10 \ mod \ 40 \\ &\Longleftrightarrow \quad x \equiv 7 \ mod \ 40 \ \vee \ x \equiv 17 \ mod \ 40 \ \vee \ x \equiv 27 \ mod \ 40 \ \vee \ x \equiv 37 \ mod \ 40 \end{aligned}$$

- *Die Kongruenz* $-14 \cdot x + 60 \equiv 4 \ mod \ 21$ *soll nach* x *aufgelöst werden. Das Ergebnis soll wieder in Kongruenzen zum Modul* 21 *formuliert werden.*

$$\begin{aligned} -14 \cdot x + 60 \equiv 4 \ mod \ 21 \quad &\Longleftrightarrow \quad -14 \cdot x \equiv -56 \ mod \ 21 \\ &\Longleftrightarrow \quad x \equiv 4 \ mod \ \underbrace{\frac{21}{ggT(21,-14)}}_{=\frac{21}{7}=3} \\ &\Longleftrightarrow \quad x \equiv 4 \ mod \ 3 \\ &\Longleftrightarrow \quad x \equiv 1 \ mod \ 3 \\ &\overset{\frac{21}{3}=7}{\Longleftrightarrow} \quad \exists \ u \in \{0,1,2,3,4,5,6\} \ mit \ x \equiv 1 + u \cdot 3 \ mod \ 21 \\ &\Longleftrightarrow \quad x \equiv 1 \ mod \ 21 \ \vee \ x \equiv 4 \ mod \ 21 \ \vee \ x \equiv 7 \ mod \ 21 \ \vee \ x \equiv 10 \ mod \ 21 \\ &\qquad \vee \ x \equiv 13 \ mod \ 21 \ \vee \ x \equiv 16 \ mod \ 21 \ \vee \ x \equiv 19 \ mod \ 21 \end{aligned}$$

Definition 4.4. *(Lineare Kongruenzen)*
Sind $m \in \mathbb{N}$ *und* $a, b \in \mathbb{Z}$ *gegeben, so nennt man*

$$(\triangle) \quad a \cdot x \equiv b \ mod \ m \quad mit \ der \ Unbekannten \ x \in \mathbb{Z}$$

eine **lineare Kongruenz modulo** m*. Ihre* **Lösungsmenge** *ist gegeben durch*

$$L_{(\triangle)} = \{x \in \mathbb{Z};\ a \cdot x \equiv b \ mod \ m\} \subset \mathbb{Z}$$

Man nennt $(\triangle)$ **lösbar**, *falls* $L_{(\triangle)} \neq \varnothing$ *ist.*

Bemerkung 4.5. *(Lösung mit Hilfe einer Diophantischen Gleichung)*
Die Lösungen einer linearen Kongruenz

$$\boxed{(\triangle) \quad a \cdot x \equiv c \ mod \ m} \quad (mit \ gegebenen \ m \in \mathbb{N} \ und \ a, c \in \mathbb{Z})$$

sind genau die Zahlen $x \in \mathbb{Z}$*, die (mit einer geeigneten Zahl* $y \in \mathbb{Z}$*) zu einer Lösung* $(x, y) \in L_{(*)}$ *der zugehörigen Diophantischen Gleichung* $\boxed{(*) \ a \cdot x + m \cdot y = c}$ *ergänzt werden können. Aus* 3.15 *ergibt sich damit:*

- *Im Fall* $ggT(a, m) \nmid c$ *ist* $(\triangle)$ *nicht lösbar.*
- *Im Fall* $ggT(a, m) \mid c$ *ist* $(\triangle)$ *lösbar. Hat man eine Lösung* $x_0 \in L_{(\triangle)}$ *gefunden, so folgt*

$$L_{(\triangle)} = \left\{ x_0 + t \cdot \frac{m}{ggT(a,m)};\ t \in \mathbb{Z} \right\} = \left\{ x \in \mathbb{Z};\ x \equiv x_0 \ mod \ \frac{m}{ggT(a,m)} \right\}$$

Man kann also eine lineare Kongruenz stets über eine zugehörige Diophantische Gleichung lösen.

Beispiel.

- *Wir betrachten die lineare Kongruenz* $\boxed{(\triangle) \quad 13 \cdot x \equiv 5 \ mod\ 9}$ *und die zugehörige Diophantische Gleichung* $\boxed{(*)\ x \cdot 13 + y \cdot 9 = 5}$.

  Mit der Kurzform des erweiterten Euklidischen Algorithmus bestimmen wir zunächst eine Lösung von $(*)$*:*

$$\boxed{\begin{array}{l|rcl} (1) & 13 & = & 1 \cdot 9 + 4 \\ (2) & 9 & = & 2 \cdot 4 + 1 \\ & (4 & = & 4 \cdot 1) \end{array}} \quad \Rightarrow \quad \boxed{\begin{array}{rcl} 1 & \overset{(2)}{=} & 9 - 2 \cdot 4 \\ & \overset{(1)}{=} & 9 - 2 \cdot (13 - 1 \cdot 9) \\ & = & (-2) \cdot 13 + 3 \cdot 9 \end{array}}$$

  Multiplikation mit 5 *ergibt nun* $5 = (-10) \cdot 13 + 15 \cdot 9$*. Damit haben wir eine Lösung* $(-10, 15) \in L_{(*)}$ *von* $(*)$*, bzw. eine Lösung* $-10 \in L_{(\triangle)}$ *von* $(\triangle)$*.*

  Da $ggT(9, 13) = 1$ *gilt, erhalten wir die Lösungsmenge von* $(*)$ *durch*

$$\begin{aligned} L_{(*)} &= \left\{ \left(-10 + t \cdot 9, 15 - t \cdot 13 \right) \ ; \ t \in \mathbb{Z} \right\} \\ &= \{\ldots,\ (-28, 41),\ (-19, 28),\ (-10, 15),\ (-1, 2),\ (8, -11),\ (17, -24),\ (26, -37),\ \ldots\} \end{aligned}$$

  und die Lösungsmenge von $(\triangle)$ *durch*

$$L_{(\triangle)} = \{-10 + t \cdot 9 \ ; \ t \in \mathbb{Z}\} = \{\ldots,\ -28,\ -19,\ -10,\ -1,\ 8,\ 17,\ 26,\ \ldots\} = \{x \in \mathbb{Z};\ x \equiv -10\ mod\ 9\}$$

- *Wir betrachten die lineare Kongruenz* $\boxed{(\triangle\triangle) \quad 14 \cdot x \equiv 8 \ mod\ 22}$ *und die zugehörige Diophantische Gleichung* $\boxed{(**)\ x \cdot 14 + y \cdot 22 = 8}$.

  Mit der Kurzform des erweiterten Euklidischen Algorithmus bestimmen wir zunächst eine Lösung von $(**)$*:*

$$\boxed{\begin{array}{l|rcl} (1) & 22 & = & 1 \cdot 14 + 8 \\ (2) & 14 & = & 1 \cdot 8 + 6 \\ (3) & 8 & = & 1 \cdot 6 + 2 \\ & (6 & = & 3 \cdot 2) \end{array}} \quad \Rightarrow \quad \boxed{\begin{array}{rcl} 2 & \overset{(3)}{=} & 8 - 1 \cdot 6 \\ & \overset{(2)}{=} & 8 - 1 \cdot (14 - 1 \cdot 8) \\ & = & 2 \cdot 8 - 1 \cdot 14 \\ & \overset{(1)}{=} & 2 \cdot (22 - 1 \cdot 14) - 1 \cdot 14 \\ & = & 2 \cdot 22 - 3 \cdot 14 \end{array}}$$

  Multiplikation mit 4 *ergibt nun* $8 = (-12) \cdot 14 + 8 \cdot 22$*. Damit haben wir eine Lösung* $(-12, 8) \in L_{(**)}$ *von* $(**)$*, bzw. eine Lösung* $-12 \in L_{(\triangle\triangle)}$ *von* $(\triangle\triangle)$*.*

  Da $ggT(14, 22) = 2$ *gilt, erhalten wir die Lösungsmenge von* $(**)$ *durch*

$$\begin{aligned} L_{(**)} &= \left\{ \left(-12 + t \cdot \tfrac{22}{2}, 8 - t \cdot \tfrac{14}{2} \right) \ ; \ t \in \mathbb{Z} \right\} \\ &= \{\ldots(-34, 22),\ (-23, 15),\ (-12, 8),\ (-1, 1),\ (10, -6),\ (21, -13),\ (32, -20),,\ \ldots\} \end{aligned}$$

  und die Lösungsmenge von $(\triangle\triangle)$ *durch*

$$L_{(\triangle\triangle)} = \left\{-12 + t \cdot \tfrac{22}{2} \ ; \ t \in \mathbb{Z}\right\} = \{\ldots,\ -34,\ -23,\ -12,\ -1,\ 10,\ 21,\ 32,,\ \ldots\} = \{x \in \mathbb{Z};\ x \equiv -12\ mod\ 11\}$$

- *Wir betrachten die lineare Kongruenz* $\boxed{(\triangle\ \triangle\ \triangle)\quad 9\cdot x \equiv 7\ mod\ 21}$ *und die zugehörige Diophantische Gleichung* $\boxed{(*\,*\,*)\ x\cdot 9 + y\cdot 21 = 7}$.

  Wegen $\underbrace{ggT(9,21)}_{=3} \nmid 7$ *ist* $(*\,*\,*)$ *nicht lösbar. Damit ist auch* $(\triangle\ \triangle\ \triangle)$ *nicht lösbar, also* $L_{(\triangle\triangle\triangle)} = \varnothing$.

Bemerkung 4.6. *(Lösung mit Äquivalenzumformungen)*
Gegeben sei eine lineare Kongruenz

$$(\triangle)\quad a\cdot x \equiv c\ mod\ m\quad (\textit{mit gegebenen } m\in\mathbb{N} \textit{ und } a,c\in\mathbb{Z})$$

(a) Wir betrachten zunächst den Fall, dass a *und* m *teilerfremd sind.* $\big($*Dann gilt auf jeden Fall* $ggT(a,m)\mid c$*, folglich ist* $(\triangle)$ *lösbar.*$\big)$
Man kann $(\triangle)$ *nun wie folgt lösen:*

1.) Mit Hilfe des erweiterten Euklidischen Algorithmus' (siehe 3.10*) bestimmt man Zahlen* $u,v\in\mathbb{Z}$ *mit* $u\cdot a+v\cdot m = 1$*. Die Zahl* u *erfüllt nun* $u\cdot a \equiv 1\ mod\ m$ *und folglich auch:*

- $ggT(u,m) = 1$
- $u\cdot a\cdot x \equiv x\ mod\ m\quad (\textit{unabhängig von } x)$

2.) Man kann nun die lineare Kongruenz $(\triangle)$*, indem man sie zunächst mit* u *multipliziert (siehe* 4.3 *(c)) und dann* $u\cdot a\cdot x$ *durch* x *ersetzt (siehe* 4.2 *(a)):*

$$(\triangle)\quad a\cdot x \equiv c\ mod\ m \overset{4.3\ (c)}{\iff} u\cdot a\cdot x \equiv u\cdot c\ mod\ m \overset{4.2\ (a)}{\iff} x \equiv u\cdot c\ mod\ m$$

$$\textit{Folglich:}\qquad L_{(\triangle)} = \{x\in\mathbb{Z};\ x \equiv u\cdot c\ mod\ m\}$$

(b) Nun betrachten wir den Fall, dass a *und* m *nicht teilerfremd sind. Falls nun* $ggT(a,m)\nmid c$ *gilt, so ist* $L_{(\triangle)} = \varnothing$*. Wir untersuchen also nur noch den Fall, dass* $ggT(a,m)\mid c$ *gilt. Man kann* $(\triangle)$ *dann wie folgt lösen:*

1.) Gemäß 4.3 *(d) kann man* $(\triangle)$ *äquivalent umformen, indem man durch* $ggT(a,m)$ *teilt:*

$$(\triangle)\quad a\cdot x \equiv c\ mod\ m \quad\Leftrightarrow\quad \frac{a}{ggT(a,m)}\cdot x \equiv \frac{c}{ggT(a,m)}\ mod\ \underbrace{\frac{m}{ggT(m,ggT(a,m))}}_{=\frac{m}{ggT(a,m)}}$$

2.) In der dabei enstandenen linearen Kongruenz

$$a'\cdot x \equiv c'\ mod\ m' \quad \left(\textit{mit } a' = \frac{a}{ggT(a,m)},\ c' = \frac{c}{ggT(a,m)},\ m' = \frac{m}{ggT(a,m)}\right)$$

sind a' *und* m' *stets teilerfremd. Man kann sie also wie in (a) lösen und hat damit natürlich auch* $(\triangle)$ *gelöst.*

3.) (wahlweise) Die Lösungen der ursprünglichen Kongruenz modulo m sind nun in der Form einer (vollständig aufgelösten) Kongruenz modulo $\frac{m}{ggT(a,m)}$ gegeben. Mit Hilfe von 4.3 (e) kann man diese nun (falls gewünscht) wieder in mehrere Kongruenzen modulo m überführen.

