Primzahlen, ggT und kgV

Definition: Eine natürliche Zahl $m \in \mathbb{N}$ heißt Teiler von $n \in \mathbb{N}$, falls ein $k \in \mathbb{N}$ existiert mit

$$n = k \cdot m$$

Man schreibt dann auch $m|n$.

Jede Zahl besitzt also offensichtlich die beiden Teiler 1 und n, denn es gilt stets

$$n = n \cdot 1 = 1 \cdot n$$

Existiert für $n > 1$ kein weiterer Teiler, so nennt man n eine **Primzahl**.

Die ersten Primzahlen lauten

$$2, 3, 5, 7, 11, 13, 17, 19, 23, \ldots$$

Primzahlzwillinge: $\{3, 5\}, \{5, 7\}, \{11, 13\}, \{17, 19\}, \ldots$?

Primzahlzerlegung einer natürlichen Zahl $n \in \mathbb{N}$

Satz: Jede natürliche Zahl $n \in \mathbb{N}$ läßt sich als Produkt von Primzahlpotenzen schreiben,

$$n = p_1^{r_1} \cdot p_2^{r_2} \cdot \ldots \cdot p_k^{r_k}$$
$$p_j : \text{Primzahl}, \quad r_j \in \mathbb{N}_0$$

Beweis: Setze folgende Aussageformen

$\tilde{A}(n) :\Leftrightarrow \forall\, k \in \{1, \ldots, n\} : A(k)$ (Primzahlzerlegung der Zahl k)

Induktionsanfang: $1 = 2^0$

Induktionsschluss:

Ist $n + 1$ eine Primzahl, so ist Behauptung mit $n + 1 = (n + 1)^1$ klar.

Ist $n+1$ keine Primzahl, so gibt es $k, m \in \{2, 3, \ldots, n\}$ mit $n+1 = k \cdot m$.

$\Rightarrow n + 1$ besitzt Primzahlzerlegung, da k und m eine besitzen.

Definition: Für zwei natürliche Zahlen $n, m \in \mathbb{N}$ nennt man

$$\mathsf{ggT}(n,m) := \max\{k \mid k \text{ teilt } n \text{ und } m\}$$

den **größten gemeinsamen Teiler** von n und m,

$$\mathsf{kgV}(n,m) := \min\{k \mid n \text{ und } m \text{ teilen } k\}$$

das **kleinste gemeinsame Vielfache** von n und m.

Gilt etwa

$$n = p_1^{r_1} \cdot p_2^{r_2} \cdot \ldots \cdot p_k^{r_k} \qquad m = p_1^{s_1} \cdot p_2^{s_2} \cdot \ldots \cdot p_k^{s_k}$$

so folgt

$$\begin{aligned} \mathsf{ggT}(n,m) &= p_1^{\min(r_1,s_1)} \cdot p_2^{\min(r_2,s_2)} \cdot \ldots \cdot p_k^{\min(r_k,s_k)} \\ \mathsf{kgV}(n,m) &= p_1^{\max(r_1,s_1)} \cdot p_2^{\max(r_2,s_2)} \cdot \ldots \cdot p_k^{\max(r_k,s_k)} \end{aligned}$$

Beispiel: Nehme

$$\begin{aligned} n &= 525 = 2^0 \cdot 3^1 \cdot 5^2 \cdot 7^1 \\ m &= 180 = 2^2 \cdot 3^2 \cdot 5^1 \cdot 7^0 \end{aligned}$$

Dann gilt

$$\begin{aligned} \mathsf{ggT}(525,180) &= 2^0 \cdot 3^1 \cdot 5^1 \cdot 7^0 = 15 \\ \mathsf{kgV}(525,180) &= 2^2 \cdot 3^2 \cdot 5^2 \cdot 7^1 = 6300 \end{aligned}$$

und

$$n \cdot m = 525 \cdot 180 = 15 \cdot 6300 = \mathsf{ggT} \cdot \mathsf{kgV}$$

Folgerung: Es gilt

$$\mathsf{ggT}(n,m) \cdot \mathsf{kgV}(n,m) = n \cdot m$$

Verfahren der iterierten Division (Euklidischer Algorithmus)

