Elementare Zahlentheorie

Florian Kainrath

SS 20

Hinweise (auf sicherlich vorhandene) (Tipp-)Fehler sind willkommen und erwünscht.

Wir verwenden die üblichen Bezeichnungen der Mengenlehre:

- Für zwei Mengen A und B schreiben wir $A \subset B$, falls A eine Teilmenge von B ist. $A \subsetneq B$ bedeutet $A \subset B$ und $A \neq B$.
- Ist A eine Menge so sei $\#A \in \{0, 1, 2, \ldots\} \cup \{\infty\}$ ihre Anzahl.

Literatur:

P. Bundschuh, *Einführung in die Zahlentheorie*, 5. Auflage, Springer, 2002

D.M. Burton, H. Dalkowski, *Handbuch der elementaren Zahlentheorie*, Heldermann, 2005

R. Remmert, P. Ullrich, *Elementare Zahlentheorie*, Birkhäuser, 1987

Inhaltsverzeichnis

1. Teilbarkeit

1.1. Die ganzen Zahlen.

1.1.1. Wir setzen

- $\mathbb{N} = \{0, 1, 2, 3, \ldots\}$ die Menge der natürlichen Zahlen (inklusive 0)
- $\mathbb{N}^+ = \mathbb{N} \setminus \{0\}$ die Menge der strikt positiven natürlichen Zahlen.
- $\mathbb{Z} = \mathbb{N} \cup (-\mathbb{N}) = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$ die Menge aller ganzen Zahlen.

Dann gilt

$$\mathbb{N}^+ \subset \mathbb{N} \subset \mathbb{Z} \quad .$$

Vorsicht: In manchen Büchern wird

$$\mathbb{N} = \{1, 2, 3, 4, \ldots\}, \quad , \mathbb{N}_0 = \{0, 1, 2, 3, 4, \ldots\}$$

gesetzt.

1.1.2. Ganze Zahlen können addiert und multipliziert werden, d.h. wir haben zwei Abbildungen

$$+ \colon \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}, (a, b) \mapsto a + b, \quad \cdot \colon \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}, (a, b) \mapsto ab \quad .$$

In der Sprache der Algebra sind + und · Verknüpfungen auf $\mathbb{Z}$.

Es gelten dann für a, b, $c \in \mathbb{Z}$ folgende Rechengesetze:

Kommutativgesetze: $a + b = b + a$, $ab = ba$.
Assoziativgesetze: $a + (b + c) = (a + b) + c$, $a(bc) = (ab)c$.
Existenz der Null: Es gibt genau ein $n \in \mathbb{Z}$ mit $n + x = x + n = x$ für alle $x \in \mathbb{Z}$ (nämlich $n = 0$).
Existenz von additiven Inversen: Für jedes $x \in \mathbb{Z}$ gibt es ein $y \in \mathbb{Z}$ mit $x + y = 0 = y + x$ (nämlich $y = -x$).
Existenz der Eins: Es gibt genau ein $e \in \mathbb{Z}$ mit $ex = xe = x$ für alle $x \in \mathbb{Z}$ (nämlich $e = 1$).
Distributivgesetz: $a(b+c) = ab+ac$ (und dann natürlich auch $(b+c)a = ba+ca$).
Kürzungsregel: Ist $c \neq 0$ und $ac = bc$ so folgt $a = b$.

In der Sprache der Algebra bedeutet dies: $(\mathbb{Z}, +, \cdot)$ ist ein kommutativer Ring ohne Nullteiler, d.h. ein Integritätsbereich.

Die Teilmengen $\mathbb{N}^+$, $\mathbb{N}$ von $\mathbb{Z}$ sind bezüglich + und · abgeschlossen, d.h. enthalten mit a, b auch $a + b$ und ab.

Wie üblich setzen wir für a, $b \in \mathbb{Z}$: $a - b = a + (-b)$. Für a, b, $c \in \mathbb{Z}$ gelten dann:

- $a(b - c) = ab - ac$.
- $-(ab) = (-a)b = a(-b)$.
- $ab = (-a)(-b)$.

1.1.3. Ganze Zahlen (und damit natürliche Zahlen) können auch ihrer Größe nach verglichen werden. Wie üblich schreiben wir $a \leq b$, falls a kleiner oder gleich b ist. Ebenso habe $a < b$, $a > b$, $a \geq b$ die übliche Bedeutung. Dann gelten für a, b, $c \in \mathbb{Z}$ folgende Regeln:

- $a \leq a$
- $(a \leq b) \wedge (b \leq a) \Rightarrow a = b$.
- $(a \leq b) \wedge (b \leq c) \Rightarrow a \leq c$.
- $a \leq b$ oder $b \leq a$.
- $a \leq b \Rightarrow a + c \leq b + c$, $a < b \Rightarrow a + c < b + c$.
- $a \leq b$, $c \geq 0 \Rightarrow ac \leq bc$, $a < b$, $c > 0 \Rightarrow ac < bc$.
- $a \leq b$, $c \leq 0 \Rightarrow ac \geq bc$, $a < b$, $c < 0 \Rightarrow ac > bc$.

In der Sprache der Algebra: $(\mathbb{Z}, +, \cdot, \leq)$ ist ein total geordneter Ring.

Wir setzen noch für $a \in \mathbb{Z}$:

$$|a| = \begin{cases} a & a \geq 0 \\ -a & a < 0 \end{cases} .$$

Dann ist $|a| \geq 0$, $|a| = 0 \iff a = 0$ und für $b \in \mathbb{N}$ gelten

$$|a| < b \iff -b < a < b, \quad |a| \leq b \iff -b \leq a \leq b .$$

Weiters ist $|ab| = |a||b|$ für alle a, $b \in \mathbb{Z}$.

1.1.4. In $\mathbb{N}$ haben wir das folgende Induktionsprinzip: Sei $A \subset \mathbb{N}$. Gelten dann

- $0 \in A$;
- $\forall n \in \mathbb{N}$: $n \in A \Rightarrow n + 1 \in A$;

so ist $A = \mathbb{N}$. Wie bekannt, beruht darauf das Beweisprinzip der vollständigen Induktion.

Das Induktionsprinzip hat folgende logisch äquivalente Fassung: Jede nicht leere Teilmenge von $\mathbb{N}$ hat ein kleinstes Element.

1.2. **Division mit Rest.**

1.2.1. Schon in der Volksschule lernen wir mit Rest zu dividieren. Das schaut dann zum Beispiel so aus:

$$\begin{array}{l} 13578 : 11 = 1234 \\ \;25 \\ \;\;37 \\ \;\;\;48 \\ \;\;\;\;4\mathrm{R} \end{array} .$$

Dies ist also ein Rechenverfahren, das für $(a, b) \in \mathbb{Z} \times \mathbb{N}^+$ (hier $a = 13578$, $b = 11$) ein Ergebnis $(q, r) \in \mathbb{Z} \times \mathbb{Z}$ liefert (hier $q = 1234$, $r = 4$). Wie hängen nun (a, b) und (q, b) zusammen? Antwort: $a = qb + r$, im Beispiel also $13578 = 1234 \cdot 11 + 4$.

Satz 1.2.2. *Seien $a \in \mathbb{Z}$, $b \in \mathbb{N}^+$. Dann gibt es eindeutig bestimmte $q \in \mathbb{Z}$, $r \in \{0, 1, \ldots b-1\}$ mit $a = qb + r$. Zusatz: Gilt $a \in \mathbb{N}$ so ist auch $q \in \mathbb{N}$.*

Beweis. Existenz von q und r: Wir setzen

$$T = \{a + kb \mid k \in \mathbb{Z}\} = \{a, a \pm b, a \pm 2b, \ldots\}.$$

Dann ist $a + |a|b \in T$. Wegen

$$a + |a|b \overset{b\geq 1,\, |a|\geq 0}{\geq} a + |a| = \begin{cases} 2a & \text{falls } a \geq 0 \\ 0 & \text{falls } a < 0 \end{cases} \geq 0$$

gilt sogar

$$a + |a|b \in T \cap \mathbb{N} \quad .$$

Daher ist die Menge $T \cap \mathbb{N}$ nicht leer und hat somit ein kleinstes Element. Sei dieses r. Wegen $r \in T$ gibt es $k \in \mathbb{Z}$ mit $r = a + kb$. Setzen wir $q = -k$, so folgt $a = qb + r$. Es bleibt $r \in \{0, \ldots, b-1\}$ zu zeigen. Wegen $r \in \mathbb{N}$ ist $r \geq 0$. Angenommen es ist $r \geq b$. Dann ist $r - b \in \mathbb{N}$ und wegen

$$r - b = a + kb - b = a + (k-1)b$$

ist auch $r - b \in T$, also $r - b \in T \cap \mathbb{N}$ und damit $r - b \geq r$. Es folgt $b \leq 0$, Widerspruch.

Eindeutigkeit von q und r: Seien $q, q' \in \mathbb{Z}$, $r, r' \in \{0, 1, \ldots, b-1\}$ mit $a = qb+r = q'b+r'$. Wir zeigen $r = r'$ und $q = q'$. Aus $qb + r = q'b + r'$ folgt

$$r - r' = (q' - q)b, \quad \text{und damit } |r - r'| = |q' - q|b \quad .$$

Wegen r, $r' \in \{0, 1, \ldots, b-1\}$ ist

$$0 \leq r < b \text{ und } -b < -r' \leq 0$$

woraus

$$-b < r - r' < b \text{ also } |r - r'| < b$$

folgt. Wir erhalten damit

$$|q' - q|b = |r - r'| < b$$

woraus wegen $b > 0$, $|q' - q| < 1$ folgt. Also ist $|q' - q| = 0$, d.h. $q' - q = 0$ und daher $q' = q$. Dann ist auch $r = a - qb = a - q'b = r'$.

Zusatz: Seien $a \in \mathbb{N}$. Angenommen es ist $q \notin \mathbb{N}$. Dann ist $q \leq -1$ und damit $a = qb + r \leq -b + r < 0$, Widerspruch. □

Definition 1.2.3. Seien $a \in \mathbb{Z}$ und $b \in \mathbb{N}^+$. Sind $q \in \mathbb{Z}$ und $r \in \{0, 1, \ldots, b-1\}$ mit $a = qb + r$, so heißt q der Quotient und r der Rest der Division von a durch b. Man sagt auch, dass a bei der Division durch b den Rest r läßt.

Beispiele 1.2.4.

1. Wir haben gesehen, dass $13578 = 1234 \cdot 11 + 4$ ist. Es folgt $-13578 = (-1234) \cdot 11 - 4 = (-1234) \cdot 11 - 11 + 11 - 4 = (-1235) \cdot 11 + 7$.

2. Wir zeigen, dass jede Quadratzahl in $\mathbb{N}$ bei der Division durch 4 den Rest 0 oder 1 läßt. Sei also n^2 ($n \in \mathbb{N}$) eine Quadratzahl. Wir dividieren zuerst n durch 4: $n = 4q + r$ mit $r \in \{0, 1, 2, 3\}$. Dann folgt

$$n^2 = (4q + r)^2 = 16q^2 + 8qr + r^2 = 4(4q^2 + 2qr) + r^2 =$$
$$= \begin{cases} 4(4q^2 + 2qr) + 0 & \text{falls } r = 0 \\ 4(4q^2 + 2qr) + 1 & \text{falls } r = 1 \\ 4(4q^2 + 2qr + 1) + 0 & \text{falls } r = 2 \\ 4(4q^2 + 2qr + 2) + 1 & \text{falls } r = 3 \end{cases} .$$

Die Behauptung folgt.

Eine Anwendung: In der Folge $(11, 111, 1111, 11111, \ldots)$ kommt keine Quadratzahl vor. Denn, jedes Folgenglied a hat die Form $a = 100n + 11$ mit $n \in \mathbb{N}$. Es folgt

$$a = 4 \cdot 25n + 2 \cdot 4 + 3 = 4 \cdot (25n + 2) + 3 \quad .$$

Also läßt jedes Folgenglied bei der Division durch 4 den Rest 3, kann also keine Quadratzahl sein.

1.3. **Teiler und Vielfache.**

Definition 1.3.1. Seien a, $b \in \mathbb{Z}$. Gibt es ein $k \in \mathbb{Z}$ mit $bk = a$, so schreibt man $b \mid a$ und sagt

- b teilt a;
- a ist durch b teilbar;
- b ist ein Teiler von a.
- a ist ein Vielfaches von b.

Ist b kein Teiler von a so schreibt man $b \nmid a$.

1.3.2. Seien $b \in \mathbb{N}^+$ und $a \in \mathbb{Z}$. Aus der Eindeutigkeitsaussage im Satz über die Division mit Rest (1.2.2) folgt sofort: b ist genau dann ein Teiler von a, wenn a bei der Division durch b den Rest 0 läßt. Mit Hilfe der Division mit Rest kann also rechnerisch entschieden werden, ob eine Zahl ein Teiler einer anderen ist.

Satz 1.3.3 (Eigenschaften der Teilerrelation)**.** *Seien a, b, $c \in \mathbb{Z}$. Dann gelten:*

1. $1 \mid b$, $b \mid 0$, $b \mid b$.
2. $0 \mid a \iff a = 0$.
3. $b \mid a \iff |b| \mid |a| \iff \pm b \mid \pm a$.
4. $(b \mid a) \wedge (a \mid c) \Rightarrow b \mid c$.
5. *Sind $n \in \mathbb{N}$ und x_1, $y_1, \ldots$, x_n, $y_n \in \mathbb{Z}$ und gilt $b \mid x_i$, $i = 1, \ldots, n$, so gilt $b \mid \sum_{i=1}^{n} x_i y_i$. Insbesondere gelten: Aus $b \mid a$ folgt $b \mid ac$ und aus $b \mid a$ und $b \mid c$ folgt $b \mid a \pm c$.*

In der Sprache der Algebra bedeutet dies: die Menge aller ganzen Zahlen, die von b geteilt werden, also die Menge $b\mathbb{Z} = \{0, \pm b, \pm 2b, \pm 3b, \ldots\}$ aller Vielfachen von b ist ein Ideal des Ringes $\mathbb{Z}$.

6. $b \mid a \Rightarrow bc \mid ac$. *Ist* $c \neq 0$ *so gilt auch die Umkehrung:* $[(c \neq 0) \wedge (bc \mid ac)] \Rightarrow b \mid a$.
7. *Ist* $a \neq 0$ *und gilt* $b \mid a$, *so ist* $|b| \leq |a|$.
8. $(a \mid b) \wedge (b \mid a) \iff |a| = |b|$.

Beweis. 1. $1 \cdot b = b = b \cdot 1 \Rightarrow 1 \mid b \wedge b \mid b$. $0 = 0 \cdot b \Rightarrow b \mid 0$.

2. Ist $a = 0$ so gilt $0 = a \mid a$ nach 1. Gelte umgekehrt $0 \mid a$. Dann gibt es $k \in \mathbb{Z}$ mit $a = k0$ und es folgt $a = 0$.

3. Wir nehmen zunächst $b \mid a$ an. Dann gibt es $k \in \mathbb{Z}$ mit $a = kb$. Es folgt

$$|a| = |kb| = |k||b| \quad ,$$

also $|b| \mid |a|$.

Gelte nun umgekehrt $|b| \mid |a|$. Dann können wir $k \in \mathbb{Z}$ wählen mit $|a| = k|b|$. Wähle $e, f \in \{-1, 1\}$ mit $a = e|a|$ und $b = f|b|$. Wegen $f^2 = 1$ gilt dann auch $|b| = fb$. Es folgt

$$a = e|a| = ek|b| = (ekf)b \quad ,$$

also $b \mid a$.

Wegen $|\pm a| = |a|$, $|\pm b| = |b|$ folgt damit auch $|b| \mid |a| \iff \pm b \mid \pm a$.

4. Es gelte also $b \mid a$ und $a \mid c$. Dann gibt es k, $l \in \mathbb{Z}$ mit $a = kb$ und $c = la$. Dann ist $c = (lk)b$, also $b \mid c$.

5. Es gelte $b \mid x_i$, für $i = 1, \ldots, n$. Dann gibt es $k_1, \ldots k_n \in \mathbb{Z}$ mit $x_i = k_i b$ für $i = 1, \ldots, n$. Es folgt

$$\sum_{i=1}^{n} x_i y_i = \sum_{i=1}^{n} k_i b y_i = b \sum_{i=1}^{n} k_i y_i \quad ,$$

also $b \mid \sum_{i=1}^{n} x_i y_i$.

6. Gilt $b \mid a$, so gilt $a = kb$ mit $k \in \mathbb{Z}$. Es folgt $ac = kbc$, also $bc \mid ac$. Gelte nun $bc \mid ac$ und $c \neq 0$. Dann ist $ac = kbc$ mit $k \in \mathbb{Z}$. Wegen $c \neq 0$ können wir c in dieser Gleichung kürzen und erhalten $a = kb$, und daher $b \mid a$.

7. Wir nehmen $a \neq 0$ und $b \mid a$ an. Dann gilt $a = kb$ mit $k \in \mathbb{Z}$. Wegen $a \neq 0$ ist auch $k \neq 0$ und damit $|k| \geq 1$. Es folgt

$$|a| = |k||b| \geq |b| \quad .$$

8. Es gelte also $a \mid b$ und $b \mid a$. Ist $a = 0$, so folgt aus $a \mid b$ nach 2. auch $b = 0$. Analog folgt aus $b \mid a$ und $b = 0$ auch $a = 0$.

Wir können daher $a \neq 0$ und $b \neq 0$ annehmen. Wir wenden nun zweimal Teil 7. an:

$$a \mid b \Rightarrow |a| \leq |b|, \quad b \mid a \Rightarrow |b| \leq |a| \quad .$$

Also ist $|a| = |b|$.

Gelte nun umgekehrt $|a| = |b|$. Nach 1. gelten dann $|a| \mid |b|$ und $|b| \mid |a|$. Anwendung von 3. liefert $a \mid b$ und $b \mid a$. □

Beispiel 1.3.4. Als Anwendung dieser Regeln lösen wir folgende Aufgabe der Mathematikolympiade in Großbritannien aus dem Jahr 2001/2002:

Bestimmen Sie alle $(x, y) \in \mathbb{Z} \times \mathbb{Z}$, die der Gleichung

$$1 + x^2 y = x^2 + 2xy + 2x + y \tag{1.3.4.1}$$

genügen.

Bemerkung: Gleichungen, in denen die Variablen auf ganze Zahlen beschränkt sind, nennt man diophantische Gleichungen (nach dem griechischen Mathematiker Diophantos von Alexandria, ca. 250 n. Chr.).

Wir nehmen nun an, dass $(x, y) \in \mathbb{Z}^2$ eine Lösung der Gleichung (1.3.4.1) ist und formen um:

$$x^2 y - 2xy - y = x^2 + 2x - 1, \quad \text{also} \quad (x^2 - 2x - 1)y = x^2 + 2x - 1 \quad .$$

Daher ist $x^2 - 2x - 1$ ein Teiler von $x^2 + 2x - 1$. Wir wollen ausnutzen, dass Teiler einer Zahl z ungleich Null betragsmäßig kleiner als z sein müssen. Für große positive x ist aber $x^2 - 2x - 1$ sowieso betragsmäßig kleiner als $x^2 + 2x - 1$, dies wird also direkt nichts bringen. Wir müssen also $x^2 + 2x - 1$ irgendwie kleiner machen. Wir benutzen dazu unsere Regeln:

$$\begin{aligned}(x^2 - 2x - 1 \mid x^2 + 2x - 1) \wedge (x^2 - 2x - 1 \mid x^2 - 2x - 1) \Rightarrow \\ x^2 - 2x - 1 \mid (x^2 + 2x - 1) - (x^2 - 2x - 1) = 4x \quad .\end{aligned}$$

Also erhalten wir jetzt $x = 0$ oder $|x^2 - 2x - 1| \leq 4|x|$.