Beispiel.

- *Wir betrachten die lineare Kongruenz* $\boxed{(\triangle) \quad 13 \cdot x \equiv 5 \ mod\ 9}$. *Wegen* $ggT(13,9) = 1$ *existieren Zahlen* $u, v \in \mathbb{Z}$ *mit* $u \cdot 13 + v \cdot 9 = 1$. *Man findet solche Zahlen mit dem Erweiteren Euklidischen Algorithmus, etwa* $u = -2$ *und* $v = 3$.

  Nun formen wir $(\triangle)$ *äquivalent um. Es gilt:*

  $$(\triangle) \quad 13 \cdot x \equiv 5 \ mod\ 9 \overset{\cdot(-2),\ ggT(-2,9)=1}{\Longleftrightarrow} -26 \cdot x \equiv -10 \ mod\ 9 \overset{-26 \cdot x \equiv x \ mod\ 9}{\Longleftrightarrow} x \equiv -10 \ mod\ 9$$

  Also ist $L_{(\triangle)} = \{x \in \mathbb{Z};\ x \equiv -10 \ mod\ 9\}$

- *Wir betrachten die lineare Kongruenz* $\boxed{(\triangle\triangle) \quad 14 \cdot x \equiv 8 \ mod\ 22}$. *Wegen* $ggT(14,22) \mid 8$ *ist* $(\triangle\triangle)$ *lösbar. Wir teilen zunächst durch* $ggT(14,22) = 2$ *und gehen dann wie oben vor:*

  $$\begin{aligned}
  (\triangle\triangle) \qquad & 14 \cdot x \equiv 8 \ mod\ 22 \\
  \overset{:2}{\Longleftrightarrow} \quad & 7 \cdot x \equiv 4 \ mod\ \frac{22}{ggT(22,2)} \\
  \Longleftrightarrow \quad & 7 \cdot x \equiv 4 \ mod\ 11 \\
  & (\textit{beachte nun:} \quad 8 \cdot 7 + (-5) \cdot 11 = 1) \\
  \overset{\cdot 8,\ ggT(8,11)=1}{\Longleftrightarrow} \quad & 56 \cdot x \equiv 32 \ mod\ 11 \\
  \overset{56 \cdot x \equiv x \ mod\ 11,\ 32 \equiv 10 \ mod\ 11}{\Longleftrightarrow} \quad & x \equiv 10 \ mod\ 11 \\
  \overset{4.3(e)}{\Longleftrightarrow} \quad & \exists\ u \in \{0,1\} \ \ mit\ x \equiv 10 + u \cdot 11 \ mod\ 22 \\
  \Longleftrightarrow \quad & x \equiv 10 \ mod\ 22 \ \vee \ x \equiv 21 \ mod\ 22
  \end{aligned}$$

  Also ist

  $$L_{(\triangle\triangle)} = \{x \in \mathbb{Z};\ x \equiv 10 \ mod\ 11\} = \{x \in \mathbb{Z};\ x \equiv 10 \ mod\ 22 \ \vee \ x \equiv 21 \ mod\ 22\}$$

Restklassen und Verknüpfungen von Restklassen

Bemerkung 4.7. *(Einführung von Restklassen)*
Sei $m \in \mathbb{N}$ *gegeben.*

(a) Wie wir schon gesehen haben, ist die Kongruenzrelation modulo m eine Äquivalenzrelation auf $\mathbb{Z}$. Die Äquivalenzklasse zu einer Zahl $a \in \mathbb{Z}$ bezeichnen wir mit

$$\overline{a} \overset{def}{=} [a]_m \overset{def}{=} \{x \in \mathbb{Z};\ x \equiv a \ mod\ m\}$$

Beispiele:

- *Für* $m = 23$ *gilt:*

$$\overline{3}\ (= [3]_{23}) = \{\ldots,\ -43,\ -20,\ 3,\ 26,\ 49,\ 72,\ \ldots\}$$

- *Für* $m = 5$ *gilt:*

$$\begin{array}{rcll}
 & \vdots & & \\
\overline{-2} & = & \{\ldots,\ -17,\ -12,\ -7,\ -2,\ 3,\ 8,\ 13,\ \ldots\} & = \overline{3} \\
\overline{-1} & = & \{\ldots,\ -16,\ -11,\ -6,\ -1,\ 4,\ 9,\ 14,\ \ldots\} & = \overline{4} \\
\hline
\overline{0} & = & \{\ldots,\ -15,\ -10,\ -5,\ 0,\ 5,\ 10,\ 15,\ \ldots\} & \\
\overline{1} & = & \{\ldots,\ -14,\ -9,\ -4,\ 1,\ 6,\ 11,\ 16,\ \ldots\} & \\
\overline{2} & = & \{\ldots,\ -13,\ -8,\ -3,\ 2,\ 7,\ 12,\ 17,\ \ldots\} & \\
\overline{3} & = & \{\ldots,\ -12,\ -7,\ -2,\ 3,\ 8,\ 13,\ 17,\ \ldots\} & \\
\overline{4} & = & \{\ldots,\ -11,\ -6,\ -1,\ 4,\ 9,\ 14,\ 19,\ \ldots\} & \\
\hline
\overline{5} & = & \{\ldots,\ -10,\ -5,\ 0,\ 5,\ 10,\ 15,\ 20,\ \ldots\} & = \overline{0} \\
\overline{6} & = & \{\ldots,\ -9,\ -4,\ 1,\ 6,\ 11,\ 16,\ 21,\ \ldots\} & = \overline{1} \\
\overline{7} & = & \{\ldots,\ -8,\ -3,\ 2,\ 7,\ 12,\ 17,\ 22,\ \ldots\} & = \overline{2} \\
 & \vdots & &
\end{array}$$

- *Zum Modul* $m = 10$ *gilt* $\overline{1} = \{\ldots,\ -29,\ -19,\ -9,\ 1,\ 11,\ 21,\ 31,\ \ldots\}$.
  Zum Modul $m = 12$ *gilt* $\overline{1} = \{\ldots,\ -35,\ -23,\ -11,\ 1,\ 13,\ 25,\ 37,\ \ldots\}$.
  Die Schreibweise $\overline{1}$ $\left(\text{bzw. allgemein } \overline{a}\right)$ *kann also nur verwendet werden, wenn klar ist, was der zugrundeliegende Modul* m *ist. Ansonsten kann man natürlich auch* $[1]_{10}$ *im Unterschied zu* $[1]_{12}$ *schreiben.*

(b) Offenbar gilt stets $a \in \overline{a}$.

Wie bei jeder Äquivalenzrelation gilt für beliebige Zahlen $a, b \in \mathbb{Z}$:

$$\overline{a} = \overline{b} \quad , \quad \text{falls } a \equiv b \bmod m$$
$$\overline{a} \cap \overline{b} = \varnothing \quad , \quad \text{falls } a \not\equiv b \bmod m$$

Beispiel: Zum Modul $m = 8$ *gilt*

$$3 \equiv 27 \bmod 8 \quad \Rightarrow \quad \overline{3} = \{\ldots,\ -13,\ -5,\ ,3,\ 11,\ 19,\ 27,\ 35,\ 43,\ \ldots\} = \overline{27}$$
$$(\text{für } x \in \mathbb{Z} \text{ ist: } x \in \overline{3} \ \Leftrightarrow\ x \in \overline{27})$$

und

$$-5 \not\equiv 12 \bmod 8 \quad \Rightarrow \quad \overline{-5} \cap \overline{12} = \{\ldots,\ -13,\ -5,\ 3,\ 11,\ 19,\ 27,\ \ldots\} \cap \{\ldots,\ -12,\ -4,\ 4,\ 12,\ 20,\ 28,\ \ldots\} = \varnothing$$
$$(\text{es gibt keine Zahl } x \in \mathbb{Z} \text{ mit } x \in \overline{-5} \text{ und } x \in \overline{12})$$

Jede Äquivalenzklasse kann daher auf unendlich viele Arten dargestellt werden.
Es gilt: $\overline{a} = \overline{x}$ *für jedes* $x \in \overline{a}$
Beispiel: Zum Modul $m = 8$ *gilt beispielsweise:*

$$\ldots = \overline{-16} = \overline{-8} = \overline{0} = \overline{8} = \overline{16} = \overline{24} = \ldots$$
$$\ldots = \overline{-19} = \overline{-11} = \overline{-3} = \overline{5} = \overline{13} = \overline{21} = \ldots$$

(c) *Bei Äquivalenzrelationen ist es üblich, jedes Element $x \in \overline{a}$ einer Äquivalenzklasse als* **Repräsentant von** $\overline{a}$ *zu bezeichnen. Ein Repräsentant der Äquivalanzklasse von a ist der Rest bei Division von a durch m:*

$$a = q{\cdot}m{+}r \ (q \in \mathbb{Z},\ r \in \{0,\ldots,m-1\}) \quad \Rightarrow \quad a \equiv r \bmod m \quad \Rightarrow \quad r \in \overline{a} \quad \Rightarrow \quad \overline{a} = \overline{r}$$

Man bezeichnet die Äquivalenzklasse von a daher auch als **Restklasse** *von a (modulo m).*
Beispiel: Zum Modul $m = 15$ gilt

$$\begin{aligned} \overline{99} &= \overline{9} && (\textit{denn } 99 = 6 \cdot 15 + 9) \\ \overline{182} &= \overline{2} && (\textit{denn } 212 = 12 \cdot 15 + 2) \\ \overline{-182} &= \overline{13} && (\textit{denn } -212 = -13 \cdot 15 + 13) \\ \overline{1515} &= \overline{0} && (\textit{denn } 1515 = 101 \cdot 15 + 0) \end{aligned}$$

(d) *Es gibt genau m Restklassen modulo m, nämlich die Restklassen $\overline{0}, \overline{1}, \ldots, \overline{m-1}$. Die Menge aller Restklassen modulo m bezeichnen wir mit*

$$R_m \stackrel{def}{=} \{\overline{a};\ a \in \mathbb{Z}\} = \left\{\overline{0},\ \overline{1},\ \ldots,\ \overline{m-1}\right\}$$

Beispiel: Es gilt:

$$\begin{aligned} R_5 &= \left\{\overline{0},\ \overline{1},\ \overline{2},\ \overline{3},\ \overline{4}\right\} &&= \{[0]_5,\ [1]_5,\ [2]_5,\ [3]_5,\ [4]_5\} \\ R_{44} &= \left\{\overline{0},\ \overline{1},\ \ldots,\ \overline{43}\right\} &&= \{[0]_{43},\ [1]_{43},\ \ldots,\ [43]_{44}\} \end{aligned}$$

Satz 4.8. *(Addition von Restklassen)*
Sei $m \in \mathbb{N}$ gegeben.

