Eindeutigkeit der Primfaktorzerlegung

Grundlegend für die Teilbarkeitslehre ist die eindeutige Darstellbarkeit jeder natürlichen Zahl (Null und Eins ausgenommen) als Produkt unzerlegbarer Elemente (Primzahlen). Die Eindeutigkeit ist eine unmittelbare Folge des Satzes:

$$p \mid a \cdot b \quad (p \text{ Primzahl}) \quad \Longrightarrow \quad p \mid a \quad \text{oder} \quad p \mid b$$

Denn lägen zwei Zerlegungen

$$p_1 p_2 \ldots p_n \;=\; p_1^* p_2^* \ldots p_m^*$$

vor, so müsste z. B. p_1 auch in der rechten Zerlegung enthalten sein (der obige Schluss wird wiederholt angewandt). Nun dürfte die Folgerung offensichtlich sein und es bleibt den Satz zu beweisen. Dazu stellen wir das Benötigte zusammen.

Der größte gemeinsame Teiler zweier Zahlen kann mit dem Euklidischen Algorithmus ermittelt werden. Sei $b < a$, die wiederholte Division mit Rest bricht nach endlich vielen Schritten und aufgehender Division ab (siehe Klasse 5, Teilbarkeit):

$$\begin{aligned}
a &= q_1 \cdot b + r_1 \\
b &= q_2 \cdot r_1 + r_2 \\
r_1 &= q_3 \cdot r_2 + r_3 \\
&\vdots \\
r_{n-2} &= q_n \cdot r_{n-1} + r_n \\
r_{n-1} &= q_{n+1} \cdot r_n \qquad\qquad \text{mit} \qquad b > a > r_1 > r_2 > \ldots > 0
\end{aligned}$$

Der größte gemeinsame Teiler von a und b ist dann r_n.

Denn jeder gemeinsame Teiler teilt nach der 1. Gleichung auch r_1, nach der 2. Gleichung auch r_2, usw., schließlich r_n. Umgekehrt beinhaltet die letzte Gleichung $r_n \mid r_{n-1}$. Aus der vorletzten Gleichung ergibt sich dann $r_n \mid r_{n-2}$, letztendlich erhalten wir $r_n \mid b$ und $r_n \mid a$.

Der Euklidische Algorithmus bietet noch eine grundlegende Erkenntnis:

Satz
Der ggT zweier Zahlen ist eine Linearkombination dieser Zahlen, kurz:

$$ggT(a,b) \;=\; xa + yb, \qquad \textit{mit ganzen Zahlen } x \textit{ und } y.$$

Wird die 1. Gleichung auch r_1 aufgelöst und der Term in die 2. Gleichung eingesetzt, ergibt sich r_2 als Linearkombination von a und b. Wiederholtes Einsetzen führt zu der behaupteten Darstellung des ggT.

Folgerung
Sind a und b teilerfremd, so ist die Gleichung $xa + yb = 1$ ganzzahlig lösbar.

Kehren wir zurück zur Eindeutigkeit der Primfaktorzerlegung.
Sei $p \mid a \cdot b$ und nehmen wir an, dass p nicht a teilt.

$$\begin{aligned}
&\Longrightarrow \quad 1 \;=\; xp + ya \qquad \mid \cdot b \\
&\Longrightarrow \quad b \;=\; \underbrace{xpb + yab}_{p \mid \qquad} \quad \Longrightarrow \quad p \mid b
\end{aligned}$$