1. Teiler, gemeinsame Teiler und größter gemeinsamer Teiler

Vorbemerkungen: 1) Wir setzen voraus, dass $(\mathbb{Z}, +, \cdot)$ ein Integritätsbereich ist, d.h. ein nullteilerfreier, kommutativer Ring mit Einselement. (D.h. man kann so rechnen, „wie wir es gewohnt sind.") Nullteilerfreiheit bedeutet, dass für $a, b \in \mathbb{Z}$ gilt, dass

$$a \cdot b = 0 \Rightarrow a = 0 \text{ oder } b = 0.$$

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

$$ax = bx \Rightarrow (a-b)x = ax - bx = 0 \overset{x \neq 0}{\Longrightarrow} a - b = 0 \Rightarrow a = b$$

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.

4) Wir verwenden die Notationen $\mathbb{N} = \{0, 1, 2, 3, \dots\}$ (wie in der Schule üblich) und $\mathbb{N}^+ = \{1, 2, 3, \dots\}$.

Definition: Es seien $m, n \in \mathbb{Z}$. Man sagt „m teilt n" wenn $\exists\, d \in \mathbb{Z} : n = md$. 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.

Bemerkung: Beachten Sie, dass diese Definition von der in der Schule üblichen abweicht. Zunächst sind $m, n \in \mathbb{Z}$ (und nicht nur $m, n \in \mathbb{N}^+$). In der Schule wird definiert, dass die Zahl m ($\in \mathbb{N}^+$) die Zahl n ($\in \mathbb{N}^+$) teilt, wenn die Division von n durch m den Rest 0 liefert („Zahlen, die eine gegebene Zahl ohne Rest teilen, heißen Teiler dieser Zahl"). Bei uns gilt (überraschend) $0 \mid 0$, da $0 = 0 \cdot 1$. (Für $m, n \in \mathbb{N}^+$ sind unsere Definition und die aus dem Schulbuch aber äquivalent.)

Satz 1 (Rechenregeln für Teilbarkeit) Alle auftretenden Größen sind aus $\mathbb{Z}$.

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

(ii) $\forall n \in \mathbb{Z} : n \mid 0$. Aus $0 \mid n$ folgt $n = 0$ (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) $n \mid 1 \Leftrightarrow n \in \{1, -1\}$ (die Teiler von 1 sind 1 und -1),

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

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

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

(ix) $(km) \mid (kn)$ und $k \neq 0 \Rightarrow m \mid n$,

(x) $m \mid n_1, \dots, m \mid n_k \Rightarrow m \mid (k_1 n_1 + \dots + k_k n_k) \quad \forall k_1, \dots, k_k \in \mathbb{Z}$ (oder $m \mid \sum_{i=1}^{k} k_i n_i \quad \forall k_1, \dots, k_k \in \mathbb{Z}$),

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

Beweis: (i) Folgt aus $n = 1 \cdot n \ \forall n \in \mathbb{Z}$.

(ii) Die erste Behauptung folgt aus $0 = 0 \cdot n \ \forall n \in \mathbb{Z}$. Wenn $0 \mid n$, so $\exists\, d \in \mathbb{Z} : n = 0 \cdot d = 0$

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

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

(v) $n \mid 1 \overset{\text{(iv)}}{\Longrightarrow} |n| \leq 1 \Rightarrow n \in \{-1, 0, 1\}$. Da $0 \nmid 1$ folgt $n \in \{1, -1\}$. Umgekehrt gilt $(\pm 1)^2 = 1 \Rightarrow \pm 1 \mid 1$.

(vi) Gilt $m \mid n$ und $n \mid m$, so folgt (wegen (iii)) $m = 0 \Leftrightarrow n = 0$ und daher $|m| = |n| = 0$.
Da daher auch $m \neq 0 \Leftrightarrow n \neq 0$ gilt, ist als zweite Möglichkeit nun $m, n \in \mathbb{Z} \setminus \{0\}$ möglich.
Wegen (iv) gilt dann $|m| \leq |n|$ und $|n| \leq |m|$ und daher $|m| = |n|$

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

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

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

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

$\Rightarrow n_1 \cdots n_k = (m_1 d_1) \cdots (m_k d_k) = (m_1 \cdots m_k)(d_1 \cdots d_k) \Rightarrow (m_1 \cdots m_k) \mid (n_1 \cdots n_k)$.