Wir setzen

$$r_0 := n \qquad r_1 := m$$

und führen folgende Iteration durch

für $j = 1, 2, \ldots$

$$r_{j-1} = q_j \cdot r_j + r_{j+1} \quad (0 \leq r_{j+1} < r_j)$$

Da $r_0 > r_1 > r_2 > \ldots$, gibt es ein $r_{k+1} = 0$ (Iterationsabbruch) und

$$r_k = \text{ggT}(n, m)$$

Beispiel: Sei $n = 3054$ und $m = 1002$.

$$\begin{array}{rcrcrcr} 3054 & = & 3 & \cdot & 1002 & + & 48 \\ 1002 & = & 20 & \cdot & 48 & + & 42 \\ 48 & = & 1 & \cdot & 42 & + & 6 \\ 42 & = & 7 & \cdot & \boxed{6} & + & 0 \end{array}$$

Bemerkung: $\mathbb{Z}$–Kombination des ggT(n, m) von n und m

Lese Euklidischen Algorithmus

$$\begin{array}{rcrcrcr} 3054 & = & 3 & \cdot & 1002 & + & 48 \\ 1002 & = & 20 & \cdot & 48 & + & 42 \\ 48 & = & 1 & \cdot & 42 & + & \boxed{6} \end{array}$$

rückwärts nach der letzten Spalte

$$\begin{aligned} 6 &= 48 - 1 \cdot 42 \\ &= 48 - 1 \cdot (1002 - 20 \cdot 48) = 21 \cdot 48 - 1002 \\ &= 21 \cdot (3054 - 3 \cdot 1002) - 1002 \\ &= 21 \cdot 3054 - 64 \cdot 1002 \end{aligned}$$

Die $\mathbb{Z}$–Kombination ist gegeben durch

$$\text{ggT}(3054, 1002) = 6 = 21 \cdot 3054 - 64 \cdot 1002$$

2.2 Reelle Zahlen

Erweiterung des Zahlenbereichs der natürlichen Zahlen

- Ganze Zahlen $\mathbb{Z}$

$$\mathbb{Z} := \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$$

- Rationale Zahlen $\mathbb{Q}$

$$\mathbb{Q} := \left\{ \frac{m}{n} \mid m \in \mathbb{Z}, n \in \mathbb{N} \right\}$$

Wie definieren wir den Zahlenbereich $\mathbb{R}$ der reellen Zahlen?
Verwende ein

Axiomensystem zur Definition reeller Zahlen

(I) Regeln der Addition (Abelsche Gruppe)

$$\begin{array}{lllll} \text{(a)} & x + (y + z) & = & (x + y) + z & \\ \text{(b)} & x + y & = & y + x & \\ \text{(c)} & x + 0 & = & 0 + x & = & x \\ \text{(d)} & x + (-x) & = & (-x) + x & = & 0 \end{array}$$

(II) Regeln der Multiplikation

$$\begin{array}{lllll} \text{(a)} & x \cdot (y \cdot z) & = & (x \cdot y) \cdot z & \\ \text{(b)} & x \cdot y & = & y \cdot x & \\ \text{(c)} & x \cdot 1 & = & 1 \cdot x & = & x \\ \text{(d)} & x \cdot \left(\frac{1}{x}\right) & = & \left(\frac{1}{x}\right) \cdot x & = & 1 \quad (x \neq 0) \end{array}$$

(III) Distributivgesetz (Regeln (I)–(III): Körper)

$$x \cdot (y + z) = x \cdot y + x \cdot z$$

(IV) Ordnungseigenschaften

(a) $x \leq y \vee y \leq x$

(b) $x \leq x$

(c) $x \leq y \wedge y \leq x \Rightarrow x = y$

(d) $x \leq y \wedge y \leq z \Rightarrow x \leq z$

(e) $x \leq y \Rightarrow x + z \leq y + z$

(f) $x \leq y \wedge z \geq 0 \Rightarrow x \cdot z \leq y \cdot z$

(V) Vollständigkeitsaxiom (Dedekind, 1872)

Sei $\mathbb{R}$ zerlegt: $\mathbb{R} = L \cup R$ ($L, R \neq \emptyset$) und $\forall\, x \in L, y \in R : \; x < y$. Dann gibt es genau eine **Schnittzahl** $s \in \mathbb{R}$ mit :

$$\forall\, x \in L,\, y \in R : \quad (x \leq s \leq y)$$

Bemerkung: Die Menge der rationalen Zahlen $\mathbb{Q}$ erfüllt nicht das Vollständigkeitsaxiom (V). Denn für

$$L := \{x \in \mathbb{Q} \mid x^2 < 2 \vee x < 0\}$$

$$R := \{x \in \mathbb{Q} \mid x^2 > 2 \wedge x > 0\}$$

gibt es keine Schnittzahl. Diese wäre $x = \sqrt{2} \notin \mathbb{Q}$.

