JOHANNES KEPLER
UNIVERSITÄT LINZ | JKU

Unterlagen zu den ersten Kapiteln der Vorlesung

Einführung in die Algebra und Diskrete Mathematik

Sommersemester 2012

Erhard Aichinger
Institut für Algebra
Johannes Kepler Universität Linz

Version 8. März 2012

Adresse:

Assoc.-Prof. Dr. Erhard Aichinger
Institut für Algebra, Johannes Kepler Universität Linz
4040 Linz, Österreich
e-mail: erhard.aichinger@jku.at

Version 8.3.2012

Druck: Kopierstelle, Abteilung Service, Universität Linz

Inhaltsverzeichnis

Kapitel 1. Elementare Zahlentheorie 1
1. Primfaktorzerlegung 1
2. Der größte gemeinsame Teiler 3
3. Das kleinste gemeinsame Vielfache 6
4. Lösen von Kongruenzen 8

Kapitel 2. Teilbarkeit in Integritätsbereichen 17
1. Kommutative Ringe mit Eins 17
2. Ideale 17
3. Integritätsbereiche 18
4. Euklidische Integritätsbereiche 19
5. Faktorielle Integritätsbereiche 21
6. Eine Anwendung in der Zahlentheorie 23

Literaturverzeichnis 25

KAPITEL 1

Elementare Zahlentheorie

Wir kürzen die Menge der ganzen Zahlen mit $\mathbb{Z}$ und die Menge $\{1, 2, 3, \ldots\}$ der natürlichen Zahlen mit $\mathbb{N}$ ab.

1. Primfaktorzerlegung

DEFINITION 1.1 (Primzahl). Eine Zahl $p \in \mathbb{N}$ ist genau dann eine *Primzahl*, wenn $p > 1$, und für alle $a, b \in \mathbb{N}$ mit $p = a \cdot b$ gilt, dass $a = 1$ oder $b = 1$.

DEFINITION 1.2 (Teilbarkeit). Seien $x, y \in \mathbb{Z}$. Die Zahl x *teilt* y genau dann, wenn es ein $z \in \mathbb{Z}$ gibt, sodass $y = z \cdot x$ ist.

Wir schreiben dann auch $x \mid y$, und die Zahl y ist ein *Vielfaches* von x.

DEFINITION 1.3 (Ideal). Eine Teilmenge I von $\mathbb{Z}$ ist ein *Ideal* von $\mathbb{Z}$, wenn

(1) $I \neq \emptyset$.
(2) Für alle $i, j \in I$ liegt auch $i - j$ in I.
(3) Für alle $z \in \mathbb{Z}$ und alle $i \in I$ liegt auch $z \cdot i$ in I.

BEISPIELE 1.4.

(1) Die Menge $\{z \cdot 2 \mid z \in \mathbb{Z}\}$ ist ein Ideal von $\mathbb{Z}$.
(2) Die Menge $\{z \cdot 5 \mid z \in \mathbb{Z}\}$ ist ein Ideal von $\mathbb{Z}$.
(3) Die Menge $\{0\}$ ist ein Ideal von $\mathbb{Z}$.
(4) $\mathbb{N}$ ist kein Ideal von $\mathbb{Z}$.

SATZ 1.5. *Sei I ein Ideal von $\mathbb{Z}$. Dann gibt es ein $a \in I$, sodass*

$$I = \{z \cdot a \mid z \in \mathbb{Z}\}. \tag{1.1}$$

Beweis: Sei I ein Ideal von $\mathbb{Z}$. Wir wollen ein $a \in I$ finden, sodass (1.1) erfüllt ist.

- *1. Fall: I enthält kein Element ungleich* 0*:* Dann gilt $I = \{0\}$, und wir wählen $a = 0$.
- *2. Fall: I enthält ein Element ungleich* 0*:* Dann gibt es auch ein $b \in I$ mit $b > 0$. Wir definieren a durch

$$a := \min\{b \in I \mid b > 0\}.$$

Nun zeigen wir, dass a das gewünschte Element ist, d.h., wir zeigen:

$$I = \{z \cdot a \mid z \in \mathbb{Z}\}. \tag{1.2}$$

"$\supseteq$": Sei x ein Element aus der Menge auf rechten Seite von (1.2). Dann gibt es ein $z \in \mathbb{Z}$, sodass $x = z \cdot a$. Nun liegt a in I, da wir ja a als ein Element von I ausgewählt haben. Wegen der Idealeigenschaft (3) aus Definition 1.3 liegt auch $z \cdot a$ in I. Somit liegt $x = z \cdot a$ auch in der linken Seite von (1.2).

"$\subseteq$": Wir fixieren $c \in I$ und zeigen, dass c ein Vielfaches von a ist. Durch Division erhalten wir $q \in \mathbb{Z}$, $r \in \{0, 1, \ldots, a-1\}$, sodass

$$c = q \cdot a + r.$$

Daher ist $r = c - q \cdot a$. Nun liegt c in I; ebenso liegt $a \in I$. Daher liegen auch $q \cdot a$ und $c - q \cdot a$ in I. Somit folgt, dass auch $r \in I$ liegt. Wegen $r < a$ folgt aus der Minimalität von a, dass $r = 0$ ist. Daher ist c ein Vielfaches von a. ■

Wir schreiben für $\{a \cdot z \mid z \in \mathbb{Z}\}$ auch $a \cdot \mathbb{Z}$ oder (a) und bezeichnen es als *das von a erzeugte Ideal*. Für ein Ideal I heißt jedes $b \in \mathbb{Z}$ mit $I = b \cdot \mathbb{Z}$ auch *erzeugendes Element* von I.

SATZ 1.6 (Fundamentallemma). *Sei p eine Primzahl, und seien $a, b \in \mathbb{Z}$. Falls p ein Produkt $a \cdot b$ teilt, so teilt p einen der beiden Faktoren a oder b.*

Beweis: Wir definieren I durch $I := \{x \in \mathbb{Z} : p \text{ teilt } a \cdot x\}$. Wir zeigen zunächst, dass I ein Ideal ist. Die Idealeigenschaften (2) und (3) aus Definition (1.3) folgen daraus, dass für alle $x_1, x_2 \in I$ und $u, v \in \mathbb{Z}$ auch $u \cdot x_1 + v \cdot x_2$ in I liegt. Das gilt, weil p, falls es $a \cdot x_1$ und $a \cdot x_2$ teilt, auch $a \cdot (u \cdot x_1 + v \cdot x_2)$ teilt. Wegen $0 \in I$ ist I nicht die leere Menge.

Das Ideal I besitzt ein erzeugendes Element c. Da wegen $p \in I$ das Ideal I nicht gleich $\{0\}$ ist, können wir $c > 0$ wählen. Wir erhalten also $I = (c)$.

Nun liegt p aber in I. Daher gibt es ein $z \in \mathbb{Z}$, sodass $p = z \cdot c$. Da p und c in $\mathbb{N}$ liegen, ist dieses z positiv. Da p prim ist, ist $z = 1$ oder $c = 1$.

- *1. Fall: $z = 1$:* Dann gilt $p = c$. Da laut Voraussetzung p die Zahl $a \cdot b$ teilt, gilt $b \in I$. Das heißt $b \in (c)$. Also ist b Vielfaches von $c = p$; p teilt also b.
- *2. Fall: $c = 1$:* Dann liegt 1 in I. Aus der Definition von I erhalten wir

$$p \mid a \cdot 1.$$

Somit teilt p die Zahl a. ■

SATZ 1.7 (Existenz und Eindeutigkeit der Primfaktorzerlegung). *Sei $\langle p_i \mid i \in \mathbb{N}\rangle = (2, 3, 5, 7, 11, \ldots)$ die Folge aller Primzahlen, und sei $n \in \mathbb{N}$. Dann gibt es genau eine Funktion $\alpha : \mathbb{N} \to \mathbb{N}_0$ mit folgenden Eigenschaften:*

(1) $\{i \in \mathbb{N} \mid \alpha(i) > 0\}$ *ist endlich.*
(2) $n = \prod_{i \in \mathbb{N}} p_i^{\alpha(i)}$.

