Unterlagen zur elementaren Zahlentheorie

Erhard Aichinger

Linz, im Oktober 2005

Univ.-Doz. Dr. Erhard Aichinger
Institut für Algebra
Universität Linz
4040 Linz, Österreich
erhard@algebra.uni-linz.ac.at

KAPITEL 1

Rechnen in den ganzen Zahlen

1. Teilbarkeit

Definition 1.1 (Primzahl). Eine Zahl $p \in \mathbb{N}$ ist genau dann eine *Primzahl*, wenn folgende beiden Bedingungen gelten:

(1) Es gilt $p > 1$.
(2) Für alle $a, b \in \mathbb{N}$ mit $p = a \cdot b$ gilt $a = 1$ oder $b = 1$.

Definition 1.2 (Teilbarkeit). Für $x, y \in \mathbb{Z}$ gilt

$$x \textit{ teilt } y$$

genau dann, wenn es ein $z \in \mathbb{Z}$ gibt, sodass $y = z \cdot x$ ist.

Wir schreiben dann auch $x|y$; die Zahl y heißt ein *Vielfaches* von x;

Satz 1.3. *Seien $a \in \mathbb{Z}$ und $n \in \mathbb{N}$. Dann gibt es genau ein Paar von Zahlen (q, r), sodass $a = q \cdot n + r$ und $r \in \{0, \ldots, n-1\}$.*

Wir bezeichnen den Rest r mit $a \bmod b$.

Definition 1.4 (Größter gemeinsamer Teiler). Für zwei Zahlen $a, b \in \mathbb{Z}$ (nicht beide 0) ist $\mathrm{ggT}\,(a, b)$ die größte Zahl $z \in \mathbb{N}$ mit $z \mid a$ und $z \mid b$.

Satz 1.5. *Seien $a, b \in \mathbb{Z}$, nicht beide 0 und sei $z \in \mathbb{Z}$. Dann gilt:*

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

So gilt zum Beispiel $\mathrm{ggT}\,(25, 15) = \mathrm{ggT}\,(40, 15)$.

Beweis: Wir zeigen, dass nicht nur der ggT, sondern sogar die Mengen der gemeinsamen Teiler der beiden Zahlenpaare gleich sind. Wir zeigen also

$$\{t \mid t \mid a \text{ und } t \mid b\} = \{t \mid t \mid a + zb \text{ und } t \mid b\}\,.$$

"$\subseteq$": Falls t sowohl a als auch b teilt, dann auch $a + zb$ und b. "$\supseteq$": Falls t sowohl $a + zb$, als auch b teilt, dann auch $a + zb - zb$ und b, also auch a und b. $\square$

Das nützen wir jetzt möglichst geschickt aus, um ggT (147, 33) zu berechnen:

$$\begin{aligned} \text{ggT }(147,33) &= \text{ggT }(147-4\cdot 33, 33)\\ &= \text{ggT }(15,33)\\ &= \text{ggT }(15, 33-2\cdot 15)\\ &= \text{ggT }(15,3)\\ &= \text{ggT }(0,3)\\ &= 3. \end{aligned}$$

Günstig ist es also, z so zu wählen, dass $a + zb$ der Rest von a bei der Division durch b wird.

Mit Hilfe des *erweiterten Euklidischen Algorithmus* findet man nicht nur den ggT von a und b, sondern auch $u, v \in Z$, sodass gilt:

$$ggT\,(a,b) = u\cdot a + v \cdot b.$$

Beispiel: Wir berechnen ggT (147, 33), und schreiben das so:

	147	33	
147	1	0	$(147 = 1\cdot 147 + 0\cdot 33)$
33	0	1	$(33 = 0\cdot 147 + 1\cdot 33)$
15	1	-4	$(15 = 1\cdot 146 - 4\cdot 33)$
3	-2	9	$(3 = -2\cdot 147 + 9\cdot 33)$
0			

Berechnet man ggT (a, b) mithilfe dieses Algorithmus, sieht man, dass sich die auftretenden Zahlen immer als Linearkombination von a und b schreiben lassen. Als Konsequenz davon erhalten wir folgenden Satz:

Satz 1.6. *Seien $a, b \in \mathbb{Z}$ (nicht beide 0). Dann gibt es $u, v \in \mathbb{Z}$, sodass*

$$\text{ggT }(a,b) = u\cdot a + v\cdot b.$$

Eine Folgerung davon ist:

Satz 1.7. *Seien $a, b \in \mathbb{Z}$, nicht beide* 0, *und sei $t \in \mathbb{Z}$ so, dass $t|a$ und $t|b$. Dann gilt auch $t|\text{ggT}\,(a, b)$.*

Beweis: Seien $u, v \in \mathbb{Z}$ so, dass ggT $(a, b) = ua + vb$. Da t die Zahl a teilt, ist auch ua ein Vielfaches von t. Ebenso ist vb ein Vielfaches von t. Somit ist auch die Summe $ua + vb$ ein Vielfaches von t. Die Zahl t ist also ein Teiler von ggT (a, b).

Wenn a und b größten gemeinsamen Teiler 1 haben, so heißen sie *teilerfremd* oder *relativ prim*.

Satz 1.8. *Seien $a, b, c \in \mathbb{Z}$, und sei zumindest eine der Zahlen a und b nicht 0. Wir nehmen an, dass a die Zahl $b \cdot c$ teilt, und dass $\mathrm{ggT}(a, b) = 1$ gilt. Dann gilt: a teilt c.*

Beweis: Es gibt $u, v \in \mathbb{Z}$, sodass

$$1 = u \cdot a + v \cdot b.$$

Weil $a \mid uac$, und da wegen $a|bc$ auch $a \mid vbc$ gilt, gilt auch

$$a \mid (ua + vb)c;$$

also auch $a \mid c$. □

Daraus kann man folgenden Satz herleiten:

Satz 1.9.