Wir nehmen also $x \neq 0$ an und wir untersuchen zunächst wann $x^2 - 2x - 1 < 0$ ist. Dies ist äquivalent zu $(x - 1)^2 - 2 < 0$, also zu $x - 1 \in \{-1, 0, 1\}$ also zu $(x \neq 0)$ $x \in \{1, 2\}$.

Wir nehmen daher jetzt an, dass $x \notin \{0, 1, 2\}$ gilt. Ist $x \geq 3$ so folgt, dass

$$x^2 - 2x - 1 \leq 4x$$

gilt. Wir erhalten daher

$$x^2 - 6x - 1 \leq 0 \quad \text{also} \quad (x - 3)^2 - 10 = x^2 - 6x - 1 \leq 0.$$

Wegen $x \geq 3$ folgt daraus $x \in \{3, 4, 5, 6\}$.

Sei nun $x < 0$. Dann gilt also

$$x^2 - 2x - 1 \leq -4x \quad \text{also} \quad (x + 1)^2 - 2 = x^2 + 2x - 1 \leq 0 \quad .$$

Es folgt $x + 1 \in \{-1, 0, 1\}$ also $(x < 0)$ $x \in \{-2, -1\}$.

Damit haben wir nun gezeigt: Ist $(x, y) \in \mathbb{Z}^2$ eine Lösung unserer Gleichung, so muss $x \in \{-2, -1, 0, 1, 2, 3, 4, 5, 6\}$ gelten. Wir erhalten daher für jeden dieser möglichen Werte von x eine lineare Gleichung in y, die wie üblich gelöst werden kann. Vorsicht: Wir haben die Bedingung $y \in \mathbb{Z}$. Es kann also vorkommen, dass diese lineare Gleichung keine Lösung

(in $\mathbb{Z}$) hat; dies passiert genau dann, wenn $x \in \{-2, 4, 5, 6\}$ gilt. Als Lösungsmenge ergibt sich damit

$$\{(-1,-1), (0,1), (1,-1), (2,-7), (3,7)\} \quad .$$

1.4. **Der größte gemeinsame Teiler.**

Definition 1.4.1. Sei $a \in \mathbb{Z}$. Wir bezeichnen mit

$$T(a) = \{t \in \mathbb{N}^+ \mid t \mid a\}$$

die Menge aller echt positiven Teiler von a.

Beispiele 1.4.2.

1. Seien $a \in \mathbb{Z}$ und $t \in \mathbb{N}^+$. Nach 1.3.3.3 gilt $t \mid a \iff t \mid -a$. Es folgt $T(a) = T(-a) = T(|a|)$.
2. Nach 1.3.3.1 gilt $T(0) = \mathbb{N}^+$.
3. $T(1) = \{1\}$.
4. In der folgenden Tabelle sind für manche natürliche Zahlen n die Anzahl der Elemente von $T(n)$ eingetragen

n	4	5	6	7	8	9	16	25	26	36
$\#T(n)$	3	2	4	2	4	3	5	3	4	9

   Was fällt auf? Antwort: In der Tabelle ist $\#T(n)$ nur dann ungerade, wenn n eine Quadratzahl ist.
   Welche Vermutung könnte man aufstellen? Antwort: Für alle $n \in \mathbb{N}^+$ gilt: $\#T(n)$ ist genau dann ungerade, wenn n eine Quadratzahl ist.

Lemma 1.4.3. *Für a, b, $k \in \mathbb{Z}$ gelten:*

1. $1 \in T(a)$. *Insbesondere ist $T(a)$ nicht leer.*
2. *Ist $a \neq 0$, so gilt*
$$\{1, |a|\} \subset T(a) \subset \{1, 2, \ldots, |a|\} \quad .$$
   Insbesondere ist $T(a)$ endlich für $a \neq 0$.
3. $a \mid b \iff T(a) \subset T(b)$.
4. $T(a) \cap T(b) = T(a) \cap T(b + ka)$.

Beweis. 1 folgt aus 1.3.3.1 und 2 folgt aus 1.3.3.1,3,7.

3. Gilt $a \mid b$ so folgt $T(a) \subset T(b)$ aus 1.3.3.4. Gelte nun umgekehrt $T(a) \subset T(b)$. Ist $a = 0$, so folgt $\mathbb{N}^+ = T(0) \subset T(b)$. Aus Teil 2 erhalten wir damit auch $b = 0$ und es folgt $a \mid b$.

Sei nun $a \neq 0$. Wegen $|a| \in T(a)$ (nach Teil 2) folgt $|a| \in T(b)$ also $|a| \mid b$, also auch $a \mid b$ (1.3.3.3).

4. Wir zeigen zuerst $T(a) \cap T(b + ka) \subset T(a) \cap T(b)$ für alle a, b, $k \in \mathbb{Z}$. Seien also a, b, $k \in \mathbb{Z}$ und $t \in T(a) \cap T(b + ka)$. Dann ist nach Definition $t \in \mathbb{N}^+$ und $t \mid a$, $t \mid b + ka$.

Wir müssen also nur noch $t \mid b$ zeigen. Dies folgt aber aus 1.3.3.5:

$$t \mid a \wedge t \mid b + ka \Rightarrow t \mid b + ka - ka = b \quad .$$

Wir zeigen nun $T(a) \cap T(b) \subset T(a) \cap T(b+ka)$ für alle $a, b, k \in \mathbb{Z}$. Seien also $a, b, k \in \mathbb{Z}$. Wir setzen $a' = a$, $b' = b + ka$, $k' = -k$ und erhalten mit Hilfe der schon bewiesenen Inklusion:

$$T(a) \cap T(b) = T(a') \cap T(b' + k'a') \subset T(a') \cap T(b') = T(a) \cap T(b + ka) \quad .$$

□

1.4.4. Seien $k \in \mathbb{N}^+$ und $a_1, \ldots, a_k \in \mathbb{Z}$. Dann ist nach Definition

$$T(a_1) \cap \ldots \cap T(a_k)$$

die Menge aller echt positive Zahlen, die alle a_i teilen, also die Menge der echt positiven, gemeinsamen Teiler der a_i. Wegen $1 \mid a_i$ für $i = 1, \ldots, k$ ist diese Menge nicht leer.

Sind alle $a_i = 0$, so gilt nach Beispiel 1.4.2.2

$$T(a_1) \cap \ldots \cap T(a_k) = \mathbb{N}^+ \quad .$$

Seien nun nicht alle a_i gleich Null, etwa $a_l \neq 0$ mit $1 \leq l \leq k$. Dann ist wegen

$$T(a_1) \cap \ldots \cap T(a_k) \subset T(a_l)$$

und Lemma 1.4.3.2 $T(a_1) \cap \ldots \cap T(a_k)$ endlich und besitzt daher ein größtes Element. Daher ist folgende Definition sinnvoll.

Definition 1.4.5. Seien $k \in \mathbb{N}^+$ und $a_1, \ldots, a_k \in \mathbb{Z}$ nicht alle Null. Dann heißt

$$\mathrm{ggT}(a_1, \ldots, a_k) := \max(T(a_1) \cap \ldots \cap T(a_k))$$

der größte gemeinsame Teiler von $a_1, \ldots, a_k$.

Beispiele 1.4.6. Es seien $a_1, \ldots, a_k \in \mathbb{Z}$ nicht alle Null.

1. Ist $k = 1$ so gilt $\mathrm{ggT}(a_1) = |a_1|$. Denn zunächst gilt nach Definition $\mathrm{ggT}(a_1) = \max T(a_1)$, und aus Lemma 1.4.3.2 folgt $\max T(a_1) = |a_1|$.
2. Es gilt
$$\mathrm{ggT}(a_1, \ldots, a_k) = \mathrm{ggT}(\pm a_1, \ldots, \pm a_k) = \mathrm{ggT}(|a_1|, \ldots, |a_k|)$$
(wegen $T(a_i) = T(-a_i) = T(|a_i|)$).
3. $\mathrm{ggT}(a_1, \ldots, a_k)$ hängt nicht von der Reihenfolge der a_i ab, d.h.: Ist σ eine Permutation der Menge $\{1, \ldots, k\}$ so gilt
$$\mathrm{ggT}(a_1, \ldots, a_k) = \mathrm{ggT}(a_{\sigma(1)}, \ldots, a_{\sigma(k)}) \quad .$$
Denn:
$$T(a_1) \cap \ldots \cap T(a_k) = T(a_{\sigma(1)}) \cap \ldots \cap T(a_{\sigma(k)}).$$
4. Ist $a \in \mathbb{Z} \setminus \{0\}$ so gilt $\mathrm{ggT}(a, 0) = |a|$. Denn $\mathrm{ggT}(a, 0) = \max(T(a) \cap T(0)) = \max(T(a) \cap \mathbb{N}^+) = \max T(a) = (\text{siehe } 1.) = |a|$.

5. Seien a, $b \in \mathbb{Z}$ nicht beide Null und $k \in \mathbb{Z}$. Wegen Lemma 1.4.3.4 gilt dann
$$\mathrm{ggT}(a,b) = \max(T(a) \cap T(b)) = \max(T(a) \cap T(b+ka)) = \mathrm{ggT}(a, b+ka) \quad .$$
6. Wir benutzen 5. um $d = \mathrm{ggT}(123456789, 432)$ zu bestimmen. Wir dividieren dazu 123456789 mit Rest durch 432 und erhalten
$$123456789 = 285779 \cdot 432 + 261 \quad .$$
Es folgt
$$d = \mathrm{ggT}(123456789, 432) = \mathrm{ggT}(123456789 - 28779 \cdot 432, 432) = \\ = \mathrm{ggT}(261, 432) \quad .$$
Analog geht es weiter. Wir dividieren 432 mit Rest usw. Wir erhalten
$$d = \mathrm{ggT}(261, 432) = \mathrm{ggT}(261, 261 + 171) = \mathrm{ggT}(261, 171) = \\ = \mathrm{ggT}(171 + 90, 171) = \mathrm{ggT}(90, 171).$$
Nun könnte man analog fortfahren, aber es lohnt sich genau hinzuschauen: Dividiert man 171 mit Rest durch 90 so erhält man $171 = 90 + 81$. Es gilt aber auch $171 = 2 \cdot 90 - 9$. Beachte, dass -9 betragsmäßig viel kleiner als 81 ist. Es folgt
$$d = \mathrm{ggT}(90, 171) = \mathrm{ggT}(90, 2 \cdot 90 - 9) = \mathrm{ggT}(90, -9) = \mathrm{ggT}(90, 9) = 9 \quad .$$
Diese Methode funktioniert nun nicht nur für die zwei Zahlen 123456789 und 432, sondern ganz allgemein.

Satz 1.4.7. *Seien a, $b \in \mathbb{N}$ mit $a > b$. Wir definieren induktiv eine Folge $(r_n)_{n\in\mathbb{N}}$ natürlicher Zahlen wie folgt:*

$r_0 = a$, $r_1 = b$,

und für $n \geq 2$: $r_n = \begin{cases} 0 & \text{falls } r_{n-1} = 0 \\ \text{Rest der Division von } r_{n-2} \text{ durch } r_{n-1} & \text{falls } r_{n-1} \neq 0 \end{cases}$.

Dann gibt es $n \in \mathbb{N}^+$ mit $r_n = 0$. Ist $n \in \mathbb{N}^+$ so klein wie möglich mit $r_n = 0$, so gilt $r_{n-1} = \mathrm{ggT}(a, b)$ (Euklidische Algorithmus zur Bestimmung des größten gemeinsamen Teilers).

Beweis. Angenommen es ist $r_n \neq 0$ für alle $n \in \mathbb{N}^+$. Da für $n \geq 2$, r_n der Rest einer Division durch r_{n-1} ist, folgt $r_n < r_{n-1}$ für $n \geq 2$. Also ist $(r_n)_{n\in\mathbb{N}^+}$ eine streng monoton fallende Folge natürlicher Zahlen. So eine kann aber nicht existieren. Also ist $r_n = 0$ für mindestens ein $n \in \mathbb{N}^+$ (und dann nach Definition $r_k = 0$ für alle $k \geq n$).

Sei nun $n \in \mathbb{N}^+$ minimal mit $r_n = 0$. Wir zeigen
$$\mathrm{ggT}(a, b) = \mathrm{ggT}(r_i, r_{i+1})$$
für $i = 0, \ldots, n-1$. Wir benutzen dazu Induktion nach i. Wegen $r_0 = a$, $r_1 = b$, ist die Aussage für $i = 0$ klar. Sei jetzt $0 \leq i \leq n-2$ und es gelte $\mathrm{ggT}(a, b) = \mathrm{ggT}(r_i, r_{i+1})$. Wir müssen $\mathrm{ggT}(a, b) = \mathrm{ggT}(r_{i+1}, r_{i+2})$ zeigen.

Wegen $i+1 \leq n-1 < n$ ist $r_{i+1} \neq 0$. Daher ist nach Definition r_{i+2} der Rest der Division von r_i durch r_{i+1}. Also gibt es $k \in \mathbb{Z}$ mit $r_i = kr_{i+1} + r_{i+2}$. Es folgt

$$\mathrm{ggT}(a,b) = \mathrm{ggT}(r_i, r_{i+1}) = \mathrm{ggT}(kr_{i+1} + r_{i+2}, r_{i+1}) \overset{1.4.6.5}{=} \mathrm{ggT}(r_{i+2}, r_{i+1}) = \mathrm{ggT}(r_{i+1}, r_{i+2}).$$

Insbesondere folgt jetzt (mit $i = n-1$)

$$\mathrm{ggT}(a,b) = \mathrm{ggT}(r_{n-1}, r_n) = \mathrm{ggT}(r_{n-1}, 0) \overset{r_{n-1}>0}{=} r_{n-1}.$$

□

Beispiel 1.4.8. Zur Illustration noch ein Beispiel dazu. Wir bestimmen $\mathrm{ggT}(-352, 106)$. Zunächst ist $\mathrm{ggT}(-352, 106) = \mathrm{ggT}(352, 106)$. Nun dividieren wir laufend mit Rest und erhalten:

$$\begin{aligned} 352 &= 3 \cdot 106 + 34 && \Rightarrow r_2 = 34, \\ 106 &= 3 \cdot 34 + 4 && \Rightarrow r_3 = 4, \\ 34 &= 8 \cdot 4 + 2 && \Rightarrow r_4 = 2, \\ 4 &= 2 \cdot 2 + 0 && \Rightarrow r_5 = 0 \quad . \end{aligned}$$

Also ist $\mathrm{ggT}(-352, 106) = r_4 = 2$.

Satz 1.4.9. *Seien $k \in \mathbb{N}^+$, $a_1, \ldots, a_k \in \mathbb{Z}$ nicht alle Null und $d \in \mathbb{N}^+$. Dann sind äquivalent:*

1. $d = \mathrm{ggT}(a_1, \ldots, a_k)$.
2. $d \mid a_i$, $i = 1, \ldots, k$ *und es gibt* $x_1, \ldots, x_k \in \mathbb{Z}$ *mit* $d = x_1a_1 + \ldots + x_ka_k$.
3. $d \mid a_i$, $i = 1, \ldots, k$ *und ist* $d' \in \mathbb{N}^+$ *mit* $d' \mid a_i$ *für alle* $i = 1, \ldots, k$, *so gilt* $d' \mid d$.

Beweis. $1 \Rightarrow 2$. Es sei also $d = \mathrm{ggT}(a_1, \ldots, a_k)$. Nach Definition des ggT gilt dann $d \mid a_i$ für alle $i = 1, \ldots, k$. Wir müssen also noch $x_1, \ldots, x_k \in \mathbb{Z}$ mit $d = x_1a_1 + \ldots + x_ka_k$ finden.

Wir setzen dazu

$$L = \{x_1a_1 + \ldots + x_ka_k \mid x_1, \ldots, x_k \in \mathbb{Z}\} \subset \mathbb{Z} \quad .$$

Sei $1 \leq j \leq k$ mit $a_j \neq 0$. Dann ist

$$0 < a_j^2 = 0 \cdot a_1 + \ldots + 0 \cdot a_{j-1} + a_j \cdot a_j + 0 \cdot a_{j+1} + \ldots + 0 \cdot a_k \in L \quad .$$

Daher ist $L \cap \mathbb{N}^+ \neq \emptyset$. Wir bezeichnen mit d' das kleinste Element von $L \cap \mathbb{N}^+$ und zeigen $d' = d$ (dann ist $d = d' \in L$). Wir wählen dazu $x_1, \ldots, x_k \in \mathbb{Z}$ mit $d' = x_1a_1 + \ldots + x_ka_k$.

Wegen $d \mid a_i$, $i = 1, \ldots k$, gilt auch $d \mid d'$ nach 1.3.3.5. Anwendung von 1.3.3.7 liefert $d = |d| \leq |d'| = d'$. Es bleibt $d' \leq d$ zu zeigen. Nach Definition des ggT genügt es dazu $d' \mid a_i$ für alle $i = 1, \ldots, k$ zu zeigen. Angenommen, dies ist falsch. Dann könen wir ein $1 \leq j \leq k$ mit $d' \nmid a_j$ wählen. Wir dividieren nun a_j durch d' mit Rest: $a_j = qd' + r$. Wegen $d' \nmid a_j$ ist $0 < r < d'$.

Nun gilt

$$r = a_j - qd' = a_j - q(x_1a_1 + \ldots + x_ka_k) =$$
$$= (-qx_1)a_1 + \ldots + (-qx_{j-1})a_{j-1} + (1 - qx_j)a_j + (-qx_{j+1})a_{j+1} + \ldots + (-qx_k)a_k \in L.$$

Wegen $r > 0$ folgt sogar $r \in L \cap \mathbb{N}^+$. Da d' das kleinste Element von $L \cap \mathbb{N}^+$ ist, folgt $r \geq d'$, was $r < d'$ widerspricht.

$2 \Rightarrow 3$. Es gelte also $d \mid a_i$ für alle $i = 1, \ldots, k$ und es seien $x_1, \ldots, x_k \in \mathbb{Z}$ mit $d = x_1a_1 + \ldots + x_ka_k$. Wir müssen noch zeigen: Ist $d' \in \mathbb{N}^+$ mit $d' \mid a_i$ für alle $i = 1, \ldots, k$, so gilt $d' \mid d$. Dies folgt aber aus 1.3.3.5

$3 \Rightarrow 1$. Wir nehmen also an, dass die Aussage in 3 wahr ist. Es sei $d' = \mathrm{ggT}(a_1, \ldots, a_k)$ und zeigen $d = d'$. Wegen $d' \mid a_i$, für alle $i = 1, \ldots, k$ gilt nach Voraussetzung $d' \mid d$.