Beweis: Wir zeigen zunächst durch Induktion nach n, dass es ein solches α gibt. Für $n = 1$ setzen wir $\alpha(i) := 0$ für alle $i \in \mathbb{N}$. Für $n > 1$ sei q der kleinste Teiler von n mit $q > 1$. Die Zahl q ist eine Primzahl; es gibt also $j \in \mathbb{N}$ mit $q = p_j$. Nach Induktionsvoraussetzung gibt es $\beta : \mathbb{N} \to \mathbb{N}_0$ mit

$$\frac{n}{q} = \prod_{i \in \mathbb{N}} p_i^{\beta(i)},$$

also gilt $n = p_j^{\beta(j)+1} \cdot \prod_{i \in \mathbb{N}\setminus\{j\}} p_i^{\beta(i)}$.

Nun zeigen wir die Eindeutigkeit. Seien $\alpha, \beta : \mathbb{N} \to \mathbb{N}_0$ so, dass $\{i \in \mathbb{N} \mid \alpha(i) > 0\}$ und $\{i \in \mathbb{N} \mid \beta(i) > 0\}$ beide endlich sind und

$$\prod_{i \in \mathbb{N}} p_i^{\alpha(i)} = \prod_{i \in \mathbb{N}} p_i^{\beta(i)}.$$

Wir zeigen, dass für alle $j \in \mathbb{N}$ gilt: $\alpha(j) = \beta(j)$. Sei dazu $j \in \mathbb{N}$. Wir nehmen an $\alpha(j) > \beta(j)$. Dann gilt

$$p_j^{\alpha(j)-\beta(j)} \prod_{i \in \mathbb{N}\setminus\{j\}} p_i^{\alpha(i)} = \prod_{i \in \mathbb{N}\setminus\{j\}} p_i^{\beta(i)}.$$

Nach Satz 1.6 teilt p_j also ein $p_i^{\beta(i)}$ mit $i \neq j$. Im Fall $\beta(i) = 0$ widerspricht das $p_j > 1$, im Fall $\beta(i) > 0$ gilt $p_j \mid p_i$. Da p_i eine Primzahl ist, gilt dann $p_i = p_j$, im Widerspruch zu $i \neq j$. ■

ÜBUNGSAUFGABEN 1.8.

(1) [**RU87**, p. 28] Sei p_n die n-te Primzahl, d. h. $p_1 = 2$, $p_2 = 3$, usw. Zeigen Sie

$$p_n \leq 2^{(2^{n-1})}.$$

Hinweis: Euklids Beweis, dass es unendlich viele Primzahlen gibt ([**Euk91**, Buch IX, Satz 20], 270 v.Chr.) beruht auf folgender Überlegung: Seien $q_1, q_2, \ldots, q_n$ Primzahlen. Dann ist der kleinste positive Teiler von $q_1 \cdot q_2 \cdots q_n + 1$ eine Primzahl, die von allen q_i verschieden ist.

(2) Sei p_n die n-te Primzahl, d. h. $p_1 = 2$, $p_2 = 3$, usw. Zeigen Sie, auch, ohne die Eindeutigkeit der Primfaktorzerlegung zu verwenden, dass folgendes gilt: Wenn

$$\begin{aligned} a &= \Pi\, p_i^{\alpha_i} \\ b &= \Pi\, p_i^{\beta_i}, \end{aligned}$$

wobei $\alpha_i, \beta_i \in \mathbb{N}_0$, und fast alle $\alpha_i, \beta_i = 0$ sind, dann gilt $a \mid b$ genau dann, wenn für alle $i \in \mathbb{N}$ gilt, dass $\alpha_i \leq \beta_i$ ist. (Zeigen Sie, dass diese Aussage für alle Primfaktorzerlegungen von a und b gilt. Folgt daraus die Eindeutigkeit der Primfaktorzerlegung?)

(3) Welche Zahlen $q \in \mathbb{N}$ erfüllen folgende Eigenschaft?
Für alle $a, b \in \mathbb{Z}$ mit $q \mid a \cdot b$ gilt $q \mid a$ oder es gibt ein $n \in \mathbb{N}$, sodass $q \mid b^n$.

(4) Zeigen Sie, dass der Durchschnitt beliebig vieler Ideale von $\mathbb{Z}$ wieder ein Ideal von $\mathbb{Z}$ ist.

2. Der größte gemeinsame Teiler

In diesem Abschnitt werden wir eine Methode vorstellen, den größten unter allen gemeinsamen Teilern zweier Zahlen zu finden: den *Euklidischen ggT-Algorithmus*.

DEFINITION 1.9 (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 $z \mid b$.

Erstaunlicherweise lässt sich der ggT zweier Zahlen immer als Linearkombination dieser Zahlen schreiben.

SATZ 1.10. *Seien $a, b \in \mathbb{Z}$ (nicht beide 0). Dann gilt:*

(1) *Es gibt $u, v \in \mathbb{Z}$, sodass* $\mathrm{ggT}(a, b) = u \cdot a + v \cdot b$.
(2) *Der ggT ist nicht nur der größte der gemeinsamen Teiler, er ist auch Vielfaches jedes gemeinsamen Teilers.*

Die zweite Bedingung bedeutet, dass für alle $t \in \mathbb{Z}$ mit $t \mid a$ und $t \mid b$ automatisch auch $t \mid \mathrm{ggT}(a, b)$ erfüllt ist.

Beweis von Satz 1.10: Sei I definiert durch

$$I = \{ua + vb \mid u, v \in \mathbb{Z}\}.$$

I ist ein Ideal von $\mathbb{Z}$. Sei c ein positives erzeugendes Element von I. Wegen $a \in I$ gilt, dass a Vielfaches von c ist. Ebenso gilt $c \mid b$.

Wir zeigen nun, dass c nicht nur ein gemeinsamer Teiler von a und b ist, sondern dass c auch ein Vielfaches jedes weiteren gemeinsamen Teilers ist. Sei also $t \in \mathbb{N}$ eine Zahl, die a und b teilt. Es gilt: $a \in (t)$ und $b \in (t)$. Falls a und b in (t) liegen, muss aber jedes Element aus I in (t) liegen. Das gilt, weil (t) die Idealeigenschaften (2) und (3) von Definition 1.3 erfüllt. Es gilt also

$$I \subseteq (t).$$

Insbesondere liegt dann c in (t). Daher gilt $t \mid c$.

Die Zahl c wird also von jedem weiteren gemeinsamen Teiler von a und b geteilt, und ist somit der größte gemeinsame Teiler. ■

SATZ 1.11. *Seien $a, b, c \in \mathbb{Z}$, sodass* $\mathrm{ggT}(a, b) = 1$. *Falls $a \mid b \cdot c$, dann gilt auch $a \mid c$.*

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

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

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

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

also auch $a \mid c$. ■

ÜBUNGSAUFGABEN 1.12.

(1) Seien $a, b, x \in \mathbb{N}$ und $u, v \in \mathbb{Z}$ so, dass
$$x = ua + vb.$$
Zeigen Sie: Wenn x sowohl a als auch b teilt, so gilt $x = \mathrm{ggT}(a, b)$.