(1) *Jede natürliche Zahl $a \geq 2$ besitzt eine Zerlegung in Primfaktoren*

$$a = p_1 \cdot \ldots \cdot p_n.$$

(2) *Die Primfaktorenzerlegung einer natürlichen Zahl $a \geq 2$ ist bis auf die Reihenfolge der Primfaktoren eindeutig. Wenn also*

$$a = p_1 \cdot \ldots \cdot p_n = q_1 \cdot \ldots \cdot q_m$$

und alle p_i, q_i Primzahlen sind, dann gilt $m = n$, und es gibt eine bijektive Abbildung $\pi : \{1, \ldots, n\} \to \{1, \ldots, m\}$, sodass $p_i = q_{\pi(i)}$.

Sind $a, b \in \mathbb{Z}$, so nennt man jede Zahl $c \in \mathbb{Z}$, die von a und b geteilt wird, ein gemeinsames Vielfaches von a und b. Unter allen gemeinsamen Vielfachen zeichnen wir das kleinste aus.

Definition 1.10. Es seien $a, b \in \mathbb{Z} \setminus \{0\}$. Dann ist $\mathrm{kgV}\ (a, b)$ definiert durch

$$\mathrm{kgV}\ (a, b) = \min \{v \in \mathbb{N} \mid a \mid v \text{ und } b \mid v\}.$$

Die Menge aller positiven gemeinsamen Vielfachen ist ja für $a, b \in \mathbb{Z} \setminus \{0\}$ bestimmt nicht leer, da sie $|a \cdot b|$ enthält.

Satz 1.11. *Seien $a, b \in \mathbb{Z} \setminus \{0\}$, und sei $s \in \mathbb{Z}$ so, dass $a \mid s$ und $b \mid s$. Dann gilt:*

$$\mathrm{kgV}\ (a, b) \mid s.$$

Jedes gemeinsame Vielfache ist also ein Vielfaches des kgV .

Beweis: Wir dividieren s durch $\mathrm{kgV}(a, b)$ und erhalten somit $r \in \{0, \ldots, \mathrm{kgV}(a, b) - 1\}$ und $q \in \mathbb{Z}$, sodass

$$s = q \cdot \mathrm{kgV}(a, b) + r.$$

Also gilt $r = s - q \cdot \mathrm{kgV}\,(a,b)$. Sowohl s also auch $q \cdot \mathrm{kgV}\,(a,b)$ sind Vielfache von a und Vielfache von b. Ihre Differenz r ist also ebenfalls ein Vielfaches von a und von b. Da $r < \mathrm{kgV}\,(a,b)$, und da $\mathrm{kgV}\,(a,b)$ das kleinste gemeinsame Vielfache ist, muss $r = 0$ gelten. Also ist s ein Vielfaches von $\mathrm{kgV}\,(a,b)$.

Zwischen ggT und kgV kann man folgenden Zusammenhang herstellen:

Satz 1.12. *Seien $a, b \in \mathbb{N}$. Dann gilt*

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

Beweis: Wir verwenden die Primfaktorzerlegung von $a = \prod p_i^{\nu_i}$, und $b = \prod p_i^{\sigma_i}$. Aus der Eindeutigkeit der Primfaktorzerlegung kann man herleiten, dass dann gelten muss:

$$\begin{aligned} \mathrm{ggT}\ (a,b) &= \prod p_i^{\min(\nu_i,\sigma_i)} \\ \mathrm{kgV}\ (a,b) &= \prod p_i^{\max(\nu_i,\sigma_i)}. \end{aligned}$$

Daraus folgt:

$$\begin{aligned} \mathrm{ggT}\ (a,b) \cdot \mathrm{kgV}\ (a,b) &= \prod p_i^{\left(\min(\nu_i,\sigma_i)+\max(\nu_i,\sigma_i)\right)} \\ &= \prod p_i^{(\nu_i+\sigma_i)} \\ &= a \cdot b. \end{aligned}$$

□

Satz 1.13. *Seien $a, b, c \in \mathbb{N}$. Dann gilt:*

(1) $\mathrm{ggT}\,(\mathrm{ggT}\,(a,b),c) = \mathrm{ggT}\,(a, \mathrm{ggT}\,(b,c))$.
(2) $\mathrm{kgV}\,(\mathrm{kgV}\,(a,b),c) = \mathrm{kgV}\,(a, \mathrm{kgV}\,(b,c))$.
(3) $\mathrm{ggT}\,(\mathrm{kgV}\,(a,b),c) = \mathrm{kgV}\,(\mathrm{ggT}\,(a,c), \mathrm{ggT}\,(b,c))$.
(4) $\mathrm{kgV}\,(\mathrm{ggT}\,(a,b),c) = \mathrm{ggT}\,(\mathrm{kgV}\,(a,c), \mathrm{kgV}\,(b,c))$.

2. Lösen von Kongruenzen

Definition 1.14. Sei $n \in \mathbb{Z}$. Dann definieren wir eine Relation $\equiv_n$ auf $\mathbb{Z}$ durch

$$a \equiv_n b :\Leftrightarrow n \mid a - b \text{ für } a, b \in \mathbb{Z}.$$

Für $a \equiv_n b$ schreiben wir auch $a \equiv b \pmod{n}$ und sagen: "a ist kongruent b modulo n."

Satz 1.15. *Seien $a, c \in \mathbb{Z}$ (nicht beide $= 0$), und sei $b \in \mathbb{Z}$. Dann sind die folgenden Bedingungen äquivalent:*

(1) *Die Kongruenz*
$$ax \equiv b \pmod{c}$$
ist lösbar, d. h., es gibt $y \in \mathbb{Z}$ sodass $c | a \cdot y - b$.
(2) $\mathrm{ggT}\ (a,c)$ *teilt b.*

Beweis: "(1) $\Rightarrow$ (2)": Sei x eine Lösung, d.h. $c \mid ax - b$. Falls c die Zahl $ax - b$ teilt, dann gilt erst recht

$$\text{ggT }(a, c) \mid ax - b.$$

ggT (a, c) teilt a, also gilt ggT $(a, c) \mid b$.