Wegen $d' = \mathrm{ggT}(a_1, \ldots, a_k)$ können wir die schon bewiesene Implikation $1 \Rightarrow 2$ verwenden: Es gibt $x_1, \ldots, x_k \in \mathbb{Z}$ mit $d' = x_1a_1 + \ldots + a_kx_k$. Wegen $d \mid a_i$ für alle $i = 1, \ldots, k$ gilt wieder nach 1.3.3.5 $d \mid d'$.

Wir wissen also jetzt $d' \mid d$ und $d \mid d'$. Anwendung von 1.3.3.8 liefert jetzt $d = |d| = |d'| = d'$. □

Korollar 1.4.10. *Es seien $k \in \mathbb{N}^+$ und $a_1, \ldots, a_k \in \mathbb{Z}$ nicht alle Null und wir setzen $d = \mathrm{ggT}(a_1, \ldots, a_k)$. Dann gilt*

$$T(a_1) \cap \ldots \cap T(a_k) = T(d)$$

(also: die Menge der gemeinsamen positiven Teiler der a_i ist die Menge der positiven Teiler des ggT der a_i; wegen 1.3.3.3 können wir in dieser Aussage positive Teiler durch Teiler ersetzen).

Beweis. Es sei $d' \in T(d)$. Dann folgen $d' \in \mathbb{N}^+$ und $d' \mid d$. Wegen $d \mid a_i$ für alle $i = 1, \ldots, k$ gilt dann auch $d' \mid a_i$, $i = 1, \ldots, k$. Es folgt $d' \in T(a_1) \cap \ldots T(a_k)$. Damit haben wir $\supset$ gezeigt.

Es sei nun umgekehrt $d' \in T(a_1) \cap \ldots \cap T(a_k)$. Nach 1.4.9.3 gilt dann $d' \mid d$, also $d' \in T(d)$. □

1.4.11. Seien $k \in \mathbb{N}^+$, $a_1, \ldots a_k \in \mathbb{Z}$ nicht alle Null und $d = \mathrm{ggT}(a_1, \ldots, a_k)$. Nach 1.4.9 gibt es $x_1, \ldots, x_k \in \mathbb{Z}$ mit $d = x_1a_1 + \ldots + a_kx_k$. Wie findet man solche x_i?

Wir behandeln zunächst den Fall $k = 2$ an einem Beispiel. Wir hatten schon berechnet (siehe Beispiel 1.4.8):

(1.4.11.1) $$352 = 3 \cdot 106 + 34,$$

(1.4.11.2) $$106 = 3 \cdot 34 + 4$$

(1.4.11.3) $$34 = 8 \cdot 4 + 2$$

(1.4.11.4) $$4 = 2 \cdot 2 + 0 \quad .$$

Es folgt $2 = \mathrm{ggT}(352, 106)$. Nun rechnen wir zurück:

$$\begin{aligned}\mathrm{ggT}(106, 352) = 2 &\overset{(1.4.11.3)}{=} 34 - 8 \cdot 4 \overset{(1.4.11.2)}{=} 34 - 8 \cdot (106 - 3 \cdot 34) = \\ &= 25 \cdot 34 - 8 \cdot 106 \overset{(1.4.11.1)}{=} 25 \cdot (352 - 3 \cdot 106) - 8 \cdot 106 \\ &= 25 \cdot 352 - 83 \cdot 106 \quad .\end{aligned}$$

Der folgende Satz zeigt, wie man den Fall $k \geq 3$ auf den Fall $k = 2$ zurückführt.

Satz 1.4.12. *Seien $k \in \mathbb{N}_{\geq 3}$, $a_1, \ldots, a_k \in \mathbb{Z}$, sodass von den $k-1$ Zahlen $a_1, \ldots, a_{k-1}$ nicht alle Null sind. Wir setzen $d = \mathrm{ggT}(a_1, \ldots, a_{k-1})$. Dann gilt*

$$\mathrm{ggT}(a_1, \ldots, a_k) = \mathrm{ggT}(d, a_k)$$

(rekursive Berechnung des ggT*).*

Sind u, v, $x_1, \ldots, x_{k-1} \in \mathbb{Z}$ mit $\mathrm{ggT}(d, a_k) = ud + va_k$ und $d = x_1a_1 + \ldots + x_{k-1}a_{k-1}$ so gilt

$$\mathrm{ggT}(a_1, \ldots, a_k) = (ux_1)a_1 + \ldots + (ux_{k-1})a_{k-1} + va_k \quad .$$

Beweis. Wir beweisen zunächst $\mathrm{ggT}(d, a_k) = \mathrm{ggT}(a_1, \ldots, a_k)$. Wir setzen dazu $d' = \mathrm{ggT}(d, a_k)$. Um $d' = \mathrm{ggT}(a_1, \ldots, a_k)$ zu zeigen, benutzen wir die Äquivalenz $1 \iff 3$ in 1.4.9. Wegen $d' = \mathrm{ggT}(d, a_k)$ gilt $d' \mid d$ und $d' \mid a_k$. Für $i = 1, \ldots, k-1$ gilt $d \mid a_i$. Aus $d' \mid d$ und $d \mid a_i$ folgt nun $d' \mid a_i$ für $i = 1, \ldots, k-1$.

Sei nun $e \in \mathbb{N}^+$ mit $e \mid a_i$, $i = 1, \ldots, k$. Wir müssen $e \mid d'$ zeigen. Wegen $e \mid a_1, \ldots, a_{k-1}$ und $d = \mathrm{ggT}(a_1, \ldots, a_{k-1})$ gilt $e \mid d$ (1.4.9). Wegen $e \mid d$ und $e \mid a_k$ gilt wiederum nach 1.4.9 $e \mid \mathrm{ggT}(d, a_k) = d'$.

Schließlich gilt

$$\begin{aligned}\mathrm{ggT}(a_1, \ldots, a_k) = \mathrm{ggT}(d, a_k) = ud + va_k = u(x_1a_1 + \ldots + x_{k-1}a_{k-1}) + va_k = \\ = (ux_1)a_1 + \ldots + (ux_{k-1})a_{k-1} + va_k \quad .\end{aligned}$$

□

Beispiel 1.4.13. Wir bestimmen $d = \mathrm{ggT}(2107, 1848, -1554)$ und x, y, $z \in \mathbb{Z}$ mit $d = 2107x + 1848y - 1554z$.

Dazu berechnen wir zunächst $\mathrm{ggT}(1848, 1554)$. Laufende Division mit Rest liefert:

$$1848 = 1 \cdot 1554 + 294, \tag{1.4.13.1}$$

$$1554 = 5 \cdot 294 + 84, \tag{1.4.13.2}$$

$$294 = 3 \cdot 84 + 42, \tag{1.4.13.3}$$

$$84 = 2 \cdot 42 + 0 \quad . \tag{1.4.13.4}$$

Also erhalten wir $\mathrm{ggT}(1848,-1554)=42$. Nun bestimmen wir x,$y\in\mathbb{Z}$ mit $42=1848x-1554y$. Dazu rechnen wir wieder zurück:

$$\begin{aligned}42 &\overset{(1.4.13.3)}{=} 294-3\cdot 84 \overset{(1.4.13.2)}{=} 294-3\cdot(1554-5\cdot 294)=\\ &=16\cdot 294-3\cdot 1554 \overset{(1.4.13.1)}{=} 16\cdot(1848-1554)-3\cdot 1554=\\ &=-19\cdot 1554+16\cdot 1848=19\cdot(-1554)+16\cdot 1848 \quad .\end{aligned}$$

Nach 1.4.12 ist nun $\mathrm{ggT}(2107,1848,-1554)=\mathrm{ggT}(2107,42)$. Um diesen zu bestimmen, dividieren wir wieder laufend mit Rest:

$$\begin{aligned}2107&=50\cdot 42+7\\ 42&=6\cdot 7+0 \quad .\end{aligned}$$

Es folgt $7=\mathrm{ggT}(2107,42)=1\cdot 2107+(-50)\cdot 42$. Insgesamt erhalten wir nun

$$\begin{aligned}7=\mathrm{ggT}(2107,1848,-1554)&=1\cdot 2107+(-50)42\\ &=1\cdot 2107+(-50)(16\cdot 1848+19\cdot(-1554))=\\ &=1\cdot 2107-800\cdot 1848+(-950)\cdot(-1554) \quad .\end{aligned}$$

Definition 1.4.14. Seien a, $b\in\mathbb{Z}$. a und b heißen teilerfremd, falls $(a,b)\neq(0,0)$ ist und falls $\mathrm{ggT}(a,b)=1$ gilt.

Satz 1.4.15. *Seien $k\in\mathbb{N}^+$, $a_1,\ldots,a_k\in\mathbb{Z}$ nicht alle Null und a, b, $c\in\mathbb{Z}$. Dann gelten:*

1. *Ist $c\neq 0$ so gilt*

$$\mathrm{ggT}(ca_1,\ldots,ca_k)=|c|\,\mathrm{ggT}(a_1,\ldots,a_k) \quad .$$

   Insbesondere: Ist $d=\mathrm{ggT}(a_1,\ldots,a_k)$ so ist $\mathrm{ggT}(a_1/d,\ldots,a_k/d)=1$.
2. *Sind a und b teilerfremd, so folgt aus $a\mid bc$ auch $a\mid c$.*
3. *Sind a und b teilerfremd, so folgt aus $a\mid c$ und $b\mid c$ auch $ab\mid c$.*
4. *Sind für $i=1,\ldots,k$ c und a_i teilerfremd, so sind auch c und $a_1\cdot\ldots\cdot a_k$ teilerfremd.*
5. *Sind a und b teilerfremd so auch a^m und b^n für alle m, $n\in\mathbb{N}^+$.*

Beweis. 1. Wir setzen $d=|c|\,\mathrm{ggT}(a_1,\ldots,a_k)$. Um $d=\mathrm{ggT}(ca_1,\ldots,ca_k)$ zu zeigen, verwenden wir die Äquivalenz 1 $\iff$ 2 in Satz 1.4.9. Wir müssen also nur zeigen, dass

- $d\mid ca_i$, $i=1,\ldots,k$, und dass
- d als Linearkombination (mit Koeffizienten in $\mathbb{Z}$) der ca_i geschrieben werden kann.

Zum Beweis des ersten Teils, sei $1\leq i\leq k$. Dann gelten $\mathrm{ggT}(a_1,\ldots,a_k)\mid a_i$ und $|c|\mid c$. Aus Satz 1.3.3.6 folgen

$$d=|c|\,\mathrm{ggT}(a_1,\ldots,a_k)\mid |c|a_i, \quad |c|a_i\mid ca_i.$$

Wegen 1.3.3.4 erhalten wir $d\mid ca_i$.

Zum Beweis des zweiten Teils benutzen wir die Äquivalenz 1 $\iff$ 2 in 1.4.9 für $\mathrm{ggT}(a_1, \ldots, a_k)$. Wir können als $x_1, \ldots, x_k \in \mathbb{Z}$ wählen mit

$$\mathrm{ggT}(a_1, \ldots, a_k) = x_1 a_1 + \ldots + x_k a_k \quad .$$

Schreiben wir noch $|c| = \varepsilon c$ mit $\varepsilon \in \{\pm 1\}$ und multiplizieren die letzte Gleichung mit $|c|$ so erhalten wir

$$d = |c| \,\mathrm{ggT}(a_1, \ldots, a_k) = |c| x_1 a_1 + \ldots + |c| x_k a_k = (\varepsilon x_1) c a_1 + \ldots (\varepsilon x_k) c a_k \quad .$$

Die Insbesondere–Aussage folgt jetzt aus

$$d = \mathrm{ggT}(a_1, \ldots, a_k) = \mathrm{ggT}(d \cdot \frac{a_1}{d}, \ldots, d\frac{a_k}{d}) \overset{d>0}{=} d\,\mathrm{ggT}(\frac{a_1}{d}, \ldots, \frac{a_k}{d}) \quad .$$

Bemerkung: Die Insbesondere–Aussage folgt auch direkt aus der Definition des ggT.

2. Da a und b teilerfremd sind, gibt es nach 1.4.9 x, $y \in \mathbb{Z}$ mit $ax + yb = \mathrm{ggT}(a, b) = 1$. Durch Multiplikation mit c folgt $c = axc + ybc$. Wegen $a \mid axc$ und $a \mid ybc$ (da ja $a \mid bc$) folgt auch $a \mid axc + ybc = c$.

3. Wegen $a \mid c$ gibt es $k \in \mathbb{Z}$ mit $c = ak$. Es folgt $b \mid c = ak$. Da a und b teilerfremd sind, folgt $b \mid k$ aus 2. Anwendung von 1.3.3.6 liefert $ab \mid ak = c$.

4. Wir benutzen Induktion nach k. Für $k = 1$ ist die Aussage trivial. Wir betrachten nun den Fall $k = 2$. Wir überlegen uns als erstes $(c, a_1 a_2) \neq (0, 0)$. Ist $c \neq 0$ so ist dies klar. Ist aber $c = 0$, so gilt nach Voraussetzung $a_i \neq 0$, $i = 1, \ldots, 2$ (da c und a_i teilerfremd sind). Also ist auch $a_1 a_2 \neq 0$. Wir setzen nun $d = \mathrm{ggT}(c, a_1 a_2)$, $d_1 = \mathrm{ggT}(d, a_1)$ und $d_2 = \mathrm{ggT}(d, a_2)$. Sei $i = 1$ oder $i = 2$. Dann gilt $d_i \mid d$ und $d_i \mid a_i$. Wegen $d \mid c$ gilt nach 1.3.3.4 auch $d_i \mid c$ und $d_i \mid a_i$. Wegen $\mathrm{ggT}(c, a_i) = 1$ folgt nach 1.4.9 $d_i \mid 1$, also $1 = d_i = \mathrm{ggT}(d, a_i)$.

Aus $d \mid a_1 a_2$ und $\mathrm{ggT}(d, a_1) = 1$ folgt aus Teil 2 $d \mid a_2$. Wir erhalten

$$1 = \mathrm{ggT}(d, a_2) = d \quad .$$

Sei jetzt $k \geq 2$ und es seien c und $a_1 \ldots a_{k-1}$ teilerfremd. Der Fall $k = 2$ zeigt dann auch, dass c und $(a_1 \ldots a_{k-1}) a_k = a_1 \ldots a_k$ teilerfremd sind.

5. Wir verwenden Teil 4 mit $c = b$, $k = m$ und $a_1 = \ldots = a_k = a$. Es folgt, dass a^m und b teilerfremd sind. Nun verwenden wir wieder Teil 4, diesmal mit $c = a^m$, $k = n$ und $a_1 = \ldots = a_k = b$. Also sind auch a^m und b^n teilerfremd. □

Satz 1.4.16. *Es sei $q \in \mathbb{Q}$. Dann gibt es eindeutig bestimmte $a \in \mathbb{Z}$, $b \in \mathbb{N}^+$ mit $q = a/b$ und $\mathrm{ggT}(a, b) = 1$ (gekürzte Bruchdarstellung von q).*

Beweis. Existenz von a, b: Zunächst gibt es a', $b' \in \mathbb{Z}$, $b' \neq 0$ mit $q = a'/b'$. Ist $b' < 0$ so ersetzen wir a' durch $-a'$ und b' durch $-b'$. Wir können daher $b' \in \mathbb{N}^+$ annehmen. Wir setzen nun $d = \mathrm{ggT}(a', b')$. Dann gelten $d \mid a'$ und $d \mid b'$. Also gibt es a, $b \in \mathbb{Z}$ mit $a' = ad$ und $b' = bd$. Wegen d, $b' \in \mathbb{N}^+$ ist dann auch $b \in \mathbb{N}^+$. Nach 1.4.15.1 gilt dann $\mathrm{ggT}(a, b) = \mathrm{ggT}(a'/d, b'/d) = 1$. Weiters ist $q = a'/b' = (ad)/(bd) = a/b$.

Eindeutigkeit von a und b: Seien a, $a' \in \mathbb{Z}$, b, $b' \in \mathbb{N}^+$ mit $a/b = q = a'/b'$ und $\mathrm{ggT}(a,b) = 1 = \mathrm{ggT}(a',b')$. Wir zeigen $a = a'$ und $b = b'$. Aus $a/b = q = a'/b'$ folgt $ab' = a'b$. Inbesondere gelten $b \mid ab'$ und $b' \mid a'b$. Wegen $\mathrm{ggT}(a,b) = 1 = \mathrm{ggT}(a',b')$ erhalten wir nach 1.4.15.2 $b \mid b'$ und $b' \mid b$. Es folgt $|b| = |b'|$ aus 1.3.3.8. Wegen b, $b' \in \mathbb{N}^+$ erhalten wir $b = b'$. Aus $ab = ab' = a'b$ folgt nun auch $a = a'$. □

Satz 1.4.17. *Seien $n \in \mathbb{N}^+$, $a_0, \ldots, a_n \in \mathbb{Z}$ mit $a_n \neq 0$. Sei $q \in \mathbb{Q}$ eine Nullstelle des Polynoms $a_nX^n + \ldots + a_1X + a_0$ und $q = a/b$ die gekürzte Bruchdarstellung von q. Dann gelten $b \mid a_n$ und $a \mid a_0$.*

Beweis. Wir multiplizieren die Gleichung

$$0 = \sum_{k=0}^{n} a_k q^k = \sum_{k=0}^{n} a_k \frac{a^k}{b^k}$$

mit b^n und erhalten

$$0 = \sum_{k=0}^{n} a_k a^k b^{n-k} \quad .$$

Nun folgt aus

$$0 = \sum_{k=0}^{n} a_k a^k b^{n-k} = a_n a^n + \sum_{k=0}^{n-1} a_k a^k b^{n-k} = a_n a^n + b \sum_{k=0}^{n-1} a_k a^k b^{n-1-k}$$

$b \mid a_n a^n$. Nach 1.4.15.5 gilt $\mathrm{ggT}(a^n, b) = 1$, woraus nach 1.4.15.2 $b \mid a_n$ folgt.

Analog zeigen wir $a \mid a_0$. Aus

$$0 = \sum_{k=0}^{n} a_k a^k b^{n-k} = a_0 b^n + \sum_{k=1}^{n} a_k a^k b^{n-k} = a_0 b^n + a \sum_{k=1}^{n} a_k a^{k-1} b^{n-k}$$

folgt $a \mid a_0 b^n$. Wegen $\mathrm{ggT}(a, b^n) = 1$ (1.4.15.5) folgt $a \mid a_0$ (1.4.15.2). □

Beispiel 1.4.18. Wir bestimmen alle $q \in \mathbb{Q}$, die Nullstellen des Polynoms $P = 3X^3 + 4X^2 - 5X - 2$ sind. Sei dazu $q \in \mathbb{Q}$ eine Nullstelle von P und sei $q = a/b$ die gekürzte Bruchdarstellung von q. Anwendung von 1.4.17 liefert $a \mid -2$ und $b \mid 3$. Es folgt $a \in \{\pm 1, \pm 2\}$ und $b \in \{1, 3\}$ und damit

$$q \in \{\pm 1, \pm 2, \pm\frac{1}{3}, \pm\frac{2}{3}\} \quad .$$

Wir haben also nur mehr endlich viele Möglichkeiten für q. Einsetzen liefert

$$P(1) = P(-2) = P(-\frac{1}{3}) = 0 \quad .$$

Wegen $\mathrm{grad}(P) = 3$, sind also 1, -2, $-1/3$ alle Nullstellen von P.