Beispiele: 1) $12 \mid 48$ (da $48 = 4 \cdot 12$) $\Rightarrow (-12) \mid 48$, $12 \mid (-48)$ und $(-12) \mid (-48)$ (siehe (iii))

2) $7 \mid 21$ (da $21 = 3 \cdot 7$) und $21 \mid 84$ (da $84 = 4 \cdot 21$) $\Rightarrow 7 \mid 84$ (siehe (viii))

3) $(-15) \mid 45$ (da $45 = (-15)(-3)$) $\Rightarrow 30 \mid (-90)$ (siehe (vii) mit $\ell = -2$)

4) $40 \mid 200$ (da $200 = 5 \cdot 40$) $\Rightarrow 8 \mid 40$ (siehe (ix) mit $\ell = 5$)

5) $7 \mid 14$ (da $14 = 2 \cdot 7$) und $7 \mid 35$ (da $35 = 5 \cdot 7$) $\Rightarrow 7 \mid (2 \cdot 35 - 14)$, also $7 \mid 56$ (siehe (x) mit $\ell_1 = 2$, $\ell_2 = -1$)

6) $3 \mid 12$ (da $12 = 4 \cdot 3$) und $2 \mid 10$ (da $10 = 2 \cdot 5$) folgt $3 \cdot 2 \mid 12 \cdot 10$, also $6 \mid 120$ (siehe (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 $-|n| \leq d \leq |n|$.
Jedes $n \in \mathbb{Z} \setminus \{0\}$ besitzt daher nur endlich viele Teiler.

3) Ist $n \in \mathbb{Z}$, so besitzen n und $-n$ (wegen Satz 1 (iii)) genau die selben Teiler (also $d \mid n \Leftrightarrow d \mid (-n)$)
Z.B. sind die Menge der Teiler von 12 und die Menge der Teiler von -12 beide gleich $\{\pm 1, \pm 2, \pm 3, \pm 4, \pm 6, \pm 12\}$.

4) Ist $n \in \mathbb{N}^+$ und man hat alle Teiler d von n mit $1 \leq d \leq \sqrt{n}$ gefunden, so sind die restlichen positiven Teiler von n genau die dazu gehörigen Komplementärteiler.

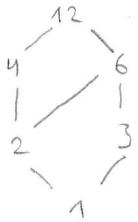
Gilt nämlich $d|n$ und $d > \sqrt{n}$, so gilt für den Komplementärteiler $\frac{n}{d}$ von n zu d, dass $\frac{n}{d} < \frac{n}{\sqrt{n}} = \sqrt{n}$. Ist z.B. $n = 60$, so sind die positiven Teiler d von 60 mit $d < \sqrt{60} = 7{,}74\ldots$ gerade $1,2,3,4,5,6$ und die restlichen positiven Teiler von 60 daher $60, 30, 20, 15, 12, 10$.

3.3.2025

5) Aus Satz 1 folgt, dass die Teilerrelation auf $\mathbb{N}^+$ eine Ordnungsrelation ist, denn:

- $\forall n \in \mathbb{N}^+ : n|n$ (wegen Satz 1(i)), d.h. die Teilerrelation ist reflexiv,
- Sind $m, n \in \mathbb{N}^+$, $m|n$ und $n|m$, so folgt (wegen Satz 1 (vii)) $|m| = |n|$, d.h. $m = n$, d.h. die Teilerrelation ist antisymmetrisch,
- Für $l, m, n \in \mathbb{N}^+$ gilt: $l|m$ und $m|n \Rightarrow l|n$ (wegen Satz 1(viii)), d.h. die Teilerrelation ist transitiv

Die Teilerrelation auf $\mathbb{N}^+$ ist aber keine Totalordnung, da z.B. $2 \nmid 3$ und $3 \nmid 2$. Für die positiven Teiler von 12 (d.h. $1,2,3,4,6,12$) kann man die Teilerordnung z.B. graphisch folgendermaßen darstellen:



Dabei steht eine (niedriger gelegene) Zahl eine (höher gelegene) Zahl, wenn sie mit ihr durch Striche verbunden ist (direkt oder über eine oder mehrere andere Zahlen).