(a) *Für $a_1, a_2, b_1, b_2 \in \mathbb{Z}$ mit $a_1 \equiv a_2 \bmod m$ und $b_1 \equiv b_2 \bmod m$ gilt stets auch $a_1 + b_1 \equiv a_2 + b_2 \bmod m$.*

(b) *Zwei Restklassen $\overline{a}, \overline{b} \in R_m$ können durch*

$$\overline{a} \oplus \overline{b} \stackrel{def}{=} \overline{a+b} \in R_m$$

'addiert' werden.
Beispiel: In R_8 gilt

$$\overline{3} \oplus \overline{4} = \overline{3+4} = \overline{7}, \quad \overline{5} \oplus \overline{6} = \overline{5+6} = \overline{11} = \overline{3} \quad \overline{4} \oplus \overline{4} = \overline{0}$$

Durch diese Definition entsteht kein Widerspruch, denn falls $\overline{a_1} = \overline{a_2}$ und $\overline{b_1} = \overline{b_2}$ gilt, ist stets auch $\overline{a_1} \oplus \overline{b_1} = \overline{a_2} \oplus \overline{b_2}$.
Beispiel: In R_9 gilt

$$\overline{2} = \overline{29} \textit{ und } \overline{7} = \overline{-47}$$

Damit die neue Definition der 'Restklassen-Addition' konsistent ist, muss daher auch $\overline{2} \oplus \overline{7} = \overline{29} \oplus \overline{-47}$ gelten. Tatsächlich ist

$$\overline{2} \oplus \overline{7} = \overline{9} = \overline{0} \quad \textit{und} \quad \overline{29} \oplus \overline{-47} = \overline{-18} = \overline{0}$$

(c) *Die in (b) definierte Addition $\oplus$ ist eine* **Verknüpfung** *auf R_m, das heißt je zwei Elementen von R_m wird durch $\oplus$ wiederum ein Element aus R_m zugeordnet.*
Beispiel: Da R_m eine endliche Menge ist, kann man eine vollständige Verknüpfungstabelle für die Verknüpfung $\oplus$ aufstellen.

$\oplus$ *in* R_7	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{4}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{5}$	$\overline{5}$	$\overline{6}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{6}$	$\overline{6}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$

Dabei gilt:

- *(Kommutativgesetz) Für alle $\overline{a}, \overline{b} \in R_m$ gilt $\overline{a} \oplus \overline{b} = \overline{b} \oplus \overline{a}$.*
  Beispiel: In R_7 gilt zum Beispiel

  $$\overline{1} \oplus \overline{5} = \overline{6} = \overline{5} \oplus \overline{1} \quad \textit{und} \quad \overline{3} \oplus \overline{6} = \overline{2} = \overline{6} \oplus \overline{3}$$

  (obige Tabelle ist an der Diagonalen symmetrisch)

- *(Assoziativgesetz) Für alle $\overline{a}, \overline{b}, \overline{c} \in R_m$ gilt $\left(\overline{a} \oplus \overline{b}\right) \oplus \overline{c} = \overline{a} \oplus \left(\overline{b} \oplus \overline{c}\right)$.*
  Beispiel: In R_7 gilt zum Beispiel

  $$\left(\overline{2} \oplus \overline{4}\right) \oplus \overline{4} = \overline{6} \oplus \overline{4} = \overline{3} \quad \textit{und auch} \quad \overline{2} \oplus \left(\overline{4} \oplus \overline{4}\right) = \overline{2} \oplus \overline{1} = \overline{3}$$

- *(Existenz eines neutralen Elements) Es gilt $\overline{a} \oplus \overline{0} = \overline{0} \oplus \overline{a} = \overline{a}$ für alle $\overline{a} \in R_m$. Man nennt daher auch $\overline{0}$* **Neutrales Element bezüglich** $\oplus$.

- *(Existenz inverser Elemente) Für alle $\overline{a} \in R_m$ gilt $\overline{a} \oplus \overline{-a} = \overline{-a} \oplus \overline{a} = \overline{0}$. Man nennt daher auch $\overline{-a}$* **Inverses Element zu** $\overline{a}$ **bezüglich** $\oplus$.
  Beispiel: In R_7 ist bezüglich $\oplus$

  -) $\overline{0}$ das Inverse zu $\overline{0}$

  -) $\overline{6}$ das Inverse zu $\overline{1}$ (denn $\overline{-1} = \overline{6}$)

  -) entsprechend $\overline{1}$ das Inverse zu $\overline{6}$

  -) $\overline{2}$ das Inverse zu $\overline{5}$ und $\overline{5}$ das Inverse zu $\overline{2}$

  -) $\overline{3}$ das Inverse zu $\overline{4}$ und $\overline{4}$ das Inverse zu $\overline{3}$

Satz 4.9. *(Multiplikation von Restklassen)*
Sei $m \in \mathbb{N}$ gegeben.

(a) *Für $a_1, a_2, b_1, b_2 \in \mathbb{Z}$ mit $a_1 \equiv a_2 \mod m$ und $b_1 \equiv b_2 \mod m$ gilt stets auch $a_1 \cdot b_1 \equiv a_2 \cdot b_2 \mod m$.*

(b) Zwei Restklassen $\overline{a}, \overline{b} \in R_m$ können durch

$$\overline{a} \odot \overline{b} \overset{def}{=} \overline{a \cdot b} \in R_m$$

'multipliziert' werden.
Beispiel: In R_{10} gilt

$$\overline{4} \odot \overline{7} = \overline{4 \cdot 7} = \overline{28} = \overline{8}, \quad \overline{8} \odot \overline{8} = \overline{8 \cdot 8} = \overline{64} = \overline{4} \quad \overline{7} \odot \overline{3} = \overline{1}$$

Durch diese Definition entsteht kein Widerspruch, denn falls $\overline{a_1} = \overline{a_2}$ und $\overline{b_1} = \overline{b_2}$ gilt, ist stets auch $\overline{a_1} \odot \overline{b_1} = \overline{a_2} \odot \overline{b_2}$.
Beispiel: In R_{20} gilt

$$\overline{12} = \overline{72} \text{ und } \overline{7} = \overline{-93}$$

Damit die neue Definition der 'Restklassen-Multiplikation' konsistent ist, muss daher auch $\overline{12} \odot \overline{7} = \overline{72} \odot \overline{-93}$ gelten. Tatsächlich ist

$$\overline{12} \odot \overline{7} = \overline{84} = \overline{4} \quad \text{und} \quad \overline{72} \odot \overline{-93} = \overline{-6696} = \overline{4}$$

(c) Die in (b) definierte Multiplikation $\odot$ ist eine **Verknüpfung** *auf R_m, das heißt je zwei Elementen von R_m wird durch $\odot$ wiederum ein Element aus R_m zugeordnet.*
Beispiel: Da R_m eine endliche Menge ist, kann man eine vollständige Verknüpfungstabelle für die Verknüpfung $\odot$ aufstellen.

$\odot$ in R_7	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{4}$	$\overline{6}$	$\overline{1}$	$\overline{3}$	$\overline{5}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{6}$	$\overline{2}$	$\overline{5}$	$\overline{1}$	$\overline{4}$
$\overline{4}$	$\overline{0}$	$\overline{4}$	$\overline{1}$	$\overline{5}$	$\overline{2}$	$\overline{6}$	$\overline{3}$
$\overline{5}$	$\overline{0}$	$\overline{5}$	$\overline{3}$	$\overline{1}$	$\overline{6}$	$\overline{4}$	$\overline{2}$
$\overline{6}$	$\overline{0}$	$\overline{6}$	$\overline{5}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

Dabei gilt:

- *(Kommutativgesetz) Für alle $\overline{a}, \overline{b} \in R_m$ gilt $\overline{a} \odot \overline{b} = \overline{b} \odot \overline{a}$.*
  Beispiel: In R_7 gilt zum Beispiel

  $$\overline{2} \odot \overline{5} = \overline{3} = \overline{5} \odot \overline{2} \quad \text{und} \quad \overline{3} \odot \overline{4} = \overline{5} = \overline{4} \odot \overline{3}$$

  (obige Tabelle ist an der Diagonalen symmetrisch)

- *(Assoziativgesetz) Für alle $\overline{a}, \overline{b}, \overline{c} \in R_m$ gilt $\left(\overline{a} \odot \overline{b}\right) \odot \overline{c} = \overline{a} \odot \left(\overline{b} \odot \overline{c}\right)$.*
  Beispiel: In R_7 gilt zum Beispiel

  $$\left(\overline{5} \odot \overline{3}\right) \odot \overline{6} = \overline{1} \odot \overline{6} = \overline{6} \quad \text{und auch} \quad \overline{5} \odot \left(\overline{3} \odot \overline{6}\right) = \overline{5} \odot \overline{4} = \overline{6}$$

- *(Distributivgesetz) Für alle $\overline{a}, \overline{b}, \overline{c} \in R_m$ gilt $\left(\overline{a} \oplus \overline{b}\right) \odot \overline{c} = (\overline{a} \odot \overline{c}) \oplus \left(\overline{b} \odot \overline{c}\right)$.*
  Beispiel: In R_7 gilt zum Beispiel

  $$\left(\overline{4} \oplus \overline{2}\right) \odot \overline{4} = \overline{6} \odot \overline{4} = \overline{3} \quad \text{und auch} \quad \left(\overline{4} \odot \overline{4}\right) \oplus \left(\overline{2} \odot \overline{4}\right) = \overline{2} \oplus \overline{1} = \overline{3}$$

- *(Existenz eines neutralen Elements) Es gilt* $\overline{a} \odot \overline{1} = \overline{1} \odot \overline{a} = \overline{a}$ *für alle* $\overline{a} \in R_m$. *Man nennt daher auch* $\overline{1}$ **Neutrales Element bezüglich** $\odot$.
- *Bezüglich* $\odot$ *existieren nicht immer inverse Elemente.*
  Beispiel: In R_7 *ist bezüglich* $\odot$

  -) $\overline{1}$ *das Inverse zu* $\overline{1}$

  -) $\overline{2}$ *das Inverse zu* $\overline{4}$ *und* $\overline{4}$ *das Inverse zu* $\overline{2}$

  -) $\overline{3}$ *das Inverse zu* $\overline{5}$ *und* $\overline{5}$ *das Inverse zu* $\overline{3}$

  -) $\overline{6}$ *das Inverse zu* $\overline{6}$

  -) $\overline{0}$ *nicht invertierbar (d.h. es gibt kein Element in* R_7*, das invers zu* $\overline{0}$ *bezüglich* $\odot$ *ist)*

