1. Teiler, gemeinsame Teiler und größter gemeinsamer Teiler

Vorbemerkungen: 1) Wir setzen die Rechenregeln für $\mathbb{Z}$ voraus, formal dass $(\mathbb{Z}, +, \cdot)$ ein Integritätsbereich (d.h. ein nullteilerfreier kommutativer Ring mit Einselement) ist. Dabei bedeutet Nullteilerfreiheit, dass für $a, b \in \mathbb{Z}$ gilt, dass

$$a \cdot b = 0 \implies a = 0 \text{ oder } b = 0$$

Daraus folgt für $a, b, x \in \mathbb{Z}$ mit $x \neq 0$, dass

$$a \cdot x = b \cdot x \implies (a-b) \cdot x = a \cdot x - b \cdot x = 0 \xrightarrow{x \neq 0} a - b = 0 \implies a = b.$$

2) Weiters setzen wir die Eigenschaften der Ordnungsrelation $\leq$ (auch in Verbindung mit Addition und Multiplikation) voraus.

3) Schließlich werden wir verwenden: Ist $A \subseteq \mathbb{Z}$, $A \neq \emptyset$ und A ist nach unten (bzw. oben) beschränkt, so besitzt A ein kleinstes (bzw. größtes) Element. (Das ist anschaulich klar, aber nicht selbstverständlich. Das offene Intervall $(0,1)$ $(\subseteq \mathbb{R})$ ist nach unten und oben beschränkt (z.B. durch 0 und 1), besitzt aber weder ein kleinstes, noch ein größtes Element.)

4) Wie in der Schule üblich ist $\mathbb{N} = \{0, 1, 2, 3, \dots\}$, allerdings wird es oft praktisch sein, mit $\mathbb{N} \setminus \{0\} = \{1, 2, 3, \dots\}$ zu arbeiten.

Definition: Es seien $m, n \in \mathbb{Z}$. Man sagt, „m teilt n" wenn $\exists d \in \mathbb{Z} : n = m \cdot d$. Man schreibt dafür $m \mid n$ und sagt auch „m ist Teiler von n" bzw. „n ist Vielfaches von m". Ist m kein Teiler von n, so schreibt man $m \nmid n$. Ist $n = m \cdot d$, so wird d der Komplementärteiler von n zu m genannt.

Bemerkungen: 1) Diese Definition weicht von der in der Schule üblichen ab. Zunächst dürfen m, n ganze Zahlen sein – und nicht nur aus $\mathbb{N} \setminus \{0\}$. 2) In der Schule wird definiert, dass eine Zahl $m (\in \mathbb{N} \setminus \{0\})$ eine andere Zahl $n (\in \mathbb{N} \setminus \{0\})$ teilt, wenn die Division von n durch m den Rest 0 liefert. („Zahlen, die eine gegebene Zahl ohne Rest teilen, heißen Teiler dieser Zahl.") Auch hier unterscheidet sich unsere Definition: Überraschenderweise gilt nämlich $0 \mid 0$ da $0 = 0 \cdot 1$. Darum haben wir nicht definiert, dass $\frac{n}{m} \in \mathbb{Z}$ sein soll und werden auch nicht so argumentieren. (Für $m, n \in \mathbb{N} \setminus \{0\}$ sind unsere Definition und die aus dem Schulbuch allerdings äquivalent.)

Satz 1 (Rechenregeln für Teilbarkeit) Alle auftretenden Größen sind ganze Zahlen

(i) $\forall n \in \mathbb{Z} : 1 \mid n$ und $n \mid n$ (d.h. jede ganze Zahl wird von 1 und sich selbst geteilt),

(ii) $\forall n \in \mathbb{Z} : n \mid 0$. Aus $0 \mid n$ folgt $n = 0$ (d.h. jede ganze Zahl teilt 0 aber 0 teilt nur sich selbst),

(iii) $m \mid n \Rightarrow (-m) \mid n$ und $m \mid (-n)$,

(iv) $m \mid n$ und $n \neq 0 \Rightarrow |m| \leq |n|$,

(v) $n \mid 1 \Leftrightarrow n \in \{1, -1\}$ (d.h. die Teiler von 1 sind genau 1 und -1),

(vi) $m \mid n$ und $n \mid m \Rightarrow n = m$ oder $n = -m$ (d.h. $|n| = |m|$),

(vii) $\ell \mid m$ und $m \mid n \Rightarrow \ell \mid n$ (Transitivität der Teilerrelation),

(viii) $m \mid n \Rightarrow (\ell m) \mid (\ell n) \quad \forall \ell \in \mathbb{Z}$,

(ix) $(\ell m) \mid (\ell n)$ und $\ell \neq 0 \Rightarrow m \mid n$,

(x) $m \mid n_1, \dots, m \mid n_k \Rightarrow m \mid (\ell_1 n_1 + \dots + \ell_k n_k) \quad \forall \ell_1, \dots, \ell_k \in \mathbb{Z}$ (d.h. $m \mid \sum_{i=1}^{k} \ell_i n_i \quad \forall \ell_1, \dots, \ell_k \in \mathbb{Z}$),

(xi) $m_1 \mid n_1, \dots, m_k \mid n_k \Rightarrow (m_1 \cdot \dots \cdot m_k) \mid (n_1 \cdot \dots \cdot n_k)$ (d.h. $\prod_{i=1}^{k} m_i \mid \prod_{i=1}^{k} n_i$).

Beweis: (i) $n = 1 \cdot n \quad \forall n \in \mathbb{Z} \Rightarrow 1 \mid n \quad \forall n \in \mathbb{Z}$ (n ist Komplementärteiler) und $n \mid n \; \forall n \in \mathbb{Z}$ (1 ist Komplementärteiler)

(ii) $0 = 0 \cdot n \; \forall n \in \mathbb{Z} \Rightarrow n \mid 0 \; \forall n \in \mathbb{Z}$ (0 ist Komplementärteiler), $0 \mid n \Rightarrow \exists d \in \mathbb{Z} : n = 0 \cdot d = 0$

(iii) $m \mid n \Rightarrow \exists d \in \mathbb{Z} : n = m \cdot d$. Daraus folgt einerseits $n = (-m) \cdot (-d)$ und daher $(-m) \mid n$ und andererseits $-n = m \cdot (-d)$ und daher $m \mid (-n)$.

(iv) $m \mid n \Rightarrow \exists d \in \mathbb{Z} : n = m \cdot d$. Dabei ist $d \neq 0$, denn aus $d = 0$ würde $n = m \cdot 0 = 0$ folgen, ein Widerspruch. Also ist $|d| \geq 1$ und daher

$$|n| = |m \cdot d| = |m| \cdot |d| \geq |m| \cdot 1 = |m|.$$

(v) Ist $n \mid 1$, so folgt $|n| \leq 1$ wegen (iv) und daher $n \in \{-1, 0, 1\}$. Wegen (ii) ist $n = 0$ unmöglich und daher $n \in \{-1, 1\}$. Umgekehrt folgt aus $1 = (\pm 1)^2$, dass $\pm 1 \mid 1$.