Satz 2 (Division mit Rest) Es sei $m \in \mathbb{Z}$ und $n \in \mathbb{N}^+$. 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 daher $0 \leq m - qn < n$ folgt. Setzt man $r := m - qn$, so sind $m = qn + r$ und $0 \leq r < n$ erfüllt.

Eindeutigkeit: Angenommen, $m = qn + r = \bar{q}n + \bar{r}$, $0 \leq r, \bar{r} < n$ 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 $n_1, \ldots, n_k \in \mathbb{Z}$ (nicht notwendig verschieden), so heißt $m \in \mathbb{Z}$ gemeinsamer Teiler von $n_1, \ldots, n_k$ wenn $m|n_1, \ldots, m|n_k$.

Notation: Für $n \in \mathbb{Z}$ schreiben wir T_n für die Menge der positiven Teiler von n, d.h. $T_n = \{m \in \mathbb{N}^+ \mid m|n\}$.

Beispiele: 1) Die Menge der positiven gemeinsamen Teiler von 8 und 12 ist $\{1,2,4\}$, denn $T_8 = \{1,2,4,8\}$ und $T_{12} = \{1,2,3,4,6,12\} \Rightarrow T_8 \cap T_{12} = \{1,2,4\}$

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 $T_{75} = \{1,3,5,15,25,75\}$

$\Rightarrow T_{30} \cap T_{45} \cap T_{75} = \{1,3,5,15\}$

Bemerkungen: 1) Zahlen $n_1,\dots,n_k \in \mathbb{Z}$ besitzen stets einen positiven gemeinsamen Teiler, nämlich 1 (siehe Satz 1(i)), also $T_{n_1} \cap \dots \cap T_{n_k} \neq \emptyset$

2) Wegen Satz 1(ii) ist $T_0 = \mathbb{N}^+$. Ist also $n_1 = \dots = n_k = 0$, so ist $T_{n_1} = \dots = T_{n_k} = \mathbb{N}^+$ und daher $T_{n_1} \cap \dots \cap T_{n_k} = \mathbb{N}^+$, da jede positive ganze Zahl ist gemeinsamer Teiler und es gibt keinen größten gemeinsamen Teiler.

3) Sind hingegen $n_1,\dots,n_k \in \mathbb{Z}$ nicht alle $= 0$, so existiert ein $i \in \{1,\dots,k\}$: $n_i \neq 0$. Wegen Bemerkung 2 auf Seite 2 ist T_{n_i} endlich. Daher ist auch $T_{n_1} \cap \dots \cap T_{n_k}$ ($\subseteq T_{n_i}$) endlich und damit noch eben bestimmbar (z.B. durch $\min\{|n_i| \mid 1 \le i \le k, n_i \neq 0\}$).

Es ist daher sinnvoll zu definieren:

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

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

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 überblickbar sind.

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

(i) $ggT(n_1,\dots,n_k) = ggT(|n_1|,\dots,|n_k|)$,
da man kaum 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 $ggT(n_{i_1},\dots,n_{i_k}) = ggT(n_1,\dots,n_k)$,
da der ggT hängt nicht von der Reihenfolge der Zahlen $n_1,\dots,n_k$ ab,

(iii) Ist $k \ge 2$ und $n_k = 0$, so ist $ggT(n_1,\dots,n_k) = ggT(n_1,\dots,n_{k-1})$
da bei der Bestimmung von $ggT(n_1,\dots,n_k)$ können alle $n_i = 0$ weggelassen werden,

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

da bei der Bestimmung von $ggT(n_1,\dots,n_k)$ können alle n_i, die mehr als einmal auftreten, beim zweiten, dritten, ... Auftreten weggelassen werden,

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

Beweis: (i) Wegen Satz 1(iii) gilt $d|n \Leftrightarrow d|{-n}$. Daher gilt für $d \in \mathbb{N}^+$, dass $d|n_1,\dots,d|n_k \Leftrightarrow d|{|n_1|},\dots,d|{|n_k|}$. Also ist $T_n = T_{|n|}$ und daher $T_{n_1} \cap \dots \cap T_{n_k} = T_{|n_1|} \cap \dots \cap T_{|n_k|}$

