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.

24.3.2025

Bemerkungen: 1) Die „Schuldefinition" 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 $\exists\, d \in \mathbb{N}, d > 1$, sodass $d \mid p$ und $p \mid n$. Die einzige Zahl > 1, die p teilt, ist aber p selbst. 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 $a, b \in \mathbb{Z}$ gilt, dass $p \mid (ab) \Rightarrow p \mid a$ oder $p \mid b$ (d.h. p ist prim),

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

Beweis: (i) $\Rightarrow$ (ii) Ist $p \mid a$, so ist die Behauptung erfüllt.

Falls $p \nmid a$, so $ggT(p,a) = 1$ nach Lemma 15. Aus Satz 12 folgt $p \mid b$.

(ii) $\Rightarrow$ (iii) Gilt $p = xy$, so folgt $p \mid (xy)$ und nach Voraussetzung $p \mid x$ 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 (vii)).

Es folgt $p = |p| = |xy| = |x| \cdot |y| = p \cdot |y|$ und daher $|y| = 1$, d.h. $y \in \{1, -1\}$.

Gilt $p \mid y$, so zeigt man analog $x \in \{1, -1\}$.

(iii) $\Rightarrow$ (i) Wenn $m \mid p$ für ein $m \in \mathbb{Z}$, so $\exists\, n \in \mathbb{Z} : p = mn$. Nach Voraussetzung ist dann $m \in \{1, -1\}$ oder $n \in \{1, -1\}$ (und daher $m \in \{p, -p\}$). Insgesamt ist $m \in \{1, -1, p, -p\}$ und p daher eine Primzahl.

Bemerkungen: 1) Auch Eigenschaft (ii) aus Satz 16 findet man bereits in den Elementen des Euklid (Buch VII, Prop. 30).

2) Eigenschaften (ii) und (iii) aus Satz 16 werden auch von $-p$ erfüllt, wenn p eine Primzahl ist. Man setzt deswegen $p > 1$ voraus, um zu verhindern, dass $-2, -3, -5, -7, \ldots$ ebenfalls als Primzahlen gelten.

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. $\exists i \in \{1,\dots,n\} : p \mid a_i$.

Beweis: Induktion nach n: $n=1$ ist trivial, $n=2$ wurde in Satz 16 bewiesen. Ist nun $n \geq 2$, so kann man $p \mid (a_1 \cdots a_{n+1})$ als $p \mid (a_1 \cdots a_n) a_{n+1}$ schreiben. Aus dem Fall $n=2$ folgt $p \mid (a_1 \cdots a_n)$ oder $p \mid a_{n+1}$. Falls $p \mid (a_1 \cdots a_n)$ folgt aus der Induktionsvoraussetzung, dass $\exists i \in \{1,\dots,n\} : p \mid a_i$.

Lemma 18 Ist $n \in \mathbb{Z}$ und $|n| \geq 2$, so 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: Die Menge $T := \{m \in \mathbb{Z} \mid m > 1, m \mid n\}$ ist nicht leer (da $|n| \in T$) und durch 1 nach unten beschränkt. Daher existiert $p := \min T$. Wir zeigen, dass p eine Primzahl ist. Nach Konstruktion gelten $p \in \mathbb{Z}$ und $p > 1$. Wäre p keine Primzahl, so würde p einen Teiler d mit $1 < d < p$ besitzen. Aus $d \mid p$ und $p \mid n$ würde (wegen Satz 1 (viii)) $d \mid n$ folgen. Da es wäre $d \in T$ und $d < p$, ein Widerspruch zur Minimalität von p.

Satz 19 Es gibt unendlich viele Primzahlen.

