



# Mehr Mathematik

## Die Zerlegung einer natürlichen Zahl in Primfaktoren ist eindeutig

Eine natürliche Zahl lässt sich immer in ein Produkt von Primzahlen zerlegen. Das ist klar. Aber ist diese Zerlegung auch immer eindeutig? Es geht also um die Frage, ob es nicht auch natürliche Zahlen gibt, die sich in zwei unterschiedliche Produkte zerlegen lassen, wobei in beiden Produkten nur Primzahlen auftreten und diese Zerlegungen sich nicht nur durch die Reihenfolge der Faktoren, sondern auch durch unterschiedliche Primzahlen unterscheiden. Bei der Zahl 10 gibt es sicher nur eine Zerlegung:  $10 = 2 \cdot 5$ . Was ist aber mit größeren oder ganz großen Zahlen?

Ein spezielles Beispiel aus dem wunderschönen Buch *Zahlenzauber* von John Conway und Richard Guy:

$$1001 = 7 \cdot 143 = 11 \cdot 91$$

Die Faktoren sehen nach Primzahlen aus und man denkt, es sind zwei verschiedene Primfaktorzerlegungen; aber das täuscht:

$$143 = 11 \cdot 13 \text{ und } 91 = 7 \cdot 13$$

Die richtige Primfaktorzerlegung von 1001 lautet somit:

$$1001 = 7 \cdot 11 \cdot 13$$

Also war unser Beispiel gar keines. Und trotzdem: Stellen Sie sich eine natürliche Zahl mit 100 Stellen vor, wohl gemerkt – nicht die Zahl 100, sondern eine Zahl mit soviel Stellen. Sie schreiben ein Rechnerprogramm, das diese Zahl nach langer Laufzeit in Primfaktoren zerlegt. Ließe sich nicht ein anderes Programm schreiben, das dann auch ganz anders arbeitet und so zu einer anderen Primfaktorzerlegung kommt?

Der Fundamentalsatz der Arithmetik besagt:

*Jede natürliche Zahl lässt sich – abgesehen von der Reihenfolge der Faktoren – nur auf eine Weise in ein Produkt von Primzahlen zerlegen.*

Beweis:

Angenommen es gibt (mindestens) eine natürliche Zahl, die sich in zwei verschiedenen Arten in ein Produkt von Primzahlen zerlegen lässt. Dann betrachten wir – und das ist der zentrale Trick – die gesamte Menge aller dieser natürlichen Zahlen, die mehr als eine Primfaktorzerlegung haben. Als Teilmenge der natürlichen Zahlen hat diese Menge ein kleinstes Element, und das nennen wir  $n$ . Für  $n$  gilt also:

$$n = p_1 \cdot p_2 \cdot p_3 \cdot \dots \cdot p_k = q_1 \cdot q_2 \cdot q_3 \cdot \dots \cdot q_l$$

Dann müssen alle  $p_i$  von allen  $q_j$  verschieden sein. Denn wäre irgendein  $p_i$  gleich einem  $q_j$ , so würde man  $n$  durch diese Zahl teilen und hätte eine kleinere Zahl, die sich auf mindestens zwei Weisen in Primfaktoren zerlegen ließe; das geht aber nicht:  $n$  war ja schon die kleinste von diesen Zahlen. Also – kein  $p$  ist gleich einem  $q$ , und kein  $q$  ist gleich einem  $p$ .



Wir nehmen an,  $p_1$  ist der kleinste Primfaktor von allen p-Faktoren, dann gilt sicher  $p_1^2 \leq n$ , und analog  $q_1^2 \leq n$ . Dann folgt  $p_1^2 \cdot q_1^2 \leq n^2$  und somit  $p_1 \cdot q_1 \leq n$  wegen  $p_1 \neq q_1$ .

Nun gehen wir über zu der Zahl  $N = n - p_1 \cdot q_1$ , wobei natürlich  $0 < N < n$  gilt, so dass sich N nach Voraussetzung eindeutig in Primfaktoren zerlegen lässt.

Da  $p_1$  die Zahl n teilt, teilt  $p_1$  auch die Zahl N, kommt also in der Primfaktorzerlegung von N vor, da  $q_1$  die Zahl n teilt, teilt auch  $q_1$  die Zahl N und  $q_1$  kommt in der Zerlegung von N vor, also teilt  $p_1 \cdot q_1$  die Zahl N, und somit teilt  $p_1 \cdot q_1$  auch  $n = N + p_1 \cdot q_1$ . Wir teilen nun n durch  $p_1$ , setzen  $n_1 = \frac{n}{p_1}$  und sehen, dass natürlich  $q_1$  die Zahl  $n_1$  teilt. Da aber  $n_1$  kleiner als n ist, hat  $n_1$  eine eindeutige Zerlegung, und die kann nur  $p_2 \cdot p_3 \cdot \dots \cdot p_k$  sein. Da jedoch  $q_1$  keines der p sein kann, haben wir einen Widerspruch. Und somit hat jede natürliche Zahl eine eindeutige Primfaktorzerlegung.



Ich habe den Beweis in Anlehnung an Hardy/Wright, *An Introduction to the Theory of Numbers* formuliert. Er stammt vermutlich von dem deutschen Mathematiker Ernst Zermelo (1871-1953), siehe Bild, der vor allem durch die erste Formulierung des Auswahlaxioms berühmt wurde. Wenn man die Argumentation in Ruhe betrachtet, erkennt man vielleicht, dass dieser Beweis eine intellektuelle Kostbarkeit ist.

Die Zahl

123456789011121314151617181910212223242526272829

lässt sich also nur auf eine Art in Primzahlen zerlegen. Man erhält mit Derive nach 1606 Sekunden  
 $\dots = 71 \cdot 521 \cdot 27953 \cdot 178330035630135427 \cdot 669523745365973682449$

Stimmt das? Rechnet man mit Mathematica nach, so erhält man das gleiche Ergebnis.  
 (Der Urheber des Fotos ist Konrad Jacobs)

(nev)