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

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

- Bei (ii) gilt $d \mid n_{i_1}, \dots, d \mid n_{i_k} \iff d \mid n_1, \dots, d \mid n_k$
- Bei (iii) und (iv) ist $d \mid n_1, \dots, d \mid n_k \iff d \mid n_1, \dots, d \mid n_{k-1}$
- Äquivalenz bei (v) folgt aus Satz 1 (x)

$$d \mid n_1, \dots, d \mid n_k \implies d \mid \left(n_k + \sum_{i=1}^{k-1} x_i n_i\right) \quad \forall x_1, \dots, x_{k-1} \in \mathbb{Z} \text{ und umgekehrt}$$

$$d \mid n_1, \dots, d \mid n_{k-1}, d \mid \left(n_k + \sum_{i=1}^{k-1} x_i n_i\right) \implies d \mid \left(\left(n_k + \sum_{i=1}^{k-1} x_i n_i\right) - \sum_{i=1}^{k-1} x_i n_i\right), \text{ also } d \mid n_k$$

Bemerkungen: 1) Satz 3 (ii) kann auch folgendermaßen formuliert werden: 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 unmittelbar einsichtig)

Beispiele: 1) $ggT(-8,-12) = ggT(-8,12) = ggT(8,-12) \overset{\text{Satz 3 (i)}}{=} ggT(8,12) = 4$

2) $ggT(30,45,75) = ggT(45,30,75) = ggT(30,75,45) = \dots \overset{\text{Satz 3 (ii)}}{=} 15$

3) $ggT(8,12,0) = ggT(8,0,12) = ggT(0,8,12) \overset{\text{Satz 3 (iii)}}{=} ggT(8,12) = 4$

4) $ggT(8,8,12) = ggT(8,12,8) = ggT(12,8,8) = ggT(8,12,12) = \dots \overset{\text{Satz 3 (iv)}}{=} ggT(8,12) = 4$

Satz 4 (Euklidischer Algorithmus) Gegeben seien $a, b \in \mathbb{N}^+$, wobei o.BdA $b \le a$ gelten soll. Gesucht ist $ggT(a,b)$. Führe wiederholt Division mit Rest durch:

$$a = b q_0 + r_1, \quad 0 \le r_1 < b$$
$$b = r_1 q_1 + r_2, \quad 0 \le r_2 < r_1$$
$$r_1 = r_2 q_2 + r_3, \quad 0 \le r_3 < r_2$$
$$\vdots$$
$$r_{n-1} = r_n q_n + r_{n+1}, \quad 0 \le r_{n+1} < r_n$$

Setze zusätzlich $r_0 := b$. Wegen $b = r_0 > r_1 > r_2 > r_3 > \dots > r_{n-1} > r_n > r_{n+1} > \dots \ge 0$ gibt es ein kleinstes $n \ge 0$ mit $r_{n+1} = 0$. Dann ist $r_n = ggT(a,b)$.

10.3.2025

Beweis: Wir zeigen zunächst, dass r_n ein gemeinsamer Teiler von a und b ist.
Aus $r_{n-1} = r_n q_n$ folgt $r_n \mid r_{n-1}$. Wegen $r_{n-2} = r_{n-1} q_{n-1} + r_n$ und Satz 1 (x) folgt $r_n \mid r_{n-2}$.
Verfahre weiter so: Ist $r_n \mid r_{n+1}$ und $r_n \mid r_m$ bereits gezeigt, so folgt $r_n \mid r_{m-1}$ wegen $r_{m-1} = r_m q_m + r_{m-1}$ und Satz 1 (x). Hat man $r_n \mid r_2$ und $r_n \mid r_1$ gezeigt, so folgt $r_n \mid b$ wegen $b = r_1 q_1 + r_2$ und Satz 1 (x). Schließlich erhält man $r_n \mid a$ aus $a = b q_0 + r_1$ und Satz 1 (x)

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

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

2) Der Grund für die Festlegung $r_0 = b$ ist folgender: Wenn $b \mid a$, so ist $a = bq_0 + r_1$ mit $r_1 = 0$ und $r_0 = ggT(a,b) = b$. Bei der euklidische Algorithmus liefert auch in diesem Fall das richtige Ergebnis.