Beweis Angenommen, es gäbe nur die Primzahlen $p_1,\dots,p_k$. Wir betrachten die Zahl $p_1 \cdots p_k + 1$. Offenbar ist 2 Primzahl. (Aus $d \mid 2$ folgt wegen Satz 1 (iv) $|d| \leq 2$, d.h. $d \in \{-2,-1,0,1,2\}$. Da $0 \nmid 2$ ist $d \in \{-2,-1,1,2\}$.) Daher ist $p_1 \cdots p_k + 1 \geq 2$ und wegen Lemma 18 existiert eine Primzahl p mit der Eigenschaft $p \mid (p_1 \cdots p_k + 1)$. Wäre $p \in \{p_1,\dots,p_k\}$, so würde $p \mid (p_1 \cdots p_k)$ gelten und daher wegen Satz 1 (x) auch $p \mid ((p_1 \cdots p_k + 1) - p_1 \cdots p_k)$, d.h. $p \mid 1$, ein Widerspruch zu Satz 1 (iv), da $p > 1$.

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

2) Im Beweis von Satz 19 wird nicht bewiesen, dass $p_1 \cdots p_k + 1$ eine Primzahl ist. Z.B. ist $2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 + 1 = 30031 = 59 \cdot 509$.

Satz 20 (Primfaktorzerlegung) Jede Zahl $n \in \mathbb{N}$, $n \geq 2$ kann als Produkt von (nicht notwendig verschiedenen) Primzahlen dargestellt werden. Diese Darstellung ist bis auf die Reihenfolge eindeutig.

(D.h. es gibt Primzahlen $p_1,\dots,p_k$, sodass $n = p_1 \cdots p_k$. 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 $q_1,\dots,q_\ell$ ist eine Anordnung von $p_1,\dots,p_k$.)

Bemerkung: Ist n eine Primzahl, so wird es Produkt mit einem Faktor aufgefasst.

Beweis: Existenz: Induktion nach n

$n=2$ ist Primzahl (siehe Beweis von Satz 19).

Es sei nun $n>2$. Ist n eine Primzahl, so ist man fertig. Ist n keine Primzahl, so gibt es nach Lemma 18 eine Primzahl p mit der Eigenschaft $p|n$. Daher $\exists\, m\in\mathbb{N}^+ : n = p\cdot m$. Da n keine Primzahl ist, ist $1<m<n$. Nach Induktionsvoraussetzung gibt es Primzahlen $p_1,\dots,p_k$, sodass $m = p_1\cdots p_k$ und daher $n = p\cdot p_1\cdots p_k$

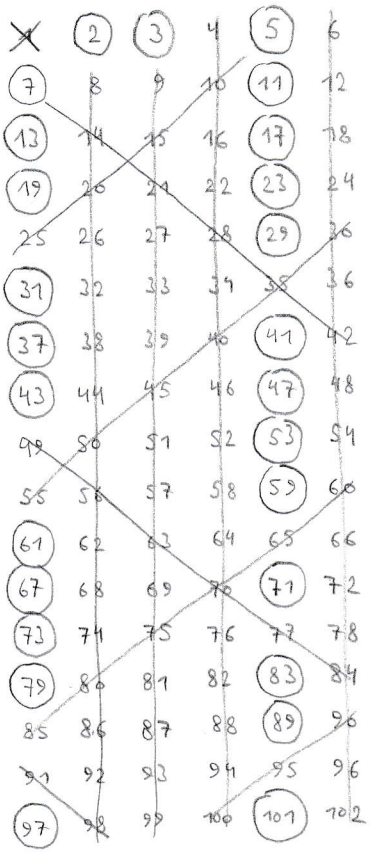
Eindeutigkeit: Angenommen, es gibt ganze Zahlen ≥ 2, die zwei verschiedene Darstellungen als Produkt von Primzahlen besitzen (d.h. Darstellungen, die sich nicht nur durch die Reihenfolge der Primfaktoren unterscheiden). Es sei n die kleinste solche Zahl und $n = p_1\cdots p_k = q_1\cdots q_\ell$ zwei verschiedene Darstellungen von n als Produkt von Primzahlen. Dann gilt $p_k \mid (q_1\cdots q_\ell)$ und nach Korollar 17 $\exists\, i\in\{1,\dots,\ell\} : p_k \mid q_i$. Da p_k und q_i beides Primzahlen sind, muss $p_k = q_i$ gelten. Daraus folgt, dass $p_1\cdots p_{k-1} = \frac{n}{p_k} = \frac{n}{q_i} = q_1\cdots q_{i-1}q_{i+1}\cdots q_\ell < n$ ebenfalls zwei verschiedene Darstellungen als Produkt von Primzahlen besitzt, ein Widerspruch zur Minimalität von n.