"(2) $\Rightarrow$ (1)": Aufgrund der Voraussetzungen existiert ein $z \in \mathbb{Z}$, sodass

$$\text{ggT }(a, c) \cdot z = b.$$

Aus dem erweiterten Euklidischen Algorithmus bekommen wir $u, v \in \mathbb{Z}$ mit

$$ggT\,(a, c) = u \cdot a + v \cdot c.$$

Es gilt dann

$$(ua + vc) \cdot z = b,$$

also

$$a \cdot uz + c \cdot vz = b,$$

und somit

$$a \cdot (uz) \equiv b \pmod{c}.$$

Also ist $x := uz$ Lösung von $ax \equiv b \,(\bmod\, c)$. $\square$

Satz 1.16. *Seien $a, c \in \mathbb{Z}$ (nicht beide $= 0$), und sei $b \in \mathbb{Z}$. Sei x_0 eine Lösung von*

$$ax \equiv b \pmod{\text{c}}. \tag{2.1}$$

Dann ist die Lösungsmenge von (2.1) *gegeben durch:*

$$L = \left\{ x_0 + k \cdot \frac{c}{ggT\,(a, c)} \mid k \in \mathbb{Z} \right\}.$$

Beweis: "$\supseteq$": Wir setzen zunächst $x_0 + k\frac{c}{\text{ggT }(a,c)}$ ein und erhalten

$$\begin{aligned} a\left(x_0 + k\tfrac{c}{\text{ggT }(a,c)}\right) &= ax_0 + ak\tfrac{c}{\text{ggT }(a,c)} \\ &\equiv_c b + ak\tfrac{c}{\text{ggT }(a,c)} \\ &= b + ck\tfrac{a}{\text{ggT }(a,c)} \\ &\equiv_c b. \end{aligned}$$

Daher ist $x_0 + k\frac{c}{\text{ggT }(a,c)}$ wirklich eine Lösung.

"$\subseteq$": Sei x_1 Lösung von $ax \equiv b \pmod{c}$. Zu zeigen ist: $\frac{c}{\text{ggT }(a,c)} \mid (x_1 - x_0)$. Da x_1 und x_0 Lösungen sind, gilt $ax_1 \equiv b \pmod{c}$ und $ax_0 \equiv b \pmod{c}$. Daher gilt

$$a\,(x_1 - x_0) \equiv 0 \pmod{c},$$

oder, äquivalent dazu,

$$c \mid a\,(x_1 - x_0).$$

Daher gilt auch

$$\frac{c}{\text{ggT }(a, c)} \mid \frac{a}{\text{ggT }(a, c)} \cdot (x_1 - x_0).$$

Da

$$\mathrm{ggT}\left(\frac{c}{\mathrm{ggT}\ (a,c)}, \frac{a}{\mathrm{ggT}\ (a,c)}\right) = 1,$$

gilt

$$\frac{c}{\mathrm{ggT}\ (a,c)} \mid (x_1 - x_0)\,.$$

□

Bemerkung: Das System $ax \equiv b \pmod c$ ist also äquivalent zu

$$x \equiv x_0 \ \left(\mathrm{mod}\ \frac{c}{\mathrm{ggT}\,(a,c)}\right),$$

wobei x_0 eine spezielle Lösung von $ax \equiv b \pmod c$ ist.

Wir betrachten nun Systeme von zwei Kongruenzen, also Systeme der Form

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2}\,, \end{aligned}$$

wobei $m_1, m_2 \in \mathbb{N}$ und $a_1, a_2 \in \mathbb{Z}$.

Beispiele: Das System

$$\begin{aligned} x &\equiv 1 \pmod 2 \\ x &\equiv 0 \pmod 4 \end{aligned}$$

kann nicht lösbar sein, denn eine Lösung $x \in \mathbb{Z}$ müsste sowohl gerade als auch ungerade sein. Das System

$$\begin{aligned} x &\equiv 1 \pmod 2 \\ x &\equiv 2 \pmod 5 \end{aligned}$$

hat zum Beispiel die Lösung $x = 7$.

Satz 1.17. *Seien $a_1, a_2 \in \mathbb{Z}$, $m_1, m_2 \in \mathbb{N}$. Das System*

$$\begin{aligned} x &\equiv a_1 \pmod{\mathrm{m}_1} \\ x &\equiv a_2 \pmod{\mathrm{m}_2} \end{aligned}$$

ist genau dann lösbar, wenn gilt

$$\mathrm{ggT}\ (m_1, m_2) \mid a_1 - a_2.$$

Beweis: “⇒”: Wir nehmen an, dass x Lösung ist. Dann gilt: $m_1 \mid (x - a_1)$ und $m_2 \mid (x - a_2)$. Daher gilt auch $\mathrm{ggT}\ (m_1, m_2) \mid (x - a_1)$ und $\mathrm{ggT}\,(m_1, m_2) \mid (x - a_2)$, und somit

$$\mathrm{ggT}\ (m_1, m_2) \mid (x - a_2) - (x - a_1) = (a_1 - a_2)\,.$$

"$\Leftarrow$" Es gibt $u, v \in \mathbb{Z}$, sodass

$$\begin{aligned} u \cdot m_1 + v \cdot m_2 &= ggT\,(m_1, m_2) \\ k \cdot u \cdot m_1 + k \cdot v \cdot m_2 &= a_1 - a_2 \\ a_2 + k \cdot v \cdot m_2 &= \underbrace{a_1 - k \cdot u \cdot m_1}_{=x} \end{aligned}$$

daher ist $x := a_1 - kum_1$ Lösung des Systems. □

Der Beweis liefert auch gleich ein Lösungsverfahren.

Beispiel: Wir lösen:

$$\begin{aligned} x &\equiv 2 \pmod{15} \\ x &\equiv 8 \pmod{21} \end{aligned}$$

Da ggT $(15, 21) = 3$ und $3 \mid (2 - 8)$ ist das System lösbar. Wir berechnen jetzt diesen ggT und *Kofaktoren* (d.h. Koeffizienten für eine Linearkombination von 15 und 21, die den ggT ergibt).

