2. Primzahlen und kleinstes gemeinsames Vielfaches

Definition: Es sei $p \in \mathbb{Z}$, $p > 1$. Wenn p nur die Teiler $1, -1, p$ und $-p$ besitzt, wird p Primzahl genannt.

4.4.2022

Bemerkungen: 1) Die „schulische Definition" eine Zahl sei Primzahl, wenn sie „nur durch 1 und sich selbst teilbar ist", erhält man, wenn man nur positive Teiler betrachtet (und stillschweigend voraussetzt, dass die betrachtete Zahl $\neq 1$ ist).

2) Beachte, dass 1 keine Primzahl ist.

Lemma 15 Es sei p eine Primzahl und $n \in \mathbb{Z}$. Dann sind äquivalent:

(i) $ggT(p,n) = 1$,

(ii) $p \nmid n$.

Beweis: (i) $\Rightarrow$ (ii) Aus $p \mid n$ folgt $ggT(p,n) = p > 1$.

(ii) $\Rightarrow$ (i) Ist $ggT(p,n) > 1$, so gibt es ein $d \in \mathbb{N}$, $d > 1$ mit der Eigenschaft, dass $d \mid p$ und $d \mid n$. Nun ist p die einzige Zahl > 1, die p teilt. Also ist $d = p$ und $p \mid n$.

Satz 16 Es sei $p \in \mathbb{Z}$, $p > 1$. Dann sind äquivalent:

(i) p ist eine Primzahl,

(ii) Für $\alpha, \beta \in \mathbb{Z}$ gilt, dass $p \mid (\alpha\beta) \Rightarrow p \mid \alpha$ oder $p \mid \beta$ (dh p ist prim),

(iii) Ist $p = xy$ für gewisse $x, y \in \mathbb{Z}$, so ist $x \in \{1, -1\}$ oder $y \in \{1, -1\}$ (dh p ist irreduzibel).

Beweis: (i) $\Rightarrow$ (ii) Ist $p \mid \alpha$, so ist die Behauptung erfüllt.
Falls $p \nmid \alpha$, so folgt $ggT(p, \alpha) = 1$ aus Lemma 15. Aus Satz 12 folgt daher $p \mid \beta$.

(ii) $\Rightarrow$ (iii) Gilt $p = xy$, so gilt erst recht $p \mid (xy)$. Nach Voraussetzung folgt daraus $p \mid x$ oder $p \mid y$.
Angenommen, es gilt $p \mid x$. Da $p = xy$, gilt auch $x \mid p$ und daher $p = |x|$ (nach Satz 1 (vi)). Aus $p = xy$ folgt nun $p = |p| = |xy| = |x| \cdot |y| = p \cdot |y|$ und daher $|y| = 1$ und somit $y \in \{1, -1\}$.
Gilt $p \mid y$ (statt $p \mid x$), so zeigt man völlig analog $x \in \{1, -1\}$.

(iii) $\Rightarrow$ (i) Angenommen $m \mid p$ (für ein $m \in \mathbb{Z}$). Dann gibt es ein $n \in \mathbb{Z}$, sodass $p = mn$. Nach Voraussetzung ist dann $m \in \{1, -1\}$ oder $n \in \{1, -1\}$ (woraus $m \in \{p, -p\}$ folgt).
Insgesamt ist $m \in \{1, -1, p, -p\}$ und p daher eine Primzahl.

Bemerkungen: 1) Auch Eigenschaft (ii) von Primzahlen findet man bereits in den Elementen des Euklid (Buch VII, Prop. 30).

2) Beachte, dass Eigenschaften (ii) und (iii) aus Satz 16 auch von jedem $-p$ (mit p Primzahl) erfüllt werden. Man muss darum $p>1$ voraussetzen, um zu verhindern, dass $-2,-3,-5,-7,\dots$ ebenfalls als Primzahlen gelten.

3) Die Aussagen „p ist Primzahl" und „p ist prim" werden oft für bedeutungsgleich gehalten, sind es (im Sinn der Ringtheorie) aber nicht. Tatsächlich gilt die folgende Variante von Satz 16 (die die Zahlen $\{\pm 2, \pm 3, \pm 5, \pm 7, \pm 11, \dots\}$ beschreibt):

Satz 16' Es sei $p \in \mathbb{Z}$, $|p|>1$. Dann sind äquivalent:

(i) $|p|$ ist eine Primzahl,

(ii) p ist prim (d.h. $p \mid ab \Rightarrow p \mid a \vee p \mid b$),

(iii) p ist irreduzibel (d.h. $p = xy \Rightarrow x \in \{1,-1\} \vee y \in \{1,-1\}$).

4) Eigenschaften (ii) und (iii) aus Satz 16 eignen sich zur Verallgemeinerung auf kommutative Ringe mit Einselement, sind dort aber nicht immer äquivalent. Bezeichnet z.B. $\mathbb{R}[x]$ den Ring der Polynome mit reellen Koeffizienten (mit der üblichen Addition und Multiplikation von Polynomen), so gilt dort die folgende Variante von Satz 16:

Satz 16'' Es sei $f \in \mathbb{R}[x]$, $\operatorname{grad} f \geq 1$ (oder äquivalent: $f \notin \mathbb{R}$, d.h. f ist kein konstantes Polynom). Dann sind äquivalent:

(i) f ist prim (d.h. für $g, h \in \mathbb{R}[x]$ gilt $f \mid (gh) \Rightarrow f \mid g$ oder $f \mid h$),

(ii) f ist irreduzibel (d.h. ist $f = gh$ für gewisse $g, h \in \mathbb{R}[x]$, so ist $g \in \mathbb{R} \setminus \{0\}$ oder $h \in \mathbb{R} \setminus \{0\}$ (d.h. g ist ein konstantes Polynom $\neq 0$ oder h ist ein konstantes Polynom $\neq 0$).

Aus historischen Gründen (und weil Eigenschaften (i) und (ii) äquivalent sind), nennt man f, die die Bedingungen (i) und (ii) erfüllen, irreduzible Polynome.

Korollar 17 Es sei p eine Primzahl und $a_1, \dots, a_n \in \mathbb{Z}$. Aus $p \mid (a_1 \cdots a_n)$ folgt, dass p (mindestens) einen der Faktoren $a_1, \dots, a_n$ teilt, d.h. $p \mid a_i$ für ein $i \in \{1, \dots, n\}$.

Beweis: Induktion nach n.

Im Fall $n=1$ ist nichts zu beweisen, da $p \mid a_1$ vorausgesetzt wird.

Der Fall $n=2$ wurde in Satz 16 bewiesen.

Es sei nun $n \geq 2$ und es gelte $p \mid (a_1 \cdots a_{n+1})$. Das kann man umschreiben zu $p \mid ((a_1 \cdots a_n) a_{n+1})$. Aus dem Fall $n=2$ folgt nun, dass $p \mid (a_1 \cdots a_n)$ oder $p \mid a_{n+1}$.