  In R_{10} *ist bezüglich* $\odot$

  -) $\overline{1}$ *invers zu sich selbst (kurz: 'selbstinvers')*

  -) $\overline{9}$ *selbstinvers*

  -) $\overline{3}$ *und* $\overline{7}$ *invers zueinander*

  -) $\overline{0},\ \overline{2},\ \overline{4},\ \overline{5},\ \overline{6},\ \overline{8}$ *nicht invertierbar*
- *Für* $\overline{a}, \overline{b} \in R_m$ *gilt stets die Implikation:*

$$\overline{a} = \overline{0} \text{ oder } \overline{b} = \overline{0} \quad \Rightarrow \quad \overline{a} \odot \overline{b} = \overline{0}$$

  Die umgekehrte Implikation ist für manche $m \in \mathbb{N}$ *jedoch falsch. Man nennt Elemente* $\overline{a}, \overline{b} \in R_m \setminus \{\overline{0}\}$ *mit* $\overline{a} \odot \overline{b} = \overline{0}$ **Nullteiler**.
  Beispiel: In R_7 *gibt es keine Nullteiler. Hier gilt* $\overline{a} \odot \overline{b} = \overline{0}$ *nur wenn* $\overline{a} = \overline{0}$ *oder* $\overline{b} = \overline{0}$ *ist.*

  In R_{15} *gilt zum Beispiel*

$$\overline{9} \neq \overline{0} \text{ und } \overline{10} \neq \overline{0} \quad \text{aber} \quad \overline{9} \odot \overline{10} = \overline{0}$$

  und auch

$$\overline{3} \neq \overline{0} \text{ und } \overline{5} \neq \overline{0} \quad \text{aber} \quad \overline{3} \odot \overline{5} = \overline{0}$$

  Die Elemente $\overline{9},\ \overline{10},\ \overline{3},\ \overline{5}$ *sind also Nullteiler in* R_{15} *(es gibt darin noch weitere Nullteiler).*

(d) Für $\overline{a} \in R_m$ *und* $n \in \mathbb{N}$ *definiert man*

$$(\overline{a})^n \overset{def}{=} \underbrace{\overline{a} \odot \overline{a} \odot \ldots \odot \overline{a}}_{n\text{-mal}}$$

Es ist sinnvoll zusätzlich $(\overline{a})^0 \overset{def}{=} \overline{1}$ *zu definieren. Es gilt stets* $(\overline{a})^n = \overline{a^n}$.

Beispiel: In R_9 gilt zum Beispiel

$$\begin{array}{lcll}
\overline{2}^2 & = & \overline{2}\odot\overline{2} & = \overline{4}\\
\overline{2}^3 & = & \overline{2}\odot\overline{2}\odot\overline{2} & = \overline{8}\\
\overline{2}^4 & = & \overline{2}\odot\overline{2}\odot\overline{2}\odot\overline{2} & = \overline{7}\\
\overline{2}^5 & = & \overline{2}\odot\overline{2}\odot\overline{2}\odot\overline{2}\odot\overline{2} & = \overline{5}\\
\overline{2}^6 & = & \overline{2}\odot\overline{2}\odot\overline{2}\odot\overline{2}\odot\overline{2}\odot\overline{2} & = \overline{1}\\
\overline{2}^7 & = & \overline{2}\odot\overline{2}\odot\overline{2}\odot\overline{2}\odot\overline{2}\odot\overline{2}\odot\overline{2} & = \overline{2}\\
\overline{2}^8 & = & \overline{2}\odot\overline{2}\odot\overline{2}\odot\overline{2}\odot\overline{2}\odot\overline{2}\odot\overline{2}\odot\overline{2} & = \overline{4}\\
 & \vdots & & \vdots
\end{array}$$

In R_m gelten die Potenzgesetze in Verbindung mit $\odot$:

$$\left(\overline{a}\odot\overline{b}\right)^n = \overline{a}^n\odot\overline{b}^n,\quad \overline{a}^n\odot\overline{a}^m = \overline{a}^{n+m},\quad \left(\overline{a}^n\right)^m = \overline{a}^{n\cdot m}\qquad \left(\textit{für } \overline{a},\overline{b}\in R_m,\ n,m\in\mathbb{N}_0\right)$$

Anwendungen

Bemerkung 4.10. *(Bestimmung von Resten)*
Für $a\in\mathbb{Z}$ und $m\in\mathbb{N}$ gilt: Die Division $a:m$ hat den Rest r, falls $r\in\{0,\dots,m-1\}$ die Zahl ist, für die $\overline{a}=\overline{r}\in R_m$ gilt. Der Rest der Division $a:m$ kann also bestimmt werden, indem man die Restklasse $\overline{a}$ in R_m vereinfacht. Dabei lassen sich 'Addition und 'Multiplikation' in R_m sinnvoll einsetzen.
Beispiel:

- *Welchen Rest lässt $101\cdot 52$ bei Division durch 6 ?*

  $$\textit{In } R_6: \quad \overline{101\cdot 52} = \overline{101}\odot\overline{52} = \overline{5}\odot\overline{4} = \overline{20} = \overline{2}$$

  Also lässt $101\cdot 52$ bei Division durch 6 den Rest 2.

- *Welchen Rest lässt $42\cdot 25-19\cdot 4-7$ bei Division durch 5?*

  $$\textit{In } R_5: \quad \overline{42\cdot 25-19\cdot 4-7} = \left(\overline{42}\odot\overline{25}\right)\oplus\left(\overline{-19}\odot\overline{4}\right)\oplus\overline{-7} = \left(\overline{2}\odot\overline{0}\right)\oplus\left(\overline{1}\odot\overline{4}\right)\oplus\overline{3} = \overline{7} = \overline{2}$$

  Also lässt $42\cdot 25-19\cdot 4-7$ bei Division durch 5 den Rest 2.

- *Welchen Rest lässt 24600382 bei Division durch 9 ?*

  $$24600382 = 2\cdot 10000000 + 4\cdot 1000000 + 6\cdot 100000 + 3\cdot 100 + 8\cdot 10 + 2$$

  In R_9 gilt

  $$\overline{10}=\overline{1},\quad \overline{100}=\overline{10}^2=\overline{1}^2=\overline{1},\quad \overline{1000}=\overline{10}^3=\overline{1}^3=\overline{1},\quad \overline{10000}=\overline{10}^4=\overline{1}^4=\overline{1}\qquad \textit{usw.}$$

  und folglich

  $$\begin{array}{lcl}
  \overline{24600382} & = & \overline{2\cdot 10000000 + 4\cdot 1000000 + 6\cdot 100000 + 3\cdot 100 + 8\cdot 10 + 2}\\
  & = & \left(\overline{2}\odot\overline{10000000}\right)\oplus\left(\overline{4}\odot\overline{1000000}\right)\oplus\left(\overline{6}\odot\overline{100000}\right)\oplus\left(\overline{3}\odot\overline{100}\right)\oplus\left(\overline{8}\odot\overline{10}\right)\oplus\overline{2}\\
  & = & \left(\overline{2}\odot\overline{1}\right)\oplus\left(\overline{4}\odot\overline{1}\right)\oplus\left(\overline{6}\odot\overline{1}\right)\oplus\left(\overline{3}\odot\overline{1}\right)\oplus\left(\overline{8}\odot\overline{1}\right)\oplus\overline{2}\\
  & = & \overline{25} \quad = \overline{7}
  \end{array}$$

  Also lässt 24600382 bei Division durch 9 den Rest 7.

- *Welchen Rest lässt* 24600382 *bei Division durch* 8 *?*

$$24600382 = 2 \cdot 10000000 + 4 \cdot 1000000 + 6 \cdot 100000 + 3 \cdot 100 + 8 \cdot 10 + 2$$

In R_8 *gilt*

$$\overline{10} = \overline{2}, \quad \overline{100} = \overline{10}^2 = \overline{2}^2 = \overline{4}, \quad \overline{1000} = \overline{10}^3 = \overline{2}^3 = \overline{0}, \quad \overline{10000} = \overline{10}^4 = \overline{0} \quad \overline{100000} = \overline{10}^5 = \overline{0} \qquad \textit{usw.}$$

und folglich

$$\begin{aligned}
\overline{24600382} &= \overline{2 \cdot 10000000 + 4 \cdot 1000000 + 6 \cdot 100000 + 3 \cdot 100 + 8 \cdot 10 + 2} \\
&= \left(\overline{2} \odot \overline{10000000}\right) \oplus \left(\overline{4} \odot \overline{1000000}\right) \oplus \left(\overline{6} \odot \overline{100000}\right) \oplus \left(\overline{3} \odot \overline{100}\right) \oplus \left(\overline{8} \odot \overline{10}\right) \oplus \overline{2} \\
&= \left(\overline{2} \odot \overline{0}\right) \oplus \left(\overline{4} \odot \overline{0}\right) \oplus \left(\overline{6} \odot \overline{0}\right) \oplus \left(\overline{3} \odot \overline{4}\right) \oplus \left(\overline{8} \odot \overline{2}\right) \oplus \overline{2} \\
&= \overline{30} \quad = \overline{6}
\end{aligned}$$

Also lässt 24600382 *bei Division durch* 8 *den Rest* 6*.*

- *Welchen Rest lässt* 24600382 *bei Division durch* 7 *?*

$$24600382 = 2 \cdot 10000000 + 4 \cdot 1000000 + 6 \cdot 100000 + 3 \cdot 100 + 8 \cdot 10 + 2$$

In R_7 *gilt*

$$\overline{10} = \overline{3}, \quad \overline{100} = \overline{2}, \quad \overline{1000} = \overline{6}, \quad \overline{10000} = \overline{4} \quad \overline{100000} = \overline{5} \quad \overline{1000000} = \overline{1} \quad \overline{10000000} = \overline{3}$$

und folglich

$$\begin{aligned}
\overline{24600382} &= \overline{2 \cdot 10000000 + 4 \cdot 1000000 + 6 \cdot 100000 + 3 \cdot 100 + 8 \cdot 10 + 2} \\
&= \left(\overline{2} \odot \overline{10000000}\right) \oplus \left(\overline{4} \odot \overline{1000000}\right) \oplus \left(\overline{6} \odot \overline{100000}\right) \oplus \left(\overline{3} \odot \overline{100}\right) \oplus \left(\overline{8} \odot \overline{10}\right) \oplus \overline{2} \\
&= \left(\overline{2} \odot \overline{3}\right) \oplus \left(\overline{4} \odot \overline{1}\right) \oplus \left(\overline{6} \odot \overline{5}\right) \oplus \left(\overline{3} \odot \overline{2}\right) \oplus \left(\overline{8} \odot \overline{3}\right) \oplus \overline{2} \\
&= \overline{72} \quad = \overline{2}
\end{aligned}$$

Also lässt 24600382 *bei Division durch* 7 *den Rest* 2*.*

- *Welche Endziffer hat* 3^{100} *?*

$$\textit{In } R_{10}: \quad \overline{3}^2 = \overline{9}, \quad \overline{3}^3 = \overline{7}, \quad \overline{3}^4 = \overline{1}$$

$$\Rightarrow \quad \overline{3}^8 = \left(\overline{3}^4\right)^2 = \overline{1}^2 = \overline{1}, \quad \overline{3}^{12} = \left(\overline{3}^4\right)^3 = \overline{1}^3 = \overline{1}, \quad \overline{3}^{16} = \overline{1}, \quad \ldots, \quad \overline{3}^{100} = \overline{1}$$

Also lässt 3^{100} *bei Division durch* 10 *den Rest* 1*, hat also die Endziffer* 1*.*

- *Welchen Rest lässt* 9^n $(n \in \mathbb{N})$ *bei Division durch* 8 *?*

$$\textit{In } R_8: \quad \overline{9} = \overline{1} \quad \Rightarrow \quad \overline{9}^n = \overline{1}^n = \overline{1} \textit{ für jedes } n \in \mathbb{N}$$