(2) Seien $a, b \in \mathbb{N}$, $y \in \mathbb{Z}$ so, dass $a \mid y$, $b \mid y$, $\mathrm{ggT}(a,b) = 1$. Zeigen Sie (ohne Primfaktorzerlegung): $a \cdot b \mid y$.
(3) Seien $a, b \in \mathbb{Z}$ (nicht beide 0), und sei $k \in \mathbb{N}$. Zeigen Sie: $\mathrm{ggT}(ka, kb) = k\mathrm{ggT}(a,b)$. Gelingt es Ihnen, $\mathrm{ggT}(ka, kb) \mid \mathrm{ggT}(a,b)$ auch ohne Verwendung der Primfaktorenzerlegung zu zeigen?
(4) Seien $a, c \in \mathbb{Z}$, $b, d \in \mathbb{N}$. Zeigen Sie: Wenn die Brüche $\frac{a}{b}$ und $\frac{c}{d}$ gekürzt, und die Nenner b und d teilerfremd sind, so ist auch der Bruch $\frac{ad+bc}{bd}$ gekürzt.
(5) Sei $n \in \mathbb{N}$, und seien $a_1, a_2, \ldots, a_n$ in $\mathbb{N}$. Wir definieren G_1, G_2 und G_3 durch:
   (a) $G_1(a_1) := a_1$, $G_1(a_1, a_2, \ldots, a_n) = \mathrm{ggT}(G_1(a_1, a_2, \ldots, a_{n-1}), a_n)$.
   (b) $G_2(a_1, a_2, \ldots, a_n) := \max\{z \in \mathbb{N} : z \mid a_i \text{ für alle } i \in \{1, 2, \ldots, n\}\}$.
   (c) $G_3 := \min\{z \in \mathbb{N} : \text{ es gibt } \lambda_1, \lambda_2, \ldots, \lambda_n \in \mathbb{Z}, \text{ sodass } z = \sum_{i=1}^{n} \lambda_i a_i\}$.
   Zeigen Sie, dass G_1, G_2 und G_3 gleich sind.
(6) Sei p_n die n-te Primzahl, d. h. $p_1 = 2$, $p_2 = 3$, usw. Zeigen Sie, auch, ohne die Eindeutigkeit der Primfaktorzerlegung zu verwenden, dass folgendes gilt: Wenn

$$\begin{aligned} a &= \prod p_i^{\alpha_i} \\ b &= \prod p_i^{\beta_i}, \end{aligned}$$

wobei $\alpha_i, \beta_i \in \mathbb{N}_0$, und fast alle $\alpha_i, \beta_i = 0$ sind, dann gilt

$$\mathrm{ggT}(a,b) = \prod p_i^{\min(\alpha_i, \beta_i)}.$$

Es ist einfach, aus den Primfaktorzerlegungen von a und b den ggT von a und b zu bestimmen. Es kann aber sehr rechenaufwendig sein, die Primfaktorzerlegung einer Zahl zu bestimmen. Schneller kann man den ggT mit dem *Euklidischen Algorithmus* berechnen, der ohne die Primfaktorzerlegungen auskommt.

SATZ 1.13. *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

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

"$\subseteq$": 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.■

Das nützen wir jetzt möglichst geschickt aus, um $\mathrm{ggT}(147, 33)$ zu berechnen:

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

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 1.14. Berechnen wir nochmals ggT(147, 33), und schreiben dies 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			

ÜBUNGSAUFGABEN 1.15.

(1) Bestimmen Sie für a und b jeweils ggT(a, b), und zwei ganze Zahlen $u, v \in \mathbb{Z}$, sodass

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

(a) $a = 254$, $b = 120$.
(b) $a = 71$, $b = 79$.
(c) $a = 610$, $b = 987$.

3. Das kleinste gemeinsame Vielfache

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

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

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

SATZ 1.17. *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:* kgV $(a, b) \mid s$. *Jedes gemeinsame Vielfache ist also ein Vielfaches des* kgV.

Beweis: Wir betrachten $(a) = \{a \cdot z \,|\, z \in \mathbb{Z}\}$ und $(b) = \{b \cdot z \,|\, z \in \mathbb{Z}\}$. Der Durchschnitt zweier Ideale ist wieder ein Ideal, und da (a) und (b) Ideale sind, ist $(a) \cap (b)$ auch ein Ideal. Es gibt also $c \in \mathbb{Z}$, sodass

$$(c) = (a) \cap (b).$$

Wegen $c \in (a)$ ist c ein Vielfaches von a, und ebenso ein Vielfaches von b. Sei nun s ein weiteres gemeinsames Vielfaches von a und b. Da s in $(a) \cap (b)$ liegt, liegt s auch in (c), und ist somit Vielfaches von c. Also ist c das *kleinste* gemeinsame Vielfache und

teilt jedes gemeinsame Vielfache von a und b. ■

Zwischen ggT und kgV kann man folgenden Zusammenhang herstellen:

SATZ 1.18. *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 dem Fundamentallemma (Satz 1.6) (bzw. Übung 1.12 (6)) 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:

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

■

ÜBUNGSAUFGABEN 1.19.

(1) Zeigen Sie ohne Verwendung der Primfaktorzerlegung, dass für alle $a, b \in \mathbb{N}$ gilt:

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

Hinweis: Zeigen Sie dazu $ab \mid \mathrm{ggT}(a,b) \cdot \mathrm{kgV}(a,b)$ und $\mathrm{kgV}(a,b) \mid \frac{ab}{\mathrm{ggT}(a,b)}$.

(2) Seien $a, b, c \in \mathbb{N}$. Zeigen Sie:
   (a) $\mathrm{ggT}(\mathrm{ggT}(a,b),c) = \mathrm{ggT}(a,\mathrm{ggT}(b,c))$.
   (b) $\mathrm{kgV}(\mathrm{kgV}(a,b),c) = \mathrm{kgV}(a,\mathrm{kgV}(b,c))$.
   (c) $\mathrm{ggT}(\mathrm{kgV}(a,b),c) = \mathrm{kgV}(\mathrm{ggT}(a,c),\mathrm{ggT}(b,c))$.
   (d) $\mathrm{kgV}(\mathrm{ggT}(a,b),c) = \mathrm{ggT}(\mathrm{kgV}(a,c),\mathrm{kgV}(b,c))$.

(3) Sei $n \in \mathbb{N}$, und seien $a_1, a_2, \ldots, a_n$ in $\mathbb{N}$. Wir definieren K_1 und K_2 durch:
   (a) $K_1(a_1) := a_1$, $K_1(a_1, a_2, \ldots, a_n) = \mathrm{kgV}(K_1(a_1, a_2, \ldots, a_{n-1}), a_n)$.
   (b) $K_2(a_1, a_2, \ldots, a_n) := \min\{z \in \mathbb{N} : a_i \mid z \text{ für alle } i \in \{1, 2, \ldots, n\}\}$.

   Zeigen Sie, dass K_1 und K_2 gleich sind.

(4) Sei $n \in \mathbb{N}$, und seien $a_1, a_2, \ldots, a_n$ in $\mathbb{N}$. Wir definieren K_2 durch

$$K_2(a_1, a_2, \ldots, a_n) := \min\{z \in \mathbb{N} : a_i \mid z \text{ für alle } i \in \{1, 2, \ldots, n\}\}.$$

   Zeigen Sie, dass alle ganzen Zahlen, die Vielfaches eines jeden a_i sind, auch ein Vielfaches von $K_2(a_1, a_2, \ldots, a_n)$ sind.