Satz 1.4.19. *Seien $m \in \mathbb{N}^+$ und $n \in \mathbb{N}^+$, sodass m keine n-te Potenz in $\mathbb{Z}$ ist (also $m \neq a^n$ für alle $a \in \mathbb{Z}$). Dann ist $\sqrt[n]{m}$ irrational.*

Beweis. Angenommen $\sqrt[n]{m} \in \mathbb{Q}$. Es sei $\sqrt[n]{m} = a/b$ die gekürzte Bruchdarstellung von $\sqrt[n]{m}$. Nun ist $\sqrt[n]{m}$ Nullstelle von $X^n - m$. Nach 1.4.17 folgt $b \mid 1$, also $b = 1$ (wegen $b \in \mathbb{N}^+$). Es folgt $\sqrt[n]{m} = a \in \mathbb{Z}$, also $m = a^n$, Widerspruch. □

1.5. **Das kleinste gemeinsame Vielfache.**

Definition 1.5.1. Sei $a \in \mathbb{Z} \setminus \{0\}$. Wir bezeichnen mit

$$V(a) = \{v \in \mathbb{N}^+ \mid a \mid v\}$$

die Menge aller echt positiven Vielfachen von a. Es ist dann also

$$V(a) = \mathbb{N}^+|a| = \{k|a| \mid k \in \mathbb{N}^+\} \quad .$$

1.5.2. Seien $k \in \mathbb{N}^+$ und $a_1, \ldots, a_k \in \mathbb{Z} \setminus \{0\}$. Für alle $i = 1, \ldots, k$ gilt dann $a_i \mid |a_1 \ldots a_k|$. Also ist $|a_1 \ldots a_k| \in V(a_1) \cap \ldots \cap V(a_k)$. Inbesondere ist $V(a_1) \cap \ldots \cap V(a_k) \neq \emptyset$. Daher besitzt $V(a_1) \cap \ldots \cap V(a_k)$ ein kleinstes Element. Die folgende Definition ist also sinnvoll.

Definition 1.5.3. Seien $k \in \mathbb{N}^+$ und $a_1, \ldots, a_k \in \mathbb{Z} \setminus \{0\}$. Dann heißt

$$\mathrm{kgV}(a_1, \ldots, a_k) := \min(V(a_1) \cap \ldots \cap V(a_k))$$

das kleinste gemeinsame Vielfache von $a_1, \ldots, a_k$.

1.5.4. Wie bestimmt man nun das kleinste gemeinsame Vielfache von k ganzen Zahlen ungleich Null? Wir beweisen dazu drei Sätze. Der erste (1.5.5) entspricht der Charakterisierung $1 \iff 3$ in Satz 1.4.9 des größten gemeinsamen Teilers. Dies benutzen wir dann um eine rekursive Darstellung des kgV zu geben (1.5.6), welche derjenigen des ggT entspricht (1.4.12). Diese rekursive Darstellung des kgV's führt das Problem darauf zurück, das kgV von zwei ganzen Zahlen zu berechnen. Dieses Problem wird dann in 1.5.7 auf die Bestimmung des ggT's zweier Zahlen zurück geführt.

Satz 1.5.5. *Seien $k \in \mathbb{N}^+$, $a_1, \ldots, a_k \in \mathbb{Z} \setminus \{0\}$ und $v \in \mathbb{N}^+$. Dann sind äquivalent:*

1. $v = \mathrm{kgV}(a_1, \ldots, a_k)$.
2. *Für alle $i = 1, \ldots, k$ gilt $a_i \mid v$ und ist $w \in \mathbb{N}^+$ mit $a_i \mid w$ für alle $i = 1, \ldots, k$, so gilt $v \mid w$ (also in Worten: v ist ein gemeinsames Vielfaches der a_i und jedes gemeinsame Vielfache der a_i ist ein Vielfaches von v).*

Beweis. $1 \Rightarrow 2$. Sei also $v = \mathrm{kgV}(a_1, \ldots, a_k)$. Dann ist v nach Definition ein Vielfaches aller a_i, also gilt $a_i \mid v$ für alle $i = 1, \ldots, k$. Sei nun $w \in \mathbb{N}^+$ mit $a_i \mid w$ für alle $i = 1, \ldots, k$. Wir müssen $v \mid w$ zeigen. Angenommen dies ist falsch. Wir dividieren w mit Rest durch v: $w = kv + r$ mit $r \in \{1, \ldots, v-1\}$. Sei $1 \leq i \leq k$. Aus $a_i \mid v$ und $a_i \mid w$ folgt $a_i \mid w - kv = r$ aus 1.3.3.5. Also ist $r \in \mathbb{N}^+$ ein gemeinsames Vielfaches der a_i. Da v das kleinste gemeinsame Vielfache der a_i ist, erhalten wir $v \leq r$. Dies widerspricht aber $r \leq v - 1$.

$2 \Rightarrow 1$. Habe nun v die Eigenschaft 2. Es sei $v' = \mathrm{kgV}(a_1, \ldots, a_k)$. Da wir die Implikation $1 \Rightarrow 2$ schon bewiesen haben, wissen wir, dass auch v' die Eigenschaft 2 hat (wenn wir in

2 v durch v' ersetzen). Wegen $a_i \mid v$ für alle $i = 1, \ldots, k$ folgt $v' \mid v$, da v' die Eigenschaft 2 hat. Wegen $a_i \mid v'$ für alle $i = 1, \ldots, k$ folgt $v \mid v'$, da v nach Voraussetzung die Eigenschaft 2 hat. Also ist $|v| = |v'|$ und damit $v = v'$. □

Satz 1.5.6. *Seien $k \in \mathbb{N}_{\geq 2}$, $a_1, \ldots, a_k \in \mathbb{Z} \setminus \{0\}$ und $v' = \mathrm{kgV}(a_1, \ldots, a_{k-1})$. Dann gilt* $\mathrm{kgV}(a_1, \ldots, a_k) = \mathrm{kgV}(v', a_k)$.

Beweis. Wir setzen $v = \mathrm{kgV}(v', a_k)$ und zeigen, dass v die Eigenschaft 2 aus 1.5.5 besitzt. Nach Definition gilt zunächst $a_k \mid v$. Sei $1 \leq i \leq k-1$. Dann gelten $a_i \mid v'$ und $v' \mid v$, woraus $a_i \mid v$ folgt.

Sei nun $w \in \mathbb{N}^+$ mit $a_i \mid w$ für alle $i = 1, \ldots, k$. Wir müssen $v \mid w$ zeigen. Wegen $v' = \mathrm{kgV}(a_1, \ldots, a_{k-1})$ und $a_i \mid w$, $i = 1, \ldots k-1$ gilt $v' \mid w$ nach 1.5.5. Also gilt $v' \mid w$ und $a_k \mid w$. Nochmalige Anwendung von 1.5.5 liefert $v \mid w$. □

Satz 1.5.7. *Seien a, $b \in \mathbb{Z} \setminus \{0\}$. Dann gilt*

$$\mathrm{kgV}(a, b) = \frac{|ab|}{\mathrm{ggT}(a, b)} \quad .$$

Beweis. Wir setzen $d = \mathrm{ggT}(a, b) \in \mathbb{N}^+$. Wegen $d \mid a$ (also auch $d \mid |a|$) gilt

$$v := |ab|/d = (|a|/d)|b| \in \mathbb{N}^+ \quad .$$

Wir zeigen, dass v die Eigenschaft 2 aus 1.5.5 besitzt.

Wegen $d \mid a$ und $d \mid b$ gelten $|a|/d \in \mathbb{Z}$ und $|b|/d \in \mathbb{Z}$. Aus

$$v = \frac{|ab|}{d} = |a|\frac{|b|}{d} = |b|\frac{|a|}{d}$$

folgen $a \mid v$ und $b \mid v$. Sei nun $w \in \mathbb{N}^+$ mit $a \mid w$ und $b \mid w$. Wegen $d \mid a$, $d \mid b$ gilt auch $d \mid w$ und daher gelten a/d, w/d, $b/d \in \mathbb{Z}$. Aus $(a/d)d = a \mid w = (w/d)d$ folgt nach 1.3.3.6 $a/d \mid w/d$. Ersetzt man in dieser Überlegung a durch b, so folgt auch $b/d \mid w/d$. Nach 1.4.15.1 gilt $\mathrm{ggT}(a/d, b/d) = 1$. Wegen $a/d \mid w/d$ und $b/d \mid w/d$, folgt aus 1.4.15.3 auch $(a/d)(b/d) \mid w/d$. Wir wenden nocheinmal 1.3.3.6 an und erhalten $(ab)/d \mid w$, also auch $v = |ab|/d \mid w$. □

Beispiel 1.5.8. Wir bestimmen $\mathrm{kgV}(102, 153, 136)$. Dazu bestimmen wir mit Hilfe von 1.5.7 $\mathrm{kgV}(102, 153)$. Wir berechnen zunächst $\mathrm{ggT}(102, 153)$. Es ist

$$153 = 1 \cdot 102 + 51, \quad 102 = 2 \cdot 51 + 0 \quad .$$

Also ist $51 = \mathrm{ggT}(102, 153)$ und damit

$$\mathrm{kgV}(102, 153) = \frac{102 \cdot 153}{51} = 2 \cdot 153 = 306 \quad .$$

Nun müssen wir nur noch $\mathrm{kgV}(306, 136)$ bestimmen. Aus

$$306 = 2 \cdot 136 + 34, \quad 136 = 4 \cdot 34 + 0$$

folgt $34 = \mathrm{ggT}(306, 136)$ und damit

$$\mathrm{kgV}(102, 153, 136) = \mathrm{kgV}(306, 136) = \frac{306 \cdot 136}{34} = 306 \cdot 4 = 1224 \quad .$$

2. Primzahlen

2.1. Der Fundamentalsatz der Arithmetik.

Definition 2.1.1. $p \in \mathbb{N}^+$ heißt Primzahl, falls $p \neq 1$ ist und falls $T(p) = \{1, p\}$ gilt (Erinnerung: für $a \in \mathbb{Z}$ ist $T(a) = \{t \in \mathbb{N}^+ \mid t \mid a\}$, siehe 1.4.1).

Wir bezeichnen mit $\mathbb{P}$ die Menge aller Primzahlen.

Lemma 2.1.2. *Seien $p \in \mathbb{P}$ und $a \in \mathbb{Z}$. Dann gilt*

$$\mathrm{ggT}(a, p) = \begin{cases} p & \text{falls } p \mid a \\ 1 & \text{falls } p \nmid a \end{cases} \quad .$$

Beweis. Gelte einmal $p \mid a$. Dann folgt

$$T(p) = \{1, p\} \subset T(a) \cap T(p) \subset T(p) \quad .$$

Also ist $T(a) \cap T(p) = \{1, p\}$ und daher $\mathrm{ggT}(a, p) = p$.

Es gelte nun $p \nmid a$. Wegen

$$\{1\} \subset T(a) \cap T(p) \subset T(p) = \{1, p\}$$

und $p \notin T(a) \cap T(p)$ folgt $T(a) \cap T(p) = \{1\}$ und daher ist $\mathrm{ggT}(a, p) = 1$. □

Satz 2.1.3. *Sei $p \in \mathbb{N}$ mit $p \geq 2$. Dann ist p genau dann eine Primzahl, wenn für alle a, $b \in \mathbb{Z}$ gilt: $p \mid ab \Rightarrow p \mid a$ oder $p \mid b$.*

Beweis. Sei einmal p eine Primzahl und a, $b \in \mathbb{Z}$ mit $p \mid ab$. Wir zeigen $p \mid a$ oder $p \mid b$. Falls $p \mid a$ gilt, sind wir fertig. Wir können daher $p \nmid a$ annehmen und müssen nun $p \mid b$ zeigen. Nach Lemma 2.1.2 gilt aber

$$p \mid ab \quad \text{und} \quad \mathrm{ggT}(p, a) = 1 \quad .$$

Daher folgt $p \mid b$ aus 1.4.15.2.

Gelte nun umgekehrt $p \mid ab \Rightarrow p \mid a$ oder $p \mid b$ für alle a, $b \in \mathbb{Z}$. Wir zeigen, dass p eine Primzahl ist. Wegen $p \geq 2$ ist $p \neq 1$. Sei nun $t \in T(p)$. Dann gibt es $u \in \mathbb{N}^+$ mit $p = tu$. Es folgt $p \mid p = tu$. Nach Voraussetzung folgt $p \mid t$ oder $p \mid u$.

1. Fall: $p \mid t$. Dann gilt $p \mid t$ und $t \mid p$, woraus (beachte t, $p \in \mathbb{N}^+$) $t = p$ folgt.

2. Fall: $p \mid u$. Wegen $tu = p$, gilt $u \mid p$. Wie eben folgt jetzt $u = p$. Aus $tp = tu = p$ erhalten wir $t = 1$.

Wir haben nun $T(p) \subset \{1, p\}$ gezeigt. Da die inverse Inklusion trivial ist, folgt $T(p) = \{1, p\}$. Daher ist p eine Primzahl. □

Korollar 2.1.4. *Seien $p \in \mathbb{P}$, $k \in \mathbb{N}^+$ und $a_1, \ldots, a_k \in \mathbb{Z}$ mit $p \mid a_1 \ldots a_k$. Dann gibt es ein $i \in \{1, \ldots, k\}$ mit $p \mid a_i$.*

Beweis. Wir machen eine Induktion nach k. Für $k = 1$ ist die Aussage trivial. Sei nun $k \geq 2$ und die Aussage gelte für $k-1$. Wir zeigen, dass sie dann auch für k zutrifft. Seien also $a_1, \ldots, a_k \in \mathbb{Z}$ mit $p \mid a_1 \ldots a_k = (a_1 \ldots a_{k-1})a_k$. Nach Satz 2.1.3 folgt $p \mid a_1 \ldots a_{k-1}$ oder $p \mid a_k$. Gilt $p \mid a_k$ so sind wir fertig. Wir können daher $p \mid a_1 \ldots a_{k-1}$ annehmen. Dann gibt es nach Induktionsvoraussetzung ein $i \in \{1, \ldots, k-1\}$ mit $p \mid a_i$ und wir sind ebenfalls fertig. □

Satz 2.1.5. *Sei $n \in \mathbb{N}$ mit $n \geq 2$. Dann ist n ein Produkt (eventuell mit nur einem Faktor) von Primzahlen und diese Darstellung von n als Produkt von Primzahlen ist bis auf die Reihenfolge der Faktoren eindeutig (Fundamentalsatz der Arithmetik).*

Beweis. Wir zeigen zunächst die Existenz. Wir benutzen dazu eine Induktion. Wir nehmen also an, dass jedes $m \in \mathbb{N}$ mit $2 \leq m < n$ ein Produkt von Primzahlen ist, und zeigen, dass dies auch für n zutrifft.

Ist n schon selbst eine Primzahl, so ist die Aussage klar. Wir können also annehmen, dass n keine Primzahl ist. Dann gibt es $t \in T(n)$ mit $1 < t < n$. Sei $u \in \mathbb{N}^+$ mit $tu = n$. Wegen $1 < t < n$ ist $2 \leq t < n$. Aus $1 < t < n$ und $n = tu$ folgt $1 < u < n$, also $2 \leq u < n$. Nach Induktionsvoraussetzung sind daher t und u Produkte von Primzahlen. Wegen $n = tu$ ist auch n ein Produkt von Primzahlen.

Eindeutigkeit: Seien $s, t \in \mathbb{N}^+$ und $p_1, \ldots, p_s, q_1, \ldots, q_t \in \mathbb{P}$ mit $p_1 \ldots p_s = n = q_1 \ldots q_t$. Wir müssen zeigen, dass $s = t$ gilt, und dass nach eventueller Umnummerierung der q_j $p_i = q_i$, $i = 1, \ldots, s$ gilt.

Wir benutzen dazu wieder eine Induktion nach n, nehmen also an, dass die Aussage für alle $2 \leq m < n$ gilt.

1.Fall $s = 1$: Dann ist $n = p_1 = q_1 \ldots q_t$. Es folgt $1 \neq q_1 \in T(p_1) = \{1, p_1\}$, also $p_1 = q_1$. Dann folgt $1 = q_2 \ldots q_t$. Wegen $q_i \geq 2$ für alle $i = 2, \ldots t$, folgt $t - 1 = 0$, also $t = 1$ und wir sind fertig.

2.Fall $s \geq 2$: Wegen $p_1 \mid p_1 \ldots p_s = n = q_1 \ldots q_t$ und 2.1.4, gibt es ein $1 \leq j \leq t$ mit $p_1 \mid q_j$. Nach einer eventuellen Umnummerierung der q_k, können wir $j = 1$, also $p_1 \mid q_1$ annehmen. Dann folgt $1 \neq p_1 \in T(q_1) = \{1, q_1\}$, also $p_1 = q_1$. Wir setzen nun $m = n/p_1 = n/q_1 = p_2 \ldots p_s = q_2 \ldots q_t$. Dann ist $m < n$ (wegen $p_1 > 1$) und $m \geq 2$ (wegen $m = p_2 \ldots p_s$, $p_2 \geq 2$ und $s \geq 2$). Nach Induktionsvoraussetzung (angewandt auf m) folgt $s - 1 = t - 1$ (also $s = t$) und nach eventueller Umnummerierung der $q_2, \ldots q_s$ $p_i = q_i$ für $i = 2, \ldots s$. □

2.2. **Die Verteilung der Primzahlen.**

Satz 2.2.1. *Es gibt unendlich viele Primzahlen.*

Beweis. Angenommen $\mathbb{P}$ sei endlich, etwa $\mathbb{P} = \{p_1, \ldots, p_k\}$. Wegen $2 \in \mathbb{P}$ ist $k \geq 1$. Setze $n = p_1 \ldots p_k + 1$. Wegen $k \geq 1$ und $p_i \geq 2$, $i = 1, \ldots, k$ ist $n \geq 3$. Nach 2.1.5 wird n daher von einer Primzahl geteilt. Also gibt es $1 \leq i \leq k$ mit $p_i \mid n$. Wegen $p_i \mid p_1 \ldots p_k$ folgt auch $p_i \mid n - p_1 \ldots p_k = 1$. Also ist $p_i = 1$, Widerspruch. □

Definition 2.2.2. Sei $n \in \mathbb{N}$ mit $n \geq 2$. Dann ist $n \in T(n)\backslash\{1\}$ und daher $T(n)\backslash\{1\} \neq \emptyset$. Wir setzen $p(n) = \min(T(n) \setminus \{1\})$. $p(n)$ ist also die kleinste natürliche Zahl, die n teilt und grösser oder gleich 2 ist.

Lemma 2.2.3. *Sei $n \in \mathbb{N}$ mit $n \geq 2$. Dann gelten:*

1. *$p(n)$ ist eine Primzahl. Insbesondere ist $p(n)$ die kleinste Primzahl, die n teilt.*
2. *Ist n keine Primzahl, so gilt $p(n) \leq \sqrt{n}$.*
3. *Sei $x \in \mathbb{R}^+$ mit $\sqrt{x} < n \leq x$. n ist genau dann eine Primzahl, wenn n von keiner Primzahl $\leq \sqrt{x}$ geteilt wird.*

Beweis. 1. Angenommen $p(n)$ ist keine Primzahl. Wegen $p(n) \geq 2$, gibt es dann ein $t \in \mathbb{N}$ mit $1 < t < p(n)$ und $t \mid p(n)$. Wegen $p(n) \mid n$, folgt $2 \leq t$ und $t \mid n$. Daher ist $t \geq p(n)$ (da $p(n)$ der kleinste Teiler ≥ 2 von n ist), was $t < p(n)$ widerspricht.