(vi) Ist $m \mid n$ und $n \mid m$, so folgt wegen (ii) dass $m = 0 \Leftrightarrow n = 0$. Ist $m = n = 0$, so ist die Behauptung erfüllt. Da nach dem eben Bewiesenen auch $m \neq 0 \Leftrightarrow n \neq 0$ gilt, ist als zweite Möglichkeit nur

$m,n \in \mathbb{Z}\setminus\{0\}$ möglich. Wegen (iv) folgt dann $|m| \le |n|$ und $|n| \le |m|$.
Also ist $|m| = |n|$, was zu $n \in \{m, -m\}$ äquivalent ist.

(vii) $\ell \mid m$ und $m \mid n \Rightarrow \exists d_1, d_2 \in \mathbb{Z}: m = \ell d_1$ und $n = m d_2$
$\Rightarrow n = m d_2 = (\ell d_1) d_2 = \ell \cdot (d_1 d_2) \Rightarrow \ell \mid n$

7.3.2022

(viii) $m \mid n \Rightarrow \exists d \in \mathbb{Z}: n = dm \Rightarrow \ell n = d(\ell m)\ \forall \ell \in \mathbb{Z} \Rightarrow (\ell m) \mid (\ell n)\ \forall \ell \in \mathbb{Z}$

(ix) $(\ell m) \mid (\ell n) \Rightarrow \exists d \in \mathbb{Z}: \ell n = (\ell m) d = \ell (md)$. Da $\ell \neq 0$ folgt $n = md$ und daher $m \mid n$.

(x) $m \mid n_1, \dots, m \mid n_k \Rightarrow \exists d_1, \dots, d_k \in \mathbb{Z}: n_1 = m d_1, \dots, n_k = m d_k$
$\Rightarrow \ell_1 n_1 + \dots + \ell_k n_k = \ell_1 (m d_1) + \dots + \ell_k (m d_k) = (\ell_1 d_1 + \dots + \ell_k d_k) m$
$\Rightarrow m \mid (\ell_1 n_1 + \dots + \ell_k n_k)$

(xi) $m_1 \mid n_1, \dots, m_k \mid n_k \Rightarrow \exists d_1, \dots, d_k \in \mathbb{Z}: n_1 = m_1 d_1, \dots, n_k = m_k d_k$
$\Rightarrow n_1 \cdot \dots \cdot n_k = (m_1 d_1) \dots (m_k d_k) = (m_1 \dots m_k)(d_1 \dots d_k)$
$\Rightarrow (m_1 \dots m_k) \mid (n_1 \dots n_k)$

Beispiele: 1) Aus $12 \mid 48$ (da $48 = 4 \cdot 12$) folgt $(-12) \mid 48$ (da $48 = (-4) \cdot (-12)$), $12 \mid (-48)$ (da $-48 = (-4) \cdot 12$) und $(-12) \mid (-48)$ (da $-48 = 4 \cdot (-12)$), (Spezialfälle von (iii)).

2) Aus $7 \mid 21$ (da $21 = 3 \cdot 7$) und $21 \mid 84$ (da $84 = 4 \cdot 21$) folgt $7 \mid 84$ (da $84 = 12 \cdot 7 = (4 \cdot 3) \cdot 7$), (Spezialfall von (vii))

3) Aus $(-15) \mid 45$ (da $45 = (-3)(-15)$) folgt $30 \mid (-90)$ (da $(-2) \cdot (-15) \mid (-2) \cdot 45$ bzw. $-90 = (-3) \cdot 30$) (Spezialfall von (viii) mit $\ell = -2$)

4) Aus $40 \mid 200$ (da $200 = 5 \cdot 40$), da $(5 \cdot 8) \mid (5 \cdot 40)$ folgt (wegen (ix) mit $\ell = 5$) $8 \mid 40$ (bzw. $40 = 5 \cdot 8$).

5) Aus $7 \mid 14$ (da $14 = 2 \cdot 7$) und $7 \mid 35$ (da $35 = 5 \cdot 7$) folgt (wegen (x) mit $\ell_1 = 2, \ell_2 = -1$) $7 \mid (2 \cdot 35 - 14)$, da $7 \mid 56$ (bzw. $56 = 7 \cdot 8$).

6) Aus $3 \mid 12$ (da $12 = 4 \cdot 3$) und $2 \mid 10$ (da $10 = 2 \cdot 5$) folgt $(3 \cdot 2) \mid (12 \cdot 10)$, da $6 \mid 120$ (bzw. $120 = 6 \cdot 20$) (Spezialfall von (xi)).

Bemerkungen: 1) Jedes $n \in \mathbb{Z}$ besitzt (wegen Satz 1 (i) und (iii)) die (trivialen) Teiler $1, -1, n$ und $-n$. Ist $d \mid n$ und $d \notin \{1, -1, n, -n\}$, so nennen wir d einen echten Teiler von n.

2) Ist $n \in \mathbb{Z} \setminus \{0\}$ und $d \mid n$, so folgt (wegen Satz 1 (iv)) $|d| \leq |n|$ und daher $-|n| \leq d \leq |n|$. Man sieht, dass jedes $n \in \mathbb{Z} \setminus \{0\}$ nur endlich viele Teiler besitzt.

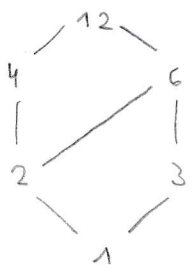
3) Ist $n \in \mathbb{Z}$, so besitzen n und $-n$ (wegen Satz 1 (iii)) genau dieselben Teiler (dh $d \mid n \iff d \mid (-n)$). Z.B. ist die Menge $\widetilde{T}_{12}$ der Teiler von 12 und die Menge $\widetilde{T}_{-12}$ der Teiler von -12 jeweils $\widetilde{T}_{12} = \widetilde{T}_{-12} = \{\pm 1, \pm 2, \pm 3, \pm 4, \pm 6, \pm 12\}$

4) Ist $n \in \mathbb{N} \setminus \{0\}$ und man hat alle Teiler $d > 0$ von n mit $1 \leq d \leq \sqrt{n}$ gefunden, so sind die restlichen positiven Teiler von n genau die Komplementärteiler. Gilt nämlich $d \mid n$ und $d > \sqrt{n}$ (> 0), so gilt für den Komplementärteiler $\frac{n}{d}$ von n zu d, dass $\frac{n}{d} < \frac{n}{\sqrt{n}} = \sqrt{n}$. Ist z.B. $n = 60$, so sind die positiven Teiler d von 60 mit $d < \sqrt{60} = 7{,}74\ldots$ gerade $1, 2, 3, 4, 5, 6$ und die restlichen positiven Teiler von 60 daher $60, 30, 20, 15, 12, 10$.

