Zu Euklids Primzahlsatz

Euklids Argument wird auch gegenüber Nichtmathematikern bedauerlicher Weise meistens so zitiert:

> Angenommen, es gibt nur endlich viele Primzahlen, dann kann man sie **alle** multiplizieren und 1 addieren. Die verwendeten Primzahlen teilen das Resultat nicht, sie lassen nämlich bei Division den Rest 1. Die Primzahlzerlegung des Resultats liefert daher eine oder mehrere **weitere** Primzahlen – Widerspruch.

Ich habe gelernt, dass die Griechen konstruktiver formuliert haben, nämlich: Zu jeder **endlichen** Menge von Primzahlen kann man mit Euklids Idee **weitere** finden. Statt eines indirekten Beweises mit unvorstellbar grossen Zahlen führt diese Formulierung auf eine reiche Spielwiese kleiner Beispiele:

Zu $\{2,3\}$ findet man: $2\cdot 3+1=7,$

zu $\{2,7\}$ findet man: $2\cdot 7+1=3\cdot 5.$

Für mit Zahlen Spielende ist -1 ein ebenso guter Rest $\neq 0$ wie $+1$, also

zu $\{2,5\}$ findet man: $2\cdot 5\pm 1=\{11,\ 3\cdot 3\}.$

Ausserdem erlaubt das Argument höhere Primzahlpotenzen:

Zu $\{2,3\}$ findet man auch: $2\cdot 2\cdot 3\cdot 3\pm 1=\{37,\ 5\cdot 7\}.$

Schön ist ferner, dass Euklids Argument nur die **Unzerlegbarkeit** der Primzahlen benutzt, die Eindeutigkeit der Primfaktorzerlegung wird nicht benötigt. Andererseits, wenn die eindeutige Primzahlzerlegung den Spielenden bekannt ist, so gibt es weitere Variationen:

Zu $\{2,\ \ 3,5\}$ findet man z.B. $3\cdot 5+\{2,2^2,2^3,2^4,2^5\}=\{17,19,23,31,47\}<7^2,$

Zu $\{2,3,\ \ 5,7\}$ findet man z.B. $5\cdot 7\pm\{2\cdot 3\}=\{41,29\},$

$5\cdot 7\pm\{2\cdot 2\cdot 3\}=\{47,23\},$ $\quad 5\cdot 7\pm\{2\cdot 3\cdot 3\}=\{53,17\}\quad <11^2.$

Ich glaube, dass diese konstruktive Variante für Unterhaltungen mit Schülern oder Nicht-Mathematikern besser geeignet ist, als der am Anfang zitierte indirekte Beweis.

Verwendet man **alle** Primzahlen $< N$, um eine Zahl $k<N^2$ wie eben darzustellen, so ist k nach Eratosthenes **sicher** Primzahl, weil durch keine Zahl $\leq\sqrt{k}$ teilbar. $N=5:$ $2\cdot 3\pm 1,\ 4\cdot 3\pm 1,\ 2\cdot 9\pm 1,\ 8\cdot 3-1<25.$ Danach bis 49 mit $\{2,3,5\}$ und bis 121 mit $\{2,3,5,7\}$. Aber es wird immer schwieriger, **alle** kleinen Primzahlen zu verwenden. Hier die Beispiele für $11^2<p<13^2$, in denen man $\{2,3,5,7,11\}$ verwenden muss:

$$\begin{array}{lll} 127=2\cdot 11+3\cdot 5\cdot 7, & 131=2\cdot 5\cdot 11+3\cdot 7, & 137=7\cdot 11+4\cdot 3\cdot 5,\\ 139=5\cdot 11+4\cdot 3\cdot 7, & 149=4\cdot 11+3\cdot 5\cdot 7, & 151=3\cdot 5\cdot 11-2\cdot 7,\\ 157=4\cdot 5\cdot 11-9\cdot 7, & 163=2\cdot 9\cdot 11-5\cdot 7, & 167=7\cdot 11+2\cdot 9\cdot 5. \end{array}$$

Diese Zahlen $<13^2$ sind Primzahlen, weil sie (offensichtlich) keine Faktoren <13 haben.