2. Wegen $p(n) \mid n$ ist $n = p(n)m$ mit $m \in \mathbb{N}^+$. Nach Vorausetzung ist n keine Primzahl. Aus 1 folgt $m \geq 2$. Daher gilt $m \in T(n) \setminus \{1\}$. Inbesondere ist $m \geq p(n)$. Wir erhalten $n = p(n)m \geq p(n)^2$, woraus $p(n) \leq \sqrt{n}$ folgt.

3. Sei einmal n eine Primzahl. Wegen $\sqrt{x} < n$ wird dann n von keiner Primzahl $\leq \sqrt{x}$ geteilt.

Gelte nun umgekehrt, dass n von keiner Primzahl $\leq \sqrt{x}$ geteilt wird. Angenommen n ist keine Primzahl. Nach Voraussetzung und wegen 1 gilt $p(n) > \sqrt{x}$. Aus 2 folgt aber: $p(n) \leq \sqrt{n} \leq \sqrt{x}$, Widerspruch. □

2.2.4. Sei $x \in \mathbb{R}^+$. Wir erhalten nun folgendes Verfahren, alle Primzahlen in $(\sqrt{x}, x]$ zu bestimmen, falls die Primzahlen $\leq \sqrt{x}$ schon bekannt sind: Wir schreiben alle $n \in \mathbb{N}$ mit $\sqrt{x} < n \leq x$ auf. Aus dieser Liste streichen wir alle Zahlen der Form pk wobei p eine Primzahl $\leq \sqrt{x}$ ist und wobei $k \in \mathbb{N}$ mit $k \geq 2$ ist (also alle echten Vielfachen aller Primzahlen $\leq \sqrt{x}$). Nach 2.2.3.3 bleiben genau die Primzahlen in $(\sqrt{x}, x]$ übrig (Sieb des Eratosthenes).

Beispiel 2.2.5. Durch direktes Ausprobieren (oder Schulwissen) erhält man, dass 2, 3, 5, 7 genau die Menge Primzahlen ≤ 10 ist. Mit Hilfe des Siebs von Eratosthenes (mit $x = 100$) können wir nun auch die Primzahlen ≤ 100 bestimmen. Wir schreiben zunächst die natürlichen Zahlen in $(10, 100]$ auf:

11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

und streichen dann alle echten Vielfachen von 2, 3, 5, 7. Übrig bleibt

11	13	17	19
	23		29
31		37	
41	43	47	
	53		59
61		67	
71	73		79
	83		89
		97	

Es folgt, dass

$$\{2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97\}$$

die Menge aller Primzahlen ≤ 100 ist.

2.2.6. Für $x \in \mathbb{R}^+$ sei $\pi(x)$ die Anzahl aller Primzahlen $\leq x$. Es ist also zum Beispiel $\pi(10) = 4$ und $\pi(100) = 25$. Über $\pi(x)$ gilt der folgende Satz, den wir hier nicht beweisen können (einen Beweis findet man zum Beispiel in Kapitel 7 in P. Bundschuh, Einführung in die Zahlentheorie, Springer).

Satz 2.2.7. *$\pi(x)$ ist asymptotisch gleich $x/\log(x)$, d.h.*

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

Dabei ist log *der natürliche Logarithmus.*

Satz 2.2.8. *Für alle $k \in \mathbb{N}^+$ gibt es ein $N \in \mathbb{N}^+$, sodass $[N+1, N+k] \cap \mathbb{P} = \emptyset$ ist. Interpretation: $\mathbb{P}$ hat beliebig lange Lücken.*

Beweis. Sei also $k \in \mathbb{N}^+$. Wir setzen $N = (k+1)! + 1$ und zeigen, dass jedes $n \in \mathbb{N} \cap [N+1, N+k]$ keine Primzahl ist. Sei dazu $n \in \mathbb{N} \cap [N+1, N+k]$. Dann gilt $n = N + j = (k+1)! + j + 1$ mit einem $1 \leq j \leq k$.

Wegen $j \leq k$ gilt $j + 1 \mid (k+1)!$, also auch $j + 1 \mid (k+1)! + j + 1 = n$. Wegen $j \geq 1$ ist $j + 1 > 1$. Schließlich ist $j + 1 < (k+1)! + j + 1 = n$. Also ist n keine Primzahl. □

2.2.9. Lange Lücken treten früher auf, als bei dem im Beweis von 2.2.8 konstruierten N. Zum Beispiel folgen auf

$$p = 2614941710599 \in \mathbb{P}$$

651 Nicht-Primzahlen. Aber $N = 652! + 1 \sim 3 \cdot 10^{1553}$.

2.2.10. Man kann auch nach möglichst kurzen Lücken fragen: Ein Paar (p, q) von Primzahlen p, q heißt Primzahlzwilling, falls $q = p + 2$ ist. Zum Beispiel sind

$$(3, 5), (5, 7), (11, 13), (17, 19), (29, 31), (41, 43)$$

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

2.3. **Teilbarkeit und Primfaktorzerlegung.**

2.3.1. Sei $z \in \mathbb{Z} \setminus \{0\}$ und es sei $|z| = p_1 \dots p_r$ die Primfaktorzerlegung von $|z|$, also $p_1, \dots, p_r \in \mathbb{P}$ (dabei sei $r = 0$, falls $|z| = 1$ ist).

Für $p \in \mathbb{P}$ sei $v_p(z)$ die Mächtigkeit von $\{1 \leq i \leq r \mid p_i = p\}$ ($v_p(z)$ zählt also wie oft p in der Primfaktorzerlegung von $|z|$ vorkommt).

Beispiel 2.3.2. Sei $z = -26936$. Dann gilt

$$|z| = 26936 = 2 \cdot 2 \cdot 2 \cdot 7 \cdot 13 \cdot 37 \quad .$$

Also gelten:

$$v_2(z) = 3,\ v_7(z) = v_{13}(z) = v_{37}(z) = 1,\ v_p(z) = 0 \quad \text{für} \quad p \in \mathbb{P} \setminus \{2, 7, 13, 37\} \quad .$$

Satz 2.3.3. *Sei $z \in \mathbb{Z} \setminus \{0\}$. Dann gilt $v_p(z) = 0$ für fast alle $p \in \mathbb{P}$ (d.h. bis auf endlich viele $p \in \mathbb{P}$) und es ist*

$$z = \operatorname{sgn}(z) \prod_{p \in \mathbb{P}} p^{v_p(z)} \quad .$$

Dabei ist $\operatorname{sgn}(z) = 1$, falls $z > 0$ und $\operatorname{sgn}(z) = -1$ falls $z < 0$.

Bemerkung: Wegen $v_p(z) = 0$ sind in dem obigen, zunächst unendlichen Produkt bis auf endlich viele Faktoren alle 1. Daher ist dieses Produkt definiert.

Umgekehrt: Für $p \in \mathbb{P}$ sei $v_p \in \mathbb{N}$ mit $v_p = 0$ für fast alle $p \in \mathbb{P}$ und es sei $\varepsilon \in \{-1, 1\}$. Setzt man

$$z = \varepsilon \prod_{p \in \mathbb{P}} p^{v_p} \quad ,$$

so gilt $v_p(z) = v_p$ für alle $p \in \mathbb{P}$.

Beweis. Sei $|z| = q_1 \dots q_r$ die Primfaktorzerlegung von $|z|$. Weiters seien $p_1, \dots, p_s$ die paarweise verschiedenen Primzahlen, die in $(q_1, \dots, q_r)$ vorkommen. Dann ist

$$|z| = q_1 \dots q_r = p_1^{v_{p_1}(z)} \dots p_s^{v_{p_s}(z)} = \prod_{p \in \{p_1, \dots, p_s\}} p^{v_p(z)} \quad .$$

Wegen $v_p(z) = 0$ für $p \in \mathbb{P} \setminus \{p_1, \dots, p_s\}$ ist das letzte Produkt gleich

$$\prod_{p \in \mathbb{P}} p^{v_p(z)} \quad .$$

Damit folgt

$$z = \operatorname{sgn}(z)|z| = \operatorname{sgn}(z) \prod_{p \in \mathbb{P}} p^{v_p(z)} \quad .$$

Seien nun umgekehrt für $p \in \mathbb{P}$ $v_p \in \mathbb{N}$ mit $v_p = 0$ für fast alle $p \in \mathbb{P}$ und sei $\varepsilon \in \{-1, 1, \}$. Wir setzen

$$z = \varepsilon \prod_{p \in \mathbb{P}} p^{v_p} \quad .$$

Es seien $p_1,\ldots,p_s$ die paarweise verschiedenen Primzahlen p mit $v_p > 0$. Dann gilt

$$|z| = \prod_{i=1}^{s} p_i^{v_{p_i}} = \overbrace{p_1 \ldots p_1}^{v_{p_1}} \ldots\ldots \overbrace{p_s \ldots p_s}^{v_{p_s}} \quad ,$$

woraus die Behauptung folgt. □

Satz 2.3.4. *Seien z, $w \in \mathbb{Z} \setminus \{0\}$. Dann gelten:*

1. $v_p(zw) = v_p(z) + v_p(w)$ *für alle* $p \in \mathbb{P}$.
2. $z \mid w \iff v_p(z) \leq v_p(w)$ *für alle* $p \in \mathbb{P}$.
3. $v_p(z) = \max\{k \in \mathbb{N} \mid p^k \mid z\}$ *für alle* $p \in \mathbb{P}$. *Insbesondere gilt* $v_p(z) = 0 \iff p \nmid z$ *für alle* $p \in \mathbb{P}$.

Beweis. 1. Kommt p in der Primfaktorzerlegung von z k mal und in der von w l mal vor, so kommt p in der Primfaktorzerlegungt von zw $k+l$ vor. Dies ist genau die Aussage in 1.

2. Es gelte einmal $z \mid w$. Dann ist $w = zu$ mit einem $u \in \mathbb{Z}$. Wegen $w \neq 0$ ist auch $u \neq 0$. Es folgt $v_p(w) = v_p(zu) = v_p(z) + v_p(u) \geq v_p(z)$.

Umgekehrt gelte nun $v_p(z) \leq v_p(w)$ für alle $p \in \mathbb{P}$. Wir setzen $a_p = v_p(w) - v_p(z) \in \mathbb{N}$ für alle $p \in \mathbb{P}$. Wegen $v_p(z) = 0$ für fast alle $p \in \mathbb{P}$ und $v_p(w) = 0$ für fast alle $p \in \mathbb{P}$ ist auch $a_p = 0$ für fast alle $p \in \mathbb{P}$. Daher können wir

$$a := \prod_{p \in \mathbb{P}} p^{a_p} \in \mathbb{N}^+$$

definieren.

Es folgt

$$|w| = \prod_{p \in \mathbb{P}} p^{v_p(w)} = \prod_{p \in \mathbb{P}} p^{a_p + v_p(z)} = \prod_{p \in \mathbb{P}} p^{a_p} p^{v_p(z)} = \prod_{p \in \mathbb{P}} p^{a_p} \prod_{p \in \mathbb{P}} p^{v_p(z)} = a|z| \quad .$$

Also gilt $|z| \mid |w|$ und damit auch $z \mid w$.

3. Sei $p \in \mathbb{P}$. Für alle $k \in \mathbb{N}$ ist $v_p(p^k) = k$ und $v_q(p^k) = 0$ für $q \in \mathbb{P}$, $q \neq p$. Also gilt nach 2 für alle $k \in \mathbb{N}$: $p^k \mid z \iff k = v_p(p^k) \leq v_p(z)$. Die Behauptung folgt. □

Satz 2.3.5. *Seien $k \in \mathbb{N}^+$ und $a_1,\ldots,a_k \in \mathbb{Z} \setminus \{0\}$. Für $p \in \mathbb{P}$ setzen wir*

$$m_p = \min\{v_p(a_1), \ldots, v_p(a_k)\}, \quad M_p = \max\{v_p(a_1), \ldots, v_p(a_k)\} \quad .$$

Dann ist $m_p = 0$ für fast alle $p \in \mathbb{P}$ und auch $M_p = 0$ für fast alle $p \in \mathbb{P}$ und es gelten

$$\mathrm{ggT}(a_1, \ldots, a_k) = \prod_{p \in \mathbb{P}} p^{m_p}, \quad \mathrm{kgV}(a_1, \ldots, a_k) = \prod_{p \in \mathbb{P}} p^{M_p} \quad .$$

Beweis. Für $i = 1, \ldots, k$ sei P_i die Menge aller $p \in \mathbb{P}$ mit $v_p(a_i) > 0$ (d.h. $p \mid a_i$). Dann ist auch $P_1 \cup \ldots \cup P_k$ endlich. Für $p \in \mathbb{P} \setminus (P_1 \cup \ldots \cup P_k)$ ist dann $v_p(a_i) = 0$ für $i = 1, \ldots, k$. Es folgt $M_p = m_p = 0$ für alle $p \in \mathbb{P} \setminus (P_1 \cup \ldots \cup P_k)$.

Wir setzen nun

$$d := \prod_{p \in \mathbb{P}} p^{m_p} \in \mathbb{N}^+ \quad .$$

und zeigen $d = \mathrm{ggT}(a_1, \ldots, a_k)$. Wir zeigen dazu zunächst $d \mid a_i$ für alle $i = 1, \ldots, k$. Sei also $1 \leq i \leq k$. Dann gilt für alle $p \in \mathbb{P}$:

$$v_p(d) = m_p = \min\{v_p(a_1), \ldots, v_p(a_k)\} \leq v_p(a_i) \quad .$$

Aus 2.3.4.2 folgt $d \mid a_i$. Daher gilt $d \mid \mathrm{ggT}(a_1, \ldots, a_k)$.

Umgekehrt: Für alle $p \in \mathbb{P}$ und alle $1 \leq i \leq k$ gilt wegen $\mathrm{ggT}(a_1, \ldots, a_k) \mid a_i$:

$$v_p(\mathrm{ggT}(a_1, \ldots, a_k)) \leq v_p(a_i) \quad .$$

Also ist für jedes $p \in \mathbb{P}$

$$v_p(\mathrm{ggT}(a_1, \ldots, a_k)) \leq \min\{v_p(a_1), \ldots, v_p(a_k)\} = m_p = v_p(d) \quad .$$

Wiederum aus 2.3.4.2 folgt $\mathrm{ggT}(a_1, \ldots, a_k) \mid d$. Also gilt $d = \mathrm{ggT}(a_1, \ldots, a_k)$.

Schließlich setzen wir

$$w = \prod_{p \in \mathbb{P}} p^{M_p}$$

und zeigen ganz analog $w = \mathrm{kgV}(a_1, \ldots, a_k)$. Sei $1 \leq i \leq k$ und $p \in \mathbb{P}$. Wegen

$$v_p(w) = M_p = \max\{v_p(a_1), \ldots, v_p(a_k)\} \geq v_p(a_i)$$

folgt aus 2.3.4.2 $a_i \mid w$ für $i = 1, \ldots, k$, also $\mathrm{kgV}(a_1, \ldots, a_k) \mid w$.

Umgekehrt: Für alle $p \in \mathbb{P}$ und alle $i = 1, \ldots, k$ gilt wegen $a_i \mid \mathrm{kgV}(a_1, \ldots, a_k)$:

$$v_p(a_i) \leq v_p(\mathrm{kgV}(a_1, \ldots, a_k)) \quad .$$

Also ist für jedes $p \in \mathbb{P}$:

$$v_p(\mathrm{kgV}(a_1, \ldots, a_k)) \geq \max\{v_p(a_1), \ldots, v_p(a_k)\} = M_p = v_p(w) \quad .$$

Es folgt $w \mid \mathrm{kgV}(a_1, \ldots, a_k)$ und daher $w = \mathrm{kgV}(a_1, \ldots, a_k)$. □

Beispiel 2.3.6. Wir bestimmen

$$\mathrm{ggT}(26936, 27676, 1406) \quad \text{und} \quad \mathrm{kgV}(26936, 27676, 1406)$$

mit Hilfe von Theorem 2.3.5. Es gelten

$$26936 = 2^3 \cdot 7 \cdot 13 \cdot 37, \quad 27676 = 2^2 \cdot 11 \cdot 17 \cdot 37, \quad 1406 = 2 \cdot 19 \cdot 37 \quad .$$

In der Notation von 2.3.5 folgen

$$\begin{aligned} &m_2 = m_{37} = 1,\ m_p = 0 \quad p \in \mathbb{P} \setminus \{2, 37\} \\ &M_2 = 3,\ M_7 = M_{11} = M_{13} = M_{17} = M_{19} = M_{37} = 1, \\ &M_p = 0 \quad p \in \mathbb{P} \setminus \{2, 7, 11, 13, 17, 19, 37\} \quad . \end{aligned}$$

Also erhalten wir

$$\begin{aligned}&\mathrm{ggT}(26936, 27676, 1406) = 2 \cdot 37 = 74,\\ &\mathrm{kgV}(26936, 27676, 1406) = 2^3 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 37 = 95703608 \quad .\end{aligned}$$

3. Kongruenzen

3.1. **Restklassen.**

Definition 3.1.1. Es seien $m \in \mathbb{N}^+$ und a, $b \in \mathbb{Z}$.

1. a heißt kongruent zu b modulo m (Schreibweise: $a \equiv b \mod m$) genau dann, wenn $m \mid (a - b)$.
2. $\bar{a} := [a] := [a]_m := \{b \in \mathbb{Z} \mid b \equiv a \mod m\} = \{b \in \mathbb{Z} \mid \exists k \in \mathbb{Z}\colon b - a = km\} = \{a + km \mid k \in \mathbb{Z}\}$ heißt die Restklasse von a modulo m. Jedes $c \in \mathbb{Z}$ mit $\bar{c} = \bar{a}$ heißt ein Repräsentant von $\bar{a}$.
3. $\mathbb{Z}/m\mathbb{Z} := \{\bar{a} \mid a \in \mathbb{Z}\}$ heißt die Menge aller Restklassen modulo m.
4. Die Abbildung $\pi = \pi_m\colon \mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$, $x \mapsto \bar{x}$ heißt die Restklassenabbildung modulo m.

3.1.2. Eine Bemerkung: $\equiv \mod m$ ist also eine Relation zwischen ganzen Zahlen. Hin und wieder (meist in der Informatik; in der Mathematik eher selten) findet man auch die Schreibweise $a \mod m$ für eine ganze Zahl a. Damit meint man dann den Rest von a bei der Division durch m.

Beispiel 3.1.3. Wegen $2 \nmid 3 = 7 - 4$ gilt nicht $7 \equiv 4 \mod 2$. Wegen $3 \mid 7 - 4$ gilt $7 \equiv 4 \mod 3$.

Wegen $13 \mid 27 - 1$ ist $1 \equiv 27 \mod 13$. Daraus folgt modulo 13 (siehe 3.1.4.4) $\overline{27} = \bar{1}$. Also ist 27 ein Repräsentant von $\bar{1}$ (modulo 13).