	21	15
21	1	0
15	0	1
6	1	-1
3	-2	3

und erhalten daraus $3 = 3 \cdot 15 - 2 \cdot 21$.

$$\begin{aligned} 3 \cdot 15 - 2 \cdot 21 &= 3 \\ (-6) \cdot 15 + 4 \cdot 21 &= 2 - 8 \\ \underbrace{8 + 4 \cdot 21}_{=92} &= \underbrace{2 + 6 \cdot 15}_{=92} \end{aligned}$$

Daher erhalten wir eine Lösung: $x = 92$.

Der folgende Satz gibt an, wie wir aus einer Lösung der Kongruenz alle Lösungen erhalten.

SATZ 1.18. *Sei x_0 eine Lösung von*

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2}. \end{aligned}$$

Dann gilt für die Lösungmenge L

$$L = \{x_0 + k \cdot \mathrm{kgV}\ (m_1, m_2) \mid k \in \mathbb{Z}\}.$$

Beweis: "$\supseteq$": Wir setzen

$$x_0 + k \cdot \mathrm{kgV}\ (m_1, m_2)$$

in die erste Kongruenz ein und erhalten

$$(x_0 + k \cdot \mathrm{kgV}\ (m_1, m_2)) \equiv a_1 \pmod{m_1}.$$

Das gleiche gilt für die zweite Kongruenz.

"$\subseteq$": Wir fixieren $x_1 \in L$. Um zu zeigen, dass $x_1 \in \{x_0 + k \cdot \mathrm{kgV}\ (m_1, m_2) \mid k \in \mathbb{Z}\}$, zeigen wir, dass $x_1 - x_0$ ein Vielfaches von kgV (m_1, m_2) ist. Wir wissen ja, dass

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \end{aligned}$$

Daher gilt $(x_1 - x_0) \equiv 0 \pmod{m_1}$ und somit $m_1 \mid (x_1 - x_0)$. Ebenso zeigt man, dass $m_2 \mid (x_1 - x_0)$ gilt.

Da das kgV jedes gemeinsame Vielfache teilt, gilt kgV $(m_1, m_2) \mid (x_1 - x_0)$. □

Die folgenden Sätze zeigen uns, wie man das Lösen von Systemen aus mehr als zwei Kongruenzen auf das Lösen von Systemen aus zwei Kongruenzen zurückführen kann. Der erste Satz zeigt, dass man ein System von Kongruenzen durch eine einzige Kongruenz ersetzen kann – vorausgesetzt, man kennt zumindest *eine* Lösung des Systems.

Satz 1.19. *Seien $r \in \mathbb{N}$, $m_1, m_2, \ldots, m_r \in \mathbb{N}$ und $a_1, a_2, \ldots, a_r \in \mathbb{Z}$. Falls das System*

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \\ &\vdots \\ x &\equiv a_r \pmod{m_r} \end{aligned} \tag{2.2}$$

eine Lösung x_0 hat, dann ist (2.2) äquivalent zu

$$x \equiv x_0 \pmod{\mathrm{kgV}\,(m_1, m_2, \ldots, m_r)}.$$

Beweisskizze: Falls x_0 eine Lösung ist, dann ist auch jedes

$$x_0 + k \cdot \mathrm{kgV}\,(m_1, m_2, \ldots, m_r)$$

eine Lösung. Andererseits haben zwei verschiedene Lösungen die gleichen Reste modulo jedem m_i, ihre Differenz ist daher ein gemeinsames Vielfaches der m_i und somit ein Vielfaches des kgV . □

Der folgende Satz sagt, wann ein System von Kongruenzen lösbar ist.

Satz 1.20 (Chinesischer Restsatz). *Seien $r \in \mathbb{N}$, $a_1, \ldots, a_r \in \mathbb{Z}$, $m_1, \ldots, m_r \in \mathbb{Z} \setminus \{0\}$. Dann sind folgende drei Aussagen äquivalent.*

(1) *Es gibt* $x \in \mathbb{Z}$*, sodass*

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \\ &\vdots \\ x &\equiv a_r \pmod{m_r}. \end{aligned}$$

(2) *Für alle* $i, j \in \{1, 2, \ldots, r\}$ *ist das System*

$$\begin{aligned} x &\equiv a_i \pmod{m_i} \\ x &\equiv a_j \pmod{m_j} \end{aligned}$$

lösbar.

(3) *Für alle* $i, j \in \{1, 2, \ldots, r\}$ *gilt*

$$\operatorname{ggT}(m_i, m_j) \mid a_i - a_j.$$

Beispiel: Wir lösen folgendes System

$$\begin{aligned} x &\equiv 2 \pmod{15} \\ x &\equiv 8 \pmod{21} \\ x &\equiv 7 \pmod{55} \end{aligned} \tag{2.3}$$

Wir kennen bereits die Lösungen von $x \equiv 2 \pmod{15}$, $x \equiv 8 \pmod{21}$. Das System (2.3) ist daher äquivalent zu

$$\begin{aligned} x &\equiv 92 \pmod{105} \\ x &\equiv 7 \pmod{55}. \end{aligned}$$

Wir berechnen $\operatorname{ggT}(55, 105)$ und die Kofaktoren nach dem Euklidschen Algorithmus und erhalten

	105	55
105	1	0
55	0	1
50	1	-1
5	-1	2
0		

und daher

$$\begin{aligned} (-1) \cdot 105 + 2 \cdot 55 &= 5 \\ (-17) \cdot 105 + 34 \cdot 55 &= 92 - 7 \\ 7 + 34 \cdot 55 &= 92 + 17 \cdot 105. \end{aligned}$$

Daraus erhalten wir also, dass 1877 die Lösung ist, also geben wir die Lösungsmenge folgendermaßen an:

$$\begin{aligned} L &= \{x \in \mathbb{Z} \mid x \equiv 1877 \pmod{1155}\} \\ &= \{x \in \mathbb{Z} \mid x \equiv 722 \pmod{1155}\}. \end{aligned}$$