Falls $p \mid (a_1 \cdots a_n)$, so folgt aus der Induktionsvoraussetzung, dass $p \mid a_i$ für ein $i \in \{1, \ldots, n\}$. Gilt $p \mid a_{n+1}$, so ist die Behauptung ebenfalls bewiesen.

Lemma 18 Es sei $n \in \mathbb{Z}$ und $|n| \geq 2$. Dann gibt es eine Primzahl p mit der Eigenschaft $p \mid n$. (D.h. jede Zahl $n \in \mathbb{Z} \setminus \{-1, 0, 1\}$ wird von einer Primzahl geteilt.)

Beweis: Wir betrachten die Menge $T = \{m \in \mathbb{Z} \mid m > 1, m \mid n\}$. Die Menge T ist nicht leer (da $|n| \in T$) und durch 1 noch unten beschränkt. Daher gibt es $p := \min T$. (D.h. wir geben dem kleinsten Teiler von n, der größer als 1 ist, den Namen p.)

Wir behaupten nun, dass p eine Primzahl ist.

Nach Voraussetzung gelten $p \in \mathbb{Z}$ und $p > 1$. Wäre p keine Primzahl, so würde p einen Teiler d mit der Eigenschaft $1 < d < p$ besitzen. Aus $d \mid p$ und $p \mid n$ folgt (wegen Satz 1 (vii)) aber $d \mid n$. D.h. es wäre $d \in T$ und $d < p$. Das ist ein Widerspruch zur Minimalität von p.

Satz 19 Es gibt unendlich viele Primzahlen.

Beweis: Wir zeigen mit Induktion nach k ($\in \mathbb{N} \setminus \{0\}$), dass es k Primzahlen gibt.

$k=1$: 2 ist Primzahl (Aus $d \mid 2$ folgt $|d| \leq 2$ wegen Satz 1 (iv). Also muss $d \in \{-2, -1, 0, 1, 2\}$ gelten. Da $0 \nmid 2$ hat man mit $\pm 1, \pm 2$ bereits alle Teiler von 2 gefunden und 2 ist Primzahl.)

Angenommen, es wurden schon k Primzahlen $p_1, \ldots, p_k$ gefunden. Wir betrachten die Zahl $p_1 \cdots p_k + 1$. Da offenbar $p_1 \cdots p_k + 1 \geq 2$ ist, gibt es nach Lemma 18 eine Primzahl p mit der Eigenschaft $p \mid (p_1 \cdots p_k + 1)$. Nun kann p aber keine der Primzahlen $p_1, \ldots, p_k$ sein. Wäre nämlich $p \in \{p_1, \ldots, p_k\}$, so würde offensichtlich $p \mid (p_1 \cdots p_k)$ gelten und daher (wegen Satz 1 (x)) auch $p \mid ((p_1 \cdots p_k + 1) - p_1 \cdots p_k)$, d.h. $p \mid 1$. Das ist aber unmöglich (wegen Satz 1 (iv)), da nach Definition $p > 1$ ist.

Bemerkungen: 1) Auch den Beweis von Satz 19 findet man im Wesentlichen bereits in den Elementen des Euklid (Buch IX, Prop. 20).

2) Da es unendlich viele Primzahlen gibt, gibt es keine größte Primzahl. Die immer wiederkehrende Zeitungsschlagzeile „Größte Primzahl gefunden" besagt uns, dass eine Primzahl gefunden wurde, die größer als alle bisher bekannten Primzahlen ist (und dabei die derzeit größte bekannte Primzahl ist).

3) Eine Stelle im Beweis von Satz 19 wird oft missverstanden. Darin wird nicht bewiesen, dass $p_1 \cdots p_k + 1$ eine Primzahl ist! Tatsächlich ist das im allgemeinen falsch, wie das Beispiel $2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 + 1 = 30\,031 = 59 \cdot 509$ zeigt. (Da wählt man $p_1 = 2$, $p_2 = 3$, $p_3 = 5$, $p_4 = 7$, $p_5 = 11$, $p_6 = 13$, so liefert der Beweis entweder $p = 59$ oder $p = 509$.)

4) Dieser Beweis von Satz 19 wird meistens indirekt formuliert. Unsere Formulierung hat den Vorteil, dass man daraus relativ einfach die folgende Tatsache ableiten kann: Bezeichnet p_n die n-te Primzahl, so ist $p_n \leq 2^{2^{n-1}}$. (Das ist eine sehr schwache Abschätzung. Tatsächlich gilt $p_n \leq C\, n \log n$ für eine geeignete Konstante $C > 0$.)

25.4.2022

5) Es gibt viele verschiedene Beweise von Satz 19.

Satz 20 (Primfaktorzerlegung) Es sei $n \in \mathbb{N}$, $n \geq 2$. Dann lässt sich n als Produkt von (nicht notwendig verschiedenen) Primzahlen darstellen. (Da es gibt Primzahlen $p_1, \ldots, p_k$, derart dass $n = p_1 \cdots p_k$.) Diese Darstellung ist bis auf die Reihenfolge eindeutig. (Da sind $n = p_1 \cdots p_k = q_1 \cdots q_\ell$ zwei Darstellungen von n als Produkt von Primzahlen, so ist $k = \ell$ und $q_1 \cdots q_\ell$ ist eine Anordnung von $p_1 \cdots p_k$.)

Beweis: Existenz: Induktion nach n.

$n = 2$ ist eine Primzahl (was im Beweis von Satz 19 bewiesen wurde). Beachte, dass 2 dabei als Produkt mit einem Faktor aufgefasst wird!

Es sei nun $n > 2$. Ist n eine Primzahl, so ist man fertig (da man n als Produkt mit einem Faktor auffassen kann). Ist n keine Primzahl, so gibt es nach Lemma 18 eine Primzahl p_0 mit der Eigenschaft $p_0 \mid n$, d.h. es gibt ein $m \in \mathbb{N} \setminus \{0\}$, derart dass $n = p_0 m$. Da n keine Primzahl ist,

ist dabei $1 < m < n$. Nach Induktionsvoraussetzung gibt es Primzahlen $p_1, \dots, p_k$ mit der Eigenschaft $m = p_1 \cdots p_k$. Also ist $n = p_0 m = p_0 p_1 \cdots p_k$ Produkt von Primzahlen.