Proposition 3.1.4. *Seien $m \in \mathbb{N}^+$ und a, $b \in \mathbb{Z}$.*

1. *Es gilt genau dann $a \equiv b \mod m$, wenn a und b bei Division durch m den gleichen Rest lassen.*
2. *Kongruenz modulo m ist eine Äquivalenzrelation auf $\mathbb{Z}$, d.h. für alle x, y, $z \in \mathbb{Z}$ gelten*
   - $x \equiv x \mod m$,
   - $x \equiv y \mod m \Rightarrow y \equiv x \mod m$,
   - $x \equiv y \mod m$ *und* $y \equiv z \mod m$ *implizieren* $x \equiv z \mod m$.
3. $\bar{a} = \bar{b} \iff a \equiv b \mod m$.
4. $\mathbb{Z}/m\mathbb{Z} = \{\bar{0}, \bar{1}, \ldots, \overline{m-1}\}$ *und* $\bar{i} \neq \bar{j}$ *für alle* $0 \leq i \neq j \leq m - 1$. *Insbesondere hat* $\mathbb{Z}/m\mathbb{Z}$ *genau* m *Elemente.*

Beweis. 1. Es seien r_a der Rest der Division von a durch m und entsprechend r_b der Rest der Division von b durch m. Dann gelten also $a = km + r_a$, $b = lm + r_b$ mit k, $l \in \mathbb{Z}$.

Es sei einmal $a \equiv b \mod m$. Dann ist $a - b = um$ mit $u \in \mathbb{Z}$. Es folgt $a = um + b = um + lm + r_b = (u + l)m + r_b$. Also ist r_b auch der Rest der Division von a durch m.

Umgekehrt gelte jetzt $r_a = r_b$. Dann folgt $a - b = km + r_a - (lm - r_b) = (k - l)m$, also $m \mid a - b$, d.h. $a \equiv b \mod m$.

2. Das folgt jetzt unmittelbar aus 1. Zum Beispiel: Gelten $x \equiv y \mod m$ und $y \equiv z \mod m$, so lassen x und y den gleichen Rest bei Division durch m und ebenso lassen y und z den gleichen Rest bei Division durch m. Daher haben auch x und z den gleichen Rest bei der Division durch m, woraus $x \equiv z \mod m$ folgt.

3. Es gelte einmal $\bar{a} = \bar{b}$. Wegen $b \equiv b \mod m$ folgt $b \in \bar{b} = \bar{a}$, also $b \equiv a \mod m$.

Umgekehrt gelte $a \equiv b \mod m$. Wir zeigen $\bar{a} = \bar{b}$, also die beiden Inklusionen $\bar{a} \subset \bar{b}$ und $\bar{a} \supset \bar{b}$.

$\subset$: Sei $c \in \bar{a}$. Dann gelten $c \equiv a \mod m$ und $a \equiv b \mod m$. Anwendung von 2 liefert $c \equiv b \mod m$, also $c \in \bar{b}$.

$\supset$: Sei $c \in \bar{b}$. Dann gilt $c \equiv b \mod m$. Wegen $a \equiv b \mod m$ gilt nach 2 auch $b \equiv a \mod m$. Aus $c \equiv b \mod m$ und $b \equiv a \mod m$ folgt nach 2 $c \equiv a \mod m$, also $c \in \bar{a}$.

4. Die Inklusion $\supset$ ist klar. Umgekehrt sei $\alpha \in \mathbb{Z}/m\mathbb{Z}$, etwa $\alpha = \bar{c}$ mit $c \in \mathbb{Z}$. Es sei $r \in \{0, \ldots, m-1\}$ der Rest der Division von c durch m. Dann gilt $m \mid c - r$, also $c \equiv r \mod m$. Nach 3 folgt $\alpha = \bar{c} = \bar{r} \in \{\bar{0}, \ldots, \overline{m-1}\}$.

Seien nun $0 \leq i, j \leq m - 1$ mit $\bar{i} = \bar{j}$. Wir müssen $i = j$ zeigen. Nach 3 gilt zunächst $i \equiv j \mod m$. Nach 1 lassen i und j bei Division durch m den gleichen Rest. Wegen $0 \leq i, j \leq m - 1$ ist der Rest der Division von i (bzw. j) durch m gleich i (bzw. j). Also ist $i = j$. □

Beispiel 3.1.5. Es ist $\mathbb{Z}/4\mathbb{Z} = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}\}$. Wegen (modulo 4) $\bar{3} = \overline{-1}$ ist auch $\mathbb{Z}/4\mathbb{Z} = \{\overline{-1}, \bar{0}, \bar{1}, \bar{2}\}$.

Satz 3.1.6. *Seien $m \in \mathbb{N}^+$ und a, a', b, $b' \in \mathbb{Z}$ mit $a \equiv a' \mod m$ und $b \equiv b' \mod m$. Dann gelten:*

1. $a \pm b \equiv a' \pm b' \mod m$.
2. $ab \equiv a'b' \mod m$.
3. *Für alle $k \in \mathbb{N}$ gilt $a^k \equiv a'^k \mod m$.*

Beweis. 1,2. Wegen $m \mid a - a'$ und $m \mid b - b'$ folgen nach 1.3.3.5 auch $m \mid (a - a') \pm (b - b') = (a \pm b) - (a' \pm b')$, also $a \pm b \equiv a' \pm b' \mod m$ und

$$m \mid (a - a')b + a'(b - b') = ab - a'b' \quad ,$$

also $ab \equiv a'b' \mod m$.

3. Wir benutzen Induktion nach k. Für $k = 0$ gilt $a^k = 1 = a'^k$ also auch $a^k \equiv a'^k \mod m$. Sei jetzt $k \in \mathbb{N}$ mit $a^k \equiv a'^k \mod m$. Wegen $a \equiv a' \mod m$ folgt aus 2

$$a^{k+1} = a^k \cdot a \equiv a'^k \cdot a' = a'^{k+1} \mod m \quad .$$

□

Beispiel 3.1.7. Wir bestimmen die Einerziffer von $2^{534\cdot 112345-14\cdot 6^5}$. Die Einerziffer einer Zahl ist der Rest der Division dieser Zahl durch 10. Wir berechnen zunächst kleine Zweierpotenzen modulo 10:

$$\overline{2^1} = \bar{2},\ \overline{2^2} = \bar{4},\ \overline{2^3} = \bar{8},\ \overline{2^4} = \bar{6},\ \overline{2^5} = \bar{2}, \overline{2^6} = \bar{4},\ \overline{2^7} = \bar{8},\ \overline{2^8} = 6, \ldots \quad .$$

Es ergibt sich die Vermutung, dass die Folge $(2^n)_{n\in\mathbb{N}^+}$ modulo 10 periodisch mit Periodenlänge 4 ist, d.h. $2^{n+4} \equiv 2^n \mod 10$ für alle $n \in \mathbb{N}^+$. Mit einer Induktion beweisen wir dies jetzt. Für $n = 1$ folgt die Behauptung aus obigen Rechnungen. Ist $n \in \mathbb{N}^+$ mit $2^{n+4} \equiv 2^n \mod 10$, so folgt

$$2^{n+1+4} = 2^{n+4} \cdot 2 \equiv 2^n \cdot 2 = 2^{n+1} \mod 10 \quad .$$

Es folgt jetzt $2^{a+4m} \equiv 2^a \mod 10$ für alle $a \in \mathbb{N}^+$ und alle $m \in \mathbb{N}$ (Induktion nach m). Also gilt für alle $a, b \in \mathbb{N}^+$: $a \equiv b \mod 4 \Rightarrow 2^a \equiv 2^b \mod 10$.

Wegen

$$534 \cdot 112345 - 14 \cdot 6^5 \equiv 2 \cdot 1 - 2 \cdot 0 = 2 \mod 4$$

folgt

$$2^{534\cdot 112345-14\cdot 6^5} \equiv 2^2 = 4 \mod 10 \quad .$$

Also ist die Einerziffer von $2^{534\cdot 112345-14\cdot 6^5}$ gleich 4.

Satz 3.1.8. *Sei $n \in \mathbb{N}^+$ und $n = (z_k z_{k-1} \ldots z_0)_{10}$ die Dezimaldarstellung von n, also $n = z_k 10^k + \ldots + 10 z_1 + z_0$. Dann gelten:*

1. $n \equiv z_k + \ldots + z_0 \mod 9$,
2. $n \equiv z_0 \mod 10$,
3. $n \equiv 10 z_1 + z_0 \mod 100$,
4. $n \equiv z_k (-1)^k + \ldots + (-1) z_1 + z_0 \mod 11$.

Beweis. 1. Es ist $10 \equiv 1 \mod 9$. Also gilt für alle $m \in \mathbb{N}$: $10^m \equiv 1^m = 1 \mod 9$. Es folgt

$$n = \sum_{m=0}^{k} z_m 10^m \equiv \sum_{m=0}^{k} z_m \mod 9 \quad .$$

2. Für $m \geq 1$ gilt $10^m \equiv 0 \mod 10$. Also ist

$$n = z_0 + \sum_{m=1}^{k} z_m 10^m \equiv z_0 + \sum_{k=1}^{m} z_m \cdot 0 = z_0 \mod 10 \quad .$$

3. Für $m \geq 2$ gilt $10^m \equiv 0 \mod 100$. Also ist

$$n = z_0 + 10 z_1 + \sum_{m=2}^{k} z_m 10^m \equiv z_0 + 10 z_1 + \sum_{k=2}^{m} z_m \cdot 0 = z_0 + 10 z_1 \mod 100 \quad .$$

4. Es ist $10 \equiv -1 \mod 11$, also $10^m \equiv (-1)^m \mod 11$ für alle $m \in \mathbb{N}$. Es folgt

$$n = \sum_{m=0}^{k} z_m 10^m \equiv \sum_{m=0}^{k} z_m (-1)^m \mod 11 \quad .$$

□

Korollar 3.1.9. *Sei $n \in \mathbb{N}^+$ und $n = (z_k z_{k-1} \dots z_0)_{10}$ die Dezimaldarstellung von n. Dann gelten:*

1. *Für $d \in \{3, 9\}$ gilt genau dann $d \mid n$, wenn $d \mid z_0 + \ldots + z_k$.*
2. *Für $d \in \{2, 5, 10\}$ gilt genau dann $d \mid n$, wenn $d \mid z_0$.*
3. *Für $d \in \{4, 25, 50, 100\}$ gilt genau dann $d \mid n$, wenn $d \mid 10z_1 + z_0$.*
4. $11 \mid n \iff 11 \mid z_0 - z_1 + \ldots + (-1)^k z_k$.

Beweis. Wir beginnen mit einer Beobachtung: Sind $m, m' \in \mathbb{N}^+$ und $a, b \in \mathbb{Z}$ mit $m' \mid m$ und $a \equiv b \mod m$, so gilt auch $a \equiv b \mod m'$. Denn $m' \mid m$ und $m \mid a - b$ impliziert $m' \mid a - b$.

Sei nun $d \in \{3, 9\}$. Dann gilt $d \mid 9$ und aus 3.1.8.1 folgt $n \equiv z_0 + \ldots + z_k \mod d$. Aus 3.1.4.1 folgt die Behauptung.

Analog folgen 2–4 aus der Beobachtung, 3.1.8 und 3.1.4.1. □

3.2. **Der Ring der Restklassen.**

3.2.1. Seien $m \in \mathbb{N}^+$ und $\alpha, \beta \in \mathbb{Z}/m\mathbb{Z}$. Wir wollen $\alpha + \beta$ und $\alpha \cdot \beta$ wie folgt definieren: Wähle $a, b \in \mathbb{Z}$ mit $\alpha = \bar{a}$ und $\beta = \bar{b}$ und setze

$$\alpha + \beta = \overline{a + b}, \quad \alpha \cdot \beta = \overline{ab} \quad .$$

Damit diese Definition sinnvoll ist, müssen wir uns aber überlegen, dass das Ergebnis unabhängig von der Wahl von a und b ist.

Angenommen es sind auch $A, B \in \mathbb{Z}$ mit $\alpha = \bar{A}$ und $\beta = \bar{B}$. Dann folgen $\bar{a} = \bar{A}$ und $\bar{b} = \bar{B}$, also $a \equiv A \mod m$ und $b \equiv B \mod m$. Aus 3.1.6 folgen $a + b \equiv A + B \mod m$ und $ab \equiv AB \mod m$, also

$$\overline{a + b} = \overline{A + B} \quad \text{und} \quad \overline{ab} = \overline{AB} \quad .$$

Wir haben damit eine Addition $+$ und eine Multiplikation $\cdot$ auf $\mathbb{Z}/m\mathbb{Z}$ definiert.

Satz 3.2.2. *Sei $m \in \mathbb{N}^+$. Dann gelten für alle $\alpha, \beta, \gamma \in \mathbb{Z}/m\mathbb{Z}$:*

1. $\alpha + \beta = \beta + \alpha$.
2. $(\alpha + \beta) + \gamma = \alpha + (\beta + \gamma)$.
3. $\alpha + \bar{0} = \alpha$.
4. *Es gibt $\delta \in \mathbb{Z}/m\mathbb{Z}$ mit $\alpha + \delta = \bar{0}$.*
5. $\alpha\beta = \beta\alpha$.
6. $(\alpha\beta)\gamma = \alpha(\beta\gamma)$.
7. $\alpha \cdot \bar{1} = \alpha$.

8. $\alpha(\beta+\gamma)=\alpha\beta+\alpha\gamma$.

Daher ist $(\mathbb{Z}/m\mathbb{Z},+,\cdot)$ *ein kommutativer Ring mit Einselement* $\bar{1}$ *und Nullelement* $\bar{0}$.

Beweis. Seien a, b, $c\in\mathbb{Z}$ mit $\alpha=\bar{a}$, $\beta=\bar{b}$ und $\gamma=\bar{c}$. Dann folgen

$$\alpha\dot{+}\beta=\overline{a\dot{+}b}=\overline{b\dot{+}a}=\beta\dot{+}\alpha\quad,$$

also 1 und 5. Weiters ist

$$(\alpha\dot{+}\beta)\dot{+}\gamma=(\bar{a}\dot{+}\bar{b})\dot{+}\bar{c}=\overline{a\dot{+}b}\dot{+}\bar{c}=\overline{(a\dot{+}b)\dot{+}c}=\overline{a\dot{+}(b\dot{+}c)}=$$
$$=\bar{a}\dot{+}\overline{b\dot{+}c}=\bar{a}\dot{+}(\bar{b}\dot{+}\bar{c})=\alpha\dot{+}(\beta\dot{+}\gamma)$$

woraus 2 und 6 folgen.

Aus

$$\alpha+\bar{0}=\bar{a}+\bar{0}=\overline{a+0}=\bar{a}=\alpha,\quad \alpha\cdot\bar{1}=\bar{a}\cdot\bar{1}=\overline{a\cdot 1}=\bar{a}=\alpha$$

folgen 3 und 7. 8 folgt aus

$$\alpha(\beta+\gamma)=\bar{a}(\bar{b}+\bar{c})=\bar{a}\cdot\overline{b+c}=\overline{a(b+c)}=\overline{ab+ac}=\overline{ab}+\overline{ac}=\bar{a}\bar{b}+\overline{ac}=$$
$$=\alpha\beta+\alpha\gamma\quad.$$

Zum Beweis von 4 setzen wir $\delta=\overline{-a}$. Dann gilt

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

□

3.2.3. Sei $m\in\mathbb{N}^+$. Dann ist insbesondere $(\mathbb{Z}/m\mathbb{Z},+)$ eine kommutative Gruppe. Wie üblich bezeichnet man für $\alpha\in\mathbb{Z}/m\mathbb{Z}$ mit $-\alpha$ das (additive) Inverse von α. Der letzte Beweis zeigt $-\bar{a}=\overline{-a}$ für alle $a\in\mathbb{Z}$.

3.2.4. Der letzte Satz zeigt, dass man in $\mathbb{Z}/m\mathbb{Z}$ ähnlich rechnen kann wie in $\mathbb{Z}$. Es gibt aber einen Unterschied: In $\mathbb{Z}$ kann durch Zahlen $\neq 0$ gekürzt werden. In $\mathbb{Z}/m\mathbb{Z}$ geht das im allgemeinen nicht mehr, wie das folgende Beispiel zeigt: In $\mathbb{Z}/15\mathbb{Z}$ gelten

$$\bar{3}\cdot\bar{10}=\bar{30}=\bar{0}=\bar{15}=\bar{3}\cdot\bar{5}\quad\text{aber}\quad\bar{10}\neq\bar{5}\quad.$$

Also kann $\bar{3}$ in $\mathbb{Z}/15\mathbb{Z}$ nicht gekürzt werden.

Der nächste Satz gibt Auskunft, welche Elemente in $\mathbb{Z}/m\mathbb{Z}$ gekürzt werden dürfen.

Satz 3.2.5. *Seien* $m\in\mathbb{N}^+$, $\alpha\in\mathbb{Z}/m\mathbb{Z}$ *und* $a\in\mathbb{Z}$ *mit* $\alpha=\bar{a}$. *Dann sind äquivalent:*

1. α *ist (multiplikativ) invertierbar, d.h. es gibt* $\beta\in\mathbb{Z}/m\mathbb{Z}$ *mit* $\alpha\beta=\bar{1}$.
2. α *ist kürzbar, d.h. für alle* γ, $\delta\in\mathbb{Z}/m\mathbb{Z}$ *gilt:* $\alpha\gamma=\alpha\delta\Rightarrow\gamma=\delta$.
3. $\mathrm{ggT}(a,m)=1$.
4. *Es gibt* x, $y\in\mathbb{Z}$ *mit* $ax+my=1$.

Sind diese Bedingungen erfüllt, so gilt $\beta=\bar{x}$.

Beweis. 1 $\Rightarrow$ 2. Es sei $\beta \in \mathbb{Z}/m\mathbb{Z}$ mit $\alpha\beta = \bar{1}$ und seien γ, $\delta \in \mathbb{Z}/m\mathbb{Z}$ mit $\alpha\gamma = \alpha\delta$. Multipliziert man die letzte Gleichung mit β so folgt $\beta\alpha\gamma = \beta\alpha\delta$ also $\gamma = \delta$.

2 $\Rightarrow$ 3. Es sei also α kürzbar. Wir setzen $d = \mathrm{ggT}(a, m)$. Dann gibt es $a' \in \mathbb{Z}$ und $m' \in \mathbb{N}$ mit $a = da'$ und $m = dm'$. Dann folgt

$$\alpha\overline{m'} = \bar{a}\overline{m'} = \overline{am'} = \overline{a'dm'} = \overline{a'm} = \overline{a'}\bar{m} = \overline{a'}\bar{0} = \bar{0} = \alpha\bar{0} \quad .$$

Da α kürzbar ist, erhalten wir $\overline{m'} = \bar{0}$, also $m' \equiv 0 \mod m$ und daher $m \mid m'$. Wegen $m = dm'$ gilt auch $m' \mid m$, also $m = m'$ (wegen m, $m' \in \mathbb{N}$). Aus $dm = dm' = m$ folgt nun $\mathrm{ggT}(a, m) = d = 1$.

3 $\Rightarrow$ 4 folgt aus Satz 1.4.9.2.