3) Wegen Satz 3(i) ist die Voraussetzung $a, b > 0$ 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) Bestimme $ggT(111, 39) = 3$:

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

oder

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

2) Bestimme $ggT(9973, 2137) = 1$:

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

oder

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

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

Wir setzen zunächst $x_i = n_i$ für $1 \leq i \leq k$. Da $n_1, \dots, n_k$ nicht alle $= 0$ sind, gibt es ein $j \in \{1, \dots, k\}$, sodass $n_j \neq 0$ und daher $\sum_{i=1}^{k} x_i n_i = \sum_{i=1}^{k} n_i^2 \geq n_j^2 > 0$. Also ist $L \neq \emptyset$.

Da L nach unten beschränkt ist (z.B. durch 0) existiert $d' := \min L$. Weiters sei $d := ggT(n_1, \dots, n_k)$. Wir zeigen $d = d'$.

Wir zeigen zunächst $d \le d'$. Da $d' \in L$ ist, gibt es $y_1, \dots, y_k \in \mathbb{Z}$, sodass $d' = \sum_{i=1}^{k} y_i n_i$. Aus $d \mid n_i$ für $1 \le i \le k$ folgt mittels 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:

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

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 $1 \le j \le k$)

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

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 $x_1, \dots, x_k \in \mathbb{Z}$, sodass $x_1 n_1 + \dots + x_k n_k = ggT(n_1, \dots, n_k)$.

Beweis: 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 $x, y \in \mathbb{Z}$, sodass $xa + yb = ggT(a, b)$.

2) Die $x_1, \dots, x_k \in \mathbb{Z}$ mit der Eigenschaft $\sum_{i=1}^{k} x_i n_i = ggT(n_1, \dots, n_k)$ sind nicht eindeutig bestimmt, wie man schon für $k = 2$ erkennen kann: Sind $a, b \in \mathbb{Z}$, nicht beide $= 0$, $d = ggT(a, b)$ und $x, y \in \mathbb{Z}$, sodass $ax + by = ggT(a, b)$, 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 unendlich viele Paare mit dieser Eigenschaft.

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 rechnet“:

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 $x, y \in \mathbb{Z}$ mit $97x - 44y = 1$.

$$ggT(97,-44) = 1 = 9 - 8 = 9 - (44 - 4\cdot 9) = 5\cdot 9 - 44 = 5(97 - 2\cdot 44) - 44$$
$$= 5\cdot 97 - 11\cdot 44 = 5\cdot 97 + 11\cdot(-44)$$

Also $x = 5$, $y = 11$ ist eine Lösung. Wegen $(5+44t)\cdot 97 + (11+97t)\cdot(-44) = 1 \quad \forall t \in \mathbb{Z}$ 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 $x_1, \dots, x_k \in \mathbb{Z}$, sodass $n_1x_1 + \dots + n_kx_k = ggT(n_1, \dots, n_k)$. Da m nach Voraussetzung gemeinsamer Teiler von $n_1, \dots, n_k$ ist, folgt $m \mid ggT(n_1, \dots, n_k)$ wegen 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 $1 \le i \le k$ mittels Satz 1(vii).

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

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

(ii) d ist gemeinsamer Teiler von $n_1, \dots, n_k$ und ist m ebenfalls 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 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 $m \mid d$ und daher $m \le d$ wegen Satz 1(iv).

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 $\le$,

(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 $\le$ gibt, die mit den Verknüpfungen $+$ und $\cdot$ verträglich ist, z. B. Polynomringen.