3. Der Ring $\mathbb{Z}_n$

In $\mathbb{Z}$ definieren wir für $n \in \mathbb{N}$ die Relation $\equiv_n$ durch

$$a \equiv_n b :\Leftrightarrow n \mid b - a.$$

Alle zu a kongruenten Elemente fassen wir zu einer *Restklasse modulo n* zusammen. Wir nennen diese Kallse $[a]_n$.

$$[a]_n := \{a + z \cdot n \mid z \in \mathbb{Z}\}$$

Die Menge aller Restklassen modulo n bezeichnen wir mit $\mathbb{Z}_n$.

$$\mathbb{Z}_n = \{[a]_n \mid a \in \mathbb{Z}\}.$$

$\mathbb{Z}_n$ hat n Elemente, und zwar $[0]_n, [1]_n, \ldots, [n-1]_n$. Auf $\mathbb{Z}_n$ definieren wir $\oplus$ und $\odot$ durch:

$$\begin{aligned} [a]_n \oplus [b]_n &:= [a+b]_n \\ [a]_n \odot [b]_n &:= [a \cdot b]_n . \end{aligned}$$

Wir müssen zeigen, dass $\oplus$ und $\odot$ wohldefiniert sind; wir geben hier nur den Beweis für die Wohldefiniertheit von $\odot$. Wir wählen also $a, a', b, b' \in \mathbb{Z}$ sodass $[a]_n = [a']_n$ und $[b]_n = [b']_n$. Zu zeigen ist, dass dann

$$[a \cdot b]_n = [a' \cdot b']_n$$

gilt. Es ist also zu zeigen:

$$\begin{aligned} &n \mid a \cdot b - a' \cdot b' \\ &n \mid a \cdot b - ab' + ab' - a'b' \\ &n \mid a \cdot (b - b') + b' \cdot (a - a') . \end{aligned}$$

Das gilt, denn laut Vorraussetzung gilt $n \mid (b - b')$ und $n \mid (a - a')$. Daher ist $[a \cdot b]_n = [a' \cdot b']_n$, und somit ist das Ergebnis von $[a]_n \odot [b]_n$ unabhängig von der Auswahl der Repräsentanten.

Wir geben nun ein Beispiel für eine *nicht* wohldefinierte Operation. Auf der Menge $\mathbb{Q}$ definieren wir die Relation

$$a \sim b :\Leftrightarrow \lfloor a \rfloor = \lfloor b \rfloor .$$

Wir definieren:

$$\lfloor a \rfloor \odot \lfloor b \rfloor := \lfloor a \cdot b \rfloor .$$

$$\begin{array}{lll} a = 0.1 & b = 100 & \lfloor 0.1 \cdot 100 \rfloor = 10 \\ a' = 0 & b' = 100 & \lfloor 0 \cdot 100 \rfloor = 0 \end{array}$$

Da $0 \not\sim 10$, ist die Operation $\odot$ ist also nicht wohldefiniert.

Mengen mit Operationen bezeichnet man als *algebraische Strukturen*. Strukturen, in denen man drei Operationen zur Verfügung hat, die bestimmte, von den Grundrechnungsarten in ganzen Zahlen bekannte, Rechengesetze erfüllen, heißen *Ringe*. Wir betrachten im folgenden Ringe mit Eins; ein Ring mit Eins hat zwei zweistellige Operationen $(+, \cdot)$, eine einstellige Operation $(-)$ und zwei nullstellige Operationen $(0, 1)$.

DEFINITION 1.21. $(R, +, -, \cdot, 0, 1)$ heißt *Ring mit Eins* genau dann, wenn für alle $x, y, z \in R$ die folgenden Eigenschaften erfüllt sind:

(1) $x + 0 = x$
(2) $x + (-x) = 0$
(3) $(x + y) + z = x + (y + z)$
(4) $x + y = y + x$
(5) $(x \cdot y) \cdot z = x \cdot (y \cdot z)$
(6) $(x + y) \cdot z = x \cdot z + y \cdot z$
(7) $x \cdot (y + z) = x \cdot y + x \cdot z$
(8) $1 \cdot x = x$
(9) $x \cdot 1 = x$.

So ist zum Beispiel $(\mathbb{Z}, +, -, \cdot, 0, 1)$ ein Ring mit Eins.

SATZ 1.22. *Sei $(R, +, -, \cdot, 0, 1)$ ein Ring mit Eins. Dann gelten für alle $x, y \in R$ folgende Eigenschaften:*

(1) $0 \cdot x = 0$
(2) $x \cdot (-y) = -(x \cdot y)$
(3) $(-x) \cdot y = -(x \cdot y)$
(4) $x \cdot 0 = 0$.

DEFINITION 1.23. Ein Element $a \in \mathbb{Z}_n$ heißt *invertierbar*, falls es ein $b \in \mathbb{Z}_n$ gibt, sodass

$$a \cdot b = [1]_n .$$

Beispiel: Betrachten wir etwa $\mathbb{Z}_6$:

$[1]_6$	ist invertierbar	$[1]_6 \cdot [1]_6 = [1]_6$
$[2]_6$	ist nicht invertierbar	
$[3]_6$	ist nicht invertierbar	
$[4]_6$	ist nicht invertierbar	
$[5]_6$	ist invertierbar	$[5]_6 \cdot [5]_6 = [1]_6$
$[0]_6$	ist nicht invertierbar	

Beispiel: In $\mathbb{Z}_5$ gilt:

$$\begin{aligned} [1]_5 \cdot [1]_5 &= [1]_5 \\ [2]_5 \cdot [3]_5 &= [1]_5 \\ [3]_5 \cdot [2]_5 &= [1]_5 \\ [4]_5 \cdot [4]_5 &= [1]_5 \end{aligned}$$

$[0]_5$ ist aber nicht invertierbar.

Der folgende Satz gibt an, welche Elemente in $\mathbb{Z}_n$ invertierbar sind.

SATZ 1.24 (Invertierbarkeit). *Sei $n \in \mathbb{N}$ und $a \in \mathbb{Z}$. Dann ist $[a]_n$ genau dann invertierbar in $\mathbb{Z}_n$, wenn* ggT $(a, n) = 1$.