4 $\Rightarrow$ 1. Seien x, $y \in \mathbb{Z}$ mit $ax + my = 1$. Wir setzen $\beta = \bar{x}$. Wegen $\bar{m} = \bar{0}$ folgt

$$\bar{1} = \overline{ax + my} = \bar{a}\bar{x} + \bar{m}\bar{y} = \bar{a}\beta + \bar{0}\bar{y} = \bar{a}\beta + \bar{0} = \alpha\beta \quad .$$

□

Korollar 3.2.6. *Sei $m \in \mathbb{N}^+$. Dann ist $\mathbb{Z}/m\mathbb{Z}$ genau dann ein Körper, wenn m eine Primzahl ist.*

Beweis. Zunächst zur Erinnerung: Ein kommutativer Ring R ist ein Körper, falls $R \neq \{0\}$ gilt, und falls es zu jedem $x \in R \setminus \{0\}$ ein $y \in R$ mit $xy = 1$ gibt.

Sei nun einmal m eine Primzahl. Dann ist

$$|\mathbb{Z}/m\mathbb{Z}| = m \geq 2$$

und daher $\mathbb{Z}/m\mathbb{Z} \neq \{\bar{0}\}$. Sei nun $\alpha \in \mathbb{Z}/m\mathbb{Z}$ mit $\alpha \neq \bar{0}$. Wir wählen $a \in \{0, 1, \ldots, m-1\}$ mit $\alpha = \bar{a}$. Wegen $\alpha \neq \bar{0}$ ist $a \in \{1, \ldots, m-1\}$. Dann gilt $m \nmid a$. Da m eine Primzahl ist, folgt daraus $\mathrm{ggT}(a, m) = 1$. Nach 3.2.5 gibt es $\beta \in \mathbb{Z}/m\mathbb{Z}$ mit $\alpha\beta = \bar{1}$.

Sei nun umgekehrt $\mathbb{Z}/m\mathbb{Z}$ ein Körper. Dann ist $\mathbb{Z}/m\mathbb{Z} \neq \{\bar{0}\}$ und daher

$$m = |\mathbb{Z}/m\mathbb{Z}| \geq 2 \quad .$$

Sei $d \in \mathbb{N}^+$ ein Teiler von m mit $d \neq m$. Wir müssen $d = 1$ zeigen. Wegen $1 \leq d \leq m-1$ ist $\bar{d} \neq \bar{0}$. Nach Voraussetzung gibt es $\beta \in \mathbb{Z}/m\mathbb{Z}$ mit $\bar{d}\beta = \bar{1}$. Aus 3.2.5 folgt $1 = \mathrm{ggT}(d, m)$. Wegen $d \mid m$ ist aber $d = \mathrm{ggT}(d, m)$. Es folgt $d = 1$. □

Beispiel 3.2.7. Als erstes Beispiel geben wir eine einfachere Lösung von Aufgabe 8 von Blatt 2. Wir rechnen dazu in $\mathbb{Z}/13\mathbb{Z}$. Wegen $\overline{81} = \overline{3} = \overline{16}$ erhalten wir für jedes $k \in \mathbb{N}$:

$$\overline{3^{4k} - 2^{4k}} = \overline{81^k - 16^k} = \overline{81}^k - \overline{16}^k = \overline{3}^k - \overline{3}^k = \overline{0},$$

also $13 \mid 3^{4k} - 2^{4k}$.

Beispiele 3.2.8. Wir lösen einige Gleichungen über Restklassenringen.

1. $\bar{4}x + \bar{7} = \bar{2}$ in $\mathbb{Z}/35\mathbb{Z}$: Zunächst gilt für jedes $x \in \mathbb{Z}/35\mathbb{Z}$:

$$\bar{4}x + \bar{7} = \bar{2} \iff \bar{4}x = \bar{2} - \bar{7} = \overline{-5} \quad .$$

Nun wollen wir natürlich durch $\bar{4}$ dividieren. Nun bedeutet dividieren mit dem multiplikativ Inversen multiplizieren. Also müssen wir untersuchen ob $\bar{4}$ in $\mathbb{Z}/35\mathbb{Z}$ multiplikativ invertierbar ist. Dazu können wir Satz 3.2.5 verwenden: Es ist $\mathrm{ggT}(4, 35) = 1$ und daher ist $\bar{4}$ in $\mathbb{Z}/35\mathbb{Z}$ multiplikativ invertierbar. Was ist das Inverse von $\bar{4}$? Wiederum nach 3.2.5 müssen wir dazu 1 als Linearkombination von 4 und 35 darstellen: $1 = 9 \cdot 4 + (-1) \cdot 35$. Es folgt $\bar{1} = \bar{9} \cdot \bar{4}$ und daher ist $\bar{9}$ das multiplikativ Inverse von $\bar{4}$. Wir erhalten daher für alle $x \in \mathbb{Z}/35\mathbb{Z}$:

$$\bar{4}x = \overline{-5} \iff x = \bar{9} \cdot \bar{4}x = \bar{9} \cdot \overline{-5} = \overline{-45} = \overline{25} \quad .$$

Also ist $x = \overline{25}$ die einzige Lösung unserer Gleichung.

2. Wir betrachten die Gleichung $\bar{5}x + \bar{3} = \bar{7}$ in $\mathbb{Z}/30\mathbb{Z}$. Zunächst gilt für jedes $x \in \mathbb{Z}/30\mathbb{Z}$:

$$\bar{5}x + \bar{3} = \bar{7} \iff \bar{5}x = \bar{7} - \bar{3} = \bar{4} \quad .$$

Wir wollen wieder durch $\bar{5}$ dividieren. Diesmal ist aber $\mathrm{ggT}(5, 30) = 5$ und daher ist $\bar{5}$ in $\mathbb{Z}/30\mathbb{Z}$ nicht invertierbar, sodass wir nicht dividieren können. Tatsächlich hat unsere Gleichung keine Lösung: Angenommen es ist $x \in \mathbb{Z}/30\mathbb{Z}$ mit $\bar{5}x = \bar{4}$. Wähle $y \in \mathbb{Z}$ mit $x = \bar{y}$. Dann folgt

$$\bar{4} = \bar{5}x = \bar{5}\bar{y} = \overline{5y} \quad .$$

Daher gilt $4 \equiv 5y \mod 30$ und daher $30 \mid 4 - 5y$. Wegen $5 \mid 30$ folgt auch $5 \mid 4 - 5y$ und daher $5 \mid 4$, Widerspruch.

3. Wir betrachten die Gleichung $\bar{3}x - \bar{7} = \overline{29}$ in $\mathbb{Z}/33\mathbb{Z}$. Zunächst ist wieder für alle $x \in \mathbb{Z}/33\mathbb{Z}$:

$$\bar{3}x - \bar{7} = \overline{29} \iff \bar{3}x = \overline{29} + \bar{7} = \overline{36} = \bar{3} \quad .$$

Wegen $\mathrm{ggT}(3, 33) = 3 > 1$ können wir nicht durch $\bar{3}$ dividieren. Wir sehen aber, dass $\bar{1}$ eine Lösung ist. Wie bekommen wir alle Lösungen?. Wähle dazu $y \in \mathbb{Z}$ mit $x = \bar{y}$. Dann erhalten wir

$$\begin{aligned} \bar{3}x = \bar{3} &\iff \overline{3y} = \bar{3} \iff 3y \equiv 3 \mod 33 \iff 3 \cdot 11 \mid 3(y-1) \iff \\ &\iff 11 \mid y - 1 \iff y = 1 + 11z \text{ für ein } z \in \mathbb{Z} \quad . \end{aligned}$$

Schreiben wir noch jedes $z \in \mathbb{Z}$ in der Form $z = 3w + r$ mit $w \in \mathbb{Z}$ und $r \in \{0, 1, 2\}$ so folgt

$$\bar{3}x = \bar{3} \iff y = 1 + 11(3w + r) = 33w + 11r + 1 \iff \bar{x} = \bar{y} = \overline{11r + 1} \quad .$$

Also sind $\bar{1}$, $\overline{12}$ und $\overline{23}$ die Lösungen unserer Gleichung.

4. Wir betrachten die Gleichung $x^2 + \bar{4}x - \overline{12} = 0$ in $\mathbb{Z}/37\mathbb{Z}$. Wie bei quadratischen Gleichungen üblich verwenden wir quadratische Ergänzung:

$$\begin{aligned} x^2 + \bar{4}x - \overline{12} = x^2 + \bar{4}x + \bar{4} - \overline{16} = (x + \bar{2})^2 - \overline{16} = (x + \bar{2})^2 - \bar{4}^2 = \\ = \left(x + \bar{2} - \bar{4}\right)(x + \bar{2} + \bar{4}) = (x - \bar{2})(x + \bar{6}) \quad . \end{aligned}$$

Da 37 eine Primzahl ist, ist $\mathbb{Z}/37$ ein Körper und daher ist ein Produkt in $\mathbb{Z}/37\mathbb{Z}$ genau dann Null, wenn ein Faktor Null ist. Also sind $\bar{2}$ und $-\bar{6} = \overline{31}$ die Lösungen unserer Gleichungen.

5. Wir lösen $x^2 + x + \bar{6} = \bar{0}$ in $\mathbb{Z}/34\mathbb{Z}$. Wir können nicht unmittelbar quadratisch ergänzen: dazu bräuchten wir einen Faktor 2 bei x, sodass wir durch 2 dividieren müssten. Aber wegen $\mathrm{ggT}(2, 34) = 2$ dürfen wir das nicht.

   Es sei $x \in \mathbb{Z}/34\mathbb{Z}$ und $y \in \mathbb{Z}$ mit $x = \bar{y}$. Dann folgt

$$x^2 + x + \bar{6} = \bar{0} \iff 34 \mid y^2 + y + 6 \quad .$$

   Wegen $34 = 2 \cdot 17$ ist dies äquivalent zu $2 \mid y^2 + y + 6$ und $17 \mid y^2 + y + 6$. Nun ist $y^2 + y = y(y + 1)$ immer gerade und daher gilt immer $2 \mid y^2 + y + 6$. Wir müssen also alle $y \in \mathbb{Z}$ mit $17 \mid y^2 + y + 6$ finden. Dies ist äquivalent zu $\bar{y}^2 + \bar{y} + \bar{6} = \bar{0}$ in $\mathbb{Z}/17\mathbb{Z}$. Nun ist $\mathrm{ggT}(2, 17) = 1$, sodass wir in $\mathbb{Z}/17\mathbb{Z}$ durch $\bar{2}$ dividieren können. Wegen $1 = 17 + (-8) \cdot 2$ ist $-\bar{8} = \bar{9}$ das multiplikativ Inverse von $\bar{2}$. Es folgt

$$\bar{y}^2 + \bar{y} + \bar{6} = \bar{y}^2 + \overline{2} \cdot \overline{9}\bar{y} + \bar{6} = \bar{y}^2 + \bar{2} \cdot \overline{9}\bar{y} + \overline{9}^2 - \bar{9}^2 + \bar{6} = (\bar{y} + \bar{9})^2 + \overline{10} \quad .$$

   Damit ist $\bar{y}^2 + \bar{y} + \bar{6} = 0$ äquivalent zu $(\bar{y} + \overline{9})^2 = -\overline{10} = \overline{7}$ (in $\mathbb{Z}/17\mathbb{Z}$). Durch Ausprobieren aller möglichen Fälle sieht man, dass die Gleichung $z^2 = \overline{7}$ keine Lösung in $\mathbb{Z}/17\mathbb{Z}$ besitzt. Also hat auch unsere ursprüngliche Gleichung keine Lösung.

6. $x^2 = \bar{0}$ in $\mathbb{Z}/16\mathbb{Z}$. Es sei $x \in \overline{\mathbb{Z}}$ und $y \in \{0, 1, 2 \ldots, 15\}$ mit $\bar{y} = x$. Dann gilt

$$\begin{aligned} x^2 = 0 &\iff 16 \mid y^2 \iff 4 = v_2(16) \leq v_2(y^2) = 2v_2(y) \iff 2 \leq v_2(y) \iff \\ &\iff 4 = 2^2 \mid y \iff y \in \{0, 4, 8, 12\} \quad . \end{aligned}$$

   Also sind $\bar{0}$, $\bar{4}$, $\bar{8}$, $\overline{12}$ die Lösungen von $x^2 = \bar{0}$ in $\mathbb{Z}/16\mathbb{Z}$.

3.3. **Der chinesische Restsatz und die Euler'sche Phifunktion.**

Lemma 3.3.1. *Es seien $k \in \mathbb{N}^+$ und $m_1, \ldots, m_k \in \mathbb{N}^+$, die paarweise teilerfremd sind, d.h. für $1 \leq i \neq j \leq k$ gilt $\mathrm{ggT}(m_i, m_j) = 1$. Dann gilt*

$$\mathrm{kgV}(m_1, \ldots, m_k) = m_1 \ldots m_k \quad .$$

Beweis. Wir benutzen Induktion nach k. Für $k = 1$ ist die Aussage trivial. Sei nun $k \in \mathbb{N}^+$, sodass die Aussage für k gilt. Seien $m_1, \ldots, m_{k+1} \in \mathbb{N}^+$, die paarweise teilerfremd sind. Dann gilt

$$\begin{aligned} \mathrm{kgV}(m_1, \ldots, m_{k+1}) &= \mathrm{kgV}(\mathrm{kgV}(m_1, \ldots, m_k), m_{k+1}) \overset{\text{Ind. Vor.}}{=} \mathrm{kgV}(m_1 \ldots m_k, m_{k+1}) = \\ &= \frac{m_1 \ldots m_{k+1}}{\mathrm{ggT}(m_1 \ldots m_k, m_{k+1})} \overset{1.4.15.4}{=} \frac{m_1 \ldots m_{k+1}}{1} = m_1 \ldots m_{k+1} \quad . \end{aligned}$$

□

Satz 3.3.2. *Gegeben sei das System von Kongruenzen*

$$\begin{aligned} X &\equiv c_1 \mod m_1 \\ X &\equiv c_2 \mod m_2 \\ &\vdots \\ X &\equiv c_k \mod m_k \end{aligned} \tag{3.3.2.1}$$

mit $k \in \mathbb{N}^+$, $m_1, \ldots, m_k \in \mathbb{N}^+$ *paarweise teilerfremd und* $c_1, \ldots, c_k \in \mathbb{Z}$. *Dann gibt es eine Lösung* $x_0 \in \mathbb{Z}$ *von* (3.3.2.1) *und ist* $x_0 \in \mathbb{Z}$ *eine Lösung von* (3.3.2.1), *so ist* $x_0 + m_1 \ldots m_k\mathbb{Z}$ *die Lösungsmenge von* (3.3.2.1) *(Chinesischer Restsatz).*

Beweis. Wir zeigen zunächst den zweiten Teil. Sei $x_0 \in \mathbb{Z}$ eine Lösung von (3.3.2.1) und sei L die Lösungsmenge von (3.3.2.1).

$x_0 + m_1 \ldots m_k\mathbb{Z} \subset L$: Sei $n \in \mathbb{Z}$ und $x = x_0 + nm_1 \ldots m_k$. Für $i = 1, \ldots, k$ gilt dann $m_i \mid nm_1 \ldots m_k = x - x_0$. Also ist $x \equiv x_0 \equiv c_i \mod m_i$ für $i = 1, \ldots, k$. Es folgt $x \in L$.

$L \subset x_0 + m_1 \ldots m_k\mathbb{Z}$. Sei $x \in L$. Dann folgt $x \equiv c_i \equiv x_0 \mod m_i$, also $m_i \mid x - x_0$ für $i = 1, \ldots, k$. Also ist $|x - x_0|$ ein positives Vielfaches aller m_i und damit ein Vielfaches von $\mathrm{kgV}(m_1, \ldots, m_k)$. Da die m_i paarweise teilerfremd sind folgt aus 3.3.1 $\mathrm{kgV}(m_1, \ldots, m_k) = m_1 \ldots m_k$. Also ist $|x - x_0|$ und damit auch $x - x_0$ ein Vielfaches von $m_1 \ldots m_k$, d.h. $x \in x_0 \in m_1 \ldots m_k\mathbb{Z}$.

Wir zeigen nun, dass (3.3.2.1) eine Lösung besitzt. Für $i = 1, \ldots, k$ setze $M_i = m_1 \ldots m_{i-1}m_{i+1} \ldots m_k$. Da m_i zu allen m_j, $j \neq i$ teilerfremd ist, folgt $\mathrm{ggT}(M_i, m_i) = 1$ für $i = 1, \ldots, k$ (1.4.15.4). Nach 3.2.5 gibt es $b_i \in \mathbb{Z}$ mit $M_ib_i \equiv 1 \mod m_i$, $i = 1, \ldots, k$. Wir setzen nun

$$x_0 = \sum_{j=1}^{k} c_jM_jb_j$$

und zeigen, dass x_0 eine Lösung von (3.3.2.1) ist. Sei dazu $1 \leq i \leq k$. Nach Konstruktion gilt dann $M_ib_i \equiv 1 \mod m_i$. Ist $j \neq i$ so gilt $m_i \mid M_j$, also auch $m_i \mid M_jb_j$, also $M_jb_j \equiv 0 \mod m_i$. Es folgt

$$x_0 = c_ib_iM_i + \sum_{\substack{j=1 \\ j\neq i}}^{k} c_jM_jb_j \equiv c_i \cdot 1 + \sum_{\substack{j=1 \\ j\neq i}}^{k} c_j \cdot 0 = c_i \mod m_i \quad .$$

□

Beispiel 3.3.3. Wir bestimmen alle $x \in \mathbb{Z}$ mit

$$x \equiv 2 \mod 3, \quad x \equiv 3 \mod 5, \quad x \equiv 4 \mod 7 \quad .$$

In der Notation des Beweises von 3.3.2.1 ist dann $M_1 = 5 \cdot 7 = 35$, $M_2 = 3 \cdot 7 = 21$ und $M_3 = 3 \cdot 5 = 15$. Wir bestimmen dann b_1, b_2, $b_3 \in \mathbb{Z}$ mit

$$M_1b_1 = 35b_1 \equiv 1 \mod 3, \quad M_2b_2 = 21b_2 \equiv 1 \mod 5, \quad M_3b_3 = 15b_3 \equiv 1 \mod 7.$$

Wegen $35 \equiv 2 \mod 3$ und $2 \cdot 2 = 4 \equiv 1 \mod 3$ können wir $b_1 = 2$ setzen. Es ist $21 \equiv 1 \mod 5$ und daher können wir $b_2 = 1$ setzen. Wegen $15 \equiv 1 \mod 7$ können wir analog $b_3 = 1$ setzen. Also ist

$$x_0 = 2 \cdot (35 \cdot 2) + 3 \cdot (21 \cdot 1) + 4 \cdot (15 \cdot 1) = 263$$

eine Lösung. Die gesamte Lösungsmenge ist nun

$$263 + 3 \cdot 5 \cdot 7\mathbb{Z} = 263 + 105\mathbb{Z} = 53 + 105\mathbb{Z}.$$

Definition 3.3.4. Für $m \in \mathbb{N}^+$ setzen wir (wie für jeden Ring)

$$\begin{aligned}(\mathbb{Z}/m\mathbb{Z})^\times &= \{\alpha \in \mathbb{Z}/m\mathbb{Z} \mid \alpha \text{ ist (multiplikativ) invertierbar } \} \overset{3.1.4.4}{=} \\ &= \{\bar{x} \mid x \in \{0, \ldots, m-1\} \text{ und } \bar{x} \text{ ist (multiplikativ) invertierbar } \} \overset{3.2.5}{=} \\ &= \{\bar{x} \mid x \in \{0, \ldots, m-1\} \text{ und } \operatorname{ggT}(x, m) = 1\} \quad .\end{aligned}$$

Man beachte: Ist $m \geq 2$ (der interessanteste Fall), so ist $\operatorname{ggT}(0, m) = m \geq 2$ und daher dann

$$(\mathbb{Z}/m\mathbb{Z})^\times = \{\bar{x} \mid x \in \{1, \ldots, m-1\} \text{ und } \operatorname{ggT}(x, m) = 1\}$$

Dann ist $(\mathbb{Z}/m\mathbb{Z})^\times$ zusammen mit der Multiplikation eine kommutative Gruppe. Wir setzen

$$\varphi(m) = \#(\mathbb{Z}/m\mathbb{Z})^\times = \#\{x \in \{0, \ldots, m-1\} \mid \operatorname{ggT}(x, m) = 1\} \quad .$$

Die Funktion $\varphi\colon \mathbb{N}^+ \to \mathbb{N}^+$ heißt Eulersche Phi–Funktion.