(5) Sei p_n die n-te Primzahl, d. h. $p_1 = 2$, $p_2 = 3$, usw. Zeigen Sie, auch ohne die Eindeutigkeit der Primfaktorzerlegung zu verwenden, dass folgendes gilt: Wenn

$$\begin{aligned} a &= \prod p_i^{\alpha_i} \\ b &= \prod p_i^{\beta_i}, \end{aligned}$$

   wobei $\alpha_i, \beta_i \in \mathbb{N}_0$, und fast alle $\alpha_i, \beta_i = 0$ sind, dann gilt

$$\mathrm{kgV}(a,b) = \prod p_i^{\max(\alpha_i,\beta_i)}.$$

4. Lösen von Kongruenzen

DEFINITION 1.20. 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 1.21. *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 $c \mid a \cdot y - b$.*
(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

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

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

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

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

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 $ax \equiv b \pmod{c}$. ■

SATZ 1.22. *Seien $a, c \in \mathbb{Z}$ (nicht beide = 0), und sei $b \in \mathbb{Z}$. Sei x_0 eine Lösung von*

$$ax \equiv b \pmod{c}. \tag{1.3}$$

Dann ist die Lösungsmenge von (1.3) *gegeben durch:*

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

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

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

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

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

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

oder, äquivalent dazu,

$$c \mid a\left(x_1 - x_0\right).$$

Daher gilt auch

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

Da

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

gilt

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

■

KOROLLAR 1.23. *Seien $a, c \in \mathbb{Z}$ (nicht beide $= 0$), sei $b \in \mathbb{Z}$, sodass $\mathrm{ggT}(a,c) \mid b$, und sei x_0 eine Lösung von $ax \equiv b \pmod{c}$ ist. Dann ist die Kongruenz $ax \equiv b \pmod{c}$ äquivalent zu $x \equiv x_0 \left(\mathrm{mod}\ \frac{c}{\mathrm{ggT}(a,c)}\right)$.*

ÜBUNGSAUFGABEN 1.24.

(1) Lösen Sie die Gleichung

$$207x \equiv 18 \pmod{1989}$$

in $\mathbb{Z}$!

(2) Bestimmen Sie für alle $a, c \in \mathbb{N}$, $b \in \mathbb{Z}$, wieviele Lösungen in $\{0, 1, \ldots, c-1\}$ die Gleichung $a \cdot x \equiv b \pmod{c}$ hat.

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

$$\begin{aligned} x &\equiv a_1 \left(\mathrm{mod}\ m_1\right) \\ x &\equiv a_2 \left(\mathrm{mod}\ m_2\right), \end{aligned}$$

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

BEISPIELE 1.25. 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

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

hingegen hat zum Beispiel die Lösung $x = 7$.

SATZ 1.26. *Seien* $a_1, a_2 \in \mathbb{Z}$, $m_1, m_2 \in \mathbb{N}$. *Das System*

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

ist genau dann lösbar, wenn $\text{ggT}(m_1, m_2) \mid (a_1 - a_2)$.

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 $\text{ggT}(m_1, m_2) \mid (x - a_1)$ und $\text{ggT}(m_1, m_2) \mid (x - a_2)$, und somit

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

"⇐" 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 $\text{ggT}(15, 21) = 3$ 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 1.27. *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

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

Beweis: "$\supseteq$": Wir setzen

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

in die erste Kongruenz ein und erhalten

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

Das gleiche gilt für die zweite Kongruenz.

"$\subseteq$": Wir fixieren $x_1 \in L$. Um zu zeigen, dass $x_1 \in \left\{ x_0 + k \cdot \mathrm{kgV}\left(m_1, m_2\right) \mid k \in \mathbb{Z} \right\}$, zeigen wir, dass $x_1 - x_0$ ein Vielfaches von $\mathrm{kgV}\left(m_1, m_2\right)$ 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 $\left(x_1 - x_0\right) \equiv 0 \pmod{m_1}$ und somit $m_1 \mid \left(x_1 - x_0\right)$. Ebenso zeigt man, dass $m_2 \mid \left(x_1 - x_0\right)$ gilt.

Da das kgV jedes gemeinsame Vielfache teilt, gilt $\mathrm{kgV}\left(m_1, m_2\right) \mid \left(x_1 - x_0\right)$. ■

ÜBUNGSAUFGABEN 1.28.

(1) Lösen Sie folgendes System von Kongruenzen!

$$\begin{aligned} x &\equiv 22 \pmod{26} \\ x &\equiv 26 \pmod{37} \end{aligned}$$

(2) Seien $m_1, m_2 \in \mathbb{N}$. Wieviele Lösungen in $\{0, 1, \ldots, m_1 \cdot m_2 - 1\}$ hat das System

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

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 1.29. *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*

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \\ &\vdots \\ x &\equiv a_r \pmod{m_r} \end{aligned} \tag{1.4}$$

eine Lösung x_0 *hat, dann ist* (1.4) *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. ■

Wir schreiben:

$$\begin{aligned} kgV(m_1, m_2) &=: m_1 \vee m_2 \\ ggT(m_1, m_2) &=: m_1 \wedge m_2. \end{aligned}$$

Es gilt dann:

PROPOSITION 1.30. *Seien* $a, b, c \in \mathbb{N}$. *Dann gilt:*

(1) $a \wedge (a \vee b) = a$,
(2) $a \vee (a \wedge b) = a$,
(3) $(a \wedge b) \wedge c = a \wedge (b \wedge c)$,
(4) $(a \vee b) \vee c = a \vee (b \vee c)$,
(5) $a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$,
(6) $a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$.

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

SATZ 1.31 (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*

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

Beweis: "(1) $\Rightarrow$ (2)" ist offensichtlich. "(2) $\Leftrightarrow$ (3)" gilt wegen Satz 1.26.

"(3) $\Rightarrow$ (1)": Wir zeigen durch Induktion nach r, dass jedes System aus r Kongruenzen, für das die Bedingung (3) erfüllt ist, lösbar ist. Ein System aus zwei Kongruenzen ist wegen Satz 1.26 lösbar. Um ein System von r (mit $r \geq 3$) Kongruenzen zu lösen, bestimmen wir zuerst nach Induktionsvoraussetzung ein y sodass

$$y \equiv a_2 \pmod{m_2}, \ldots, y \equiv a_r \pmod{m_r}.$$

Wegen Satz 1.29 ist $x \equiv a_1 \pmod{m_1}, \ldots, x \equiv a_r \pmod{m_r}$ äquivalent zu

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv y \pmod{m_2 \vee \ldots \vee m_r}. \end{aligned} \tag{1.5}$$

Jetzt müssen wir zeigen, dass (1.5) lösbar ist. Das gilt nach Satz 1.26 genau dann, wenn

$$m_1 \wedge (m_2 \vee \ldots \vee m_r) \mid y - a_1. \tag{1.6}$$

Es gilt $a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$. Daher ist (1.6) äquivalent zu

$$(m_1 \wedge m_2) \vee (m_1 \wedge m_3) \vee \ldots \vee (m_1 \wedge m_r) \mid y - a_1.$$

Wir zeigen dazu, dass für $i > 1$ gilt:

$$(m_1 \wedge m_i) \mid (y - a_1). \tag{1.7}$$

Wir wissen aber

$$y - a_1 \equiv_{m_i} a_i - a_1 \equiv_{(m_i \wedge m_1)} 0.$$

Das beweist, dass für alle $i > 1$ gilt $(m_i \wedge m_1) \mid (y - a_1)$. Nun ist jedes gemeinsame Vielfache eine Vielfaches des kleinsten gemeinsamen Vielfachen, und somit gilt (1.6). ■

BEISPIEL 1.32. Wir lösen folgendes System

$$\begin{aligned} x &\equiv 2 \pmod{15} \\ x &\equiv 8 \pmod{21} \\ x &\equiv 7 \pmod{55} \end{aligned} \tag{1.8}$$

Wir kennen bereits die Lösungen von $x \equiv 2 \pmod{15}$, $x \equiv 8 \pmod{21}$. Das System (1.8) ist daher äquivalent zu

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

Wir berechnen 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:

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

ÜBUNGSAUFGABEN 1.33.

(1) Finden Sie alle Lösungen in $\mathbb{Z}$ von

$$\begin{aligned} x &\equiv 26 \pmod{56} \\ x &\equiv 82 \pmod{84} \\ x &\equiv 124 \pmod{126}. \end{aligned}$$

(2) Finden Sie alle Lösungen in $\mathbb{Z}$ von

$$\begin{aligned} x &\equiv 3 \pmod{4} \\ x &\equiv 8 \pmod{9} \\ x &\equiv 1 \pmod{25}. \end{aligned}$$

(3) Seien $a, b, c \in \mathbb{Z}$. Bestimmen Sie für alle $a, b, c \in \mathbb{Z}$, ob die Gleichung

$$a \cdot x + b \cdot y = c$$

in $\mathbb{Z} \times \mathbb{Z}$ lösbar ist, und bestimmen Sie alle Lösungen.