SATZ 1.25. *Seien a, b invertierbare Elemente aus $\mathbb{Z}_n$. Dann ist auch $a \cdot b$ invertierbar.*

Beweis: Seien $u, v \in \mathbb{Z}_n$ so, dass $a \cdot u = [1]_n$ und $b \cdot v = [1]_n$. Dann gilt: $a \cdot b \cdot v \cdot u = [1]_n$. $\square$

DEFINITION 1.26 (Euler'sche $\varphi-$Funktion). Sei $n \in \mathbb{N}$, $n > 1$. Dann ist $\varphi(n)$ definiert durch

$$\begin{aligned} \varphi(n) &:= |\{a \in \mathbb{Z}_n \mid a \text{ invertierbar}\}| = \\ &= |\{x \in \{1, 2, \ldots, n-1\} \mid \text{ggT } (x, n) = 1\}| . \end{aligned}$$

Wir berechnen $\varphi(12) = |\{1, 5, 7, 11\}| = 4$ und $\varphi(8) = |\{1, 3, 5, 7\}| = 4$.

SATZ 1.27 (Satz von Euler). *Sei $n \in \mathbb{N}$, $n > 1$, $a \in \mathbb{Z}$,* ggT $(a, n) = 1$. *Dann gilt:*

$$a^{\varphi(n)} \equiv 1 \pmod{n} .$$

Wir überprüfen diesen Satz durch zwei Beispiele:

- Gilt $7^{\varphi(12)} \equiv 1 \pmod{12}$? Ja, denn es ist $7^4 \equiv 1 \pmod{12}$,
- Gilt $3^{\varphi(5)} \equiv 1 \pmod{5}$? Ja, denn es gilt $3^4 \equiv 1 \pmod{5}$.

Beweis von Satz 1.27: Wir wählen $n \in \mathbb{N}$ und $a \in \mathbb{Z}$ beliebig aber fest, und nehmen an, dass ggT $(a, n) = 1$. Sei

$$I := \{x \in \mathbb{Z}_n \mid x \text{ ist invertierbar}\} .$$

Wir wissen bereits, dass $|I| = \varphi(n)$. Wir definieren

$$\begin{array}{rcccl} f & : & I & \longrightarrow & \mathbb{Z}_n \\ & & x & \longmapsto & x \odot [a]_n \end{array}$$

und zeigen, dass f injektiv ist. Dazu fixieren wir $x, y \in I$ mit $f(x) = f(y)$. Das heißt: $x \cdot [a]_n = y \cdot [a]_n$. Da ggT $(a, n) = 1$, gibt es $b \in \mathbb{Z}$ mit $[a]_n \cdot [b]_n = [1]_n$. Wir erhalten also $x \cdot [a]_n \cdot [b]_n = y \cdot [a]_n \cdot [b]_n$ und damit $x = y$. Daher ist f injektiv. Nun zeigen wir:

$$f(I) = I.$$

"$\subseteq$": Wir fixieren $x \in f(I)$. Es gibt also $y \in I$, sodass $x = y \cdot [a]_n$. Da $y \in I$, ist y invertierbar, und somit ist auch $y \cdot [a]_n = x$ invertierbar.

"$\supseteq$": Sei $x \in I$. Wir wählen $b \in \mathbb{Z}$ mit $[b]_n \cdot [a]_n = [1]_n$. Das Element $x \cdot [b]_n$ ist invertierbar und es gilt $f(x \cdot [b]_n) = x$. Also ist x wirklich das Bild eines invertierbaren Elements und liegt somit in $f(I)$.

Die Funktion f ist also eine bijektive Abbildung von I nach I.

Es gilt also:

$$\begin{aligned}\prod_{x\in I} x &= \prod_{x\in I} f(x)\\ \prod_{x\in I} x &= \prod_{x\in I} \left(x\cdot [a]_n\right)\\ \prod_{x\in I} x &= \left(\prod_{x\in I} x\right)\cdot \left([a]_n\right)^{\varphi(n)}\end{aligned}$$

Sei $y\in\mathbb{Z}_n$ das Inverse zu $\prod_{x\in I} x$. Dann gilt:

$$y\cdot\prod_{x\in I} x = y\cdot\left(\prod_{x\in I} x\right)\cdot \left([a]_n\right)^{\varphi(n)}$$

$$[1]_n = \left([a]_n\right)^{\varphi(n)}$$
$$1 \equiv a^{\varphi(n)} \pmod{n}.$$

□

Korollar 1.28. *Sei p eine Primzahl, und sei $z\in\mathbb{Z}$. Dann gilt*

$$z^p \equiv z \pmod{p}.$$

Falls p kein Teiler von z ist, gilt

$$z^{p-1}\equiv 1 \pmod{p}.$$

Beweis: Wir wählen eine Primzahl p und $z\in\mathbb{Z}$ beliebig, aber fest, und nehmen an, dass p die Zahl z nicht teilt. Wir wissen, dass $\varphi(p) = p-1$, und daher gilt nach dem Satz von Euler

$$z^{p-1}\equiv 1 \pmod{p}.$$

Da $p|(z^{p-1}-1)$, gilt auch $p|(z^p-z)$, und somit $z^p\equiv z \pmod{p}$.

Wenn $p\mid z$, dann teilt p sowohl z als auch z^p. □

Satz 1.29. *Für alle $a,b\in\mathbb{Z}_p$ gilt: $(a+b)^p = a^p+b^p$.*

Satz 1.30. *Seien p,q Primzahlen, $p\neq q$ und seien $a,s\in\mathbb{Z}$. Dann gilt:*

$$a^{1+s(p-1)(q-1)}\equiv a \pmod{p\cdot q}.$$

Beweis:

- *1. Fall:* $\operatorname{ggT}(a,pq) = 1$*:* Wir wissen ja, dass $a^{p-1}\equiv 1 \pmod{p}$ gilt (Satz von Euler), daher gilt auch $\left(a^{p-1}\right)^{(q-1)\cdot s}\equiv 1 \pmod{p}$. Somit ist p ein Teiler von $a^{(p-1)\cdot(q-1)\cdot s}-1$ und damit auch von $a^{(p-1)\cdot(q-1)\cdot s+1}-a$. Ebenso zeigen wir

$$q\mid a^{(p-1)\cdot(q-1)\cdot s+1}-a.$$

Damit gilt insgesamt:

$$pq \mid a^{(p-1)\cdot(q-1)\cdot s+1} - a.$$

- *2. Fall:* ggT $(a, pq) = p$: Da der ggT $(a, q) = 1$ ist, gilt mit dem Satz von Euler $a^{q-1} \equiv 1 \pmod{q}$, und somit $a^{(q-1)\cdot(p-1)} \equiv 1 \pmod{q}$. Das heißt

$$q \mid a^{(q-1)\cdot(p-1)\cdot s} - 1.$$

Wir wissen ja, dass $p \mid a$. Daher gilt $p \cdot q \mid \left(a^{(q-1)\cdot(p-1)\cdot s} - 1\right) \cdot a$.
- *3. Fall:* ggT $(a, pq) = q$: Beweis genauso wie im 2. Fall.
- *4. Fall:* ggT $(a, pq) = p \cdot q$: Dann ist zu zeigen, dass $0 \equiv 0 \,(\bmod\; pq)$. □

Satz 1.31 (Multiplikativität der φ-Funktion). *Seien $n, m \in \mathbb{N}$, $n \geq 2$, $m \geq 2$. Wenn n, m relativ prim sind, dann gilt*

$$\varphi(n \cdot m) = \varphi(n) \cdot \varphi(m).$$

Der Beweis der Multiplikativität erfordert noch etwas Information über Ringe.

Satz 1.32. *Falls R_1 und R_2 Ringe mit Eins sind, dann ist*

$$(R_1 \times R_2, +_{R_1 \times R_2}, -_{R_1 \times R_2}, \cdot_{R_1 \times R_2}, 0_{R_1 \times R_2}, 1_{R_1 \times R_2})$$

wieder ein Ring mit Eins. Dabei sind die Verknüpfungen auf $R_1 \times R_2$ definiert durch

- $\begin{pmatrix} r_1 \\ r_2 \end{pmatrix} +_{R_1 \times R_2} \begin{pmatrix} s_1 \\ s_2 \end{pmatrix} := \begin{pmatrix} r_1 +_{R_1} s_1 \\ r_2 +_{R_2} s_2 \end{pmatrix}$
- $\begin{pmatrix} r_1 \\ r_2 \end{pmatrix} \cdot_{R_1 \times R_2} \begin{pmatrix} s_1 \\ s_2 \end{pmatrix} := \begin{pmatrix} r_1 \cdot_{R_1} s_1 \\ r_2 \cdot_{R_2} s_2 \end{pmatrix}$
- $-_{R_1 \times R_2} \begin{pmatrix} r_1 \\ r_2 \end{pmatrix} := \begin{pmatrix} -_{R_1} r_1 \\ -_{R_2} r_2 \end{pmatrix}$
- $0_{R_1 \times R_2} := \begin{pmatrix} 0_{R_1} \\ 0_{R_2} \end{pmatrix}$
- $1_{R_1 \times R_2} := \begin{pmatrix} 1_{R_1} \\ 1_{R_2} \end{pmatrix}$.

$R_1 \times R_2$ mit diesen Operationen erfüllt auch alle Ring mit Eins-Rechengesetze.

Rechnen wir zum Beispiel in $\mathbb{Z}_4 \times \mathbb{Z}_5$.

$$\begin{pmatrix} [3]_4 \\ [4]_5 \end{pmatrix} \cdot \begin{pmatrix} [2]_4 \\ [3]_5 \end{pmatrix} = \begin{pmatrix} [2]_4 \\ [2]_5 \end{pmatrix}$$

$R_1 \times R_2$ heißt das *direkte Produkt* von R_1 und R_2.

Definition 1.33. R, S seien Ringe mit Eins. Die Abbildung $\varphi : R \to S$ heißt Ring mit Eins-Homomorphismus: $\Leftrightarrow$

$$\begin{aligned} \forall r_1, r_2 \in R : \quad & \varphi(r_1 +_R r_2) = \varphi(r_1) +_S (r_2), \\ & \varphi(-_R r_1) = -_S \varphi(r_1), \\ & \varphi(r_1 \cdot_R r_2) = \varphi(r_1) \cdot_S \varphi(r_2), \\ & \varphi(0_R) = 0_S, \\ & \varphi(1_R) = 1_S. \end{aligned}$$

Definition 1.34. Ein Homomorphismus φ heißt:

- *Epimorphismus* $:\Leftrightarrow$ φ ist surjektiv;
- *Monomorphismus* $:\Leftrightarrow$ φ ist injektiv;
- *Isomorphismus* $:\Leftrightarrow$ φ ist bijektiv.

Beispiel: Wollen wir uns dies zunächst an zwei Beispielen veranschaulichen.

- $\varphi : \mathbb{Z} \to \mathbb{Z}_5,\ z \mapsto [x]_5$ ist surjektiv, aber nicht injektiv. Also ist φ ein Epimorphismus.
- Wir untersuchen $\alpha : \mathbb{Z}_5 \to \mathbb{Z},\ [x]_5 \mapsto x$. Hier ergibt sich folgendes Problem: $\alpha([3]_5) = 3$, und $\alpha([3]_5) = \alpha([8]_5) = 8$. — Das Problem ist, dass α nicht wohldefiniert ist. Man kann das auch so ausdrücken, dass man sagt, dass die Relation
$$\alpha = \{([x]_5, x) \mid x \in \mathbb{Z}\}$$
nicht funktional (d. h. eine Funktion = Graph einer Funktion) ist. Sie ist nicht funktional, weil $([2]_5, 2) \in \alpha$ und $([2]_5, 7) \in \alpha$.