Notation: Meistens fasst man in Primfaktorzerlegungen mehrfach auftretende Primzahlen zusammen, also z.B. $12 = 2^2\cdot 3$. Auch wir werden Primfaktorzerlegungen meistens in der Form $p_1^{\alpha_1}\cdots p_k^{\alpha_k}$ schreiben. Dabei sind $p_1,\dots,p_k$ paarweise verschiedene Primzahlen und $\alpha_1,\dots,\alpha_k\in\mathbb{N}$. Manchmal ist es praktisch, $\alpha_1,\dots,\alpha_k\geq 1$ vorauszusetzen, oft ist $\alpha_1,\dots,\alpha_k\geq 0$ aber besser, da man Primzahlen, die nicht auftreten, mit Exponent 0 ergänzen kann, also z.B. $12 = 2^2\cdot 3^1\cdot 5^0$.

31.3.2025

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 2f reicht es dabei, die Vielfachen aller 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 Vielfachen von 5 und 7 durch diagonale Striche streichen kann (da $5 = 6-1$ und $7 = 6+1$).

Satz 21 Es sei $n \in \mathbb{N}$, $n \geq 2$. Ist $2^n - 1$ eine Primzahl, so ist n eine Primzahl.

Beweis: 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 $2^n - 1 = 2^{ab} - 1 = (2^a - 1) \cdot (2^{a(b-1)} + 2^{a(b-2)} + \dots + 2^a + 1)$, denn

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

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

Bemerkung: Die Umkehrung von Satz 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 Primzahl ist), wird MERSENNE'sche Primzahl genannt.

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, handelt es sich meistens um eine Mersennesche Primzahl. Der Grund ist, dass man für Zahlen der Gestalt 2^n-1 einen speziellen, sehr effizienten Primzahltest kennt (den LUCAS-LEHMER-Test). 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 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 $a, b \in \mathbb{N}^+$ 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 $a \mid b$, existiert $d \in \mathbb{N}^+$: $b = a \cdot d$. Ist $d = p_1^{\delta_1} \cdots p_k^{\delta_k}$ Primfaktorzerlegung von d (mit $\delta_1, \ldots, \delta_k \geq 0$), so ist

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

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 $d = p_1^{\delta_1} \cdots p_k^{\delta_k} \in \mathbb{N}^+$. 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 $a \in \mathbb{N}^+$ Primfaktorzerlegung $a = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ (mit $\alpha_1, \ldots, \alpha_k \geq 0$), so besitzt a genau $(\alpha_1+1) \cdots (\alpha_k+1)$ paarweise verschiedene positive Teiler.

Beweis: Bezeichnet T_a die Menge der positiven Teiler von a, so ist (wegen Satz 22) $T_a = \{ p_1^{\delta_1} \cdots p_k^{\delta_k} \mid 0 \leq \delta_i \leq \alpha_i \text{ für } 1 \leq i \leq k \}$. Für δ_i gibt es also genau die α_i+1 Möglichkeiten $0, 1, 2, \ldots, \alpha_i - 1, \alpha_i$ (für $1 \leq i \leq k$) und daher $|T_a| = (\alpha_1+1)(\alpha_2+1) \cdots (\alpha_k+1)$.

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

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

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

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 $1 \le i \le n$ ist

$$\min\{\alpha_{11},\dots,\alpha_{1n}\} \le \alpha_{1i},\ \min\{\alpha_{21},\dots,\alpha_{2n}\} \le \alpha_{2i},\ \dots,\ \min\{\alpha_{k1},\dots,\alpha_{kn}\} \le \alpha_{ki}.$$