Also lässt 9^n *bei Division durch* 8 *immer den Rest* 1*.*

- *Welchen Rest lässt* 5^{100} *bei Division durch* 7 *?*

$$\textit{In } R_7: \quad \overline{5}^2 = \overline{4}, \quad \overline{5}^3 = \overline{6}, \quad \overline{5}^4 = \overline{2}, \quad \overline{5}^5 = \overline{3}, \quad \overline{5}^6 = \overline{1}$$

$$\Rightarrow \quad \overline{5}^{100} = \left(\overline{5}^6\right)^{16} \odot \overline{5}^4 = \overline{1} \odot \overline{2} = \overline{2}$$

Also lässt 5^{100} *bei Division durch* 7 *den Rest* 2*.*

- *Welchen Rest lässt* 6^{100} *bei Division durch* 48 *?*

$$\text{In } R_{48}: \quad \overline{6}^2 = \overline{36}, \quad \overline{6}^3 = \overline{24}, \quad \overline{6}^4 = \overline{0}, \quad \overline{6}^5 = \overline{0}, \quad \overline{6}^6 = \overline{0}, \quad \ldots, \quad \overline{6}^{100} = \overline{0}$$

Also ist 6^{100} *durch* 48 *teilbar.* (*Dies hätte man auch ohne das Rechnen mit Restklassen beantworten können, z.B. mit Hilfe der PFZ.*)

Folgerung 4.11. *(Teilbarkeitsregeln)*
Wir betrachten eine natürliche Zahl $a \in \mathbb{N}$ *und ihre Darstellung im Dezimalsystem:*

$$a = a_0 + a_1 \cdot 10 + a_2 \cdot 10^2 + \ldots + a_n \cdot 10^n = \sum_{k=0}^{n} a_k \cdot 10^k \quad \text{mit geeigneten 'Ziffern' } a_0, \ldots, a_n \in \{0, \ldots, 9\}$$

(i) In R_2 *gilt* $\overline{10} = \overline{0}$*. Daraus folgt* $\overline{a} = \overline{a_0}$*. Insbesondere ist* a *genau dann durch* 2 *teilbar, wenn* a_0 *durch* 2 *teilbar ist.*
Beispiel:

$$2805 = 2 \cdot 10^3 + 8 \cdot 10^2 + 0 \cdot 10 + 5 \quad \Rightarrow \quad \text{Zum Modul } m = 2: \ \overline{2805} = \overline{5} \neq \overline{0} \quad \Rightarrow \quad 2 \nmid 2805$$

$$376 = 3 \cdot 10^2 + 7 \cdot 10 + 6 \quad \Rightarrow \quad \text{Zum Modul } m = 2: \ \overline{376} = \overline{6} = \overline{0} \quad \Rightarrow \quad 2 \mid 376$$

(ii) In R_5 *gilt* $\overline{10} = \overline{0}$*. Daraus folgt* $\overline{a} = \overline{a_0}$*. Insbesondere ist* a *genau dann durch* 5 *teilbar, wenn* a_0 *durch* 5 *teilbar ist.*
Beispiel:

$$2805 = 2 \cdot 10^3 + 8 \cdot 10^2 + 0 \cdot 10 + 5 \quad \Rightarrow \quad \text{Zum Modul } m = 5: \ \overline{2805} = \overline{5} = \overline{0} \quad \Rightarrow \quad 5 \mid 2805$$

$$376 = 3 \cdot 10^2 + 7 \cdot 10 + 6 \quad \Rightarrow \quad \text{Zum Modul } m = 5: \ \overline{376} = \overline{6} \neq \overline{0} \quad \Rightarrow \quad 5 \nmid 376$$

(iii) In R_4 *gilt* $\overline{100} = \overline{0}$*. Daraus folgt* $\overline{a} = \overline{a_0 + a_1 \cdot 10}$*. Insbesondere ist* a *genau dann durch* 4 *teilbar, wenn* $a_0 + a_1 \cdot 10$ *durch* 4 *teilbar ist.*
Beispiel:

$$2805 = 2 \cdot 10^3 + 8 \cdot 10^2 + 0 \cdot 10 + 5 \quad \Rightarrow \quad \text{Zum Modul } m = 4: \ \overline{2805} = \overline{5} \neq \overline{0} \quad \Rightarrow \quad 4 \nmid 2805$$

$$376 = 3 \cdot 10^2 + 7 \cdot 10 + 6 \quad \Rightarrow \quad \text{Zum Modul } m = 4: \ \overline{376} = \overline{76} = \overline{0} \quad \Rightarrow \quad 4 \mid 76$$

(iv) In R_8 *gilt* $\overline{1000} = \overline{0}$*. Daraus folgt* $\overline{a} = \overline{a_0 + a_1 \cdot 10 + a_2 \cdot 10^2}$*. Insbesondere ist* a *genau dann durch* 8 *teilbar, wenn* $a_0 + a_1 \cdot 10 + a_2 \cdot 10^2$ *durch* 8 *teilbar ist.*
Beispiel:

$$2805 = 2 \cdot 10^3 + 8 \cdot 10^2 + 0 \cdot 10 + 5 \quad \Rightarrow \quad \text{Zum Modul } m = 8: \ \overline{2805} = \overline{805} \neq \overline{0} \quad \Rightarrow \quad 8 \nmid 2805$$

Für die dreistellige Zahl 376 *bringt die Anwendung der Teilbarkeitsregel durch* 8 *keine Vereinfachung.*

Im Folgenden betrachten wir die **Quersumme** $Q(a)$ *und die* **alternierende Quersumme** $Q_{alt}(a)$*, definiert durch:*

$$Q(a) \overset{def}{=} a_0 + a_1 + \ldots + a_n = \sum_{k=0}^{n} a_k \quad \text{und} \quad Q_{alt}(a) \overset{def}{=} a_0 - a_1 + a_2 - a_3 + \ldots + (-1)^n a_n = \sum_{k=0}^{n} (-1)^k \cdot a_k$$

(v) *In R_3 gilt $\overline{10} = \overline{1}$. Daraus folgt $\overline{a} = \overline{Q(a)}$. Insbesondere ist a genau dann durch 3 teilbar ist, wenn $Q(a)$ durch 3 teilbar ist.*
Beispiel:

$Q(2805) = 2+8+0+5 = 15 \quad \Rightarrow \quad$ *Zum Modul* $m = 3: \ \overline{2805} = \overline{15} = \overline{0} \quad \Rightarrow \quad 3 \mid 2805$

$Q(376) = 3+7+6 = 16 \quad \Rightarrow \quad$ *Zum Modul* $m = 3: \ \overline{376} = \overline{16} \neq \overline{0} \quad \Rightarrow \quad 3 \nmid 376$

(vi) *In R_9 gilt $\overline{10} = \overline{1}$. Daraus folgt $\overline{a} = \overline{Q(a)}$. Insbesondere ist a genau dann durch 9 teilbar ist, wenn $Q(a)$ durch 9 teilbar ist.*
Beispiel:

$Q(2805) = 2+8+0+5 = 15 \quad \Rightarrow \quad$ *Zum Modul* $m = 9: \ \overline{2805} = \overline{15} \neq \overline{0} \quad \Rightarrow \quad 9 \nmid 2805$

$Q(376) = 3+7+6 = 16 \quad \Rightarrow \quad$ *Zum Modul* $m = 9: \ \overline{376} = \overline{16} \neq \overline{0} \quad \Rightarrow \quad 9 \nmid 376$

(vii) *In R_{11} gilt $\overline{10} = \overline{-1}$. Daraus folgt $\overline{a} = \overline{Q_{alt}(a)}$. Insbesondere ist a genau dann durch 11 teilbar ist, wenn $Q_{alt}(a)$ durch 11 teilbar ist.*
Beispiel:

$Q_{alt}(2805) = -2+8-0+5 = 11 \quad \Rightarrow \quad$ *Zum Modul* $m = 11: \ \overline{2805} = \overline{11} = \overline{0} \quad \Rightarrow \quad 11 \mid 2805$

$Q_{alt}(376) = 3-7+6 = 2 \quad \Rightarrow \quad$ *Zum Modul* $m = 11: \ \overline{376} = \overline{2} \neq \overline{0} \quad \Rightarrow \quad 11 \nmid 376$

Invertierbarkeit bezüglich $\odot$

Definition 4.12. *(Invertierbare Restklassen)*
Sei $m \in \mathbb{N}$ gegeben. Eine Restklasse $\overline{a} \in R_m$ heißt **(bezüglich $\odot$) invertierbar**, *falls eine weitere Restklasse $\overline{b} \in R_m$ mit $\overline{a} \odot \overline{b} = \overline{1}$ existiert. In diesem Fall nennt man $\overline{b}$ das* **Inverse von $\overline{a}$ (bezüglich $\odot$)** *und schreibt auch $\overline{a}^{-1}$ für $\overline{b}$. Die Menge der invertierbaren Restklassen bezeichnet man mit*

$$R_m^* \overset{def}{=} \{\overline{a} \in R_m;\ a \text{ ist bzgl. } \odot \text{ invertierbar}\} \subseteq R_m$$

Beispiel.

- *In R_{10} gilt*

$$\begin{aligned} \overline{1} \odot \overline{1} = \overline{1} \quad &\Rightarrow \quad \overline{1}^{-1} = \overline{1} \\ \overline{3} \odot \overline{7} = \overline{1} \quad &\Rightarrow \quad \overline{3}^{-1} = \overline{7} \text{ und } \overline{7}^{-1} = \overline{3} \\ \overline{9} \odot \overline{9} = \overline{1} \quad &\Rightarrow \quad \overline{9}^{-1} = \overline{9} \end{aligned}$$

$\overline{0},\ \overline{2},\ \overline{4},\ \overline{5},\ \overline{6},\ \overline{8}$ *sind nicht bzgl. $\odot$ invertierbar*

$$\text{Also:} \quad R_{10}^* = \{\overline{1},\ \overline{3},\ \overline{5},\ \overline{7},\}$$

- *In R_{15} gilt*

$$\begin{aligned}
\overline{1} \odot \overline{1} = \overline{1} &\Rightarrow \overline{1}^{-1} = \overline{1} \\
\overline{2} \odot \overline{8} = \overline{1} &\Rightarrow \overline{2}^{-1} = \overline{8} \text{ und } \overline{8}^{-1} = \overline{2} \\
\overline{4} \odot \overline{4} = \overline{1} &\Rightarrow \overline{4}^{-1} = \overline{4} \\
\overline{7} \odot \overline{13} = \overline{1} &\Rightarrow \overline{7}^{-1} = \overline{13} \text{ und } \overline{13}^{-1} = \overline{7} \\
\overline{11} \odot \overline{11} = \overline{1} &\Rightarrow \overline{11}^{-1} = \overline{11} \\
\overline{14} \odot \overline{14} = \overline{1} &\Rightarrow \overline{14}^{-1} = \overline{14}
\end{aligned}$$

  $\overline{0}, \overline{3}, \overline{5}, \overline{6}, \overline{9}, \overline{10}, \overline{12}$ *sind nicht bzgl. $\odot$ invertierbar*

$$\text{Also: } R_{15}^* = \left\{\overline{1}, \overline{2}, \overline{4}, \overline{7}, \overline{8}, \overline{11}, \overline{13}, \overline{14}\right\}$$