(4) Bestimmen Sie eine Lösung in $\mathbb{Z}^3$ von

$$12x + 15y + 20z = 1.$$

(5) Bestimmen Sie alle Lösungen in $\mathbb{Z}^3$ von

$$12x + 15y + 20z = 1.$$

(6) Sei T eine endliche Teilmenge von $\mathbb{Z}$. Eine Funktion $f : T \to \mathbb{Z}$ heißt *kompatibel* genau dann, wenn für alle $x_1, x_2 \in T$ mit $x_1 \neq x_2$ der Quotient $\frac{f(x_1)-f(x_2)}{x_1-x_2}$ ganzzahlig ist.

Sei f eine beliebige kompatible Funktion auf einer endlichen Teilmenge T von $\mathbb{Z}$, und sei $z \in \mathbb{Z} \setminus T$. Zeigen Sie: Es gibt eine kompatible Funktion $g : T \cup \{z\} \to \mathbb{Z}$, sodass $g(t) = f(t)$ für alle $t \in T$.

Hinweis: Die Funktion g heißt *kompatible Erweiterung* von f auf $T \cup \{z\}$. Sie müssen nur ein passendes $g(z)$ finden. Stellen Sie dazu ein System von Kongruenzen auf, von dem $g(z)$ Lösung sein muss, und zeigen Sie, dass dieses System lösbar ist.

(7) Eine Funktion $f : \mathbb{Z} \to \mathbb{Z}$ heißt *kompatibel* genau dann, wenn für alle $x_1, x_2 \in \mathbb{Z}$ mit $x_1 \neq x_2$ der Quotient $\frac{f(x_1)-f(x_2)}{x_1-x_2}$ ganzzahlig ist. Zeigen Sie, dass folgende Funktionen kompatibel sind:
   (a) $f(x) = x^n$ für $n \in \mathbb{N}$,
   (b) $f(x) = \frac{x\cdot(x-1)}{2}$.

(8) Eine Funktion $f : \mathbb{Z} \to \mathbb{Z}$ heißt *kompatibel* genau dann, wenn für alle $x_1, x_2 \in \mathbb{Z}$ mit $x_1 \neq x_2$ der Quotient $\frac{f(x_1)-f(x_2)}{x_1-x_2}$ ganzzahlig ist. Zeigen Sie, dass die Menge der kompatiblen Funktionen von $\mathbb{Z}$ überabzählbar ist.

KAPITEL 2

Teilbarkeit in Integritätsbereichen

1. Kommutative Ringe mit Eins

DEFINITION 2.1. Eine Algebra $\langle R, +, -, \cdot, 0, 1\rangle$ ist ein *kommutativer Ring mit Eins*, wenn $+, \cdot$ binäre Operationen auf R sind, $-$ eine unäre Operation auf R ist, und $0, 1$ Elemente aus R sind, sodass 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) $x \cdot y = y \cdot x$
(7) $x \cdot 1 = x$
(8) $x \cdot (y + z) = x \cdot y + x \cdot z$.

SATZ 2.2. *Sei $\langle R, +, -, \cdot, 0, 1\rangle$ ein kommutativer Ring mit 1, und seien $x, y \in R$. Dann gilt*

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

Beweis: (1): $-(-x) = -(-x) + 0 = 0 + (-(-x)) = (x + (-x)) + (-(-x)) = x + ((-x) + (-(-x)) = x + 0 = x$. (2): $x \cdot 0 = x \cdot 0 + 0 = x \cdot 0 + (x \cdot 0 + (-x \cdot 0)) = (x \cdot 0 + x \cdot 0) + (-x \cdot 0) = x \cdot (0 + 0) + (-x \cdot 0) = x \cdot 0 + (-x \cdot 0) = 0$. (3): Wir verwenden jetzt außer den bei der Definition von kommutativen Ringen verwendeten Gleichungen auch die Folgerungen, dass für alle $z \in R$ auch $(-z) + z = 0$ und $0 + z = z$ gilt. $-(x \cdot y) = -(x \cdot y) + x \cdot 0 = -(x \cdot y) + x \cdot (y + (-y)) = -(x \cdot y) + (x \cdot y + x \cdot (-y)) = (-(x \cdot y) + x \cdot y) + x \cdot (-y) = 0 + x \cdot (-y) = x \cdot (-y)$. Mithilfe des Kommutativgesetzes folgt nun auch $(-x) \cdot y = -(x \cdot y)$. ■

2. Ideale

DEFINITION 2.3. Sei R ein kommutativer Ring mit Eins. Eine nichtleere Teilmenge I von R ist ein *Ideal* von R, wenn für alle $r \in R$ und $i, j \in I$ auch $r \cdot i \in I$ und $i + j \in I$ gilt.

Aus dieser Definition sieht man, dass der Durchschnitt von Idealen von R wieder ein Ideal von R ist.

DEFINITION 2.4. Sei R ein kommutativer Ring mit Eins, und sei A eine Teilmenge von R. Dann ist das *von A erzeugte Ideal* $\langle A\rangle_R$ definiert durch

$$\langle A\rangle_R := \bigcap \{I \mid I \text{ Ideal von } R \text{ und } A \subseteq I\}.$$

SATZ 2.5. *Sei R ein kommutativer Ring mit Eins, und sei $A \subseteq R$. Dann gilt*

$$\langle A\rangle_R = \{\sum_{i=1}^{n} r_i a_i \mid n \in \mathbb{N}_0, a_1, \ldots, a_n \in A, r_1, \ldots, r_n \in R\}.$$

Beweis: Sei $J := \{\sum_{i=1}^{n} r_i a_i \mid n \in \mathbb{N}_0, a_1, \ldots, a_n \in A, r_1, \ldots, r_n \in R\}$. Da $0 \in J$, und da J abgeschlossen unter $+$ und unter Multipkation mit Elementen von R ist, ist J ein Ideal von R. Außerdem gilt offensichtlich $A \subseteq J$. J ist also ein Ideal von R mit $A \subseteq J$. Aus der Definition von $\langle A\rangle_R$ als Durchschnitt aller solchen Ideale sieht man also $\langle A\rangle_R \subseteq J$.

Um die Inklusion $J \subseteq \langle A\rangle_R$ zu zeigen, wählen wir ein Element $j \in J$. Es gibt also $n \in \mathbb{N}_0$, $a_1, \ldots, a_n \in A$ und $r_1, \ldots, r_n \in R$, sodass $j = \sum_{i=1}^{n} r_i a_i$. Aus der Definition von $\langle A\rangle_R$ sehen wir, dass $A \subseteq \langle A\rangle_R$ gilt. Damit liegt jedes a_i in $\langle A\rangle_R$. Da $\langle A\rangle_R$ ein Ideal von R ist, liegt also auch jeder Summand $r_i a_i$ in $\langle A\rangle_R$, und schließlich auch die Summe j. ■

DEFINITION 2.6. Sei R ein kommutativer Ring mit Eins, und sei I ein Ideal von R. Das Ideal I ist ein *Hauptideal* von R, wenn es ein $a \in R$ gibt, sodass $I = \langle\{a\}\rangle_R$. Wir schreiben für $\langle\{a\}\rangle_R = Ra$ auch kürzer (a).

ÜBUNGSAUFGABEN 2.7.

(1) (Erzeugen von Idealen) Bestimmen Sie jeweils, ob das von der Menge S erzeugte Ideal $\langle S\rangle$ des Rings R gleich dem ganzen Ring R ist!
   (a) $R = \mathbb{Z}$, $S = \{105, 70, 42, 30\}$.
   (b) $R = \mathbb{Z} \times \mathbb{Z}$, $S = \{(4, 3), (6, 5)\}$.
   (c) $R = \mathbb{Z}_{101}$, $S = \{[75]_{101}\}$.