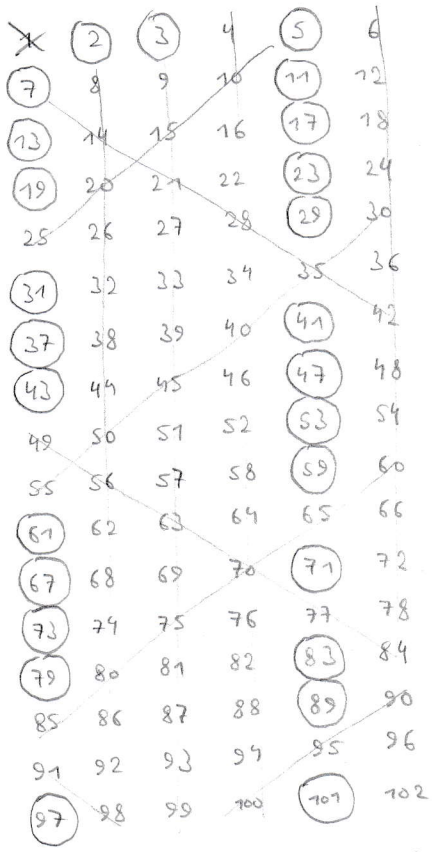
Eindeutigkeit: Angenommen, es gibt ganze Zahlen ≥ 2, die zwei verschiedene Darstellungen als Produkt von Primzahlen besitzen. (Da die Darstellungen unterscheiden sich nicht nur durch ihre Reihenfolge.) Dann gibt es eine kleinste derartige Zahl. (Die Menge derartiger Zahlen ≥ 2 wäre je nach Voraussetzung nicht leer und nach unten beschränkt.) Es sei n die kleinste Zahl ≥ 2 mit zwei Darstellungen (die sich nicht nur durch die Reihenfolge unterscheiden). Weiters seien $n = p_1 \cdots p_r = q_1 \cdots q_s$ zwei verschiedene Darstellungen von n als Produkte von Primzahlen. Dann gilt $p_r \mid (q_1 \cdots q_s)$ und wegen Korollar 17 gibt es ein $i \in \{1, \dots, s\}$ mit der Eigenschaft $p_r \mid q_i$. Da p_r und q_i beides Primzahlen sind, muss $p_r = q_i$ gelten. Es folgt $p_1 \cdots p_{r-1} = \frac{n}{p_r} = \frac{n}{q_i} = q_1 \cdots q_{i-1} q_{i+1} \cdots q_s < n$. Dann besitzt $\frac{n}{p_r}$ $(< n)$ aber ebenfalls zwei verschiedene Darstellungen als Produkt von Primzahlen, was der Minimalität von n widerspricht.

Bemerkung: Mit „Eindeutigkeit bis auf die Reihenfolge" ist gemeint, dass man z.B. bei der Primfaktorzerlegung von 12 die drei Schreibweisen $12 = 2 \cdot 2 \cdot 3 = 2 \cdot 3 \cdot 2 = 3 \cdot 2 \cdot 2$ nicht unterscheidet.

Notation: Meistens ist es praktischer, beim Aufschreiben von Primfaktorzerlegungen mehrfach auftretende Primzahlen zusammenzufassen, d.h. man schreibt z.B. $12 = 2^2 \cdot 3$. Auch in Beweisen werden wir für die Primfaktorzerlegung von n meistens $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ schreiben. Dabei bezeichnen $p_1, \dots, p_k$ paarweise verschiedene Primzahlen und es ist $\alpha_1, \dots, \alpha_k \in \mathbb{N} \cup \{0\}$. Oft ist praktisch, dabei $\alpha_1, \dots, \alpha_k \geq 1$ vorauszusetzen, oft ist die Voraussetzung $\alpha_1, \dots, \alpha_k \geq 0$ aber praktischer. Bei der zweiten Variante kann man in der Primfaktorzerlegung Primzahlen, die nicht auftreten, nämlich mit Exponenten 0 ergänzen, also z.B. $12 = 2^2 \cdot 3^1 \cdot 5^0 = 2^2 \cdot 3^1 \cdot 5^0 \cdot 7^0 = 2^2 \cdot 3^1 \cdot 5^0 \cdot 7^0 \cdot 11^0 \cdot 13^0 = \dots$. Das ist z.B. praktisch, wenn die Primfaktorzerlegungen von zwei Zahlen auftreten, bei denen Primzahlen in der Primfaktorzerlegung der einen Zahl auftreten, aber eventuell nicht in der der anderen.

Sieb des Eratosthenes: Um alle Primzahlen bis zu einer gegebenen Schranke x zu finden, kann man das sogenannte Sieb des Eratosthenes anwenden. Dabei streicht man nach dem Finden einer Primzahl p alle ihre Vielfachen $2p, 3p, 4p, \dots$ bis zur Schranke x, da sie offenbar keine Primzahlen sein können. Die kleinste noch nicht gestrichene Zahl ist die nächste Primzahl. Wegen Bemerkung 4)

auf Seite 4 reicht es dabei, die Vielfachen von Primzahlen $\leq \sqrt{x}$ zu streichen.
Wir verwenden das Sieb des Eratosthenes, um alle Primzahlen ≤ 102 zu finden:



Für $x = 102$ reicht es (wegen $7 < \sqrt{102} < 11$) alle Vielfachen der Primzahlen 2, 3, 5 und 7 zu streichen. Die Zahlen dabei in Sechserblöcken aufzuschreiben, hat den Vorteil, dass man die Vielfachen von 2 und 3 durch senkrechte Striche und die von 5 und 7 durch diagonale Striche streichen kann (da $5 = 6-1$ und $7 = 6+1$).

<u>Lemma 21</u> Es sei $n \in \mathbb{N} \setminus \{0,1\}$. Ist $2^n - 1$ eine Primzahl, so ist n eine Primzahl.

<u>Beweis</u>: Ist n keine Primzahl, so gibt es $a, b \in \mathbb{N}$ mit den Eigenschaften $n = a \cdot b$ und $1 < a, b < n$. Dann ist aber

$$2^n - 1 = 2^{a \cdot b} - 1 = (2^a - 1) \cdot (2^{a(b-1)} + 2^{a(b-2)} + \cdots + 2^a + 1)$$

denn

$$\frac{(2^{a(b-1)} + 2^{a(b-2)} + \cdots + 2^a + 1) \cdot (2^a - 1)}{\begin{array}{l} 2^{ab} + 2^{a(b-1)} + \cdots + 2^{2a} + 2^a \\ \quad - 2^{a(b-1)} - \cdots - 2^{2a} - 2^a - 1 \end{array}}$$

$$\frac{}{2^{ab} \qquad\qquad\qquad\qquad\qquad\qquad - 1}$$

Da $(2^a - 1) \mid (2^n - 1)$ und $1 < 2^a - 1 < 2^n - 1$, also ist $2^n - 1$ keine Primzahl.

<u>Bemerkung</u>: Die Umkehrung von Lemma 21 gilt nicht. Da ist p eine Primzahl, so braucht $2^p - 1$ keine Primzahl zu sein. Zwar sind $2^2 - 1 = 3$, $2^3 - 1 = 7$,

$2^5 - 1 = 31$ und $2^7 - 1 = 127$ Primzahlen, aber $2^{11} - 1 = 2047 = 23 \cdot 89$ ist keine Primzahl.

Definition: Eine Primzahl der Gestalt $2^p - 1$ (wobei p ebenfalls eine Primzahl ist), wird Mersennesche Primzahl genannt.

2.5.2022

Bemerkung: Das Sieb des Eratosthenes ist zu langsam, um wirklich große Primzahlen zu finden. Wird eine neue Primzahl gefunden, die größer als alle bisher bekannten ist, so handelt es sich meistens um eine Mersennesche Primzahl. Der Grund dafür ist, dass man für Zahlen der Gestalt $2^n - 1$ einen speziellen, sehr effizienten Test kennt (den Lucas-Lehmer-Test), der es ermöglicht, relativ rasch zu überprüfen, ob es sich dabei um eine Primzahl handelt. Mersennesche Primzahlen werden im Rahmen des Projekts GIMPS (Great Internet Mersenne Prime Search) auf den Computern von Freiwilligen gesucht. Derzeit sind über 50 Mersennesche Primzahlen bekannt. Man weiß nicht, ob es unendlich viele Mersennesche Primzahlen gibt.

