5 Primfaktorzerlegung und ggT

Definition 5.1 Eine natürliche Zahl p mit $p > 1$ heißt *Primzahl*, falls sie keine natürlichen Teiler außer 1 und sich selbst besitzt. M.a.W.

$$a, b \in \mathbb{N},\ p = ab \quad \Longrightarrow \quad a = 1 \text{ oder } b = 1$$

Der folgende Satz wird oft auch als der "Hauptsatz" oder "Fundamentalsatz der Arithmetik" bezeichnet.

Satz 5.2 Jede natürliche Zahl $n > 1$ läßt sich als ein Produkt von Primzahlen schreiben:

$$n = p_1 \cdot p_2 \cdot \ldots \cdot p_r,\ p_1, p_2, \ldots, p_r \text{ Primzahlen.}$$

Diese Zerlegung ist eindeutig bis auf die Reihenfolge der Faktoren. D.h., wenn auch $n = q_1 \cdot q_2 \cdot \ldots \cdot q_s$ ist mit q_j prim für $j = 1, \ldots, s$, so ist $r = s$, und wenn wir ferner $p_1 \leq p_2 \leq \ldots \leq p_r$ und $q_1 \leq q_2 \leq \ldots \leq q_r$ annehmen, so ist $p_i = q_i$ für $i = 1, \ldots, r$.

5.3 Der **Beweis der Existenz** einer solchen Zerlegung ist sehr leicht: wenn n schon selbst eine Primzahl ist, sind wir fertig. Anderenfalls schreibe

$$n = a \cdot b, \quad 1 < a < n, \quad 1 < b < n\,.$$

Wenn a und b Primzahlen sind, sind wir fertig. Anderenfalls kann einer der Faktoren weiter zerlegt werden, sagen wir $b = c \cdot d$, $1 < c < b$. Einsetzen liefert

$$p = a \cdot c \cdot d\,.$$

Dieses Verfahren wird fortgesetzt, solange noch Faktoren nicht prim sind. Da die Anzahl der Faktoren immer größer wird, bricht das Verfahren nach höchstens m Schritten ab, wobei m die größte Zahl mit $2^m \leq n$ ist, und wir haben die gewünschte Zerlegung gefunden. □

Die Eindeutigkeit der Zerlegung in Primfaktoren ist erheblich schwieriger zu zeigen. Einen durchsichtigen Beweis erhält man, wenn man sich *vorher* den folgenden Satz überlegt.

Satz 5.4 ***(Satz vom größten gemeinsamen Teiler)*** *Gegeben seien zwei ganze Zahlen a und b. Dann gibt es eine ganze Zahl g mit folgenden Eigenschaften:*

(1) $g \mid a$ *und* $g \mid b$,

(2) $m \in \mathbb{Z}$, $m \mid a$ *und* $m \mid b \quad \Longrightarrow \quad m \mid g$.

In Worten: g ist ein Teiler von a und von b, und jede Zahl, die gleichzeitig a und b teilt, ist ein Teiler von g.

Vorbereitend zum Beweis zunächst ein Rechenverfahren:

5.5 Euklidischer Algorithmus Gegeben sind $a \in \mathbb{Z},\ b \in \mathbb{N}$.

1. Teile a durch b mit Rest r.
2. Ersetze a durch b, ersetze b durch r.
3. Wiederhole Schritt 1 und Schritt 2 mit den neuen Zahlen.
   Führe dieses durch bis der Rest 0 wird. Dieses geschieht in endlich vielen Schritten, da b (bzw. r) im Laufe des Verfahrens immer kleiner wird.
4. Der Output des Algorithmus ist der letzte von Null verschiedene Rest (d.h. die letzte Zahl b).

Beweis des Satzes vom ggT: Man zieht sich leicht auf den Fall $b > 0$ zurück. Sei dann g die mit dem euklidischen Algorithmus bestimmte Zahl.

Behauptung: Dieses g hat die beiden im Satz genannten Eigenschaften.

Beweis: Man gibt zunächst allen beteiligten Zahlen einen Namen:

$$
\begin{array}{llllll}
a & b & r & & & \\
a_1 & b_1 & r_1 & \text{wobei} & a_1 = b & b_1 = r \\
a_2 & b_2 & r_2 & \text{wobei} & a_2 = b_1 & b_2 = r_1 \\
\vdots & & & & & \\
a_{\ell-1} & b_{\ell-1} & r_{\ell-1} & & & \\
a_\ell & b_\ell & r_\ell = 0 & \text{wobei} & a_\ell = b_{\ell-1} & b_\ell = r_{\ell-1}
\end{array}
$$

An jeder Stelle k gilt

$$
\begin{aligned}
a_k &= q_k b_k + r_k \qquad \text{mit } q_k \in \mathbb{Z}\,. \\
a_k &= b_{k-1}, \quad b_k = r_{k-1}
\end{aligned}
$$

Beweis von Eigenschaft (1) für die Zahl $g = b_\ell$:

$$
\begin{array}{ll}
a_\ell = q_\ell b_\ell & \Longrightarrow g \mid a_\ell \\
g \mid b_{\ell-1} \text{ und } g \mid r_{\ell-1} & \Longrightarrow g \mid a_{\ell-1} \\
g \mid b_{\ell-2} \text{ und } g \mid r_{\ell-2} & \Longrightarrow g \mid a_{\ell-2} \\
\vdots & \\
g \mid b_1 \text{ und } g \mid r_1 & \Longrightarrow g \mid a_1 \text{ d.h. } g \mid b \\
g \mid b \text{ und } g \mid r & \Longrightarrow g \mid a
\end{array}
$$