5) Aus Satz 1 folgt, dass die Teilerrelation auf $\mathbb{N} \setminus \{0\}$ eine Ordnungsrelation ist. Es gelten je

- $\forall n \in \mathbb{N} \setminus \{0\} : n \mid n$ (wegen Satz 1 (i)), dh die Teilerrelation ist reflexiv,
- Gilt für $m, n \in \mathbb{N} \setminus \{0\}$, dass $m \mid n$ und $n \mid m$, so folgt (aus Satz 1 (vii)), dass $|m| = |n|$, dh $m = n$, dh die Teilerrelation ist antisymmetrisch,
- Für $l, m, n \in \mathbb{N} \setminus \{0\}$ folgt aus $l \mid m$ und $m \mid n$, dass $l \mid n$ (Satz 1 (viii)), dh die Teilerrelation ist transitiv.

Die Teilerrelation ist aber keine Totalordnung, dh es gibt Paare von Zahlen, die in keiner Relation zueinander stehen (z.B. $2 \nmid 3$ und $3 \nmid 2$). Für die positiven Teiler von 12 (dh $1, 2, 3, 4, 6, 12$) kann man die Teilerordnung z.B. graphisch folgendermaßen darstellen:



Ist eine Zahl mit einer höher gelegenen durch einen Strich (oder mehrere Striche) verbunden, so teilt sie die höher gelegene Zahl. Z.B. teilt 1 jede andere Zahl, da sie direkt oder mit mehreren Strichen verbunden ist und 2 teilt 4, 6 und 12.

Satz 2 (Division mit Rest) Es seien $m \in \mathbb{Z}$ und $n \in \mathbb{N} \setminus \{0\}$. Dann gibt es eindeutig bestimmte $q, r \in \mathbb{Z}$ mit den Eigenschaften $m = qn + r$ und $0 \leq r < n$.

Beweis: Existenz: Es sei $q \in \mathbb{Z}$, derart dass $q \leq \frac{m}{n} < q+1$, woraus $qn \leq m < qn + n$ und $0 \leq m - qn < n$ folgt. Setzt man $r := m - qn$, so sind $m = qn + r$ und $0 \leq r < n$ erfüllt.
Eindeutigkeit: Angenommen $m = qn + r = \bar{q}n + \bar{r}$ und $0 \leq r, \bar{r} < n$ für gewisse $q, \bar{q}, r, \bar{r} \in \mathbb{Z}$. Dann folgt $(q - \bar{q})n = \bar{r} - r$ und daher $q - \bar{q} = \frac{\bar{r} - r}{n}$. Aus $-n < \bar{r} - r < n$ folgt $-1 < \frac{\bar{r} - r}{n} < 1$. Da $\frac{\bar{r} - r}{n} \in \mathbb{Z}$, muss $\frac{\bar{r} - r}{n} = 0$ gelten, woraus $r = \bar{r}$ folgt. Also ist $qn = \bar{q}n$ und daher auch $q = \bar{q}$.

Definition: Sind $n_1, \dots, n_k \in \mathbb{Z}$ (nicht notwendig verschieden), so heißt $m \in \mathbb{Z}$ gemeinsamer Teiler von $n_1, \dots, n_k$ wenn m alle diese Zahlen teilt, dh $m | n_1, \dots, m | n_k$.

Notation: Ist $n \in \mathbb{Z}$, so schreiben wir T_n für die Menge der positiven Teiler von n, dh
$T_n = \{ m \in \mathbb{N} \setminus \{0\} \mid m | n \}$.

Beispiele: 1) Die Menge der positiven gemeinsamen Teiler von 8 und 12 ist $\{1, 2, 4\}$.
Aus $T_8 = \{1, 2, 4, 8\}$ und $T_{12} = \{1, 2, 3, 4, 6, 12\}$ folgt, dass diese Menge $T_8 \cap T_{12} = \{1, 2, 4\}$ ist.
2) Die Menge der positiven gemeinsamen Teiler von 30, 45 und 75 ist $\{1, 3, 5, 15\}$, denn
$T_{30} = \{1, 2, 3, 5, 6, 10, 15, 30\}$, $T_{45} = \{1, 3, 5, 9, 15, 45\}$ und $T_{75} = \{1, 3, 5, 15, 25, 75\}$
und daher $T_{30} \cap T_{45} \cap T_{75} = \{1, 3, 5, 15\}$.

Bemerkungen: 1) Die Menge der positiven Teiler von 0 ist $T_0 = \mathbb{N} \setminus \{0\}$ (wegen Satz 1 (iii)).
Ist also $n_1 = \dots = n_k = 0$, so ist jede positive ganze Zahl gemeinsamer Teiler von $n_1, \dots, n_k$. (Aus $T_{n_1} = \dots = T_{n_k} = \mathbb{N} \setminus \{0\}$ folgt $T_{n_1} \cap \dots \cap T_{n_k} = \mathbb{N} \setminus \{0\}$.) 14.3.2022
2) Sind die Zahlen $n_1, \dots, n_k \in \mathbb{Z}$ nicht alle $= 0$, so besitzen sie stets einen positiven gemeinsamen Teiler, nämlich 1 (siehe Satz 1 (i)). Da die Menge der positiven gemeinsamen Teiler von $n_1, \dots, n_k$ ist nichtleer. Ist $n_i \neq 0$, so ist die Menge der Teiler von n_i endlich (siehe Bemerkung 2, Seite 4). Also ist auch die Menge T_{n_i} der positiven Teiler von n_i endlich und daher nach oben beschränkt. Die Menge $T_{n_1} \cap \dots \cap T_{n_k}$ ($\subseteq T_{n_i}$) ist dann erst recht endlich und daher nach oben beschränkt.
Insgesamt ist (wenn $n_1, \dots, n_k \in \mathbb{Z}$ nicht alle $= 0$ sind) die Menge der positiven gemeinsamen Teiler von $n_1, \dots, n_k$ nichtleer (da $1 \in T_{n_1} \cap \dots \cap T_{n_k}$) und nach oben beschränkt (z.B. durch $\min \{ |n_i| \mid 1 \leq i \leq k, n_i \neq 0 \}$).
Es ist daher sinnvoll zu definieren:

Definition: Sind $n_1,\dots,n_k \in \mathbb{Z}$ nicht alle $=0$, so sei

$$ggT(n_1,\dots,n_k) = \max(T_{n_1} \cap \dots \cap T_{n_k}) = \max\{m \in \mathbb{N}\setminus\{0\} \mid m|n_1,\dots,m|n_k\}.$$

Dabei ist ggT die Abkürzung für größter gemeinsamer Teiler.