Bemerkung: In der Zahlentheorie sind im Lauf der Jahre viele Arten spezieller Primzahlen untersucht worden. Ein weiteres Beispiel sind sogenannte Primzahlzwillinge, d.h. Zahlen $p, p+2$, die beide Primzahlen sind. Die ersten Primzahlzwillinge sind $(3,5), (5,7), (11,13), (17,19), \ldots$ Man weiß nicht, ob es unendlich viele Primzahlzwillinge gibt.

Satz 22 Es seien $a, b \in \mathbb{N} \setminus \{0\}$ mit Primfaktorzerlegungen $a = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ und $b = p_1^{\beta_1} \cdots p_k^{\beta_k}$ (mit $\alpha_1, \ldots, \alpha_k, \beta_1, \ldots, \beta_k \geq 0$). Dann sind äquivalent:

(i) $a \mid b$,

(ii) $\alpha_i \leq \beta_i$ für $1 \leq i \leq k$.

Beweis: (i) $\Rightarrow$ (ii) Da $a \mid b$, gibt es ein $d \in \mathbb{N} \setminus \{0\}$ mit der Eigenschaft $b = a \cdot d$. Es sei $d = p_1^{\delta_1} \cdots p_k^{\delta_k}$ die Primfaktorzerlegung von d (mit $\delta_1, \ldots, \delta_k \geq 0$). (Tritt eine Primzahl in der Primfaktorzerlegung von d auf, so muss sie offensichtlich auch in der Primfaktorzerlegung von b auftreten.) Es gilt dann

$$p_1^{\beta_1} \cdots p_k^{\beta_k} = b = a \cdot d = p_1^{\alpha_1} \cdots p_k^{\alpha_k} \cdot p_1^{\delta_1} \cdots p_k^{\delta_k} = p_1^{\alpha_1 + \delta_1} \cdots p_k^{\alpha_k + \delta_k}.$$

Wegen der Eindeutigkeit der Primfaktorzerlegung folgt $\beta_i = \alpha_i + \delta_i \geq \alpha_i$ für $1 \leq i \leq k$.

(ii) $\Rightarrow$ (i) Für $1 \leq i \leq k$ sei $\delta_i := \beta_i - \alpha_i \geq 0$ und $d = p_1^{\delta_1} \cdots p_k^{\delta_k} \in \mathbb{N} \setminus \{0\}$. Dann ist $\alpha_i + \delta_i = \beta_i$ für $1 \leq i \leq k$ und daher

$$a \cdot d = p_1^{\alpha_1} \cdots p_k^{\alpha_k} p_1^{\delta_1} \cdots p_k^{\delta_k} = p_1^{\alpha_1 + \delta_1} \cdots p_k^{\alpha_k + \delta_k} = p_1^{\beta_1} \cdots p_k^{\beta_k} = b.$$

Beispiele: 1) $4 \mid 12$ denn $4 = 2^2 \cdot 3^0$ und $12 = 2^2 \cdot 3^1$;

2) $12 \mid 120$ denn $12 = 2^2 \cdot 3^1 \cdot 5^0$ und $120 = 2^3 \cdot 3^1 \cdot 5^1$.

Korollar 23 Hat $a \in \mathbb{N} \setminus \{0\}$ Primfaktorzerlegung $a = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ (mit $\alpha_1, \dots, \alpha_k \geq 0$), so besitzt a genau $(\alpha_1+1) \cdots (\alpha_k+1)$ paarweise verschiedene positive Teiler.

Beweis: Wegen Satz 22 ist $T_a = \{ p_1^{\delta_1} \cdots p_k^{\delta_k} \mid 0 \leq \delta_i \leq \alpha_i \text{ für } 1 \leq i \leq k \}$. Für δ_i gibt es also genau die $\alpha_i + 1$ Möglichkeiten $0, 1, 2, \dots, \alpha_i - 1, \alpha_i$ (für $1 \leq i \leq k$) und daher ist $|T_a| = (\alpha_1+1)(\alpha_2+1) \cdots (\alpha_k+1)$.

Beispiele: 1) $12 = 2^2 \cdot 3^1$ besitzt $(2+1) \cdot (1+1) = 3 \cdot 2 = 6$ verschiedene positive Teiler, nämlich $2^0 \cdot 3^0 = 1$, $2^1 \cdot 3^0 = 2$, $2^2 \cdot 3^0 = 4$, $2^0 \cdot 3^1 = 3$, $2^1 \cdot 3^1 = 6$ und $2^2 \cdot 3^1 = 12$.

2) $60 = 2^2 \cdot 3^1 \cdot 5^1$ besitzt $(2+1) \cdot (1+1) \cdot (1+1) = 3 \cdot 2 \cdot 2 = 12$ verschiedene positive Teiler.

Satz 24 Es seien $a_1, \dots, a_n \in \mathbb{N} \setminus \{0\}$. Für $1 \leq i \leq n$ sei $a_i = p_1^{\alpha_{1i}} p_2^{\alpha_{2i}} \cdots p_k^{\alpha_{ki}}$ (mit $\alpha_{1i}, \alpha_{2i}, \dots, \alpha_{ki} \geq 0$) die Primfaktorzerlegung von a_i. Dann ist

$$ggT(a_1, \dots, a_n) = p_1^{\min\{\alpha_{11}, \alpha_{12}, \dots, \alpha_{1n}\}} \cdot p_2^{\min\{\alpha_{21}, \alpha_{22}, \dots, \alpha_{2n}\}} \cdots p_k^{\min\{\alpha_{k1}, \alpha_{k2}, \dots, \alpha_{kn}\}}$$

die Primfaktorzerlegung von $ggT(a_1, \dots, a_n)$.

Beweis: Es sei $d := p_1^{\min\{\alpha_{11}, \dots, \alpha_{1n}\}} \cdots p_k^{\min\{\alpha_{k1}, \dots, \alpha_{kn}\}}$. Für $1 \leq i \leq n$ ist $\min\{\alpha_{11}, \dots, \alpha_{1n}\} \leq \alpha_{1i}$, $\min\{\alpha_{21}, \dots, \alpha_{2n}\} \leq \alpha_{2i}$, $\dots$, $\min\{\alpha_{k1}, \dots, \alpha_{kn}\} \leq \alpha_{ki}$. Wegen Satz 22 folgt $d \mid a_i$ für $1 \leq i \leq n$. Dh d ist ein gemeinsamer Teiler von $a_1, \dots, a_n$.