- *In R_{17} gilt*

$$\begin{aligned}
\overline{1} \odot \overline{1} = \overline{1} &\Rightarrow \overline{1}^{-1} = \overline{1} \\
\overline{2} \odot \overline{9} = \overline{1} &\Rightarrow \overline{2}^{-1} = \overline{9} \text{ und } \overline{9}^{-1} = \overline{2} \\
\overline{3} \odot \overline{6} = \overline{1} &\Rightarrow \overline{3}^{-1} = \overline{6} \text{ und } \overline{6}^{-1} = \overline{3} \\
\overline{4} \odot \overline{13} = \overline{1} &\Rightarrow \overline{4}^{-1} = \overline{13} \text{ und } \overline{13}^{-1} = \overline{4} \\
\overline{5} \odot \overline{7} = \overline{1} &\Rightarrow \overline{5}^{-1} = \overline{7} \text{ und } \overline{7}^{-1} = \overline{5} \\
\overline{8} \odot \overline{15} = \overline{1} &\Rightarrow \overline{8}^{-1} = \overline{15} \text{ und } \overline{15}^{-1} = \overline{8} \\
\overline{10} \odot \overline{12} = \overline{1} &\Rightarrow \overline{10}^{-1} = \overline{12} \text{ und } \overline{12}^{-1} = \overline{10} \\
\overline{11} \odot \overline{14} = \overline{1} &\Rightarrow \overline{11}^{-1} = \overline{14} \text{ und } \overline{14}^{-1} = \overline{11} \\
\overline{16} \odot \overline{16} = \overline{1} &\Rightarrow \overline{16}^{-1} = \overline{16}
\end{aligned}$$

  $\overline{0}$ *ist nicht bzgl. $\odot$ invertierbar*

$$\text{Also: } R_{17}^* = \left\{\overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}, \overline{6}, \overline{7}, \overline{8}, \overline{9}, \overline{10}, \overline{11}, \overline{12}, \overline{13}, \overline{14}, \overline{15}, \overline{16}\right\}$$

Bemerkung 4.13. *(Eigenschaften invertierbarer Restklassen)*
Sei $m \in \mathbb{N}$ mit $m \geq 2$ gegeben.

(a) Bzgl. $\odot$ invertierbare Elemente von R_m sind niemals Nullteiler. (*Anders formuliert: Nullteiler sind nicht invertierbar.*)
  Beispiel: *In R_{12} gilt*

$$\overline{2} \odot \overline{6} = \overline{0}, \quad \overline{3} \odot \overline{4} = \overline{0}, \quad \overline{8} \odot \overline{9} = \overline{0}, \quad \overline{10} \odot \overline{6} = \overline{0}$$

  Also sind $\overline{2}, \overline{3}, \overline{4}, \overline{6}, \overline{8}, \overline{9}, \overline{10}$ Nullteiler in R_{12} und damit nicht invertierbar bzgl. $\odot$.

(b) $\overline{0}$ ist nicht invertierbar.

(c) Inverse Elemente zu $\overline{a} \in R_m^*$ sind stets eindeutig bestimmt. (*Ein Element aus R_m hat also entweder kein oder genau ein Inverses.*)

(d) $\overline{1}$ und $\overline{m-1}$ sind stets invertierbar mit $\overline{1}^{-1} = \overline{1}$ und $\overline{m-1}^{-1} = \overline{m-1}$.

(e) Falls $\overline{a} \in R_m^*$ ist auch $\overline{a}^{-1} \in R_m^*$ und es gilt $\left(\overline{a}^{-1}\right)^{-1} = \overline{a}$.

(f) Für $\overline{a}, \overline{b} \in R_m^*$ ist auch $\overline{a} \odot \overline{b} \in R_m^*$ mit

$$\left(\overline{a} \odot \overline{b}\right)^{-1} = \overline{a}^{-1} \odot \overline{b}^{-1}$$

Beispiel: In R_{20} gilt

$$\overline{3}^{-1} = \overline{7} \quad \textit{und} \quad \overline{11}^{-1} = \overline{11}$$

Weiterhin ist

$$\left(\overline{3} \odot \overline{11}\right)^{-1} = \overline{13}^{-1} = \overline{17} \quad \textit{und auch} \quad \overline{3}^{-1} \odot \overline{11}^{-1} = \overline{7} \odot \overline{11} = \overline{17}$$

Satz 4.14. *(Charakterisierung invertierbarer Restklassen und Bestimmung von Inversen) Sei $m \in \mathbb{N}$ gegeben und $a \in \mathbb{Z}$. Dann ist $\overline{a} \in R_m$ genau dann bezüglich $\odot$ invertierbar, wenn a und m teilerfremd sind. In diesem Fall kann man Zahlen $u, v \in \mathbb{Z}$ mit $1 = u \cdot a + v \cdot m$ bestimmen (vergleiche 3.10). Es gilt dann stets $\overline{a}^{-1} = \overline{u}$. (Insbesondere ist u modulo m eindeutig bestimmt.)*

Beispiel.

- *Es ist zu prüfen, ob $\overline{10}$ in R_{27} invertierbar ist. Falls dies der Fall ist, soll auch das Inverse $\overline{10}^{-1}$ bestimmt werden:*

  $$ggT(10, 27) = 1 \quad \Rightarrow \quad \overline{10} \textit{ ist in } R_{27} \textit{ invertierbar}$$

  Mit dem erweiterten Euklidischen Algorithmus berechnet man: $1 = 3 \cdot 27 - 8 \cdot 10$

  $$\Rightarrow \quad \overline{1} = \overline{3 \cdot 27 - 8 \cdot 10} = \left(\overline{3} \odot \overline{27}\right) \oplus \left(\overline{-8} \odot \overline{10}\right) = \left(\overline{3} \odot \overline{0}\right) \oplus \left(\overline{-8} \odot \overline{10}\right) = \overline{-8} \odot \overline{10}$$

  Also ist $\overline{10}^{-1} = \overline{-8} = \overline{19}$ in R_{27}.

  Alternativ gilt (beispielsweise) auch: $1 = -37 \cdot 27 + 100 \cdot 10$

  $$\Rightarrow \quad \overline{1} = \overline{-37 \cdot 27 + 100 \cdot 10} = \left(\overline{-37} \odot \overline{27}\right) \oplus \left(\overline{100} \odot \overline{10}\right) = \left(\overline{-37} \odot \overline{0}\right) \oplus \left(\overline{100} \odot \overline{10}\right) = \overline{100} \odot \overline{10}$$

  Auch hierbei ergibt sich $\overline{10}^{-1} = \overline{100} = \overline{19}$ in R_{27}.

- *Es ist zu prüfen, ob $\overline{25}$ in R_{52} invertierbar ist. Falls dies der Fall ist, soll auch das Inverse $\overline{25}^{-1}$ bestimmt werden:*

  $$ggT(25, 52) = 1 \quad \Rightarrow \quad \overline{25} \textit{ ist in } R_{52} \textit{ invertierbar}$$

  Mit dem erweiterten Euklidischen Algorithmus berechnet man: $1 = 25 \cdot 25 - 12 \cdot 52$

  $$\Rightarrow \quad \overline{1} = \overline{25 \cdot 25 - 12 \cdot 52} = \left(\overline{25} \odot \overline{25}\right) \oplus \left(\overline{-12} \odot \overline{52}\right) = \left(\overline{25} \odot \overline{25}\right) \oplus \left(\overline{-12} \odot \overline{0}\right) = \overline{25} \odot \overline{25}$$

  Also ist $\overline{25}^{-1} = \overline{25}$ in R_{52}.

- *Es ist zu prüfen, ob $\overline{16}$ in R_{52} invertierbar ist. Falls dies der Fall ist, soll auch das Inverse $\overline{16}^{-1}$ bestimmt werden:*

  $$ggT(16, 52) \neq 1 \quad \Rightarrow \quad \overline{16} \textit{ ist in } R_{52} \textit{ nicht invertierbar}$$

- *Wir können nun auch (relativ schnell) R_m^* angeben, ohne die Inversen zu berechnen. Beispielsweise ist:*

$$\begin{aligned} R_6^* &= \{\overline{1},\ \overline{5}\} \\ R_{11}^* &= \{\overline{1},\ \overline{2},\ \overline{3},\ \overline{4},\ \overline{5},\ \overline{6},\ \overline{7},\ \overline{8},\ \overline{9},\ \overline{10}\} \\ R_{18}^* &= \{\overline{1},\ \overline{5},\ \overline{7},\ \overline{11},\ \overline{13},\ \overline{17}\} \\ R_{25}^* &= \{\overline{1},\ \overline{2},\ \overline{3},\ \overline{4},\ \overline{6},\ \overline{7},\ \overline{8},\ \overline{9},\ \overline{11},\ \overline{12},\ \overline{13},\ \overline{14},\ \overline{16},\ \overline{17},\ \overline{18},\ \overline{19},\ \overline{21},\ \overline{22},\ \overline{23},\ \overline{24}\} \end{aligned}$$

Folgerung 4.15. *(Invertierbarkeit in R_p)*
Ist $p \in \mathbb{P}$, so sind alle Elemente $\overline{a} \in R_p \setminus \{\overline{0}\}$ bezüglich $\odot$ invertierbar.

$$\textit{Also:}\quad R_p^* = \{\overline{1},\ \overline{2},\ \ldots,\ \overline{p-1}\}$$

Definition 4.16. *(Eulersche φ-Funktion)*
Die **Eulersche φ-Funktion** *ist definiert duch*

$$\varphi : \mathbb{N} \to \mathbb{N},\ \varphi(m) \overset{def}{=} |R_m^*|\ \ (= \textit{Anzahl der invertierbaren Elemente in } R_m)$$

Beispiel.
Aus dem Beispiel nach Definition 4.12 *ergibt sich*

$$\varphi(10) = 4, \quad \varphi(15) = 8, \quad \varphi(17) = 16$$

Aus dem Beispiel nach Satz 4.14 *ergibt sich*

$$\varphi(6) = 2, \quad \varphi(11) = 10, \quad \varphi(18) = 6, \quad \varphi(25) = 20$$

Bemerkung 4.17. *(Berechnung von $\varphi(m)$)*
Nach 4.14 *gilt $\varphi(m) = |\{a \in \{1,\ldots,m\};\ ggT(a,m) = 1\}|$ für alle $m \in \mathbb{N}$. Es folgt:*

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

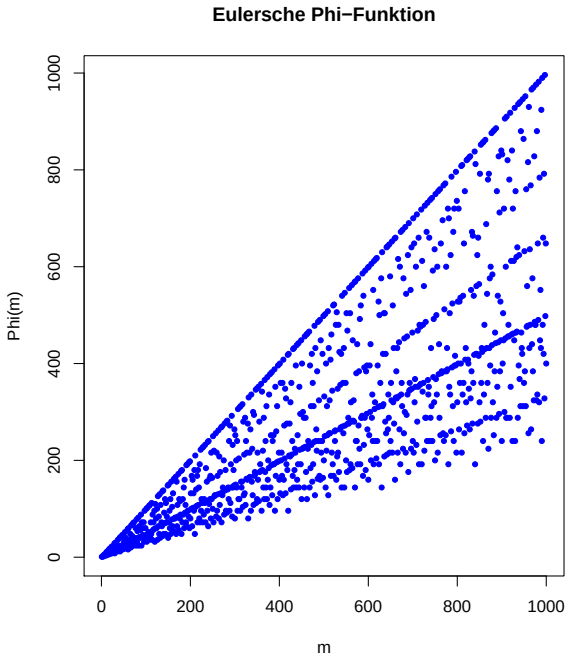
Weiterhin gilt für $m_1, m_2 \in \mathbb{N}$ stets:

$$m_1, m_2 \text{ teilerfremd} \quad \Rightarrow \quad \varphi(m_1 \cdot m_2) = \varphi(m_1) \cdot \varphi(m_2)$$

Damit kann man $\varphi(m)$ stets aus der (kanonischen) PFZ $m = \prod_{j=1}^{k} {p_j}^{e_j}$ von m berechnen. Es gilt:

$$\varphi(m) = \prod_{j=1}^{k} {p_j}^{e_j - 1} \cdot (p_j - 1) = m \prod_{j=1}^{k} \left(1 - \frac{1}{p_j}\right)$$

Trägt man die Punkte $(m, \varphi(m))$ für $m = 1,\ldots,1000$ in ein Koordinatensystem ein, so erhält man:



Beispiel.