Wegen Satz 22 folgt $d \mid a_i$ für $1 \le i \le n$, d.h. d ist gemeinsamer Teiler von $a_1,\dots,a_n$.
Es sei nun $b \in \mathbb{N}^+$ ein gemeinsamer Teiler von $a_1,\dots,a_n$ mit Primfaktorzerlegung $b = p_1^{\beta_1} \cdots p_k^{\beta_k}$ (mit $\beta_1,\dots,\beta_k \ge 0$). Aus $b \mid a_i$ folgt wegen Satz 22, dass $\beta_1 \le \alpha_{1i}, \beta_2 \le \alpha_{2i}, \dots, \beta_k \le \alpha_{ki}$ (für $1 \le i \le n$) und daher $\beta_1 \le \min\{\alpha_{11},\dots,\alpha_{1n}\}$, $\beta_2 \le \min\{\alpha_{21},\dots,\alpha_{2n}\}$, $\dots$, $\beta_k \le \min\{\alpha_{k1},\dots,\alpha_{kn}\}$. Wieder wegen Satz 22 folgt $b \mid d$. Aus Korollar 8 folgt $d = ggT(a_1,\dots,a_n)$.

Korollar 25 Besitzen $a,b \in \mathbb{N}^+$ die Primfaktorzerlegungen $a = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ und $b = p_1^{\beta_1} \cdots p_k^{\beta_k}$ (mit $\alpha_1,\dots,\alpha_k,\beta_1,\dots,\beta_k \ge 0$), 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 Fall $n=2$ von Satz 24.

Beispiele: 1) $ggT(30,45,75) = ggT(2\cdot3\cdot5,\ 3^2\cdot5,\ 3\cdot5^2) = ggT(2^1\cdot3^1\cdot5^1,\ 2^0\cdot3^2\cdot5^1,\ 2^0\cdot3^1\cdot5^2)$
$= 2^{\min\{0,1\}} \cdot 3^{\min\{1,2\}} \cdot 5^{\min\{1,2\}} = 2^0\cdot3^1\cdot5^1 = 3\cdot5 = 15$

2) $ggT(8100,24696) = ggT(2^2\cdot3^4\cdot5^2,\ 2^3\cdot3^2\cdot7^3) = ggT(2^2\cdot3^4\cdot5^2\cdot7^0,\ 2^3\cdot3^2\cdot5^0\cdot7^3)$
$= 2^{\min\{2,3\}} \cdot 3^{\min\{4,2\}} \cdot 5^{\min\{2,0\}} \cdot 7^{\min\{0,3\}} = 2^2\cdot3^2\cdot5^0\cdot7^0 = 36$

Definition Sind $n_1,\dots,n_k \in \mathbb{Z}$ (nicht notwendig verschieden), so heißt $m \in \mathbb{Z}$ gemeinsames Vielfaches von $n_1,\dots,n_k$, wenn es Vielfaches aller dieser Zahlen ist, d.h. $n_1 \mid m, \dots, n_k \mid m$. 7.4.2025

Beispiele: 1) Die Menge der positiven gemeinsamen Vielfachen von 8 und 12 ist $\{24, 2\cdot24, 3\cdot24, \dots\} = \{24, 48, 72, \dots\}$. Wegen $24 = 3\cdot8 = 2\cdot12$ ist 24 gemeinsames Vielfaches von 8 und 12. Wegen Satz 7 (vii) ist $24k$ (mit $k \in \mathbb{N}^+$) ebenfalls positives gemeinsames Vielfaches von 8 und 12 (bzw. $24 = (3k)\cdot8 = (2k)\cdot12$ $\forall k \in \mathbb{N}^+$). Wir werden in Satz 27 zeigen, dass es keine weiteren positiven gemeinsamen Vielfachen von 8 und 12 gibt.

2) Die Menge der positiven gemeinsamen Teiler von 30, 45 und 75 ist $\{450, 2\cdot450, 3\cdot450, \dots\} = \{450, 900, 1350, \dots\}$. Wegen $450 = 15\cdot30 = 10\cdot45 = 6\cdot75$ ist 450 gemeinsames Vielfaches von 30, 45 und 75. Wegen Satz 7 (vii) ist $450k$ (mit $k \in \mathbb{N}^+$)

ebenfalls positives gemeinsames Vielfaches von 30, 45 und 75. Aus Satz 27 wird folgen, dass es keine weiteren positiven gemeinsamen Vielfachen von 30, 45 und 75 gibt.