Es sei nun $b \in \mathbb{N} \setminus \{0\}$ ein gemeinsamer Teiler von $a_1, \dots, a_n$ mit Primfaktorzerlegung $b = p_1^{\beta_1} \cdots p_k^{\beta_k}$ (mit $\beta_1, \dots, \beta_k \geq 0$). Aus $b \mid a_i$ folgt wegen Satz 22, dass $\beta_1 \leq \alpha_{1i}$, $\beta_2 \leq \alpha_{2i}$, $\dots$, $\beta_k \leq \alpha_{ki}$ (für $1 \leq i \leq n$). Daraus erhält man sofort $\beta_1 \leq \min\{\alpha_{11}, \dots, \alpha_{1n}\}$, $\beta_2 \leq \min\{\alpha_{21}, \dots, \alpha_{2n}\}$, $\dots$, $\beta_k \leq \min\{\alpha_{k1}, \dots, \alpha_{kn}\}$. Wieder wegen Satz 22 folgt nun $b \mid d$. Dh d erfüllt die Bedingungen von Korollar 8(ii) und somit $d = ggT(a_1, \dots, a_n)$.

Korollar 25 Besitzen $a, b \in \mathbb{N} \setminus \{0\}$ die Primfaktorzerlegungen $a = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ und $b = p_1^{\beta_1} \cdots p_k^{\beta_k}$ (mit $\alpha_1, \dots, \alpha_k, \beta_1, \dots, \beta_k \geq 0$), so ist $ggT(a,b) = p_1^{\min\{\alpha_1, \beta_1\}} \cdots p_k^{\min\{\alpha_k, \beta_k\}}$ die Primfaktorzerlegung von $ggT(a,b)$.

Beweis: Das ist der (wichtige) Spezialfall $n = 2$ von Satz 24.

Beispiele: 1) $ggT(30, 45, 75) = ggT(2 \cdot 3 \cdot 5, 3^2 \cdot 5, 3 \cdot 5^2) = ggT(2^1 \cdot 3^1 \cdot 5^1, 2^0 \cdot 3^2 \cdot 5^1, 2^0 \cdot 3^1 \cdot 5^2)$

$= 2^{\min\{0,1\}} \cdot 3^{\min\{1,2\}} \cdot 5^{\min\{1,2\}} = 2^0 \cdot 3^1 \cdot 5^1 = 3 \cdot 5 = 15$

2) $ggT(8100, 24696) = ggT(2^2 \cdot 3^4 \cdot 5^2, 2^3 \cdot 3^2 \cdot 7^3) = ggT(2^2 \cdot 3^4 \cdot 5^2 \cdot 7^0, 2^3 \cdot 3^2 \cdot 5^0 \cdot 7^3)$

$= 2^{\min\{2,3\}} \cdot 3^{\min\{2,4\}} \cdot 5^{\min\{0,2\}} \cdot 7^{\min\{0,3\}} = 2^2 \cdot 3^2 \cdot 5^0 \cdot 7^0 = 36$

Definition: Sind $n_1, \dots, n_k \in \mathbb{Z}$ (nicht notwendig verschieden), so heißt m gemeinsames Vielfaches von $n_1, \dots, n_k$, wenn m Vielfaches aller dieser Zahlen ist, d.h. $n_1 | m, \dots, n_k | m$.

Beispiele: 1) Die Menge der positiven gemeinsamen Vielfachen von 8 und 12 ist $\{24, 2\cdot 24, 3\cdot 24, \dots\} = \{24, 48, 72, \dots\}$. Wegen $24 = 3 \cdot 8 = 2 \cdot 12$ ist 24 gemeinsames Vielfaches von 8 und 12. Wegen Satz 1(vii) ist $24k$ (mit $k \in \mathbb{N} \setminus \{0\}$) ebenfalls positives gemeinsames Vielfaches von 8 und 12 (bzw. $24k = (3k)8 = (2k)12 \quad \forall k \in \mathbb{N} \setminus \{0\}$). Wir werden in Satz 27 zeigen, dass es keine weiteren positiven gemeinsamen Vielfachen von 8 und 12 geben kann.

2) Die Menge der positiven gemeinsamen Vielfachen von 30, 45 und 75 ist $\{450, 2\cdot 450, 3\cdot 450, \dots\} = \{450, 900, 1350, \dots\}$. Wegen $450 = 15 \cdot 30 = 10 \cdot 45 = 6 \cdot 75$ ist 450 gemeinsames Vielfaches von 30, 45 und 75. Wegen Satz 1(vii) ist $450k$ (mit $k \in \mathbb{N} \setminus \{0\}$) ebenfalls positives gemeinsames Vielfaches von 30, 45 und 75. Auch in diesem Beispiel wird aus Satz 27 folgen, dass es keine weiteren positiven gemeinsamen Vielfachen von 30, 45 und 75 geben kann.

Bemerkungen: 1) Wegen Satz 1(ii) gibt es kein positives Vielfaches von 0. Ist daher nur eine der Zahlen $n_1, \dots, n_k$ gleich 0 (d.h. $\exists\, i \in \{1, \dots, k\} : n_i = 0$), so gibt es kein positives gemeinsames Vielfaches von $n_1, \dots, n_k$.

2) Sind $n_1, \dots, n_k \in \mathbb{Z} \setminus \{0\}$, so besitzen sie stets ein positives gemeinsames Vielfaches, nämlich $|n_1 \cdot \dots \cdot n_k| = |n_1| \cdot \dots \cdot |n_k|$. Da die Menge der positiven gemeinsamen Vielfachen von $n_1, \dots, n_k$ ist nicht leer. (Tatsächlich ist sie unendlich, da sie auch $2 \cdot |n_1 \cdots n_k|$, $3 \cdot |n_1 \cdots n_k|$, ... enthält.) Da die Menge der positiven gemeinsamen Vielfachen von $n_1, \dots, n_k$ durch 1 nach unten beschränkt ist, ist es sinnvoll sie zu definieren:

Definition: Sind $n_1, \dots, n_k \in \mathbb{Z} \setminus \{0\}$, so sei $kgV(n_1, \dots, n_k) = \min\{m \in \mathbb{N} \setminus \{0\} \mid n_1 | m, \dots, n_k | m\}$. Dabei ist kgV die Abkürzung für kleinstes gemeinsames Vielfaches.

9.5.2022

Beispiele: 1) $kgV(8, 12) = 24$. Die Menge der positiven Vielfachen von 8 ist $\{8, 2\cdot 8, 3\cdot 8, \dots\} = \{8, 16, 24, \dots\}$, die Menge der positiven Vielfachen von 12 ist $\{12, 2\cdot 12, 3\cdot 12, \dots\} = \{12, 24, 36, \dots\}$. Daher ist

$kgV(8, 12) = \min(\{8, 16, 24, \dots\} \cap \{12, 24, 36, \dots\}) = 24$.

2) $kgV(6, 10, 15) = 30$. Die Menge der positiven Vielfachen von 6, 10 bzw. 15 ist $\{6, 2\cdot 6, 3\cdot 6, \dots\} = \{6, 12, 18, 24, 30, \dots\}$, $\{10, 2\cdot 10, 3\cdot 10, \dots\} = \{10, 20, 30, \dots\}$ bzw.