- $\varphi(13) = 12, \quad \varphi(47) = 46, \quad \varphi(101) = 100$
- $$\begin{array}{rcccccl} \varphi(64) & = & \varphi(2^6) & = & 2^6 - 2^5 & = & 2^5 \cdot (2-1) & = & 32 \\ \varphi(625) & = & \varphi(5^4) & = & 5^4 - 5^3 & = & 5^3 \cdot (5-1) & = & 500 \\ \varphi(49) & = & \varphi(7^2) & = & 7^2 - 7^1 & = & 7^1 \cdot (7-1) & = & 42 \end{array}$$
- $\varphi(1001) = \varphi(7 \cdot 11 \cdot 13) = \varphi(7) \cdot \varphi(11) \cdot \varphi(13) = 6 \cdot 10 \cdot 12 = 720$
- $\varphi(1000) = \varphi\left(2^3 \cdot 5^3\right) = \varphi\left(2^3\right) \cdot \varphi\left(5^3\right) = \left(2^3 - 2^2\right) \cdot \left(5^3 - 5^2\right) = 4 \cdot 100 = 400$
- $$\begin{aligned} \varphi(676269) &= \varphi\left(3^5 \cdot 11^2 \cdot 23\right) \\ &= \varphi\left(3^5\right) \cdot \varphi\left(11^2\right) \cdot \varphi(23) \\ &= \left(3^5 - 3^4\right) \cdot \left(11^2 - 11\right) \cdot 22 \\ &= 162 \cdot 110 \cdot 22 \\ &= 392040 \end{aligned}$$

5 Gruppen

Definition, Beispiele und erste Eigenschaften

Definition 5.1. *(Gruppen)*

(a) Ist $G \neq \varnothing$ eine beliebige Menge, so nennt man eine Abbildung

$$* : G \times G \to G,\ (x, y) \mapsto x * y$$

eine **Verknüpfung auf** G. *(Einfacher gesagt: Für beliebige Elemente x, y von G ist $x * y$ ebenfalls ein Element von G.)*
Beispiele:

- *Addition $+$, Subtraktion $-$ und Multiplikation $\cdot$ sind Verknüpfungen auf $\mathbb{Z}$.*
- *Weitere Verknüpfungen auf $\mathbb{Z}$ sind zum Beispiel*

$$(x, y) \mapsto \max(x, y) \quad \textit{und} \quad (x, y) \mapsto \min(x, y)$$

- *Die Division $:$ ist keine Verknüpfung auf $\mathbb{Z}$, denn für $x, y \in \mathbb{Z}$ kann $x : y \notin \mathbb{Z}$ sein.*
- *Die Division $:$ ist auch keine Verknüpfung auf $\mathbb{Q}$, denn für $y = 0$ ist $x : y$ nicht definiert.*
- *Die Division $:$ ist aber eine Verknüpfung auf $\mathbb{Q} \setminus \{0\}$.*
- *Auf der Menge der Restklassen R_m ($m \in \mathbb{N}$ fest) kennen wir die Verknüpfungen $\oplus$ und $\odot$.*
- *$\odot$ ist auch eine Verknüpfung auf R_m^* (vergleiche 4.13 (f)).*
- *Auf $\mathbb{Z}$ wird durch*

$$x * y \overset{def}{=} x + y + 2 \quad (x, y \in \mathbb{Z})$$

eine (neue) Veknüpfung $*$ definiert. Beispielsweise gilt

$$2 * 3 = 7, \quad (-4) * 15 = 13, \quad 0 * 0 = 2, \quad (-8) * (-2) = -8$$

- *Auf $\mathbb{Z}$ wird durch*

$$x \lhd y \overset{def}{=} x \quad (x, y \in \mathbb{Z})$$

eine (neue) Veknüpfung $\lhd$ definiert. Beispielsweise gilt

$$2 \lhd 3 = 2, \quad (-4) \lhd 15 = -4, \quad 0 \lhd 0 = 0, \quad (-8) \lhd (-2) = -8$$

(b) Ist $G \neq \varnothing$ eine beliebige Menge und $*$ eine Verknüpfung auf G, so nennt man $(G, *)$ eine **Gruppe**, *wenn die folgenden Bedingungen gelten:*

(i) **Assoziativgesetz**: *Für alle $x, y, z \in G$ gilt $(x * y) * z = x * (y * z)$.*

(ii) **Existenz eines Neutralen Elements:** *Es existiert ein Element $e \in G$ mit $x * e = e * x = x$ für alle $x \in G$.*

(*Falls $*$ eine Addition $+$ ist, schreibt man meist 0 statt e. Falls $*$ eine Multiplikation $\cdot$ ist, schreibt man meist 1 statt e.*)

(iii) **Existenz Inverser Elemente:** *Zu jedem Element $x \in G$ existiert ein weiteres Element $Inv(x) \in G$ mit $x * Inv(x) = Inv(x) * x = e$.*
(*Falls $*$ eine Addition $+$ ist, schreibt man meist $-x$ statt $Inv(x)$. Falls $*$ eine Multiplikation $\cdot$ ist, schreibt man meist x^{-1} oder $\frac{1}{x}$ statt $Inv(x)$.*)

Eine Gruppe $(G, *)$ heißt **kommutativ (bzw. abelsch)**, *wenn zusätzlich gilt:*

(iv) **Kommutativgesetz**: *Für alle $x, y \in G$ gilt $x * y = y * x$*

Beispiele:

- $(\mathbb{Z}, +)$ *und* $(\mathbb{Q}, +)$ *sind kommutative Gruppen.*
- $(\mathbb{Z}, -)$ *ist keine Gruppe (das Assoziativgesetz gilt nicht und es gibt auch kein Neutrales Element).*
- $(\mathbb{Z}, \max)$ *ist keine Gruppe (es gibt kein Neutrales Element).*
- $(\mathbb{Q}, \cdot)$ *ist keine Gruppe (Neutrales ist 1, aber 0 ist nicht invertierbar).*
- $(\mathbb{Q} \setminus \{0\}, \cdot)$ *ist eine kommutative Gruppe.*
- $(R_m, \oplus)$ *ist eine kommutative Gruppe.*
- $(R_m, \odot)$ *ist keine Gruppe (nicht alle Elemente haben ein Inverses Element), aber $(R_m^*, \odot)$ ist eine kommutative Gruppe.*
- $(\mathbb{Z}, *)$ *mit der durch Verknüpfung $x * y \overset{def}{=} x + y + 2$ $(x, y \in \mathbb{Z})$ definierten Verknüpfung $*$ ist eine kommutative Gruppe (Assoziativ- und Kommutativgesetz können nachgeprüft werden, Neutrales Element ist $e = -2$ und für alle $x \in \mathbb{Z}$ gilt $Inv(x) = x - 4$).*

Bemerkung 5.2. *(Eigenschaften von Gruppen)*
Sei nun $(G, *)$ eine beliebige Gruppe. Dann gilt:

(a) Es gibt genau ein Neutrales Element in G.

(b) Es gilt die **Kürzungsregel**: *Für alle $x, y, z \in G$ gilt die Äquivalenz*

$$x * z = y * z \quad \Leftrightarrow \quad x = y \quad \Leftrightarrow \quad z * x = z * y$$

(c) Jedes Element von G hat genau ein Inverses Element.

(d) Für alle $x, y \in G$ gilt

$$Inv(Inv(x)) = x \quad und \quad Inv(x * y) = Inv(y) * Inv(x)$$

Bemerkung 5.3. *(Iterierte Anwendung der Veknüpfung in der Gruppe)*
Ist $(G, *)$ eine Gruppe und $x \in G$, so definiert man $x^0 \overset{def}{=} e$ und

$$x_{(n)} \overset{def}{=} \underbrace{x * x * \ldots * x}_{n\text{-mal}} \quad und \quad x_{(-n)} \overset{def}{=} \underbrace{Inv(x) * Inv(x) * \ldots * Inv(x)}_{n\text{-mal}} \qquad (für\ n \in \mathbb{N})$$

Beispiele:

- *In der Gruppe* $(\mathbb{Z},+)$ *ist*

  $5_{(4)} = 5+5+5+5 = 20, \quad 6_{(-3)} = Inv(6)+Inv(6)+Inv(6) = (-6)+(-6)+(-6) = -18,$

  $(-2)_{(-7)} = Inv(-2)+Inv(-2)+Inv(-2)+Inv(-2)+Inv(-2)+Inv(-2)+Inv(-2) = 2+2+2+2+2+2+2 = 14$

- *In der Gruppe* $(\mathbb{Q}\setminus\{0\},\cdot)$ *ist*

  $$\left(-\frac{5}{3}\right)_{(-3)} = Inv\left(-\frac{5}{3}\right)\cdot Inv\left(-\frac{5}{3}\right)\cdot Inv\left(-\frac{5}{3}\right) = \left(-\frac{3}{5}\right)\cdot\left(-\frac{3}{5}\right)\cdot\left(-\frac{3}{5}\right) = -\frac{27}{125}$$

- *In der Gruppe* $(R_{10},\oplus)$ *ist*

  $\overline{7}_{(4)} = \overline{7}\oplus\overline{7}\oplus\overline{7}\oplus\overline{7} = \overline{8}$ *und* $\overline{6}_{(-5)} = Inv(\overline{6})\oplus Inv(\overline{6})\oplus Inv(\overline{6})\oplus Inv(\overline{6})\oplus Inv(\overline{6}) = \overline{4}\oplus\overline{4}\oplus\overline{4}\oplus\overline{4}\oplus\overline{4} = \overline{0}$

- *In der Gruppe* $(R_7^*,\odot)$ *ist*

  $$\overline{4}_{(3)} = \overline{4}\odot\overline{4}\odot\overline{4} = \overline{1} \quad \text{und} \quad \overline{3}_{(-2)} = Inv(\overline{3})\odot Inv(\overline{3}) = \overline{5}\odot\overline{5} = \overline{4}$$

Für alle $x,y\in G$ *und alle* $n,m\in\mathbb{Z}$ *gelten nun die als 'Potenzgesetze' bekannten Rechenregeln:*

$$x_{(1)} = x, \quad x_{(-1)} = Inv(x), \quad e_{(n)} = e, \quad x_{(n)} * x_{(m)} = x_{(n+m)}, \quad \left(x_{(n)}\right)_{(m)} = x_{(n\cdot m)}$$

und falls $(G,*)$ *kommutativ ist, auch:* $x_{(n)} * y_{(n)} = (x*y)_{(n)}$

Beispiele: *In einer beliebigen Gruppe* $(G,*)$ *gilt für alle* $x,y\in G$*:*

- $$\begin{aligned} x_{(7)} * x_{(-3)} &= (x*x*x*x*x*x*x)*(Inv(x)*Inv(x)*Inv(x)) \\ &= x*x*x*x \\ &= x_{(4)} \end{aligned}$$