Beispiele: 1) $ggT(8,12) = \max\{1,2,4\} = 4$,

2) $ggT(30,45,75) = \max\{1,3,5,15\} = 15$.

Bemerkung: Die im letzten Beispiel angewandte Methode der Bestimmung des ggT ist nur für kleine Zahlen $n_1,\dots,n_k$ gut anwendbar, bei denen die Mengen $T_{n_1},\dots,T_{n_k}$ leicht zu überblicken sind.

Satz 3 Es seien $n_1,\dots,n_k \in \mathbb{Z}$ nicht alle $=0$. Dann gelten:

(i) $ggT(n_1,\dots,n_k) = ggT(|n_1|,\dots,|n_k|)$

(d.h. man kann bei der Berechnung des ggT stets zu den Beträgen übergehen),

(ii) Ist $i_1,\dots,i_k$ irgendeine Anordnung der Indizes $1,\dots,k$, so ist

$ggT(n_{i_1},\dots,n_{i_k}) = ggT(n_1,\dots,n_k)$

(d.h. der ggT hängt nicht von der Reihenfolge der Zahlen $n_1,\dots,n_k$ ab),

(iii) Ist $k \geq 2$ und $n_k = 0$, so ist $ggT(n_1,\dots,n_k) = ggT(n_1,\dots,n_{k-1})$

(d.h. bei der Bestimmung von $ggT(n_1,\dots,n_k)$ können alle $n_i = 0$ weggelassen werden),

(iv) Ist $k \geq 2$ und $n_k = n_{k-1}$, so ist $ggT(n_1,\dots,n_k) = ggT(n_1,\dots,n_{k-1})$

(d.h. bei der Bestimmung von $ggT(n_1,\dots,n_k)$ können alle n_i, die ein zweites, drittes, etc. Mal auftreten, weggelassen werden),

(v) Für alle $x_1,\dots,x_{k-1} \in \mathbb{Z}$ ist $ggT(n_1,\dots,n_{k-1},n_k + \sum_{i=1}^{k-1} x_i n_i) = ggT(n_1,\dots,n_k)$.

Beweis: (i) Wegen Satz 1(iii) gilt $d|n \iff d||n|$. Daher gilt für $d \in \mathbb{N}\setminus\{0\}$, dass $d|n_1,\dots,d|n_k \iff d||n_1|,\dots,d||n_k|$. Also ist $T_n = T_{|n|}$ und $T_{n_1} \cap \dots \cap T_{n_k} = T_{|n_1|} \cap \dots \cap T_{|n_k|}$, d.h. die Menge der gemeinsamen Teiler von $n_1,\dots,n_k$ und die Menge der gemeinsamen Teiler von $|n_1|,\dots,|n_k|$ stimmen überein. Daraus folgt

$$ggT(n_1,\dots,n_k) = \max(T_{n_1} \cap \dots \cap T_{n_k}) = \max(T_{|n_1|} \cap \dots \cap T_{|n_k|}) = ggT(|n_1|,\dots,|n_k|).$$

(ii) – (v) beweist man weitgehend analog. Bei jeder Aussage stimmen die Mengen der positiven gemeinsamen Teiler auf beiden Seiten überein.

(Bei (ii) gilt ja $d|n_{i_1},\dots,d|n_{i_k} \iff d|n_1,\dots,d|n_k$ und bei (iii) und (iv) ist $d|n_1,\dots,d|n_k \iff d|n_1,\dots,d|n_{k-1}$. Die entsprechende Äquivalenz bei (v) folgt aus Satz 1 (x): Aus $d|n_1,\dots,d|n_k$ folgt $d|(n_k+\sum_{i=1}^{k-1}x_in_i)$ $\forall x_1,\dots,x_{k-1}\in\mathbb{Z}$ und umgekehrt folgt aus $d|n_1,\dots,d|n_{k-1}$, $d|(n_k+\sum_{i=1}^{k-1}x_in_i)$, dass $d|\left((n_k+\sum_{i=1}^{k-1}x_in_i)-\sum_{i=1}^{k-1}x_in_i\right)$, also $d|n_k$.)

Bemerkungen: 1) Satz 3 (ii) kann man auch folgendermaßen formulieren. Bezeichnet S_k die Menge aller Permutationen der Zahlen $1,2,\dots,k$, so ist

$$ggT(n_{\sigma(1)},\dots,n_{\sigma(k)}) = ggT(n_1,\dots,n_k) \quad \forall \sigma\in S_k.$$

2) In Satz 3 (iii), (iv) und (v) kann der Index k (bzw. $k-1$ in Satz 3 (iv)) durch einen beliebigen anderen Index $1,2,\dots,k-1$ ersetzt werden. Das folgt aus Satz 3 (ii), ist aber auch offensichtlich.

Beispiele: 1) Aus Satz 3 (i) folgt $ggT(-8,-12) = ggT(-8,12) = ggT(8,-12) = ggT(8,12) = 4$

2) Aus Satz 3 (ii) folgt $ggT(30,45,75) = ggT(45,30,75) = ggT(30,75,45) = \dots = 15$.

3) Aus Satz 3 (iii) folgt $ggT(8,12,0) = ggT(8,0,12) = ggT(0,8,12) = ggT(8,12) = 4$.

4) Aus Satz 3 (iv) folgt $ggT(8,8,12) = ggT(8,12,8) = ggT(12,8,8) = ggT(8,12,12)$
$= ggT(8,8,12,12) = \dots = ggT(8,12) = 4$.

Satz 4 (Euklidischen Algorithmus) Gegeben sind $a,b\in\mathbb{N}\setminus\{0\}$, wobei o.B.d.A. $b\le a$ gelten soll. Gesucht ist $ggT(a,b)$. Führe nun wiederholt Division mit Rest durch:

$$\begin{aligned}
a &= bq_0 + r_1, && 0\le r_1 < b\\
b &= r_1q_1 + r_2, && 0\le r_2 < r_1\\
r_1 &= r_2q_2 + r_3, && 0\le r_3 < r_2\\
&\vdots\\
r_{m-1} &= r_mq_m + r_{m+1}, && 0\le r_{m+1} < r_m
\end{aligned}$$

Setze zusätzlich $r_0 = b$. Wegen $b = r_0 > r_1 > r_2 > r_3 > \dots > r_m > r_{m+1} > \dots \ge 0$ gibt es ein kleinstes $n\ge 0$ mit $r_{n+1} = 0$. Es gilt dann $r_n = ggT(a,b)$.