$\{15, 2\cdot 15, 3\cdot 15, \dots\} = \{15, 30, 45, \dots\}$ und daher

$kgV(6,10,15) = \min(\{6,12,18,24,30,\dots\} \cap \{10,20,30,\dots\} \cap \{15,30,45,\dots\}) = 30.$

Satz 26 Es seien $n_1, \dots, n_k \in \mathbb{Z} \setminus \{0\}$. Dann gelten:

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

(dh man kann bei der Berechnung des kgV stets zu den Beträgen übergehen),

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

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

(dh das kgV hängt nicht von der Reihenfolge der Zahlen $n_1, \dots, n_k$ ab),

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

(dh bei der Bestimmung des kgV können alle n_i, die ein zweites, drittes, etc. Mal auftreten, weggelassen werden).

Beweis: (i) Wegen Satz 1 (iii) gilt $n \mid m \iff |n| \mid m$. Daher gilt für $m \in \mathbb{N} \setminus \{0\}$, dass $n_1 \mid m, \dots, n_k \mid m \iff |n_1| \mid m, \dots, |n_k| \mid m$. Also stimmen die Mengen der positiven gemeinsamen Vielfachen von $n_1, \dots, n_k$ und der positiven gemeinsamen Vielfachen von $|n_1|, \dots, |n_k|$ überein. Daraus folgt die Behauptung.

(ii) und (iii) beweist man analog. Bei beiden Aussagen stimmen die Mengen der positiven gemeinsamen Vielfachen auf beiden Seiten überein.

Satz 27 Es seien $n_1, \dots, n_k \in \mathbb{Z} \setminus \{0\}$ und $m \in \mathbb{Z}$. Dann sind äquivalent:

(i) m ist ein gemeinsames Vielfaches von $n_1, \dots, n_k$,

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

Beweis: Es bezeichne $v := kgV(n_1, \dots, n_k)$.

(i) $\Rightarrow$ (ii) Wir führen Division mit Rest durch, dh $m = qv + r$ für $q, r \in \mathbb{Z}$ mit $0 \leq r < v$. Aus $n_i \mid m$ und $n_i \mid v$ folgt (wegen Satz 1 (x)) $n_i \mid r$ (für $1 \leq i \leq k$). Da r ein gemeinsames Vielfaches von $n_1, \dots, n_k$ und $r < v$. Da v das kleinste positive gemeinsame Vielfache von $n_1, \dots, n_k$ ist, folgt $r = 0$. Also ist $m = qv$ und daher $v \mid m$.

(ii) $\Rightarrow$ (i) Aus $n_i \mid v$ und $v \mid m$ folgt $n_i \mid m$ für $1 \leq i \leq k$ (wegen Satz 1 (viii)).

Beispiel: Wir können nun (nachträglich) beweisen, dass $\{24, 2\cdot 24, 3\cdot 24, \dots\}$ die Menge der positiven gemeinsamen Vielfachen von 8 und 12 ist. Wir haben vor Satz 26 $kgV(8,12) = 24$ bestimmt. Laut Satz 27 ist jedes gemeinsame Vielfache von 8 und 12 ein Vielfaches von 24 und die Menge der positiven gemeinsamen Vielfachen von 8 und 12 daher $\{24k \mid k \in \mathbb{N} \setminus \{0\}\}$.

Völlig analog könnte man zeigen, dass die Menge der positiven gemeinsamen Vielfachen von 30, 45 und 75 die Menge $\{450k \mid k \in \mathbb{N} \setminus \{0\}\}$ ist.

Korollar 28 Es seien $n_1,\dots,n_k \in \mathbb{Z}\setminus\{0\}$ und $v \in \mathbb{N}\setminus\{0\}$. Dann sind äquivalent:

(i) $v = kgV(n_1,\dots,n_k)$,

(ii) v ist ein gemeinsames Vielfaches von $n_1,\dots,n_k$ und ist m ebenfalls ein gemeinsames Vielfaches von $n_1,\dots,n_k$, so gilt $v \mid m$.

Beweis: (i) $\Rightarrow$ (ii) Ist $v = kgV(n_1,\dots,n_k)$, so ist v gemeinsames Vielfaches von $n_1,\dots,n_k$. Ist m ebenfalls gemeinsames Vielfaches von $n_1,\dots,n_k$, so gilt $v \mid m$ nach Satz 27.

(ii) $\Rightarrow$ (i) Nach Voraussetzung ist v ein gemeinsames Vielfaches von $n_1,\dots,n_k$. Ist m ein positives gemeinsames Vielfaches von $n_1,\dots,n_k$, so gilt nach Voraussetzung $v \mid m$. Wegen Satz 1 (iv) folgt $v \leq m$.

Bemerkungen: 1) Man kann Satz 27 und Korollar 28 folgendermaßen interpretieren: Bezeichnet V die Menge der positiven gemeinsamen Vielfachen von $n_1,\dots,n_k$, so sind äquivalent:

(i) $kgV(n_1,\dots,n_k)$ ist minimal in V bezüglich der üblichen Ordnungsrelation $\leq$,

(ii) $kgV(n_1,\dots,n_k)$ ist minimal in V bezüglich der Teilerrelation.

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

Satz 29 Es seien $n_1,\dots,n_k \in \mathbb{Z}\setminus\{0\}$. Dann ist

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

Beweis: Es sei $v := kgV(n_1,\dots,n_k)$. Da $\ell \neq 0$, sind $\ell n_1,\dots,\ell n_k \in \mathbb{Z}\setminus\{0\}$.
Es sei $w := kgV(\ell n_1,\dots,\ell n_k)$. Zu zeigen ist also $w = |\ell| \cdot v$.
Da $n_i \mid v$ (für $1 \leq i \leq k$) folgt $(\ell n_i) \mid (\ell v)$ (für $1 \leq i \leq k$ und jedes $\ell \in \mathbb{Z}\setminus\{0\}$) wegen Satz 1 (viii). Also ist ℓv ein gemeinsames Vielfaches von $\ell n_1,\dots,\ell n_k$.
Aus Korollar 28 folgt $w \mid (\ell v)$.
Da $\ell \mid (\ell n_1)$ und $(\ell n_1) \mid w$ folgt $\ell \mid w$ (wegen Satz 1 (vii)) und daher $\frac{w}{\ell} \in \mathbb{Z}$.
Aus $(\ell n_i) \mid w$ (für $1 \leq i \leq k$) folgt: $\forall i \in \{1,\dots,k\}\ \exists m_i \in \mathbb{Z}: \ell n_i m_i = w$. Daraus folgt $n_i m_i = \frac{w}{\ell}$ (für $1 \leq i \leq k$) und daher $n_i \mid \frac{w}{\ell}$ (für $1 \leq i \leq k$). Also ist $\frac{w}{\ell}$ ein gemeinsames Vielfaches von $n_1,\dots,n_k$. Aus Korollar 28 folgt $v \mid \frac{w}{\ell}$. Daher existiert ein $m \in \mathbb{Z}$, derart dass $vm = \frac{w}{\ell}$ und somit $\ell v m = w$. Offenbar gilt auch $(\ell v) \mid w$.
Da $w \mid (\ell v)$ und $(\ell v) \mid w$ gezeigt ist, folgt wegen Satz 1 (vi), dass

$$kgV(\ell n_1,\dots,\ell n_k) = w = |w| = |\ell v| = |\ell| \cdot |v| = |\ell| \cdot v = |\ell| \cdot kgV(n_1,\dots,n_k).$$