(2) (Erzeugen von Idealen) Bestimmen Sie jeweils, ob das von der Menge S erzeugte Ideal $\langle S\rangle$ des Rings $\mathbb{R}[x, y]$ gleich dem ganzen Ring $\mathbb{R}[x, y]$ ist!
   (a) $S = \{xy, x^3y + 1\}$.
   (b) $S = \{x^2y, xy^2 + 1\}$.
   (c) $S = \{xy + x, 1 + y^2\}$.

(3) (Zornsches Lemma) Sei R ein kommutativer Ring mit Eins. Ein Ideal von R ist *maximal*, wenn es ein maximales Element in

$$\{I \mid I \text{ ist Ideal von } R \text{ und } I \neq R\}$$

ist. Zeigen Sie, dass jedes von R verschiedene Ideal in einem maximalen Ideal von R enthalten ist! Wo verwenden Sie, dass R ein Einselement hat?

3. Integritätsbereiche

Ein kommutativer Ring mit Eins R ist ein *Integritätsbereich*, wenn er zumindest zwei Elemente hat und für alle a, b mit $a \neq 0$ und $b \neq 0$ auch $ab \neq 0$ gilt.

DEFINITION 2.8. Sei R ein kommutativer Ring mit Eins, und seien $a, b \in R$. Dann gilt $a \mid b$, wenn es ein $r \in R$ gibt, sodass $b = ra$.

DEFINITION 2.9. Sei R ein kommutativer Ring mit Eins.

- Ein Element $u \in R$ ist *invertierbar*, wenn es ein $v \in R$ mit $uv = 1$ gibt.
- Ein Element $p \in R$ ist *prim*, wenn es nicht invertierbar ist, und für alle $a, b \in R$ mit $p \mid ab$ gilt: $p \mid a$ oder $p \mid b$.
- Ein Element $r \in R$ ist *irreduzibel*, wenn es nicht invertierbar ist, und für alle $s, t \in R$ mit $r = st$ gilt: s ist invertierbar oder t ist invertierbar.
- Zwei Elemente $a, b \in R$ sind *assoziiert*, wenn es ein invertierbares Element $u \in R$ gibt, sodass $au = b$. Wir schreiben dann $a \sim b$ oder $a \sim_R b$.

LEMMA 2.10. *Sei R ein Integritätsbereich, und sei p ein primes Element von R mit $p \neq 0$. Dann ist p irreduzibel.*

Beweis: Sei p prim, $p \neq 0$, und seien $s, t \in R$ so, dass $p = st$. Dann gilt $p \mid st$. Da p prim ist, gilt $p \mid s$ oder $p \mid t$. Im Fall $p \mid s$ gibt es ein $s_1 \in R$, sodass $ps_1 = s$. Durch Multiplikation dieser Gleichung mit t erhalten wir $ps_1t = st = p$. Also gilt $p(s_1t - 1) = 0$. Wegen $p \neq 0$ ist also t invertierbar. Im Fall $p \mid t$ erhalten wir analog, dass s invertierbar ist. ■

ÜBUNGSAUFGABEN 2.11.

(1) (Invertierbare Elemente) Sei R ein kommutativer Ring mit Eins. Zeigen Sie:
   (a) Das Produkt invertierbarer Elemente ist wieder invertierbar.
   (b) Jeder Teiler eines invertierbaren Elements ist invertierbar.
   (c) Ein Element $r \in R$ ist genau dann invertierbar, wenn das von r erzeugte Ideal (r) gleich R ist.
(2) (Integritätsbereiche) Zeigen Sie, dass jeder endliche Integritätsbereich ein Körper ist. (*Hinweis:* Betrachten Sie für $r \neq 0$ die Abbildung $x \mapsto r \cdot x$.)
(3) (Prime Elemente) Sei R ein Integritätsbereich. Ein Ideal I von R ist *prim*, wenn $I \neq R$ und für alle $a, b \in R$ gilt: $a \cdot b \in I \Rightarrow (a \in I$ oder $b \in I)$. Zeigen Sie:
   (a) Ein Element r ist genau dann prim, wenn das Hauptideal (r) prim ist.
   (b) Wenn r prim und u invertierbar ist, so ist auch $r \cdot u$ prim.
(4) (Einfache Ringe) Ein Ring R ist *einfach*, wenn er keine Ideale außer $\{0\}$ und R hat. Zeigen Sie, dass die beiden folgenden Behauptungen äquivalent sind:
   (a) R ist ein einfacher kommutativer Ring mit Eins, und $|R| \geq 2$.
   (b) R ist ein Körper.
(5) (Irreduzible Elemente) Sei R ein Integritätsbereich, und sei $r \in R$ mit $r \neq 0$.
   (a) Zeigen Sie, dass folgende Bedingungen äquivalent sind.
      (i) r ist irreduzibel.
      (ii) Das Ideal (r) ist ein maximales Element in der Menge aller Hauptideale von R, die ungleich R sind.
   (b) Zeigen Sie: Wenn r irreduzibel ist, ist auch jedes zu r assoziierte Element irreduzibel.

4. Euklidische Integritätsbereiche

DEFINITION 2.12. Sei R ein Integritätsbereich. Der Integritätsbereich R ist ein *Euklidischer Bereich*, wenn es eine Funktion $\delta : R \setminus \{0\} \to \mathbb{N}_0$ gibt, sodass folgendes gilt.

(1) Für alle $a, b \in R \setminus \{0\}$ gilt $\delta(a) \leq \delta(a\,b)$.

(2) Für alle $a, b \in R$ mit $b \neq 0$ gibt es $q, r \in R$, sodass
   (a) $a = b\,q + r$, und
   (b) $r = 0$ oder $\delta(r) < \delta(b)$.

SATZ 2.13. *Der Ring $\mathbb{Z}$ ist ein Euklidischer Bereich.*

Beweis: Die Funktion $\delta(z) := |z|$ für $z \in \mathbb{Z} \setminus \{0\}$ leistet das Gewünschte. ■

SATZ 2.14. *Sei K ein Körper, und sei $K[t]$ der Polynomring über K. Dann ist $K[t]$ ein Euklidischer Bereich.*

Beweis: Wir setzen $\delta(f) := \deg(f)$. ■

DEFINITION 2.15. Sei $\mathbb{Z}[i]$ die Teilmenge der komplexen Zahlen, die durch

$$\mathbb{Z}[i] := \{a + b\,i \mid a, b \in \mathbb{Z}\}$$

definiert ist. Als Operationen verwenden wir die Addition und Multiplikation der komplexen Zahlen. Dann nennen wir $\mathbb{Z}[i]$ den *Ring der Gaußschen ganzen Zahlen*.

SATZ 2.16. *$\mathbb{Z}[i]$ ist ein Euklidischer Bereich.*

Beweis: Als Unterring des Körpers $\mathbb{C}$ ist $\mathbb{Z}[i]$ ein Integritätsbereich. Wir definieren nun $\delta(x + y\,i) := x^2 + y^2$ für alle $x, y \in \mathbb{Z}$. Dann gilt $\delta(z_1 \cdot z_2) = \delta(z_1) \cdot \delta(z_2)$ für alle $z_1, z_2 \in \mathbb{Z}[i]$, und somit ist Eigenschaft (1) von Definition 2.12 erfüllt.

