Zahlentheorie Primzahlen

Prof. Dr. Dörte Haftendorn, www.uni-lueneburg.de/mathe-lehramt Mai.05

Definition: Natürliche Zahlen mit genau zwei natürlichen Teilern heißen Primzahlen.

Genau die Primzahlen p haben keine echten Teiler, also keine Teiler t mit 1<t<p.

Hilfssatz: Jede natürliche Zahl n größer 1 hat mindestens einen Primteiler.

Bew: Es gibt, da $T_n\backslash\{1\}$ endlich ist, ein kleinstes Element m in $T_n\backslash\{1\}$. Ein echter Teiler von m wäre auch Teiler von n, also hat m keine echten Teiler, ist also Primteiler. q.e.d.

Fundamental-Lemma über Primzahlen:

Wenn eine Primzahl ein Produkt teilt, dann teilt sie mindestens einen Faktor.

Kurz: $p \ prim \ \wedge \ p \mid a \cdot b \Rightarrow \ p \mid a \ \vee \ \ p \mid b$

Bew.: Angenommen $p \nmid a \Rightarrow ggT(p,a) = 1 \Rightarrow \exists s,t \in Z: \ 1 = s \cdot p + t \cdot a$ als Linearkombination nach dem erweiterten Euklid-Algorithmus. Multipliation mit b ergibt $b = s \cdot p \cdot b + t \cdot a \cdot b = s \cdot p \cdot b + t \cdot p \cdot k = p \cdot (s \cdot b + t \cdot k)$ mit $k \in N \wedge (s \cdot b + t \cdot k) \in Z \Rightarrow p \mid b$. Es reicht, wenn p relativ prim zu a ~~und~~ oder b ist. q.e.d.

Fundamentalsatz der Zahlentheorie

Jede natürliche Zahl größer 1 hat eine eindeutige Primfaktor-Zerlegung, PFZ.

$n > 1, \Rightarrow \exists p_i \ prim \wedge \alpha_i \in N: \ n = \prod_i p_i^{\alpha_i}$ Die Primfaktoren und ihre Exponenten sind bis auf die Reihenfolge eindeutig bestimmt.

Beweis der Existenz: Angenommen es gibt Zahlen ohne PFZ, dann sei m die kleinste dieser Zahlen. Nach obigem Hilfssatz hat m einen Primteiler p und des gilt m=p m* und m*<m. Damit muss m* eine PFZ haben, denn m war ja minimal. p m* ist ein Produkt und somit hat m selbst eine PFZ im Widerspruch zur Annahme. q.e.d. (Existenz)

Beweis der Eindeutigkeit: Angenommen es existiert ein m mit nichteindeutiger PFZ und m sei minimal mit dieser Eigenschaft. Dann gilt $m = p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s$, Vielfachheiten ausgeschrieben. Fall 1: $p_1 = q_k \Rightarrow m = p_1 m^* = q_k m^{\sim} \ \| : p_1 \Rightarrow m^* = m^{\sim}$ Diese beiden Zahlen sind aber beide kleiner als m, haben daher eine eindeutige PFZ, sind also bei passender Sortierung völlig gleich. Damit ist auch die Zerlegung von m eindeutig, Widerspruch, q.e.d. (Fall1).

Fall 2: $p_1 \neq q_k \forall k \Rightarrow m = p_1 m^* = q_1 m^{\sim} \Rightarrow p_1 \mid m^{\sim}$ nach dem Fundamental-Lemma. Da wieder $m^{\sim}$ eine eindeutige PFZ hat, muss p_1 einer dier Primfaktoren sein und das ist ein Widerspruch zu $p_1 \neq q_k \forall k$. Also kann es gar kein solches m geben. q.e.d (Fall2 und Satz).

Satz (Euklid): Es gibt unendlich viele Primzahlen

Bew.: Angenommen es gibt nur endlich viele Primzahlen $p_1, p_2, \cdots, p_n$. Wir betrachten $m = p_1 p_2 \cdots p_n + 1$. Fall 1: m ist selbst prim. Wegen $m > p_i \ \forall i$ ist m dann eine neue Primpzahl und wir haben einen Widerspruch. Q.e.d.(Fall1)

Fall 2: m ist nicht selbst prim. Dann hat m nach dem Hilfssatz einen Primteiler q. Gilt nun $q = p_i$ für einen Index i, o.B.d.A. $q = p_1$, dann folgt $m = q \cdot k = p_1 p_2 \cdots p_n + 1$ und damit $q \cdot (k - p_2 \cdots p_n) = 1$, ein Widerspruch. Damit ist auch in diesem Fall eine neue Primzahl nötig und der Satz ist bewiesen.