Satz 30 Es sei $k \geq 2$ und $n_1, \dots, n_k \in \mathbb{Z} \setminus \{0\}$. Dann ist

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

Beweis: Es sei $v = \operatorname{kgV}(n_1, \dots, n_k)$. Dann ist v ein gemeinsames Vielfaches von $n_1, \dots, n_k$ und daher erst recht ein gemeinsames Vielfaches von $n_1, \dots, n_{k-1}$. Aus Satz 27 folgt, dass $\operatorname{kgV}(n_1, \dots, n_{k-1}) \mid v$. Aus $\operatorname{kgV}(n_1, \dots, n_{k-1}) \mid v$ und $n_k \mid v$ folgt (wieder wegen Satz 27), dass $\operatorname{kgV}\left(\operatorname{kgV}(n_1, \dots, n_{k-1}), n_k\right) \mid v$. Dh es gilt $\operatorname{kgV}\left(\operatorname{kgV}(n_1, \dots, n_{k-1}), n_k\right) \mid \operatorname{kgV}(n_1, \dots, n_k)$.

Es sei $w = \operatorname{kgV}\left(\operatorname{kgV}(n_1, \dots, n_{k-1}), n_k\right)$. Dann gelten $\operatorname{kgV}(n_1, \dots, n_{k-1}) \mid w$ und $n_k \mid w$. Aus $\operatorname{kgV}(n_1, \dots, n_{k-1}) \mid w$ folgt wegen Satz 27, dass w ein gemeinsames Vielfaches von $n_1, \dots, n_{k-1}$ ist. Da auch $n_k \mid w$ gilt, ist w ein gemeinsames Vielfaches von $n_1, \dots, n_k$. Daraus folgt (wieder wegen Satz 27), dass $\operatorname{kgV}(n_1, \dots, n_k) \mid w$. Also gilt auch

$$\operatorname{kgV}(n_1, \dots, n_k) \mid \operatorname{kgV}\left(\operatorname{kgV}(n_1, \dots, n_{k-1}), n_k\right).$$

Aus Satz 1(vi) folgt $\operatorname{kgV}(n_1, \dots, n_k) = \operatorname{kgV}\left(\operatorname{kgV}(n_1, \dots, n_{k-1}), n_k\right)$.

Satz 31 Es seien $a_1, \dots, a_n \in \mathbb{N} \setminus \{0\}$. Für $1 \leq i \leq n$ sei $a_i = p_1^{\alpha_{1i}} p_2^{\alpha_{2i}} \cdots p_k^{\alpha_{ki}}$ (mit $\alpha_{1i}, \alpha_{2i}, \dots, \alpha_{ki} \geq 0$) die Primfaktorzerlegung von a_i. Dann ist

$$\operatorname{kgV}(a_1, \dots, a_n) = p_1^{\max\{\alpha_{11}, \alpha_{12}, \dots, \alpha_{1n}\}} p_2^{\max\{\alpha_{21}, \alpha_{22}, \dots, \alpha_{2n}\}} \cdots p_k^{\max\{\alpha_{k1}, \alpha_{k2}, \dots, \alpha_{kn}\}}$$

die Primfaktorzerlegung von $\operatorname{kgV}(a_1, \dots, a_n)$.

16.5.2022

Beweis: Es sei $v := p_1^{\max\{\alpha_{11}, \dots, \alpha_{1n}\}} \cdots p_k^{\max\{\alpha_{k1}, \dots, \alpha_{kn}\}}$. Für $1 \leq i \leq n$ ist $\alpha_{1i} \leq \max\{\alpha_{11}, \dots, \alpha_{1n}\}, \alpha_{2i} \leq \max\{\alpha_{21}, \dots, \alpha_{2n}\}, \dots, \alpha_{ki} \leq \max\{\alpha_{k1}, \dots, \alpha_{kn}\}$. Wegen Satz 22 folgt $a_i \mid v$ für $1 \leq i \leq n$. Dh v ist ein gemeinsames Vielfaches von $a_1, \dots, a_n$.

Es sei nun $b \in \mathbb{N} \setminus \{0\}$ ein gemeinsames Vielfaches von $a_1, \dots, a_n$ mit Primfaktorzerlegung $b = p_1^{\beta_1} \cdots p_k^{\beta_k}$ (mit $\beta_1, \dots, \beta_k \geq 0$). Aus $a_i \mid b$ folgt wegen Satz 22, dass $\alpha_{1i} \leq \beta_1, \alpha_{2i} \leq \beta_2, \dots, \alpha_{ki} \leq \beta_k$ (für $1 \leq i \leq n$). Daraus erhält man sofort $\max\{\alpha_{11}, \dots, \alpha_{1n}\} \leq \beta_1, \max\{\alpha_{21}, \dots, \alpha_{2n}\} \leq \beta_2, \dots, \max\{\alpha_{k1}, \dots, \alpha_{kn}\} \leq \beta_k$. Wieder wegen Satz 22 folgt nun $v \mid b$. Dh v erfüllt die Bedingungen von Korollar 28(ii) und somit $v = \operatorname{kgV}(a_1, \dots, a_n)$.

Korollar 32 Besitzen $a, b \in \mathbb{N} \setminus \{0\}$ die Primfaktorzerlegungen $a = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ und $b = p_1^{\beta_1} \cdots p_k^{\beta_k}$ (mit $\alpha_1, \dots, \alpha_k, \beta_1, \dots, \beta_k \geq 0$), so ist $\operatorname{kgV}(a, b) = p_1^{\max\{\alpha_1, \beta_1\}} \cdots p_k^{\max\{\alpha_k, \beta_k\}}$ die Primfaktorzerlegung von $\operatorname{kgV}(a, b)$.

Beweis: Das ist der (wichtige) Spezialfall $n = 2$ von Satz 31

Beispiele: 1) $\mathrm{kgV}(8,12) = \mathrm{kgV}(2^3, 2^2\cdot 3) = \mathrm{kgV}(2^3\cdot 3^0, 2^2\cdot 3^1) = 2^{\max\{3,2\}}\cdot 3^{\max\{0,1\}}$

$= 2^3\cdot 3^1 = 24$

2) $\mathrm{kgV}(30,45,75) = \mathrm{kgV}(2\cdot 3\cdot 5, 3^2\cdot 5, 3\cdot 5^2) = \mathrm{kgV}(2^1\cdot 3^1\cdot 5^1, 2^0\cdot 3^2\cdot 5^1, 2^0\cdot 3^1\cdot 5^2)$

$= 2^{\max\{0,1\}}\cdot 3^{\max\{1,2\}}\cdot 5^{\max\{1,2\}} = 2\cdot 3^2\cdot 5^2 = 450$

Bemerkung: Für $x,y\in\mathbb{R}$ gilt $\min\{x,y\}+\max\{x,y\} = x+y$. (Ist o.B.d.A. $x\le y$, so ist ja $\min\{x,y\}=x$ und $\max\{x,y\}=y$ und daher $\min\{x,y\}+\max\{x,y\}=x+y$.)

