Satz von Euklid

Es gibt mehr Primzahlen als jede vorgelegte Anzahl von Primzahlen – Buch IX, Proposition 20

Gibt es wirklich unendlich viele Primzahlen?

Diese Frage werden wir im Folgenden beantworten. Eine Primzahl ist eine natürliche Zahl, die größer als 1 ist und nur durch sich selbst und durch 1 teilbar ist. Die erste Primzahl ist also die 2.

Um heraus zu bekommen, ob es unendlich viele Primzahlen gibt, nehmen wir das Gegenteil an und versuchen einen Widerspruch in dieser Annahme zu finden. Da es nur entweder endlich viele oder unendlich viele Primzahlen geben kann, muss sich unsere Frage so beantworten lassen (Beweis durch Widerspruch, *reductio ad absurdum*).

Nehmen wir also an, es gebe nur endlich viele Primzahlen. Diese n Primzahlen können wir als folgende Liste darstellen

$$p_1, ..., p_n$$

Wenn wir diese Zahlen alle genau ein mal miteinander multiplizieren, erhalten wir eine weitere Zahl. Nennen wir diese Zahl m. Die Zahl m ist offensichtlich keine Primzahl. Aber die folgende Zahl, $m+1$, könnte eine Primzahl sein. Wenn sie jedoch eine Primzahl ist, gibt es eine Primzahl, die größer ist als p_n, nämlich $m+1$. Das ist ein Widerspruch. Wenn sie keine Primzahl ist, muss sie einen Teiler t besitzen, der eine Primzahl ist.

Warum ist das so?

Hilfssatz von Euklid: Teilt eine Primzahl p ein Produkt $a \cdot b$, so auch einen (oder beide) der Faktoren. – Buch VII, Proposition 30

Seien a und b 2 beliebige ganze Zahlen. Wir nehmen an eine Primzahl p teilt das Produkt $a \cdot b$, ist jedoch kein Teiler von a. Das heißt a und p sind teilerfremd. Daraus folgend müsste p ein Teiler von b sein. Es gibt also 2 ganze Zahlen k und l, die die Gleichung

$$k \cdot p + l \cdot a = 1$$

Diese Gleichung muss im Rahmen dieses Beweises leider *Magie* bleiben. Eine Erklärung liefert das Lemma von Bézout.

erfüllen. Diese Gleichung multiplizieren wir mit b. Umgeformt ergibt sich dann

$$p \cdot (k \cdot b) + l \cdot (a \cdot b) = b$$

Es gibt, laut unsere Annahme, eine ganze Zahl c für die $a \cdot b = c \cdot p$ gilt. Wir setzen ein und klammern aus

$$p \cdot (k \cdot b + c \cdot l) = b$$

Damit teilt die Primzahl p die ganze Zahl b, denn p ergibt im Produkt mit einer anderen ganzen Zahl die ganze Zahl b.

Damit haben wir gezeigt, dass sich jede ganze Zahl in Primzahlen zerlegen lässt (sog. Primfaktoren).

Nach unserer Annahme müsste t dann eine der Primzahlen von $p_1, ..., p_n$ sein. Damit ist t sowohl Teiler von m (das haben wir ja so definiert) und Teiler von $m+1$. Damit kann t nur 1 sein. Aber 1 gehört nicht zu den Primzahlen. Also haben wir für die beiden möglichen Fälle einen Widerspruch gefunden und die Annahme widerlegt.

Somit haben wir bewiesen, dass es unendlich viele Primzahlen gibt.

Die ersten Primzahlen sind übrigens 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97, 101, 103, 107, 109, 113, 127, 131, 137, 139, 149, 151, 157, 163, 167, 173, 179, 181, 191, 193, 197, 199, 211, 223, 227, 229, 233, 239, 241, 251, 257, 263, 269, 271,...