Primzahlkriterium und Fundamentalsatz der Arithmetik

Wir geben hier einen alternativen Beweis für das Primzahlkriterium aus Propostion 5.3.46 des Buches (ohne die Eindeutigkeit der Primfaktorzerlegung zu benutzen). Daraus leiten wir in der Folge den Fundamentalsatz der Arithmetik (Theorem 5.3.45 des Buches) ab. Man bemerke, dass wir Spezialfälle des Primzahlkriteriums schon bewiesen haben. Das das Produkt zweier ungerader Zahlen ungerade ist, sehen wir, dass die Primzahl 2 ein Produkt genau dann teilt, wenn sie einen der Faktoren teilt.

PROPOSITION. *Eine Zahl $p \in \mathbb{N}$ mit $p > 1$ ist genau dann eine Primzahl, wenn für beliebige Zahlen $k, \ell \in \mathbb{Z}$ aus $p|k\ell$ immer $p|k$ oder $p|\ell$ folgt.*

BEWEIS. Ist p nicht prim, dann ist $p = rs$ für $r, s \in \mathbb{N}$ mit $r, s < p$. Dann gilt natürlich $p|rs$ aber p kann weder r noch s teilen.

Die andere Implikation beweisen wir indirekt. Wir nehmen also an, dass es Primzahlen gibt, für die das gangegebene Kriterium nicht gilt. Sei p die kleinste aller dieser Primzahlen. Dann gibt es also Zahlen k und ℓ sodass p weder k noch ℓ teilt, aber $p|k\ell$ gilt. Wir können uns auf $k, \ell \in \mathbb{N}$ einschränken und wir betrachten jenen Fall für den das Produkt $k\ell$ so klein wie möglich ist.

Dann muss zunächst $k, \ell < p$ gelten. Wir können nämlich k und ℓ mit Rest durch p dividieren und erhalten $k = ap + u$, $\ell = bp + v$ mit $0 \leq u, v < p$. Dann ist aber $k\ell = abp^2 + avp + ubp + uv$, also $uv = k\ell - (abp + av + bu)p$. Wären a oder b ungleich 0, dann wäre $uv < k\ell$ und $p|uv$, aber natürlich kann p weder u noch v teilen und das wäre ein Widerspruch zur Minimalität von $k\ell$.

Schreiben wir also $k\ell = pm$ für $m \in \mathbb{N}$, dann muss $1 < m < p$ gelten. Aus Lemma 2.1.4 wissen wir bereits, dass man m als Produkt von Primzahlen schreiben kann. Ist p' einer der Primfaktoren, dann gilt natürliche $p'|k\ell$ und wegen $p' < p$ muss die Primzahl p' einen der beiden Faktoren teilen. Ist etwa $k = p'k'$ und $m = p'm'$, dann folgt aus $k\ell = pm$ natürlich $p'k'\ell = p'pm'$, also $k'\ell = pm'$. Damit gilt aber $p|k'\ell$ und $k'\ell < k\ell$, also muss wegen der Minimalität von $k\ell$ entweder $p|k'$ (und damit $p|k$) oder $p|\ell$ gelten, was wiederum einen Widerspruch darstellt. □

Mit Induktion nach der Anzahl der Faktoren beweist man dann sofort: Ist p ein Primzahl und sind $k_1, \ldots, k_n \in \mathbb{Z}$ sodass $p|(k_1 \cdots k_n)$ gilt, dann gibt es mindestens ein i, sodass $p|k_i$ gilt. Mit diesem Kriterium wird der Beweis des Fundamentalsatzes der Arithmetik dann ziemlich einfach:

THEOREM. *Sei $m > 1$ eine ganze Zahl. Dann kann man m als Produkt von Primzahlen schreiben, wobei die Darstellung eindeutig ist, wenn man die Primzahlen der Größe nach ordnet.*

BEWEIS. Die Existenz der Primzahlzerlegung wurde bereits in Lemma 2.1.4 bewiesen. Zur Eindeutigkeit betrachten wir für $n \geq 1$ folgende Aussage: Sind $p_1, \ldots, p_n$ und $q_1, \ldots, q_k$ mit $k \geq n$ Primzahlen, sodass $p_1 \cdots p_n = q_1 \cdots q_k$ gilt, dann ist $k = n$ und die p_i unterscheiden sich von den q_j höchstens in der Reihenfolge. Wir beweisen diese Aussage durch Induktion nach n.

Für den Induktionsanfang ist $n = 1$, also haben wir Primzahlen p und $q_1, \ldots, q_k$ gegeben, sodass $p = q_1 \cdots q_k$ gilt. Dann ist q_1 ein Teiler von p und als Primzahl ist $q_1 > 1$, also $q_1 = p$ und damit auch $k = 1$.

Nehmen wir als Induktionsvoraussetzung an, dass die obige Aussage für je n Primzahlen p_i gilt und betracheten wir Primzahlen $p_1, \ldots, p_{n+1}$ und $q_1, \ldots, q_\ell$, sodass $p_1 \cdots p_{n+1} = q_1 \cdots q_\ell$ gilt. Dann teilt die Primzahl p_{n+1} das Produkt $q_1 \cdots q_\ell$, also gibt es ein i, sodass $p_{n+1} | q_i$ und damit $p_{n+1} = q_i$ gilt. Damit können wir aus $p_1 \cdots p_{n+1} = q_1 \cdots q_\ell$ sofort

$$p_1 \cdots p_n = q_1 \cdots q_{i-1} q_{i+1} \cdots q_\ell$$

folgern. Wendet man darauf die Induktionsvoraussetzung an, so folgt die Behauptung sofort. □