Beweis: Wir zeigen zunächst, dass r_n ein gemeinsamer Teiler von a und b ist. Aus $r_{n-1} = r_nq_n$ folgt sofort $r_n | r_{n-1}$. Wegen $r_{n-2} = r_{n-1}q_{n-1} + r_n$ und Satz 1 (x) folgt $r_n | r_{n-2}$. Verfahre nun weiter so: Ist $r_n | r_{m+1}$ und $r_n | r_m$ bereits gezeigt, so folgt $r_n | r_{m-1}$ wegen $r_{m-1} = r_mq_m + r_{m+1}$ und Satz 1 (x). Hat man $r_n | r_2$ und $r_n | r_1$ gezeigt, so folgt $r_n | b$ wegen $b = r_1q_1 + r_2$ und Satz 1 (x).

Schließlich erhält man $r_n | a$ aus $a = bq_0 + r_1$ und Satz 1(x).

Es sei nun d ein beliebiger positiver gemeinsamer Teiler von a und b. Aus $r_1 = a - bq_0$ und Satz 1(x) folgt $d | r_1$. Wegen $r_2 = b - r_1 q_1$ und Satz 1(x) erhält man $d | r_2$. Verfahre weiter so: Ist $d | r_{m-1}$ und $d | r_m$ bereits gezeigt, so folgt $d | r_{m+1}$ wegen $r_{m+1} = r_{m-1} - r_m q_m$ und Satz 1(x). Schließlich erhält man $d | r_n$ und daher $d \leq r_n$ wegen Satz 1 (iv).

Bemerkungen: 1) Die Berechnung des ggT mit Hilfe des euklidischen Algorithmus ist normalerweise wesentlich effizienter und rascher als die Bestimmung von $\max(T_a \cap T_b)$.

2) Die Festlegung $r_0 = b$ hat folgenden Grund: Wenn $b | a$, so gilt offenbar $ggT(a,b) = b$. Wendet man den euklidischen Algorithmus an, so ergibt sich $a = bq_0 + r_1$ mit $r_1 = 0$ und $r_0 = ggT(a,b) = b$. Da der euklidische Algorithmus liefert auch in diesem Fall das richtige Ergebnis.

3) Wegen Satz 3(i) ist die Voraussetzung, dass $a, b > 0$ keine Einschränkung. Sind $a, b \in \mathbb{Z} \setminus \{0\}$, so ist $ggT(a,b) = ggT(|a|, |b|)$ und man kann den euklidischen Algorithmus auf $|a|$ und $|b|$ anwenden.

4) Der euklidische Algorithmus heißt so, weil man ihn im wesentlichen bereits in den Elementen des Euklid, Buch VII, Proposition 2 (circa 300 v. Chr.) findet.

Beispiele: 1) Bestimmung von $ggT(111, 39) = 3$:

$$\begin{aligned} 111 &= 2 \cdot 39 + 33 \\ 39 &= 1 \cdot 33 + 6 \\ 33 &= 5 \cdot 6 + 3 \\ 6 &= 2 \cdot 3 \end{aligned}$$

oder

$$\left.\begin{aligned} T_{111} &= \{1, 3, 37, 111\} \\ T_{39} &= \{1, 3, 13, 39\} \end{aligned}\right\} \Rightarrow T_{39} \cap T_{111} = \{1, 3\}$$

2) Bestimmung von $ggT(9973, 2137) = 1$:

$$\begin{aligned} 9973 &= 4 \cdot 2137 + 1425 \\ 2137 &= 1 \cdot 1425 + 712 \\ 1425 &= 2 \cdot 712 + 1 \\ 712 &= 712 \cdot 1 \end{aligned}$$

oder

$$\left.\begin{aligned} T_{9973} &= \{1, 9973\} \\ T_{2137} &= \{1, 2137\} \end{aligned}\right\} \Rightarrow T_{9973} \cap T_{2137} = \{1\}$$

21.3.2022

Satz 5 Es seien $n_1,\dots,n_k \in \mathbb{Z}$, nicht alle $=0$. Dann gilt

$$ggT(n_1,\dots,n_k) = \min\left\{ \sum_{i=1}^{k} x_i n_i \;\middle|\; x_1,\dots,x_k \in \mathbb{Z},\ \sum_{i=1}^{k} x_i n_i > 0 \right\}$$

Beweis: Es bezeichne $L\ (\subseteq \mathbb{N}\setminus\{0\})$ die Menge $L := \left\{ \sum_{i=1}^{k} x_i n_i \;\middle|\; x_1,\dots,x_k \in \mathbb{Z},\ \sum_{i=1}^{k} x_i n_i > 0 \right\}$.

Wir setzen zunächst $x_i = n_i$ für $1 \le i \le k$. Da $n_1,\dots,n_k$ nicht alle $=0$ sind, gibt es ein $j \in \{1,\dots,k\}$, derart dass $n_j \neq 0$ und daher $\sum_{i=1}^{k} x_i n_i = \sum_{i=1}^{k} n_i^2 \ge n_j^2 > 0$.

Das zeigt, dass $L \neq \emptyset$ ist. Da L durch 0 noch unten beschränkt ist, ist es also sinnvoll $d' := \min L$ zu definieren. Weiters sei $d := ggT(n_1,\dots,n_k)$.

Wir wollen zeigen, dass $d = d'$.

Wir zeigen zunächst $d \le d'$. Da $d' \in L$, gibt es $y_1,\dots,y_k \in \mathbb{Z}$, derart dass $d' = \sum_{i=1}^{k} y_i n_i$.

Da $d \mid n_i$ für $1 \le i \le k$ folgt aus Satz 1(x), dass $d \mid d'$ und daher $d \le d'$ wegen Satz 1 (iv).

Wir zeigen nun $d' \le d$: Wir wenden dazu Satz 2 (Division mit Rest) für $1 \le j \le k$ auf n_j und d' an:

$$\forall j \in \{1,\dots,k\}\ \exists q_j, r_j \in \mathbb{Z} \text{ mit } n_j = q_j d' + r_j \text{ und } 0 \le r_j < d'$$

Wir wollen nun zeigen, dass $r_j = 0$ (und daher $d' \mid n_j$) für $1 \le j \le k$ gelten muss. (Hat man das gezeigt, so ist d' ein gemeinsamer Teiler von $n_1,\dots,n_k$ und daher $d' \le d$.) Haben $y_1,\dots,y_k$ die selbe Bedeutung wie oben, so folgt (für $1 \le j \le k$)

$$r_j = n_j - q_j d' = n_j - q_j \sum_{i=1}^{k} y_i n_i = \underbrace{(1 - q_j y_j)}_{=: z_{jj}} n_j + \sum_{\substack{1 \le i \le k \\ i \neq j}} \underbrace{(-q_j y_i)}_{=: z_{ij}} n_i$$

Wäre $r_j > 0$, so wäre $r_j = \sum_{i=1}^{k} z_{ij} n_i \in L$ und $r_j < d'$. Das ist ein Widerspruch zur Definition von d'. Daher ist $r_j = 0$.