Bemerkung: Die Primzahlen unter 11^2 kann man mit den einfachen Teilbarkeitsregeln für $2,3,5$ identifizieren – mit nur zwei ernsthaften Ausnahmen: $7\cdot 13=91,\ 7\cdot 17=119.$

Zusatz: Eindeutigkeit der Primfaktorzerlegung

Beweis der Eindeutigkeit der Primfaktorisierung nach einer Anregung von Knuth Esser – ohne Benutzung des Algorithmus für den ggT. – *Zusatz: Das geht schon auf Hardy zurück!* Es sei $k \in \mathbb{N}$ die **kleinste** Zahl, die **keine** eindeutige Primzahlzerlegung hat, also

$$p_1 \cdots p_r = k = q_1 \cdots q_s,$$
$$p_i \neq q_j \text{ für alle } i \in \{1, \ldots, r\},\ j \in \{1, \ldots, s\} \text{ und } r, s \geq 2.$$

Alle Primzahlen p_i sind von den Primzahlen q_j verschieden, da man sonst die gleichen Faktoren kürzen könnte, im Widerspruch zur Minimalität von k. Ausserdem können wir annehmen, dass p_1, q_1 die kleinsten Faktoren in den beiden Produkten sind. Wir haben also $p_1 \leq p_i,\ q_1 \leq q_j$, für alle i, j.

Wie könnte man vorgehen, um zu zeigen, dass es so ein k nicht geben kann?

Wir werden aus den zwei Faktorisierungen von k eine **kleinere** Zahl k_1 mit zwei Faktorisierungen basteln und weil die Primfaktorzerlegung von Zahlen $< k$ eindeutig ist, werden wir folgern können, dass p_1 **nicht** von allen q_j verschieden ist – ein Widerspruch.

In der Tat, für die Zahl $k_1 := k - p_1 \cdot q_1 < k$ haben wir diese zwei Faktorisierungen:

$$k - p_1 \cdot q_1 = p_1 \cdot (p_2 \cdots p_r - q_1) = k_1 = q_1 \cdot (q_2 \cdots q_s - p_1),$$

in denen wegen $k_1 < k$ die Primfaktoren (bis auf die Reihenfolge) übereinstimmen müssen. Um nicht an negative Zahlen denken zu müssen, überprüfen wir zunächst $0 < k_1$: Weil p_1 und q_1 der jeweils kleinste Faktor in den beiden Faktorisierungen von k ist, haben wir $p_1, q_1 \leq \sqrt{k}$, also $p_1 \cdot q_1 \leq k$ und damit $0 \leq k_1$. Schliesslich folgt $k_1 > 0$, denn $p_1 \cdot q_1 = k$ hätte die Konsequenz $p_1 = \sqrt{k} = q_1$, im Widerspruch zu $p_1 \neq q_1$.
Zurück zur Hauptsache: Weil die Primzahlzerlegung von k_1 (bis auf die Reihenfolge der Faktoren) eindeutig ist, muss der erste Faktor links, also die (von q_1 verschiedene) Primzahl p_1, den zweiten Faktor rechts, also $(q_2 \cdots q_s - p_1)$, teilen. Daher teilt p_1 auch das Primzahlprodukt $q_2 \cdots q_s < k$ und folglich muss p_1, wieder wegen der Eindeutigkeit der Faktorisierung für Zahlen $< k$, mit einer der Primzahlen q_j übereinstimmen - im Widerspruch zu der Ausgangssituation, in der alle p_i von allen q_j verschieden sind.
Also kann es die kleinste Zahl k mit **nicht eindeutiger** Primfaktorisierung nicht geben. Anders ausgedrückt: die Faktorisierung ist eindeutig (bis auf die Reihenfolge und die Verteilung von Vorzeichen).
In einer Vorlesung Artins hiess diese Beweismethode: *Prinzip vom kleinsten Verbrecher.*