KAPITEL 5

Rechnen in den ganzen Zahlen

1. Teilbarkeit

DEFINITION 5.1 (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 5.2 (Teilbarkeit). Für $x, y \in \mathbb{Z}$ gilt

$$x \text{ teilt } y$$

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 5.1. *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 5.3 (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 5.2. *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.■

[0]Unterlagen zur Vorlesung Algebra von Erhard Aichinger, Peter Mayr. Alle Rechte vorbehalten. 28.11.2007.

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 $u, v \in \mathbb{Z}$, 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	$(15 = 1 \cdot 147 - 4 \cdot 33)$
3	-2	9	$(3 = -2 \cdot 147 + 9 \cdot 33)$
0			

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

SATZ 5.3. *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 5.4. *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 $t|$*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 5.5. *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* 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 weil $a|bc$ auch $a \mid vbc$ gilt, gilt

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

und daher $a \mid c$. ■

Daraus kann man folgenden Satz herleiten:

SATZ 5.6.

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

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

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 5.7. *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 5.8. *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 und b. Sei $(p_1, p_2, p_3, \ldots) = (2, 3, 5, \ldots)$ die Folge der Primzahlen, und seien $(\nu_i)_{i\in\mathbb{N}}$ und $(\sigma_i)_{i\in\mathbb{N}}$ so dass $a = \prod_{i\in\mathbb{N}} p_i^{\nu_i}$ und $b = \prod_{i\in\mathbb{N}} p_i^{\sigma_i}$. Aus der Eindeutigkeit der Primfaktorzerlegung kann man herleiten, dass dann gelten muss:

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

Daraus folgt:

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

■

SATZ 5.9. *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. Das Lösen von Kongruenzen

DEFINITION 5.5. 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 5.10. *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) ⇒ (2)": Sei x eine Lösung, d.h. $c \mid ax - b$. Falls c die Zahl $ax - b$ teilt, dann gilt erst recht

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

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

"(2) ⇒ (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 5.11. *Seien $a, c \in \mathbb{Z}$ (nicht beide $= 0$), und sei $b \in \mathbb{Z}$. Sei x_0 eine Lösung von*

$$ax \equiv b \pmod{c}. \tag{5.1}$$

Dann ist die Lösungsmenge von (5.1) *gegeben durch:*

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

Beweis: "⊇": 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.

"⊆": 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

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

■

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

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

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

Beispiele: 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 5.12. *Seien $a_1,\,a_2\in\mathbb{Z}$, $m_1,\,m_2\in\mathbb{N}$. Das System*

$$\begin{aligned}x&\equiv a_1\ \left(\mathrm{mod}\ \mathrm{m}_1\right)\\ x&\equiv a_2\ \left(\mathrm{mod}\ \mathrm{m}_2\right)\end{aligned}$$

ist genau dann lösbar, wenn gilt

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

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

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

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

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

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 $\mathrm{ggT}(15, 21) = 3$ 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 5.13. *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: "⊇": 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 $\mathrm{kgV}\left(m_1, m_2\right) \mid \left(x_1 - x_0\right)$. ■