Bemerkungen: 1) Wegen Satz 1 (ii) gibt es kein positives Vielfaches von 0. Ist daher 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 $|n_1\cdots n_k|=|n_1|\cdots|n_k|$. D.h. die Menge der positiven gemeinsamen Vielfachen von $n_1,\dots,n_k$ ist nicht leer. (Tatsächlich ist sie unendlich, da sie $2|n_1\cdots n_k|$, $3|n_1\cdots n_k|$, ... enthält.) Da die Menge der positiven gemeinsamen Vielfachen von $n_1,\dots,n_k$ durch 1 nach unten beschränkt ist, ist es sinnvoll zu definieren:

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

Beispiele: 1) $\operatorname{kgV}(8,12)=24$. Die Menge der positiven Vielfachen von 8 ist $\{8,2\cdot8,3\cdot8,\dots\}=\{8,16,24,\dots\}$, die Menge der positiven Vielfachen von 12 ist $\{12,2\cdot12,3\cdot12,\dots\}=\{12,24,36,\dots\}$. Daher ist

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

2) $\operatorname{kgV}(6,10,15)=30$. Die Mengen der positiven Vielfachen von 6, 10 bzw. 15 sind $\{6,2\cdot6,3\cdot6,\dots\}=\{6,12,18,24,30,\dots\}$, $\{10,2\cdot10,3\cdot10,\dots\}=\{10,20,30,\dots\}$ bzw. $\{15,2\cdot15,3\cdot15,\dots\}=\{15,30,45,\dots\}$ und daher

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

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

(i) $\operatorname{kgV}(n_1,\dots,n_k)=\operatorname{kgV}(|n_1|,\dots,|n_k|)$,
d.h. 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 $\operatorname{kgV}(n_{i_1},\dots,n_{i_k})=\operatorname{kgV}(n_1,\dots,n_k)$,
d.h. das kgV hängt nicht von der Reihenfolge der Zahlen $1,\dots,k$ ab,

(iii) Ist $k\geq2$ und $n_k=n_{k-1}$, so ist $\operatorname{kgV}(n_1,\dots,n_k)=\operatorname{kgV}(n_1,\dots,n_{k-1})$,
d.h. bei der Bestimmung von $\operatorname{kgV}(n_1,\dots,n_k)$ können alle n_i, die mehr als einmal auftreten, beim zweiten, dritten, ... Auftreten weggelassen werden.

Beweis: (i) Wegen Satz 1 (iii) gilt $n|m\iff|n||m$. Daher gilt für $m\in\mathbb{N}^+$, dass $n_1|m,\dots,n_k|m\iff|n_1||m,\dots,|n_k||m$. Daher 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 nun Division mit Rest durch, d.h. $m = qv + r$ mit $0 \le r < v$. Aus $n_i \mid m$ und $n_i \mid v$ folgt (wegen Satz 1(xi)) $n_i \mid r$ (für $1 \le i \le k$). Da r ist 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 $v \mid m$.

(ii) $\Rightarrow$ (i) $n_i \mid v$ und $v \mid m$ folgt $n_i \mid m$ (für $1 \le i \le k$) wegen Satz 1(vii).

Beispiel: Wir können nun (mühelos) begründen, 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 $\{24k \mid k \in \mathbb{N}^+\}$. Analog kann man zeigen, dass die Menge der positiven gemeinsamen Vielfachen von 30, 45 und 75 die Menge $\{450k \mid k \in \mathbb{N}^+\}$ ist.

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

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

(ii) v ist gemeinsames Vielfaches von $n_1,\dots,n_k$ und ist m ebenfalls 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 $v \le m$.

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 $\le$,

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

Beweis: Es sei $v := \operatorname{kgV}(n_1,\dots,n_k)$. Da $\ell \neq 0$, sind $\ell n_1,\dots,\ell n_k \in \mathbb{Z}\setminus\{0\}$.

Es sei $w = \operatorname{kgV}(\ell n_1,\dots,\ell n_k)$. Zu zeigen ist also $w = |\ell| v$.

Aus $n_i | v$ folgt $(\ell n_i) | (\ell v)$ (für $1 \le i \le k$ und $\ell \in \mathbb{Z}\setminus\{0\}$) wegen Satz 1(viii). Also ist ℓv gemeinsames Vielfaches von $\ell n_1,\dots,\ell n_k$ und daher $w | (\ell v)$ wegen Satz 27.

