Universität Hamburg
DER FORSCHUNG | DER LEHRE | DER BILDUNG

Dr. Max Pitz
WS 2017/18

Grundlagen der Mathematik

Lemma von Euklid und Fundamentalsatz der Arithmetik

Lemma 1 (Lemma von Euklid)**.** *Es sei $p \in \mathbb{N}$, $p \geq 2$. Dann gilt:*

$$p \text{ ist genau dann eine Primzahl, wenn } \forall a, b \in \mathbb{N}(p|a \cdot b \Rightarrow p|a \vee p|b).$$

In Worten: Wenn eine Primzahl ein Produkt teilt, so teilt sie einen der Faktoren. Umgekehrt muss jede Zahl mit dieser Eigenschaft eine Primzahl sein.

Beweis. "$\Leftarrow$" Angenommen, m ist keine Primzahl. Dann existieren Teiler $1 < a, b < m$ von m mit $m = a \cdot b$. Also $m|a \cdot b$, aber weder $m|a$ noch $m|b$.

"$\Rightarrow$"Wir müssen zeigen, dass jede Primzahl p die Eigenschaft hat, dass wenn $p|a \cdot b$, dann $p|a$ oder $p|b$. Wir führen einen Widerspruchsbeweis. Angenommen, die Aussage ist falsch.

Erste Minimalitätsannahme: Sei p die kleinste Primzahl, für die die Aussage falsch ist.

Für dieses p gibt es also ein Produkt $n = a \cdot b$, so dass zwar $p|n$, aber $p \nmid a$ und $p \nmid b$.

Zweite Minimalitätsannahme: Sei n die kleinste solche Zahl.

Wir beweisen nun die folgenden zwei Hilfsbehauptungen:

Behauptung 1: Es gilt $a < p$ und $b < p$.

Denn falls $a > p$, so ergibt Division mit Rest $a = qp + r$ mit $0 < r < p$, und

$$a \cdot b = (qp + r)b = qpb + rb,$$

also

$$rb = a \cdot b - qpb.$$

Da p beide Zahlen der rechten Seite teilt, folgt dass p die linke Seite teilt. Dann wäre aber $n' = rb$ ein kleineres Produkt als n, im Widerspruch zur zweiten Minimalitätsannahme. Somit ist Behauptung 1 bewiesen.

Die Annahme $p|n = a \cdot b$ bedeutet, dass ein $q \in \mathbb{N}_0$ existiert mit $p \cdot q = a \cdot b$.

Behauptung 2: Es gilt $q = 1$.

Dann andernfalls gilt $q \geq 2$, und somit hat q einen Primteiler p', den wir aus der Gleichung $pq = a \cdot b$ rauskürzen können. Details: Wenn $p' \cdot m = q$ dann gilt $p' \leq q < p$. Aus der ersten Minimalitätsannahme folgt, dass für die kleinere Primzahl p' die Aussage von Euklids Lemma gilt. Da $p'|q$ und $q|a \cdot b$ folgt

$$p'|a \cdot b \Rightarrow p'|a \vee p'|b.$$

Ohne Einschränkung können wir annehmen, dass $p'|a$, also dass $p' \cdot q' = a$. Einsetzen in

$$p \cdot q = a \cdot b$$

liefert

$$p \cdot p' \cdot m = p' \cdot q' \cdot b.$$

Nach Kürzregel gilt also

$$p \cdot m = q' \cdot b.$$

Also teilt $p|q' \cdot b$. Aus der zweiten Minimalitätsannahme (da $q' \cdot b < a \cdot b$) folgt, dass $p|q'$ oder $p|b$, was, da $q'|a$, in beiden Fällen ein Widerspruch gibt. Somit ist Behauptung 2 bewiesen.

Mit $q = 1$ folgt aber, dass $p = a \cdot b$. Da p Primzahl, folgt dass $a = 1$ und $b = p$ oder umgekehrt. Also gilt Euklids Lemma doch für die Primzahl p. □

Theorem 2 (Fundamentalsatz der Arithmetik)**.** *Jede natürliche Zahl $n \geq 2$ hat eine – bis auf die Reihenfolge der Faktoren – eindeutige Primfaktorzerlegung.*

Beweis. Existenz der PFZ: Angenommen, es gibt Zahlen n, die keine PFZ haben. Sei n der kleinste Verbrecher. Die Zahl n hat einen Primfaktor p, also $p \cdot n' = n$. Da n der kleinste Verbrecher war, hat n' eine PFZ. Dann ist aber mit der zusätzlichen Primzahl p eine PFZ für n gefunden.

Eindeutigkeit der PFZ: Angenommen, $n \geq 2$ ist der kleinste Verbrecher, der zwei verschiedene PFZ hat, also

$$p_1 \cdot \ldots \cdot p_m = n = q_1 \cdot \ldots \cdot q_k.$$

Nach Euklids Lemma folgt aus $p_1 | q_1 \cdot \ldots \cdot q_k$ dass $p_1 | q_i$, also $p_1 = q_1$. Durch Umordnen können wir annehmen, dass $p_1 | q_1$. Da n der kleinste Verbrecher war, hat die Zahl

$$p_2 \cdot \ldots \cdot p_m = n' = q_2 \cdot \ldots \cdot q_k$$

eine – bis auf die Reihenfolge der Faktoren – eindeutige Primfaktorzerlegung, wir können also (nach Umsortierung) $p_i = q_i$ für alle $2 \leq i \leq m = k$ annehmen. Da $p_1 = q_1$ war dann aber auch die PFZen für n gleich. □