Beispiel 3.3.5. Es ist $\varphi(1) = \#\{x \in \{0\} \mid \operatorname{ggT}(x, 1) = 1\} = \#\{0\} = 1$. Für eine Primzahl p gilt

$$\varphi(p) = \#\{x \in \{0, \ldots, p-1\} \mid \operatorname{ggT}(x, p) = 1\} = \#\{1, \ldots, p-1\} = p - 1 \quad .$$

Satz 3.3.6. *Es seien m, $n \in \mathbb{N}^+$ mit $\operatorname{ggT}(m, n) = 1$. Dann gilt $\varphi(mn) = \varphi(m)\varphi(n)$.*

Beweis. Wir setzen $I = \{x \in \{0, \ldots, mn-1\} \mid \operatorname{ggT}(x, mn) = 1\}$. Dann gilt also $\varphi(mn) = \#I$. Unser Ziel ist nun, eine bijektive Abbildung

$$f\colon I \to (\mathbb{Z}/m\mathbb{Z})^\times \times (\mathbb{Z}/n\mathbb{Z})^\times$$

zu definieren. Dann folgt

$$\varphi(mn) = \#I = \#\big((\mathbb{Z}/m\mathbb{Z})^\times \times (\mathbb{Z}/n\mathbb{Z})^\times\big) = \big(\#(\mathbb{Z}/m\mathbb{Z})^\times\big) \cdot \big(\#(\mathbb{Z}/n\mathbb{Z})^\times\big) = \varphi(m)\varphi(n).$$

Es sei $x \in I$. Dann ist $\operatorname{ggT}(x, m)$ ein gemeinsamer Teiler von x und m, also auch von x und mn. Wegen $\operatorname{ggT}(x, mn) = 1$ folgt damit auch $\operatorname{ggT}(x, m) = 1$. Analog sieht man $\operatorname{ggT}(x, n) = 1$ ein. Für $x \in I$ bezeichnen wir die Restklasse von x modulo m mit $[x]_m$, und analog mit $[x]_n$ die Restklasse von x modulo n. Wegen $\operatorname{ggT}(x, m) = 1 = \operatorname{ggT}(x, n) = 1$ erhalten wir $[x]_m \in (\mathbb{Z}/m\mathbb{Z})^\times$, $[x]_n \in (\mathbb{Z}/n\mathbb{Z})^\times$ aus 3.2.5. Wir können daher durch $x \mapsto ([x]_m, [x]_n)$ eine Abbildung

$$f\colon I \to (\mathbb{Z}/m\mathbb{Z})^\times \times (\mathbb{Z}/n\mathbb{Z})^\times$$

definieren. Wir zeigen, dass f bijektiv ist.

f ist injektiv: es seien $x, y \in I$ mit $f(x) = f(y)$, d.h. $[x]_m = [y]_m$ und $[x]_n = [y]_n$. Daraus folgt $m \mid x - y$ und $n \mid x - y$. Da m und n nach Voraussetzung teilerfremd sind, ist auch mn ein Teiler von $x - y$ (1.4.15.3), also ist $x \equiv y \mod mn$. Wegen $x, y \in \{0, \ldots, mn - 1\}$ erhalten wir $x = y$.

Eine Frage zum Verständnis: Wie folgt die Injektivität von f direkt aus dem chinesischem Restsatz?

f ist surjektiv: Es sei $(\alpha, \beta) \in (\mathbb{Z}/m\mathbb{Z})^\times \times (\mathbb{Z}/n\mathbb{Z})^\times$ beliebig. Wir wählen a, $b \in \mathbb{Z}$ mit $\alpha = [a]_m$ und $[b]_n = \beta$. Nach 3.2.5 gelten dann $\mathrm{ggT}(a, m) = 1 = \mathrm{ggT}(b, n)$. Jetzt verwenden wir den chinesischen Restsatz (3.3.2). Da m und n teilerfremd sind, können wir ein $x' \in \mathbb{Z}$ mit $x' \equiv a \mod m$ und $x' \equiv b \mod n$ wählen. Weiters erfüllt jedes $x \in \mathbb{Z}$ mit $x \equiv x' \mod mn$ ebenfalls $x \equiv a \mod m$ und $x \equiv b \mod n$. Also finden wir ein $x \in \{0, \ldots, mn - 1\}$ mit $x \equiv a \mod m$ und $x \equiv b \mod n$. Es folgen

$$[x]_m = [a]_m = \alpha, \quad [x]_n = [b]_n = \beta$$

und damit

$$([x]_m, [x]_n) = (\alpha, \beta).$$

Wenn wir jetzt noch $x \in I$ zeigen können, erhalten wir $f(x) = (\alpha, \beta)$ (und damit die Surjektivität von f). Angenommen es ist $x \notin I$. Dann folgt $\mathrm{ggT}(x, mn) > 1$. Nach Aufgabe 24 von Blatt 4 können wir dann eine Primzahl p mit $p \mid x$ und $p \mid mn$ wählen. Dann gilt $p \mid m$ oder $p \mid n$. Wir betrachten zunächst den Fall $p \mid m$: wegen $[x]_m = [a]_m$ gilt $x \equiv a \mod m$, also $m \mid x - a$. Wegen $p \mid m$ folgt $p \mid x - a$. Aus $p \mid x$ erhalten wir dann $p \mid a$. Daher ist p ein gemeinsamer Teiler von m und a und wir erhalten den Widerspruch $\mathrm{ggT}(a, m) > 1$. Analog führt $p \mid n$ zum Widerspruch $\mathrm{ggT}(b, n) > 1$.

□

Satz 3.3.7. *Es sei $m \in \mathbb{N}_{\geq 2}$ und $m = p_1^{a_1} \ldots p_r^{a_r}$ die Primfaktorzerlegung von m (also: $r \in \mathbb{N}^+$, $p_1, \ldots, p_r \in \mathbb{P}$ paarweise verschieden, und $a_1, \ldots, a_r \in \mathbb{N}^+$). Dann gilt*

$$\varphi(m) = (p_1 - 1)p_1^{a_1 - 1} \ldots (p_r - 1)p_r^{a_r - 1}.$$

Beweis. Wir benutzen eine Induktion nach r. Also starten wir mit dem Fall $r = 1$, also $m = p_1^{a_1}$. Zur Abkürzung schreiben wir $p = p_1$ und $a = a_1$, also $m = p^a$. Dann gilt

$$\begin{aligned}\varphi(m) = \varphi(p^a) &= \#\{x \in \{0, \ldots, p^a - 1\} \mid \mathrm{ggT}(x, p^a) = 1\} = \\ &= \#\{0, \ldots, p^a - 1\} - \#\{x \in \{0, \ldots, p^a - 1\} \mid \mathrm{ggT}(x, p^a) > 1\} = \\ &= p^a - \#\{x \in \{0, \ldots, p^a - 1\} \mid \mathrm{ggT}(x, p^a) > 1\}.\end{aligned}$$

Nun ist p die einzige Primzahl, die p^a teilt. Wegen Aufgabe 24 gilt daher für $x \in \{0, \dots, p^a - 1\}$: $\mathrm{ggT}(x, p^a) > 1 \iff p \mid x$. Damit folgt

$$\begin{aligned}\varphi(m) &= p^a - \#\{x \in \{0, \dots, p^a - 1\} \mid p \mid x\} = \\ &= p^a - \#\{0 \cdot p, 1 \cdot p, \dots (p^{a-1} - 1)p\} = \\ &= p^a - p^{a-1} = p^{a-1}(p-1).\end{aligned}$$

Wir nehmen nun, $r \geq 2$ an, und dass die Aussage für $r - 1$ stimmt. Setzen wir $m' = p_1^{a_1} \dots p_{r-1}^{a_{r-1}}$ so gelten $m = m' p_r^{a_r}$ und $\mathrm{ggT}(m', p_r^{a_r}) = 1$ (z.B. wieder nach Aufgabe 24). Daher folgt aus 3.3.6

$$\begin{aligned}\varphi(m) = \varphi(m')\varphi(p_r^{a_r}) &\overset{\text{Fall } r=1}{=} \varphi(m')(p_r - 1)p_r^{a_r - 1} \overset{\text{I.V.}}{=} \\ &= (p_1 - 1)p_1^{a_1 - 1} \dots (p_{r-1} - 1)p_{r-1}^{a_{r-1} - 1}(p_r - 1)p_r^{a_r - 1}.\end{aligned}$$

□

Satz 3.3.8. *Es seien $m \in \mathbb{N}^+$ und $a \in \mathbb{Z}$ mit $\mathrm{ggT}(a, m) = 1$. Dann folgt $a^{\varphi(m)} \equiv 1 \mod m$ (Satz von Euler).*

Beweis. Wir setzen $\alpha = \bar{a} \in \mathbb{Z}/m\mathbb{Z}$. Wegen $\mathrm{ggT}(a, m) = 1$ gilt $\alpha \in (\mathbb{Z}/m\mathbb{Z})^\times$. Wir nummerieren nun die Elemente von $(\mathbb{Z}/mZ)^\times$:

$$(\mathbb{Z}/m\mathbb{Z})^\times = \{\beta_1, \dots, \beta_{\varphi(m)}\}.$$

und setzen

$$\gamma = \prod_{i=1}^{\varphi(m)} \beta_i \in (\mathbb{Z}/m\mathbb{Z})^\times.$$

Die Abbildung $(\mathbb{Z}/m\mathbb{Z})^\times \to (\mathbb{Z}/m\mathbb{Z})^\times$, $\gamma \mapsto \alpha\gamma$ ist injektiv, da α kürzbar ist. Wegen $\gamma = \alpha(\alpha^{-1}\gamma)$ für alle $\gamma \in (\mathbb{Z}/m\mathbb{Z})^\times$ ist sie auch surjektiv, also bijektiv. Es gibt daher eine Permutation (eine bijektive Abbildung) $\sigma\colon \{1, \dots, \varphi(m)\} \to \{1, \dots, \varphi(m)\}$ mit $\alpha\beta_i = \beta_{\sigma(i)}$ für alle $1 \leq i \leq \varphi(m)$. Damit folgt

$$\begin{aligned}\gamma \cdot \bar{1} = \gamma = \prod_{i=1}^{\varphi(m)} \beta_i &\overset{(\mathbb{Z}/m\mathbb{Z})^\times \text{ ist kommutativ}}{=} \prod_{i=1}^{\varphi(m)} \beta_{\sigma(i)} = \prod_{i=1}^{\varphi(m)} (\alpha\beta_i) \overset{(\mathbb{Z}/m\mathbb{Z})^\times \text{ ist kommutativ}}{=} \\ &= \alpha^{\varphi(m)} \prod_{i=1}^{\varphi(m)} \beta_i = \gamma\alpha^{\varphi(m)}.\end{aligned}$$

Da γ kürzbar ist folgt $\alpha^{\varphi(m)} = \bar{1}$ und daher $a^{\varphi(m)} \equiv 1 \mod m$. □

Korollar 3.3.9. *Es seien $a \in \mathbb{Z}$ und $p \in \mathbb{P}$. Dann gelten*

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

Beweis. 1. Gilt $p \nmid a$, so folgt $\mathrm{ggT}(a,p) = 1$ (wegen $p \in \mathbb{P}$). Nach Beispiel 3.3.5 gilt $\varphi(p) = p-1$ und die Behauptung folgt aus 3.3.8.

2. Gilt $p \nmid a$ so folgt aus 1:

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

Gilt aber $p \mid a$, so so gilt auch $p \mid a^p$ und daher ist $a^p \equiv 0 \equiv a \mod p$. □

3.4. **Das RSA Verschlüsselungsverfahren.**

3.4.1. Gegenstand der Kryptographie sind Verschlüsselungsverfahren, die man braucht, wenn man Nachrichten geheim übertragen will. Wir definieren zunächst was wir unter einem Verschlüsselungsverfahren verstehen:

Ein Verschlüsselungsverfahren oder Kryptosystem ist ein Fünftupel (P, C, K, E, D) mit folgenden Eigenschaften:

1. P ist eine Menge. Sie heißt Klartextraum und ihre Elemente Klartexte. (englisch: plaintext).
2. C ist eine Menge. Sie heißt Chiffretextraum und ihre Elemente Chiffretexte (englisch: ciphertext).
3. K ist eine Menge. Sie heißt Schlüsselraum und ihre Elemente Schlüssel (englisch key).
4. $E = (E_k)_{k \in K}$ ist eine Familie von Funktionen $E_k \colon P \to C$. Diese Funktionen heißen Verschlüsselungsfunktionen (englisch: encryption function).
5. $D = (D_k)_{k \in K}$ ist eine Familie von Funktionen $D_k \colon C \to P$. Diese Funktionen heißen Entschlüsselungsfunktionen (englisch: decryption function).
6. Für jedes $e \in K$ gibt es ein $d \in K$ mit $D_d(E_e(p)) = p$ für jedes $p \in P$, also mit $D_d \circ E_e = Id_P$.

Ein Verschlüsselungsverfahren (P, C, K, E, D) heißt symmetrisch, wenn für jedes $e \in K$, dasjenige $d \in K$ mit $D_d \circ E_e = Id_P$ leicht zu bestimmen ist (unter der Voraussetzung, dass die einzige verfügbare Information das Verschlüsselungsverfahren selbst ist). Sonst heißt es asymmetrisch.

In den meisten asymmetrischen Verfahren wird der Schlüssel e, der zum Verschlüsseln verwendet wird, öffentlich gemacht, d.h. es wird nicht versucht diesen Schlüssel geheim zu halten. Daher nennt man solche Verfahren auch Public Key Verfahren.

Gängige Public Key Verfahren sind ineffizient (langsam), wenn man lange Nachrichten geheim halten will. Daher geht man in der Praxis meist folgendermaßen vor: Es wird ein symmetrisches Verschlüsselungsverfahren gewählt, mit dessen Hilfe man Informationen ver– und entschlüsselt. Dafür wird jedoch eine Methode benötigt, den Schlüssel geheim wählen zu können. Zu diesem Zweck werden Public Key Verfahren verwendet.

Eines davon ist das RSA–Verfahren. Es beruht auf dem folgenden Resultat.

Lemma 3.4.2. *Seien p, q zwei verschiedene Primzahlen und $e \in \mathbb{N}^+$ mit der Eigenschaft* $\mathrm{ggT}((p-1)(q-1), e) = 1$. *Dann ist die Abbildung*

$$\mathbb{Z}/pq\mathbb{Z} \to \mathbb{Z}/pq\mathbb{Z}, \quad \alpha \mapsto \alpha^e$$

bijektiv. Ihre Umkehrabbildung wird gegeben durch $\alpha \mapsto \alpha^d$, wobei $d \in \mathbb{N}$ mit $ed \equiv 1 \mod (p-1)(q-1)$ ist (da e und $(p-1)(q-1)$ teilerfremd sind, gibt es so ein d nach Satz 3.2.5).

Beweis. Es genügt $\alpha^{de} = \alpha$ für jedes $\alpha \in \mathbb{Z}/pq\mathbb{Z}$ zu zeigen. Es sei also $\alpha \in \mathbb{Z}/pq\mathbb{Z}$. Wir wählen $a \in \mathbb{Z}$ mit $\alpha = \bar{a}$. Also müssen wir uns jetzt $a^{de} \equiv a \mod pq$, d.h. $pq \mid a^{de} - a$ überlegen. Da p und q verschieden sind (also teilerfremd sind) ist dies äquivalent zu

$$p \mid a^{de} - a \text{ und } q \mid a^{de} - a \quad .$$

für alle $a \in \mathbb{Z}$. Es genügt die linke Teilbarkeit zu zeigen. Gilt $p \mid a$, so auch $p \mid a^{de}$ und damit $p \mid a^{de} - a$. Gilt jedoch $p \nmid a$ so gilt $a^{p-1} \equiv 1 \mod p$ (kleiner Fermat 3.3.9). Wegen $de \equiv 1 \mod (p-1)(q-1)$ gibt es $k \in \mathbb{Z}$ mit $de = 1 + k(p-1)(q-1)$. Wegen de, $(p-1)(q-1) \in \mathbb{N}^+$ ist $k \in \mathbb{N}$. Es folgt

$$a^{de} = a \cdot (a^{p-1})^{k(q-1)} \equiv a \cdot 1^{k(q-1)} = a \mod p \quad ,$$

also $p \mid a^{de} - a$. □

Wenn nun zwei Partner etwa Alice und Bob mit Hilfe des RSA Verfahrens einen Schlüssel bestimmen wollen, gehen sie so vor: Alice wählt zwei verschiedene Primzahlen p und q und eine natürliche Zahl e mit $\mathrm{ggT}((p-1)(q-1), e) = 1$. Weiters berechnet sie $N = pq$ und ein $d \in \mathbb{N}$ mit $ed \equiv 1 \mod (p-1)(q-1)$. Das kann sie bekanntlich mit dem erweiterten euklidischen Algorithmus. Sie veröffentlicht nun (N, e) als öffentlichen Schlüssel.

Will nun Bob einen geheimen Schlüssel $x \in \mathbb{Z}/N\mathbb{Z}$ an Alice senden, so berechnet er $c = x^e$ und schickt c an Alice, welche x aus $x = c^d$ erhält.

Die Sicherheit des RSA Verfahren beruht auf zwei Tatsachen:

- Zur Zeit ist die einzige bekannte Methode, Kongruenzen der Form $x^e \equiv a \mod N = pq$ zu lösen, das d mit $ed \equiv 1 \mod (p-1)(q-1)$ zu bestimmen.
- Um dieses d zu bestimmen, benötigt man zur Zeit noch $(p-1)(q-1)$, also p und q. Man muss also die Primfaktorzerlegung von N bestimmen können. Dafür gibt es noch kein Verfahren mit vernünftiger Laufzeit.

Um die Sicherheit des RSA Verfahrens zu gewährleisten wird momentan empfohlen die Primzahlen p und q in der Größenordnung von 2^{2048} zu wählen. Zur Wahl von e: die kleinst mögliche Wahl für e ist $e = 3$. Die Wahl von einem kleinem e birgt aber Unsicherheiten. Es wird daher empfohlen $e \sim 2^{16} + 1$ zu wählen.