Aus $\ell | (\ell n_1)$ und $(\ell n_1) | w$ folgt $\ell | w$ (wegen Satz 1(viii)) und daher $\frac{w}{\ell} \in \mathbb{Z}$.

Aus $(\ell n_i) | w$ (für $1 \le i \le k$) folgt: $\forall i \in \{1,\dots,k\}\ \exists m_i \in \mathbb{Z} : \ell n_i m_i = w$ und daher $n_i m_i = \frac{w}{\ell}$ (für $1 \le i \le k$). Also ist $\frac{w}{\ell}$ ein gemeinsames Vielfaches von $n_1,\dots,n_k$. Aus Satz 27 folgt $v | \frac{w}{\ell}$.

Also $\exists m \in \mathbb{Z} : vm = \frac{w}{\ell}$ und daher $\ell v m = w$. Da es gilt auch $(\ell v) | w$.

Aus $w | (\ell v)$ und $(\ell v) | w$ folgt mittels Satz 1(vi)

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

28.4.2025

Satz 30 Es sei $k \ge 2$ und $n_1,\dots,n_k \in \mathbb{Z}\setminus\{0\}$. Dann ist $\operatorname{kgV}(n_1,\dots,n_k) = \operatorname{kgV}(\operatorname{kgV}(n_1,\dots,n_{k-1}), n_k)$

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

Es sei $w = \operatorname{kgV}(\operatorname{kgV}(n_1,\dots,n_{k-1}), n_k)$. Dann gelten $\operatorname{kgV}(n_1,\dots,n_{k-1}) | w$ und $n_k | w$.

Aus $\operatorname{kgV}(n_1,\dots,n_{k-1}) | w$ folgt wegen Satz 27, dass w gemeinsames Vielfaches von $n_1,\dots,n_{k-1}$ ist. Da auch $n_k | w$ gild, ist w gemeinsames Vielfaches von $n_1,\dots,n_k$ und wegen Satz 27 folgt $\operatorname{kgV}(n_1,\dots,n_k) | w$. Also gilt auch $\operatorname{kgV}(n_1,\dots,n_k) \mid \operatorname{kgV}(\operatorname{kgV}(n_1,\dots,n_{k-1}), n_k)$.

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

Satz 31 Es sei $a_1,\dots,a_n \in \mathbb{N}^+$. Für $1 \le i \le n$ sei $a_i = p_1^{\alpha_{1i}} p_2^{\alpha_{2i}} \cdots p_k^{\alpha_{ki}}$ (mit $\alpha_{1i},\alpha_{2i},\dots,\alpha_{ki} \ge 0$) 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 $\operatorname{kgV}(a_1,\dots,a_n)$.

Beweis: Es sei $v := p_1^{\max\{\alpha_{11},\dots,\alpha_{1n}\}} \cdots p_k^{\max\{\alpha_{k1},\dots,\alpha_{kn}\}}$. Für $1 \le i \le n$ ist

$$\alpha_{1i} \le \max\{\alpha_{11},\dots,\alpha_{1n}\},\ \alpha_{2i} \le \max\{\alpha_{21},\dots,\alpha_{2n}\},\ \dots,\ \alpha_{ki} \le \max\{\alpha_{k1},\dots,\alpha_{kn}\}.$$

Wegen Satz 22 folgt $a_i | v$ für $1 \le i \le n$, dh v ist ein gemeinsames Vielfaches von $a_1,\dots,a_n$.