Seien nun $b, a \in \mathbb{Z}[i]$ mit $a \neq 0$, und seien $u', v' \in \mathbb{Q}$ so, dass $b = a \cdot (u' + v'\,i)$. Wir wählen nun $u, v \in \mathbb{Z}$, sodass $|u - u'| \leq \frac{1}{2}$ und $|v - v'| \leq \frac{1}{2}$. Sei nun

$$q := u + v\,i \text{ und } r := b - q\,a.$$

Dann gilt

$$\begin{aligned}\delta(r) &= \delta((u' + v'\,i) \cdot a - (u + v\,i) \cdot a) = \delta(a \cdot ((u' - u) + (v' - v)\,i)) \\ &= \delta(a) \cdot \delta((u' - u) + (v' - v)\,i) = \delta(a) \cdot ((u' - u)^2 + (v' - v)^2) \leq \delta(a) \cdot \frac{1}{2}.\end{aligned}$$

Da $a \neq 0$, gilt $\delta(a) = a\overline{a} \neq 0$, und somit gilt $\delta(r) < \delta(a)$. ■

DEFINITION 2.17. Ein Integritätsbereich R ist ein *Hauptidealbereich*, wenn es für jedes Ideal I von R ein $a \in R$ gibt, sodass $I = (a)$.

SATZ 2.18. *Jeder Euklidische Bereich ist ein Hauptidealbereich.*

Beweis: Sei R ein Euklidischer Bereich, und sei I ein Ideal von R. Wenn $I = \{0\}$, so gilt $I = (0)$. Wenn $I \neq 0$, so wählen wir ein $a \in I \setminus \{0\}$, für das $\delta(a)$ minimal ist. Sei nun $b \in I$, und seien $q, r \in R$ so, dass $b = q\,a + r$ und ($r = 0$ oder $\delta(r) < \delta(a)$). Da $r = b - q\,a \in I$, kann $\delta(r) < \delta(a)$ wegen der Minimalität von $\delta(a)$ nicht gelten. Also gilt $r = 0$ und $b = q\,a \in (a)$. Somit gilt $I = (a)$. ■

BEISPIEL 2.19. Der Polynomring $\mathbb{Q}[x, y]$ ist kein Hauptidealbereich.

Beweis: Sei $I := \{p \in \mathbb{Q}[x,y] \mid \overline{p}(0,0) = 0\}$. Dann gilt $x \in I$ und $y \in I$. Wenn I ein Hauptideal ist, so gibt es $f \in I$ mit $f \mid x$ und $f \mid y$. Also gilt $\deg_y(f) = 0$ und $\deg_x(f) = 0$, und somit ist f ein konstantes Polynom. Da $f \in I$, gilt $\overline{f}(0,0) = 0$, und somit $f = 0$. Das ist ein Widerspruch zu $f \mid x$. Somit ist I kein Hauptideal. ■

5. Faktorielle Integritätsbereiche

DEFINITION 2.20. Sei R ein Integritätsbereich. R ist *faktoriell*, wenn folgendes gilt:

(1) Für alle $r \in R\backslash\{0\}$, die nicht invertierbar sind, gibt es ein $s \in \mathbb{N}$ und irreduzible $f_1, \ldots, f_s \in R$, sodass
$$r = f_1 \cdots f_s.$$
(2) Für alle $m, n \in \mathbb{N}$ und für alle irreduziblen $f_1, \ldots, f_m, g_1, \ldots, g_n \in R$ mit
$$f_1 \cdots f_m = g_1 \cdots g_n$$
gilt $m = n$, und es gibt eine bijektive Abbildung $\pi : \{1, \ldots, m\} \to \{1, \ldots, n\}$, sodass für alle $i \in \{1, \ldots, m\}$ gilt: $f_i \sim_R g_{\pi(i)}$.

LEMMA 2.21. *Sei R ein Hauptidealbereich, und sei $p \in R$ ein irreduzibles Element von R. Dann ist p prim.*

Beweis: Seien $a, b \in R$ so, dass $p \mid a \cdot b$. Sei $J := \{s\,p + t\,a \mid s, t \in R\}$ das von $\{p, a\}$ erzeugte Ideal von R. Da J ein Hauptideal ist, gibt es $c \in J$ mit $(c) = J$. Dann gilt $c \mid p$ und $c \mid a$. Sei $d \in R$ so, dass $c\,d = p$. Da p irreduzibel ist, ist c invertierbar oder d invertierbar. Wenn c invertierbar ist, so gilt $1 \in J$. Also gibt es $s', t' \in R$ mit $s'p + t'a = 1$. Dann gilt $s'pb + t'ab = b$, und somit $p \mid b$. Wenn d invertierbar ist, so gilt wegen $c \mid a$ auch $p = c\,d \mid a\,d$. Da d invertierbar ist, gilt $a\,d \mid a$, und somit $p \mid a$. ■

SATZ 2.22. *Jeder Hauptidealbereich ist faktoriell.*

Beweis: Sei G die Menge aller $r \in R \setminus \{0\}$, die nicht invertierbar sind und sich nicht als Produkt endlich vieler irreduzibler Elemente schreiben lassen. Wir nehmen an $G \neq \emptyset$. Sei
$$\mathcal{A} := \{(r) \mid r \in G\}$$
Wir betrachten zunächst den Fall, dass die geordnete Menge $(\mathcal{A}, \subseteq)$ ein maximales Element hat. Sei A ein solches maximales Element, und sei $a \in G$ so, dass $(a) = A$. Da a nicht irreduzibel und nicht invertierbar ist, gibt es nicht invertierbare Elemente $b, c \in R$ mit $b\,c = a$. Nun gilt $(a) \subseteq (c)$. Wenn $(a) = (c)$, so gibt es $d \in R$ mit $d\,a = c$. Dann gilt $a = b\,c = b\,d\,a$, also $a(1 - bd) = 0$. Da R ein Intergritätsbereich ist, gilt $a = 0$ oder $bd = 1$. Wenn $a = 0$, so gilt $A \notin \mathcal{A}$, ein Widerspruch. Wenn $bd = 1$, so ist b invertierbar, ebenfalls ein Widerspruch. Also gilt $(a) \neq (c)$. Wegen der Maximalität von (a) gilt $(c) \notin \mathcal{A}$. Also gilt $c \notin G$. Da c nicht invertierbar ist, lässt sich c als Produkt endlich vieler irreduzibler Elemente schreiben. Da $(a) \subsetneq (b)$, erhält man genauso, dass sich b als Produkt endlich vieler irreduzibler Elemente schreiben lässt. Somit ist auch

a ein Produkt endlich vieler irreduzibler Elemente, im Widerspruch zu $a \in G$. Der Fall, dass $(\mathcal{A}, \subseteq)$ ein maximales Element hat, kann also nicht eintreten.

Wir betrachten nun den Fall, dass $(\mathcal{A}, \subseteq)$ kein maximales Element hat. Dann gibt es eine Folge $(a_i)_{i\in\mathbb{N}}$ aus G, sodass $(a_1) \subsetneq (a_2) \subsetneq (a_3)\cdots$. Wir bilden nun die Menge $A := \cup_{i\in\mathbb{N}}(a_i)$. Die Menge A ist ein Ideal des Rings R. Da R ein Hauptidealbereich ist, gibt es ein $b \in A$ mit $(b) = A$. Wegen $b \in A$ gibt es ein $j \in \mathbb{N}$, sodass $b \in (a_j)$. Dann gilt auch $(b) \subseteq (a_j)$, und somit $(a_{j+1}) \subseteq (b) \subseteq (a_j)$, im Widerspruch zu $(a_j) \subsetneq (a_{j+1})$. Daher kann auch der Fall, dass $(\mathcal{A}, \subseteq)$ kein maximales Element hat, nicht eintreten.

Insgesamt gilt also $G = \emptyset$; somit lässt sich jedes nicht invertierbare Element von $R\setminus\{0\}$ als Produkt endlich vieler irreduzibler Elemente schreiben.

Wir zeigen nun die Eindeutigkeit der Zerlegung, indem wir die Eigenschaft (2) aus Definition 2.20 durch Induktion nach m zeigen. Wenn $m = 1$, so gilt $f_1 \mid g_1\cdots g_n$. Wegen Lemma 2.21 gibt es dann ein $j \in \{1, \ldots, n\}$, sodass $f_1 \mid g_j$. Da g_j irreduzibel ist, gibt es ein invertierbares Element $u \in R$ mit $g_j = u\, f_1$. Somit gilt $f_1 = u f_1 \prod_{\substack{i=1\\ i\neq j}}^{n} g_i$, also $1 = u \cdot \prod_{\substack{i=1\\ i\neq j}}^{n} g_i$. Damit ist jedes g_i mit $i \neq j$ invertierbar, und folglich gilt $n = 1$ und $j = 1$.