17.3.2025

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 $d|n_i$ (für $1\le i\le k$) folgt $(\ell d)|(\ell n_i)$ (für $1\le i\le k$ und $\ell \in \mathbb{Z}\setminus\{0\}$) wegen Satz 1(viii).
Also ist ℓd gemeinsamer Teiler von $\ell n_1,\dots,\ell n_k$ und daher $(\ell d)|e$ wegen Satz 7.
Da $(\ell d)|e$, existiert ein $m\in\mathbb{Z}$, derart dass $e = \ell d m$ und daher $\frac{e}{\ell} = dm \in \mathbb{Z}$
Aus $e|(\ell n_i)$ (für $1\le i\le k$) folgt: $\forall i\in\{1,\dots,k\}\ \exists n_i \in \mathbb{Z}: \ell n_i = e m_i$. Daraus folgt
$n_i = \frac{e}{\ell} m_i$ und daher $\frac{e}{\ell} | n_i$ (für $1\le i\le k$). Also ist $\frac{e}{\ell}$ gemeinsamer Teiler von $n_1,\dots,n_k$.
Aus Satz 7 folgt $\frac{e}{\ell}|d$. Da es existiert ein $m\in\mathbb{Z}$, sodass $d = \frac{e}{\ell} m$ und somit
$\ell d = em$. Also gilt auch $e|(\ell d)$
Da sowohl $(\ell d)|e$ als auch $e|(\ell d)$ gezeigt wurden, folgt mittels Satz 1(vi)

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

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

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

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

Beweis: Es sei $d = ggT(n_1,\dots,n_k)$. Dann ist d gemeinsamer Teiler von $n_1,\dots,n_k$ und daher erst recht gemeinsamer Teiler von $n_1,\dots,n_{k-1}$. Aus Satz 7 folgt $d | ggT(n_1,\dots,n_{k-1})$.
Aus $d | ggT(n_1,\dots,n_{k-1})$ und $d|n_k$ folgt (wieder wegen Satz 7), dass
$d | ggT\left(ggT(n_1,\dots,n_{k-1}), n_k\right)$, d.h. $ggT(n_1,\dots,n_k) \mid ggT\left(ggT(n_1,\dots,n_{k-1}), n_k\right)$.
Es sei $t = ggT\left(ggT(n_1,\dots,n_{k-1}), n_k\right)$. Dann gelten $t | ggT(n_1,\dots,n_k)$ und $t|n_k$.
Aus $t | ggT(n_1,\dots,n_{k-1})$ folgt wegen Satz 7, dass t ein gemeinsamer Teiler von $n_1,\dots,n_{k-1}$ ist. Da auch $t|n_k$ 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 1 (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 finden 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 man dabei o.B.d.A. voraussetzen, dass $n_i>0$ für $1\le i\le k$ und dass $n_1,\dots,n_k$ paarweise verschieden sind.

Wegen Satz 3 (ii) kann man weiters o.B.d.A. voraussetzen, dass $n_1 = \min\{n_1,\dots,n_k\}$. Für $2\le i\le k$ führe 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 wegen Satz 3 (v)

$$ggT(n_1,n_2,\dots,n_k) = ggT(n_1,q_2n_1+r_2,\dots,q_kn_1+r_k) = ggT(n_1,r_2,\dots,r_k).$$

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 $ggT(4990, 2994, 7485) = 499$ 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 $ggT(m, n_1) = 1$ gilt es (nach Korollar 6) $x, y \in \mathbb{Z}$, sodass $mx + n_1 y = 1$. Daraus folgt $mn_2 x + n_1 n_2 y = n_2$. Da $m \mid m$ und $m \mid (n_1 n_2)$ nach Voraussetzung erhält man mit Hilfe von Satz 1 (x) $m \mid (mn_2 x + n_1 n_2 y)$, also $m \mid n_2$

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 dann $(m_1 \cdot m_2) \mid n$.

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 $m_2 \mid \frac{n}{m_1}$. Da $\exists k \in \mathbb{Z} : \frac{n}{m_1} = km_2$ und daher $n = km_1 m_2$. Also gilt $(m_1 m_2) \mid n$.

Bemerkung: Ohne die Voraussetzung $ggT(m_1, m_2) = 1$ ist Korollar 13 falsch. Sei z. B. $m_1 = 4$, $m_2 = 6$ und $n = 12$, so gilt $4 \mid 12$ und $6 \mid 12$ aber $(4 \cdot 6) \nmid 12$ (da $24 \nmid 12$).

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 $ggT(n_1, n_2) = 1$. Da 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 $ggT(n_1, \dots, n_k) = 1$.

Ein Gegenbeispiel für die Umkehrung ist z. B. $ggT(6, 10, 15) = 1$, aber $ggT(6, 10) = 2$, $ggT(6, 15) = 3$ und $ggT(10, 15) = 5$.