Korollar 6 Es seien $n_1,\dots,n_k \in \mathbb{Z}$, nicht alle $=0$. Dann gibt es $x_1,\dots,x_k \in \mathbb{Z}$, derart dass $x_1 n_1 + \dots + x_k n_k = ggT(n_1,\dots,n_k)$.

Beweis: Das folgt sofort aus Satz 5.

Bemerkungen: 1) Ein wichtiger Spezialfall von Korollar 6 ist: Sind $a, b \in \mathbb{Z}$, nicht beide $=0$, so gibt es $x, y \in \mathbb{Z}$, derart dass $xa + yb = ggT(a,b)$.

2) Die $x_1,\dots,x_n \in \mathbb{Z}$ mit der Eigenschaft, dass $\sum_{i=1}^{k} x_i n_i = ggT(n_1,\dots,n_k)$ ist, sind nicht eindeutig bestimmt, was man schon im Fall $k=2$ erkennen kann:
Sind $a,b \in \mathbb{Z}$, nicht beide $=0$, $d = ggT(a,b)$ und $x,y \in \mathbb{Z}$, derart dass $ax+by=d$, so ist auch

$$a\left(x+\frac{b}{d}t\right) + b\left(y-\frac{a}{d}t\right) = ax+by+\frac{ab}{d}t-\frac{ab}{d}t = ax+by = d \quad \forall t \in \mathbb{Z},$$

d.h. es gibt tatsächlich stets unendlich viele Lösungen
3) Sind $a,b \in \mathbb{Z}\setminus\{0\}$, $d = ggT(a,b)$ und man will $x,y \in \mathbb{Z}$ mit der Eigenschaft $ax+by=d$ bestimmen, so kann man das tun, indem man den euklidischen Algorithmus für $|a|$ und $|b|$ „rückwärts einsetzt:"

Beispiel: $ggT(97,-44) = 1$, denn

$$\begin{aligned} 97 &= 2\cdot 44 + 9 \\ 44 &= 4\cdot 9 + 8 \\ 9 &= 1\cdot 8 + 1 \\ 8 &= 8\cdot 1 \end{aligned}$$

Wir bestimmen nun $x,y \in \mathbb{Z}$ mit $97x-44y=1$:

$$\begin{aligned} ggT(97,-44) = 1 = 9-8 &= 9-(44-4\cdot 9) = 5\cdot 9 - 44 = 5\cdot(97-2\cdot 44)-44 \\ &= 5\cdot 97 - 11\cdot 44 = 5\cdot 97 + 11\cdot(-44) \end{aligned}$$

Da $x=5, y=11$ ist eine Lösung. Wegen $(5+44t)\cdot 97 + (11+97t)\cdot(-44) = 1 \ \forall t \in \mathbb{Z}$ ist $x = 5+44t$, $y = 11+97t$ für jedes $t \in \mathbb{Z}$ eine Lösung.

Satz 7 Es seien $n_1,\dots,n_k \in \mathbb{Z}$, nicht alle $=0$ und $m \in \mathbb{Z}$. Dann sind äquivalent:

(i) m ist gemeinsamer Teiler von $n_1,\dots,n_k$,

(ii) $m \mid ggT(n_1,\dots,n_k)$.

Beweis: (i) $\Rightarrow$ (ii) Nach Korollar 6 gibt es $x_1,\dots,x_k \in \mathbb{Z}$ mit der Eigenschaft $n_1x_1+\dots+n_kx_k = ggT(n_1,\dots,n_k)$. Da m nach Voraussetzung gemeinsamer Teiler von $n_1,\dots,n_k$ ist, folgt $m \mid ggT(n_1,\dots,n_k)$ aus Satz 1 (x).
(ii) $\Rightarrow$ (i) Aus $m \mid ggT(n_1,\dots,n_k)$ und $ggT(n_1,\dots,n_k) \mid n_i$ folgt $m \mid n_i$ für $1 \le i \le k$ mit Hilfe von Satz 1 (vii).

Korollar 8 Es seien $n_1,\dots,n_k \in \mathbb{Z}$, nicht alle $=0$ und $d \in \mathbb{N}\setminus\{0\}$. Dann sind äquivalent:

(i) $d = ggT(n_1,\dots,n_k)$,

(ii) d ist ein gemeinsamer Teiler von $n_1,\dots,n_k$ und ist m ebenfalls ein gemeinsamer Teiler von $n_1,\dots,n_k$, so gilt $m \mid d$.

Beweis: (i) $\Rightarrow$ (ii) Ist $d = ggT(n_1,\dots,n_k)$, so ist d gemeinsamer Teiler von $n_1,\dots,n_k$. Ist m ebenfalls ein gemeinsamer Teiler von $n_1,\dots,n_k$, so gilt $m \mid d$ nach Satz 7.

(ii) $\Rightarrow$ (i) Nach Voraussetzung ist d ein gemeinsamer Teiler von $n_1,\dots,n_k$. Ist m ein positiver gemeinsamer Teiler von $n_1,\dots,n_k$, so gilt nach Voraussetzung $m \mid d$. Wegen Satz 1 (iv) folgt $m \leq d$.

Bemerkungen: 1) Man kann Satz 7 und Korollar 8 folgendermaßen interpretieren: Bezeichnet $T = T_{n_1} \cap \dots \cap T_{n_k}$ die Menge der positiven gemeinsamen Teiler von $n_1,\dots,n_k$, so sind äquivalent:

(i) $ggT(n_1,\dots,n_k)$ ist maximal in T bezüglich der üblichen Ordnungsrelation $\leq$,

(ii) $ggT(n_1,\dots,n_k)$ ist maximal in T bezüglich der Teilerrelation

2) Bedingung (ii) kann verwendet werden, um den Begriff des größten gemeinsamen Teilers auf Ringen zu definieren, auf denen es keine Ordnungsrelation $\leq$ gibt, die mit den Verknüpfungen $+$ und $\cdot$ verträglich ist, z.B. auf Polynomringen.

Satz 9 Es seien $n_1,\dots,n_k \in \mathbb{Z}$, nicht alle $= 0$. Dann ist

$$ggT(\ell n_1,\dots,\ell n_k) = |\ell|\, ggT(n_1,\dots,n_k) \quad \forall \ell \in \mathbb{Z}\setminus\{0\}.$$

Beweis: Es sei $d := ggT(n_1,\dots,n_k)$. Da $\ell \neq 0$, sind $\ell n_1,\dots,\ell n_k$ nicht alle $= 0$. Es sei $e := ggT(\ell n_1,\dots,\ell n_k)$. Zu zeigen ist also $e = |\ell| \cdot d$.