Sei nun $m > 1$. Wegen $f_1 \mid g_1\cdots g_n$ und Lemma 2.21 gibt es daher ein $j \in \{1, \ldots, n\}$, sodass $f_1 \mid g_j$. Da g_j irreduzibel ist, gibt es ein invertierbares $u \in R$ mit $u f_1 = g_j$. Außerdem gilt $n > 1$, denn falls $n = 1$, so gilt $f_1 f_2 \mid g_1$, im Widerspruch dazu dass g_1 irreduzibel ist. Es gilt also

$$f_2 \cdot f_3\cdots f_m = (ug_1)g_2g_3\cdots g_{j-1} \cdot g_{j+1}\cdots g_n.$$

Nach Induktionsvoraussetzung gibt es eine bijektive Abbildung $\sigma : \{2, \ldots, m\} \to \{1, \ldots, n\}\setminus\{j\}$, sodass $f_i \sim g_{\sigma(i)}$ für alle $i \in \{2, \ldots, m\}$. Somit leistet $\pi := \sigma \cup \{(1, j)\}$ das Gewünchte. ■

ÜBUNGSAUFGABEN 2.23.
Sei R ein Integritätsbereich, und sei $I \subseteq R$. I ist eine *vollständige Auswahl irreduzibler Elemente*, wenn alle $i \in I$ irreduzibel sind und es für jedes irreduzible $f \in R$ genau ein $i \in I$ mit $f \sim_R i$ gibt. Sei $a \in \mathbb{R} \setminus \{0\}$. Eine Funktion $\alpha : I \to \mathbb{N}_0$ ist eine *Zerlegung* von a, wenn

(1) $\{i \in I \mid \alpha(i) \neq 0\}$ ist endlich.
(2) $a \sim_R \Pi_{i\in I}\, i^{\alpha(i)}$.

Dabei definieren wir für alle $i \in I$, dass $i^0 := 1$ ist. Ebenso ist ein Produkt $\Pi_{i\in\emptyset}$ immer gleich 1.

(1) Zeigen Sie: Sei R ein faktorieller Integritätsbereich und sei I eine vollständige Auswahl irreduzibler Elemente von R. Seien $a, b \in R \setminus \{0\}$, sei α eine Zerlegung von a bezüglich I und β eine Zerlegung von b bezüglich I. Dann sind äquivalent:
   (a) $a \mid b$.

(b) Für alle $i \in I$ gilt $\alpha(i) \leq \beta(i)$.

(2) Sei R ein faktorieller Integritätsbereich und sei I eine vollständige Auswahl irreduzibler Elemente von R. Sei $f \in R \setminus \{0\}$. Dann gibt es genau eine Zerlegung $\alpha : I \to \mathbb{N}_0$ von f.

6. Eine Anwendung in der Zahlentheorie

Wir brauchen zunächst folgende Beobachtung:

LEMMA 2.24. *Sei p eine ungerade Primzahl. Dann gilt:*

(1) *Für jedes $x \in \{1, \ldots, p-1\}$ gibt es ein $y \in \{1, \ldots, p-1\}$ mit $x \cdot y \equiv 1 \pmod{p}$.*
(2) *Für jedes $x \in \mathbb{Z}$ gilt: wenn $x^2 \equiv 1 \pmod{p}$, so gilt $x \equiv 1 \pmod{p}$ oder $x \equiv -1 \pmod{p}$.*
(3) $(p-1)! \equiv -1 \pmod{p}$ *und* $(\frac{p-1}{2}!)^2 \equiv (-1)^{\frac{p-3}{2}} \pmod{p}$.

Beweis: (1) Da $\mathrm{ggT}(x, p) = 1$, gibt es $u, v \in \mathbb{Z}$ mit $ux + vp = 1$. Somit gilt für $y := u \bmod p$, dass $y\,x \equiv 1 \pmod{p}$. (2) Wenn $p \mid x^2 - 1 = (x+1)(x-1)$, so gilt wegen des Fundamentallemmas (Satz 1.6) $p \mid x+1$ oder $p \mid x-1$. (3) Für jedes $x \in \{2, \ldots, p-2\}$ gibt es ein $y \in \{2, \ldots, p-2\}$ mit $x\,y \equiv 1 \pmod{p}$. Dieses y erfüllt $y \neq x$. Somit gilt $\prod_{i=2}^{p-2} i \equiv 1 \pmod{p}$, also $(p-1)! \equiv -1 \pmod{p}$. Für $i \in \{1, \ldots, \frac{p-1}{2}\}$ gilt $-i \equiv p - i \pmod{p}$, also gilt

$$-1 \equiv_p (p-1)! = \prod_{i=1}^{\frac{p-1}{2}} i \cdot \prod_{i=1}^{\frac{p-1}{2}} (p-i)$$

$$\equiv_p (\frac{p-1}{2}!) \cdot (-1)^{\frac{p-1}{2}} \cdot (\frac{p-1}{2}!) = (\frac{p-1}{2}!)^2 \cdot (-1)^{\frac{p-1}{2}}.$$

■

Wir beweisen nun den folgenden Satz:

SATZ 2.25. *Sei p eine Primzahl mit $p \equiv 1 \pmod{4}$. Dann gibt es $a, b \in \mathbb{N}$, sodass $a^2 + b^2 = p$.*

Beweis: Sei $x := \frac{p-1}{2}!$. Wegen Lemma 2.24 gilt dann

$$x^2 \equiv -1 \pmod{p}. \tag{2.1}$$

Im Ring $\mathbb{Z}[i]$ gilt natürlich ebenfalls $p \mid (1 + x^2)$, also $p \mid (1 + x\,i) \cdot (1 - x\,i)$. Da jedes Vielfache von p im Ring $\mathbb{Z}[i]$ einen durch p teilbaren Realteil hat, gilt in $\mathbb{Z}[i]$ weder $p \mid (1 + x\,i)$ noch $p \mid (1 - x\,i)$. Im Ring $\mathbb{Z}[i]$ ist p also nicht prim. Wegen Satz 2.16 und Satz 2.18 ist $\mathbb{Z}[i]$ ein Hauptidealbereich. Somit ist wegen Lemma 2.21 jedes irreduzible Element von $\mathbb{Z}[i]$ prim. Also ist p in $\mathbb{Z}[i]$ nicht irreduzibel. Es gibt folglich $a, b, c, d \in \mathbb{Z}$, sodass $p = (a+b\,i)(c+d\,i)$, und $a+b\,i$ und $c+d\,i$ nicht invertierbar sind. Sei $N(u + v\,i) := u^2 + v^2$ für alle $u, v \in \mathbb{Z}$. Dann gilt

$$p^2 = N(p) = N((a + b\,i)(c + d\,i)) = N(a + b\,i) \cdot N(c + d\,i) = (a^2 + b^2)(c^2 + d^2).$$

Alle Elemente $z \in \mathbb{Z}[i]$ mit $N(z) = 1$ sind invertierbar. Somit muss $a^2 + b^2 = p$ gelten. Die Zahlen $a' := |a|$ und $b' := |b|$ leisten also das Gewünschte. ■

Literaturverzeichnis

[Euk91] Euklid, *Die Elemente*, Wissenschaftliche Buchgesellschaft, Darmstadt, 1991, Buch I–XIII. [Book I–XIII], Based on Heiberg's text, Translated from the Greek and edited by Clemens Thaer.

[RU87] R. Remmert and P. Ullrich, *Elementare Zahlentheorie*, Birkhäuser Verlag, Basel, 1987.