Beweis von Eigenschaft (2) für die Zahl g: Sei d ein gemeinsamer Teiler von a und b

$$\begin{aligned} d \mid a \text{ und } d \mid b \quad &\Longrightarrow d \mid r \\ d \mid a_1 \text{ und } d \mid b_1 \quad &\Longrightarrow d \mid r_1 \\ &\vdots \\ d \mid a_{\ell-1} \text{ und } d \mid b_{\ell-1} \quad &\Longrightarrow d \mid r_{\ell-1} \end{aligned}$$

Also gilt $d \mid g$, wie gewünscht. □

Satz 5.6 *Der größte gemeinsame Teiler g von a und b besitzt eine Darstellung*

$$g = xa + yb \text{ mit } x, y \in \mathbb{Z}\,.$$

Beweis Dieses ergibt sich leicht durch sukzessives Einsetzen in der obigen Reihe von Gleichungen. Zu Anfang ist

$$\begin{aligned} r &= a - qb \\ r_1 &= a_1 - q_1 b_1 = b - q_1 r \\ &= b - q_1(a - qb) \\ &= -q_1 a + (1 + q_1 q)b\,. \end{aligned}$$

Sei schon gezeigt

$$\begin{aligned} r_{k-1} &= xa + yb \qquad b_k = xa + yb \\ r_k &= x'a + y'b\,. \end{aligned}$$

Dann erhält man entsprechendes auch für den nächsten Rest, also r_{k+1}:

$$\begin{aligned} r_{k+1} &= a_{k+1} - q_{k+1} b_{k+1} \\ &= b_k - q_{k+1} r_k \\ &= (xa + yb) - q_{k+1}(x'a + y'b) \\ &= (x - q_{k+1}x')a + (y - q_{k+1}y')b \end{aligned}$$

□

Wir steuern nun den Satz von der eindeutigen Primfaktorzerlegung an und beweisen zuvor einen Hilfssatz über Primzahlen.

Hilfssatz 5.7 Wenn eine Primzahl ein Produkt teilt, so teilt sie wenigstens einen der Faktoren:

$$p \text{ Primzahl}, a, b \in \mathbb{N},\ p \mid ab \quad \Longrightarrow \quad p \mid a \text{ oder } p \mid b\,.$$

Beweis Der Beweis beruht wesentlich auf der Existenz von ggT's. Es sei

$$g \text{ der ggT von } p \text{ und } a$$
$$h \text{ der ggT von } p \text{ und } b\,.$$

Es gilt $g \mid p$; weil p eine Primzahl ist, bestehen nur die Möglichkeiten $g = 1$ oder $g = p$. Entpsrechend kann nur $h = 1$ oder $h = p$ sein.

Wir diskutieren nun die verschiedenen Möglichkeiten.

1. Fall $g = p$. Wegen $g \mid a$ gilt dann $p \mid a$, wie gewünscht.

2. Fall $h = p$. Entsprechend gilt dann $p \mid b$.

Wenn diese Fälle beide nicht eintreten, bleibt nur noch die letzte Möglichkeit

3. Fall $g = 1$ und $h = 1$. Nun benutzen wir den Zusatz zum Satz über den ggT: Es gibt ganze Zahlen x, y, x', y' mit

$$xp + ya = 1, \quad x'p + y'b = 1\,.$$

Multiplizieren der beiden Gleichungen liefert

$$xx'p^2 + xy'bp + yx'ap + yy'ab = 1\,.$$

Nun verwenden wir die Voraussetzung $p \mid ab$. Hieraus folgt, daß p die gesamte linke Seite der letzten Gleichung teilt. Also gilt $p \mid 1$. Das ist unmöglich, also kann der 3. Fall gar nicht eintreten.

5.8 Beweis des Hauptsatzes 5.2. Sei $p_1 p_2 \dots p_r = q_1 q_2 \dots q_r$. Wir wenden den Hilfssatz auf die Primzahl $p = p_1$ und das Produkt $q_1 \cdot q$ mit $q = q_2 \dots q_s$ an. Es gilt $p_1 \mid q_1$ oder $p_1 \mid q$. Wenn $p_1 \mid q_1$ gilt, so muß offenbar $p_1 = q_1$ sein, denn q_1 ist Primzahl (und $p_1 \neq 1$). Im Fall $p_1 \mid q$ schreibe $q = q_2 \cdot q'$ und schließe entsprechend $p_1 = q_2$ oder $p_1 \mid q'$. Da der zweite Faktor $q, q', \dots$ nach jedem Schritt ein q_i weniger enthält, muß irgendwann einmal $p_1 = q_i$ sein. Wir können noch die Rollen der linken und rechten Seite, d.h. der p_i und q_i vertauschen und so $p_1 \leq q_1$ annehmen. Wegen $p_1 \leq q_1 \leq q_i = p_1$ muß dann aber $p_1 = q_1$ sein. Wir teilen nun beide Seiten durch p_1 und bearbeiten entsprechend die Gleichung

$$p_2 p_3 \dots p_r = q_2 q_3 \dots q_s\,.$$

Es folgt $p_2 = q_2$. Wir verfahren entsprechend, solange noch auf einer Seite wenigstens ein Faktor steht. Wenn $r < s$ oder $s < r$ wäre, so hätten wir irgendwann den Widerspruch, daß links 1 stünde und rechts nicht, bzw. umgekehrt. Also muß $r = s$ sein, und wir enden schließlich bei $p_r = q_r$. □