Da $d \mid n_i$ (für $1 \leq i \leq k$) folgt $(\ell d) \mid (\ell n_i)$ (für $1 \leq i \leq k$ und jedes $\ell \in \mathbb{Z}\setminus\{0\}$) wegen Satz 1 (viii). Also ist ℓd ein gemeinsamer Teiler von $\ell n_1,\dots,\ell n_k$. Aus Korollar 8 folgt $(\ell d) \mid e$.

Da $(\ell d) \mid e$ existiert ein $m \in \mathbb{Z}$, derart dass $e = \ell d m$ und daher $\frac{e}{\ell} = dm \in \mathbb{Z}$.

Aus $e \mid (\ell n_i)$ (für $1 \leq i \leq k$) folgt: $\forall i \in \{1,\dots,k\}\ \exists m_i \in \mathbb{Z} : \ell n_i = e m_i$. Daraus folgt $n_i = \frac{e}{\ell} m_i$ (für $1 \leq i \leq k$) und daher $\frac{e}{\ell} \mid n_i$ (für $1 \leq i \leq k$). Also ist $\frac{e}{\ell}$ ein gemeinsamer Teiler von $n_1,\dots,n_k$. Aus Korollar 8 folgt $\frac{e}{\ell} \mid d$. Daher existiert ein $m \in \mathbb{Z}$, derart dass $d = \frac{e}{\ell} m$ und somit $\ell d = em$. Offenbar gilt auch $e \mid (\ell d)$.

Da $(\ell d) \mid e$ und $e \mid (\ell d)$ gezeigt ist, folgt wegen Satz 1 (vi), dass

$$ggT(\ell n_1,\dots,\ell n_k) = e = |e| = |\ell d| = |\ell| \cdot |d| = |\ell| \cdot d = |\ell| \cdot ggT(n_1,\dots,n_k).$$

28.3.2022

Korollar 10 Sind $n_1,\dots,n_k \in \mathbb{Z}$, nicht alle $= 0$ und $d = ggT(n_1,\dots,n_k)$, so ist $ggT\left(\frac{n_1}{d},\dots,\frac{n_k}{d}\right) = 1$.

Beweis: Da $d \mid n_i$ (für $1 \le i \le k$), sind $\frac{n_1}{d}, \dots, \frac{n_k}{d} \in \mathbb{Z}$, nicht alle $= 0$ und

$$d = ggT(n_1, \dots, n_k) = ggT\left(d \cdot \frac{n_1}{d}, \dots, d \cdot \frac{n_k}{d}\right) \overset{\text{Satz 9}}{=} d \cdot ggT\left(\frac{n_1}{d}, \dots, \frac{n_k}{d}\right).$$

Da $d \neq 0$ folgt $ggT\left(\frac{n_1}{d}, \dots, \frac{n_k}{d}\right) = 1$.

Beispiele: 1) $ggT(40, 60, 100) = ggT(5 \cdot 8, 5 \cdot 12, 5 \cdot 20) = 5 \cdot ggT(8, 12, 20) = 5 \cdot 4 = 20$,

2) $ggT\left(\frac{40}{20}, \frac{60}{20}, \frac{100}{20}\right) = ggT(2, 3, 5) = 1$.

Satz 11 Es sei $k \ge 2$ und $n_1, \dots, n_k \in \mathbb{Z}$, wobei schon $n_1, \dots, n_{k-1}$ nicht alle $= 0$ sein sollen. Dann ist $ggT(n_1, \dots, n_k) = ggT(ggT(n_1, \dots, n_{k-1}), n_k)$.

Beweis: Es sei $d = ggT(n_1, \dots, n_k)$. Dann ist d ein gemeinsamer Teiler von $n_1, \dots, n_k$ und daher erst recht ein gemeinsamer Teiler von $n_1, \dots, n_{k-1}$. Aus Satz 7 folgt, dass $d \mid ggT(n_1, \dots, n_{k-1})$. Aus $d \mid ggT(n_1, \dots, n_{k-1})$ und $d \mid n_k$ folgt (wieder wegen Satz 7), dass $d \mid ggT(ggT(n_1, \dots, n_{k-1}), n_k)$. Da es gilt $ggT(n_1, \dots, n_k) \mid ggT(ggT(n_1, \dots, n_{k-1}), n_k)$.

Es sei $t = ggT(ggT(n_1, \dots, n_{k-1}), n_k)$. Dann gelten $t \mid ggT(n_1, \dots, n_{k-1})$ und $t \mid n_k$.

Aus $t \mid ggT(n_1, \dots, n_{k-1})$ folgt wegen Satz 7, dass t ein gemeinsamer Teiler von $n_1, \dots, n_{k-1}$ ist. Da auch $t \mid n_k$ gilt, ist t ein gemeinsamer Teiler von $n_1, \dots, n_k$. Daraus folgt (wieder wegen Satz 7), dass $t \mid ggT(n_1, \dots, n_k)$. Also gilt auch

$ggT(ggT(n_1, \dots, n_{k-1}), n_k) \mid ggT(n_1, \dots, n_k)$.

Aus Satz 7 (vi) folgt $ggT(ggT(n_1, \dots, n_{k-1}), n_k) = ggT(n_1, \dots, n_k)$.

Bemerkung: Satz 11 besagt, dass man $ggT(n_1, \dots, n_k)$ für $k > 2$ rekursiv berechnen kann, indem man zuerst $ggT(n_1, n_2)$ bestimmt (z.B. mit Hilfe des euklidischen Algorithmus), danach $ggT(ggT(n_1, n_2), n_3) = ggT(n_1, n_2, n_3)$ (wieder mit Hilfe des euklidischen Algorithmus) – usw.

Beispiel: Wir bestimmen $ggT(4990, 2994, 7485)$. Dazu bestimmen wir zuerst $ggT(4990, 2994)$ mit Hilfe des euklidischen Algorithmus:

$$\left.\begin{aligned} 4990 &= 1 \cdot 2994 + 1996 \\ 2994 &= 1 \cdot 1996 + 998 \\ 1996 &= 2 \cdot 998 \end{aligned}\right\} \Rightarrow ggT(4990, 2994) = 998$$

Im nächsten Schritt berechnen wir

$$ggT(4990, 2994, 7485) = ggT(ggT(4990, 2994), 7485) = ggT(998, 7485)$$

wieder mit Hilfe des euklidischen Algorithmus:

$$\left.\begin{aligned} 7485 &= 7 \cdot 998 + 499 \\ 998 &= 2 \cdot 499 \end{aligned}\right\} \Rightarrow ggT(998, 7485) = 499 \Rightarrow ggT(4990, 2994, 7485) = 499$$