Satz 33 Sind $a,b\in\mathbb{N}\setminus\{0\}$, so gilt $\mathrm{ggT}(a,b)\cdot\mathrm{kgV}(a,b) = a\cdot b$.

Beweis: Besitzen a und b Primfaktorzerlegungen $a = p_1^{\alpha_1}\cdots p_k^{\alpha_k}$ und $b = p_1^{\beta_1}\cdots p_k^{\beta_k}$ (und $\alpha_1,\dots,\alpha_k,\beta_1,\dots,\beta_k\ge 0$), so gilt (wegen Korollar 25, Korollar 32 und der Bemerkung unmittelbar vor Satz 33)

$$\mathrm{ggT}(a,b)\cdot\mathrm{kgV}(a,b) = p_1^{\min\{\alpha_1,\beta_1\}}\cdots p_k^{\min\{\alpha_k,\beta_k\}}\cdot p_1^{\max\{\alpha_1,\beta_1\}}\cdots p_k^{\max\{\alpha_k,\beta_k\}}$$

$$= p_1^{\min\{\alpha_1,\beta_1\}+\max\{\alpha_1,\beta_1\}}\cdots p_k^{\min\{\alpha_k,\beta_k\}+\max\{\alpha_k,\beta_k\}} = p_1^{\alpha_1+\beta_1}\cdots p_k^{\alpha_k+\beta_k}$$

$$= p_1^{\alpha_1}\cdots p_k^{\alpha_k}\cdot p_1^{\beta_1}\cdots p_k^{\beta_k} = a\cdot b$$

Bemerkung: Kennt man drei der vier Größen a,b, $\mathrm{ggT}(a,b)$ und $\mathrm{kgV}(a,b)$, so kann man Satz 33 verwenden, um die vierte zu berechnen.

Beispiel: Für $a=8$ und $b=12$ ist $\mathrm{ggT}(a,b)=4$ und daher

$$\mathrm{kgV}(a,b) = \frac{a\cdot b}{\mathrm{ggT}(a,b)} = \frac{8\cdot 12}{4} = 24.$$

Korollar 34 Es seien $a,b\in\mathbb{N}\setminus\{0\}$. Dann sind äquivalent:

(i) $\mathrm{ggT}(a,b)=1$,

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

Beweis: (i) $\Rightarrow$ (ii) $\mathrm{kgV}(a,b) = 1\cdot\mathrm{kgV}(a,b) = \mathrm{ggT}(a,b)\cdot\mathrm{kgV}(a,b) \overset{\text{Satz 33}}{=} a\cdot b$

(ii) $\Rightarrow$ (i) Aus $a\cdot b \overset{\text{Satz 33}}{=} \mathrm{ggT}(a,b)\cdot\mathrm{kgV}(a,b) = a\cdot b\cdot\mathrm{ggT}(a,b)$ folgt sofort $\mathrm{ggT}(a,b)=1$.

Satz 35 Es sei $n\ge 2$ und $a_1,\dots,a_n\in\mathbb{N}\setminus\{0\}$. Dann sind äquivalent:

(i) $a_1,\dots,a_n$ sind paarweise relativ prim,

(ii) $\mathrm{kgV}(a_1,\dots,a_n) = a_1\cdots a_n$.

Beweis: (i) $\Rightarrow$ (ii) Induktion nach n. Der Fall $n=2$ wurde bereits in Korollar 34 bewiesen. Es sei nun $n\ge 2$. Sind $a_1,\dots,a_{n+1}$ paarweise relativ prim, so sind auch $a_1,\dots,a_n$ paarweise relativ prim und daher nach Induktionsvoraussetzung

$\mathrm{kgV}(a_1,\dots,a_n) = a_1 \cdots a_n$. Weiters sind die beiden Zahlen $a_1 \cdots a_n$ und a_{n+1} relativ prim. (Wären sie das nicht, so würde es eine Primzahl p geben, für die $p \mid (a_1 \cdots a_n)$ und $p \mid a_{n+1}$ gilt. Wegen Korollar 17 folgt aus $p \mid (a_1 \cdots a_n)$, dass $p \mid a_i$ für ein $i \in \{1,\dots,n\}$. Das heißt aber, dass a_i und a_{n+1} nicht relativ prim wären, Widerspruch.) Aus Korollar 34 folgt $\mathrm{kgV}(a_1 \cdots a_n, a_{n+1}) = a_1 \cdots a_n \cdot a_{n+1} = a_1 \cdots a_{n+1}$. Insgesamt erhält man mit Hilfe von Satz 30

$$\mathrm{kgV}(a_1,\dots,a_{n+1}) = \mathrm{kgV}\big(\mathrm{kgV}(a_1,\dots,a_n), a_{n+1}\big) \overset{IV}{=} \mathrm{kgV}(a_1 \cdots a_n, a_{n+1}) = a_1 \cdots a_{n+1}.$$

(ii) $\Rightarrow$ (i) Sind $a_1,\dots,a_n$ nicht paarweise relativ prim, so gibt es $k,\ell \in \{1,\dots,n\}$ mit $k \neq \ell$, derart dass a_k und a_ℓ nicht relativ prim sind. D.h. $\mathrm{ggT}(a_k, a_\ell) > 1$ und es gibt ein $d \in \mathbb{N}$, $d > 1$ mit der Eigenschaft $d \mid a_k$ und $d \mid a_\ell$. Dann gilt aber auch $d \mid (a_1 \cdots a_{j-1} a_{j+1} \cdots a_n)$ für jedes $j \in \{1,\dots,n\}$, da unter den Zahlen $a_1,\dots,a_{j-1},a_{j+1},\dots,a_n$ ja entweder a_k oder a_ℓ auftreten muss. Also ist

$$\frac{a_1 \cdots a_{j-1} a_{j+1} \cdots a_n}{d} \in \mathbb{Z} \quad \text{und daher} \quad \frac{a_1 \cdots a_n}{d} = a_j \cdot \frac{a_1 \cdots a_{j-1} a_{j+1} \cdots a_n}{d} \quad \text{für } 1 \le j \le n.$$

Das zeigt, dass $\frac{a_1 \cdots a_n}{d}$ ein gemeinsames Vielfaches von $a_1,\dots,a_n$ ist und daher

$$\mathrm{kgV}(a_1,\dots,a_n) \le \frac{a_1 \cdots a_n}{d} < a_1 \cdots a_n.$$

Bemerkung: Bedingung (i) in Satz 35 kann nicht durch die schwächere Bedingung „$a_1,\dots,a_n$ sind relativ prim" ersetzt werden. Z.B. ist $\mathrm{ggT}(6,10,15) = 1$ aber $\mathrm{kgV}(6,10,15) = 30 < 6 \cdot 10 \cdot 15 = 900$.