Weitere Regeln beim Rechnen mit Ungleichungen (aus Axiomen (IV))

(1) $x \leq y \Rightarrow -x \geq -y$

(2) $x \leq y \wedge z \leq 0 \Rightarrow x \cdot z \geq y \cdot z$

(3) $x^2 \geq 0$

(4) $x \leq y \wedge u \leq v \Rightarrow x + u \leq y + v$

(5) $0 \leq x \leq y \wedge 0 \leq u \leq v \Rightarrow x \cdot u \leq y \cdot v$

Definition: Zu $a \in \mathbb{R}$ heißt

$$|a| := \begin{cases} a & \text{falls } a \geq 0 \\ -a & \text{falls } a < 0 \end{cases}$$

der **Betrag** von a.

$|a - b|$ = (nichtnegative) Abstand der Zahlen a, b auf der Zahlengerade.

Eigenschaften:

(1) $|a| \geq 0$

(2) $|a| = 0 \Rightarrow a = 0$

(3) $|ab| = |a|\,|b|$

(4) $|a + b| \leq |a| + |b|$ (**Dreiecksungleichung)**

(5) $U_\varepsilon(a) := \{x \in \mathbb{R} \,|\, |x - a| < \varepsilon\} \quad (\varepsilon > 0)$

$= (a - \varepsilon, a + \varepsilon)$ (ε**–Umgebung von** a**)**

Definition: Sei $M \subset \mathbb{R}$, also M eine Teilmenge von $\mathbb{R}$.

1) Die Zahl $x \in \mathbb{R}$ heißt **obere Schranke** von M, falls gilt:

$$\forall\, w \in M : w \leq x$$

Analog definiert man den Begriff **untere Schranke von** M.

2) Die Menge M heißt **nach oben** (bzw. **nach unten**) **beschränkt**, falls es eine obere (bzw. untere) Schranke von M gibt.

3) Die Zahl $s \in \mathbb{R}$ heißt **Supremum von** M, falls s die kleinste obere Schranke von M ist, d.h.

- s ist eine obere Schranke von M
- für jede beliebige obere Schranke x von M gilt: $s \leq x$

Bezeichnung: $s := \sup M$.

Analog definiert man den Begriff **Infimum von** M.

Beispiel: Sei $I := [1,2) = \{x \in \mathbb{R} \,|\, 1 \leq x < 2\}$

Dann ist

- jede Zahl $x \geq 2$ eine obere Schranke von I,
- jede Zahl $x \leq 1$ eine untere Schranke von I.

Also gilt

$$\sup [1,2) = 2 \qquad \inf [1,2) = 1$$

Beispiel: Man betrachte die Menge

$$M := \left\{ x \in \mathbb{R} \,|\, x = \frac{1}{n} + \frac{1}{n+1}, \quad n \in \mathbb{N} \right\} = \left\{ \frac{3}{2}, \frac{5}{6}, \frac{7}{12}, \frac{9}{20}, \frac{11}{30}, \ldots \right\}$$

Daher gilt

$$\sup M = \frac{3}{2} \qquad \inf M = 0$$

Satz: Jede nichtleere, nach oben (bzw. unten) beschränkte Menge $M \subset \mathbb{R}$ besitzt ein Supremum (bzw. Infimum).

Beweis: Mit Hilfe des Vollständigkeitsaxioms.

Folgerungen:

1) Die Menge $\mathbb{N}$ der natürlichen Zahlen ist nicht nach oben beschränkt.
2) Für alle $x \in \mathbb{R}$ gilt:

$$x \geq 0 \quad \Rightarrow \quad \exists\, n \in \mathbb{N} \,:\, 0 < \frac{1}{n} < x$$

3) Zwischen zwei reellen Zahlen $x < y$ gibt es immer (unendlich viele) rationale Zahlen.