Definition 1.35. Sei R ein Ring mit Eins. Dann heißt $r \in R$ *invertierbar*, falls es ein $y_r \in R$ gibt, sodass

$$r \cdot y_r = 1_R \text{ und } y_r \cdot r = 1_R.$$

Satz 1.36. *Seien $n, m \in \mathbb{N}$ mit* $\operatorname{ggT}(n, m) = 1$. *Dann ist die Abbildung*

$$\begin{array}{cccc} \varphi : & \mathbb{Z}_{m \cdot n} & \longrightarrow & \mathbb{Z}_n \times \mathbb{Z}_m \\ & [x]_{m \cdot n} & \longmapsto & ([x]_n, [x]_m) \end{array}$$

ein Ring mit Eins-Isomorphismus.

Beweis: Wir führen den Beweis in drei Schritten.

(1) φ ist wohldefiniert: Zu zeigen ist, dass für alle $y, z \in \mathbb{Z}$ mit $[y]_{m \cdot n} = [z]_{m \cdot n}$ die Gleichheiten $[y]_n = [z]_n$ und $[y]_m = [z]_m$ gelten. Zu zeigen ist ist also, dass für alle $y, z \in \mathbb{Z}$ gilt:
$$m \cdot n \mid y - z \Rightarrow (m \mid y - z \wedge n \mid y - z).$$
Das ist aber offensichtlich.

(2) φ ist Homomorphismus: Wir überprüfen die Homomorphismuseigenschaft für $+$. Wir berechnen dazu

$$\begin{aligned}\varphi\left([x]_{n\cdot m}+[y]_{n\cdot m}\right) &= \varphi\left([x+y]_{n\cdot m}\right)\\ &= \left([x+y]_n, [x+y]_m\right)\\ &= \left([x]_n+[y]_n, [x]_m+[y]_m\right)\\ &= \begin{pmatrix}[x]_n\\ [x]_m\end{pmatrix}+\begin{pmatrix}[y]_n\\ [y]_m\end{pmatrix}\\ &= \varphi\left([x]_{n\cdot m}\right)+\varphi\left([y]_{n\cdot m}\right).\end{aligned}$$

(3) φ ist bijektiv: Da beide Mengen endlich und gleich groß sind, reicht es, zu zeigen, dass φ injektiv ist. Wir nehmen also an $\varphi\left([x]_{nm}\right)=\varphi\left([y]_{nm}\right)$. Das heißt $\left([x]_n, [x]_m\right)=\left([y]_n, [y]_m\right)$. Daher gilt $n \mid x-y$ und $m \mid x-y$. Da der ggT $(n,m)=1$ ist, gilt: $n\cdot m \mid x-y$. Wir erhalten daher $[x]_{nm}=[y]_{nm}$. Die Abbildung φ ist also injektiv, somit surjektiv und damit bijektiv. $\square$

Wenn der ggT $(n,m)=1$ ist, dann ist $\mathbb{Z}_n\times\mathbb{Z}_m$ also isomorph zu $\mathbb{Z}_{n\cdot m}$. Da Isomorphismen die Invertierbarkeit erhalten, haben beide Ringe gleich viele invertierbare Elemente. Daraus können wir jetzt die Multiplikativität der $\varphi-$Funktion, also Satz 1.31, herleiten.

Beweis von Satz 1.31:

(1) Anzahl der invertierbaren Elemente von $\mathbb{Z}_n\times\mathbb{Z}_m$: Wir zeigen, dass $\binom{a}{b}\in\mathbb{Z}_n\times\mathbb{Z}_m$ genau dann invertierbar ist, wenn a invertierbar in $\mathbb{Z}_n$ und b invertierbar in $\mathbb{Z}_m$ ist. Dazu fixieren wir zunächst $\binom{a}{b}\in\mathbb{Z}_n\times\mathbb{Z}_m$ und nehmen an, dass $\binom{a}{b}$ invertierbar ist; es gibt also $\binom{c}{d}\in\mathbb{Z}_n\times\mathbb{Z}_m$, sodass $\binom{a}{b}\cdot\binom{c}{d}=1_{\mathbb{Z}_n\times\mathbb{Z}_m}=\binom{[1]_n}{[1]_m}$. Daher ist a in $\mathbb{Z}_n$ invertierbar (mit Inversem c), ebenso b in $\mathbb{Z}_m$ (mit Inversem d).

Nun fixieren wir $a\in\mathbb{Z}_n$, $b\in\mathbb{Z}_m$, beide invertierbar. Falls $a\cdot c=[1]_n$, und $b\cdot d=[1]_m$, dann ist $\binom{c}{d}$ das Inverse zu $\binom{a}{b}$. In $\mathbb{Z}_n$ gibt es $\varphi(n)$ invertierbare Elemente, in $\mathbb{Z}_m$ gibt es $\varphi(m)$ invertierbare Elemente, und somit gibt es in $\mathbb{Z}_n\times\mathbb{Z}_m$ genau $\varphi(n)\cdot\varphi(m)$ invertierbare Elemente.

(2) Anzahl der invertierbaren Elemente in $\mathbb{Z}_{n\cdot m}$: Hier gibt es $\varphi(n\cdot m)$ invertierbare Elemente (nach der Definition von φ).

Damit ist

$$\varphi(n\cdot m)=\varphi(n)\cdot\varphi(m)$$

für $n,m\in\mathbb{N}$ mit ggT $(n,m)=1$ bewiesen. $\square$

Aus der Primfaktorzerlegung von n und aus $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$ kann man jetzt leicht $\varphi(n)$ durch

$$\begin{aligned}\varphi(n) &= \varphi\left(\prod p_i^{\alpha_i}\right)\\ &= \prod \varphi\left(p_i^{\alpha_i}\right)\\ &= \prod p_i^{\alpha_i}\left(1-\frac{1}{p_i}\right)\\ &= \prod p_i^{\alpha_i}\cdot\prod\left(1-\frac{1}{p_i}\right)\\ &= n\cdot\prod\left(1-\frac{1}{p_i}\right)\end{aligned}$$

berechnen. Dazu noch ein Beispiel:

Beispiel: $\varphi(12) = 12\cdot\left(1-\frac{1}{2}\right)\cdot\left(1-\frac{1}{3}\right) = 4 = 2\cdot 2 = \varphi(3)\cdot\varphi(4)$.