Es sei nun $b \in \mathbb{N}^+$ ein gemeinsames Vielfaches von $a_1,\dots,a_n$ mit Primfaktorzerlegung $b = p_1^{\beta_1} \cdots p_k^{\beta_k}$ (mit $\beta_1,\dots,\beta_k \ge 0$). Aus $a_i | b$ folgt wegen Satz 22, dass

$\alpha_{1i} \le \beta_1, \alpha_{2i} \le \beta_2, \dots, \alpha_{ki} \le \beta_k$ (für $1 \le i \le n$) und daher

$\max\{\alpha_{11}, \dots, \alpha_{1n}\} \le \beta_1, \max\{\alpha_{21}, \dots, \alpha_{2n}\} \le \beta_2, \dots, \max\{\alpha_{k1}, \dots, \alpha_{kn}\} \le \beta_k$. Wieder wegen Satz 22 folgt $v \mid b$. Da v erfüllt die Bedingungen von Korollar 28 (ii) und daher $v = kgV(a_1, \dots, a_n)$

Korollar 32 Besitzen $a, b \in \mathbb{N}^+$ die 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 ist $kgV(a,b) = p_1^{\max\{\alpha_1, \beta_1\}} \cdots p_k^{\max\{\alpha_k, \beta_k\}}$ die Primfaktorzerlegung von $kgV(a,b)$.

Beweis: Das ist der Fall $n = 2$ von Satz 31.

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

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

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

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

Satz 33 Sind $a, b \in \mathbb{N}^+$, so ist $ggT(a,b) \cdot kgV(a,b) = a \cdot b$

Beweis: Besitzen a und b Primfaktorzerlegungen $a = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ und $b = p_1^{\beta_1} \cdots p_k^{\beta_k}$ (mit $\alpha_1, \dots, \alpha_k, \beta_1, \dots, \beta_k \ge 0$), so gilt

$$ggT(a,b) \cdot kgV(a,b) \overset{\text{Kor. 25, Kor. 32}}{=} p_1^{\min\{\alpha_1,\beta_1\}} \cdots p_k^{\min\{\alpha_k,\beta_k\}} \cdot p_1^{\max\{\alpha_1,\beta_1\}} \cdots p_k^{\max\{\alpha_k,\beta_k\}}$$

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

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

Beispiel Für $a = 8$ und $b = 12$ ist $ggT(a,b) = 4$ und $kgV(a,b) = \frac{ab}{ggT(a,b)} = \frac{8 \cdot 12}{4} = 24$.

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

(i) $ggT(a,b) = 1$,

(ii) $kgV(a,b) = ab$

Beweis: (i) $\Rightarrow$ (ii) $kgV(a,b) = 1 \cdot kgV(a,b) = ggT(a,b) \cdot kgV(a,b) = ab$

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

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

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

(ii) $kgV(a_1, \dots, a_n) = a_1 \cdots a_n$

Beweis: (i) $\Rightarrow$ (ii) Induktion nach n. Der Fall $n=2$ wurde in Korollar 34 bewiesen.

Es sei nun $n \geq 2$. Sind $a_1, \dots, a_{n+1}$ paarweise relativ prim, so sind auch $a_1, \dots, a_n$ paarweise relativ prim und nach Induktionsvoraussetzung ist $kgV(a_1, \dots, a_n) = a_1 \cdots a_n$. 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. Aus $p \mid (a_1 \cdots a_n)$ folgt wegen Korollar 17, 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 sind, Widerspruch.) Wegen Korollar 34 gilt $kgV(a_1 \cdots a_n, a_{n+1}) = (a_1 \cdots a_n) a_{n+1} = a_1 \cdots a_{n+1}$ und daher

$$kgV(a_1, \dots, a_{n+1}) \overset{\text{Satz 30}}{=} kgV(kgV(a_1, \dots, a_n), a_{n+1}) \overset{\text{IV}}{=} kgV(a_1 \cdots a_n, a_{n+1}) \overset{\text{Kor. 34}}{=} a_1 \cdots a_{n+1}$$

(ii) $\Rightarrow$ (i) Sind $a_1, \dots, a_n$ nicht paarweise relativ prim, so gibt es $k, l \in \{1, \dots, n\}$ mit $k \neq l$, sodass a_k und a_l nicht relativ prim sind. D.h. $ggT(a_k, a_l) > 1$ und es gibt ein $d \in \mathbb{N}^+$, $d > 1$ sodass $d \mid a_k$ und $d \mid a_l$. 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

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

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

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

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 $ggT(6, 10, 15) = 1$ aber $kgV(6, 10, 15) = 30 < 6 \cdot 10 \cdot 15 = 900$