- $$\begin{aligned} \left(x_{(-2)}\right)_{(3)} &= x_{(-2)}*x_{(-2)}*x_{(-2)} \\ &= (Inv(x)*Inv(x))*(Inv(x)*Inv(x))*(Inv(x)*Inv(x)) \\ &= x_{(-6)} \end{aligned}$$

- *Falls* $(G,*)$ *kommutativ ist, gilt auch:*

  $$\begin{aligned} \left(x_{(4)}\right)*\left(y_{(4)}\right) &= (x*x*x*x)*(y*y*y*y) \\ &\overset{(KG)}{=} (x*y)*(x*y)*(x*y)*(x*y) \\ &= (x*y)_{(4)} \end{aligned}$$

- *Falls* $*$ *eine Addition* $+$ *ist, schreibt man meist* $n\cdot x$ *statt* $x_{(n)}$*. Falls* $*$ *eine Multiplikation* $\cdot$ *ist, schreibt man meist* x^n *statt* $x_{(n)}$*. Angewendet auf bestimmte (kommutative)*

Gruppen ergibt sich beispielsweise (für $x, y \in G$ und $n, m \in \mathbb{Z}$):

	$x_{(1)} = x$	$x_{(-1)} = Inv(x)$	$e_{(n)} = e$	$x_{(n)} * x_{(m)} = x_{(n+m)}$	$\left(x_{(n)}\right)_{(m)} = x_{(n\cdot m)}$	$x_{(n)} * y_{(n)} = (x * y)_{(n)}$
$(\mathbb{Z}, +)$	$1 \cdot x = x$	$(-1) \cdot x = -x$	$n \cdot 0 = 0$	$(n \cdot x) + (m \cdot x) = (n + m) \cdot x$	$m \cdot (n \cdot x) = (n \cdot m) \cdot x$	$(n \cdot x) + (n \cdot y) = n \cdot (x + y)$
$(\mathbb{Q}^*, \cdot)$	$x^1 = x$	$x^{(-1)} = \frac{1}{x}$	$1^n = 1$	$x^n \cdot x^m = x^{(n+m)}$	$(x^n)^m = x^{(n\cdot m)}$	$x^n \cdot y^n = (x \cdot y)^n$
$(R_m^*, \odot)$	$\overline{x}^1 = \overline{x}$	$\overline{x}^{(-1)} = \overline{x}^{-1}$	$\overline{1}^n = \overline{1}$	$\overline{x}^n \odot \overline{x}^m = \overline{x}^{(n+m)}$	$(\overline{x}^n)^m = \overline{x}^{(n\cdot m)}$	$\overline{x}^n \odot \overline{y}^n = (\overline{x} \odot \overline{y})^n$

Definition 5.4. *(Gruppenordnung und Elementordnung)*

(a) Für eine Gruppe $(G, *)$ nennt man $|G| \in \mathbb{N} \cup \{\infty\}$ die **Ordnung der Gruppe** *G. Man nennt die Gruppe $(G, *)$* **endlich**, *falls $|G| \in \mathbb{N}$ ist.*

(b) Ist $(G, *)$ eine endliche Gruppe, so existiert zu jedem $x \in G$ ein $n \in \mathbb{N}$ mit $x_{(m)} = e$. Das kleinstmögliche solche m bezeichnet man als **Ordnung** *von x:*

$$ord\ (x) \overset{def}{=} \min\left\{m \in \mathbb{N};\ x_{(m)} = e\right\} \in \mathbb{N}$$

Beispiel.

- *In $(\mathbb{Z}, +)$ gilt $|\mathbb{Z}| = \infty$.*
- *In $(R_6, \oplus)$ gilt $|R_6| = 6$. Hier ist $e = \overline{0}$. Wir bestimmen die Ordnungen der einzelnen Elemente:*

  –) $\overline{1} \neq \overline{0}$, $\overline{1}_{(2)} = \overline{2} \neq \overline{0}$, $\overline{1}_{(3)} = \overline{3} \neq \overline{0}$, $\overline{1}_{(4)} = \overline{4} \neq \overline{0}$, $\overline{1}_{(5)} = \overline{5} \neq \overline{0}$, $\boxed{\overline{1}_{(6)} = \overline{6} = \overline{0}}$

  $\Rightarrow$ $ord\ \left(\overline{1}\right) = 6$

  –) $\overline{2} \neq \overline{0}$, $\overline{2}_{(2)} = \overline{4} \neq \overline{0}$, $\boxed{\overline{2}_{(3)} = \overline{6} = \overline{0}}$

  $\Rightarrow$ $ord\ \left(\overline{2}\right) = 3$

  –) $\overline{3} \neq \overline{0}$, $\boxed{\overline{3}_{(2)} = \overline{6} = \overline{0}}$

  $\Rightarrow$ $ord\ \left(\overline{3}\right) = 2$

  –) $\overline{4} \neq \overline{0}$, $\overline{4}_{(2)} = \overline{8} \neq \overline{0}$, $\boxed{\overline{4}_{(3)} = \overline{12} = \overline{0}}$

  $\Rightarrow$ $ord\ \left(\overline{4}\right) = 3$

  –) $\overline{5} \neq \overline{0}$, $\overline{5}_{(2)} = \overline{10} \neq \overline{0}$, $\overline{5}_{(3)} = \overline{15} \neq \overline{0}$, $\overline{5}_{(4)} = \overline{20} \neq \overline{0}$ $\overline{5}_{(5)} = \overline{25} \neq \overline{0}$, $\boxed{\overline{5}_{(6)} = \overline{30} = \overline{0}}$

  $\Rightarrow$ $ord\ \left(\overline{5}\right) = 6$

  –) $\boxed{\overline{0} = \overline{0}}$

  $\Rightarrow$ $ord\ \left(\overline{0}\right) = 1$

- *In* $(R_9^*, \odot)$ *gilt* $|R_9^*| = \varphi(9) = 6$. *Hier ist* $e = \overline{1}$. *Wir bestimmen die Ordnungen der einzelnen Elemente:*

  –) $\boxed{\overline{1} = \overline{1}}$

  $\Rightarrow$ *ord* $(\overline{1}) = 1$

  –) $\overline{2} \neq \overline{1}, \quad \overline{2}_{(2)} = \overline{4} \neq \overline{1}, \quad \overline{2}_{(3)} = \overline{8} \neq \overline{1}, \quad \overline{2}_{(4)} = \overline{7} \neq \overline{1}, \quad \overline{2}_{(5)} = \overline{5} \neq \overline{1}, \quad \boxed{\overline{2}_{(6)} = \overline{1}}$

  $\Rightarrow$ *ord* $(\overline{2}) = 6$

  –) $\overline{4} \neq \overline{1}, \quad \overline{4}_{(2)} = \overline{7} \neq \overline{1}, \quad \boxed{\overline{4}_{(3)} = \overline{1}}$

  $\Rightarrow$ *ord* $(\overline{4}) = 3$

  –) $\overline{5} \neq \overline{1}, \quad \overline{5}_{(2)} = \overline{7} \neq \overline{1}, \quad \overline{5}_{(3)} = \overline{8} \neq \overline{1}, \quad \overline{5}_{(4)} = \overline{4} \neq \overline{1}, \quad \overline{5}_{(5)} = \overline{2} \neq \overline{1}, \quad \boxed{\overline{5}_{(6)} = \overline{1}}$

  $\Rightarrow$ *ord* $(\overline{5}) = 6$

  –) $\overline{7} \neq \overline{1}, \quad \overline{7}_{(2)} = \overline{4} \neq \overline{1}, \quad \boxed{\overline{7}_{(3)} = \overline{1}}$

  $\Rightarrow$ *ord* $(\overline{7}) = 3$

  –) $\overline{8} \neq \overline{1}, \quad \boxed{\overline{8}_{(2)} = \overline{1}}$

  $\Rightarrow$ *ord* $(\overline{8}) = 2$

Satz 5.5. *(Zusammenhang zwischen Elementordnung und Gruppenordnung)*
Gegeben sei eine endliche Gruppe $|G|$. *Dann gilt ord* $(x) \mid |G|$ *für alle* $x \in G$. *Daraus folgt, dass für alle* $x \in G$ *stets* $x_{(|G|)} = e$ *gilt.*

Folgerung 5.6. *(Satz von Euler und Kleiner Satz von Fermat)*

(a) Für alle $m \in \mathbb{N}$ *und alle* $a \in \mathbb{Z} \setminus \{0\}$ *mit* $ggT(a, m) = 1$ *gilt:* $\quad a^{\varphi(m)} \equiv 1 \mod m$

Beispiele:

- *Es gilt* $\varphi(20) = 8$. *Daher folgt:* $a^8 \equiv 1 \mod 20$, *falls* $ggT(a, 20) = 1$, *also beispielsweise*

  $$3^8 \equiv 7^8 \equiv 9^8 \equiv 11^8 \equiv 13^8 \equiv \ldots \equiv 1 \mod 20$$

  Die Zahlen $3^8, 7^8, 9^8, 11^8, 13^8 \ldots$ *lassen alle den Rest* 1 *bei Division durch* 20.

- *Es gilt* $\varphi(8) = 4$. *Daher folgt:* $a^4 \equiv 1 \mod 8$, *falls* $ggT(a, 8) = 1$, *also falls a ungerade ist. Vierte Potenzen ungerader Zahlen lassen stets den Rest* 1 *bei Division durch* 8.

- *Es gilt* $\varphi(125) = 100$. *Daher folgt:* $a^{100} \equiv 1 \mod 125$, *falls* $ggT(a, 125) = 1$, *also falls a kein Vielfaches von* 5 *ist.*

  Also: Falls $5 \nmid a$, *hat* a^{100} *Rest* 1 *bei Division durch* 125.

(b) Für alle $p \in \mathbb{P}$ *und alle* $a \in \mathbb{Z}$ *gilt:* $\quad a^p \equiv a \mod p$
Ist $a \notin V(p)$, *so gilt auch:* $\quad a^{p-1} \equiv 1 \mod p$

Beispiele:

- $a^3 \equiv a \mod 3 \Rightarrow a^3$ *und a lassen stets denselben Rest bei Division durch* 3.

- $a^{11} \equiv a \mod 11 \Rightarrow a^{11}$ *und a lassen stets denselben Rest bei Division durch* 11.

(Ausblick)

Die bisher erhaltenen (und natürlich auch weitere) Ergebnisse aus der Theorie der Gruppen lassen sich auf alle Gruppen übertragen. Das bedeutet: Wann immer man erkannt hat, dass eine Verknüpfung auf einer Menge die Gruppenaxiome erfüllt, kann man die im allgemeinen Rahmen bewiesenen Aussagen (z.B. Bemerkung 5.2 und -bei endlichen Gruppen- Satz 5.5) anwenden.

Interessante Beispiele für (endliche, nichtkommutative) Gruppen stellen die sogenannten **Permutationsgruppen** S_n dar: Ein Element von S_n beschreibt eine bestimmte Vertauschung(Umsortierung) von n gegebenen Objekten, die Verknüpfung besteht in der Hintereinanderausführung zweier solcher Vertauschungen.
Als Untergruppen von Permutationsgruppen findet man die sogenannten **Symmetriegruppen** wieder, die die Möglichkeiten beschreiben, einen regelmäßigen Körper (z.B. Würfel oder Ikosaeder) zu drehen.

Gruppenstrukturen kommen in weiteren zahlreichen Bereichen der Mathematik vor. Betrachtet man Mengen, die mehr als eine Verknüpfung tragen, so findet man ein vergleichbares Konzept beispielsweise in der Theorie der **Ringe** und **Körper**.