Die Reihenfolge, in der man dabei vorgeht, ist (wegen Satz 3 (iii)) völlig unerheblich.
Man kann genauso gut zuerst $ggT(2994, 7485)$ bestimmen:

$$\left.\begin{aligned} 7485 &= 2 \cdot 2994 + 1497 \\ 2994 &= 2 \cdot 1497 \end{aligned}\right\} \Rightarrow ggT(2994, 7485) = 1497$$

$$\left.\begin{aligned} 4990 &= 3 \cdot 1497 + 499 \\ 1497 &= 3 \cdot 499 \end{aligned}\right\} \Rightarrow ggT(4990, 1497) = 499$$

$$\rightarrow ggT(4990, 2994, 7485) = ggT(4990, ggT(2994, 7485)) = ggT(4990, 1497) = 499$$

Bemerkung: Um $ggT(n_1, \dots, n_k)$ für $k > 2$ zu berechnen, kann man anstelle von Satz 11 auch die folgende Verallgemeinerung des euklidischen Algorithmus verwenden.
Wegen Satz 3 kann dabei o.B.d.A. vorausgesetzt werden, dass $n_i > 0$ ist für $1 \le i \le k$ und dass $n_1, \dots, n_k$ paarweise verschieden sind.
Wegen Satz 3 (ii) können wir o.B.d.A. voraussetzen, dass $n_1 = \min\{n_1, \dots, n_k\}$.
Für $2 \le i \le k$ führen wir nun Division mit Rest durch. Ist $n_i = q_i n_1 + r_i$ mit $0 \le r_i < n_1$ für $2 \le i \le k$, so ist $ggT(n_1, \dots, n_k) = ggT(n_1, r_2, \dots, r_k)$ wegen Satz 3 (v):

$$ggT(n_1, \dots, n_k) = ggT(n_1, \dots, n_{k-1}, n_k - q_k n_1) = ggT(n_1, \dots, n_{k-1}, r_k)$$

$$= ggT(n_1, \dots, n_{k-2}, n_{k-1} - q_{k-1} n_1, r_k) = ggT(n_1, \dots, n_{k-2}, r_{k-1}, r_k) = \dots \text{ usw.}$$

Beispiele: 1) Wir zeigen $ggT(721, 613, 114) = 1$ auf diese Weise:

$$ggT(721, 613, 114) = ggT(6 \cdot 114 + 37, 5 \cdot 114 + 43, 114) = ggT(37, 43, 114)$$

$$= ggT(37, 1 \cdot 37 + 6, 3 \cdot 37 + 3) = ggT(37, 6, 3) = ggT(12 \cdot 3 + 1, 2 \cdot 3 + 0, 3) = ggT(1, 0, 3) = 1$$

2) Wir überprüfen nochmals $ggT(4990, 2994, 7485) = 499$ auf diese Weise:

$$ggT(4990, 2994, 7485) = ggT(1 \cdot 2994 + 1996, 2994, 2 \cdot 2994 + 1497) = ggT(1996, 2994, 1497)$$

$$= ggT(1 \cdot 1497 + 499, 2 \cdot 1497 + 0, 1497) = ggT(499, 0, 1497) = ggT(499, 0, 3 \cdot 499) = 499$$

Satz 12 Es seien $m, n_1, n_2 \in \mathbb{Z}$ und $m \neq 0$. Aus $m \mid (n_1 \cdot n_2)$ und $ggT(m, n_1) = 1$ folgt $m \mid n_2$.

Beweis: Da $ggT(m, n_1) = 1$, gibt es (nach Korollar 6) $x, y \in \mathbb{Z}$, sodass $mx + n_1 y = 1$.

Es folgt sofort, dass $mn_2x + n_1n_2y = n_2$. Da $m \mid m$ und (nach Voraussetzung) $m \mid n_1n_2$ erhält man (wegen Satz 1 (x)), dass $m \mid (mn_2x + n_1n_2y)$, d.h. $m \mid n_2$.

Korollar 13 Es seien $m_1, m_2, n \in \mathbb{Z}$, $m_1, m_2 \neq 0$ und $ggT(m_1, m_2) = 1$. Aus $m_1 \mid n$ und $m_2 \mid n$ folgt $(m_1 \cdot m_2) \mid n$.

Beweis: Wir schreiben $m_2 \mid n$ um zu $m_2 \mid (m_1 \cdot \frac{n}{m_1})$. Da $ggT(m_1, m_2) = 1$ folgt wegen Satz 12, dass $m_2 \mid \frac{n}{m_1}$. D.h. es gibt ein $k \in \mathbb{Z}$, derart dass $\frac{n}{m_1} = km_2$ und daher $n = km_1m_2$. Also gilt $(m_1 \cdot m_2) \mid n$.

Bemerkung: Ohne die Voraussetzung $ggT(m_1, m_2) = 1$ ist Korollar 13 falsch. Es sei z.B. $m_1 = 4$, $m_2 = 6$ und $n = 12$. Es gelten $4 \mid 12$ und $6 \mid 12$ aber $(4 \cdot 6) \nmid 12$ (d.h. $24 \nmid 12$).

Definition: Es sei $k \geq 2$. Die Zahlen $n_1, \dots, n_k \in \mathbb{Z}$, nicht alle $= 0$, heißen relativ prim (oder teilerfremd) wenn $ggT(n_1, \dots, n_k) = 1$.

Definition: Es sei $k \geq 2$. Die Zahlen $n_1, \dots, n_k \in \mathbb{Z} \setminus \{0\}$ heißen paarweise relativ prim (oder paarweise teilerfremd) wenn $ggT(n_i, n_j) = 1$ für $1 \leq i, j \leq k$, $i \neq j$.

Lemma 14 Es sei $k \geq 2$. Sind $n_1, \dots, n_k \in \mathbb{Z} \setminus \{0\}$ paarweise relativ prim, so sind sie auch relativ prim. Die Umkehrung gilt nicht.

Beweis: Nach Voraussetzung ist $ggT(n_1, n_2) = 1$. D.h. der einzige positive gemeinsame Teiler von n_1 und n_2 ist 1. Daher ist 1 erst recht der einzige positive gemeinsame Teiler von $n_1, \dots, n_k$ und daher $ggT(n_1, \dots, n_k) = 1$.

Dass die Umkehrung nicht gilt, sieht man z.B. an folgendem Gegenbeispiel:

$ggT(6, 10, 15) = 1$, aber $ggT(6, 10) = 2$, $ggT(6, 15) = 3$ und $ggT(10, 15) = 5$

(denn $T_6 = \{1, 2, 3, 6\}$, $T_{10} = \{1, 2, 5, 10\}$ und $T_{15} = \{1, 3, 5, 15\}$, woraus $T_6 \cap T_{10} \cap T_{15} = \{1\}$ aber $T_6 \cap T_{10} = \{1, 2\}$, $T_6 \cap T_{15} = \{1, 3\}$ und $T_{10} \cap T_{15} = \{1, 5\}$ folgen).